Algebraic Groups and Number Theory

This is Volume 139 in the
PURE AND APPLIED MATHEMATICS series

H. Bass, A. Borel, J. Moser, and S. -T. Yau, editors
Paul A. Smith and Samuel Eilenberg, founding editors

Algebraic Groups and Number Theory

Vladimir Platonov
Andrei Rapinchuk
Academy of Sciences
Belarus, Minsk

Translated by Rachel Rowen
Raanana, Israel

ACADEMIC PRESS, INC.
Harcourt Brace & Company, Publishers
Boston San Diego New York
London Sydney Tokyo Toronto

This book is printed on acid-free paper. ♾

ACADEMIC PRESS, INC.
1250 Sixth Avenue, San Diego, CA 92101-4311

United Kingdom Edition published by
ACADEMIC PRESS LIMITED
24–28 Oval Road, London NW1 7DX

Library of Congress Cataloging-in-Publication Data

Platonov, V. P. (Vladimir Petrovich), date–
[Algebraicheskie gruppy i teoriia chisel. English]
Algebraic goups and number theory / Vladimir Platonov, Andrei Rapinchuk ; translated by Rachel Rowen.
p. cm. — (Pure and applied mathematics ; v. 139)
Includes bibliographical references.
ISBN 0-12-558180-7 (acid free)
1. Algebraic number theory. 2. Linear algebraic groups.
I. Rapinchuk, Andrei. II. Title. III. Series: Pure and applied mathematics (Academic Press) ; 139.
QA3.P8 vol. 139
[QA247]
510 s—dc20
[512'.74] 92–35876
CIP

Printed in the United States of America
93 94 95 96 BB 9 8 7 6 5 4 3 2 1

Contents

Preface to the English Edition

After publication of the Russian edition of this book (which came out in 1991) some new results were obtained in the area; however, we decided not to make any changes or add appendices to the original text, since that would have affected the book's balanced structure without contributing much to its main contents.

As the editory fo the translation, A. Borel took considerable interest in the book. He read the first version of the translation and made many helpful comments. We also received a number of useful suggestions from G. Prasad. We are grateful to them for their help. We would also like to thank the translator and the publisher for their cooperation.

V. Platonov
A. Rapinchuk

Preface to the Russian Edition

This book provides the first systematic exposition in mathematical literature of the theory that developed on the meeting ground of group theory, algebraic geometry and number theory. This line of research emerged fairly recently as an independent area of mathematics, often called the arithmetic theory of (linear) algebraic groups. In 1967 A. Weil wrote in the foreword to *Basic Number Theory*: "In charting my course, I have been careful to steer clear of the arithmetical theory of algebraic groups; this is a topic of deep interest, but obviously not yet ripe for book treatment."

The sources of the arithmetic theory of linear algebraic groups lie in classical research on the arithmetic of quadratic forms (Gauss, Hermite, Minkowski, Hasse, Siegel), the structure of the group of units in algebraic number fields (Dirichlet), discrete subgroups of Lie groups in connection with the theory of automorphic functions, topology, and crystallography (Riemann, Klein, Poincaré and others). Its most intensive development, however, has taken place over the past 20 to 25 years. During this period reduction theory for arithmetic groups was developed, properties of adele groups were studied and the problem of strong approximation solved, important results on the structure of groups of rational points over local and global fields were obtained, various versions of the local-global principle for algebraic groups were investigated, and the congruence problem for isotropic groups was essentially solved.

It is clear from this far from exhaustive list of major accomplishments in the arithmetic theory of linear algebraic groups that a wealth of important material of particular interest to mathematicians in a variety of areas

has been amassed. Unfortunately, to this day the major results in this area have appeared only in journal articles, despite the long-standing need for a book presenting a thorough and unified exposition of the subject. The publication of such a book, however, has been delayed largely due to the difficulty inherent in unifying the exposition of a theory built on an abundance of far-reaching results and a synthesis of methods from algebra, algebraic geometry, number theory, analysis and topology. Nevertheless, we finally present the reader such a book.

The first two chapters are introductory and review major results of algebraic number theory and the theory of algebraic groups which are used extensively in later chapters. Chapter 3 presents basic facts about the structure of algebraic groups over locally compact fields. Some of these facts also hold for any field complete relative to a discrete valuation. The fourth chapter presents the most basic material about arithmetic groups, based on results of A. Borel and Harish-Chandra.

One of the primary research tools for the arithmetic theory of algebraic groups is adele groups, whose properties are studied in Chapter 5. The primary focus of Chapter 6 is a complete proof of the Hasse principle for simply connected algebraic groups, published here in definitive form for the first time. Chapter 7 deals with strong and weak approximations in algebraic groups. Specifically, it presents a solution of the problem of strong approximation and a new proof of the Kneser-Tits conjecture over local fields.

The classical problems of the number of classes in the genus of quadratic forms and of the class numbers of algebraic number fields influenced the study of class numbers of arbitrary algebraic groups defined over a number field. The major results achieved to date are set forth in Chapter 8. Most are attributed to the authors.

The results presented in Chapter 9 for the most part are new and rather intricate. Recently substantial progress has been made in the study of groups of rational points of algebraic groups over global fields. In this regard one should mention the works of Kneser, Margulis, Platonov, Rapinchuk, Prasad, Raghunathan and others on the normal subgroup structure of groups of rational points of anisotropic groups and the multiplicative arithmetic of skew fields, which use most of the machinery developed in the arithmetic theory of algebraic groups. Several results appear here for the first time. The final section of this chapter presents a survey of the most recent results on the congruence subgroup problem.

Thus this book touches on almost all the major results of the arithmetic theory of linear algebraic groups obtained to date. The questions related to the congruence subgroup problem merit exposition in a separate book, to which the authors plan to turn in the near future. It should be noted that many well-known assertions (especially in Chapters 5, 6, 7, and 9) are

presented with new proofs which tend to be more conceptual. In many instances a geometric approach to representation theory of finitely generated groups is effectively used.

In the course of our exposition we formulate a considerable number of unresolved questions and conjectures, which may give impetus to further research in this actively developing area of contemporary mathematics.

The structure of this book, and exposition of many of its results, was strongly influenced by V. P. Platonov's survey article, "Arithmetic theory of algebraic groups," published in *Uspekhi matematicheskikh nauk* (1982, No. 3, pp. 3–54). Much assistance in preparing the manuscript for print was rendered by O. I. Tavgen, Y. A. Drakhokhrust, V. V. Benyashch-Krivetz, V. V. Kursov, and I. I. Voronovich. Special mention must be made of the contribution of V. I. Chernousov, who furnished us with a complete proof of the Hasse principle for simply connected groups and devoted considerable time to polishing the exposition of Chapter 6. To all of them we extend our sincerest thanks.

V. P. Platonov
A. S. Rapinchuk

1. Algebraic number theory

The first two sections of this introductory chapter provide a brief overview of several concepts and results from number theory. A detailed exposition of these problems may be found in the works of Lang [2] and Weil [6] (cf. also Chapters 1–3 of ANT). It should be noted that, unlike such mathematicians as Weil, we have stated results here only for algebraic number fields, although the overwhelming majority of results also hold for global fields of characteristic > 0, i.e., fields of algebraic functions over a finite field. In §1.3 we present results about group cohomology, necessary for understanding the rest of the book, including definitions and statements of the basic properties of noncommutative cohomology. Sections 1.4–1.5 contain major results on simple algebras over local and global fields. Special attention is given to research on the multiplicative structure of division algebras over these fields, particularly the triviality of the Whitehead groups. Moreover, in §1.5 we collect useful results on lattices over vector spaces and orders in semisimple algebras.

The rest of the book presupposes familiarity with field theory, especially Galois theory (finite and infinite), as well as with elements of topological algebra, including the theory of profinite groups.

1.1. Algebraic number fields, valuations, and completions.

1.1.1. Arithmetic of algebraic number fields. Let K be an algebraic number field, i.e., a finite extension of the field $\mathbb{Q}$, and $\mathcal{O}_K$ the ring of integers of K. $\mathcal{O}_K$ is a classical object of interest in algebraic number theory. Its structure and arithmetic were first studied by Gauss, Dedekind, Dirichlet and others in the previous century, and continue to interest mathematicians today. From a purely algebraic point of view the ring $\mathcal{O} = \mathcal{O}_K$ is quite straightforward: if $[K : \mathbb{Q}] = n$, then $\mathcal{O}$ is a free $\mathbb{Z}$-module of rank n. For any nonzero ideal $\mathfrak{a} \subset \mathcal{O}$ the quotient ring $\mathcal{O}/\mathfrak{a}$ is finite; in particular, any prime ideal is maximal. Rings with such properties (i.e., noetherian, integrally closed, with prime ideals maximal) are known as Dedekind rings. It follows that any nonzero ideal $\mathfrak{a} \subset \mathcal{O}$ can be written uniquely as the product of prime ideals: $\mathfrak{a} = \mathfrak{p}^{\alpha_1} \dots \mathfrak{p}^{\alpha_r}$. This property is a generalization of the fundamental theorem of arithmetic on the uniqueness (up to associates) of factorization of any integer into a product of prime numbers. Nevertheless, the analogy here is not complete: unique factorization of the elements of $\mathcal{O}$ to prime elements, generally speaking, does not hold. This fact, which demonstrates that the arithmetic of $\mathcal{O}$ can differ significantly from the arithmetic of $\mathbb{Z}$, has been crucial in shaping the problems of algebraic number theory. The precise degree of deviation is measured by the ideal class group (previously called the divisor class

group) of K. Its elements are fractional ideals of K, i.e., $\mathcal{O}$-submodules $\mathfrak{a}$ of K, such that $x\mathfrak{a} \subset \mathcal{O}$ for a suitable nonzero x in $\mathcal{O}$. Define the product of two fractional ideals $\mathfrak{a}$, $\mathfrak{b} \subset \mathcal{O}$ to be the $\mathcal{O}$-submodule in K generated by all xy, where $x \in \mathfrak{a}$, $y \in \mathfrak{b}$. With respect to this operation the set of fractional ideals becomes a group, which we denote $\mathrm{Id}(\mathcal{O})$, called the *group of ideals* of K. The principal fractional ideals, i.e., ideals of the form $x\mathcal{O}$ where $x \in K^*$, generate the subgroup $P(\mathcal{O}) \subset \mathrm{Id}(\mathcal{O})$, and the factor group $\mathrm{Cl}(\mathcal{O}) = \mathrm{Id}(\mathcal{O})/P(\mathcal{O})$ is called the *ideal class group of* K. A classic result, due to Gauss, is that the group $\mathrm{Cl}(\mathcal{O})$ is always finite; its order, denoted by h_K, is the class number of K. Moreover, the factorization of elements of $\mathcal{O}$ into primes is unique if and only if $h_K = 1$. Another classic result (Dirichlet's unit theorem) establishes that the group of invertible elements of $\mathcal{O}^*$ is finitely generated. These two facts are the starting point for the arithmetic theory of algebraic groups (cf. Preface). However generalizing classical arithmetic to algebraic groups we cannot appeal to ring-theoretic concepts, but rather we develop such number theoretic constructions as valuations, completions, and also adeles and ideles, etc.

1.1.2. Valuations and completions of algebraic number fields. We define a *valuation of* K to be a function $|\ |_v : K \to \mathbb{R}$ satisfying the following conditions for all x, y in K:

(1) $|x|_v \geq 0$, with $|x|_v = 0$ iff $x = 0$;
(2) $|xy|_v = |x|_v|y|_v$;
(3) $|x + y|_v \leq |x|_v + |y|_v$.

If we replace condition 3 by the stronger condition

(3′) $|x + y|_v \leq max\{|x|_v, |y|_v\}$

then the valuation is called *non-archimedean*; if not, it is *archimedean*.

An example of a valuation is the *trivial* valuation, defined as follows: $|x|_v = 1$ for all x in K^*, and $|0|_v = 0$. We shall illustrate nontrivial valuations for the case $K = \mathbb{Q}$. The ordinary absolute value $|\ |_\infty$ is an archimedean valuation. Also, each prime number p can be associated with a valuation $|\ |_p$, which we call the *p-adic* valuation. More precisely, writing any rational number $\alpha \neq 0$ in the form $p^r \cdot \beta/\gamma$, where $r, \beta, \gamma \in \mathbb{Z}$ and β and γ are not divisible by p, we write $|\alpha|_p = p^{-r}$ and $|0|_p = 0$. Sometimes, instead of the p-adic valuation $|\ |_p$, it is convenient to use the corresponding logarithmic valuation $v = v_p$, defined by the formula $v(\alpha) = r$ and $v(0) = -\infty$, so that $|\alpha|_p = p^{-v(\alpha)}$. Axiomatically v is given by the following conditions:

(1) $v(x)$ is an element of the additive group of rational integers (or another ordered group) and $v(0) = -\infty$;

(2) $v(xy) = v(x) + v(y)$;
(3) $v(x + y) \geq \min\{v(x), v(y)\}$.

We shall use both ordinary valuations, as well as corresponding logarithmic valuations, and from the context it will be clear which is being discussed.

It is worth noting that the examples cited actually exhaust all the non-trivial valuations of $\mathbb{Q}$.

THEOREM 1.1 (OSTROWSKI). *Any non-trivial valuation of* $\mathbb{Q}$ *is equivalent either to the archimedean valuation* $|\ |_\infty$ *or to a p-adic valuation* $|\ |_p$.

(Recall that two valuations $|\ |_1$ and $|\ |_2$ on K are called *equivalent* if they induce the same topology on K; in this case $|\ |_1 = |\ |_2^\lambda$ for a suitable real $\lambda > 0$).

Thus, restricting any non-trivial valuation $|\ |_v$ of an algebraic number field K to $\mathbb{Q}$, we obtain either an archimedean valuation $|\ |_\infty$ (or its equivalent) or a p-adic valuation. (It can be shown that the restriction of a non-trivial valuation is always non-trivial.) Thus any non-trivial valuation of K is obtained by extending to K one of the valuations of $\mathbb{Q}$. On the other hand, for any algebraic extension L/K, any valuation $|\ |_v$ of K can be extended to L, i.e., there exists a valuation $|\ |_w$ of L (denoted $w|v$) such that $|x|_w = |x|_v$ for all x in K. In particular, proceeding from the given valuations of $\mathbb{Q}$ we can obtain valuations of an arbitrary number field K. Let us analyze the extension procedure in greater detail. To begin with, it is helpful to introduce the completion K_v of K with respect to a valuation $|\ |_v$. If we look at the completion of K as a metric space with respect to the distance arising from the valuation $|\ |_v$, we obtain a complete metric space K_v which becomes a field under the natural operations and is complete with respect to the corresponding extension of $|\ |_v$, for which we retain the same notation. It is well known that if L is an algebraic extension of K_v (and, in general, of any field which is complete with respect to the valuation $|\ |_v$), then $|\ |_v$ has a unique extension $|\ |_w$ to L. Using the existence and uniqueness of the extension, we shall derive an explicit formula for $|\ |_w$, which can be taken for a definition of $|\ |_w$. Indeed, $|\ |_v$ extends uniquely to a valuation of the algebraic closure $\bar{K}_v$. It follows that $|\sigma(x)|_w = |x|_w$ for any x in $\bar{K}_v$ and any σ in $Gal\,(\bar{K}_v/K_v)$. Now let L/K_v be a finite extension of degree n and $\sigma_1, \ldots, \sigma_n$ various embeddings of L in $\bar{K}_v$ over K_v. Then for any a in L and its norm $N_{L/K}(a)$ we have $|N_{L/K}(a)|_v = |\prod_{i=1}^{n} \sigma_i(a)|_v = \prod_{i=1}^{n} |\sigma_i(a)|_w = |a|_w^n$. As a result we have the following explicit description of the extension $|\ |_w$

$$|a|_w = |N_{L/K}(a)|_v^{1/n} \quad \text{for any } a \text{ in } L. \tag{1.1}$$

Now let us consider extensions of valuations to a finite extension L/K, where K is an algebraic number field. Let $|\ |_v$ be a valuation of K and $|\ |_w$ its unique extension to the algebraic closure $\bar{K}_v$ of K_v. Then for any embedding $\tau : L \to \bar{K}_v$ over K (of which there are n, where $n = [L : K]$), we can define a valuation u over L, given by $|x|_u = |\tau(x)|_w$, which clearly extends the original valuation $|\ |_v$ of K. In this case the completion L_u can be identified with the compositum $\tau(L)K_v$. Moreover, any extension may be obtained in this way, and two embeddings $\tau_1, \tau_2 : L \to \bar{K}_v$ give the same extension if they are conjugate over K_v, i.e., if there exists λ in $Gal\,(\bar{K}_v/K_v)$ with $\tau_2 = \lambda\tau_1$. In other words, if $L = K(\alpha)$ and $f(t)$ is the irreducible polynomial of α over K, then the extensions $|\ |_{u_1}, \ldots, |\ |_{u_r}$ of $|\ |_v$ over L are in 1 : 1 correspondence with the irreducible factors of f over K_v, viz. $|\ |_{u_i}$ corresponds to $\tau_i : L \to \bar{K}_v$ sending α to a root of f_i. Further, the completion L_{u_i} is the finite extension of K_v generated by a root of f_i. It follows that

$$L \bigotimes_K K_v \simeq \bigoplus_{i=1}^{r} L_{u_i}; \tag{1.2}$$

in particular $[L : K]$ is the sum of all the local degrees $[L_{u_i} : K_v]$.

Moreover, one has the following formulas for the norm and the trace of an element a in L:

$$\begin{aligned} N_{L/K}(a) &= \prod_{u|v} N_{L_u/K_v}(a), \\ \mathrm{Tr}_{L/K}(a) &= \sum_{u|v} \mathrm{Tr}_{L_u/K_v}(a). \end{aligned} \tag{1.3}$$

Thus the set V^K of all pairwise inequivalent valuations of K (or, to put it more precisely, of the equivalence classes of valuations of K) is the union of the finite set V_∞^K of the archimedean valuations, which are the extensions to K of $|\ |_\infty$, the ordinary absolute value, on $\mathbb{Q}$, and the set V_f^K of non-archimedean valuations obtained as extensions of the p-adic valuation $|\ |_p$ of $\mathbb{Q}$, for each prime number p. The archimedean valuations correspond to embeddings of K in $\mathbb{R}$ or in $\mathbb{C}$, and are respectively called *real* or *complex valuations* (their respective completions being $\mathbb{R}$ or $\mathbb{C}$). If $v \in V_\infty^K$ is a real valuation, then an element α in K is said to be *positive* with respect to v if its image under v is a positive number. Let s (respectively t) denote the number of real (respectively pairwise nonconjugate complex) embeddings of K. Then $s + 2t = n$ is the dimension of L over K.

Non-archimedean valuations lead to more complicated completions. To wit, if $v \in V_f^K$ is an extension of the p-adic valuation, then the completion

K_v is a finite extension of the field $\mathbb{Q}_p$ of p-adic numbers. Since $\mathbb{Q}_p$ is a locally compact field, it follows that K_v is locally compact (with respect to the topology determined by the valuation).[1] The closure of the ring of integers $\mathcal{O}$ in K_v is the *valuation ring* $\mathcal{O}_v = \{a \in K_v : |a|_v \leq 1\}$, sometimes called the ring of v-adic integers. $\mathcal{O}_v$ is a local ring with a maximal ideal $\mathfrak{p}_v = \{\, a \in K_v : |a|_v < 1 \,\}$ (called the *valuation ideal*) and the group of invertible elements $U_v = \mathcal{O}_v \setminus \mathfrak{p}_v = \{\, a \in K_v : |a|_v = 1 \,\}$. It is easy to see that the valuation ring of $\mathbb{Q}_p$ is the ring of p-adic integers $\mathbb{Z}_p$, and the valuation ideal is $p\mathbb{Z}_p$. In general $\mathcal{O}_v$ is a free module over $\mathbb{Z}_p$, whose rank is the dimension $[K_v : \mathbb{Q}_p]$, so $\mathcal{O}_v$ is an open compact subring of K_v. Moreover, the powers $\mathfrak{p}_v^i$ of $\mathfrak{p}_v$ form a system of neighborhoods of zero in $\mathcal{O}_v$. The quotient ring $k_v = \mathcal{O}_v/\mathfrak{p}_v$ is a finite field and is called the *residue field* of v. $\mathfrak{p}_v$ is a principal ideal of $\mathcal{O}_v$; any of its generators π is called a *uniformizing parameter* and is characterized by $v(\pi)$ being the (positive) generator of the value group $\Gamma = v(K_v^*) \simeq \mathbb{Z}$. Once we have established a uniformizing parameter π, we can write any a in K_v^* as $a = \pi^r u$, for suitable $u \in U_v$; this yields a continuous isomorphism $K_v^* \simeq \mathbb{Z} \times U_v$, given by $a \mapsto (r, u)$, where $\mathbb{Z}$ is endowed with the discrete topology. Thus, to determine the structure of K_v^* we need only describe U_v. It can be shown quite simply that U_v is a compact group, locally isomorphic to $\mathcal{O}_v$. It follows that $U_v \simeq F \times \mathbb{Z}_p^n$, where $n = [K_v : \mathbb{Q}_p]$, and F is the group of all roots of unity in K_v. Thus $K_v^* \simeq \mathbb{Z} \times F \times \mathbb{Z}_p^n$.

Two important concepts relating to field extensions are the ramification index and the residue degree. We introduce these concepts first for the local case. Let L_w/K_v be a finite n-dimensional extension. Then the value group $\Gamma_v = v(K_v^*)$ has finite index in $\Gamma_w = w(L_w^*)$, and the corresponding index $e(w|v) = [\Gamma_w : \Gamma_v]$ is called the *ramification index*. The residue field $l_w = \mathcal{O}_{L_w}/\mathfrak{P}_{L_w}$ for L_w is a finite extension of the residue field k_v, and $f(w|v) = [l_w : k_v]$ is the *residue degree*. Moreover $e(w|v)f(w|v) = n$. An extension for which $e(w|v) = 1$ is called *unramified* and an extension for which $f(w|v) = 1$, is called *totally ramified*.

Now let L/K be a finite n-dimensional extension over an algebraic number field. Then for any valuation v in V_f^K and any extension w to L, the ramification index $e(w|v)$ and residue degree $f(w|v)$ are defined respectively as the ramification index and residue degree for the extension of the completions L_w/K_v. (One can also give an intrinsic definition based on

[1] Henceforth completions of a number field with respect to non-trivial valuations are called *local fields*. It can be shown that the class of local fields thus defined coincides with the class of non-discrete locally compact fields of characteristic zero. We note also that we shall use the term local field primarily in connection with non-archimedean completions, and to stress this property will say *non-archimedean local field*.

the value groups $\tilde{\Gamma}_v = v(K^*)$, $\tilde{\Gamma}_w = w(L^*)$ and the residue fields

$$\tilde{k}_w = \mathcal{O}_K(v)/\mathfrak{p}_K(v), \qquad \tilde{l}_w = \mathcal{O}_L(w)/\mathfrak{P}_L(w),$$

where $\mathcal{O}_K(v)$, $\mathcal{O}_L(w)$ are the valuation rings of v and w in K and L, and $\mathfrak{p}_K(v)$, $\mathfrak{P}_L(w)$ are the respective valuation ideals, but in fact $\tilde{\Gamma}_v = \Gamma_v$, $\tilde{\Gamma}_w = \Gamma_w$, $\tilde{k}_v = k_v$ and $\tilde{l}_w = l_w$.) $[L_w : K_v] = e(w|v)f(w|v)$. Thus, if $w_1, \dots, w_r$ are all the extensions of v to L, then

$$\sum_{i=1}^{r} e(w_i|v)f(w_i|v) = \sum_{i=1}^{r} [L_{w_i} : K_v] = n.$$

Generally speaking $e(w_i|v)$ and $f(w_i|v)$ may differ for different i, but there is an important case when they are the same; namely, when L/K is a Galois extension. Let $\mathcal{G}$ denote its Galois group. Then all extensions $w_1, \dots, w_r$ of v to L are conjugate under $\mathcal{G}$, i.e., for any $i = 1, \dots, r$ there exists σ_i in $\mathcal{G}$ such that $w_i(x) = w_1(\sigma_i(x))$ for all x in L. It follows that $e(w_i|v)$ and $f(w_i|v)$ are independent of i (we shall write them merely as e and f); moreover the number of different extensions r is the index $[\mathcal{G} : \mathcal{G}(w_1)]$ of the *decomposition group* $\mathcal{G}(w_1) = \{\sigma \in \mathcal{G} : w_1(\sigma x) = w_1(x)$ for all x in $L\}$. Consequently $efr = n$, and $\mathcal{G}(w_1)$ is the Galois group of the corresponding extension L_{w_1}/K_v of the completions.

1.1.3. Unramified and totally ramified extension fields.

Let $v \in V_f^K$ and assume the associated residue field k_v is the finite field F_q of q elements.

PROPOSITION 1.1. *For any integer $n \geq 1$ there exists a unique unramified n-dimensional extension L/K_v. It is generated over K_v by all the $(q^n - 1)$-roots of unity, and therefore is a Galois extension. Sending $\sigma \in \mathrm{Gal}(L/K_v)$ to the corresponding $\bar{\sigma} \in \mathrm{Gal}(l/k_v)$, where $l \simeq F_{q^n}$ is the residue field of L, induces an isomorphism of the Galois groups $\mathrm{Gal}(L/K_v) \simeq \mathrm{Gal}(l/k_v)$.*

In defining $\bar{\sigma}$ corresponding to $\sigma \in \mathrm{Gal}(L/K_v)$ we note that the valuation ring $\mathcal{O}_L$ and its valuation ideal $\mathfrak{P}_L$ are invariant under σ and thus σ induces an automorphism $\bar{\sigma}$ of the residue field $l = \mathcal{O}_L/\mathfrak{P}_L$. Note further, that $\mathrm{Gal}(l/k_v)$ is cyclic and is generated by the Frobenius automorphism given by $\varphi(x) = x^q$ for all x in k_v; the corresponding element of $\mathrm{Gal}(L/K_v)$ is also called the Frobenius automorphism (of the extension L/K_v) and is written as $\mathrm{Fr}(L/K_v)$.

The norm properties of unramified extensions give

PROPOSITION 1.2. *Let L/K_v be an unramified extension. Then $U_v = N_{L/K}(U_L)$; in particular $U_v \subset N_{L/K_v}(L^*)$.*

PROOF: We base our argument on the canonical filtration of the group of units, which is useful in other cases as well. Namely, for any integer $i \geq 1$ let $U_v^{(i)} = 1 + \mathfrak{p}_v^i$ and $U_L^{(i)} = 1 + \mathfrak{P}_L^i$. It is easy to see that these sets are open subgroups and actually form bases of the neighborhoods of the identity in U_v and U_L respectively. We have the following isomorphisms:

$$U_v/U_v^{(1)} \simeq k_v^*, \quad U_v^{(i)}/U_v^{(i+1)} \simeq k_v^+, \quad \text{for } i \geq 1. \tag{1.4}$$

(The first isomorphism is induced by the reduction modulo $\mathfrak{p}_v$ map $a \mapsto a \pmod{\mathfrak{p}_v}$; to obtain the second isomorphism we fix a uniformizing parameter π of K_v, and then take $1 + \pi^i a \mapsto a \pmod{\mathfrak{p}_v}$.

Similarly

$$U_L/U_L^{(1)} \simeq l^*, \quad U_L^{(i)}/U_L^{(i+1)} \simeq l^+, \quad \text{for } i \geq 1. \tag{1.5}$$

Since L/K_v is unramified, π is also a uniformizing parameter of L, and in what follows we shall also be assuming that the second isomorphism in (1.5) is defined by means of π. For a in U_L we have (with bar denoting reduction modulo $\mathfrak{P}_L$)

$$\overline{N_{L/K_v}(a)} = \overline{\prod_{\sigma \in \mathrm{Gal}(L/K_v)} \sigma(a)} = \prod_{\tau \in \mathrm{Gal}(l/k_v)} \tau(\bar{a}) = N_{l/k_v}(\bar{a}).$$

Thus the norm map induces a homomorphism $U_L/U_L^{(1)} \to U_v/U_v^{(1)}$, which with identifications (1.4) and (1.5) is N_{l/k_v}. Further, for any $i \geq 1$ and any a in $\mathcal{O}_L$ we have

$$N_{L/K_v}(1+\pi^i a) = \prod_{\sigma \in \mathrm{Gal}(L/K_v)} \sigma(1+\pi^i a) \equiv 1 + \pi^i \operatorname{Tr}_{L/K_v}(a) \pmod{\mathfrak{P}_v^{(i+1)}}.$$

It follows that N_{L/K_v} induces homomorphisms $U_L^{(i)}/U_L^{(i+1)} \to U_v^{(i)}/U_v^{(i+1)}$, which with identifications (1.4) and (1.5) is the trace map Tr_{l/k_v}. But the norm and trace are surjective for extensions of finite fields; therefore the group $W = N_{L/K_v}(U_L)$ satisfies $U_v = WU_v^{(i)}$ for all $i \geq 1$. Since $U_v^{(i)}$ form a base of neighborhoods of identity, the above condition means that W is dense in U_v. On the other hand, since U_L is compact and the norm is continuous, it follows that W is closed, and therefore $W = U_v$. Q.E.D.

The proof of Proposition 2 also yields

COROLLARY. *If L/K_v is an unramified extension, then $N_{L/K_v}(U_L^{(i)}) = U_v^{(i)}$ for any integer $i \geq 1$.*

We need one more assertion concerning the properties of the filtration in the group of units under the norm map, in arbitrary extensions.

PROPOSITION 1.3. *For any finite extension L/K_v we have*

(1) $U_v^{(1)} \cap N_{L/K_v}(L^*) = N_{L/K_v}(U_L^{(1)})$;
(2) *if e is the ramification index of L/K_v, then for any integer $i \geq 1$ we have $N_{L/K_v}(U_L^{(i)}) \subset U_v^{(j)}$, where j is the smallest integer $\geq i/e$.*

PROOF: We begin with the second assertion. Let M be a Galois extension of K_v containing L. Then for a in L, $N_{L/K}(a) = \prod_\sigma \sigma(a)$, where the product is taken over all embeddings $\sigma : L \hookrightarrow M$ over K_v. Since in the local case v extends to a unique valuation w on L, it follows that $w(a) = w(\sigma(a))$ for any a in L and any σ; in particular, if we choose a uniformizing parameter π_L in L we have $\sigma(\pi_L) = \pi_L b_\sigma$ for suitable b_σ in U_M. It follows that for $a = 1 + \pi_L^i c \in U_L^{(i)}$ we have

$$N_{L/K_v}(a) = \prod_\sigma \sigma(1 + \pi_L^i c) = \prod_\sigma (1 + \pi_L^i b_\sigma^i \sigma(c)) \in (1 + \pi_L^i \mathcal{O}_M) \cap K_v.$$

But from our definition of the ramification index we have $\mathfrak{p}_v \mathcal{O}_L = \mathfrak{P}_L^e$, so that $\pi_L^i \mathcal{O}_M \cap K_v = \pi_L^i \mathcal{O}_L \cap K_v = \mathfrak{P}_L^i \cap \mathcal{O}_v \subset \mathfrak{p}_v^j$ (where j is chosen as indicated in the assertion) and $N_{L/K_v}(a) \in U_v^{(j)}$. In particular $N_{L/K_v}(U_L^{(1)}) \subset U_v^{(1)}$; therefore to prove the first assertion we must show that $U_v^{(1)} \cap N_{L/K_v}(L^*) \subset N_{L/K_v}(U_L^{(1)})$. Let $a \in L^*$ and $N_{L/K_v}(a) \in U_v^{(1)}$. Then (1.1) implies $a \in U_L$. Isomorphism (1.5) shows that $U_L^{(1)}$ is a maximal pro-p-subgroup in U_L for the prime p corresponding to the valuation v, from which it follows that $U_L \simeq U_L/U_L^{(1)} \times U_L^{(1)}$. In particular, $a = bc$ where $c \in U_L^{(1)}$ and b is an element of finite order coprime to p. We have $d = N_{L/K_v}(b) = N_{L/K_v}(a) N_{L/K_v}(c)^{-1} \in U_v^{(1)}$. Any element of finite order taken from $U_v^{(1)}$ has order a power of p; on the other hand, the order of d is a divisor of the order of b and hence is coprime to p. Thus $d = 1$ and $N_{L/K_v}(a) = N_{L/K_v}(c) \in N_{L/K_v}(U_L^{(1)})$. Q.E.D.

Now we return to the unramified extensions of K_v. It can be shown that the composite of unramified extensions is unramified; hence there exists a maximal unramified extension K_v^{nr} of K_v, which is Galois, and $\mathrm{Gal}(K_v^{nr}/K_v)$ is isomorphic to the Galois group $\mathrm{Gal}(\bar{k}_v/k_v)$ of the algebraic closure of the residue field k_v, i.e., is isomorphic to $\hat{\mathbb{Z}}$, the profinite completion of the infinite cyclic group whose generator is the Frobenius automorphism.

Let L/K be a finite extension of a number field K. We know that almost all valuations v in V_f^K are unramified in K, i.e., the corresponding extension of the completions L_w/K_v is unramified for any $w|v$; in particular, the Frobenius automorphism $\mathrm{Fr}(L_w/K_v)$ is defined. If L/K is a Galois extension, then, as we have noted, $\mathrm{Gal}(L_w/K_v)$ can be identified with the decomposition group $\mathcal{G}(w)$ of the valuation in the Galois group $\mathcal{G} = \mathrm{Gal}(L/K)$, so $\mathrm{Fr}(L_w/K_v)$ may be viewed as an element of $\mathcal{G}$.

We know that any two valuations w_1, w_2 extending v are conjugate under $\mathcal{G}$, from which it follows that the Frobenius automorphisms $\mathrm{Fr}(L_w/K_v)$ corresponding to *all* extensions of v form a conjugacy class $F(v)$ in $\mathcal{G}$. But does this produce all the conjugacy classes in $\mathcal{G}$? In other words, for any σ in $\mathcal{G}$ is there a valuation v in V_f^K such that for suitable $w|v$ the extension L_w/K_v is unramified and $\mathrm{Fr}(L_w/K_v) = \sigma$?

THEOREM 1.2 (CHEBOTAREV). *Let L/K be a finite Galois extension with Galois group $\mathcal{G}$. Then, for any σ in $\mathcal{G}$ there are infinitely many v in V_f^K such that for suitable $w|v$ the extension L_w/K_v is unramified and $\mathrm{Fr}(L_w/K_v) = \sigma$. In particular, there exist infinitely many v such that $L_w = K_v$, i.e., $L \subset K_v$.*

Actually Chebotarev defined a quantitative measure (density) of the set of v in V_f^K such that the conjugacy class $F(v)$ is a given conjugacy class $C \subset \mathcal{G}$. The density is equal to $[C]/[\mathcal{G}]$ (and the density of the entire set V_f^K is thereby 1). Therefore, Theorem 1.2 (more precisely, the corresponding assertion about the density) is called the Chebotarev Density Theorem. For cyclic extensions of $K = \mathbb{Q}$ it is equivalent to Dirichlet's theorem on prime numbers in arithmetic progressions. We note, further, that the last part of Theorem 1.2 can be proven indirectly, without using analytical methods.

Using geometric number theory one can prove

THEOREM 1.3 (HERMITE). *If $K/\mathbb{Q}$ is a finite extension, unramified relative to all primes p (i.e., $K_v/\mathbb{Q}_p$ is unramified for all p and all $v|p$), then $K = \mathbb{Q}$.*

We will not present a detailed analysis of totally ramified extensions (in particular, the distinction between weakly and strongly ramified extensions) at this point, but will limit ourselves to describing them using Eisenstein polynomials. Recall that a polynomial $e(t) = t^n + a_{n-1}t^{n-1} + \ldots + a_0 \in K_v[t]$ is called an *Eisenstein polynomial* if $a_i \in \mathfrak{p}_v$ for all $i = 0, \ldots, n-1$ and $a_0 \notin \mathfrak{p}_v^2$. It is well known that an Eisenstein polynomial is irreducible in $K_v[t]$.

PROPOSITION 1.4. *If Π is the root of an Eisenstein polynomial $e(t)$, then $L = K_v[\Pi]$ is a totally ramified extension of K_v with uniformizing parameter Π. Conversely, if L/K_v is totally ramified and Π is a uniformizing*

parameter of L then $L = K_v[\Pi]$ and the minimal polynomial of Π over K_v is an Eisenstein polynomial.

COROLLARY. *If L/K_v is totally ramified, then $N_{L/K_v}(L^*)$ contains a uniformizing parameter of K_v.*

The *ramification groups* $\mathcal{G}^i$ ($i \geq 0$), subgroups of $\mathcal{G}$, are helpful in studying ramification in a Galois extension L/K with Galois group $\mathcal{G}$. If $w|v$, then by definition $\mathcal{G}^0$ is the decomposition group $\mathcal{G}(w)$ of w, which can be identified with the local Galois group $\mathrm{Gal}(L_w/K_v)$. Next,

$$\mathcal{G}^{(1)} = \{\, \sigma \in \mathcal{G}^{(0)} : \sigma(a) \equiv a \pmod{\mathfrak{P}_{L_w}} \text{ for all } a \in \mathcal{O}_{L_w} \,\}$$

is the *inertia group*. It is the kernel of the homomorphism $\mathrm{Gal}(L_w/K_v) \to \mathrm{Gal}(l_w/k_v)$ sending each automorphism of L_w to the induced automorphism of l_w. Therefore $\mathcal{G}^{(1)}$ is a normal subgroup of $\mathcal{G}^{(0)}$ and by the surjectivity of the above homomorphism $\mathcal{G}^{(0)}/\mathcal{G}^{(1)} \simeq \mathrm{Gal}(l_w/k_v)$. Moreover, the fixed field $E = L_w^{\mathcal{G}^{(1)}}$ is the maximal unramified extension of K_v contained in L_w, and L_w/E is completely ramified. The ramification groups are defined as follows: $\mathcal{G}^{(i)} = \{\sigma \in \mathcal{G}^{(0)} : \sigma(a) \equiv a \pmod{\mathfrak{P}_{L_w}^{i}}\}$. They are normal in $\mathcal{G}^{(0)}$, and $\mathcal{G}^{(i)} = \{e\}$ for suitably large i. Furthermore, the factors $\mathcal{G}^{(i)}/\mathcal{G}^{(i+1)}$ for $i \geq 1$ are p-groups where p is the prime corresponding to v. Note that the groups $\mathcal{G}^{(i)} = \mathcal{G}^{(i)}(v)$ thus defined are dependent on the particular extension $w|v$ and for other choice of w would be replaced by suitable conjugates. In particular, the fixed field $L^{\mathcal{H}}$ of the subgroup $\mathcal{H} \subset \mathcal{G}$ generated by the inertia groups $\mathcal{G}^{(1)}(w)$ for all extensions $w|v$, is the maximal normal subextension in L which is unramified with respect to all valuations extending v.

1.2. Adeles and ideles; strong and weak approximation; the local-global principle.

An individual valuation v in V_f^K does not have a significant effect on the arithmetic of K. However when several valuations are considered together (for example, when taking the entire set V^K), we are led to important insights in the arithmetic properties of K. In this section we introduce constructions which enable us to study all the completions of K simultaneously.

1.2.1. Adeles and ideles. The *set of adeles* A_K of the algebraic number field K is the subset of the direct product $\prod_{v \in V^K} K_v$ consisting of those $x = (x_v)$ such that $x_v \in \mathcal{O}_v$ for almost all v in V_f^K. A_K is a ring with respect to the operations in the direct product. We shall introduce a topology on A_K; namely, the base of the open sets consists of sets of the form

$\prod_{v \in S} W_v \times \prod_{v \in V^K \setminus S} \mathcal{O}_v$, where $S \subset V^K$ is a finite subset containing V_∞^K and $W_v \subset K_v$ are open subsets for each v in S. (This topology, called the *adele topology*, is stronger than the topology induced from the direct product $\prod_{v \in V^K} K_v$.) A_K is a locally compact topological ring with respect to the adele topology. For any finite subset $S \subset V^K$ containing V_∞^K the ring of S-integral adeles is defined: $A_K(S) = \prod_{v \in S} K_v \times \prod_{v \notin S} \mathcal{O}_v$; if $S = V_\infty^K$ then the corresponding ring is called the *ring of integral adeles* and is written $A_K(\infty)$. It is clear that $A_K = \bigcup_S A_K(S)$, where the union is taken over all finite subsets $S \subset V^K$ containing V_∞^K. It is easy to show that for any a in K and almost all $v \in V_f^K$ we have $|a|_v \leq 1$, i.e., $a \in \mathcal{O}_v$. If $a \in K^*$, then applying this inequality to a^{-1} actually yields $a \in U_v$ for almost all $v \in V_f^K$. Below we shall use the notation $V(a) = \{v \in V_f^K : a \notin U_v\}$. It follows that there exists a diagonal embedding $K \to A_K$, given by $x \mapsto (x, x, \dots)$, whose image is called the *ring of principal adeles* and can be identified with K.

PROPOSITION 1.5. *The ring of principal adeles is discrete in A_K.*

Note that since $\mathcal{O} = \bigcap_{v \in V_f^K} (K \cap \mathcal{O}_v)$, the intersection $K \cap A_K(\infty)$ is the ring of integers $\mathcal{O} \subset K$; thus to prove our proposition it suffices to establish the discreteness of $\mathcal{O}$ in $\prod_{v \in V_\infty^K} K_v = K \otimes_{\mathbb{Q}} \mathbb{R}$. Let $x_1, \dots, x_n$ be a $\mathbb{Z}$-base of $\mathcal{O}$ which is also a $\mathbb{Q}$-base of K, and consequently also an $\mathbb{R}$-base of $K \otimes_{\mathbb{Q}} \mathbb{R}$. $\mathcal{O}$ is thereby a $\mathbb{Z}^n$-lattice in the space $K \otimes_{\mathbb{Q}} \mathbb{R}$, and the desired discreteness follows from the discreteness of $\mathbb{Z}$ in $\mathbb{R}$. (Incidentally, we note that $K \cap A_K(S)$ (where $S \supset V_\infty^K$) is the ring of S-integers

$$\mathcal{O}(S) = \{\, x \in K : |x|_v \leq 1 \text{ for all } v \in V^K \setminus S \,\},$$

and moreover $\mathcal{O}(V_\infty^K)$ is the usual ring of integers $\mathcal{O}$.)

The multiplicative analog of adeles is ideles of K, the set J_K which, by definition, consists of $x = (x_v) \in \prod_{v \in V^K} K_v^*$, such that $x_v \in U_v$ for almost all v in V_f^K. J_K is clearly a subgroup of the direct product; moreover, J_K actually is the group of invertible elements of A_K. We note, however, that J_K curiously is not a topological group with respect to the topology induced from A_K (taking the inverse element is not a continuous operation in this topology.) The "proper" topology on J_K is induced by the topology on $A_K \times A_K$ with the embedding $J_K \to A_K \times A_K$, $x \mapsto (x, x^{-1})$. Explicitly, this topology can be given via a base of open sets, which consists of sets of

the form $\prod_{v\in S} W_v \times \prod_{v\in V^K\setminus S} U_v$ where $S \subset V^K$ is a finite subset containing V_∞^K and $W_v \subset K_v^*$ are open subsets for v in S. This topology, called the *idele topology*, is stronger than the induced adele topology, and with respect to it J_K is a locally compact topological group. (One cannot help but note the analogy between adeles and ideles. Indeed, both concepts are special cases of adeles of algebraic groups and of the more general construction of a bounded topological product, which we shall look at in Chapter 5). The analogy between adeles and ideles can be taken further. For any finite subset $S \subset V^K$ containing V_∞^K, the *group of S-integral ideles* is defined: $J_K(S) = \prod_{v\in S} K_v^* \times \prod_{v\notin S} U_v$, which for $S = V_\infty^K$ is called the *group of integral ideles* and is denoted by $J_K(\infty)$. As we have noted, if $a \in K^*$, then $a \in U_v$ for almost all v, and consequently we have the diagonal embedding $K^* \to J_K$, whose image is called the *group of principal ideles.*

PROPOSITION 1.6. *The group of principal ideles is discrete in J_K.*

The assertion follows from Proposition 1.5 and the fact that the induced adele topology on J_K is weaker than the idele topology.

An alternate proof may be presented using the *product formula*, which asserts that $\prod_{v\in V^K} |a|_v^{n_v} = 1$ for any a in K^*, where V^K consists of the extensions of the valuations $|\ |_p$ and $|\ |_\infty$ of $\mathbb{Q}$, and $n_v = [K_v : \mathbb{Q}_p]$ (respectively $n_v = [K_v : \mathbb{R}]$) is the local dimension with respect to the p-adic (respectively, Archimedean) valuation v. The product formula can be stated more elegantly as $\prod_{v\in V^K} \|a\|_v = 1$, introducing the normalized valuation $\|a\|_v = |a|_v^{n_v}$. This defines the same topology on K as the original valuation $|\ |_v$, and actually $\|\ \|_v$ is a valuation equivalent to $|\ |_v$, except for the case where v is complex. For non-Archimedean v the normalized valuation admits the following intrinsic description: if $\pi \in K_v$ is a uniformizing parameter, then $\|\pi\|_v = q^{-1}$, where q is the number of elements of the residue field k_v.

Now let us return to Proposition 1.6. For Archimedean v we shall let $W_v = \{x \in K_v^* : \|x-1\|_v < \frac{1}{2}\}$ and shall show that the neighborhood of the identity $\Omega = \prod_{v\in V_\infty^K} W_v \times \prod_{v\in V_f^K} U_v$ satisfies $\Omega \cap K^* = \{1\}$. Indeed, if $a \in \Omega\cap K^*$ and $a \neq 1$, then we would have $\prod_{v\in V^K} \|a-1\|_v < \prod_{v\in V_\infty^K} \frac{1}{2} \cdot \prod_{v\in V_f^K} 1 < 1$, which contradicts the product formula.

Using normalized valuations we can define a continuous homomorphism $J_K \to \mathbb{R}^+$, given by $(x_v) \mapsto \prod_N \|x_v\|_v$, whose kernel J_K^1 is called the *group of special ideles.* (Note, that by the product formula $J_K^1 \supset K^*$.) Since K is discrete in A_K and K^* is discrete in J_K, naturally the question arises of constructing fundamental domains for K in A_K and for K^* in J_K. We shall not explore these questions in detail at this point (cf. Lang [2], ANT), but will consider them later, more generally, in connection with arbitrary algebraic groups. Let us note only that the factor spaces A_K/K and J_K^1/K^* are compact, but J_K/K^* is not.

Let us state the fundamental isomorphism from the group $J_K/J_K(\infty)K^*$ to the ideal class group $\mathrm{Cl}(K)$ of K. We can describe it as follows. First, establish a bijection between the set V_f^K of non-Archimedean valuations of K and the set $\mathcal{P}$ of non-zero prime (maximal) ideals of $\mathcal{O}$, under which the ideal $\mathfrak{p}(v) = \mathcal{O} \cap \mathfrak{p}_v$ corresponds to v. Then the ideal $i(x) = \prod_{v\in V_f^K} \mathfrak{p}(v)$ corresponds to the idele $x = (x_v)$. (Note that since $x \in J_K$, $v(x_v) = 0$ for almost all v in V_f^K, so the product is well-defined.) Moreover, the power $\mathfrak{p}^\alpha$ of $\mathfrak{p}$ for a negative integer α is defined in the group $\mathrm{Id}(K)$ of fractional ideals of K (cf. §1.1, ¶1). From the theorem that any fractional ideal in K (as well as any non-zero ideal in $\mathcal{O}$) uniquely decomposes as the product of powers of prime ideals it is easy to see that $i : x \mapsto i(x)$ is a surjection of J_K onto $\mathrm{Id}(K)$, whose kernel is the group $J_K(\infty)$ of integral ideles. In view of the fact that $i(K^*)$ is the group of principal fractional ideals, i induces the requisite isomorphism $J_K/J_K(\infty)K^* \simeq \mathrm{Cl}(K)$. In particular, the index $[J_K : J_K(\infty)K^*]$ is the class number h_K of K. This observation is fundamental to the definition of the class number of algebraic groups (cf. Chapter 8).

1.2.2. Strong and weak approximation. We shall need *truncations* $A_{K,S}$ of adele rings, where S is a finite subset of V^K, which we define as the image of $A = A_K$ under the natural projection onto the direct product $\prod_{v\notin S} K_v$. For any finite subset $T \subset V^K$ containing S, we shall let $A_{K,S}(T)$ denote the image of the ring of T-integral adeles $A_K(T)$ in $A_{K,S}$. To simplify the notation we shall write respectively A_S,$A_S(T)$ instead of $A_{K,S}$,$A_{K,S}(T)$ when the field is clear from the context. In particular, for $S = V_\infty^K$ the ring A_{K,V_∞^K} will be written as A_f and called the ring of *finite adeles.* A topology is introduced on A_S in the obvious way: for the base of open sets we take the sets of the form $\prod_{v\in T} W_v \times \prod_{v\notin S\cup T} \mathcal{O}_v$, where $T \subset V^K \setminus S$ is a subset, and W_v is an open subset of K_v for each v in T. We have $A = K_S \times A_S$ for $K_S = \prod_{v\in S} K_v$. K_S is given the direct product topology, and then A is the product of the topological rings K_S and A_S. Moreover, the diagonal embedding of K in A is the product of the diagonal embeddings in K_S and A_S respectively.

It is worth noting that although the image of the diagonal embedding of

K in A is discrete, each embedding $K \to K_S$, $K \to A_S$ is dense.

THEOREM 1.4 (WEAK APPROXIMATION). *The image of K under the diagonal embedding is dense in K_S.*

THEOREM 1.5 (STRONG APPROXIMATION). *If $S \neq \emptyset$ then the image of K under the diagonal embedding is dense in A_S.*

Theorem 1.4 holds for any field K and any finite set S of inequivalent valuations; but, in contrast, Theorem 1.5 (and all concepts pertaining to adeles) is meaningful only for number fields (or, more generally, global fields). To elucidate the arithmetic meaning of Theorem 1.4 let us analyze in detail the case where $K = \mathbb{Q}$ and $S = \{\infty\}$. Since, for any adele $x \in A_f = A_{\mathbb{Q},S}$ we can select an integer m such that $mx \in A_f(\infty)$, we actually need only show that $\mathbb{Z}$ is densely embedded in the product $A_f(\infty) = \prod_p \mathbb{Z}_p$.

Any open subset of $A_f(\infty)$ contains a set of the form

$$W = \prod_{i=1}^{r}(a_i + p_i^{\alpha_i}\mathbb{Z}_{p_i}) \times \prod_{p \neq p_i} \mathbb{Z}_p$$

where $\{p_1, \dots, p_r\}$ is a finite collection of prime numbers, $\alpha_i > 0$ are integers, and $a_i \in \mathbb{Z}$. Then asking whether $\mathbb{Z} \cap W$ is non-empty is the same as asking whether the system of equivalences $x \equiv a_i \pmod{p_i^{\alpha_i}}$ $(i = 1, 2, \dots, r)$ is solvable, and, by the classic Chinese remainder theorem, it is. Thus, in the given case the strong approximation theorem is equivalent to the Chinese remainder theorem. In Chapter 7 we shall examine weak and strong approximation for algebraic groups.

1.2.3. The local-global principle. Investigating arithmetic questions over local fields is considerably simpler than the original task of looking at them over number fields. This naturally brings us to the question underlying the local-global method: when does the fact that a given property is satisfied over all completions K_v of a number field K mean that it is satisfied over K? One of the first results in this area is the classical

THEOREM 1.6 (MINKOWSKI-HASSE). *Let $f = f(x_1, \dots, x_n)$ be a non-degenerate quadratic form over an algebraic number field K. If f is isotropic*[2] *over all completions K_v, then f is isotropic over K as well.*

The assertion on the feasibility of moving from local to global in a given case is called the local-global, or Hasse, principle. The local-global principle pervades the arithmetic theory of algebraic groups, and various of its aspects will come up time and again throughout the book. One should

[2] i.e., $f(x_1, \dots, x_n) = 0$ has a non-trivial solution.

not, however, think that the local-global principle for homogeneous forms always holds. We shall conclude this section with a classic example.

First let us point out several aspects of the connection between the adele ring A_K of K and the adele ring A_L of a finite extension L of K. There exists a natural isomorphism $A_K \otimes L \simeq A_L$ in both the algebraic and the topological sense. This isomorphism is obtained from the local isomorphisms (1.2), $K_v \otimes_K L \simeq \prod_{w|v} L_w$, and we need only note that for almost all v in V_f^K these isomorphisms yield $\mathcal{O}_v \otimes \mathcal{O}_L \simeq \prod_{w|v} \mathcal{O}_w$. Further, the formulas in (1.3) show that the norm and trace maps $N_{L/K}$ and $\mathrm{Tr}_{L/K}$ extend to maps $N_{L/K} : A_L \to A_K$ and $\mathrm{Tr}_{L/K} : A_L \to A_K$ by the formulas

$$N_{L/K}((x_w)) = ((\prod_{w|v} N_{L_w/K_v}(x_w))_v)$$

$$\mathrm{Tr}_{L/K}((x_w)) = ((\sum_{w|v} \mathrm{Tr}_{L_w/K_v}(x_w))_v).$$

We can easily verify that the norm map $N_{L/K}$ thus obtained induces a continuous homomorphism of idele groups, $N_{L/K} : J_L \to J_K$. The Hasse norm principle is said to be satisfied for the extension L/K if

$$N_{L/K}(J_L) \cap K^* = N_{L/K}(L^*).$$

By Proposition 1.2 for almost all v in V_f^K any element a in K^* belongs to U_v and L_w/K_v is unramified, hence the condition $a \in N_{L/K}(J_L)$ is actually equivalent to $a \in N_{L/K}(\prod_{w|v} L_w^*) = N_{L/K}((L \otimes_K K_v)^*)$ for all v in V_f^K. In the language of algebraic geometry, this means that for all v in V^K there is a solution over all K_v for the equation $f(x_1, \dots, x_n) = a$, where f is the homogeneous polynomial of degree n describing the norm of an element x in terms of its coordinates $x_1, \dots, x_n$ with respect to a given base of L/K; and the validity of the Hasse norm principle in this case means that there is a solution over K. (It would be incorrect to formulate the norm principle as $a \in N_{L/K}(L^*) \iff a \in N_{L_w/K_v}(L_w^*)$ for all v and all $w|v$, since in general $N_{L/K}(L^*) \not\subset N_{L_w/K_v}(L^*)$ when L/K is not a Galois extension.)

Hasse's norm theorem (cf. Hasse [1], also the corollary of Theorem 6.11) states that the norm principle holds for cyclic Galois extensions. On the other hand, it has been found that the norm principle is not satisfied for $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{13}, \sqrt{17})$, i.e., when L/K is an abelian Galois extension with Galois group of type (2,2). To be more precise, by a simple computation with Hilbert symbols (cf. ANT, ex. 5.3) it can be shown that 5^2 is a local norm at each point, but is not a global norm. (We shall return to the Hasse norm principle in Chapter 6, §6.3.)

1.3. Cohomology.

1.3.1. Basic concepts. By and large the formalism of cohomology is not used extensively in this book. A major exception, however, is the Galois cohomology of algebraic groups over local and global fields, to which we devote all of Chapter 6. This subject, as a rule, is not handled in most courses on cohomological algebra, since it is based on noncommutative cohomology, whose definition and fundamental properties will be discussed later. For the time being we shall mention some essential properties of ordinary (commutative) cohomology, the proof of which may be found in Cartan-Eilenberg [1], Serre [2], Brown [1], as well as Chapter 4 of ANT.

Let A be an abelian group on which G acts by automorphisms (so-called G-group)[3]. This determines a family of abelian groups $\{H^i(G,A)\}_{i\geq 0}$ called the *cohomology groups* of G with coefficients in A. Namely, define $H^0(G,A) = A^G$ to be the subgroup of fixed points of A under G. To define higher cohomology groups we consider the groups $C^i(G,A)$ of all functions $f: G^i \to A$, called *cochains*, (also $C^0(G,A) = A$) and introduce the *coboundary* operators $d_i: C^i(G,A) \to C^{i+1}(G,A)$ by

$$(d_i f)(g_1,\dots,g_{i+1}) = g_1 f(g_2,\dots,g_{i+1}) + \sum_{j=1}^{i}(-1)^j f(g_1,\dots,g_j g_{j+1},\dots,g_{i+1}) + (-1)^{i+1} f(g_1,\dots,g_i).$$

Then $H^i(G,A) = \ker d_i / \operatorname{im} d_{i-1}$, where the elements of $\ker d_i = Z^i(G,A)$ are the *cocycles* and the elements of $\operatorname{im} d_{i-1} = B^i(G,A)$ are the *coboundaries*. A fundamental property of cohomology groups is that they produce a cohomological resolution of the fixed point functor $F(A) = H^0(G,A)$. This means that if $0 \to A \to B \to C \to 0$ is an exact sequence of G-groups and G-homomorphisms (i.e., homomorphisms that commute with G), then there exist connecting homomorphisms $\delta: H^i(G,C) \to H^{i+1}(G,A)$ such that the sequence

$$(1.6)\quad 0 \to H^0(G,A) \to H^0(G,B) \to H^0(G,C) \xrightarrow{\delta_0} H^1(G,A) \to \cdots \to H^i(G,A) \to H^i(G,B) \to H^i(G,C) \xrightarrow{\delta_i} H^{i+1}(G,A) \to \cdots$$

is exact. (The remaining homomorphisms are induced naturally by the homomorphisms $0 \to A \to B \to C \to 0$.)

[3] Frequently we shall also use the term G-module, since assigning to A the structure of a G-group is equivalent to assigning to A the structure of a module over the integer group ring $\mathbb{Z}[G]$.

Cohomology groups of small dimension have simple interpretations. For example, $H^1(G,A)$ is the quotient group of the group of skew homomorphisms $f: G \to A$ satisfying $f(g_1g_2) = f(g_1) + g_1 f(g_2)$, modulo the subgroup consisting of maps of the form $f(g) = ga - a$ for some a in A. In particular, if G acts trivially on A, then $H^1(G,A) = \operatorname{Hom}(G,A)$. On the other hand, if $G = \langle\sigma\rangle$ is a cyclic group of degree n, then for any G-group A we have $H^1(G,A) = A_0/A_1$, where A_0 is the kernel of the operator $\operatorname{Tr} a = a + \sigma a + \ldots + \sigma^{n-1}a$, and A_1 is the subgroup consisting of elements of the form $\sigma a - a$.

$H^2(G,A)$ is the quotient group of the group of *factor sets* $f: G\times G \to A$, satisfying

$$g_1 f(g_2,g_3) - f(g_1g_2,g_3) + f(g_1,g_2g_3) - f(g_1,g_2) = 0,$$

modulo the subgroup of *trivial* factor sets, consisting of functions of the form

$$f(g_1,g_2) = \varphi(g_1g_2) - \varphi(g_1) - g_1\varphi(g_2)$$

for a suitable function $\varphi: G \to A$. Factor sets arise in the theory of group extensions E of G by A, i.e., of exact sequences

$$1 \to A \to E \to G \to 1.$$

Using them we can establish that the elements of $H^2(G,A)$ are in one-to-one correspondence with the isomorphism classes of extensions inducing the prescribed action of G on A. In particular, if G acts trivially on A, then $H^2(G,A)$ parametrizes the central extensions of G by A. In Chapter 9 we shall encounter the groups $H^2(G,\mathbf{J})$, where $\mathbf{J} = \mathbb{Q}/\mathbb{Z}$, which are called the *Schur multipliers*. In this connection we point out several straightforward assertions.

LEMMA 1.1.

(1) *Let $1 \to \mathbf{J} \to E \xrightarrow{\varrho} G \to 1$ be a central extension. Then for any two commuting subgroups $A, B \subset G$, the map $\varphi: A \times B \to \mathbf{J}$ given by $\varphi(a,b) = [\tilde{a},\tilde{b}]$, where $\tilde{a} \in \varrho^{-1}(a)$, $\tilde{b} \in \varrho^{-1}(b)$ and $[x,y] = xyx^{-1}y^{-1}$, is well-defined and bimultiplicative.*

(2) *If G is a finitely generated abelian group, then $1 \to \mathbf{J} \to E \to G \to 1$ is trivial if and only if E is abelian. In particular, if G is cyclic then $H^2(G,\mathbf{J}) = 0$.*

The first assertion can be proven by direct computation. The proof of the second assertion relies on the divisibility of $\mathbf{J}$ and the fact that a quotient group of an abstract group by its center cannot be a non-trivial cyclic group.

We also need to compute $H^2(S_n,\mathbf{J})$ for the symmetric group S_n.

LEMMA 1.2.

(1) *If $n \leq 3$ then for any subgroup H of S_n we have $H^2(H, \mathbf{J}) = 0$;*
(2) *if $n \geq 4$ then $H^2(S_n, \mathbf{J})$ has order 2 and for any subgroup $C \subset S_n$ generated by two disjoint transpositions, the restriction map $H^2(S_n, \mathbf{J}) \to H^2(C, \mathbf{J})$ is an isomorphism.*

PROOF: For any finite G and any prime number p dividing the order of G, the p-part of $H^i(G, A)$ is isomorphic to $H^i(G_p, A)$ for each $i \geq 1$, where G_p is the Sylow p-subgroup of G (cf. ANT, Ch. 4, §6). Therefore assertion (1) follows Lemma 1.1 (2) and the fact that for $n \leq 3$ all Sylow subgroups of S_n are cyclic.

The fact that $H^2(S_n, \mathbf{J})$ has order 2 for $n \geq 4$ was discovered by Schur [1] (cf. also Huppert [1]). Clearly $H^2(C, \mathbf{J})$ has order 2. Therefore it suffices to find a cocycle α in $H^2(S_n, \mathbf{J})$ whose restriction to C is non-trivial. We can construct it as follows: consider the abstract group $\tilde{S}_n$ with generators $\sigma, \tau_i (i = 1, \dots, n-1)$ and relations

$$\begin{aligned} \sigma^2 = \tau_i^2 = [\tau_i, \sigma] = 1, &\quad i = 1, \dots, n-1, \\ (\tau_i \tau_{i+1})^3 = 1, &\quad i = 1, \dots, n-2, \\ [\tau_i, \tau_j] = \sigma, &\quad i+1 < j \end{aligned} \tag{1.7}$$

Since S_n is generated by the transpositions $(i, i+1)$, for $i = 1, \dots, n-1$, with the determining set of relations of the form

$$\begin{aligned} (i, i+1)^2 = 1, &\quad i = 1, \dots, n-1 \\ \big((i, i+1)(i+1, i+2)\big)^3 = 1, &\quad i = 1, \dots, n-2 \\ \big[(i, i+1), (j, j+1)\big] = 1, &\quad i+1 < j \end{aligned} \tag{1.8}$$

(cf. Huppert [1]), there exists a unique homomorphism $\tilde{S}_n \xrightarrow{\theta} S_n$ such that $\theta(\sigma) = 1$, $\theta(\tau_i) = (i, i+1)$. It follows from (1.7) and (1.8) that $\ker \theta$ is in the center of $\tilde{S}_n$ and is the cyclic group of order 2 generated by σ. We set σ equal to $\frac{1}{2} + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$ and let α denote the cocycle in $H^2(S_n, \mathbf{J})$ corresponding to the extension $\tilde{S}_n \xrightarrow{\theta} S_n$. In other words, consider an arbitrary section $\varphi: S_n \to \tilde{S}_n$ and let

$$\alpha(g, h) = \varphi(g)\varphi(h)\varphi(gh)^{-1}.$$

Replacing C by a conjugate, we can view C as generated by the transpositions (12) and (34). If the restriction of α to C were trivial, then by Lemma 1.1 (2), $\theta^{-1}(C)$ must be abelian. However $[\varphi((1,2)), \varphi((3,4))] = [\tau_1, \tau_2] = \sigma \neq 1$. Q.E.D.

Of the higher cohomology groups we shall only encounter the groups $H^3(G, \mathbb{Z})$, where G is a finite group operating trivially on $\mathbb{Z}$, which arises when we study obstructions to the Hasse principle (cf. §6.3). However, as the following result shows, their computation reduces to the computation of $H^2(G, \mathbf{J})$.

LEMMA 1.3. *Let G be a finite group. Then there exists a natural isomorphism $H^3(G, \mathbb{Z}) \simeq H^2(G, \mathbf{J})$ of cohomology groups when the action of G is trivial.*

Indeed, it is well known (cf. ANT, Ch. 4, §6) that the cohomology groups $H^i(G, A)$ are annihilated by multiplication by $|G|$. Since the additive group $\mathbb{Q}$ is uniquely divisible, it follows that $H^i(G, \mathbb{Q}) = 0$ for all $i \geq 1$. Thus the exact sequence $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbf{J} \to 0$ yields the exact sequence

$$0 = H^2(G, \mathbb{Q}) \to H^2(G, \mathbf{J}) \to H^3(G, \mathbb{Z}) \to H^3(G, \mathbb{Q}) = 0,$$

which in turn yields the necessary result.

Clearly $H^i(G, A)$ is a functor in the second argument: any G-homomorphism of abelian G-groups $f: A \to B$ yields a corresponding homomorphism of cohomology groups $f^*: H^i(G, A) \to H^i(G, B)$. We shall discuss several functorial properties regarding the first argument. If H is a subgroup of G, then by restricting cocycles to H we obtain the *restriction map* res: $H^i(G, A) \to H^i(H, A)$. If N is a normal subgroup of G and A an abelian G-group, then the group of fixed points A^N is a (G/N)-group, and the canonical homomorphism $G \to G/N$ induces the *inflation map* inf: $H^i(G/N, A^N) \to H^i(G, A)$. Moreover, we can define the action of G/N on $H^i(N, A)$; it turns out that the image of res: $H^i(G, A) \to H^i(N, A)$ lies in the group of fixed points $H^i(N, A)^{G/N}$. Lastly, we can define the *transgression map* tra: $H^1(N, A)^{G/N} \to H^2(G, A^N)$ such that we have the exact sequence

$$\begin{aligned} 0 \to H^1(G/N, A^N) \xrightarrow{\inf} H^1(G, A) \xrightarrow{\text{res}} H^1(H, A)^{G/N} \\ \xrightarrow{\text{tra}} H^2(G/N, A^N) \xrightarrow{\inf} H^2(G, A) \end{aligned} \tag{1.9}$$

which is the initial segment of the Hochschild-Serre spectral sequence corresponding to the extension

$$1 \to N \to G \to G/N \to 1$$

(we refer the reader to Koch [1] for the main points in the construction of (1.9), which we shall not go into here).

There is a method which allows us to replace the cohomology of a subgroup $H \subset G$ by the cohomology of G. To do so, we associate with any H-module A an induced $G-H$-module $\mathrm{ind}_G^H(A)$, which consists of those maps $f: G \to A$ such that $f(hg) = hf(g) (h \in H, g \in G)$; the action of G on $\mathrm{ind}_G^H(A)$ is given by $(gf)(x) = f(xg)$. We obtain a homomorphism $\mathrm{ind}_G^H(A) \to A$ by sending each element $f \in \mathrm{ind}_G^H(A)$ to $f(1)$, thereby providing a homomorphism

$$H^i(G, \mathrm{ind}_G^H(A)) \to H^i(H, A). \tag{1.10}$$

By Shapiro's lemma, homomorphism (1.10) is an isomorphism. Now let us suppose that H has finite index in G and that A is a G-group. Then we can define a surjective G-homomorphism $\pi: \mathrm{ind}_G^H(A) \to A$, by

$$\pi(f) = \sum_{x \in G/H} xf(x^{-1}).$$

Passing to cohomology, we then obtain the *corestriction map*

$$\mathrm{cor}: H^i(H, A) \simeq H^i(G, \mathrm{ind}_G^H(A)) \to H^i(G, A),$$

where $\simeq$ denotes the inverse isomorphism of (1.10). Note that for the 0-th cohomology groups, $\mathrm{cor}: A^H \to A^G$ is the trace map $\mathrm{Tr}(a) = \sum_{g \in G/H} g(a)$ (or, in multiplicative notation, the norm).

Sometimes it is necessary to consider continuous cohomology of a topological group G with coefficients in a topological abelian G-group A for which the action of G on A is continuous. The definition is obtained by considering continuous cochains instead of the usual cochains. With the exception of several places in §9.5, where we look at adele group cohomology, in this book we shall deal exclusively with continuous cohomology of a pro-finite (i.e., compact totally disconnected) group G with coefficients in a discrete group A. In this setting the continuity of action of G on A means that $A = \bigcup_U A^U$, where the union is taken over all open normal subgroups $U \subset G$. A pro-finite group G may be described as a projective limit $G = \varprojlim G/U$, where U runs through some fundamental system of neighborhoods of 1 consisting of normal subgroups (the basic properties of pro-finite groups will be reviewed in §3.2); then the cohomology group $H^i(G, A)$ of a discrete G-group A may be written as the inductive limit $\varinjlim H^i(G/U, A^U)$ with respect to the inflation maps $H^i(G/U, A^U) \to H^i(G/V, A^V)$ for $U \supset V$. One of the fundamental examples arises from consideration of the absolute Galois group $\mathcal{G} = \mathcal{G}(\bar{K}/K)$ of a perfect field K and its natural action on the additive or multiplicative group of $\bar{K}$ or on some other object A with a K-structure (cf. §2.2). Then the corresponding cohomology groups $H^i(\mathcal{G}, A)$ are Galois and are written $H^i(K, A)$.

It is easily shown that the cohomology of a pro-finite group G with coefficients in a discrete group A satisfies all the usual basic properties of cohomology. In particular, an exact sequence of discrete G-groups and G-homomorphisms $0 \to A \to B \to C \to 0$ gives rise to the exact cohomological sequence (1.6), and an extension $1 \to N \to G \to G/N \to 1$ of pro-finite groups yields the initial segment of the Hochschild-Serre spectral sequence (1.9).

1.3.2. Non-abelian cohomology. In working with algebraic groups, we find cocycles which take on values in a group of points over some (finite or infinite) Galois extension of the base field, i.e., the range of the cocycles, generally speaking, is a noncommutative group. Similar situations are encountered elsewhere, such as in studying the crossed product of a noncommutative algebra with a finite group. By the same token, noncommutative cohomology fully deserves a study of its own, for which we refer the interested reader to Giraud [1]. For the time being we shall review some basic concepts relating to noncommutative cohomology, which we shall need in our study of Galois cohomology of algebraic groups (cf. Serre [2]).

Let us consider a (discrete or pro-finite) group G acting on some set A, assuming in the topological setting the latter to be discrete, and the action of G on A to be continuous. In this case A is called a *G-set*. If A is a group and G acts on A by automorphisms, then A is said to be a *G-group*. For a G-set A we define $H^0(G, A)$ to be the set of G-fixed elements A^G. If A is a G-group then $H^0(G, A)$ is a group.

For a G-group A, a continuous map $f: G \to A$ is said to be a *1-cocycle* with values in A if for any s, t in G we have $f(st) = f(s)s(f(t))$. Often it will be useful to treat 1-cocycles as families indexed by elements of G and to write f as $\{f_s : s \in G\}$, bearing in mind that $f_s = f(s)$. Sometimes the action of G on A is conveniently written in exponential form as ${}^s a$ instead of $s(a)$. With respect to these conventions, the condition on 1-cocycles is written as $f_{st} = f_s {}^s f_t$. The set of all 1-cocycles will be written as $Z^1(G, A)$. $Z^1(G, A)$ is non-empty; it always contains the unit cocycle defined by $f_s = e$, the unit element of A, for all s in G. Two cocycles (a_s) and (b_s) are said to be *equivalent* if there is an element c in A such that $b_s = c^{-1} a_s {}^s c$ for all s in G. (One can easily verify that the relation thus defined between cocycles is indeed an equivalence in $Z^1(G, A)$.) The set of equivalence classes is called the first cohomology set with coefficients in A and is written $H^1(G, A)$. If A is an abelian group, then this definition

of H^1 is equivalent to the one presented in §1.3.1; in particular, $H^1(G, A)$ then is an abelian group. In general $H^1(G, A)$ does not have any natural group structure and is only a set with a distinguished element which is the equivalence class of the unit cocycle. As above, if $G = \varprojlim G/U$ is a profinite group then $H^1(G, A) = \varinjlim H^1(G/U, A^U)$ is the direct limit of the sets with distinguished element, relative to the inflation maps $H^1(G/U, A^U) \to H^1(G/V, A^V)$ for $U \supset V$, defined in the obvious way. In general, if $f: A \to B$ is a homomorphism of a G-group A in an H-group B, compatible with $g: H \to G$, i.e., if $f({}^{g(s)}a) = {}^s f(a)$ for all $s \in H$, $a \in A$, then we may define the map $Z^1(G, A) \to Z^1(H, B)$ sending (a_s) to $\big(b_s = f(a_{g(s)})\big)$, which induces a morphism of sets with distinguished element

$$H^1(G, A) \to H^1(H, A).$$

We shall say that a sequence of cohomology sets is *exact* if it is exact as a sequence of sets with distinguished elements, i.e., if a pre-image of the distinguished element is equal to the image of the preceding map. (The distinguished element in the zero cohomology set $H^0(G, A)$ is the unit element of A.) Let us mention the main types of exact sequences that we shall use. Let A be a subgroup of a G-group B, invariant under the action of G. Then there is a natural action of G on B/A, thereby making B/A a G-set, and we obtain the set $H^0(G, B/A)$, whose distinguished element is the class A. For any element of $H^0(G, B/A) = (B/A)^G$ choose a representative b in B and for s in G let $a_s = b^{-1}{}^s b$. It is easily shown that $a_s \in A$ and $(a_s) \in Z^1(G, A)$. Moreover, the equivalence class of this cocycle is independent of the choice of b, and we obtain a map $\delta: H^0(G, B/A) \to H^1(G, A)$.

Direct computation shows that we have the exact sequence of sets with distinguished element

(1.11)
$$1 \to H^0(G, A) \to H^0(G, B) \to H^0(G, B/A) \xrightarrow{\delta} H^1(G, A) \xrightarrow{\alpha} H^1(G, B)$$

where α is induced by the embedding $A \hookrightarrow B$. Furthermore, if $c_1, c_2 \in H^0(G, B/A)$, then $\delta(c_1) = \delta(c_2)$ if and only if there exists b in B^G with $c_2 = bc_1$. Consequently the elements of the kernel of $H^1(G, A) \to H^1(G, B)$ are in one-to-one correspondence with the orbits in $(B/A)^G$ under the action of B^G. If A is a normal subgroup of B, then (1.11) is extendable to one more term:

(1.12)
$$\cdots \to H^0(G, B/A) \xrightarrow{\delta} H^1(G, A) \xrightarrow{\alpha} H^1(G, B) \xrightarrow{\beta} H^1(G, B/A).$$

Special attention should be given to the case where A is a central subgroup of B (precisely the situation encountered in examining the universal

coverings of algebraic groups). Let $C = B/A$ and take the canonical homomorphism $\varphi: B \to C$. Then $H^1(G, A)$ is a group, and there is a group homomorphism $\delta: H^0(G, C) = C^G \to H^1(G, A)$, which we shall refer to as the *coboundary map*. Using the centrality of A we can define the natural action of the group $H^1(G, A)$ on the set $H^1(G, B)$: if $a = (a_s) \in Z^1(G, A)$, $b = (b_s) \in Z^1(G, B)$, then $a \cdot b = (a_s b_s) \in Z^1(G, B)$. The orbits of this action, it turns out, are the fibers of the morphism $\beta: H^1(G, B) \to H^1(G, C)$. Furthermore, by the commutativity of A the group $H^2(G, A)$ is defined, and, as we shall presently show, there is a map $\partial: H^1(G, C) \to H^2(G, A)$ extending (1.12) to the exact sequence

(1.13)
$$\cdots \to H^1(G, B) \xrightarrow{\beta} H^1(G, C) \xrightarrow{\partial} H^2(G, A).$$

Let $c = (c_s) \in Z^1(G, C)$; for each s in G we can find an element b_s in B such that $\varphi(b_s) = c_s$. Then put $a_{s,t} = b_s {}^s b_t b_{st}^{-1}$. It is easily shown that $a_{s,t} \in A$ and that the map $G \times G \to A$ given by $(s, t) \mapsto a_{s,t}$ is a 2-cocycle (i.e., an element of $Z^2(G, A)$). It turns out that the class defined by this cocycle is independent of the choice of elements b_s and of the choice of cocycle c in its equivalence class in $H^1(G, C)$, and thus we obtain the well-defined connecting morphism $\partial: H^1(G, C) \to H^2(G, A)$. The corresponding sequence (1.13) can be shown directly to be exact. Note that in the noncommutative case ∂ has no bearing on any group structure; moreover, its image in $H^2(G, A)$ generally is not a subgroup.

In the noncommutative case the exact sequences described above carry substantially less information than in the commutative case; indeed, knowing something about the kernel of a morphism of sets with distinguished element generally does not allow us to draw inferences about all of its fibers. This difficulty can be partially overcome with the help of a method based on the concept of *twisting* (cf. Serre [2], Ch. 1, §5). We review some basic definitions. Let A be a G-group and F a G-set with a given A-action which commutes with the action of G, i.e., $s(a \cdot f) = s(a) \cdot s(f)$ for any $s \in G$, $a \in A$, $f \in F$. Then, fixing an arbitrary cocycle $a = (a_s) \in Z^1(G, A)$ we can define a new action of G on F by the formula

$$\bar{s}(f) = a_s(s(f)) \quad \text{for } s \text{ in } G.$$

F with this action is denoted by ${}_aF$. We say that ${}_aF$ is obtained from F by twisting by a. It is easy to see that ${}_aF$ depends functorially on F (with respect to A-morphisms $F \to F'$) and that twisting commutes with direct products. For cocycles a and b equivalent in $Z^1(G, A)$, the G-sets ${}_aF$ and ${}_bF$ are isomorphic. Moreover, if F has some structure (such as that of a group) and the elements of A preserve this structure, then ${}_aF$ also has this

structure. A whole series of examples of twists will be examined in §2.3, but for the time being we shall limit ourselves to one example which comes up when considering exact sequences. Namely, consider the case where $A = F$ acts on itself by inner automorphisms. Then, for any cocycle a in $Z^1(G, A)$ the twisted group ${}_aA$ is defined, and moreover the first cohomology sets of A and $A' = {}_aA$ are interrelated in the following way:

LEMMA 1.4. *There is a bijection $t_a: Z^1(G, A') \to Z^1(G, A)$ defined by sending a cocycle $x = (x_s)$ in $Z^1(G, A')$ to the cocycle $y = (x_s a_s)$ in $Z^1(G, A)$. Passing to cohomology, t_a induces a bijection $\tau_a: H^1(G, A') \to H^1(G, A)$, which takes the distinguished element of $H^1(G, A')$ to the class of the cocycle a.*

Thus, we are able to multiply cocycles, however by going over to the twisted group. By this method, replacing the sets in sequences (1.11)–(1.13) by the corresponding twisted groups (as we shall henceforth say, *twisting* these sequences), one can describe the fibers of all the maps in the original sequences. For example, take the case described in the construction of sequence (1.11) where $a \in Z^1(G, A)$, and suppose we wish to describe the fiber $\alpha^{-1}(\alpha(a))$ (the same letter a denotes the corresponding equivalence class in $H^1(G, A)$). To do so we must pass to the twisted groups $A' = {}_aA$ and $B' = {}_aB$ and examine their analog of exact sequence (1.11)

$$(1.11') \quad 1 \to H^0(G, A') \to H^0(G, B') \to H^0(G, B'/A') \xrightarrow{\delta} H^1(G, A') \xrightarrow{\alpha'} H^1(G, B').$$

Then the bijection τ_a of Lemma 1.4 determines a bijection between the elements of $\ker \alpha'$ and the elements of the fiber $\alpha^{-1}(\alpha(a))$. On the other hand, it follows from (1.11) that the elements of $\ker \alpha'$ are in one-to-one correspondence with the orbits in $(B'/A')^G$ under $(B')^G$. Let us find a criterion for the class of some cocycle b in $Z^1(G, B)$ to lie in the image of α. To do so, consider the action of B on B/A (a homogeneous space) by translations; then the twisted space ${}_b(B/A)$ is defined for any b in $Z^1(G, B)$.

LEMMA 1.5. $b \in \operatorname{im} \alpha \Leftrightarrow H^0(G, {}_b(B/A)) \neq \emptyset$.

The fibers of ∂ in the sequence (1.13) are computed in an analogous manner. Namely, let $c = (c_s) \in Z^1(G, C)$. Since A is a central subgroup of B, then C acts on B by inner automorphisms, these being trivial on A. Using c to twist the exact sequence $1 \to A \to B \to C \to 1$, we obtain the exact sequence $1 \to A \to {}_cB \to {}_cC \to 1$, which gives rise to a new connecting morphism $\partial_c: H^1(G, {}_cC) \to H^2(G, A)$. Direct computation shows that this morphism bears on the bijection $\tau_c: H^1(G, {}_cC) \to H^1(G, C)$ of Lemma 1.4 in the following way: $\partial(\tau_c(x)) = \partial_c(x)\partial(c)$, multiplication

taken in $H^2(G, A)$. It follows that the elements of the fiber $\partial^{-1}(\partial(c))$ are in one-to-one correspondence with the elements of $\ker \partial_c$, which in turn correspond bijectively to the elements of the quotient set of $H^1(G, {}_cB)$ under the action of $H^1(G, A)$.

If H is a normal subgroup of G (assumed to be closed in the topological setting), then, as in the commutative case, the quotient group G/H acts on A^H, so one can define $H^1(G/H, A^H)$ and the inflation map $H^1(G/H, A^H) \to H^1(G, A)$. If $H^1(G, A) \to H^1(H, A)$ is the restriction map, then the noncommutative analog of the Hochschild-Serre spectral sequence (1.9),

$$1 \to H^1(G/H, A^H) \to H^1(G, A) \to H^1(H, A),$$

is exact.

We have yet to consider induced sets and the noncommutative variant of Shapiro's lemma. We shall go into these questions in greater detail, since they do not appear in Serre [1]. Let H be a (closed) subgroup of G. Then for any H-set (respectively H-group) B we can define the G-set (respectively G-group) $A = \operatorname{ind}_G^H(B)$ consisting of all (continuous) maps $a: G \to B$ satisfying $a(ts) = {}^t a(s)$ for all t in H, s in G, and the action of G on A is given by ${}^r a(s) = a(sr)$ for r in G. The G-set (respectively G-group) A, or any G-set (G-group) which is isomorphic to A, is said to be *G–H induced*. The map $A \to B$ given by $a \mapsto a(1)$ is consistent with the inclusion $H \subset G$, and therefore for $i = 0, 1$ induces morphisms

$$\varphi_i: H^i(G, A) \to H^i(H, B).$$

PROPOSITION 1.7 (SHAPIRO'S LEMMA, NONCOMMUTATIVE VERSION). *The maps φ_i are bijections.*

PROOF: We shall consider the cases $i = 0$ and $i = 1$ separately. First, let $i = 0$. If $a \in H^0(G, A)$ then a is a map $G \to A$, invariant under the action of G, i.e., $a = {}^r a$ for all $r \in G$. Recalling the definition of the action of G on A, we see that the latter equality is equivalent to $a(s) = a(sr)$ for all s, $r \in G$. Setting $s = 1$ we see a is a constant map. By definition $\varphi_0(a) = a(1) \in B^H = H^0(H, B)$, from which it follows that $\varphi_0(a) = \varphi_0(b)$ implies $a = b$ for $a, b \in H^0(G, A)$, in other words φ_0 is injective. On the other hand, for any c in $H^0(H, B)$, the trivial map $a: G \to B$ given by $a(s) = c$ lies in A; moreover it can be easily shown that $a \in H^0(G, A)$ and $\varphi_0(a) = c$.

Now let $i = 1$. To prove that φ_1 is injective we assume that the classes of cocycles $a = (a_r)$ and $b = (b_r) \in Z^1(G, A)$ are sent to the same element by φ_1. Then for suitable c in B we have $a_r(1) = c^{-1} b_r(1) {}^r c$ for all r in

H. Clearly there exists an element d in A for which $d(1) = c$. Then, substituting the equivalent cocycle $b^1 = (d^{-1}b_r{}^r d)$ for b, we may assume

$$a_r(1) = b_r(1) \quad \text{for all } r \in H. \tag{1.14}$$

The definition of cocycle gives for all r, s, $t \in G$

$$a_{rs}(t) = a_r(t)^r a_s(t) = a_r(t)a_s(tr)$$
$$b_{rs}(t) = b_r(t)^r b_s(t) = b_r(t)b_s(tr).$$

If we set $r = t^{-1}$, then (1.14) implies

$$a_{t^{-1}s}(t)b_{t^{-1}s}(t)^{-1} = a_{t^{-1}}(t)b_{t^{-1}}(t)^{-1} \tag{1.15}$$

for all s in H. We define the function $c: G \to B$ by the equation

$$c(t) = b_{t^{-1}}(t)a_{t^{-1}}(t)^{-1}.$$

Then, for s in H, (1.15) gives us

$$\begin{aligned} c(st) &= b_{t^{-1}s^{-1}}(st)a_{t^{-1}s^{-1}}(st)^{-1} \\ &= s\big(b_{t^{-1}s^{-1}}(t)a_{t^{-1}s^{-1}}(t)^{-1}\big) = s\big(b_{t^{-1}}(t)a_{t^{-1}}(t)^{-1}\big) = s\big(c(t)\big), \end{aligned}$$

i.e., $c \in A$. On the other hand, we can immediately verify that $a_r = c^{-1}b_r{}^r c$ for all r in G, which means that a and b are equivalent cocycles. This proves that φ_1 is injective.

To prove that φ_1 is surjective, we consider an arbitrary cocycle $b = (b_r) \in Z^1(H, B)$. Let $v: G/H \to G$ be a (continuous) section for which $v(H) = 1$. Then for s in G we set $w(s) = sv(Hs)^{-1} \in H$. For each s in G we define $a_s: G \to B$ by the formula $a_s(t) = {}^{w(t)}b_{w(v(t)s)}$. Direct computation shows that $a_s \in A$ and the family $a = (a_s)$ forms a cocycle in $Z^1(G, A)$, and moreover $\varphi_1(a) = b$. This completes the proof of the proposition.

The following straightforward assertion is helpful in applications.

LEMMA 1.6. *Let H be of finite index in G. Then a G-group A is $G - H$-induced if and only if there exists an H-subgroup $B \subset A$ such that A is a direct product of the ${}^sB$, where s runs over some system of representatives of the cosets of H.*

For example, if L is a finite Galois extension of an algebraic number field K with Galois group $\mathcal{G}$, u is an extension of $v \in V^K$ to L, and $\mathcal{H} = \mathcal{G}(u)$ is the corresponding decomposition group, then as (1.2) shows, the $\mathcal{G}$-module $L \otimes_K K_v$ is isomorphic to $\operatorname{ind}_{\mathcal{G}}^{\mathcal{G}(u)}(L_u)$.

1.4. Simple algebras over local fields.

1.4.1. Simple algebras and Brauer groups. Let A be a finite-dimensional central simple algebra over the field K (centrality meaning that the center of A is K). Then A is a full matrix algebra $M_n(D)$ over some central division algebra (skew field) D over K, and $\dim_K A = n^2 \dim_K D$. $\dim_K D$ in turn is the square of a positive integer d, called the *index* of D and respectively of A. It is well known that if K is finite or algebraically closed, then necessarily $d = 1$, i.e., there are no noncommutative finite-dimensional central division algebras over K. If $K = \mathbb{R}$ and $d > 1$, then D is isomorphic to the skew field of the usual Hamilton's quaternions $\mathbb{H}$. Over non-Archimedean local fields or algebraic number fields there exist skew fields of an arbitrary index. To describe them we shall need several results from the theory of simple algebras (cf., for example, Herstein [1], Pierce [1]).

One useful result is the Skolem-Noether theorem: given two simple subalgebras B_1, B_2 of a finite-dimensional central simple K-algebra A, any isomorphism $\sigma: B_1 \to B_2$ which is trivial on K extends to an inner automorphism of A. Maximal subfields $P \subset D$ play an important role in the study of a skew field D. They necessarily contain K and have dimension d (the index of D) over K; thus $D \otimes_K P \simeq M_d(P)$. Conversely, for any field $P \supset K$, if $[P : K] = d$ and $D \otimes_K P \simeq M_d(P)$ (i.e., P is a splitting field of D), then P is isomorphic to a maximal subfield of D.

Consider an arbitrary splitting field P of a simple algebra A (for example, one could take the algebraic closure $\bar{K}$ of K), and fix a corresponding isomorphism $\varphi: A \otimes_K P \simeq M_r(P)$. Then the map $\operatorname{Nrd}_{A/K}(x) = \det \varphi(x \otimes 1)$ is called the *reduced norm*, is multiplicative, and is independent of P and φ. The reduced norm is given by a homogeneous polynomial of degree r with coefficients in K, in the coordinates of x with respect to any given base A over K; in particular $\operatorname{Nrd}_{A/K}(A^*) \subset K^*$. A property of the reduced norm which we shall use often is that for any x in D, $\operatorname{Nrd}_{D/K}(x)$ is the usual norm $N_{P/K}(x)$ from any maximal subfield $P \subset D$ which contains x. The study of the multiplicative group A^* essentially reduces to the study of the image of $\operatorname{Nrd}_{A/K}(A^*)$ and the corresponding special linear group $SL_1(A) = \{x \in A^* : \operatorname{Nrd}_{A/K}(x) = 1\}$. The structure of $SL_1(A)$ (especially when $A = M_n(D)$ for $n > 1$, cf. §7.2) depends in turn on whether or not $SL_1(A)$ is the commutator group $[A^*, A^*]$. (Note that the inclusion $[A^*, A^*] \subset SL_1(A)$ is a consequence of the multiplicativity of the reduced norm.) This problem, raised by Tanaka and Artin in 1943, is equivalent to the question of the triviality of the *reduced Whitehead group* $SK_1(A) = SL_1(A)/[A^*, A^*]$ from algebraic K-theory. On the connection between these problems and the well-known Kneser-Tits conjecture in the theory of algebraic groups, see §7.2. Platonov solved the Tanaka-Artin problem in 1975 and found

the answer to be negative. In [13]–[16] he developed a reduced K-theory which in many cases makes it possible to calculate $SK_1(A)$ and establish its connection with other arithmetical problems (cf. Chapter 7). Nevertheless, in the cases of interest to us of local and global fields, $SK_1(A)$ is always trivial (this result was attained for local fields by Nakayama-Matsushima [1] in 1943 and for algebraic number fields by Wang [1] in 1950). Since this result will be used repeatedly throughout the book, we shall present a new proof below, which differs substantially from the original in that it is shorter and more conceptual.

We introduce an equivalence on the set of central simple algebras over K, regarding $A_1 = M_{n_1}(D_1) \sim A_2 = M_{n_2}(D_2)$ if the skew fields D_1 and D_2 are isomorphic, and we define the product of the equivalence classes as $[A_1] \cdot [A_2] = [A_1 \otimes_K A_2]$ (note that the tensor product over K of two simple K-algebras, one of which is central, is also a simple K-algebra). This operation makes the set of equivalence classes of finite-dimensional central simple K-algebras into an abelian group (the inverse of $[A]$ is the class of the opposite algebra A^0, which is obtained from A by a new product given by $a \cdot b = ba$, where the product on the right is taken in A). This group is called the *Brauer group* of K and is denoted as $\mathrm{Br}(K)$. For any extension L/K the equivalence classes of central simple K-algebras for which L is a splitting field generate a subgroup of $\mathrm{Br}(K)$, denoted as $\mathrm{Br}(L/K)$. The order of an element $[A]$ in $\mathrm{Br}(K)$ is always finite and is called the *exponent* of A. Note that the exponent of A divides the index and in general is distinct from the index. An important result in the theory of algebra is that the exponent and index coincide over local and global fields, à propos of which let us point out a conjecture that this property also holds for C_2-fields (cf. M. Artin [1]). Note that $\mathrm{Br}(K)$ has a cohomological interpretation. Namely, associating to a simple algebra its factor set gives the isomorphism

$$\mathrm{Br}(K) \simeq H^2(K, \bar{K}^*).$$

1.4.2. Simple algebras over local fields. Throughout this subsection D denotes a skew field of index n over a (non-archimedean) local field K, v denotes a valuation of K, $\mathcal{O}$ denotes the valuation ring of v, with valuation ideal $\mathfrak{p}$, and $U = \mathcal{O}^*$ denotes the corresponding group of units. The valuation v uniquely extends to D by the formula

$$\tilde{v}(x) = \frac{1}{n} v(\mathrm{Nrd}_{D/K}(x)), \qquad \text{for } x \in D; \tag{1.16}$$

moreover D is complete in the topology given by this valuation. Let

$$\mathcal{O}_D = \{x \in D : \tilde{v}(x) \geq 0\} \text{ and } \mathfrak{P}_D = \{x \in D : \tilde{v}(x) > 0\}$$

respectively be the ring of integers and valuation ideal of $\tilde{v}$. Clearly $\mathfrak{P}_D$ is a maximal right and left ideal of $\mathcal{O}_D$, thereby yielding a residue skew field $\bar{D}$. Let $f = [\bar{D} : k]$ (where k is the residue field of K) and let $e = [\tilde{\Gamma} : \Gamma]$ be the corresponding ramification index (where $\Gamma = v(K^*)$ and $\tilde{\Gamma} = \tilde{v}(D^*)$ are the respective value groups of v and $\tilde{v}$). Then, as in the commutative case (cf. §1.1.2), $ef = \dim_K D = n^2$. On the other hand, $\bar{D}$, being a finite skew field, is commutative, and consequently $\bar{D} = k(\alpha)$ for a suitable α in $\bar{D}$. Let $\beta \in \mathcal{O}_D$ be an element whose residue $\bar{\beta}$ is α (henceforth bar denotes the image in the residue field or residue skew field). Then for the field $L = K(\beta)$ and its corresponding residue field l we have

$$f = [\bar{D} : \bar{K}] = [l : k] \leq [L : K] = n.$$

It follows from (1.16) that multiplication by n defines a homomorphism from $\tilde{\Gamma}$ to Γ, and since $\Gamma \simeq \mathbb{Z}$, we see $e = [\tilde{\Gamma} : \Gamma] \leq n$. Therefore $e = f = n$ and $\bar{D}$ is the residue field l of a suitable subfield $L \subset D$, which is automatically a maximal subfield of D and is unramified over K. The value group $\tilde{\Gamma}$ is infinite cyclic, so there exists an element Π in D^*, called a *uniformizing parameter*, such that $\tilde{v}(\Pi) = \frac{1}{n}$. We have $\mathfrak{P}_D = \Pi\mathcal{O}_D = \mathcal{O}_D\Pi$, and moreover any other uniformizing parameter Π' in $\mathcal{O}_D$ has the form $\Pi' = \Pi u$, for $u \in U_D = \mathcal{O}_D^*$. Analogously, for any $i \geq 1$ we have $\mathfrak{P}_D^i = \Pi^i\mathcal{O}_D = \mathcal{O}_D\Pi^i$.

Let us fix a maximal unramified subfield $L \subset D$ (noting that any maximal unramified subfield $L' \subset D$ is isomorphic to L over K and therefore, by the Skolem-Noether theorem, is conjugate to L). L/K is cyclic Galois and $\mathrm{Gal}(L/K)$ is generated by the Frobenius automorphism φ (cf. §1.1.3). By the Skolem-Noether theorem, there exists an element g in D^* such that

$$\varphi(x) = gxg^{-1} \qquad \forall x \in L. \tag{1.17}$$

Then $\tilde{v}(g) \in \frac{1}{n}\mathbb{Z}$ in $\mathbb{Q}/\mathbb{Z}$, called the *invariant* of D and written $\mathrm{inv}_K(D)$, is well defined. The invariant $\mathrm{inv}(A)$ of a simple algebra $A = M_n(D)$ is defined as the invariant of D.

THEOREM 1.7. *$A \mapsto \mathrm{inv}_k A$ defines an isomorphism $\mathrm{Br}(K) \simeq \mathbb{Q}/\mathbb{Z}$. Moreover, if P/K is a finite extension of degree m, then we have the following commutative diagram, where $[m]$ denotes multiplication by m.*

$$\begin{array}{ccc} \mathrm{Br}(K) & \xrightarrow{\mathrm{inv}_K} & \mathbb{Q}/\mathbb{Z} \\ {\scriptstyle [A] \downarrow [A \otimes_K P]} \Big\downarrow & & \Big\downarrow {\scriptstyle [m]} \\ \mathrm{Br}(P) & \xrightarrow{\mathrm{inv}_P} & \mathbb{Q}/\mathbb{Z} \end{array} \tag{1.18}$$

Since (1.18) is commutative, if D is a skew field of index n over K, then for any field extension P/K of dimension n we have $D \otimes_K P \simeq M_n(P)$, and consequently P is isomorphic to a maximal subfield of D. Another important observation is that over K the exponent of any skew field is its index. Indeed, we must show that if $\tilde{v}(g) = \frac{a}{n}$ then $(a,n) = 1$. To prove this we note that by (1.16) $\mathcal{O}_D$ and $\mathfrak{P}_D$ are invariant relative to conjugation in D and therefore any element h in D^* induces an automorphism $\sigma_h: \bar{x} \mapsto \overline{hxh^{-1}}$ of $\bar{D}$ over k. Set $\sigma = \sigma_\Pi$. Since $\bar{D}$ is commutative it follows that $\sigma_u = \mathrm{id}$ for u in U_D, and thus σ is independent of the choice of Π. We have observed that $\bar{D}$ is the residue field l of the maximal unramified subfield $L \subset D$, so actually $\sigma \in \mathrm{Gal}(l/k)$. We have $g = \Pi^a u$, for suitable $u \in U_D$, and therefore $\varphi = \sigma^a$ (using the same letter to designate the Frobenius automorphism of L/K and of l/k). Since φ generates $\mathrm{Gal}(l/k)$, necessarily $(a,n) = 1$. At the same time we have shown that $\sigma = \sigma_\Pi$ generates $\mathrm{Gal}(l/k)$, a fact to be used below.

The above results on the structure of skew fields over p-adic number fields go back to Hasse [1] and Witt [1]. Recently structure theorems have been obtained for a broad class of skew fields over arbitrary Henselian fields (cf. Platonov, Yanchevskiĭ [3], [4]).

1.4.3. Multiplicative structure of skew fields over local fields. To begin with, we shall establish that for any finite-dimensional skew field D over a local field K we have $\mathrm{Nrd}_{D/K}(D^*) = K^*$ and $SL(1,D)$ is the commutator group $[D^*, D^*]$. (We shall present a more thorough analysis of D^*, using filtrations by congruence subgroups, in the following subsection.)

We have already seen that there exists a maximal unramified subfield $L \subset D$ and therefore the group U of units is in $N_{L/K}(L^*) \subset \mathrm{Nrd}_{D/K}(D^*)$ (cf. Proposition 1.2). It remains to be shown that $\mathrm{Nrd}_{D/K}(D^*)$ contains the uniformizing parameter π of K. To do so we note that $t^n + (-1)^n\pi$ (where n is the index of D) is an Eisenstein polynomial (cf. §1.1.3), and therefore defines an n-dimensional extension P/K, and $\pi \in N_{P/K}(P^*)$. But, as we have noted, P is isomorphic to a maximal subfield of D, and therefore $N_{P/K}(P^*) \subset \mathrm{Nrd}_{D/K}(D^*)$, i.e. $\pi \in \mathrm{Nrd}_{D/K}(D^*)$. This proves $\mathrm{Nrd}_{D/K}(D^*) = K^*$.

To prove that $SL_1(D)$ (denoted as $D^{(1)}$ for the sake of brevity) is the commutator group $[D^*, D^*]$ is somewhat more complicated. To begin with, we note that $L^{(1)} = L \cap D^{(1)}$ is contained in $[D^*, D^*]$. Indeed, by Hilbert's Theorem 90 (cf. Lang [3], Ch. 8), any element $x \in L^{(1)} = \{t \in L^* : N_{L/K}(t) = 1\}$ has the form $x = \varphi(y)y^{-1}$ for suitable y in L^*. Then, by (1.17) $x = gyg^{-1}y^{-1} \in [D^*, D^*]$. Hence the assertion is a consequence of the following result.

THEOREM 1.8 (PLATONOV, YANCHEVSKIĬ [2]). *The normal subgroup of $D^{(1)}$ generated by $L^{(1)}$ is $D^{(1)}$.*

PROOF: Let $x \in D^{(1)}$. Then the residue $\bar{x} \in l^{(1)} = \{a \in l^* : N_{l/k}(a) = 1\}$. Indeed, x can be written as $x = ab$, where a is in the group of units U_L of L and $b \in 1+\mathfrak{P}_D$. Then $\bar{x} = \bar{a}$. On the other hand, $N_{L/K}(a) = \mathrm{Nrd}_{D/K}(a) = \mathrm{Nrd}_{D/K}(b^{-1}) = N_{M/K}(b)^{-1}$ for a maximal subfield $M \subset D$ containing b. But $b \in (1+\mathfrak{P}_D) \cap M = 1+\mathfrak{P}_M$, so by Proposition 1.3, $N_{M/K}(b^{-1}) \in 1+\mathfrak{p}$, where $\mathfrak{p}$ is the valuation ideal in K. Therefore

$$N_{l/k}(\bar{a}) = \prod_{i=0}^{n-1} \varphi^i(\bar{a}) = \overline{\prod_{i=0}^{n-1} \varphi^i(a)} = \overline{N_{L/K}(a)} = 1.$$

Since $l^{(1)}$ is cyclic, there exists an element z in $l^{(1)}$ such that $\bar{x}z$ is a generator of $l^{(1)}$, and consequently $l = k(\bar{x}z)$. But $z = \bar{y}$ for suitable y in $L^{(1)}$. Indeed, by Hilbert's Theorem 90 $z = \varphi(s)/s$ for suitable s in l^*; then if u in U_L satisfies $\bar{u} = s$, it follows that $y = \varphi(u)/u$ is the element we are looking for. Further, note that the extension $P = K(xy)$ is a maximal unramified subfield of D, since

$$n \geq [P : k] \geq [k(\overline{xy}) : k] = [l : k] = n,$$

from which it follows $[P : K] = [k(\overline{xy}) : k] = n$, as desired. Thus $P \simeq L$ over K and consequently, by the Skolem-Noether theorem, $P = sLs^{-1}$ for suitable s in D^*. Considering that $N_{L/K}(L^*) = UK^{*n}$ (Proposition 1.2) and that for g in (1.17) $v(\mathrm{Nrd}_{D/K}(g), n) = 1$ holds (cf. §1.4.2), we see that $\mathrm{Nrd}_{D/K}(s) = \mathrm{Nrd}_{D/K}(g^i c)$ for suitable i in $\mathbb{Z}$ and c in L. Writing $t = s(g^i c)^{-1}$, we have $P = tg^i cLc^{-1}g^{-i}t^{-1} = tLt^{-1}$ and $\mathrm{Nrd}_{D/K}(t) = 1$. Consequently, $x \in P^{(1)}y^{-1} \subset t^{-1}L^{(1)}tL^{(1)}$. Q.E.D.

A noteworthy consequence of Theorem 1.8 is that any element of $D^{(1)}$ is the product of no more than two commutators. Whether this can be lowered to one commutator is unknown.

1.4.4. Filtrations of D^* and $D^{(1)}$. (Cf. Riehm [1].) The material in this section will be used only in §9.5, and therefore may be skipped on the first reading.

As before, let D be a skew field of index n over a local field K. We shall use the same notation introduced in §1.4.2–1.4.3. Also, we set $U_i = 1+\mathfrak{P}_D^i$, $C_i = U_i \cap D^{(1)}$, for $i \geq 1$, and $U_0 = U_D = \mathcal{O}_D^*$ and $C_0 = D^{(1)}$. It follows from (1.16) that U_i and C_i are normal subgroups of D^* (called the *congruence subgroups* of D and $D^{(1)}$ respectively, of level $\mathfrak{P}_D^i$ or simply i). Since U_D and $D^{(1)}$ are clearly compact groups, and U_i and C_i are open in U_D and $D^{(1)}$ respectively (and, moreover, generate a base of neighborhoods of the identity), and the indexes $[U : U_i]$ and $[D^{(1)} : C_i]$ are finite. We shall describe the structure of the factors U_i/U_{i+1} and C_i/C_{i+1}.

PROPOSITION 1.8. *There are natural isomorphisms*

$$\varrho_0 : U_0/U_1 \to l^*$$
$$\varrho_i : U_i/U_{i+1} \to l^+ \quad i \geq 1 \quad \textit{(additive group of } l\textit{)}.$$

Moreover $\varrho_0(C_0) = l^{(1)} = \{x \in l^* : N_{l/k}(x) = 1\}$; $\varrho_i(C_i) = l$ *if* $i \not\equiv 0 \pmod n$ *and* $\varrho_i(C_i) = l^{(0)} = \{x \in l : \mathrm{Tr}_{l/k}(x) = 0\}$ *if* $i \equiv 0 \pmod n$.

PROOF: As above, for a in $\mathcal{O}_D$ let $\bar{a}$ denote its image in $l = \mathcal{O}_D/\mathfrak{P}_D$. Then ϱ_0 is induced by $a \mapsto \bar{a}$ and ϱ_i $(i \geq 1)$ is induced by $1 + a\Pi^i \mapsto \bar{a}$. (Note that ϱ_i depends on the choice of the uniformizing parameter Π.) We computed the image of $\varrho_0(C_0)$ in the proof of Theorem 1.8. To compute $\varrho_i(C_i)$ $(i \geq 1)$ we shall require

LEMMA 1.7. $\mathrm{Nrd}_{D/K}(1 + \mathfrak{P}_D^i) = 1 + \mathfrak{p}^j$, *where* j *is the smallest integer* $\geq i/n$. The proof follows easily from Proposition 1.3.

Now for x in l take a in $\mathcal{O}_D$ such that $\bar{a} = x$. Let $z = 1 + a\Pi^i$. Then $t = \mathrm{Nrd}_{D/K}(z) \in 1 + \mathfrak{p}^j$ where j is the smallest integer $\geq i/n$. If $i \not\equiv 0 \pmod n$ then $j \geq \frac{i+1}{n}$, and by Lemma 1.7 there is y in U_{i+1} satisfying $\mathrm{Nrd}_{D/K}(y) = t$. Setting $z_1 = zy^{-1}$, we have $\mathrm{Nrd}_{D/K}(z_1) = 1$, i.e., $z_1 \in C_i$ and $\varrho_i(z_1) = x$. Thus $\varrho_i(C_i) = l$ for $i \not\equiv 0 \pmod n$.

Now let $i = jn$. Since $\mathcal{O}_D = \mathcal{O}_L + \mathfrak{P}_D$, we have

$$\mathfrak{P}_D^i = \mathcal{O}_L\pi^j + \mathfrak{P}_D\pi^j = \mathfrak{P}_L^j + \mathfrak{P}_D^{i+1}$$

(where $\mathcal{O}_L$, $\mathfrak{P}_L$ respectively are the ring of integers and valuation ideal of L; note that $\mathfrak{P}_L = \mathcal{O}_L\pi$ for the uniformizing parameter π in K, since L/K is unramified). It follows that $U_i = (U_i \cap L^*)U_{i+1}$ and $U_i \cap L^* = 1 + \mathfrak{P}_L^j$. Therefore if $z \in U_i$ and $z = st$, where $s \in U_i \cap L^*$, $t \in U_{i+1}$, then $N_{L/K}(s) = \mathrm{Nrd}_{D/K}(t)^{-1} \in 1 + \mathfrak{P}^{j+1}$. On the other hand, if $s = 1 + r\pi^j$ for r in $\mathcal{O}_L$, then $N_{L/K}(s) = \prod_{m=0}^{n-1} \varphi^m(1 + r\pi^j) \equiv 1 + \mathrm{Tr}_{L/K}(r)\pi^j \pmod{\mathfrak{p}^{j+1}}$. Thus $\mathrm{Tr}_{L/K}(r) \equiv 0 \pmod{\mathfrak{p}}$, whence $\mathrm{Tr}_{l/k}(\bar{r}) = 0$ and $\varrho_i(C_i) \subset l^{(0)}$. Conversely, if $\mathrm{Tr}_{L/K}(r) \equiv 0 \pmod{\mathfrak{p}}$ then for $s = 1 + r\pi^j$ we have $N_{L/K}(s) \in 1 + \mathfrak{p}^{j+1}$, so there is a t in $1 + \mathfrak{P}_L^{j+1}$ satisfying $N_{L/K}(s) = N_{L/K}(t)$, and the element $z = st^{-1} \in L^{(1)} \cap (1 + \mathfrak{P}_L^j)$ satisfies $\varrho_i(z) \equiv \bar{r}$. Q.E.D.

COROLLARY: For any $i \geq 0$ the quotient groups U_0/U_i and C_0/C_i are finite solvable.

The solvability of the quotient groups U_0/U_i and C_0/C_i is actually a direct consequence of our proposition. As we have noted above, U_i and C_i are a base of the neighborhoods of the identity in U_0 and C_0 respectively, and

therefore (cf. §3.3) $U_0 = \varprojlim U_0/U_i$, and $C_0 = \varprojlim C_0/C_i$ are prosolvable groups.

Now, following Riehm [1], we define the mutual commutator groups $[C_0, C_i]$ and $[C_1, C_i]$ $(i \geq 1)$. To do so we shall need one computation.

LEMMA 1.8. *Let* $x = 1 + a\Pi^i$, $y = 1 + b\Pi^j$, *where* $a, b \in \mathcal{O}_D$, $i, j \geq 1$. *Then the commutator* $[x, y] = xyx^{-1}y^{-1}$ *has the form* $1 + c\Pi^{i+j}$, *where* $\bar{c} = \bar{a}\sigma^i(\bar{b}) - \sigma^j(\bar{a})\bar{b}$ *(here, as in §1.4.2,* σ *is the automorphism of* l *over* k *given by* $\bar{d} \mapsto \overline{\Pi d \Pi^{-1}}$*). In particular,* $[U_i, U_j] \subset U_{i+j}$.

PROOF: Write (s, t) for $st - ts$. Then we can easily verify that

$$[x, y] = 1 + (x - 1, y - 1)x^{-1}y^{-1},$$

from which it follows that

$$[x, y] = 1 + (a\Pi^i b\Pi^j - b\Pi^j a\Pi^i)x^{-1}y^{-1} = 1 + c\Pi^{i+j},$$

where $c = (a\Pi^i b\Pi^{-i} - b\Pi^j a\Pi^{-j})(\Pi^{i+j}x^{-1}y^{-1}\Pi^{-(i+j)})$. If we pass to the residue and bear in mind that $\bar{x} = \bar{y} = 1$, we obtain the necessary result.

THEOREM 1.9. *Let* $n > 2$. *Then*

(1) $[C_1, C_i] = C_{i+1}$ *for any* $i \geq 1$;

(2) $$[C_0, C_i] = \begin{cases} C_i, & \text{if } i \not\equiv 0 \pmod n \\ C_{i+1}, & \text{if } i \equiv 0 \pmod n. \end{cases}$$

In particular, $[C_0, C_0] = C_1$.

PROOF: First we shall show that $\varrho_{i+1}([C_1, C_i]) = \varrho_{i+1}(C_{i+1})$. Indeed it follows from Lemma 1.8 and Proposition 1.8 that the image $\varrho_i([C_1, C_i])$ is generated as an abelian group by elements of the form $\alpha\sigma(\beta) - \sigma^i(\alpha)\beta$, where $\alpha \in l$, and $\beta \in l$ or $l^{(0)}$, depending on whether or not i is divisible by n. We leave it to the reader to show that these elements generate l or $l^{(0)}$ respectively, which is $\varrho_{i+1}(C_{i+1})$. Thus, for any i

$$[C_1, C_i]C_{i+2} = C_{i+1}. \tag{1.19}$$

Now we shall show that actually $[C_1, C_i] = C_{i+1}$. We can either argue directly, as does Riehm, or use a result presented in Chapter 3 (cf. Theorem 3.3) from which it follows, in particular, that any non-central normal subgroup of $D^{(1)}$ is open (it goes without saying that the proof of Theorem 3.3 does not rely on Theorem 1.9). Then for a suitable j we

have $[C_1, C_i] \supset C_j$, and we may take j to be the smallest integer with this property. Suppose that $j > i+1$; then $j-2 \geq i$, so that by (1.19) we have

$$[C_1, C_i] \supset [C_1, C_{j-2}]C_j = C_{j-1},$$

which contradicts the definition of j. Thus, $j = i+1$, proving the first assertion.

It follows from assertion (1) that $[C_0, C_i] \supset [C_1, C_i] = C_{i+1}$, so to prove (2) we need only show that

$$\varrho_i([C_0, C_i]) = \begin{cases} l, & \text{if } i \not\equiv 0 \pmod{n} \\ 0, & \text{if } i \equiv 0 \pmod{n}. \end{cases} \tag{1.20}$$

Direct computation shows that for $x \in U_D$ and $y = 1 + a\Pi^i$, $i \geq 1$, we have $\varrho_i([x,y]) = (\bar{x}\sigma^i(\bar{x})^{-1} - 1)\bar{a}$. If $i \equiv 0 \pmod{n}$, then clearly $\varrho_i([x,y]) = 0$. But if $i \not\equiv 0 \pmod{n}$, then, using the structure of finite fields, we can easily establish the existence of an element α in $l^{(0)}$ such that $\sigma^i(\alpha) \neq \alpha$. Choosing an element x from $D^{(1)}$ such that $\bar{x} = \alpha$, we obtain the first assertion of (1.20). To complete the proof of Theorem 1.9 we have only to note that always $[C_0, C_0] \subset C_1 = [C_0, C_1]$, and thus $[C_0, C_0] = C_1$.

REMARK: With a slight refinement of the above argument one can also consider the case $n = 2$. The results are as follows (cf. Riehm [1]):

If $p = \operatorname{char} K \neq 2$ then the assertions of Theorem 1.9 hold; for $n = p = 2$ the analog of assertion (1) assumes the form

$$[C_1, C_{2i+1}] = C_{2i+2} \quad \text{if either } |k| > 2 \text{ or } i \geq 1;$$
$$[C_1, C_{2i}] = C_{2(i+1)} \quad \text{for all } i.$$

If $|k| = 2$ then $[C_1, C_1]$ contains C_4 but does not contain C_3. The second assertion of Theorem 1.9 always holds; in particular $[C_0, C_0] = C_1$.

COROLLARY: $C_0 = L^{(1)}[C_0, C_0]$ where L is a maximal unramified subfield of D.

For $n > 2$ (respectively $n = 2$) this follows from Theorem 1.9 and Proposition 1.8 (respectively, from the remark and Proposition 1.8). Another proof, which does not distinguish between $n > 2$ and $n = 2$, is immediate from Theorem 1.8.

In §9.5 we shall need to view the group $F(i) = C_i/C_{i+1}$ $(i \geq 1)$ as a module over the group $\Delta = C_0/C_1$, by means of the action of C_0 by conjugation (note by Theorem 1.9 that C_1 acts trivially on $F(i)$). Using ϱ_0 and ϱ_i and Proposition 1.8, we can identify Δ and $F(i)$ respectively with $l^{(1)}$ and $l^{(0)}$, depending on whether or not i is divisible by n. Then a simple computation shows that the Δ-module structure of $F(i)$ is given by

$$\delta \cdot x = \delta\sigma^i(\delta)^{-1}x, \qquad \text{for } \delta \in \Delta,\ x \in F(i) \tag{1.21}$$

(the product on the right is taken in l).

PROPOSITION 1.9. *If $i \not\equiv 0 \pmod{n}$ then $F(i)$ is a simple Δ-module, except when l/k is F_9/F_3 or F_{64}/F_4 (where F_q is the finite field of q elements). In the latter case the Δ-submodules of $F(i) \simeq F_{64}$ correspond to the vector subspaces of F_{64} over F_8.*

PROOF: Let m denote the subfield of l generated over the prime subfield by elements of the form $\delta\sigma^i(\delta)^{-1}$ for δ in $l^{(1)}$. Then the assertion is clearly equivalent to $m = l$ if l/k is distinct from F_9/F_3, F_{64}/F_4, and to $m = F_8$ if l/k is F_{64}/F_4. The proof is elementary and is left to the reader.

Using Proposition 1.9, Riehm obtains a complete description of the normal subgroups of C_0. Since we will not need these results further on, we shall confine ourselves to stating the basic theorems without analyzing the exceptional cases. For this we shall set $E_r = (K^* \cap C_0)C_r$ and shall say that a normal subgroup $N \subset C_0$ has *level* r if $N \subset E_r$ but $N \not\subset E_{r+1}$. Since $\bigcap_r E_r = K^* \cap C_0$, any noncentral normal subgroup in C_0 has a certain level.

THEOREM 1.10. *Suppose D is not a quaternion algebra over a finite extension of $\mathbb{Q}_2$. If $N \subset C_0$ is a normal subgroup of level r, then*

$$C_{r+1} \subset N \subset E_r.$$

If $n \nmid r$ and the Δ-module $F(r)$ is simple, then the stronger condition $C_r \subset N \subset E_r$ holds.

Note that $C_r \subset N \subset E_r$ means that N may differ from a congruence subgroup only by a central subgroup, and thus we obtain a comprehensive description of the normal subgroups.

Proposition 1.9 can be used for other ends — namely, to help describe the module $B = B\big(F(1), F(r)\big)$ of Δ-bilinear maps $b\colon F(1) \times F(r) \to F_p = \mathbb{Z}/p\mathbb{Z}$, where $p = \operatorname{char} k$ and the operation of Δ on F_p is trivial.

THEOREM 1.11 (PRASAD, RAGHUNATHAN [4]).

(1) *If $r \not\equiv -1 \pmod{n}$ then $B = 0$.*
(2) *If $r \equiv -1 \pmod{n}$, $n > 2$, then B consists precisely of all maps of the following form:*

$$b(\lambda)(x,y) = \operatorname{Tr}_{l/F_p}(\lambda x\sigma(y)) \text{ where } \lambda \in l \tag{1.22}$$

in case l/k is distinct from F_{64}/F_4;

$$b(\lambda,\mu)(x,y) = \operatorname{Tr}_{l/F_p}(\lambda x\sigma(y) + \mu x\sigma(y)^8) \text{ where } \lambda,\ \mu \in l \tag{1.23}$$

in case $l/k \simeq F_{64}/F_4$.

(The appearance of the trace in (1.22) and (1.23) is not accidental. Indeed, for any finite separable field extension P/M, one has the nondegenerate bilinear form $f(x,y) = \mathrm{Tr}_{P/M}(xy)$, so any M-linear functional $\varphi: P \to M$ is given by $\varphi(x) = \mathrm{Tr}_{P/M}(ax)$ for suitable a in P.)

PROOF: Let $r, s > 0$ and $r + s \equiv 0 \pmod{n}$. Then for any λ in l the bilinear form given by

$$b_r(\lambda)(x,y) = \mathrm{Tr}_{l/F_p}(\lambda x \sigma^r(y)) \tag{1.24}$$

is Δ-invariant. Actually, by (1.21) for any δ in Δ we have

$$\begin{aligned} b_r(\lambda)(\delta\cdot x, \delta\cdot y) &= \mathrm{Tr}_{l/F_p}(\lambda(\delta\sigma^r(\delta)^{-1})x\sigma^r(\delta\sigma^s(\delta)^{-1}y)) \\ &= \mathrm{Tr}_{l/F_p}(\lambda(\delta\sigma^{r+s}(\delta)^{-1})x\sigma^r(y)) = b_r(\lambda)(x,y), \end{aligned}$$

since $r + s \equiv 0 \pmod{n}$. If moreover $r \not\equiv 0 \pmod{n}$, then $F(r) \simeq l$ and $F(s) \simeq l$, so $b_r(s)$ yields a nondegenerate bilinear map $F(r) \times F(s) \to F_p$, i.e., it defines an isomorphism $F(r)$ with the dual module $\widehat{F(s)} = \mathrm{Hom}(F(s), F_p)$. If also $r \equiv 0 \pmod{n}$, then $F(r)$ and $F(s)$ are each trivial Δ-modules, and therefore also $F(r) \simeq F(s)$. Since clearly $B(F(r), F(s)) = \mathrm{Hom}_\Delta(F(r), \widehat{F(s)})$, to prove the theorem's first assertion it suffices to show that $\mathrm{Hom}_\Delta(F(r), F(s)) = 0$ if $r \not\equiv s \pmod{n}$.

Let $\varphi \in \mathrm{Hom}_\Delta(F(r), F(s))$, $\varphi \not\equiv 0$. Then for any a in $F(r)$ and any δ in Δ we have

$$\varphi(\delta(\sigma^r(\delta))^{-1}a) = \delta(\sigma^s(\delta))^{-1}\varphi(a). \tag{1.25}$$

Let $\mathcal{F}_1$ and $\mathcal{F}_2$ denote the additive subgroups of l generated by elements of the form $\delta(\sigma^r(\delta))^{-1}$ and $\delta(\sigma^s(\delta))^{-1}$ respectively. If we choose a in $F(r)$ such that $\varphi(a) \neq 0$, then (1.25) yields that if $\delta_i \in \Delta$ and $\sum \delta_i(\sigma^r(\delta_i))^{-1} = 0$ then $\sum \delta_i(\sigma^s(\delta_i))^{-1} = 0$; consequently $\psi: \delta(\sigma^r(\delta))^{-1} \mapsto \delta(\sigma^s(\delta))^{-1}$ extends to an additive homomorphism from $\mathcal{F}_1$ to $\mathcal{F}_2$. Moreover, $\mathcal{F}_1$ and $\mathcal{F}_2$ are clearly closed under multiplication, i.e., they are finite fields, and the extension of ψ is actually an isomorphism from $\mathcal{F}_1$ to $\mathcal{F}_2$. It follows that $\psi(x) = x^{p^l}$ for a suitable integer l. Thus

$$(\delta(\sigma^r(\delta))^{-1})^{p^l} = \delta(\sigma^s(\delta))^{-1} \tag{1.26}$$

for any δ in Δ. Let $k = F_{p^a}$. Then $\Delta = \{x^{p^a-1} : x \in l^*\}$ and $\sigma(x) = x^{p^{ab}}$ for a suitable integer b, so that (1.26) yields

$$x^{-p^l(p^{abr}-1)(p^a-1)} = x^{-(p^{abs}-1)}$$

for all x in l^*, whence $p^l(p^{abr}-1)(p^a-1) \equiv p^{abs}-1 \pmod{p^{an}-1}$. But, from the last equation (cf. Prasad, Raghunathan [2], supplement to §7) it follows that $br \equiv bs \pmod{n}$, which means $r \equiv s \pmod{n}$ since $(b,n) = 1$, thus proving the first assertion.

To prove the second assertion let us first suppose that l/k is distinct from F_{64}/F_4, so that $F(r)$ is a simple Δ-module. Let $b = b(x,y) \in B$. Then $x \mapsto b(x,1)$ is an F_p-linear map from l to F_p, and hence $b(x,1) = \mathrm{Tr}_{l/F_p}(\lambda x)$ for a suitable λ in l. Consider $b_0 = b - b_1(\lambda)$, where $b_1(\lambda)$ is given by (1.24). Since b and $b_1(\lambda)$ are Δ-invariant, for any x in $F(1)$ the set $x^\perp = \{y \in F(r) : b_0(x,y) = 0\}$ is a Δ-submodule of $F(r)$ containing 1; thus $x^\perp = F(r)$ so $b_0 = 0$, i.e. $b = b_1(\lambda)$, as required.

We have yet to consider the case where $l = F_{64}$, $k = F_4$. Here the irreducible Δ-submodules of $F(r)$ correspond to vector subspaces of l over F_8, and the only nontrivial automorphism of F_{64}/F_8 has the form $x \mapsto x^8$. Let $z \in l/F_8$. Then, reasoning as above, we can establish the existence of $\theta, \omega \in l$ such that

$$\begin{aligned} b(x,1) &= \mathrm{Tr}_{l/F_p}(\theta x) \\ b(x,z) &= \mathrm{Tr}_{l/F_p}(\omega x) \end{aligned}$$

for all x in l. Since $z^8 \neq z$, one can find λ, μ in l satisfying the equations

$$\begin{aligned} \lambda + \mu &= \theta \\ \lambda\sigma(z) + \mu\sigma(z)^8 &= \omega. \end{aligned}$$

Since in this case $\delta(\sigma^r(\delta))^{-1} \in F_8$ for all δ in $l^{(1)}$, the bilinear map $b(\lambda,\mu)$ (cf. (1.23)) is Δ-invariant. Then $b_0 = b - b(\lambda,\mu)$ is also Δ-invariant. It follows that for any x in $F(1)$ the space $x^\perp$ is a Δ-submodule of $F(r)$, containing 1 and z and hence $x^\perp = F(r)$. Thus $b_0 = 0$ and $b = b(\lambda,\mu)$. Q.E.D.

1.5. Simple algebras over algebraic number fields.

1.5.1. The Brauer group. Let A be a simple algebra over an algebraic number field K. For any $v \in V^K$, $A_v = A \otimes_K K_v$ is also a simple algebra and, according to the notation in §1.4.1, $[A] \to [A_v]$ defines the Brauer group homomorphism $\mathrm{Br}(K) \xrightarrow{\theta_v} \mathrm{Br}(K_v)$. To describe $\mathrm{Br}(K)$ we must consider the product

$$\theta : \prod_{v\in V^K} \theta_v : \mathrm{Br}(K) \to \prod_{v\in V^K} \mathrm{Br}(K_v).$$

In §1.4.2 we saw that for v in V_f^K we have $\mathrm{inv}_{K_v}: \mathrm{Br}(K_v) \to \mathbb{Q}/\mathbb{Z}$. In order to consider all the valuations in a unified manner we stipulate that we shall

regard the invariant of the quaternion skew field over $K_v = \mathbb{R}$ to be the class in $\mathbb{Q}/\mathbb{Z}$ that contains $\frac{1}{2}$. Then $\mathrm{inv}_{K_v}\colon \mathrm{Br}(K_v) \to \mathbb{Q}/\mathbb{Z}$ is defined for all v and is injective.

THEOREM 1.12 (BRAUER, HASSE, NOETHER). *θ is an injective map, and its image consists of $a = (a_v) \in \prod_v \mathrm{Br}(K_v)$ such that $a_v = 0$ for almost all v and $\sum_v \mathrm{inv}_{K_v}(a_v) = 0$.*

Thus any finite-dimensional skew field D over K is determined up to isomorphism by the invariants $\mathrm{inv}_{K_v}[D_v]$ of the algebras $D_v = D \otimes_K K_v$, which for the sake of brevity we shall write as $\mathrm{inv}_v D$. Conversely, for any choice of invariants, almost all of which equal 0 and the sum of which also equals 0, there is a skew field over K which has the given invariants.

Several consequences follow from the injectivity of θ. Firstly, by §1.4.1, a field extension P of K of degree n equal to the index of D, is isomorphic to a maximal subfield of D if and only if $D_v \otimes_{K_v} P_w$ is a matrix algebra for all v in V^K and all $w|v$ (the latter condition is equivalent to saying that the local dimensions $[P_w : K_v]$ are divisible by the index of D_v for all v in V^K and all $w|v$). Then, by applying the Grünwald-Wang theorem from class field theory (cf., for example, Artin–Tate [1]), we conclude that D contains a maximal subfield $L \subset D$ which is a cyclic extension of K.

Taking into account the structure of skew fields over local fields, it is natural to pose the more subtle question of whether there always exists a maximal subfield $L \subset D$ which is a cyclic extension of K and for which L_v/K_v are unramified extensions for all v in V_f^K such that D_v is a skew field. Unfortunately, it is not always the case (counterexamples do exist even over $\mathbb{Q}$); however, this condition can be obtained by imposing several restrictions on D, used in Platonov, Rapinchuk [4].

The Grünwald-Wang theorem, used together with Theorem 1.12, enables us to establish that over algebraic number fields, just as over local fields, the exponent of a simple algebra is the same as its index, and, in particular, the only skew fields of exponent 2 are generalized quaternions.

1.5.2. Multiplicative structure. Let D be a skew field of index n over an algebraic number field K. We shall describe the image of the reduced norm $\mathrm{Nrd}_{D/K}(D^*)$ and shall show that $SL_1(D)$ is the commutator group $[D^*, D^*]$ of the multiplicative group D^*.

THEOREM 1.13 (EICHLER). *The group $\mathrm{Nrd}_{D/K}(D^*)$ is the set of elements of K^* that are positive under all real valuations v in V_∞^K such that $D_v \not\simeq M_n(K_v)$.*

PROOF: See Weil [6], pp. 279–284 (cf. also §6.7).

THEOREM 1.14 (WANG). *$SL_1(D) = [D^*, D^*]$.*

Wang's original proof of this theorem is quite complicated and uses important results from number theory. We shall present a modified argument (cf. Platonov [15], Yanchevskiĭ [1]), based exclusively on Eichler's theorem.

First, we shall obtain a reduction of the proof of Theorem 1.14 to skew fields having prime power index. We shall need several results about the Dieudonné determinant (cf. Artin [1], Dieudonné [2]). Let $GL_m(D)$ be the group of invertible elements of a matrix algebra $A = M_m(D)$. Then there exists a surjective homomorphism $GL_m(D) \xrightarrow{\delta} D^*/[D^*, D^*]$, called the *Dieudonné determinant*, whose kernel contains the commutator group $[GL_m(D), GL_m(D)]$, and for which

$$\delta\left(\begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_m \end{pmatrix}\right) = a_1 \dots a_m [D^*, D^*].$$

Also, it is well known that in all cases, with one exception – $m = 2$, $D = F_2$, the field with two elements – $\ker \delta$ is $[GL_m(D), GL_m(D)]$. In particular, δ induces an isomorphism $SK_1(A) \simeq SK_1(D)$ and therefore for any field P (distinct from F_2 for $m = 2$) $SL_m(P)$ is the commutator group $GL_m(P)$.

LEMMA 1.9. *Let $a \in SL_1(D)$ and $a \in [(D \otimes_K B)^*, (D \otimes_K B)^*]$, where B is an associative m-dimensional K-algebra with 1. Then $a^m \in [D^*, D^*]$.*

PROOF: The regular representation $B \hookrightarrow M_m(K)$ is exact and induces the embedding $D \otimes B \to M_m(D)$. Moreover, the element a in D goes to the matrix

$$\begin{pmatrix} a & & 0 \\ & \ddots & \\ 0 & & a \end{pmatrix}.$$

Now if $a \in SL_1(D)$ and $a \in [(D \otimes_K B)^*, (D \otimes_K B)^*]$, then clearly

$$\begin{pmatrix} a & & 0 \\ & \ddots & \\ 0 & & a \end{pmatrix} \in [GL_m(D), GL_m(D)],$$

so that by applying the Dieudonné determinant we obtain $a^m \in [D^*, D^*]$, as required.

Lemma 1.9 yields

COROLLARY 1.1. *For a skew field D of index n, the group $SK_1(D)$ has exponent n.*

Indeed, if $L \subset D$ is a maximal subfield, then $[L : K] = n$ and $D \otimes_K L = M_n(L)$. Therefore, applying Lemma 1.9 to $B = L$ and bearing in mind that $SL_n(L) = [GL_n(L), GL_n(L)]$, we obtain our assertion.

Furthermore, it is well known that if $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ then

$$D = D_1 \otimes_K \dots \otimes_K D_r,$$

where D_i is a skew field of index $p_i^{\alpha_i}$. With this notation, we have

COROLLARY 1.2. *If $SK_1(D_i) = 1$ for all $i = 1, \dots, r$, then $SK_1(D) = 1$.*

For the proof, let B_i denote the tensor product $\bigotimes_{j \neq i} D_j^0$ of the corresponding opposite algebras. Then B_i is an n_i^2-dimensional K-algebra, where $n_i = n/p_i^{\alpha_i}$; moreover, $D \otimes_K B_i \simeq M_{n_i^2}(D_i)$ for all $i = 1, \dots, r$. A consequence of the properties of the Dieudonné determinant and the triviality of $SK_1(D_i)$ is that $SL_{n_i^2}(D_i) = [GL_{n_i^2}(D_i), GL_{n_i^2}(D_i)]$; it follows that for any a in $SL_1(D)$ we have $a^{n_i^2} \in [D^*, D^*]$ by Lemma 1.9. But the numbers n_i^2 $(i = 1, \dots, r)$ are relatively prime, therefore $u_i n_1^2 + \dots + u_r n_r^2 = 1$ for suitable integers u_i, whence $a = (a^{n_1^2})^{u_1} \dots (a^{n_r^2})^{u_r} \in [D^*, D^*]$, as we wished to show.

Thus we need only prove Theorem 1.14 for D of index p^α, where p is a prime number and $\alpha \geq 0$. We shall do so by induction on α, noting that the assertion clearly holds for $\alpha = 0$. Now, let us suppose that for any skew field Δ of index $p^{\alpha-1}$ over an algebraic number field we have $SK_1(\Delta) = 1$; then we shall show also that $SK_1(D) = 1$ for D of index p^α. Let $a \in SL_1(D)$. It suffices to find an extension F/K of degree coprime to p, such that $a \in [(D \otimes_K F)^*, (D \otimes_K F)^*]$, since in that case $a^{[F:K]} \in [D^*, D^*]$, by Lemma 1.9, while also $a^{p^\alpha} \in [D^*, D^*]$ by Corollary 1.1. For then, since p and $[F : K]$ are coprime, there exist $s, t \in \mathbb{Z}$ for which $s[F : K] + tp^\alpha = 1$, and then $a = (a^{[F:K]})^s (a^{p^\alpha})^t \in [D^*, D^*]$, as required. To construct F let us consider a maximal subfield $L \subset D$ containing a. Let P be a normal closure of L over K, and $\mathcal{G} = \mathrm{Gal}(P/K)$ the corresponding Galois group. Consider the Sylow p-subgroup $\mathcal{G}_p \subset \mathcal{G}$, and take $F = P^{\mathcal{G}_p}$. Then, $[F : K]$ is clearly coprime to p. We shall show that $a \in [(D \otimes_K F), (D \otimes_K F)]$.

$\mathrm{Gal}(P/F)$ is $\mathcal{G}_p$. Let $\mathcal{H} \subset \mathcal{G}_p$ be the subgroup corresponding to the subfield $LF \subset P$. A consequence of the properties of p-groups is that there exists a normal subgroup $\mathcal{N} \subset \mathcal{G}_p$ of index p, containing $\mathcal{H}$. Then the corresponding fixed field $M = P^{\mathcal{N}}$ is a cyclic extension of F of degree p, contained in LF.

If $\alpha = 1$, then $M = LF$ is itself a cyclic extension of F of degree p. Then $N_{M/F}(a) = 1$ since $a \in SL_1(D)$, so that by Hilbert's Theorem 90 $a = \sigma(b)/b$ for suitable b in LF, where σ is the generator of $\mathrm{Gal}(M/F)$. But by the Skolem-Noether theorem, there is an element g in $(D \otimes_K F)^*$ such that $\sigma(b) = gbg^{-1}$ (identifying LF with $L \otimes_K F \subset D \otimes_K F$), and consequently $a = gbg^{-1}b^{-1} \in [(D \otimes_K F)^*, (D \otimes_K F)^*]$, as required. (Note that we have not yet used the hypothesis that K is an algebraic number field, and thus $SK_1(D) = 1$ for any skew field D of index p over an arbitrary field K.)

When $\alpha > 1$, let Δ denote the centralizer of M in $D \otimes_K F$. Then Δ is a skew field of index $p^{\alpha-1}$ with center M (by the double centralizer theorem, cf. Pierce [1]). Clearly $a \in \Delta$, and moreover

$$1 = \mathrm{Nrd}_{(D \otimes_K F)/F}(a) = N_{LF/F}(a) = N_{M/F}(N_{LF/M}(a)) = N_{M/F}(\mathrm{Nrd}_{\Delta/M}(a)).$$

Therefore $t = \mathrm{Nrd}_{\Delta/M}(a)$ has the form

$$t = \sigma(s)/s \tag{1.27}$$

for some s in M, where σ is the generator of $\mathrm{Gal}(M/F)$. By the Skolem-Noether theorem there is a g in $(D \otimes_K F)^*$ satisfying $\sigma(b) = gbg^{-1}$ for all b in M. We see at once that $g\Delta g^{-1} = \Delta$, since Δ is the centralizer of M and $\mathrm{Nrd}_{\Delta/M}(gxg^{-1}) = g\,\mathrm{Nrd}_{\Delta/M}(x)g^{-1}$ for any x in Δ. Now suppose we can choose an element s in (1.27) from the image of $\mathrm{Nrd}_{\Delta/M}(\Delta^*)$ (s in (1.27) is determined up to multiplication by an element from F^*). If $s = \mathrm{Nrd}_{\Delta/M}(z)$, where $z \in \Delta$, then $\mathrm{Nrd}_{\Delta/M}(gzg^{-1}z^{-1}) = \sigma(s)/s = \mathrm{Nrd}_{\Delta/M}(a)$, so that $a' = a(gzg^{-1}z^{-1})^{-1} \in SL_1(\Delta)$. By induction

$$SL_1(\Delta) = [\Delta^*, \Delta^*] \subset [(D \otimes_K F)^*, (D \otimes_K F)^*],$$

from which we conclude $a \in [(D \otimes_K F)^*, (D \otimes_K F)^*]$.

We have yet to show that s in (1.27) can be taken from $\mathrm{Nrd}_{\Delta/M}(\Delta^*)$. To do so we shall use Theorem 1.13. If p is odd, then $\Delta_w = \Delta \otimes_M M_w$ is a full matrix algebra for all w in V_∞^M; consequently $\mathrm{Nrd}_{\Delta/M}(\Delta^*) = M^*$, and we have nothing to prove. Now let $p = 2$. In this case M is a quadratic extension of F, and $\mathrm{Nrd}_{\Delta/M}(\Delta^*)$ is the subgroup consisting of those m in M which are positive with respect to all real w in V_∞^M such that Δ_w is not a full matrix algebra; we shall let S denote the set of all such w. Let S_0 consist of the restriction of the valuations $w \in S$ to F. Then above each v in S_0 there are two valuations $w', w'' \in S$, and $M_{w'} = M_{w''} = F_v$; moreover $w'' = w'\sigma$. If s is an arbitrary element satisfying (1.27), then by $t = \sigma(s)/s \in \mathrm{Nrd}_{\Delta/M}(\Delta^*)$, s has the same sign with respect to w' and w''. Therefore there is f_v in K_v such that sf_v is positive with respect to w' and w''. Using Theorem 1.4 on weak approximation, we choose an element f in K such that f and f_v have the same sign in K_v for all v in S_0. Now, setting $s_1 = sf$, we obtain $t = \sigma(s)/s = \sigma(s_1)/s_1$ and $s_1 \in \mathrm{Nrd}_{\Delta/M}(\Delta^*)$, which completes the proof of Theorem 1.14. Q.E.D.

1.5.3. Lattices and orders. Let K be an algebraic number field, $\mathcal{O}$ be its ring of integers. A *lattice* (or, to be more precise, an $\mathcal{O}$-lattice) in a finite-dimensional vector space V over K is a finitely generated $\mathcal{O}$-submodule $L \subset V$ containing some base of V over K. (Usually we shall take $V = K^n$). The lattice $L \subset V$ is said to be *free* if the $\mathcal{O}$-module L is free, i.e., has a base. If $\mathcal{O}$ is a principal ideal domain or, equivalently, the class number of K equals 1, then any lattice is free. In general any lattice $L \subset V$ has a *pseudobase*, i.e., if $\dim_K V = n$ then there exist $x_1, \dots, x_n$ such that $L = \mathcal{O}x_1 \oplus \cdots \oplus \mathcal{O}x_{n-1} \oplus \mathfrak{a}x_n$, where $\mathfrak{a} \subset \mathcal{O}$ is some ideal (cf. O'Meara [1]).

An *order* in a finite-dimensional K-algebra A is a subring $B \subset A$ containing the unit element of A which is an $\mathcal{O}$-lattice. An order is said to be *maximal* if it is not contained in a larger order.

The study of lattices and orders essentially reduces to the study of the corresponding local structures. Namely, by a local lattice in a finite-dimensional vector space V_{K_v} over K_v, where $v \in V_f^K$, we mean a finitely generated $\mathcal{O}_v$-submodule $L_v \subset V_{K_v}$ containing a base of V_{K_v}. Since $\mathcal{O}_v$ is a principal ideal domain, any local lattice has a base over $\mathcal{O}_v$. The definition of order and maximal order in a finite-dimensional K_v-algebra is now formulated in the obvious way. Clearly, if L is a lattice in a finite-dimensional vector space V over K (respectively, if B is an order in a finite-dimensional K-algebra A), then $L_v = L \otimes_{\mathcal{O}} \mathcal{O}_v$ (respectively, $B_v = B \otimes_{\mathcal{O}} \mathcal{O}_v$) is a lattice in the space $V_{K_v} = V \otimes_K K_v$ (respectively, in the algebra $A_{K_v} = A \otimes_K K_v$). Thus, for each lattice $L \subset V$ there is a corresponding set of localizations $\{ L_v \subset V_{K_v} : v \in V_f^K \}$. This raises the question of how far L is determined by its localizations L_v.

THEOREM 1.15.

(1) $L = \bigcap_v (V \cap L_v)$, *in particular a lattice is uniquely determined by its localizations;*
(2) *for any two lattices* $L, M \subset V$ *we have* $L_v = M_v$ *for almost all* v;
(3) *if* $L \subset V$ *is a lattice and* $\{N_v \subset V_{K_v}\}$ *is an arbitrary set of local lattices such that* $N_v = L_v$ *for almost all* v, *then there exists a lattice* $M \subset V$ *such that* $M_v = N_v$ *for all* v.

PROOF: Let L, M be two lattices, $x_1, \dots, x_n$ a base of V in L, and $y_1, \dots, y_r$ a finite system of generators of M as $\mathcal{O}$-module. Then $y_i = \sum_{j=1}^n a_{ij} x_j$ for suitable $a_{ij} \in K$. If we choose an integer m such that $ma_{ij} \in K$ for all i, j, we obtain $mM \subset L$. By interchanging L and M we also have l in $\mathbb{Z}$ such that $lL \subset M$, i.e., $L \subset \frac{1}{l} M$. If $v \notin V(lm)$ (notation as in §1.2.1), then $L_v = M_v$, thus proving the second assertion.

To prove assertions (1) and (3) it will be helpful to consider an embedding

of V in the corresponding adele space $V_{A_f} = V \otimes_K A_f$, where A_f is the ring of finite adeles of K. From the strong approximation theorem it follows that $L_{A_f(\infty)} = L \otimes_{\mathcal{O}} A_f(\infty) = \prod_{v \in V_f^K} L_v$ (where $A_f(\infty) = \prod_{v \in V_f^K} \mathcal{O}_v$ is the ring of integral finite adeles) is the closure of L in V_{A_f}. Therefore $L' = \prod_{v \in V_f^K} (V \cap L_v)$ is the closure of L in V in the induced topology, so to prove the first assertion we have only to establish that L is closed. To do so, let us take our base $x_1, \dots, x_n$ of V in L and put $M = \mathcal{O}x_1 + \cdots + \mathcal{O}x_n$. Since $\mathcal{O} = \bigcap_{v \in V_f^K} (K \cap \mathcal{O}_v)$, it follows that $M = \bigcap_{v \in V_f^K} (V \cap M_v)$. But $\prod_v M_v$, as well as $\prod_v L_v$, is open in V_{A_f}, so M is open, and consequently $L \subset V$ is open and closed.

Lastly, if a set of local lattices $N_v \subset V_{K_v}$ satisfies $N_v = L_v$ for almost all v, then $\prod_{v \in V_f^K} N_v$ is an open compact subgroup in V_{A_f} and therefore is commensurable with $\prod_{v \in V_f^K} L_v$ (i.e., their intersection has finite index in each of them). It follows that $M = \bigcap_{v \in V_f^K} (V \cap N_v)$ is commensurable with $L = \bigcap_{v \in V_f^K} (V \cap L_v)$, and therefore M is obviously the desired lattice. Q.E.D.

Next we shall look at orders in algebras, but shall limit ourselves to several questions on the existence of maximal orders and the embeddability of an arbitrary order in a maximal one, since precisely these questions arise in the study of maximal arithmetic and maximal compact subgroups of algebraic groups. To begin with, note that a consequence of Theorem 1.15 is

PROPOSITION 1.10. *An order* $B \subset A$ *is maximal if and only if for each* v *in* V_f^K *the order* $B_v \subset A_{K_v}$ *is maximal.*

Straightforward examples show that it is possible for arbitrary algebras not to have maximal orders. Our object is to prove that maximal orders always exist in finite-dimensional semisimple algebras. Recall that a *semisimple* K*-algebra* is the direct sum of a finite number of simple (not necessarily central) K-algebras. Thus, a finite-dimensional semisimple algebra has the form $A = \bigoplus_{i=1}^r M_{n_i}(D_i)$, where D_i is a finite-dimensional division algebra over K. For characteristic 0 the fact that an algebra A is semisimple is equivalent to $A \otimes_K \bar{K} = \bigoplus_{i=1}^r M_{m_i}(\bar{K})$ for suitable integers m_i (cf. Pierce [1]). Therefore it is natural to begin by considering maximal orders in a matrix algebra $A = M_n(K_v)$. Our discussion will be based on the study of the natural action of A on $V = K_v^n$, into which we incorporate elementary topological concepts related to compactness. For any lattice

$L \subset V$ put $A^L = \{ g \in M_n(K_v) : g(L) \subset L \}$, the *stabilizer* of L. Then with respect to the base of L this set A^L coincides with $M_n(\mathcal{O}_v)$, so, in particular, A^L is an order and an open compact subring (indeed, these are equivalent concepts).

PROPOSITION 1.11.

(1) *For any compact subring $B \subset A$ there is a lattice $L \subset V$ such that $B \subset A^L$;*
(2) *the ring A^L is a maximal order in A, for any lattice $L \subset V$;*
(3) *any order $B \subset A$ is contained in some maximal order, and there is only a finite number of such maximal orders.*

PROOF: Let $L_0 = \mathcal{O}_v^n$ be the lattice spanned by the standard base of $V = K_v^n$. Since A^{L_0} is open and B is compact, there exists a finite set $x_1, \dots, x_r$ in A such that $B \subset \bigcup_{i=1}^r (x_i + A^{L_0})$. It follows that the $\mathcal{O}_v$-submodule of $L \subset V$ generated by $B(L_0) = \bigcup_{x \in B} x(L_0)$ is actually generated by $L_0 \cup x_1(L_0) \cup \dots \cup x_r(L_0)$, or in other words is a lattice. Moreover, clearly $B(L) \subset L$, which proves the first assertion.

Now suppose A^L is contained in some order $B \subset A$. Since any order is clearly an open compact subring, $B \subset A^M$ for a suitable lattice $M \subset V$ by (1). Thus $A^L \subset A^M$ and our aim is to show that $A^L = A^M$. Replacing M by a lattice of the form αM for α in $\mathcal{O}_v \setminus \{0\}$ does not change the ring A^M, so we may assume that $M \subset L$, but $M \not\subset \pi L$, where π is a uniformizing parameter of K_v. Then we can choose a base $e_1, \dots, e_n$ of L such that $e_1, \pi^{\alpha_2} e_2, \dots, \pi^{\alpha_n} e_n$ constitute a base of M for suitable non-negative integers $\alpha_2, \dots, \alpha_n$. Consider a transformation g_i in A^L which interchanges the vectors e_1 and e_i while leaving fixed e_j for all $j \neq 1, i$. Since $A^L \subset A^M$ we have $g_i \in A^M$, whence $g_i(e_1) = e_i \in M$ and $\alpha_i = 0$. Consequently $L = M$, so $A^L = A^M$, proving the second assertion.

From (1) and (2) it follows that any order $B \subset A$ is contained in some maximal order $C = A^L$, so it remains to be shown that the set $\{C_l\}$ of maximal orders in A containing B is finite. We have $C_l = A^{M_l}$, $B \supset \pi^\alpha C$ for suitable lattices $M_l \subset V$ and some non-negative integer α. Then for any l we have $C_l \supset B \supset \pi^\alpha C$. We shall show that at the same time $\pi^\alpha C_l \subset C$. As in the proof of (2), without loss of generality we may assume that the lattices L and M_l have bases of the form $e_1, e_2, \dots, e_n$ and $e_1, \pi^{\alpha_2} e_2, \dots, \pi^{\alpha_n} e_n$ for $\alpha_i \geq 0$. Since $C_l \supset \pi^\alpha C$, then $C(M_l) \subset \pi^{-\alpha} C_l(M_l) = \pi^{-\alpha} M_l$. Again, using the above transformations $g_i \in C$, we obtain $\alpha_i \leq \alpha$, i.e., $\pi^\alpha L \subset M_l$. Then $\pi^\alpha C_l(L) \subset C_l(M_l) = M_l \subset L$, i.e., $\pi^\alpha C_l \subset C$. Thus $\pi^\alpha C \subset C_l \subset \pi^{-\alpha} C$, from which it follows that there is a finite number of distinct C_l since $[\pi^{-\alpha} C : \pi^\alpha C]$ is finite. This completes the proof of the proposition.

REMARK: A consequence of the description of maximal orders in $A = M_n(K_v)$ as stabilizers of lattices $L \subset V$ is that they are conjugate in A.

It is easy to deduce from this proposition the analogous assertions about maximal compact subgroups of $G = GL_n(K_v)$. For any lattice $L \subset V$ let G^L denote the group of automorphisms of L, i.e., $G^L = \{g \in G : g(L) = L\}$ (in general, for any subgroup $\Gamma \subset G$ we set $\Gamma^L = \{g \in \Gamma : g(L) = (L)\}$ and call Γ^L the stabilizer of L in Γ). Clearly $G^L = (A^L)^*$ can be identified with $GL_n(\mathcal{O}_v)$ with respect to the base of L, so G^L is an open compact subgroup of G and $\det g \in U_v$ for any g in G^L.

PROPOSITION 1.12.

(1) *For any compact subgroup $B \subset G$ there is a lattice $L \subset V$ such that $B \subset G^L$;*
(2) *G^L is a maximal compact subgroup of G for any lattice $L \subset V$; in particular any compact subgroup is contained in some maximal compact subgroup;*
(3) *all maximal compact subgroups of G are conjugate.*

The proof follows easily from Proposition 1.11.

From Proposition 1.11 one can easily derive a fundamental theorem on orders in semisimple algebras over local fields.

THEOREM 1.16. *Let A be a semisimple algebra over K_v. Then any order $B \subset A$ is contained in some maximal order, and moreover there is a finite number of maximal orders containing B.*

PROOF: Writing A as the direct sum of simple algebras, one reduces the proof to the case where A is simple. Let F be the center of A and $\mathcal{O}_F$ be the corresponding ring of integers. Then for any $\mathcal{O}_v$-order $B \subset A$ the product $\mathcal{O}_F B$ is simultaneously an $\mathcal{O}_v$-order and $\mathcal{O}_F$-order in A. From this remark it follows that we need only consider the case $F = K_v$. Clearly, to prove the theorem it suffices to show that the set $\{B_i\}$ of all orders in A containing B is finite. To do so we choose a finite extension P of K_v such that $A \otimes_{K_v} P \simeq M_n(P)$ and put $\tilde{B} = B \otimes_{\mathcal{O}_v} \mathcal{O}_P$, $\tilde{B}_i = B_i \otimes_{\mathcal{O}_v} \mathcal{O}_P$. Then $\tilde{B}$ and $\tilde{B}_i$ are orders in $M_n(P)$, and $\tilde{B} \subset \tilde{B}_i$. But Proposition 1.11 implies that there is only a finite number of distinct orders $\tilde{B}_i$; thus it remains to be shown that $\tilde{B}_i = \tilde{B}_j$ only if $B_i = B_j$. To do so choose $\mathcal{O}_v$-bases $x_1, \dots, x_{n^2}$ and $y_1, \dots, y_{n^2}$ of B_i and B_j respectively. Then $x_l = \sum_{m=1}^{n^2} a_{lm} y_m$ and $y_l = \sum_{m=1}^{n^2} b_{lm} x_m$ for suitable a_{lm}, $b_{lm} \in K_v$. Since $x_1, \dots, x_{n^2}$ and $y_1, \dots, y_{n^2}$ are also $\mathcal{O}_P$-bases of $\tilde{B}_i = \tilde{B}_j$, then actually a_{lm}, $b_{lm} \in \mathcal{O}_P \cap K_v = \mathcal{O}_v$, whence $B_i = B_j$. Q.E.D.

If we combine Proposition 1.11 with Theorem 1.16 we see that there exist maximal orders in semisimple algebras over an algebraic number field.

THEOREM 1.17. *Let A be a semisimple algebra over an algebraic number field K. Then any order $B \subset A$ is contained in some maximal order.*

PROOF: As above, this reduces to the case of a central simple K-algebra A. It suffices to show that the set $\{B_i\}$ of orders in A containing B is finite. First this assertion is proved for a matrix algebra $A = M_n(K)$. Clearly here A has a maximal order $C = M_n(\mathcal{O})$. Then, by assertion (2) of Theorem 1.15 it follows that $B_v = C_v$ is a maximal order in $A_{K_v} = M_n(K_v)$ for almost all v in V_f^K. Moreover, for the remaining v the number of orders in A_{K_v} containing B_v is finite. This, together with assertion (1) of Theorem 1.15, yields the required result. In general to reduce to the case just considered, we choose a finite extension P/K satisfying $A \otimes_K P \simeq M_n(P)$, and replace B and B_i with $\tilde{B} = B \otimes_{\mathcal{O}} \mathcal{O}_P$ and $\tilde{B}_i = B_i \otimes_{\mathcal{O}} \mathcal{O}_P$ in $M_n(P)$. Then there exists only a finite number of distinct $\tilde{B}_i$, and thus of distinct B_i as well. Q.E.D.

REMARK: Although it can be shown that over K_v all maximal orders are conjugate, over K in general there also exist non-conjugate maximal orders.

2. Algebraic Groups

This chapter, like the first, presents introductory material. In §2.1 we set forth (generally without proofs) basic results on the structure of algebraic groups, including the classification of semisimple groups over algebraically closed fields and over arbitrary fields, as well. In §2.2 we consider several aspects of the classification of K-groups, using Galois cohomology. In §2.3 we apply this approach to obtain an explicit classification of the classical groups. §2.3 also contains some supplementary material related to the classical groups, including, in particular, relative and absolute versions of Witt's theorem. Lastly, §2.4 sets forth essential results from algebraic geometry, including the construction of several algebraic varieties which we shall need later on.

2.1. Structural properties of algebraic groups.

In this section we present some basic definitions and results on algebraic groups over algebraically closed fields as well as over arbitrary fields, which will be used constantly throughout the book. Actually, we shall not present the proofs here, since our main objective is to unify terminology and notation; however we shall give precise references for the proofs of key results. We recommend the books Borel [8] and Humphreys [1] (for an algebraically closed ground field), and the article Borel and Tits [1] as basic references. While, strictly speaking, an acquaintance with the results set forth below is sufficient in order to understand this book, a preliminary systematic study of the above sources, and of the foundations of algebraic geometry, Lie algebras, and root systems, based on Shafarevich [1] and Bourbaki [4], for example, is highly recommended.

2.1.1. Algebraic groups. For the most part we shall make do with the "naïve" definition of a linear algebraic group as a subgroup of the general linear group $GL_n(\Omega)$ which is closed in the Zariski topology, where Ω is a *universal domain* (an algebraically closed field having infinite transcendence degree over its prime subfield). For example, this is the case with reduction theory in Chapter 4, where one can even assume $\Omega = \mathbb{C}$. However, in several instances, especially when working with adeles or groups of points over various completions, it is natural to take a more abstract approach in which an algebraic group G is viewed as an algebraic variety with morphisms

$$\begin{aligned} G \times G \xrightarrow{\mu} G \text{ given by } (x, y) \mapsto xy \\ G \xrightarrow{i} G \text{ given by } x \mapsto x^{-1} \end{aligned} \tag{2.1}$$

satisfying the usual group axioms. In principle, when working with groups of points over arbitrary rings sometimes a schematic approach is useful, too, however we did our best not to use it extensively. It should be noted that these sundry approaches actually all lead to the same class of objects, since any affine algebraic group (under the second definition) is linear, i.e., is isomorphic to a Zariski-closed subgroup of a suitable $GL_n(\Omega)$. (By a *morphism* of algebraic groups we mean a morphism of algebraic varieties which is also a group homomorphism; an *isomorphism* is a morphism for which there is an inverse morphism.) Since no more general algebraic groups than linear ones will be considered in this book, the word "linear" will frequently be omitted.

In several instances it is convenient to view an algebraic group G as a Zariski-closed subset not only of $GL_n(\Omega)$ but of the matrix algebra $M_n(\Omega)$ as well. This can always be achieved by increasing n (called the *degree* of G) by 1. Indeed, it suffices to realize $GL_n(\Omega)$ itself as a closed subset of $M_{n+1}(\Omega)$. The desired embedding is given by

$$g \mapsto \begin{pmatrix} & & & 0 \\ & g & & 0 \\ & & & \vdots \\ 0 & 0 & \dots & (\det g)^{-1} \end{pmatrix},$$

the matrix entries of the image defined by the following equations for $y = (y_{ij}) \in M_{n+1}(\Omega)$:

$$y_{i,n+1} = y_{n+1,i} = 0, \quad i = 1, \dots, n$$
$$y_{n+1n+1} \cdot \det((y_{ij})_{i,j=1,\dots,n}) - 1 = 0.$$

It follows that the *coordinate ring* of $GL_n(\Omega)$ is

$$A = \Omega[x_{11}, x_{12}, \dots, x_{nn}, \det(x_{ij})^{-1}],$$

and the coordinate ring of an algebraic group $G \subset GL_n(\Omega)$ is $A/\mathfrak{a}$, where $\mathfrak{a}$ is the ideal of all polynomials in A vanishing on G. (Several frequently used concepts of algebraic geometry are discussed in §2.4.) In particular, if $f: G \to H$ is a morphism of two algebraic groups $G \subset GL_n(\Omega)$ and $H \subset GL_m(\Omega)$, then there also exist polynomials

$$f_{kl} = f_{kl}(x_{11}, \dots, x_{nn}, \det(x_{ij})^{-1}) \text{ for } k, l = 1, \dots, m \tag{2.2}$$

such that

$$f(g) = (f_{kl}(g))_{k,l=1,\dots,m}.$$

In this book we shall study algebraic groups defined over a subfield K of Ω, usually either an algebraic number field or its completion. In this regard, recall that an algebraic group $G \subset GL_n(\Omega)$ is said to be *defined over* K(or simply a *K-group*) if $\mathfrak{a}$, the ideal of the coordinate ring A of $GL_n(\Omega)$ consisting of those polynomials that vanish on G, is generated by $\mathfrak{a}_K = \mathfrak{a} \cap A_K$, where $A_K = K[x_{11}, \dots, x_{nn}, \det(x_{ij})^{-1}]$. (Henceforth we shall use systematically the notation A_K, $\mathfrak{a}_K$, and analogous symbols to denote the corresponding K-objects, even in quite diverse situations. For example, G_K will always denote the group of K-points of the algebraic K-group $G \subset GL_n(\Omega)$, i.e., $G \cap GL_n(K)$.) A morphism $f: G \to H$ of two K-groups, $G \subset GL_n(\Omega)$ and $H \subset GL_m(\Omega)$, is defined over K (in other words, is a K-morphism) if the polynomials (2.2) which define it come from A_K.

In this book we shall deal mainly with groups over perfect fields. Therefore, unless stated otherwise, K will denote a perfect field (moreover, in the context of the theory set forth, K is either finite or has characteristic 0). Then the test of definition of arbitrary varieties over a Galois extension of K, which we shall look at in §2.2.4, becomes quite straightforward. Note that a K-group can also be defined abstractly as an algebraic K-variety whose K-morphisms are K-morphisms (of varieties) satisfying the group axioms (2.1). However, it can be shown (cf. Borel [8]) that under this definition an affine K-group is K-isomorphic to a linear algebraic group defined over K.

2.1.2. Restriction of scalars. Let $G \subset GL_n(\Omega)$ be an algebraic group defined over a finite (separable) extension L of K. We wish to construct an algebraic K-group G' whose group of K-points G'_K is naturally isomorphic to G_L. This can be done using $\mathbf{R}_{L/K}(G)$, the group obtained from G by restricting scalars from L to K. To construct $G' = \mathbf{R}_{L/K}(G)$ we choose a base $w_1, \dots, w_d$ of L over K and consider the corresponding regular representation $\varrho: L \to M_d(K)$, which just takes any x in L to the matrix of the left translation $y \mapsto xy$ (with respect to the given base). In order to define $\varrho(L) \subset M_d(K)$, take the system of linear equations

$$F_k(y^{\alpha\beta}) = 0, \qquad \alpha, \beta = 1, \dots, d, \qquad k = 1, \dots, r,$$

whose coefficients are the matrices $y = (y^{\alpha\beta}) \in M_d(K)$. Also, let $P_l(x_{ij})$, for $l = 1, \dots, m$, be a finite set of generators of $\mathfrak{a}_L$ where

$$\mathfrak{a} \subset \Omega[x_{11}, \dots, x_{nn}, \det(x_{ij})^{-1}]$$

is the ideal of the functions vanishing on G. Identifying $M_n(M_d(K))$ with $M_{nd}(K)$, we may associate to each $P_l(x_{ij}) = \sum a_{\gamma_{11}\dots\gamma_{nn}} x_{11}^{\gamma_{11}} \dots x_{nn}^{\gamma_{nn}}$ the

"matrix" polynomial

$$\tilde{P}_l(y_{ij}^{\alpha\beta}) = \sum \varrho(a_{\gamma_{11}\dots\gamma_{nn}})(y_{11}^{\alpha\beta})^{\gamma_{11}} \dots (y_{nn}^{\alpha\beta})^{\gamma_{nn}} \in M_d(K[y_{ij}^{\alpha\beta}])$$

in the n^2d^2 variables $y_{ij}^{\alpha\beta}$, where $\alpha, \beta = 1, \dots, d$ and $i, j = 1, \dots, j$. Then the image of G'_L in $M_{nd}(K)$ under ϱ is defined by the equations

$$\begin{aligned} F_k(y_{ij}^{\alpha\beta}) &= 0 \qquad \forall i, j = 1, \dots, n; \quad k = 1, \dots, r \\ \tilde{P}_l(y_{ij}^{\alpha\beta}) &= 0 \qquad\quad l = 1, \dots, m \end{aligned} \tag{2.3}$$

(where 0 in the last equation denotes the zero matrix in $M_d(K)$). Let G' denote the set of solutions of (2.3) in $GL_n(\Omega)$. Then G' is the desired algebraic K-group. Note that $G' = \mathbf{R}_{L/K}(G)$ is independent of the choice of the base L/K (up to K-isomorphism).

The set of equations (2.3) defining G' shows that G' may be interpreted as the group of points of G in the $\bar{K}$-algebra $L \otimes_K \bar{K}$. Note that $L \otimes_K \bar{K} \simeq \bar{K}^d$, the embedding of L in $\bar{K}^d$ obtained by $x \mapsto (\sigma_1(x), \dots, \sigma_d(x))$, where $\sigma_1, \dots, \sigma_d$ are the distinct embeddings of L in $\bar{K}$ over K. Hence there exists a $\bar{K}$-isomorphism

$$G' \simeq G^{\sigma_1} \times \dots \times G^{\sigma_d}, \tag{2.4}$$

where G^{σ_i} is the subgroup of $GL_n(\Omega)$ determined by the equations from $\mathfrak{a}_L^{\sigma_i}$, which is obtained by applying σ_i to all polynomials in $\mathfrak{a}_L$.

For any L-morphism $f: G \to H$ of algebraic L-groups G and H, there is a corresponding K-morphism $\tilde{f} = \mathbf{R}_{L/K}(f): \mathbf{R}_{L/K}(G) \to \mathbf{R}_{L/K}(G)$ (obtained analogously to the construction of $\tilde{P}$ from P). Thus $\mathbf{R}_{L/K}$ is a functor from the category of L-groups and L-homomorphisms to the category of K-groups and K-homomorphisms. Note that not every K-morphism $\tilde{f}: \mathbf{R}_{L/K}(G) \to \mathbf{R}_{L/K}(H)$ has the form $\tilde{f} = \mathbf{R}_{L/K}(f)$ for a suitable L-morphism $f: G \to H$. (Namely, if L/K is a Galois extension, then $\mathbf{R}_{L/K}(G)$ has K-defined automorphisms induced by automorphisms of L/K, which can not be written in the form $\mathbf{R}_{L/K}(f)$.) However, using (2.4) it is easy to obtain the equality $\mathbf{X}(\mathbf{R}_{L/K}(G))_K = \mathbf{X}(G)_L$ for the groups of rational characters (cf. §2.2.7 for the definition of characters, and Borel [1, Proposition 1.6]).

Restriction of scalars has two noteworthy arithmetic properties. Let L/K be an extension of an algebraic number field and let $v \in V^K$. Then, writing $L \otimes_K K_v = \bigoplus_{w|v} L_w$ (cf. §1.1), we have

$$\mathbf{R}_{L/K}(G)_{K_v} \simeq \prod_{w|v} G_{L_w}$$

for any L-group G. Now let $K = \mathbb{Q}$ and let $w_1, \dots, w_d$ be a base of $\mathcal{O}/\mathbb{Z}$ where $\mathcal{O} = \mathcal{O}_L$, the ring of integers of L. Taking the regular representation ϱ with respect to this base, we obtain $\mathbf{R}_{L/K}(G)_{\mathbb{Z}} \simeq G_{\mathcal{O}_L}$ and $\mathbf{R}_{L/K}(G)_{\mathbb{Z}_p} \simeq \prod_{v|p} G_{\mathcal{O}_v}$ for any prime number p.

2.1.3. The Lie algebra of an algebraic group. The variety of any algebraic group G is homogeneous; i.e. for any two points $g_1, g_2 \in G$ the translation map $x \mapsto g_2 g_1^{-1} x$ is a morphism of G as an algebraic variety, sending g_1 to g_2. Since a variety always has a simple point, one concludes that all the points of G are simple, i.e., G is a smooth variety. (Concepts related to simple points and tangent spaces are discussed in §§2.2.4 and 2.3.1.) The tangent space $T_e(G)$ of G at the identity is called the *Lie algebra* $L(G)$ of G. Clearly $\dim L(G) = \dim G$. If $G \subset GL_n(\Omega)$ then $L(G) \subset M_n(\Omega) = L(GL_n(\Omega))$, and the Lie bracket is given by the standard formula

$$[X, Y] = XY - YX.$$

If $G \subset GL_n(\Omega)$ is defined over K, then $L(G)$ is an algebra with a K-structure, i.e. $L(G)_K = L(G) \cap M_n(K)$ satisfies $L(G)_K \otimes_K \Omega = L(G)$. For explicit determination of the Lie algebra the method of dual numbers can be used (cf. Borel [8], Humphreys [1]).

If $G \subset GL_n(\Omega)$ then for any g in G we have $gL(G)g^{-1} = L(G)$, giving rise to a morphism of algebraic groups $G \to GL(L(G))$ defined by $g \mapsto \varphi_g$, where $\varphi_g(X) = gXg^{-1}$ for X in $L(G)$; this is called the *adjoint representation of* G and is written Ad. Also, one has the map ad: $L(G) \to \mathrm{End}(L(G))$ given by $\mathrm{ad}\, X(Y) = [X, Y]$, called the *adjoint representation of the Lie algebra* $L(G)$. Using dual numbers it is easy to show that ad is the differential at 1 of the representation Ad. The *Killing form* is the symmetric bilinear form f on $L(G)$ given by

$$f(X, Y) = \mathrm{tr}(\mathrm{ad}\, X\, \mathrm{ad}\, Y), \quad \text{for } X, Y \in L(G),$$

where tr denotes the trace in the matrix algebra $\mathrm{End}(L(G))$; note that f is invariant under the adjoint action of G.

2.1.4. The connected component of 1. Since G is a smooth variety, its irreducible components are also its connected components. The connected component G^0 of the identity is an open-and-closed normal subgroup of G having finite index. Moreover $\dim G = \dim G^0$ and $L(G) = L(G^0)$. If G is defined over K, then G^0 is also defined over K. Note that most of the groups to be studied in this book are connected. In particular, all reductive or semisimple groups will be assumed to be connected.

2.1.5. The Jordan decomposition. Let $g \in GL_n(\Omega)$; then there is a unique way of writing $g = g_s g_u$, where g_s is a semisimple matrix (i.e., g_s

can be diagonalized via conjugation), g_u is unipotent (i.e., all the eigenvalues of g_u are 1), and $g_s g_u = g_u g_s$. We call $g = g_s g_u$ the *Jordan decomposition*. If $g \in G$, where $G \subset GL_n(\Omega)$ is an algebraic group, then $g_s, g_u \in G$. Moreover, if $f: G \to H$ is a morphism of algebraic groups, then $f(g)_s = f(g_s)$ and $f(g)_u = f(g_u)$. Thus we see the Jordan decomposition is independent of the matrix realization of G. Furthermore, if $g \in G_K$ then g_s, $g_u \in G_K$ (recall that K is assumed to be perfect). Analogously, any matrix $X \in M_n(\Omega)$ can be written in the form $X = X_s + X_n$, where X_s and X_n are respectively semisimple and nilpotent matrices such that $X_s X_n = X_n X_s$. This decomposition, called the *additive Jordan decomposition*, is also uniquely determined. If $X \in L(G)$ then X_s, $X_n \in L(G)$, and the projections $X \mapsto X_s$ and $X \mapsto X_n$ are functorial, i.e., they respect differentials of morphisms of algebraic groups. Moreover, X_s, $X_n \in L(G)_K$ for X in $L(G)_K$.

2.1.6. Quotient varieties. If G is a K-group and H is a K-subgroup of G, then the space of cosets G/H can be provided with the structure of a quasiprojective variety such that the canonical map $G \to G/H$ is a K-morphism of algebraic varieties (for greater detail, cf. §2.2.4). When H is a normal subgroup of G then G/H is an affine variety, and the structure of the algebraic variety on G/H is consistent with the natural group operation; thus G/H is an algebraic K-group and $G \to G/H$ is a K-morphism of algebraic groups.

2.1.7. Diagonalizable groups and algebraic tori. An algebraic group G is said to be *diagonalizable* if there is a suitable faithful representation $f: G \to GL_m(\Omega)$ for which the group $f(G)$ is diagonalizable, i.e., is conjugate to a subgroup of the group D_n of diagonal matrices. Then the image of any representation $f: G \to GL_m(\Omega)$ is also diagonalizable. It can be shown that the diagonalizable groups are those commutative algebraic groups which consist only of semisimple elements. Of special importance are the connected diagonalizable groups known as *algebraic tori*. Algebraic tori can also be defined as those algebraic groups G for which there is an isomorphism $G \simeq (\mathbb{G}_m)^d$, where $\mathbb{G}_m = GL_1(\Omega)$ is the multiplicative group of Ω and $d = \dim G$.

A *character* of an algebraic group G is a morphism of algebraic groups $\chi: G \to \mathbb{G}_m$. The characters of G generate a commutative group under the operation $(\chi_1 + \chi_2)(g) = \chi_1(g)\chi_2(g)$, which we denote as $\mathbf{X}(G)$. It is easy to see that for the d-dimensional torus G the group $\mathbf{X}(G)$ is isomorphic to $\mathbb{Z}^d$ and, in particular, is a finitely generated torsion-free $\mathbb{Z}$-module.

In general a K-torus G need not have an isomorphism $G \simeq (\mathbb{G}_m)^d$ defined over K; when it does, however, G is said to be *K-split*. The following conditions are equivalent:

(1) G is K-split;
(2) all its characters are defined over K;
(3) $f(G)$ is diagonalizable over K, i.e., is conjugate to a subgroup of D_n by a matrix from $GL_n(K)$, under any (equivalently, some) faithful K-representation $f: G \to GL_n(\Omega)$.

Note that the latter two conditions also are equivalent for any diagonalizable K-group and thus allow us to define a K-split group. In general a diagonalizable K-group splits over some finite field extension L of K, which is called a *splitting field* of G. From (2) it follows that an extension L of K will be a splitting field of G if and only if $\mathbf{X}(G) = \mathbf{X}(G)_L$. In terms of Galois theory this means that if we consider the natural action of $\mathcal{G} = \mathrm{Gal}(\bar{K}/K)$ on $\mathbf{X}(G)$ (recall that we assume K to be perfect), which endows the discrete group $\mathbf{X}(G)$ with the structure of a continuous module over the profinite group $\mathcal{G}$, then the open subgroup $\mathcal{H} \subset \mathcal{G}$ corresponding to L acts trivially on $\mathbf{X}(G)$, i.e., $\mathbf{X}(G) = \mathbf{X}(G)^{\mathcal{H}}$. It follows, in particular that any given diagonalizable K-group G has a minimal splitting field which is automatically a Galois extension of K and is contained in any other splitting field.

Thus, for any K-split torus G we have $\mathbf{X}(G) = \mathbf{X}(G)_K$. At the other extreme, G is a *K-anisotropic torus* if $\mathbf{X}(G)_K = 0$. It is well known that any K-torus G has K-subtori G_a and G_d, respectively K-split and K-anisotropic, such that $G = G_a G_d$ and $G_a \cap G_d$ is finite (i.e., G is an almost direct product of G_a and G_d).

The correspondence $G \xrightarrow{\phi} \mathbf{X}(G)$ is a contravariant functor from the category $\mathcal{A}$ of K-diagonalizable groups split over a finite Galois extension L/K with Galois group $\mathcal{F}$ and of K-morphisms, to the category $\mathcal{B}$ of finitely generated modules over the group ring $\Gamma = \mathbb{Z}[\mathcal{F}]$ and of Γ-module homomorphisms.

THEOREM 2.1. *Φ is a contravariant category equivalence, for which the subcategory $\mathcal{A}_0 \subset \mathcal{A}$ consisting of the algebraic tori defined over K, corresponds to the subcategory $\mathcal{B}_0 \subset \mathcal{B}$ of $\mathbb{Z}$-torsion-free finitely generated Γ-modules.*

Theorem 2.1 is fundamental for the study of algebraic tori, the subject of Voskresenkiĭ's book [3]. This theorem makes it possible to define an algebraic torus by giving the corresponding character module. Moreover, as Voskresenskiĭ has shown, many geometric and arithmetic properties of tori can be described in this context. In our book we shall not deal with the theory of tori (for which we refer the reader to Voskresenskiĭ [3]) and shall limit ourselves to several typical examples and constructions that will be needed later on.

To begin with, note that there is also a covariant equivalence between $\mathcal{A}_0$ and $\mathcal{B}_0$ given by $G \overset{\Psi}{\mapsto} \mathbf{X}_*(G)$ where $\mathbf{X}_*(G) = \mathrm{Hom}(\mathbb{G}_m, G)$ is the group of *cocharacters* or *one-parameter subgroups* of G, provided with the structure of a Γ-module in the natural way. There is a natural bilinear map $\mathbf{X}_*(G) \times \mathbf{X}(G) \to \mathbb{Z}$ which is defined as follows: if $\varphi \in \mathbf{X}_*(G)$ and $\chi \in \mathbf{X}(G)$ then $\chi \circ \varphi$ is a morphism from $\mathbb{G}_m$ to $\mathbb{G}_m$; therefore $(\chi \circ \varphi)(t) = t^m$ for some m in $\mathbb{Z}$ $(t \in \Omega^*)$ and we define $\langle \chi, \varphi \rangle = m$. This map enables us to identify $\mathbf{X}_*(G)$ with the dual Γ-module $\mathrm{Hom}_{\mathbb{Z}}(\mathbf{X}(G), \mathbb{Z})$ of $\mathbf{X}(G)$. It follows, in particular, that if G is a K-split torus, i.e., $\mathbf{X}(G) = \mathbf{X}(G)_K$, then also $\mathbf{X}_*(G) = \mathbf{X}_*(G)_K$. On the other hand, if G is K-anisotropic then $\mathbf{X}_*(G) = 0$. Conversely, if $\mathbf{X}_*(G) = \mathbf{X}_*(G)_K$ (respectively $\mathbf{X}_*(G) = 0$) then G is K-split (respectively K-anisotropic).

EXAMPLE: Let $[L : K] = d$. Set $G = \mathbf{R}_{L/K}(\mathbb{G}_m)$. Then, as follows from §2.1.2, there exists a K-isomorphism $G \simeq (\mathbb{G}_m)^d$, i.e., G is a d-dimensional torus. The explicit description of the restriction of scalars allows G to be realized as a K-subgroup of $GL_d(\Omega)$. Let φ denote the restriction to G of the ordinary determinant. Then φ is a K-morphism $G \to \mathbb{G}_m$, i.e., an element of $\mathbf{X}(G)_K$. In terms of field theory the restriction of φ to $G_K = L^*$ is the determinant of the regular representation of L over K, i.e., the usual norm $N_{L/K}: L^* \to K^*$. Therefore the kernel of φ, usually designated by $\mathbf{R}^{(1)}_{L/K}(\mathbb{G}_m)$ is called the *norm torus* corresponding to L/K.

The minimal splitting field is the normal closure P of L over K. Set $\mathcal{F} = \mathrm{Gal}(P/K)$ and $\mathcal{H} = \mathrm{Gal}(P/L)$. Then $\mathbf{X}(G)$ as a module over $\Gamma = \mathbb{Z}[\mathcal{F}]$ is isomorphic to $\mathbb{Z}[\mathcal{F}/\mathcal{H}]$, the free $\mathbb{Z}$-module with base consisting of cosets $g\mathcal{H}$ for $g \in \mathcal{F}$, on which $\mathcal{F}$ acts by left translation. The norm map $\varphi: G \to \mathbb{G}_m$ corresponds to the homomorphism of Γ-modules $\mathbb{Z} \to \mathbb{Z}[\mathcal{F}/\mathcal{H}]$, given by $z \mapsto z\sigma$ for $\sigma = \sum g\mathcal{H}$, the sum taken over all cosets. Then the character module $\mathbf{X}(H)$ of the norm torus $H = \mathbf{R}^{(1)}_{L/K}(\mathbb{G}_m)$ is the quotient module $\mathbb{Z}[\mathcal{F}/\mathcal{H}]/\mathbb{Z}\sigma$. Since the module of fixed points $\mathbb{Z}[\mathcal{F}/\mathcal{H}]^{\mathcal{F}}$ is $\mathbb{Z}\sigma$, it follows that $\mathbf{X}(H)_K = 0$, i.e., H is anisotropic. The same result can be obtained by considering cocharacter modules instead of character modules. Namely, $\mathbf{X}_*(G)$ is isomorphic to $\mathbb{Z}[\mathcal{F}/\mathcal{H}]$, and $\mathbf{X}_*(H)$ is the kernel of the augmentation map $\mathbb{Z}[\mathcal{F}/\mathcal{H}] \to \mathbb{Z}$ given by $\sum a_g g\mathcal{H} \to \sum a_g$. Clearly $\mathbf{X}_*(H)^{\mathcal{F}} = \mathbf{X}_*(H) \cap \mathbb{Z}\sigma = (0)$. Thus we see again that H is a K-anisotropic torus.

The above example may be generalized as follows. Consider finite extensions $L_1, \ldots, L_r$ over K, and for each $i = 1, \ldots, r$ construct the corresponding norm map $\varphi_i: \mathbf{R}_{L_i/K}(\mathbb{G}_m) \to \mathbb{G}_m$. Then

$$\{(x_1, \ldots, x_r) \in \mathbf{R}_{L_1/K}(\mathbb{G}_m) \times \ldots \times \mathbf{R}_{L_r/K}(\mathbb{G}_m): \varphi_1(x_1) \ldots \varphi_r(x_r) = 1\}$$

is a torus which is naturally called *multinorm*.

Tori of the form $\mathbf{R}_{L/K}(\mathbb{G}_m)$ and their finite direct products are called *quasisplit* (over K). They are precisely the K-tori whose groups of characters are permutation modules, i.e., free finitely generated $\mathbb{Z}$-modules with a base whose elements are permuted by the absolute Galois group. Quasisplit tori are the easiest to study, and sometimes when dealing with arbitrary tori it turns out to be helpful to cover the torus under consideration by (or to embed it in) a suitable quasisplit torus. We present several examples of such constructions to be used later on.

PROPOSITION 2.1. *Let F be a diagonalizable K-group split by an extension P/K. Then F can be embedded in an exact sequence*

$$1 \to F \to T \to S \to 1,$$

where T and S are K-tori split by P, and T is quasisplit.

PROOF: Let $\mathcal{H}$ denote the kernel of the natural action of $\mathcal{G} = \mathrm{Gal}(\bar{K}/K)$ on the group of characters $\mathbf{X}(F)$, and let $L = \bar{K}^{\mathcal{H}}$ be the corresponding fixed field. Then L is a finite Galois extension of K with Galois group $\mathcal{F} = \mathcal{G}/\mathcal{H}$, and clearly $L \subset P$. Now consider $\mathbf{X}(F)$ as a module over the group ring $\Gamma = \mathbb{Z}[\mathcal{F}]$ and write it as a quotient module of a free module Γ^l. Then there is an exact sequence of the form

$$0 \to \Delta \to \Gamma^l \to \mathbf{X}(F) \to 0.$$

Passing from Δ and Γ^l to the corresponding tori, we obtain the exact sequence

$$1 \to F \to T \to S \to 1,$$

where T and S are K-tori and $T = \mathbf{R}_{L/K}(\mathbb{G}_m)^l$. Q.E.D.

If we assume F is a torus and use the cocharacter module instead of the character module, by a similar argument we obtain

PROPOSITION 2.2. *Any K-torus F can be put into an exact sequence*

$$1 \to S \to T \to F \to 1,$$

where S and T are K-tori and T is quasisplit.

We shall also require

PROPOSITION 2.3 (ONO [5]). *For any K-torus F there exists an integer $m > 0$ and a quasisplit torus T' such that $F^m \times T'$ is isogeneous to some quasisplit K-torus T.*

(Recall that by an *isogeny* of algebraic groups we mean a surjective homomorphism with a finite kernel. Two groups are said to be *isogeneous* if there is an isogeny between them. The concept of isogeny with respect to semisimple groups is taken up in §2.1.13. Isogeny for tori is quite different; in particular, isogeny is an equivalence relation. In terms of character groups this relation is expressed as follows: two tori T_1, T_2 from the category $\mathcal{A}_0$ described in Theorem 2.1 are isogeneous if and only if the $\mathbb{Q}[\mathcal{F}]$-modules $\mathbf{X}(T_1) \otimes_{\mathbb{Z}} \mathbb{Q}$ and $\mathbf{X}(T_2) \otimes_{\mathbb{Z}} \mathbb{Q}$ are isomorphic.

Proposition 2.3 is actually a restatement of Artin's theorem on induced characters in terms of tori. We omit the proof here and refer the reader to Ono [5] and to his article in "Arithmetic groups and automorphic functions."

2.1.8. Solvable and unipotent groups. Throughout this subsection we assume the base field has characteristic 0. An algebraic group G is said to be *unipotent* if all of its elements are unipotent. An example of a unipotent group is the additive group of Ω, i.e.

$$\mathbb{G}_a = \left\{ g = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \in GL_2(\Omega) : x \in \Omega \right\}.$$

If $G \subset GL_n(\Omega)$ is unipotent then $(g - E_n)^n = 0$ for any g in G, and therefore the truncated logarithmic map

$l: G \to M_n(\Omega)$ given by

$$l(g) = (g - E_n) - \frac{(g - E_n)^2}{2} + \ldots + (-1)^n \frac{(g - E_n)^{(n-1)}}{n-1}$$

defines a polynomial isomorphism of varieties from G to its Lie algebra $L(G)$; the inverse map is the truncated exponential map $e: L(G) \to G$ given by $e(X) = E_n + X + \frac{X^2}{2!} + \cdots + \frac{X^{n-1}}{(n-1)!}$. In particular, G is always connected. Now let $G \subset GL_n(\Omega)$ be a unipotent K-group. Then G is *trigonalizable over* K; i.e., there exists a matrix g in $GL_n(K)$ such that gGg^{-1} is contained in the group $\mathbf{U}_n$ of upper unitriangular matrices. It follows, in particular, that G is nilpotent. Moreover, it can be shown that there is a central series

$$G = G_0 \supset G_1 \supset \ldots \supset G_n = \{e\}$$

in G such that $G_i/G_{i+1} \simeq \mathbb{G}_a$ for $i = 0, \ldots, n-1$. Note that most of the above statements do not carry over for positive characteristic.

We shall require a technical assertion about unipotent groups.

LEMMA 2.1. *Suppose a K-split torus T acts by automorphisms on a connected unipotent K-group U. Then for any T-invariant K-subgroup $V \subset U$ we can find a T-invariant Zariski-closed subset $P \subset U$ defined over K such that the product morphism induces K-isomorphisms of varieties $P \times V \xrightarrow{\sim} U$ and $V \times P \xrightarrow{\sim} U$. Moreover, if U is abelian then P can be chosen to be a suitable K-subgroup of U.*

Indeed, if U is abelian then the map $l: U \to L(U)$ introduced above is a group isomorphism; so it suffices to choose a T-invariant K-complement $W \subset L(U)$ of $L(V)$ and to set $P = e(W)$. The general case is examined by induction on $\dim U/V$, and then using central series (2.4) one reduces the problem to the case $\dim U/V = 1$. Here again we may put $P = e(W)$, where W is a one-dimensional T-invariant K-complement of $L(V)$ in $L(U)$.

Now let $G \subset GL_n(\Omega)$ be a connected solvable group. Then G is conjugate to a group of upper triangular matrices (Lie-Kolchin Theorem). This yields the structure theorem for solvable groups: the set G_u of unipotent elements of G constitutes a normal subgroup of G, and G is a semidirect product of G_u by an (arbitrary) maximal torus $T \subset G$. If G is a K-group then G_u is also a K-group and there exists a maximal K-torus $T \subset G$; moreover, in this case the semidirect decomposition $G = TG_u$ is also K-defined. There is a composition series (over Ω)

$$G = G_0 \supset G_1 \supset \ldots \supset G_n = \{e\} \tag{2.5}$$

such that the factors G_i/G_{i+1} are isomorphic to $\mathbb{G}_m$ or $\mathbb{G}_a$. If there is a series (2.5) of K-subgroups such that the G_i/G_{i+1} are K-isomorphic to $\mathbb{G}_m$ or $\mathbb{G}_a$, then G is said to be *K-split*. Indeed, this is equivalent to the existence of a maximal K-split torus $T \subset G$, and then any K-torus in G is K-split. In particular, any unipotent K-group is K-split, and in this case all the factors of the corresponding series (2.5) are K-isomorphic to $\mathbb{G}_a$.

2.1.9. Connected groups. Two classes of subgroups stand out in the study of a connected group G: maximal tori $T \subset G$ and Borel subgroups $B \subset G$ (i.e., maximal connected solvable subgroups). Since the dimension of G is finite, maximal tori and Borel subgroups always exist. Furthermore, all maximal tori in G (respectively Borel subgroups) are conjugate in G. (In particular, $r = \dim T$ is independent of the choice of T, and is called the (absolute) *rank* of G, written $\operatorname{rank} G$). Also, it is well known that any Borel subgroup is its own normalizer in G. Consequently, if we fix some maximal torus $T \subset G$ (respectively, Borel subgroup $B \subset G$), then the set of all maximal tori in G (respectively, of Borel subgroups) can be identified with the coset space G/N (respectively G/B), where $N = N_G(T)$ is the normalizer of T in G. (Cf. also Theorem 2.19 in §2.4.) Subgroups $P \subset G$ containing B are said to be *parabolic*. They are connected and are

characterized by the fact that the quotient variety G/P (cf. Borel [8]) is projective.

If G is a K-group then there exists a maximal torus $T \subset G$ which is defined over K. However, G as a rule need not have a Borel subgroup defined over K; those groups for which such a subgroup does exist are called *quasisplit over* K. G is said to be *K-split* if there exists a maximal K-torus $T \subset G$ which is K-split. (For connected solvable groups this concept coincides with the definition in the previous subsection.)

THEOREM 2.2. *Let G be a connected algebraic group over an infinite perfect field K. Then G_K (cf. §2.1.1) is dense in G in the Zariski topology.*

The maximal connected solvable normal subgroup of G is called the *radical* $R(G)$ of G, and the maximal connected unipotent normal subgroup of G is the *unipotent radical* $R_u(G)$ of G. (Obviously $R_u(G)$ is the unipotent part $R(G)_u$ of $R(G)$.) A connected group G is said to be *reductive* (respectively *semisimple* if $R_u(G) = \{e\}$ (respectively $R(G) = \{e\}$). Evidently for G connected, $G/R(G)$ is semisimple and $G/R_u(G)$ is reductive.

If G is a K-group then both the radicals $R(G)$ and $R_u(G)$ are K-defined. We have

THEOREM 2.3 (MOSTOW [1]). *Let K be of characteristic zero and let G be a connected K-group. Then there exists a reductive K-subgroup $H \subset G$ such that G is a semidirect product $HR_u(G)$. Moreover any reductive K-subgroup $H' \subset G$ is conjugate by an element of $R_u(G)_K$ to a subgroup of H.*

The decomposition $G = HR_u(G)$ described in the theorem is called the *Levi decomposition*. One can use it to reduce many problems to reductive groups. Theorem 2.3 is the analog of the theorem for Lie groups obtained by Levi and Maltsev (cf. Maltsev [1,2]).

2.1.10. Reductive groups. The basic properties of reductive groups are listed in the following theorem.

THEOREM 2.4. *Let G be a reductive K-group. Then*

(1) *$R(G)$ is the connected component $S = Z(G)^0$ of the center and is a torus;*
(2) *the commutator subgroup $H = [G, G]$ is a semisimple K-group;*
(3) *$G = HS$ is an almost direct product (i.e. $H \cap S$ is finite);*
(4) *if $\operatorname{char} K = 0$, then any algebraic representation $f: G \to GL_n(\Omega)$ is completely reducible.*

A deeper analysis of reductive, and especially semisimple, groups is based on the concept of a *root system*. To define this concept we consider a

reductive group G and fix a maximal torus $T \subset G$. Let $\mathfrak{g} = L(G)$ be the Lie algebra of G and let $\operatorname{Ad}: G \to GL(\mathfrak{g})$ be the adjoint representation. Then it follows from §2.1.7 that $\operatorname{Ad} T$ is diagonalizable in $GL(\mathfrak{g})$. This can also be expressed as follows: let $\mathfrak{g}_\alpha$ denote the weight space for the weight α in $\mathbf{X}(T)$, i.e.,

$$\mathfrak{g}_\alpha = \{ X \in \mathfrak{g} : \operatorname{Ad}(t)X = \alpha(t)X, \forall t \in T \},$$

and set

$$R(T, G) = \{ \alpha \in \mathbf{X}(T) : \alpha \neq 0 \text{ and } \mathfrak{g}_\alpha \neq 0 \};$$

then $\mathfrak{g} = L(T) \oplus (\oplus_{\alpha \in R(T,G)} \mathfrak{g}_\alpha)$, where $L(T)$ is the Lie algebra of T which is the weight 0 space. Then the remarkable fact is that $R = R(T, G)$ is an abstract root system in the space $V = \mathbf{X}(T/S) \otimes_{\mathbb{Z}} \mathbb{R}$ (cf. Bourbaki [4, Ch. 6] for the definition), and so naturally is called the *root system of G relative to T*. Note that if G is semisimple then $S = \{e\}$ and we obtain a root system in $\mathbf{X}(T) \otimes_{\mathbb{Z}} \mathbb{R}$. Each space $\mathfrak{g}_\alpha$ is one-dimensional and has a corresponding one-dimensional unipotent subgroup $U_\alpha \subset G$ (the subgroup such that $\mathfrak{g}_\alpha = L(U_\alpha)$). The subgroup $G_\alpha \subset G$ generated by U_α and $U_{-\alpha}$ is a semisimple group of rank 1; consequently $G_\alpha \simeq SL_2(\Omega)$ or $PSL_2(\Omega)$. We also mention an equivalent description of G_α as the commutator subgroup of the centralizer of the connected component $(\ker \alpha)^0$. Let $\Pi \subset R$ be a system of simple roots and R_+^Π the corresponding system of positive roots (cf. Bourbaki [4, Ch. 6]). Then the group $U(\Pi)$ generated by all U_α for $\alpha \in R_+^\Pi$ is normalized by T, and the semidirect product $B(\Pi) = TU(\Pi)$ is a Borel subgroup of G. Moreover $\Pi \to B(\Pi)$ defines a bijection between the systems of simple roots in R and the Borel subgroups of G containing T. Thus, a given Borel subgroup $B \subset G$ uniquely determines some system Π of simple roots, and one can choose an ordering V_+ in V such that $R_+^\Pi = R \cap V_+$.

Associated with a root system R we have the *Weyl group* of R, written $W = W(R)$ (Bourbaki [4]), generated by the set S of reflections with respect to the simple roots $\alpha \in \Pi$. Moreover, the pair (W, S) is a Coxeter group (cf. Bourbaki [4, Ch. 4 and 6]). W has a unique element w of maximal length (with respect to S). It is characterized by $w(R_+^\Pi) = -R_+^\Pi$, and its length actually equals the number of positive roots. Note that $W(R)$ can be identified with the Weyl group $W(T, G)$ of G with respect to T, which is defined as $N_G(T)/T$, where $N_G(T)$ is the normalizer of T. We review briefly how this is done. The action of $N_G(T)$ on T by conjugation determines a homomorphism from $W(T, G)$ to $\operatorname{Aut}(R)$. For any α in R let $T_\alpha = T \cap G_\alpha$. Then $W(T_\alpha, G_\alpha)$ has order 2; and any element n_α in $N_{G_\alpha} \backslash T_\alpha$ induces the reflection w_α on R. It follows that the image of $W(T, G)$ in $\operatorname{Aut}(R)$ contains $W(R)$. But $W(T, G)$ and $W(R)$ have the same order,

since the first group acts simply transitively on the set of Borel subgroups containing T, while the second group does the same on the systems of simple roots in R.

The Weyl group $W(T,G)$ has another interesting application, bearing on the *Bruhat decomposition.* For each element w in $W(T,G)$ we choose some representative n_w in $N_G(T)$ and consider the double coset Bn_wB where B is a Borel subgroup of G containing T.

THEOREM 2.5 (THE BRUHAT DECOMPOSITION). *For a reductive group G we have a decomposition*

$$G = \bigcup_{w\in W} Bn_wB, \tag{2.6}$$

where the right hand side is the disjoint union of the double cosets.

COROLLARY. *The intersection of any two Borel subgroups of G contains a maximal torus.*

Indeed, let us consider an arbitrary Borel subgroup $B \subset G$ and let (2.6) be the corresponding Bruhat decomposition. By the conjugacy theorem any other Borel subgroup is of the form gBg^{-1}, $g \in G$. Using the Bruhat decomposition we can write g as b_1nb_2 where $b_i \in B$ $(i = 1, 2)$ and n lies in the normalizer of the maximal torus $T \subset B$. Then

$$B \cap gBg^{-1} = b_1(B \cap nBn^{-1})b_1^{-1} \supset b_1Tb_1^{-1},$$

and so $T_1 = b_1Tb_1^{-1}$ is the desired torus.

Since Bn_wB is independent of the choice of n_w, often we just write BwB instead of Bn_wB, and in this way W "parametrizes" the double cosets modulo B in the decomposition of G. The double coset Bn_wB corresponding to the element of maximal length $w \in W$ is called a *large cell*, and plays an especially important role. To wit: let $B = B(\Pi)$ where $\Pi \subset R$ is a system of simple roots, and let $w_0 \in W$ be the element of maximal length with respect to $S = \{w_\alpha : \alpha \in \Pi\}$. Then $w_0(R_+^\Pi) = -R_+^\Pi$ is the set of negative roots in R, and $w_0Bw_0^{-1} = B^-$, where $B^- = TU(-\Pi)$ and $U(-\Pi)$ is the subgroup generated by U_α for all negative roots α. Putting $U = U(\Pi)$ and $U^- = U(-\Pi)$ for the sake of brevity, we then have $Bw_0B = UTU^-w_0$. Further, consider the product morphism $U \times T \times U^- \xrightarrow{\varphi} G$. Computing its differential at 1 and taking into account the decomposition $\mathfrak{g} = L(T) \oplus (\oplus_{\alpha\in R}\mathfrak{g}_\alpha)$, one can show that φ is dominant, from which it follows that the "large cell" is an open subset of G. Moreover, it is easy to verify that φ is injective, i.e., is a birational isomorphism, implying that G is a rational variety. Lastly, we have $\dim G = \dim T + [R] = \dim T + 2l(w_0)$ where $l(w_0)$ is the length of w_0.

EXAMPLE: Let $G = GL_n(\Omega)$. Then $\mathfrak{g} = M_n(\Omega)$. The group of all diagonal matrices is a maximal torus T of G. Write ε_i for the character of T given by $\varepsilon_i\colon \mathrm{diag}(t_1,\dots,t_n) \mapsto t_i$. Clearly, for any matrix $X = (x_{ij}) \in M_n(\Omega)$ and any $t = \mathrm{diag}(t_1,\dots,t_n)$ in T we have $\mathrm{Ad}(t)(X) = (t_it_j^{-1}x_{ij})$, and therefore $R(T,G) = \{\varepsilon_i - \varepsilon_j : i \neq j\}$. For our simple roots we can take $\Pi = \{\varepsilon_i - \varepsilon_{i+1} : i = 1,\dots,n-1\}$, and then $R_+^\Pi = \{\varepsilon_i - \varepsilon_j : i < j\}$. It is easy to show that the Borel subgroup $B(\Pi)$ in this case coincides with the group of upper triangular matrices. The normalizer of the torus $N_G(T)$ is the group of monomial matrices; consequently $W(T,G)$ is isomorphic to the symmetric group S_n. In turn, $W(R)$ is also isomorphic to S_n and acts on the roots by permuting the indices. The canonical system of generators $W(R) = S_n$, corresponding to Π, consists of transpositions $(i, i+1)$, $i = 1,\dots,n-1$. The element of maximal length $w_0 \in W(R)$ sends any i to $n - i + 1$. $B^- = w_0Bw_0^{-1}$ is the group of lower triangular matrices, and the product UTU^- consists of those matrices for which all the principal minors are nonzero.

2.1.11. Regular semisimple elements. Let G be a reductive algebraic group, let $T \subset G$ be a maximal torus, and let $R(T,G)$ be the associated root system. A semisimple element g in G is said to be *regular* if the dimension of its centralizer $Z_G(g)$ equals the rank of G. In this case the connected component $Z_G(g)^0$ is a torus. Regular elements always exist. Moreover, an element t in T is regular if and only if $\alpha(t) \neq 1$ for all α in R. It follows that the regular semisimple elements of T form a dense open subset $\Theta \subset T$. If we then consider the morphism $G \times \Theta \xrightarrow{\varphi} G$ given by $(g,\theta) \xmapsto{\varphi} g\theta g^{-1}$ and calculate dimensions we find that the set of semisimple regular elements is open in G. Moreover, direct computation shows that the differential of φ at any point is surjective. A semisimple element X in $L(G)$ is said to be *regular* if its centralizer is the Lie algebra of a torus. The properties of semisimple regular elements in Lie algebras are analogous to the corresponding properties in groups. In particular, they form a nonempty open subset of $L(G)$.

2.1.12. Parabolic subgroups. In addition to the notation and conventions of the previous subsection, let $\Pi \subset R$ be a system of simple roots and let $B(\Pi)$ be the corresponding Borel subgroup. It follows from the Bruhat decomposition and the properties of the Weyl group W that any subgroup $P \subset G$ containing B has the form $P_\Delta = BW_\Delta B$ for some subset $\Delta \subset \Pi$, where W_Δ is the subgroup of W generated by the reflections $\{w_\alpha : \alpha \in \Delta\}$. Moreover $L(P_\Delta) = L(T) \oplus (\bigoplus_{\alpha\in\Theta}\mathfrak{g}_\alpha)$ where Θ is the union of the set of positive roots R_+^Π and of those negative roots which are linear combinations

of roots from Δ. Subgroups of the form P_Δ are called *standard parabolic subgroups*. Since Borel subgroups are conjugate, any parabolic subgroup of G is conjugate to some standard parabolic subgroup.

2.1.13. Semisimple groups. The concept of *isogeny* is useful in analyzing semisimple groups. We recall that an *isogeny* is a surjective morphism $f: G \to H$ of algebraic groups having finite kernel. (For characteristic > 0 the class of isogenies admissible as far as the classification of semisimple groups is concerned must be restricted somewhat, to the *central isogenies*. These are characterized by the fact that for any Ω-algebra A the kernel of the induced homomorphism $f_A: G_A \to H_A$ of groups of A-points lies in the center of G_A. Since, in characteristic zero any isogeny is central, we shall not discuss the characteristic > 0 case in detail.) G is said to be an almost direct product of its subgroups $G_1, \ldots, G_r$ if the product morphism $G_1 \times \ldots \times G_r \to G$ is an isogeny. We call a connected noncommutative algebraic group G *(absolutely) simple* if it has no nontrivial connected normal subgroups (here we depart from the traditional terminology "almost simple group").

PROPOSITION 2.4. *Let G be a semisimple group and G_i $(i \in I)$ the minimal connected normal subgroups of G. Then I is a finite set (say $I = \{1, \ldots, r\}$), and G is an almost direct product of $G_1, \ldots, G_r$. In particular, G is an almost direct product of simple groups.*

In fact, each G_i $(i = 1, \ldots, r)$ corresponds to the irreducible component R_i in the decomposition $R = \bigcup_{i=1}^r R_i$ of the root system R of G (cf. Bourbaki [4, Ch. 6]); viz., G_i is generated by U_α for $\alpha \in R_i$. In general one cannot replace "almost direct product" by "direct product"; however we shall describe two cases in which one can. G is said to be *simply connected* if, for any connected group H, any (central) isogeny $f: H \to G$ is an isomorphism; G is said to be *adjoint* if any (central) isogeny $f: G \to H$ is an isomorphism.

THEOREM 2.6. *Let G be a semisimple group.*

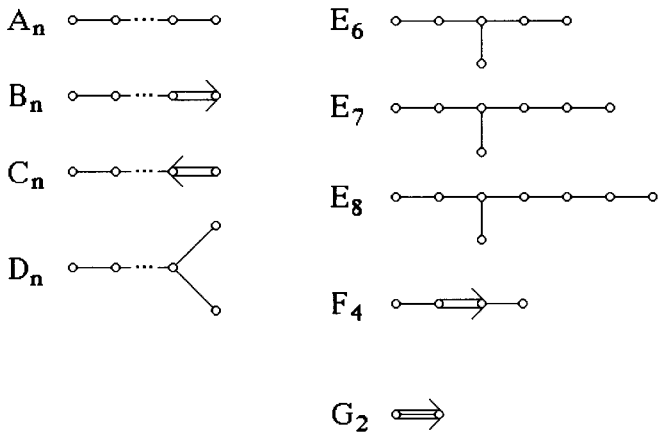
(1) *There exists a simply connected group $\tilde{G}$, an adjoint group $\bar{G}$ and (central) isogenies $\pi: \tilde{G} \to G$ and $\varphi: G \to \bar{G}$.*
(2) *Any simply connected (resp., adjoint) group is a direct product of its minimal connected normal subgroups, which, moreover, are also simply connected (resp., adjoint).*
(3) *Suppose $R = R(T, G)$ is a root system of G and $\Pi \subset R$ is the system of simple roots. Then G is simply connected (respectively, adjoint) if $X(T)$ has a base $\{\lambda_\alpha : \alpha \in \Pi\}$ such that $w_\alpha \lambda_\beta = \lambda_\beta - \delta_{\alpha\beta}\alpha$, where $\delta_{\alpha\beta}$ is the Kronecker delta (respectively, Π spans $\mathbf{X}(T)$).*

EXAMPLE: Let $G = SL_n(\Omega)$. As in the preceding example, for T the diagonal torus, $R(T, G)$ consists of $\varepsilon_i - \varepsilon_j$, where $\varepsilon_i: \mathrm{diag}(t_1, \ldots, t_n) \mapsto t_i$, and $\Pi = \{\varepsilon_i - \varepsilon_{i+1} : i = 1, \ldots, n-1\}$. For each $j = 1, \ldots, n-1$, put $\lambda_j(t) = t_1 \ldots t_j$. Then $w_{\alpha_i}(\lambda_j) = \lambda_j - \delta_{ij}\alpha_i$, and consequently G is simply connected.

The isogeny $\pi: \tilde{G} \to G$ of Theorem 2.6 (1) is called a *universal covering* and $F = \ker \pi$ the *fundamental group* of G. Thus, any semisimple group has a universal covering which is a direct product of simply connected simple groups. Thus the classification of semisimple groups is completed up to isogeny, by the following result:

THEOREM 2.7. *A simply connected simple algebraic group is uniquely determined up to isomorphism by its root system.*

The root system of a simple group is irreducible and reduced, and therefore either belongs to one of the four classical series A_n, B_n, C_n, D_n, or is one of the five exceptional systems E_6, E_7, E_8, F_4, G_2. It is helpful to assign to the root system its corresponding Dynkin diagram, the list of possible diagrams being:



The Dynkin diagram of a semisimple group is the union of the Dynkin diagrams of its simple components (as explained in Bourbaki [4, Ch. 6]). We also present a table of the simply connected groups corresponding to the classical systems (cf. §2.2.3 for greater detail) and the structure of the centers of simple groups, thus providing a complete description of the simple groups.

Type	Realization	Structure of the Center
A_n	$\mathbf{SL}_{n+1}$	$\mathbb{Z}/(n+1)\mathbb{Z}$
B_n	$\mathbf{Spin}_{2n+1}$	$\mathbb{Z}/2\mathbb{Z}$
C_n	$\mathbf{Sp}_{2n}$	$\mathbb{Z}/2\mathbb{Z}$
D_n	$\mathbf{Spin}_{2n}$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, n$ even
		$\mathbb{Z}/4\mathbb{Z}, n$ odd
E_6	—	$\mathbb{Z}/3\mathbb{Z}$
E_7	—	$\mathbb{Z}/2\mathbb{Z}$
E_8	—	$\{e\}$
F_4	—	$\{e\}$
G_2	—	$\{e\}$

In the Lie algebra $\mathfrak{g} = L(G)$ of a semisimple group G one can choose a canonical base, called the *Chevalley base*. Namely, there exist $X_\alpha \in \mathfrak{g}_\alpha$ for $\alpha \in R$, and $H_\alpha \in L(T)$ for $\alpha \in \Pi$, such that $\{X_\alpha\}_{\alpha\in R} \cup \{H_\alpha\}_{\alpha\in\Pi}$ is a base of $\mathfrak{g}$ and the following conditions hold:

$$\begin{aligned}
[H_\alpha, H_\beta] &= 0, && \alpha, \beta \in \Pi \\
[H_\alpha, H_\beta] &= c_{\alpha\beta} X_\beta, && c_{\alpha\beta} \in \mathbb{Z},\ \alpha \in \Pi,\ \beta \in R \\
[X_\alpha, X_{-\alpha}] &= H_\alpha, && \alpha \in \Pi \\
[X_\alpha, X_\beta] &= d_{\alpha\beta} X_{\alpha+\beta}, && d_{\alpha\beta} \in \mathbb{Z}, \text{ if } \alpha+\beta \in R \\
[X_\alpha, X_\beta] &= 0, && \text{if } \beta \neq -\alpha \text{ and } \alpha+\beta \notin R
\end{aligned}$$

The base satisfying these properties (where $c_{\alpha\beta}$ and $d_{\alpha\beta}$ take on certain values depending only on α, β and R; cf. Steinberg [2, Theorem 1] for more details) is uniquely determined up to a change of signs of X_α and up to an automorphism of $\mathfrak{g}$.

In order to describe the K-forms of a semisimple group G, we need to know the structure of the automorphism group $\operatorname{Aut} G$. In fact $\operatorname{Aut} G$ is a semidirect product of the group of inner automorphisms $\operatorname{Int} G$ (which can be identified with the corresponding adjoint group $\bar{G}$), by a certain finite group which we shall now define. To begin with, let us assume that G is simply connected. Then any symmetry σ of the Dynkin diagram of the root system $R = R(T, G)$ induces an automorphism $f_\sigma \in \operatorname{Aut} G$ such that $f_\sigma(T) = T$, $f_\sigma(B) = B$, and $d_e f_\sigma(X_\alpha) = X_{\sigma\alpha}$ for α in Π, and X_α is the corresponding element of the base of the Chevalley Lie algebra $\mathfrak{g}$. Moreover, $\sigma \mapsto f_\sigma$ gives an injection of the group $\operatorname{Sym}(R)$ of symmetries of the Dynkin diagram of R into $\operatorname{Aut} G$, whose image we shall also write as $\operatorname{Sym}(R)$.

THEOREM 2.8. *For any simply connected semisimple group G, the automorphism group $\operatorname{Aut} G$ is the semidirect product of $\operatorname{Int} G \simeq \bar{G}$ by $\operatorname{Sym}(R)$. If G is an arbitrary semisimple group and $\tilde{G} \xrightarrow{\pi} G$ is a universal covering, then $\operatorname{Aut} G$ is isomorphic to the subgroup of $\operatorname{Aut} \tilde{G}$ fixing $\ker \pi$, the fundamental group.*

We have reviewed the fundamentals of the theory of semisimple algebraic groups over an algebraically closed field. For semisimple groups defined over an arbitrary field K the theory is more complicated and not as complete. (We shall touch on several aspects of this theory in §2.1.14.) However, for semisimple K-split groups the theory can be developed almost in parallel with the case of an algebraically closed field. In particular, for any root system R there exists a simply connected semisimple K-split group G with a maximal K-split torus $T \subset G$ such that $R(T, G)$ is R. This group is given by the Chevalley construction (cf. Steinberg [2]). In general, the theory of semisimple K-split groups coincides with the theory of Chevalley groups, as set forth in Steinberg's book. In the corresponding Lie algebra $\mathfrak{g}$ we can choose a Chevalley base lying in $\mathfrak{g}_K$. $\operatorname{Aut} G$ is a semidirect product $\operatorname{Sym}(R) \cdot \bar{G}$ defined over K, and moreover all automorphisms from $\operatorname{Sym}(R)$ are defined over K. Any K-split semisimple group G has a universal covering $\pi\colon \tilde{G} \to G$ defined over K.

2.1.14. Relative root systems. Let G be a semisimple K-group and let $S \subset G$ be a maximal K-split torus. $\dim S$ is called the *K-rank* of G and is written $\operatorname{rank}_K G$. Since all maximal K-split tori in G are conjugate under G_K, the K-rank is well-defined. Groups with K-rank > 0 (respectively K-rank $= 0$) are called *K-isotropic* (respectively *K-anisotropic*). It can be shown that G being K-anisotropic is equivalent to G_K not having any unipotent elements other than the identity.

The theory set forth above for an algebraically closed base field will henceforth be called the *absolute case*. Borel and Tits [1] developed a structure theory for isotropic groups which, although analogous to the absolute case, leads to more modest results; viz., it determines the structure of the group modulo information about the structure of the anisotropic kernel. As in the absolute case, the theory is based on associating a root system to the group under consideration. To do so, fix a maximal K-split torus S and consider the adjoint action of S on $\mathfrak{g} = L(G)$. For α in $\mathbf{X}(S)$ put

$$\mathfrak{g}_\alpha = \{ X \in \mathfrak{g} : \operatorname{Ad}(s)X = \alpha(s)X, \forall s \in S \}$$

and define $R(S, G) = \{ \alpha \in \mathbf{X}(S) : \alpha \neq 0 \text{ and } \mathfrak{g}_\alpha \neq 0 \}$. Then we can write $\mathfrak{g} = L(Z(S)) \oplus (\oplus_{\alpha\in R(S,G)} \mathfrak{g}_\alpha)$ where $L(Z(S))$ is the Lie algebra of the centralizer Z(S) of S which coincides with the weight 0 space; moreover, all the weight spaces $\mathfrak{g}_\alpha$ are defined over K. $R_K = R(S, G)$ turns out to be a root system in $V = X(S) \otimes_{\mathbb{Z}} \mathbb{R}$, called the *relative system of roots* or *system of K-roots*. One difference from the absolute case is that the $\mathfrak{g}_\alpha$ ($\alpha \in R_K$) generally are not one-dimensional, and R_K need not be reduced. The Weyl group $W(R_K)$ of the root system R_K can be identified with the Weyl group $W(S, G)$ of G relative to S, defined as the quotient group

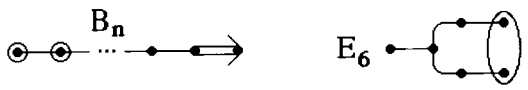
$N(S)/Z(S)$ of the normalizer of S modulo its centralizer; moreover, any element of $W(S,G)$ has a representative in $N(S)_K$. Suppose $\Pi \subset R_K$ is a system of simple roots and R^{Π}_{+K} is the corresponding system of positive roots. Let U_α for $\alpha \in R_K$ be the commutative unipotent subgroups having $\mathfrak{g}_\alpha$ as its Lie algebra, and let $U(\Pi)$ be the group generated by U_α for all $\alpha \in R^{\Pi}_{+K}$. Then $U(\Pi)$ is a unipotent group normalized by $Z(S)$, and the semidirect product $P(\Pi) = Z(S)U(\Pi)$ is a minimal parabolic K-subgroup. Moreover, $\Pi \to P(\Pi)$ maps bijectively the systems of simple roots in R_K to the minimal parabolic K-subgroups of G containing S. Writing $P = P(\Pi)$ and $U = U(\Pi)$ for the sake of brevity, and choosing a representative $n_w \in N(S)_K$ for each w in $W(S,G)$, we obtain the Bruhat decomposition

$$G_K = \bigcup_{w \in W(S,G)} P_K n_w P_K,$$

and moreover $P_K n_w P_K = U_K n_w P_K$. Note that in the relative case the relation between the irreducibility of R_K and the K-simplicity of G, which means that G has no nontrivial connected normal K-subgroups, goes only in one direction; if G is K-simple then R_K is irreducible.

A graphic description of a semisimple K-group G can be conveniently given in the form of a Dynkin diagram with additional data—called a *Tits index*, which we now describe (cf. Tits [2], Borel-Tits [1]). Consider a maximal K-split torus $S \subset G$ and a maximal K-torus $T \subset G$ containing S. Let $R = R(T,G)$ be the root system of G relative to T and let $\Pi \subset R$ be a system of simple roots. Since G and T are defined over K, the Galois group $\mathcal{G} = \mathrm{Gal}(\bar{K}/K)$ acting on $\mathbf{X}(T)$ restricts to permutations on R.

Let us define the induced action (called the *-action) of $\mathcal{G}$ on the Dynkin diagram, or more precisely on Π, since the vertices of the Dynkin diagram are in one-to-one correspondence with the elements of Π. Namely, for any $\sigma \in \mathcal{G}$, $\sigma(\Pi)$ is a system of simple roots in $R = \sigma(R)$, and therefore there is a unique w in $W(R)$ for which $w(\sigma(\Pi)) = \Pi$; put $\sigma^* = w \circ \sigma \colon \Pi \to \Pi$. G is called an *inner* (respectively, *outer*) form if the *-action is trivial (respectively, nontrivial). Furthermore, we call a vertex of the Dynkin diagram *distinguished* (and circle it) if the restriction of the corresponding simple root to S is nontrivial. Vertices of the diagram belonging to the same orbit of $\mathcal{G}$ are placed "close" to each other, and in case they are distinguished a common circle is drawn around them. Dynkin diagrams with distinguished vertices and the *-action specified are called *Tits indexes*. For example:



It is also customary to indicate the order of the homomorphic image of $\mathcal{G}$ which acts effectively on Π. Thus, the second diagram has type ${}^2E_6$, whereas all inner forms have type ${}^1X$ (where X is the appropriate Dynkin diagram). Note that if a diagram has no symmetries (for example, B_n), then any K-group of this type is automatically an inner form.

Using Tits indexes it is easy to determine the diagram of the *anisotropic kernel* of G (as we call the commutator group of the centralizer $Z(S)$ of a maximal K-split torus, which is a semisimple K-anisotropic group). Namely, we discard the distinguished vertices and their corresponding edges. (If all the vertices are distinguished, then G is quasisplit.) One can also find a maximal K-split torus S and its corresponding relative root system. Namely, S is defined in T by the equations $\alpha(x) = 1$ where α runs through all non-distinguished roots, and also by the equations $\alpha_1(x) = \ldots = \alpha_l(x)$ if $\alpha_1, \ldots, \alpha_l$ lie in the same orbit under the *-action. It follows that if a quasisplit group is an inner form (in particular, if the corresponding diagram has no symmetries) then it is split. The relative roots are obtained by the restriction to S of the roots from R for which this restriction is nontrivial. (For examples of the relevant computations, cf. Ch. 6.)

2.2. Classification of K-forms using Galois cohomology.

2.2.1. L/K-forms. Let X be an object with a K-structure (a variety, algebraic group, etc. defined over K) and L/K be a finite Galois extension. A K-object Y is said to be an L/K-form of X if there is an L-defined isomorphism $f \colon X \to Y$. The Galois group $\mathcal{F} = \mathrm{Gal}(L/K)$ acts naturally on the L-morphisms of K-objects, and, for any σ in $\mathcal{F}$, the morphism $a_\sigma = f^{-1} \cdot f^\sigma$ lies in the group $\mathrm{Aut}_L(X)$ of L-defined automorphisms of X; moreover $\sigma \mapsto a_\sigma$ defines a (noncommutative) 1-cocycle on $\mathcal{F}$ with values in $\mathrm{Aut}_L(X)$ (cf. §1.3.2). Thus there is a map

$$F(L/K, X) \xrightarrow{\varphi} H^1(\mathcal{F}, \mathrm{Aut}_L(X))$$

from the set of classes of K-isomorphic L/K forms of X to the first cohomology set.

THEOREM 2.9. *If X is an affine K-variety or an algebraic K-group, then φ is a bijection.*

Let us give a rough sketch of the main aspects of the proof (cf. Serre [1], Voskresenskiĭ [3, Ch. 3]). First, φ is shown to be well-defined (i.e., to be independent of the choice of Y in its class of K-isomorphic L/K-forms and of the choice of L-isomorphism $f \colon X \to Y$), and injective. This part of the proof is formal and holds for much more general situations. The proof of

the surjectivity of φ requires a more subtle line of reasoning and is based on the construction of twisting, which we have already encountered.

Twisting was used in §1.3.2 to study exact sequences in noncommutative cohomology, but it can also be used to prove that φ is surjective. Namely, as in §1.3.2, consider a group G, a G-group A, and a G-set F acted on by A, the action of A being compatible with the action of G. Then for any cocycle a in $Z^1(G, A)$ we have the "twisted set" ${}_aF$, depending up to G-isomorphism only on the equivalence class of a in $H^1(G, A)$. Put $H = {}_aF$ and write $f: F \to H$ for the map induced by the identity map of F. Then it follows from the definition of ${}_aF$ that the cocycle $\{f^{-1} \cdot f^s\}_{s \in G} \in Z^1(G, A)$ is our original a.

Note, however, that if F has more structures (such as an algebraic variety) then this abstract argument requires further refinement to prove that the twisted object ${}_aF$ also has this structure. In the case described in Theorem 2.9, this is obtained by considering the *algebra of regular functions*, also called the *coordinate ring*. Any affine algebraic variety is determined by its coordinate ring, and assigning the structure of an algebraic group is equivalent to assigning the structure of a Hopf algebra to the coordinate ring (cf. Borel [8]). Accordingly, to construct an L/K-form of X corresponding to $a = \{a_\sigma\} \in H^1(\mathcal{F}, \mathrm{Aut}_L(G))$ we consider the coordinate ring $A = L[X]$ of L-defined functions, and introduce a new action of $\mathcal{F}$ on it, given by

$$\sigma'(f) = (\sigma \circ a_\sigma)^*(f),$$

where $(\sigma \circ a_\sigma)^*$ denotes the K-automorphism of A corresponding to $\sigma \circ a_\sigma$. The L-algebra B thus obtained will serve as the coordinate ring of L-defined functions for the desired variety Y. Moreover, Y will have the structure of an algebraic K-group if X has such a structure. Loosely speaking, we say that Y is obtained from X by twisting using a, and write $Y = {}_aX$.

REMARK: Theorem 2.9 also holds for projective varieties.

EXAMPLE 1: Let $X = \mathbb{G}_m$ be a one-dimensional K-split torus, let $L = K(\sqrt{c})$ be a quadratic extension of K, and let τ be the generator of $\mathcal{F} = \mathrm{Gal}(L/K)$. Consider the cocycle $a = \{a_\sigma\} \in Z^1(\mathcal{F}, \mathrm{Aut}_L X)$ given by $a_e = \mathrm{id}_X$ and $a_\tau = \theta$, where $\theta(x) = x^{-1}$ for all x in X. Then $A = L[X]$ is $L[t, t^{-1}]$ and $A_K = K[t, t^{-1}]$; moreover the automorphisms θ and τ act on A as follows:

$$\theta^*: f(t) + g(t^{-1}) \mapsto f(t^{-1}) + g(t)$$
$$\tau: f(t) + g(t^{-1}) \mapsto f^\tau(t) + g^\tau(t^{-1}).$$

It follows that the action of τ on the twisted algebra $B = L[t, t^{-1}]$ is given by

$$\tau: f(t) + g(t^{-1}) \mapsto f^\tau(t^{-1}) + g^\tau(t).$$

Direct computation shows that the K-algebra $B_K = B^{\mathcal{F}}$ is isomorphic to $C = K[u, v]/(u^2 - cv^2 - 1)$ (for indeterminates u, v), the isomorphism from C to B_K given by

$$u \mapsto \frac{t + t^{-1}}{2}, \qquad v \mapsto \frac{t - t^{-1}}{2\sqrt{c}}.$$

But $C = K[Y]$, where $Y = \mathbf{R}^{(1)}_{L/K}(\mathbb{G}_m)$ is the subtorus of elements of norm 1; moreover the isomorphism $C \simeq B_K$ respects the Hopf algebra structures on C and B_K. Thus ${}_aX = Y$.

In many cases the description of X itself and of its K-structure is determined by the description of the set of K-points X_K. (Examples are vector spaces; vector spaces with certain bilinear maps, such as quadratic forms; algebras, etc.) Then, loosely speaking, by an "object" we frequently mean the set X_K, and by a twisted object, the corresponding set Y_K. Such usage of the term "object" has obvious limitations. In particular, it cannot be applied to algebraic varieties, since one can have $X_K = Y_K = \emptyset$, with X and Y being not K-isomorphic. In many cases, however, this terminology is effective, and we shall make use of it.

EXAMPLE 2: Let $V = K^2$ be a 2-dimensional space over K, provided with a quadratic form f which in the standard base e_1, e_2 is given by $f(x_1, x_2) = x_1 x_2$. Again consider a quadratic extension $L = K(\sqrt{c})$, and let τ be the generator of $\mathcal{F} = \mathrm{Gal}(L/K)$. Let $\mathbf{O}_2(f)$ be the orthogonal group of the quadratic form f and let $b = \{b_\sigma\}$ denote the cocycle in $Z^1(\mathcal{F}, \mathbf{O}_2(f)_L)$, given by $b_e = \mathrm{id}$, $b_\tau = g$, where g in $\mathbf{O}_2(f)$ switches e_1 and e_2. Consider the space $V \otimes_K L$ and, twisting by means of a, set $W = {}_a(V \otimes L)_K$. Direct computation shows that the vectors $u_1 = \frac{1}{2}(e_1 + e_2)$ and $u_2 = \frac{1}{2}\sqrt{c}(e_1 - e_2)$ constitute a K-base of W, and moreover f (or, to be more precise, its extension to $V \otimes L$) in this base has the form $f(y_1, y_2) = y_1^2 - cy_2^2$. Thus, twisting (V, f) yields (W, h), where h has the form $h(y_1, y_2) = y_1^2 - cy_2^2$. Note that this example is directly related to the preceding one, since $\mathbf{SO}_2(f) = \mathbb{G}_m$ and $\mathbf{SO}_2(h) = \mathbf{R}^{(1)}_{L/K}(\mathbb{G}_m)$. We recommend that the reader analyze this connection by himself.

The second example allows the following generalization.

2.2.2. Spaces with tensors. Consider a pair (V, x), where V is a finite-dimensional vector space over K and x is a tensor on V of type (p, q), i.e., an element of $T^q_p(V) = T^p(V) \otimes T^q(V^*)$ (the reader who is not familiar with tensors can take x to be a bilinear form on V, i.e., a tensor of type $(0, 2)$; we shall not have to deal with tensors of other types in this book). For any Galois extension L/K with Galois group $\mathcal{F}$ we can consider $V_L = V \otimes_K L$ and $x_L = x \otimes 1 \in T^p_q(V_L) = T^p_q(V) \otimes_K L$. A pair (W, y), where W is a

space over K of the same dimension as V and $y \in T_q^p(W)$, is called an L/K-form of (V,x) if there is an isomorphism $(V_L, x_L) \simeq (W_L, y_L)$. As in §2.2.1, there is a map

$$F(L/K,(V,x)) \xrightarrow{\varphi} H^1(L/K, \mathrm{Aut}_L(V_L,x_L)).$$

PROPOSITION 2.5. *φ is a bijection.*

We need only prove the surjectivity of φ, for which we use

LEMMA 2.2. *$H^1(\mathcal{F}, GL_n(L)) = 1$ for any $n \geq 1$. In particular,*

$$H^1(\mathcal{F}, L^*) = 1.$$

The latter assertion is known as Hilbert's Theorem 90. If L/K is a cyclic extension and σ is the generator of its Galois group $\mathcal{F}$, then, using the description of $H^1(\mathcal{F}, L^*)$ in this case (cf. §1.3.1) we can give an equivalent reformulation, used repeatedly in §§1.3–1.4: any element a in L^*, such that $N_{L/K}(a) = 1$, is of the form $a \in \sigma(b)/b$, where $b \in L^*$.

PROOF: Consider the space $V = K^n$. Then $V_L = L^n$, and $\mathcal{F} = \mathrm{Gal}(L/K)$ acts componentwise. Now let $a = \{a_\sigma\}$ be a 1-cocycle on $\mathcal{F}$ with values in $GL_n(L)$. Define a new action of $\mathcal{F}$ on V_L, by putting

$$\sigma'(v) = a_\sigma \sigma(v)$$

for σ in $\mathcal{F}$ and v in V_L, and let U denote the space of fixed points. Clearly, for any v in V_L the vector $b(v) = \sum_{\sigma \in \mathcal{F}} a_\sigma \sigma(v)$ lies in U. We shall show that the $b(v)$ generate V_L over L, whence it follows, in particular, that $U \otimes_K L \simeq V_L$. Indeed, let u be any linear form on V_L annihilating all $b(v)$. Then for any h in L and any v in V_L we have

$$0 = u(b(hv)) = \sum \sigma(h) u(a_\sigma \sigma(v)),$$

so it follows that each $u(a_\sigma\sigma(v)) = 0$ by the theorem on the linear independence of characters (cf. Lang [3]), whence $u = 0$. Thus we can choose vectors $v_1, \ldots, v_n$ in V_L such that $b(v_1), \ldots, b(v_n)$ are linearly independent. Then, writing c for the matrix sending the canonical base to $v_1, \ldots, v_n$, we obtain the nonsingular matrix $b = \sum_\sigma a_\sigma \sigma(c)$, and direct calculation shows that $a_\sigma = b\sigma(b)^{-1}$, as required.

Now take an arbitrary cocycle $a = \{a_\sigma\}$ on $\mathcal{F}$ with values in $\mathrm{Aut}_L(V_L, x_L)$. Since the latter group is a subgroup of $GL(V_L)$, it follows from Lemma 2.2 that there exists $b \in GL(V_L)$ such that $a_\sigma = b^{-1}\sigma(b)$. Extend b to an automorphism of $T_q^p(V_L)$ and show that the tensor $x' = b(x)$ lies in $T_q^p(V)$. To do so it suffices to show that x' is fixed by $\mathcal{F}$; indeed,

$$\sigma(x') = \sigma(b)(\sigma(x)) = \sigma(b)(x) = b(b^{-1}\sigma(b))(x) = ba_\sigma(x) = bx = x',$$

as required. Now consider the K-space $W = b^{-1}(V_K)$, and let y denote the tensor over W corresponding to x'. Then the pair (W,y) corresponds to the cocycle a; note that actually W coincides with U (introduced in the proof of the lemma), and y coincides with the restriction of x to W. Furthermore, as we have shown, y is defined over K. Q.E.D.

Taking nondegenerate bilinear symmetric (=quadratic) forms on V in Proposition 2.5 we obtain

PROPOSITION 2.6. *Let f be a nondegenerate quadratic form defined on an n-dimensional vector space V over a field K, and let $\mathbf{O}_n(f)$ be the orthogonal group of f (cf. §2.3). Then for any Galois extension L/K with Galois group $\mathcal{F}$, $H^1(\mathcal{F}, \mathbf{O}_n(f)_L)$ is in one-to-one correspondence with the equivalence classes over K of those quadratic forms on V that are L-equivalent to f.*

Taking the nondegenerate bilinear alternating forms on V and bearing in mind that all of them are equivalent over K (Bourbaki [1, Ch. 9, §5]), we obtain

PROPOSITION 2.7. *Let f be a nondegenerate bilinear alternating form on an n-dimensional vector space V over a field K. Then for any Galois extension L/K we have $H^1(\mathcal{F}, \mathbf{Sp}_n(f)_L) = 1$, where $\mathbf{Sp}_n(f)$ is the symplectic group of f (cf. §2.3).*

Proposition 2.5 has other applications as well. In particular, the extra structure of "algebra" on a vector space is given by a tensor of type (1,2); hence the L/K-forms of A are in one-to-one correspondence with $H^1(\mathcal{F}, \mathrm{Aut}_L(A_L))$, where $\mathrm{Aut}_L(A_L)$ is the group of L-automorphisms of $A_L = A \otimes_K L$. Setting $A = M_n(K)$ and bearing in mind that any automorphism of A_L is inner, i.e., $\mathrm{Aut}_L(A_L) = PGL_n(L)$, we see that $H^1(\mathcal{F}, PGL_n(L))$ is in one-to-one correspondence with the L/K-forms of A, i.e., with the central simple K-algebras of dimension n^2 which are split by L.

In the above examples the groups of L-automorphisms are groups of L-points of algebraic groups (this is always the case when dealing with the automorphism group of a space with a tensor). This leads us to our next topic.

2.2.3. Cohomology of algebraic groups. Let G be an algebraic group and L/K a finite Galois extension with Galois group $\mathcal{F}$. Then $\mathcal{F}$ acts on

the group of L-points G_L, and we can define $H^1(\mathcal{F}, G_L)$, written henceforth as $H^1(L/K, G)$. If $M \supset L$ are two finite Galois extensions of K, then one obtains $H^1(M/K, G) \xrightarrow{\varrho_L^M} H^1(L/K, G)$. This allows us to extend the definition of $H^1(L/K, G)$ to infinite Galois extensions L/K. Namely, $\mathrm{Gal}(L/K)$ can be viewed as the inverse limit $\varprojlim \mathrm{Gal}(L_i/K)$ of the Galois groups of the finite subextensions, and then we set $H^1(L/K, G) = \varinjlim H^1(L_i/K, G)$, where the direct limit is taken with respect to the system of maps $\varrho_{L_j}^{L_i}$ for $L_i \supset L_j$. In this case $H^1(L/K, G)$ can be defined equivalently as the set of continuous 1-cohomology of the profinite group $\mathrm{Gal}(L/K)$ with coefficients in the discrete group G_L. We shall write $H^1(K, G)$ instead of $H^1(\bar{K}/K, G)$.

Passing to the direct limit in Theorem 2.9, we see that $H^1(K, G)$ in general parametrizes the classes of K-isomorphic $\bar{K}/K$-forms of a K-object X having G as its automorphism group, i.e., K-isomorphism classes of such Y that become isomorphic to X over $\bar{K}$. Note also that for any algebraic group G defined over K

$$H^0(K, G) = G_K.$$

The exact sequences of noncommutative cohomology, described in §1.3 yield, as a special case, analogous exact sequences for the Galois cohomology of algebraic groups. In particular, any exact sequence

$$1 \to F \to G \to H \to 1$$

of K-groups and K-homomorphisms has a corresponding exact sequence of sets with distinguished element

$$1 \to F_K \to G_K \xrightarrow{\varphi} H_K \xrightarrow{\psi_K} H^1(K, F) \to H^1(K, G) \to H^1(K, H), \tag{2.7}$$

where ψ_K is the *coboundary map*. In addition, if F lies in the center of G, then ψ_K is a group homomorphism, and there is a map

$$\partial_K : H^1(K, H) \to H^2(K, F)$$

extending (2.7) to one more term:

$$\ldots \to H^1(K, H) \xrightarrow{\partial_K} H^2(K, F).$$

Let us present some examples of computations of the cohomology of algebraic groups. Consider the exact sequence

$$1 \to \mathbf{SL}_n \to \mathbf{GL}_n \xrightarrow{d} \mathbb{G}_m \to 1,$$

where d is induced by the determinant, and in this case write the corresponding exact cohomological sequence (2.7) as

$$GL_n(K) \xrightarrow{d} K^* \to H^1(K, \mathbf{SL}_n) \to H^1(K, \mathbf{GL}_n). \tag{2.8}$$

It follows from Lemma 2.2 that $H^1(K, \mathbf{GL}_n) = 1$. But $\det : GL_n(K) \to K^*$ is surjective. Therefore, a consequence of (2.8) is

LEMMA 2.3. $H^1(K, \mathbf{SL}_n) = 1$.

Moreover, the special case of Lemma 2.2 for $n = 1$ (Hilbert's Theorem 90) asserts that $H^1(K, \mathbb{G}_m) = 1$. Then $H^1(K, \mathbf{R}_{L/K}(\mathbb{G}_m)) = H^1(L, \mathbb{G}_m) = 1$ for any finite extension L/K, by Shapiro's Lemma. Hence the definition of a quasisplit K-torus yields

LEMMA 2.4. *Let T be a quasisplit K-torus. Then $H^1(K, T) = 1$.*

Now consider the exact sequence

$$1 \to \mathbf{R}^{(1)}_{L/K}(\mathbb{G}_m) \to \mathbf{R}_{L/K}(\mathbb{G}_m) \xrightarrow{\varphi} \mathbb{G}_m \to 1,$$

where φ is the norm map. Passing to cohomology, we then have the exact sequence

$$L^* \xrightarrow{N_{L/K}} K^* \to H^1(K, \mathbf{R}^{(1)}_{L/K}(\mathbb{G}_m)) \to H^1(K, \mathbf{R}_{L/K}(\mathbb{G}_m)) \to 1,$$

which implies:

LEMMA 2.5. $H^1(K, \mathbf{R}^{(1)}_{L/K}(\mathbb{G}_m)) \simeq K^*/N_{L/K}(L^*)$.

Now let us consider the exact sequence

$$1 \to \mu_n \to \mathbb{G}_m \xrightarrow{[n]} \mathbb{G}_m \to 1, \tag{2.9}$$

where $[n]$ denotes the morphism of raising to the n-th power, and $\mu_n = \ker[n]$ is the group of n-th roots of unity. (2.9) yields the exact sequences

$$\begin{gathered} K^* \xrightarrow{[n]} K^* \to H^1(K, \mu_n) \to H^1(K, \mathbb{G}_m) = 1 \quad \text{and} \\ 1 = H^1(K, \mathbb{G}_m) \to H^2(K, \mu_n) \to H^2(K, \mathbb{G}_m) \xrightarrow{[n]} H^2(K, \mathbb{G}_m). \end{gathered} \tag{2.10}$$

Since $H^1(K, \mathbb{G}_m) = 1$ and $H^2(K, \mathbb{G}_m)$ is the same as $\mathrm{Br}(K)$, (2.10) yields

LEMMA 2.6. $H^1(K, \mu_n) \simeq K^*/K^{*n}$, *and* $H^2(K, \mu_n) = \mathrm{Br}(K)_n$ *is the subgroup of* $\mathrm{Br}(K)$ *consisting of elements of exponent* n.

Lastly, if in the proof of Proposition 2.6 we use Lemma 2.3 instead of Lemma 2.2, then we obtain the following interpretation of the first cohomology set $H^1(K, \mathbf{SO}_n(f))$ of the special orthogonal group $\mathbf{SO}_n(f)$ of a nonsingular quadratic form f (cf. also §6.6).

PROPOSITION 2.8. *The elements of $H^1(K, \mathbf{SO}_n(f))$ are in one-to-one correspondence with the K-equivalence classes of those quadratic forms of degree n over K that have the same discriminant as f.*

Other examples of cohomology computations will occur in Chapter 6, which is specifically devoted to the Galois cohomology of algebraic groups. For the time being we shall conclude our brief study of this topic by reducing the computation of the cohomology of connected groups to that of reductive groups.

LEMMA 2.7. *Let K be a field of characteristic 0. Then for any unipotent group U defined over K we have $H^1(K,U) = 1$.*

PROOF: To begin with, let us establish the additive form of Hilbert's Theorem 90, which asserts that $H^1(K,\mathbb{G}_a) = 1$, i.e., $H^1(\mathcal{F},L) = 1$ for any finite Galois extension L/K with Galois group $\mathcal{F}$. Let $c \in L$ be an element such that $\mathrm{Tr}_{L/K}(c) \neq 0$. Given a 1-cocycle $a = \{a_\sigma\} \in Z^1(\mathcal{F},L)$, we put

$$b = \frac{1}{\mathrm{Tr}_{L/K}(c)} \sum_{\tau\in\mathcal{F}} a_\tau \tau(c).$$

Direct computation then shows that $a_\sigma = b - \sigma(b)$ for any $\sigma \in \mathcal{F}$, i.e., a is trivial. In fact, the normal basis theorem (cf. Lang [3, p. 229]) implies that L is an induced $\mathcal{F}$-module, and therefore $H^i(\mathcal{F},L) = 1$ for all $i \geq 1$, by Shapiro's Lemma.

For an arbitrary unipotent K-group U the proof is by induction on $\dim U$. Using the series mentioned in §2.1.8, we can find a normal K-subgroup $W \subset U$ isomorphic to $\mathbb{G}_a$. Then the exact sequence

$$1 \to W \to U \to U/W \to 1$$

yields the exact cohomological sequence

$$H^1(K,W) \to H^1(K,U) \to H^1(K,U/W).$$

But as proved above, $H^1(K,W) = 1$, and $H^1(K,U/W) = 1$ by the inductive hypothesis, so $H^1(K,U) = 1$ as desired.

Note that the lemma remains true for any perfect field K, assuming U is connected (same proof). In general (i.e., if U is not connected or K is not perfect) $H^1(K,U) \neq 1$ (cf. Serre [1, Ch. 3]).

PROPOSITION 2.9. *Let G be a connected group defined over a field K of characteristic 0, and let H be a maximal reductive K-subgroup (cf. Theorem 2.3). Then the embedding $H \subset G$ induces a bijection $H^1(K,H) \xrightarrow{\sim} H^1(K,G)$.*

PROOF: Let $G = HU$ be the corresponding Levi decomposition, where $U = R_u(G)$ is the unipotent radical of G (cf. §2.1.9) and $\pi: G \to H \simeq G/U$ is the canonical map. Then the composition $H \xrightarrow{\varphi} G \xrightarrow{\pi} H$, where φ is the natural embedding, is the identity map; so the composition of the corresponding cohomology maps

$$H^1(K,H) \xrightarrow{\varphi_*} H^1(K,G) \xrightarrow{\pi_*} H^1(K,H)$$

is also the identity map. Therefore, to prove the proposition it suffices to prove that π_* is injective. π_* can be put into an exact cohomological sequence

$$H^1(K,U) \to H^1(K,G) \xrightarrow{\pi_*} H^1(K,H), \tag{2.11}$$

arising from the exact sequence $1 \to U \to G \to H \to 1$. By Lemma 2.7, $H^1(K,U) = 1$; hence it follows from (2.11) that $\ker \pi_*$ is trivial.

Unfortunately, in noncommutative cohomology in general we cannot claim that the triviality of $\ker \pi_*$ implies the injectivity of π_*. Instead, we use a standard trick based on twisting. Namely, let $\pi_*(g) = \pi_*(h)$ for $g, h \in Z^1(K,G)$ (we shall use the same letters to denote the corresponding cohomology classes. We write ${}_gG$ (respectively ${}_gU$) for the group obtained from G (respectively U) by twisting using g, and let $\tau_g: H^1(K,{}_gG) \to H^1(K,G)$ be the corresponding bijection (cf. Lemma 1.5). Put $F = {}_gG/{}_gU = {}_g(G/U)$ and consider the sequence

$$H^1(K,{}_gU) \to H^1(K,{}_gG) \xrightarrow{{}_g\pi_*} H^1(K,F), \tag{2.12}$$

in analogy to (2.11). Obviously $f = \tau_g^{-1}(h) \in \ker {}_g\pi_*$. On the other hand ${}_gU$ is isomorphic to U over $\bar{K}$ and hence is unipotent, so $H^1(K,{}_gU) = 1$ by Lemma 2.7. Then, by (2.12), $\ker {}_g\pi_*$ is trivial, and therefore $f = 1$ and $g = h$. Q.E.D.

2.2.4. Classification of K-forms of algebraic groups. We shall consider two special cases: algebraic tori and semisimple groups.

Let T be a d-dimensional algebraic K-torus with splitting field L and let $\mathcal{F} = \mathrm{Gal}(L/K)$. Then there is an L-isomorphism $T \simeq \mathbb{G}_m^d$. Thus all such K-tori are L/K-forms of the d-dimensional K-split torus $\mathbb{G}_m^d$. Therefore, according to Theorem 2.9, the K-isomorphism classes of such tori are in one-to-one correspondence with the elements of $H^1(\mathcal{F},\mathrm{Aut}_L(\mathbb{G}_m^d))$. But Theorem 2.1 implies that

$$\mathrm{Aut}_L(\mathbb{G}_m^d) = \mathrm{Aut}_K(\mathbb{G}_m^d) \simeq GL_d(\mathbb{Z}),$$

from which it follows that the K-isomorphism classes are in one-to-one correspondence with the equivalence classes of d-dimensional integral representations of $\mathcal{F}$. For example, if L/K is a quadratic extension, then any $\mathbb{Z}$-torsion free finitely generated $\mathbb{Z}[\mathcal{F}]$-module M can be written in the form $M = \mathbb{Z}^l \oplus \mathbb{Z}[\mathcal{F}]^m \oplus I^n$, where I is the kernel of the augmentation map $\mathbb{Z}[\mathcal{F}] \to \mathbb{Z}$, and l, m and n are uniquely determined. Therefore any L-split K-torus T can be written as

$$T = \mathbb{G}_m^l \times \mathbf{R}_{L/K}(\mathbb{G}_m)^m \times \mathbf{R}^{(1)}_{L/K}(\mathbb{G}_m)^n$$

for some positive, uniquely determined integers l, m, n; and any K-anisotropic torus in this class must have the form $T = \mathbf{R}^{(1)}_{L/K}(\mathbb{G}_m)^n$.

We proceed to the semisimple case. First we shall show that for any semisimple K-group G there exists a K-split group G_0 such that $G \simeq G_0$ over $\bar{K}$. To see this, consider a universal $\bar{K}$-covering $\tilde{G} \xrightarrow{\pi} G$ (cf. §2.1.13). Then there is a $\bar{K}$-isomorphism $\varphi\colon \tilde{G} \simeq \tilde{G}_0$ where $\tilde{G}_0$ is a K-split simply connected group of the same type as G, and to prove the existence of G_0 it suffices to show that $\varphi(\ker \pi)$ is a K-group. But the center Z of $\tilde{G}_0$ is contained in a maximal K-split torus; hence the Galois group acts trivially on the group of characters $\mathbf{X}(Z)$, so any subgroup of Z, in particular $\varphi(\ker \pi)$, is defined over K. Thus any semisimple K-group G can be obtained from a suitable K-split group G_0 by twisting with a cocycle from $H^1(K, \mathrm{Aut}_{\bar{K}}(G_0))$. Since $\mathrm{Aut}_{\bar{K}}(G_0)$ is precisely the subgroup of $\mathrm{Aut}_{\bar{K}}(\tilde{G}_0)$ fixing $\ker \pi$ (Theorem 2.8), the universal K-covering $\tilde{G}_0 \to G_0$ can be twisted using any element from $H^1(K, \mathrm{Aut}_{\bar{K}}(G_0))$. This yields

PROPOSITION 2.10. *Let G be a semisimple K-group. Then there exists a universal covering $\pi\colon \tilde{G} \to G$ defined over K.*

As we shall see later, the existence of a universal K-covering for arbitrary semisimple K-groups is an important tool in the arithmetic theory of algebraic groups. Unfortunately there is no canonical analog of the universal covering for arbitrary reductive groups; however in several cases a special covering (cf. Sansuc [1]) can be used instead. A K-isogeny $f\colon H \to G$ of reductive K-groups is called a *special covering* if H is a direct product of a simply connected semisimple K-group D by a K-quasisplit torus S. Although straightforward examples show that in general a reductive group need not have a special covering, we do have

PROPOSITION 2.11. *For an arbitrary reductive K-group G there is a positive integer m and a quasisplit K-torus T such that $G^m \times T$ has a special covering.*

PROOF: By Theorem 2.4 G is an almost direct product of its semisimple part D_1 and a maximal central torus S_1. Using Proposition 2.3 we find $m > 0$ and a quasisplit K-torus T such that $S_1^m \times T$ is covered by a suitable quasisplit torus S, i.e., there is an isogeny $S \xrightarrow{\varphi} S_1^m \times T$ defined over K. Consider also the universal K-covering $D \xrightarrow{\pi} D_1$, and set $H = D^m \times S$. Then the composition map

$$H = D^m \times S \xrightarrow{\pi^m \times \varphi} D_1^m \times S_1^m \times T = (D_1 \times S_1)^m \times T \to G^m \times T$$

will be the desired covering.

By Proposition 2.10 the classification of semisimple K-groups reduces to that of simply connected ones. From Theorem 2.6 it follows that a simply connected K-group is a direct product of simply connected (almost) K-simple groups (i.e., groups containing no proper nontrivial connected normal K-subgroups), and, moreover, any simply connected K-simple group has the form $\mathbf{R}_{L/K}(G)$ where G is an absolutely simple L-group. Therefore it suffices to consider K-forms of simply connected simple groups.

Let G be a given simple, simply connected K-split group and let $\bar{G} = G/Z(G)$ be the corresponding adjoint group. We identify $\bar{G}$ with $\mathrm{Int}_{\bar{K}} G$, the group of inner automorphisms of G. Then the full automorphism group $\mathrm{Aut}_{\bar{K}} G$ is a semidirect product of $\bar{G}_{\bar{K}}$ by $\mathrm{Sym}(R)$, the group of symmetries of the Dynkin diagram of the root system R of G (cf. §2.1.13); moreover, $\mathcal{G} = \mathrm{Gal}(\bar{K}/K)$ acts on $\mathrm{Sym}(R)$ trivially. Thus, we have a split exact sequence of K-groups

$$1 \to \bar{G}_{\bar{K}} \to \mathrm{Aut}_{\bar{K}} G \underset{\psi}{\overset{\varphi}{\rightleftarrows}} \mathrm{Sym}(R) \to 1, \tag{2.13}$$

which yields the exact cohomological sequence

$$H^1(K, \bar{G}) \to H^1(K, \mathrm{Aut}_{\bar{K}} G) \underset{\beta}{\overset{\alpha}{\rightleftarrows}} H^1(K, \mathrm{Sym}(R)).$$

Since $\mathrm{Sym}(R) = \mathrm{Sym}(R)_K$, any cocycle a on $\mathcal{G}$ with values in $\mathrm{Sym}(R)$ is just a continuous homomorphism $\mathcal{G} \to \mathrm{Sym}(R)$, and $H^1(K, \mathrm{Sym}(R))$ is the set of conjugacy classes of such homomorphisms. It is well known that $\psi(\mathrm{Sym}(R)) \subset \mathrm{Aut}_{\bar{K}} G$ consists of those automorphisms that fix the maximal K-split torus $T \subset G$ and the Borel K-subgroup $B \subset G$ containing it. Therefore, for any a in $H^1(K, \mathrm{Sym}(R))$ the K-form of the group corresponding to $\beta(a) \in H^1(K, \mathrm{Aut}_{\bar{K}} G)$ has a Borel K-subgroup, i.e., is quasisplit over K. Thus, for any a in $H^1(K, \mathrm{Sym}(R))$ the fiber $\alpha^{-1}(a)$ contains a quasisplit K-group ${}_aG$ which, moreover, is uniquely determined up

to K-isomorphism. The groups that correspond to the elements of $\alpha^{-1}(a)$ are said to have the same inner type. This term is explained by the fact that $\alpha^{-1}(a)$ is the image of the map $H^1(K, {}_a\bar{G}) \to H^1(K, \mathrm{Aut}({}_aG)) \simeq H^1(K, \mathrm{Aut}_{\bar{K}} G)$, where the last isomorphism is a "translation" by $\beta(a)$ (cf. §1.3.2); thus groups of the same inner type are obtained from the corresponding quasisplit group by twisting using an element from $H^1(K, {}_a\bar{G})$, i.e., using inner automorphisms. The fiber of α over the trivial cocycle in $H^1(K, \mathrm{Sym}(R))$ consists of what we call inner forms of G, this definition being consistent with the definition of inner forms given in the previous subsection. Inner forms, and only these, are obtained by means of twisting using elements of $H^1(K, \bar{G})$. In the next section, using these results we shall obtain an explicit classification of the groups of classical type.

2.3. The classical groups.

The goal of this section is to introduce algebraic groups whose groups of rational points are classical groups over skew fields, i.e., special linear, symplectic, special orthogonal and special unitary groups. These groups, with few exceptions, turn out to be simple algebraic groups related to the classical types A_n, B_n, C_n and D_n. It is noteworthy that the converse result holds: every group of classical type, with the exception of ${}^3D_4$ and ${}^6D_4$ in Tits' notation [2], can be described, up to isogeny, as one of the classical groups. Unfortunately, this result, due to A. Weil [3], has not yet appeared in book form (except for M. Kneser's lecture notes [12]). Therefore we shall present complete proofs of those results. The argument is based on the classification of K-forms by means of Galois cohomology and the notion of twisting.

2.3.1. The special linear group. Let D be a finite-dimensional central skew field of index d over K, and let $n \geq 1$. Then $A = M_n(D)$ is a simple algebra and we have the reduced norm map $\mathrm{Nrd}_{A/K}: A^* \to K^*$ (cf. §1.4.1). Set $SL_n(D) = \{ x \in A^* : \mathrm{Nrd}_{A/K}(x) = 1 \}$ and show that this group is the group of K-points of a certain algebraic group G, which we denote as $\mathbf{SL}_n(D)$. Let $\varrho: D \to M_{d^2}(K)$ be the regular representation of D.[1] $\varrho(D)$, being a linear subspace of $M_{d^2}(K)$, is determined by a system

$$f_k(x_{ij}) = 0, \quad i, j = 1, \ldots, d^2; \; k = 1, \ldots, l$$

of linear equations for the entries x_{ij} of a matrix $x = (x_{ij})$, with coefficients in K. Identifying $M_{nd^2}(K)$ with $M_n(M_{d^2}(K))$, we let $\tilde{A}$ denote the subset

[1] i.e., an element x in D is sent to the matrix corresponding (with respect to a fixed base) to the K-linear transformation $y \mapsto xy$ of D, viewing D as a d^2-dimensional vector space over K.

of $M_{nd^2}(K)$ consisting of the elements $x = (x_{ij}^{\alpha\beta})$ for $i, j = 1, \ldots, d^2$ and $\alpha, \beta = 1, \ldots, n$ such that

$$f_k(x_{ij}^{\alpha\beta}) = 0 \quad \text{for all } \alpha, \beta = 1, \ldots, n \text{ and } k = 1, \ldots, l. \tag{2.14}$$

Clearly, ϱ identifies A with $\tilde{A}$. Moreover, it is well known (cf. §1.4.1) that the reduced norm of x in A can be expressed as a polynomial with coefficients in K in the coordinates of x with respect to an arbitrary base A/K. It follows that there exists a polynomial $g(x_{ij}^{\alpha\beta})$ over K such that

$$\mathrm{Nrd}_{A/K}((x^{\alpha\beta})) = g(\varrho(x^{\alpha\beta})) \quad \text{for } \alpha, \beta = 1, \ldots, n.$$

Then obviously the set of matrices $x = (x_{ij}^{\alpha\beta}) \in M_{nd^2}(K)$ satisfying (2.14) and the equation

$$g(x_{ij}^{\alpha\beta}) = 1 \tag{2.15}$$

can be identified with $SL_n(D)$ in the natural way. Now take G to be the set of solutions of (2.14) and (2.15) in $M_{nd^2}(\Omega)$. Then G is an algebraic K-group whose set of K-points is $SL_n(D)$. In addition, using isomorphisms $D \otimes_K \Omega \simeq M_d(\Omega)$ and $A \otimes_K \Omega \simeq M_{nd}(\Omega)$ it is easy to construct an Ω-isomorphism $G \simeq SL_{nd}(\Omega)$, from which it follows that G is a simply connected simple K-group of type A_{nd-1}.

PROPOSITION 2.12. *For $G = \mathbf{SL}_n(D)$ we have $\mathrm{rank}_K G = n - 1$. In particular, $H = \mathbf{SL}_1(D)$ is a K-anisotropic group.*

PROOF: Let T denote the set of matrices $x = (x_{ij}^{\alpha\beta}) \in G$

$$\text{such that } \begin{cases} x_{ij}^{\alpha\beta} = 0 & \text{for } \alpha \neq \beta \\ x^{\alpha\beta} = (x_{ij}^{\alpha\beta})_{i,j=1,\ldots,d^2} \text{ is a scalar matrix} & \text{for } \alpha = \beta. \end{cases}$$

It is easy to see that T is a K-split $(n-1)$-dimensional torus in G. Moreover, its centralizer $Z_G(T)$ consists of all matrices $x = (x_{ij}^{\alpha\beta}) \in G$ such that $x_{ij}^{\alpha\beta} = 0$ for $\alpha \neq \beta$. Let $H = \mathbf{SL}_1(D)$. It follows that $H^n = H \times \ldots \times H$ is naturally embedded in $Z_G(T)$, and the restriction to H^n of the canonical morphism $Z_G(T) \to Z_G(T)/T$ is an isogeny. Therefore it suffices to establish that H is K-anisotropic. But any maximal K-torus in H has the form $\mathbf{R}^{(1)}_{L/K}(\mathbb{G}_m)$, where $L \subset D$ is a maximal subfield, and therefore K is anisotropic (cf. §2.1.7). Q.E.D.

Now we shall compute the cohomology of $G = \mathbf{SL}_n(D)$. To do so, first consider the algebraic group $H = \mathbf{GL}_n(D)$ which is defined to be the subgroup of $GL_{nd^2}(\Omega)$ consisting of those matrices which satisfy (2.14). Then H has as the group of K-points the group $GL_n(D)$ of invertible elements of $A = M_n(D)$, and over $\bar{K}$ is isomorphic to $GL_{nd}(\Omega)$. Analogously to Lemma 2.2 one can prove

LEMMA 2.8. $H^1(K, \mathbf{GL}_n(D)) = 1$ *for any* $n \geq 1$.

The cohomology of G is computed using the exact sequence

$$1 \to G \to H \xrightarrow{\varphi} \mathbb{G}_m \to 1, \tag{2.16}$$

where φ is induced by $\mathrm{Nrd}_{A/K}$. Corresponding to (2.16) we have the exact cohomological sequence

$$GL_n(D) \xrightarrow{\mathrm{Nrd}_{A/K}} K^* \to H^1(K, G) \to H^1(K, H) = 1,$$

from which we obtain

LEMMA 2.9.
$H^1(K, \mathbf{SL}_n(D)) \simeq K^*/\mathrm{Nrd}_{A/K}(GL_n(D)) = K^*/\mathrm{Nrd}_{D/K} D^*$.

2.3.2. The symplectic and orthogonal groups. Let $f(x, y)$ be a nondegenerate alternating (respectively, symmetric) bilinear form on the vector space $V = K^n$ over a field K of characteristic $\neq 2$ (for the definition and basic properties of bilinear and sesquilinear forms we refer the reader to any of the following books: Bourbaki [1], Dieudonné [2], Artin [1]). Note that if f is a nondegenerate alternating form, then n is necessarily even, i.e., $n = 2m$. The group of automorphisms preserving f, i.e., those linear transformations $\sigma: V \to V$ such that

$$f(\sigma(x), \sigma(y)) = f(x, y) \quad \text{for all } x, y \in V,$$

when f is an alternating form, is called the *symplectic group* and is written $Sp_{2m}(f)$, and when f is a symmetric form, it is called the *orthogonal group* and is written $O_n(f)$. (By virtue of the well-known one-to-one correspondence between symmetric bilinear forms and quadratic forms, the orthogonal group usually is defined in terms of the corresponding quadratic form, and in this case we write $f(x)$ instead of $f(x, x)$.) The determinant of any transformation in $Sp_{2m}(f)$ is always 1, and of any transformation in $O_n(f)$ is ± 1, so $SO_n(f) = \{\sigma \in O_n(f) : \det \sigma = 1\}$ is a subgroup of $O_n(f)$ of index 2.

Let $e_1, \ldots, e_n$ be a base of V and let $F = (f(e_i, e_j))$ be the matrix of f. Then, writing transformations by matrices with respect to $e_1, \ldots, e_n$ we obtain

$$\begin{aligned} Sp_{2m}(F) &= \{g \in GL_{2m}(K) : {}^t gFg = F\}, \text{ where } {}^t F = -F \\ O_n(F) &= \{g \in GL_n(K) : {}^t gFg = F\}, \text{ where } {}^t F = F \\ SO_n(F) &= \{g \in O_n(f) : \det g = 1\}, \end{aligned} \tag{2.17}$$

where ^{t} denotes the matrix transpose. Now let $\mathbf{Sp}_{2m}(F)$, $\mathbf{O}_n(F)$ and $\mathbf{SO}_n(F)$ denote the set of matrices $g \in GL_n(\Omega)$ satisfying the respective conditions in (2.17). Then each of these sets is an algebraic K-group, whose group of K-points coincides with the corresponding group $Sp_{2m}(F)$, $O_n(F)$ or $SO_n(F)$. (Sometimes, for convenience of notation, we shall write $\mathbf{O}_n(f)$ instead of $\mathbf{O}_n(F)$.)

When the base $e_1, \ldots, e_n$ is changed to another base $e_1', \ldots, e_n'$, F changes to the equivalent matrix $F' = {}^t xFx$, where x is the change of base matrix; then $\mathbf{Sp}_{2m}(F') = x\mathbf{Sp}_{2m}x^{-1}$, and so on. On the other hand, it is well known (cf. Bourbaki [1]) that any nonsingular skew-symmetric matrix F in $M_{2m}(K)$ is equivalent over K to the standard skew-symmetric matrix

$$J = \begin{pmatrix} 0 & E_m \\ -E_m & 0 \end{pmatrix}, \tag{2.18}$$

so that we have a K-isomorphism $\mathbf{Sp}_{2m}(F) \simeq \mathbf{Sp}_{2m}(J)$. Take T to be

$$\{t = \mathrm{diag}(\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_m) \in GL_{2m}(\Omega) : \alpha_i\beta_i = 1,\ i = 1, \ldots, m\}.$$

It is easy to see that T is a K-split torus in $G = \mathbf{Sp}_{2m}(J)$; moreover direct computation shows that $Z_G(T) = T$. Thus G is K-split and T is its maximal K-split torus. Analyzing the root system $R = R(T, G)$ as described in Bourbaki [4], we see that R is an irreducible root system of type C_m. Moreover, using the criterion for the group to be simply connected (cf. assertion (3) of Theorem 2.6) it can be shown that G is simply connected. Thus we obtain

PROPOSITION 2.13. *Let* $G = \mathbf{Sp}_{2m}(F)$ $(m \geq 1)$, *where* F *is a nonsingular skew-symmetric matrix. Then* G *is a* K*-split group of type* C_m.

Similarly, over $\bar{K}$ any nonsingular symmetric matrix is equivalent to one of the matrices

$$Q_1 = \begin{pmatrix} 0 & E_m \\ E_m & 0 \end{pmatrix}, \qquad n = 2m$$

or

$$Q_2 = \begin{pmatrix} 0 & & E_m & 0 \\ & & & \vdots \\ E_m & & 0 & 0 \\ 0 & \ldots & 0 & 1 \end{pmatrix}, \qquad n = 2m + 1. \tag{2.19}$$

Then $T = \{\operatorname{diag}(\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_m) : \alpha_i\beta_i = 1,\ i = 1, \dots, m\}$ (resp., $T = \{\operatorname{diag}(\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_m, 1) : \alpha_i\beta_i = 1,\ i = 1, \dots, m\}$) is a maximal torus in $G = \mathbf{SO}_n(Q_1)$ (resp., $G = \mathbf{SO}_n(Q_2)$) and the corresponding root system $R(T, G)$ has type D_m ($m \geq 2$) in the first case (under the convention that $D_2 = A_1 + A_1$ and $D_3 = A_3$) and type B_m ($m \geq 1$) in the second, cf. Bourbaki [4] ($G = \mathbf{SO}_2(Q_1)$ is a one-dimensional torus). Thus, $G = \mathbf{SO}_n(F)$ for $n \geq 3$ is a semisimple group of type $B_{\frac{n-1}{2}}$ (for odd n) or $D_{\frac{n}{2}}$ (for even n). (Actually, G is simple except for the case $n = 4$, when $D_2 = A_1 + A_1$).) G is not simply connected; its universal K-covering is the *spinor group* $\tilde{G} = \operatorname{Spin}_n(F)$ constructed by using Clifford algebras (cf. Bourbaki [1], Dieudonné [2]). The kernel $\Phi = \ker \pi$ of the universal K-covering $\pi: \tilde{G} \to G$ has order 2 and consists of $\{\pm 1\}$ in the sense of the corresponding Clifford algebra. Hence it follows that for $l \leq n$ we have a commutative diagram of universal coverings

$$\begin{array}{ccc} \operatorname{Spin}_n & \longrightarrow & \mathbf{SO}_n \\ \uparrow & & \uparrow \\ \operatorname{Spin}_l & \longrightarrow & \mathbf{SO}_l \end{array}$$

in which the vertical arrows are embeddings.

PROPOSITION 2.14. *Let $G = \mathbf{SO}_n(F)$ for $n \geq 3$, where F is a nonsingular symmetric matrix. Then G is a nonsimply connected semisimple K-group of type $B_{\frac{n-1}{2}}$ if n is odd, and of type $D_{\frac{n}{2}}$ if n is even. Moreover, $\operatorname{rank}_K G$ is the Witt index of the corresponding quadratic form f. In particular, G is K-anisotropic if and only if f is anisotropic.*

All that remains to be proven is the assertion about the K-rank of G. For this, recall that the Witt index of a form f is the dimension of a maximal totally isotropic subspace $W \subset V = K^n$ (i.e., of a subspace such that $f(x) = 0$ for all x in W). Set $l = \dim W$. Then f is equivalent over K to a form $x_1x_{l+1} + \cdots + x_lx_{2l} + f_0(x_{2l+1}, \dots, x_n)$, where f_0 is K-anisotropic. Therefore, without loss of generality, we may assume that f itself is such a form. Let

$$T = \{t = \operatorname{diag}(\alpha_1, \dots, \alpha_l, \beta_1, \dots, \beta_l) \in GL_n(\bar{K}) : \alpha_i\beta_i = 1 \text{ for } 1 \leq i \leq l\}$$

be a split l-dimensional torus. It is easy to see that $T \subset \mathbf{SO}_n(f)$, and direct computation shows that $Z_G(T) \simeq T \times \mathbf{SO}_{n-2l}(f_0)$. Therefore it suffices to establish that $H = \mathbf{SO}_{n-2l}(f_0)$ is K-anisotropic. But if $S \subset H$ is a nontrivial K-split torus, then there exists a nonzero eigenvector $v \in K^{n-2l}$ for S with a nontrivial character $\chi: S \to K$. Thus for any s in S we have $f_0(v) = f_0(sv) = f_0(\chi(s)v) = \chi(s)^2 f_0(v)$; from which it follows that $f_0(v) = 0$, which contradicts f_0 being K-anisotropic. This completes the proof of Proposition 2.14.

2.3.3. Unitary groups. Let us begin with a few remarks about algebras with involution. Let A be a finite-dimensional (associative) algebra over a field K and let $L = Z(A)$ be the center of A. By an *involution* of A we mean an arbitrary K-linear antiautomorphism $\tau: A \to A$ of order 2. Then τ is said to be of the first kind if its restriction to the center is trivial, and of the second kind otherwise. An algebra A with involution τ is written (A, τ).

Some examples of involution are:

(1) $A = M_n(K)$, $\tau(x) = {}^t x$ the matrix transpose;
(2) $A = M_n(K)$, $\tau(x) = J{}^t xJ^{-1}$, where J is given by (2.18);
(3) $A = A_1 \oplus A_2$, $A_i = M_n(K)$, $\tau(x, y) = ({}^t y, {}^t x)$.

Our objective is to show that any involution on a simple algebra goes over to one of the involutions listed above, after extension of the center to an algebraically closed field. So, let (A, τ) be an arbitrary simple K-algebra with involution. Then its center L is a field. Throughout the remainder of the section we shall assume that K is the fixed subfield L^τ of L under τ.

Let σ be another involution of A such that $\tau\,|_L = \sigma\,|_L$. Then $\varphi = \sigma\tau^{-1}$ is an automorphism of A which acts trivially on the center, so by the Skolem-Noether theorem $\varphi = \operatorname{Int} g$ for a suitable g in A^*. Then $\sigma(x) = g\tau(x)g^{-1}$ for $x \in A$ and $\sigma^2 = \mathrm{id}$ yields $g\tau(g)^{-1} \in L$. If we assume that τ is an involution of the first kind, i.e., that $L = K$, then we immediately obtain $\tau(g) = \pm g$. If, however, τ is an involution of the second kind, then since $N_{L/K}(g\tau(g)^{-1}) = g\tau(g)^{-1}\tau(g\tau(g)^{-1}) = 1$, we can find a in L satisfying $g\tau(g)^{-1} = a\tau(a)^{-1}$ by Hilbert's Theorem 90. Then, substituting ga^{-1} for g, we may assume that $\tau(g) = g$. Thus we obtain

LEMMA 2.10. *Let τ and σ be two involutions of a simple algebra A whose restrictions to the center of A coincide. Then, for suitable g in A^**

$$\sigma(x) = g\tau(x)g^{-1} \quad \text{for } x \in A, \tag{2.20}$$

where moreover $\tau(g) = \pm g$ for τ of the first kind and $\tau(g) = g$ for τ of the second kind. Conversely, for any involution τ and any g in A^* satisfying the properties described, the map σ given by (2.20) is an involution of A.

Now let (A, τ) be a simple K-algebra with involution. If τ is an involution of the first kind, then K is the center of A and therefore $A \otimes_K \bar{K} \overset{\varphi}{\simeq} M_n(\bar{K})$. We shall show that φ can be chosen here in such a way that the

$\bar{K}$-linear extension of τ (which we shall also denote by τ) becomes one of the involutions (1) or (2).

Let $\nu = \varphi\tau\varphi^{-1}$. Applying Lemma 2.10 to the matrix transpose (viewed as an involution of $M_n(\bar{K})$) and ν, we obtain the existence of an element F in $GL_n(\bar{K})$ such that ${}^tF = \pm F$ and $\nu(x) = F\,{}^txF^{-1}$. Furthermore, there exists a matrix B in $GL_n(\bar{K})$ such that $F = B\,{}^tB$ if F is symmetric and $F = {}^tBJB$ if F is skew-symmetric (where J is the same as in (2.18)). Then a direct computation shows that $\psi\colon A \otimes_K \bar{K} \simeq M_n(\bar{K})$ for $\psi = \operatorname{Int} B^{-1} \circ \varphi$ satisfies the required properties.

If τ is an involution of the second kind, then $[L : K] = 2$, so

$$A \otimes_K \bar{K} = (A \otimes_K L) \otimes_L \bar{K} \overset{\varphi}{\simeq} M_n(\bar{K}) \oplus M_n(\bar{K}).$$

Here $A \otimes_K \bar{K}$ is a semisimple, but not necessarily simple, algebra; nevertheless the proof of Lemma 2.10 goes through without any changes. Reasoning as above, we can construct an isomorphism $\psi\colon A \otimes_K \bar{K} \xrightarrow{\sim} M_n(\bar{K}) \oplus M_n(\bar{K})$ under which τ goes over to the involution described in (3).

Now let $f(x, y)$ be a nondegenerate Hermitian or skew Hermitian sesquilinear form on an m-dimensional vector space $V = D^m$ over a skew field D with involution τ, let L be the center of D, and let $K = L^\tau$ be the fixed field under τ. The group of automorphisms preserving f is called the *unitary group*, denoted by $U_m(D, f)$; its subgroup consisting of automorphisms having reduced norm 1 is called the *special unitary group* $SU_m(D, f)$. Let $e_1, \ldots, e_m$ be a base of V and let $F = (f(e_i, e_j))$ be the matrix of f. Then ${}^*F = \pm F$ and, with respect to $e_1, \ldots, e_m$,

$$U_m(D, f) = \{g \in GL_m(D) : {}^*gFg = F\},$$

and

$$SU_m(D, f) = \{g \in U_m(D, f) : \operatorname{Nrd}_{M_m(D)/L}(g) = 1\},$$

where ${}^*g = (\tau(g^{\beta\alpha}))$ if $g = (g^{\alpha\beta})$. (Note that * is an involution of $A = M_n(D)$ of the same kind as τ.) In order to realize $U_m(D, f)$ and $SU_m(D, f)$ as groups of K-rational points of certain algebraic groups as in §2.3.1, we consider the regular representation $\varrho\colon D \to M_{ln^2}(K)$ of D over K (n is the index of D and $l = [L : K]$), and the corresponding equations of the form (2.14) defining D as a subspace of $M_{ln^2}(K)$. Further, let $\tilde{\tau}\colon M_{ln^2}(K) \to M_{ln^2}(K)$ be an invertible linear map extending the involution $\varrho\tau\varrho^{-1}$ on $\varrho(D)$, and let $\Phi = (\varrho(f^{\alpha\beta}))$ be the matrix in $M_{lmn^2}(K)$ corresponding to $F = (f^{\alpha\beta})$. Then the image of $U_m(D, f)$ in $M_{lmn^2}(K)$ under the homomorphism induced by ϱ consists of matrices

$$g = (g_{ij}^{\alpha\beta}) \qquad \text{for } \alpha, \beta = 1, \ldots, m \text{ and } i, j = 1, \ldots, ln^2$$

satisfying (2.14) and

$$(\tilde{\tau}(g_{ij}^{\alpha\beta}))\Phi(g_{ij}^{\alpha\beta}) = \Phi. \tag{2.21}$$

Similarly, the image of $SU_m(D, f)$ is given by (2.14), (2.21) and an equation of the form (2.15). The solutions of these equations over $\bar{K}$ yield the algebraic groups $\mathbf{U}_m(D, f)$ and $\mathbf{SU}_m(D, f)$ respectively.

To understand the structure of these groups, we put $\sigma(x) = F^{-1*}xF$. Then σ is an involution on $A = M_m(D)$ by Lemma 2.10; moreover

$$U_m(D, f) = \{\, g \in GL_m(D) : \sigma(g)g = E_m \,\}$$
$$SU_m(D, f) = \{\, g \in U_m(D, f) : \operatorname{Nrd}_{A/L}(g) = 1 \,\}.$$

Above we showed that if τ is an involution of the first kind one can choose the isomorphism $A \otimes_K \bar{K} \simeq M_{mn}(\bar{K})$ in such a way that σ extends to one of the involutions ν in (1) or (2). Then the corresponding groups

$$\mathbf{U}_m(D, f) = \{g \in (A \otimes_K \bar{K})^* : \sigma(g)g = E_m\}$$
$$\mathbf{SU}_m(D, f) = \{g \in \mathbf{U}_m(D, f) : \operatorname{Nrd}_{A \otimes_K \bar{K}/\bar{K}}(g) = 1\}$$

become

$$G = \{g \in GL_{mn}(\bar{K}) : \nu(g)g = E_{mn}\} \text{ and}$$
$$H = \{g \in SL_{mn}(\bar{K}) : \nu(g)g = E_{mn}\},$$

which are none other than the orthogonal and special orthogonal groups, if ν is as in (1) (an involution *of the first type*) and which coincide with the symplectic group if ν is as described in (2) (an involution *of the second type*). Note that there is an invariant description of involutions of first and second type: τ has the first (respectively, second) type if $\dim_K D^\tau = \frac{n(n+1)}{2}$ (resp. $\dim_K D^\tau = \frac{n(n-1)}{2}$). Moreover, ν has the same type as τ if F is Hermitian, and has the opposite type if F is skew Hermitian.

Now let τ be an involution of the second kind. Then we can choose an isomorphism $A \otimes_K \bar{K} \simeq M_{mn}(\bar{K}) \oplus M_{mn}(\bar{K})$ in such a way that τ extends to an involution ν as in (3). Then $\mathbf{U}_m(D, f)$ and $\mathbf{SU}_m(D, f)$ become the groups

$$G = \{\, (X, Y) \in GL_{mn}(\bar{K}) \times GL_{mn}(\bar{K}) : (X, Y)({}^tY, {}^tX) = (E_{mn}, E_{mn}) \,\}$$

and

$$H = \{\, (X, Y) \in SL_{mn}(\bar{K}) \times SL_{mn}(\bar{K}) : (X, Y)({}^tY, {}^tX) = (E_{mn}, E_{mn}) \,\}.$$

Now it is evident that

$$G = \{\, (X, {}^tX^{-1}) : X \in GL_{mn}(\bar{K}) \,\} \quad \text{and}$$
$$H = \{\, (X, {}^tX^{-1}) : X \in SL_{mn}(\bar{K}) \,\},$$

so we conclude that $\mathbf{U}_m(D, f)$ and $\mathbf{SU}_m(D, f)$ are isomorphic over $\bar{K}$ to $GL_{mn}(\bar{K})$ and $SL_{mn}(\bar{K})$ respectively.

PROPOSITION 2.15. *Let $G = \mathbf{SU}_m(D, f)$, where D is a skew field of index n with involution τ and f is a nondegenerate Hermitian or skew Hermitian form on D^m. Then over $\bar{K}$ we have:*

(1) *$G \simeq \mathbf{Sp}_{mn}$, i.e., is a simple simply connected group of type $C_{\frac{mn}{2}}$, if τ is an involution of the first kind of the first type and f is skew Hermitian, or if τ is an involution of the first kind of the second type and f is Hermitian;*

(2) *$G \simeq \mathbf{SO}_{mn}$, i.e., is a semisimple not simply connected group of type $B_{\frac{mn-1}{2}}$ or $D_{\frac{mn}{2}}$ (note that type B occurs only when $n = 1$, i.e., $D = K$) if τ is an involution of the first kind of the first type and f is Hermitian, or if τ is an involution of the first kind of the second type and f is skew Hermitian;*

(3) *$G \simeq \mathbf{SL}_{mn}$, i.e., is a simply connected simple group of type A_{mn-1} if τ is an involution of the second kind.*

In all these cases $\operatorname{rank}_K G$ coincides with the Witt index of f, i.e., with the dimension of a maximal totally isotropic subspace in D^m.

Note that the groups $\mathbf{SO}_n(F)$ and $\mathbf{Sp}_{2m}(F)$ considered in §2.3.2 can be treated as unitary groups with respect to the identity involution on $D = K$. Moreover, the Galois cohomology of the unitary groups is computed in precisely the same way as that of the orthogonal groups in Proposition 2.6. Namely, by using Lemma 2.8 instead of Lemma 2.2 we obtain the following result.

PROPOSITION 2.16. *The elements of $H^1(K, \mathbf{U}_m(D, f))$ are in one-to-one correspondence with the equivalence classes of m-dimensional nondegenerate forms over D having the same type as f. Moreover, the proper equivalence classes (i.e., equivalence relative to $SL_m(D)$) of those forms having the same discriminant as f are in one-to-one correspondence with the elements of*

$$\ker(H^1(K, \mathbf{SU}_m(D, f)) \to H^1(K, \mathbf{SL}_m(D)).$$

Instead of giving a proof of Proposition 2.16 in the spirit of Propositions 2.6–2.8, we point out that all of these assertions stem from the following general principle, based on (1.11) in §1.3.2: If X is a homogeneous K-space of an algebraic K-group G (i.e., there is a transitive K-defined action $G \times X \to X$), x is a point in X_K, and $H = G(x)$ is its stabilizer (so X can be identified with G/H), then the orbits of G_K on X_K are in one-to-one correspondence with the elements of $\ker(H^1(K, H) \to H^1(K, G))$.

2.3.4. Classical groups. Our goal is to establish the converse of Proposition 2.15, i.e., to show that, except for ${}^3D_4$ and ${}^6D_4$, and up to isogeny, any

simple K-group belonging to one of the classical types is either $\mathbf{SL}_m(D)$ or one of the unitary groups (in particular, the symplectic or orthogonal groups). First we consider inner forms of type A_{n-1}. We know that simply connected groups of this type are obtained from $G = \mathbf{SL}_n$ by twisting using cocycles from $H^1(K, \bar{G})$, where $\bar{G} = \mathbf{PSL}_n$. But $\bar{G}$ is also the group of automorphisms of the full matrix algebra M_n, and for any cocycle $a = \{a_\sigma\}$ in $H^1(K, \bar{G})$ we can consider the twisted algebra $A = {}_aM_n$. Let $B = A^{\mathrm{Gal}(\bar{K}/K)}$ be the set of fixed points. Then $B \otimes_K \bar{K} \simeq M_n(\bar{K})$, whence it follows that B is a simple algebra, and therefore $B = M_m(D)$ for some central skew field D over K of index d, where $md = n$. As in the definition of the special linear group, we consider the regular representation $\varrho: D \to M_{d^2}(K)$ and the corresponding representation $\psi: B \to M_{md^2}(K)$. We have a chain of isomorphisms

$$M_n(\bar{K}) \overset{\varphi}{\simeq} B \otimes_K \bar{K} \overset{\psi}{\simeq} \psi(B) \otimes_K \bar{K}.$$

Since ψ is a K-isomorphism, we have $(\psi\varphi)^{-1}(\psi\varphi)^\sigma = \varphi^{-1}\varphi^\sigma = a_\sigma$. On the other hand, since by definition $\mathrm{Nrd}_{B/K}(b) = \det(\varphi^{-1}(b))$ for b in B, the restriction of $\psi\varphi$ to $SL_n(\bar{K})$ carries $SL_n(\bar{K})$ isomorphically onto the group $\mathbf{SL}_n(D)$ defined in §2.2.1. Thus we obtain

PROPOSITION 2.17. *The simply connected groups pertaining to inner forms of type A_{n-1} are the groups $\mathbf{SL}_m(D)$, where D is a central skew field of index d over K and $n = md$.*

Next we take up outer forms of type A_{n-1}. These forms are obtained from $G = \mathbf{SL}_n$ by twisting using a cocycle $a = \{a_\sigma\}$ from $H^1(K, \operatorname{Aut} G)$ which does not lie in $H^1(K, \bar{G})$ and consequently has a nontrivial image in $H^1(K, \operatorname{Sym} R)$. But $\operatorname{Sym} R$ has order 2, for any root system R of type A_{n-1} $(n > 1)$; moreover $\alpha \mapsto -\alpha$ (where $\alpha \in R$) yields an automorphism of R which does not lie in $W(R)$. It follows that $\operatorname{Aut} G$ is generated by $\bar{G}$ and the automorphism of order 2 given by $x \mapsto {}^t x^{-1}$.

As before, let us realize $\operatorname{Aut} G$ as the automorphism group of some algebra A. Take $A = M_n(\bar{K}) \oplus M_n(\bar{K})$ with involution τ given by $\tau(X, Y) = ({}^tY, {}^tX)$, and consider the embedding $\mathbf{GL}_n \to A$ given by $X \to (X, {}^tX^{-1})$. We have seen that $\mathbf{GL}_n$ is thereby identified with $\mathbf{U} = \{Z \in A : Z\tau(Z) = E\}$; let $\mathbf{SU}$ denote the image of $\mathbf{SL}_n$ under this embedding. We claim that $\operatorname{Aut} G$ can be identified naturally with the group of all algebra automorphisms of A that commute with τ. Indeed it follows from the Skolem-Noether theorem that the group of automorphisms of A is generated by the inner automorphisms and the automorphism $(X, Y) \to (Y, X)$ which, clearly, commutes with τ, and one can easily see that each inner automorphism commuting with τ is induced by an element of $\mathbf{SU}$. It follows that by

restricting the automorphisms of A to $\mathbf{SU}$ we obtain all the automorphisms of $\mathbf{SU} \simeq G$; moreover each automorphism of A is uniquely determined by its restriction to $\mathbf{SU}$.

Now let $a = \{a_\sigma\} \in H^1(K, \mathrm{Aut}_{\bar{K}} G)$ be an arbitrary cocycle not lying in $H^1(K, \bar{G})$. Consider a as a cocycle in $H^1(K, \mathrm{Aut}_{\bar{K}} A)$ and construct the twisted algebra $B = {}_aA$. Since the a_σ commute with τ, B has an involution ν which commutes with the action of $\mathrm{Gal}(\bar{K}/K)$. Set $C = B^{\mathrm{Gal}(\bar{K}/K)}$. Then the restriction of ν to C induces an involution θ of C, and there exists an isomorphism of algebras with involution

$$(A, \tau) \overset{\varphi}{\sim} (C \otimes \bar{K}, \theta).$$

Let us describe the structure of C. Since $C \otimes \bar{K} \simeq M_n(\bar{K}) \oplus M_n(\bar{K})$, then C is either a direct sum of two central simple algebras over K or a central simple algebra over some quadratic extension L of K. We shall show that in our case the latter holds. Indeed, $Z(C) = {}_a(\bar{K} \oplus \bar{K})^{\mathrm{Gal}(\bar{K}/K)}$. By assumption the image of a in $H^1(K, \mathrm{Sym}\, R)$ is nontrivial, i.e., is a nontrivial homomorphism from $\mathrm{Gal}(L/K) = \mathrm{Gal}(\bar{K}/K)/\mathrm{Gal}(\bar{K}/L)$ to $\mathrm{Sym}\, R$ for some quadratic extension L/K. It is easy to see, then, that the action of $\mathrm{Gal}(\bar{K}/K)$ on ${}_a(\bar{K} \oplus \bar{K})$ coincides with the action of $\mathrm{Gal}(\bar{K}/K)$ on $L \otimes \bar{K}$ (via the second factor); hence $Z(C) = L$. Moreover, since τ acts on $\bar{K} \oplus \bar{K}$ by switching the components, the restriction of θ to L is nontrivial. Thus, C is a simple algebra over L with involution θ of the second kind.

Now it is well known (cf. Albert [1]), that $C = M_m(D)$ for some division algebra D over L of index d, $(md = n)$, provided with an involution ∂ of the second kind such that the restrictions of θ and ∂ to L coincide. Then, by Lemma 2.10, $\theta(x) = F^* x F^{-1}$ for x in $M_n(D)$, where $^*(x_{ij}) = (\partial(x_{ji}))$ and $^*F = F$. Consider the Hermitian form f on the space $V = D^m$ having matrix F with respect to the canonical base $e_1, \ldots, e_n$. We claim that ${}_aG \simeq \mathbf{SU}_m(D, f)$. Indeed consider the regular representation $\varrho: D \to M_{2d^2}(K)$ over K and the corresponding representation $\psi: C \to M_{2md^2}(K)$. We have a chain of isomorphisms

$$(A, \tau) \overset{\varphi}{\sim} (C \otimes_K \bar{K}, \theta) \overset{\psi}{\sim} (\psi(C) \otimes \bar{K}, \psi \circ \theta \circ \psi^{-1}).$$

Then $(\psi\varphi)^{-1}(\psi\varphi)^\sigma = a_\sigma$, since φ is defined over K. Thus $\psi\varphi$ and the above embedding $G \to A$ yield the $\bar{K}$-isomorphism ${}_aG \simeq SU_m(D, f)$, as desired. Thus we have

PROPOSITION 2.18. *The simply connected K-groups pertaining to outer forms of type ${}^2A_{n-1}$ are the groups $\mathbf{SU}_m(D, f)$, where D is a skew field of index $d = n/m$, with involution τ of the second kind, such that K is the fixed subfield under τ of the center of D, and f is a nondegenerate Hermitian form on D^m.*

Now we shall proceed to describe the K-forms of type C_n. Any simply connected split group of this type is $G = \mathbf{Sp}_{2n}(\bar{K}) = \{X \in GL_{2n}(\bar{K}) : {}^tXJX = J\}$, where J is defined in (2.18). Consider the involution τ of $A = M_{2n}(\bar{K})$ given by $\tau(X) = J^{-1}{}^tXJ$. (This involution is of the first kind of the second type.) Any automorphism of G is inner (cf. Theorem 2.8), so any form arising from G is obtained by twisting using a cocycle $a = \{a_\sigma\} \in H^1(K, \bar{G})$. Clearly a_σ can be regarded as an automorphism of A that commutes with the action of τ. Then, as above, we conclude that the twisted algebra $B = {}_aA$ has involution ν which commutes with the action of $\mathrm{Gal}(\bar{K}/K)$, and therefore the restriction to $C = B^{\mathrm{Gal}(\bar{K}/K)}$ induces an involution θ of the latter. We have an isomorphism of algebras with involution

$$(A, \tau) \simeq (C \otimes_K \bar{K}, \theta).$$

Since C is simple over K, we have $C = M_n(D)$ for some central skew field of index $d = \frac{2n}{m}$ over K, having involution of the first kind. (cf. Albert [1]).

Note that the last assertion is a straightforward consequence of the following fact: an algebra E over K has an involution of the first kind if and only if it is isomorphic to its opposite algebra E^0, in particular a simple algebra has an involution of the first kind if and only if it represents an element of order 2 in the Brauer group. In our case C has involution of the first kind; consequently C, and D as well, represents an element of order 2 in the Brauer group, implying that D has an involution of the first kind, to be denoted by ∂. We may assume ∂ to be either of the first or of the second type, as we wish (indeed, if, say, ∂ is of the first type, then ∂', given by $\partial'(x) = c\partial(x)c^{-1}$ where c is an arbitrary invertible ∂-skew symmetric element, is of the second type; also, $x \mapsto cx$ gives a bijection between the ∂-symmetric and ∂'-skew-symmetric elements of D). Then Lemma 2.10 yields $\theta(x) = F^* x F^{-1}$, where $^*(x_{ij}) = (\partial(x_{ji}))$, $^*F = -F$ if ∂ is of the first type, and $^*F = F$ if ∂ is of the second type. Now, introducing, respectively, a skew Hermitian or Hermitian form f on $V = D^m$ having matrix F, and arguing as above, we obtain ${}_aG = \mathbf{SU}_m(D, f)$. Thus, we may assert

PROPOSITION 2.19. *The simply connected K-forms of type C_n are precisely the groups $\mathbf{SU}_m(D, f)$, where D is a central skew field of index $d = \frac{2n}{m}$ over K endowed with involution τ of the first kind, and f is a nondegenerate sesquilinear form which is Hermitian if τ is of the second type, and skew Hermitian if τ is of the first type.*

Lastly, we consider K-forms of type B_n and D_n, other than ${}^3D_4$ and ${}^6D_4$. A simply connected K-split group of this type is the spin group $\bar{G} = \mathrm{Spin}_m(f)$, where f is a quadratic form of maximal Witt index over K (whose matrix Q coincides with either Q_1 or Q_2 in (2.19), depending on

whether m is even or odd). However, it will be easier for us to work with the corresponding orthogonal group $G = \mathbf{SO}_m(f)$. Let $\pi: \tilde{G} \to G$ denote the universal covering.

Let us see how $\operatorname{Aut} G$ and $\operatorname{Aut} \tilde{G}$ are related. It is well known (cf. §2.1, Theorem 2.8) that $\operatorname{Aut} G$ can be identified with the subgroup of $\operatorname{Aut} \tilde{G}$ fixing $\ker \pi$. If G has type B_n, then $\ker \pi = Z(G)$, from which it follows that $\operatorname{Aut} G$ and $\operatorname{Aut} \tilde{G}$ coincide. (This also follows from the fact that the Dynkin diagram of the root system of type B_n has no nontrivial symmetries, and therefore all its automorphisms are inner).

Now suppose G belongs to type D_n, i.e., m is even. In this case there is an outer automorphism of G, induced by conjugation by a matrix from $\mathbf{O}_m(f) \setminus \mathbf{SO}_m(f)$, so $[\operatorname{Aut} G : \operatorname{Int} G] \geq 2$. On the other hand, if $n \neq 4$, then the corresponding Dynkin diagram has exactly two symmetries, so $[\operatorname{Aut} \tilde{G} : \operatorname{Int} \tilde{G}] = 2$. Thus, in this case, too, $\operatorname{Aut} G = \operatorname{Aut} \tilde{G}$; moreover all the automorphisms of G are obtained from conjugation by the elements of $\mathbf{O}_m(f)$. In the remaining case, $n = 4$, the group of symmetries of the Dynkin diagram is isomorphic to the symmetric group S_3. Then, considering the action of S_3 on the center of $\tilde{G}$, it is easy to show that $\operatorname{Aut} G$ is isomorphic to a subgroup of index 3 in $\operatorname{Aut} \tilde{G}$, and all such subgroups are conjugate in $\operatorname{Aut} \tilde{G}$. So, again all the automorphisms of G are induced by conjugation by elements of $\mathbf{O}_m(f)$.

It follows from this discussion of $\operatorname{Aut} G$ and $\operatorname{Aut} \tilde{G}$ that if a K-form H of $\tilde{G}$ is of type other than ${}^3D_4$ and ${}^6D_4$, then H is obtained from $\tilde{G}$ by twisting using a cocycle $a = (a_\sigma) \in H^1(K, \operatorname{Aut} G)$. In this case $H = {}_a\tilde{G}$ is a universal covering of ${}_aG$. Thus it suffices to describe the K-forms for G. Repeating verbatim the argument used to describe K-forms of type C_n, we conclude that ${}_aG$ is $\mathbf{SU}_l(D, f)$, where D is a finite-dimensional central skew field of index $d = m/l$ over K with involution τ of the first kind, and f is a nondegenerate Hermitian (resp. skew Hermitian) form on $V = D^l$ depending on whether τ has first (resp. second) type. Now, for groups of type B_n, on the one hand m must be odd, but on the other, d must be a power of 2, since D has exponent 2 in $\operatorname{Br}(K)$. Therefore $d = 1$, i.e., $D = K$, $\tau = \mathrm{id}$ and f is an ordinary quadratic form.

PROPOSITION 2.20.

(1) *The simply connected K-forms of type B_n are the spin groups of nondegenerate quadratic forms over K of degree $m = 2n + 1$.*
(2) *The simply connected K-forms of type D_n, other than ${}^3D_4$ and ${}^6D_4$, are the universal coverings of the special unitary groups $\mathbf{SU}_l(D, f)$, where D is a finite-dimensional central skew field of index $d = \frac{2n}{l}$ over K with involution τ of the first kind, and f is a nondegenerate form which is Hermitian if τ is of the first type, and skew-Hermitian if τ is of the second type. (For $d = 1$ and $\tau = \mathrm{id}$ we obtain the spin groups $\operatorname{Spin}_{2n}(f)$ of nondegenerate quadratic forms).*

When K is a local field or an algebraic number field, the above results can be made considerably more precise. It is well known (cf. Albert [1, Theorem 10.22]) that over a local field there is no skew field of index $d > 1$ having an involution of the second kind. Therefore, in this case the simply connected K-groups of type ${}^2A_{n-1}$ are just the special unitary groups $\mathbf{SU}_n(L, f)$, where L is a quadratic extension of K and f is a nondegenerate form on $V = L^n$, Hermitian relative to the nontrivial automorphism $\sigma \in \operatorname{Gal}(L/K)$. Taking an orthogonal base $e_1, \ldots, e_n$ of V we can write f as

$$f(x_1, \ldots, x_n; y_1, \ldots, y_n) = a_1\sigma(x_1)y_1 + \cdots + a_n\sigma(x_n)y_n,$$

where the coefficients a_i satisfy $\sigma(a_i) = a_i$, i.e., $a_i \in K$. In particular, writing $f(x) = f(x, x)$ for the sake of brevity, we have

$$f(x_1, \ldots, x_n) = a_1 N_{L/K}(x_1) + \cdots + a_n N_{L/K}(x_n).$$

Furthermore, it is well known (cf. §§1.4–1.5) that over local fields and algebraic number fields the exponent of a simple algebra in the Brauer group equals its index; therefore skew fields with an involution of the first kind are quaternion skew fields. Any quaternion skew field D over K has a canonical involution τ, given with respect to the standard base 1, i, j, k of D by $\tau(a_0 + a_1 i + a_2 j + a_3 k) = a_0 - a_1 i - a_2 j - a_3 k$ (cf. Pierce [1]). In our terminology, this involution belongs to the second type, and moreover the set of symmetric elements coincides with the center K of D. Hence any τ-Hermitian form f on $V = D^m$ can be written with respect to an orthogonal base of V as

$$f(x_1, \ldots, x_n; y_1, \ldots, y_n) = \tau(x_1)a_1 y_1 + \cdots + \tau(x_n)a_n y_n. \tag{2.22}$$

The a_i here have to satisfy $\tau(a_i) = a_i$, hence $a_i \in K$. Therefore

$$f(x_1, \ldots, x_n) = a_1 \operatorname{Nrd}_{D/K}(x_1) + \cdots + a_n \operatorname{Nrd}_{D/K}(x_n).$$

Thus any simply connected K-group of type C_n (where K is either a local field or an algebraic number field) is a special unitary group $\mathbf{SU}_n(D, f)$, corresponding to a bilinear form f as in (2.22).

Lastly, simply connected K-groups of type D_n that are not isomorphic to spin groups of quadratic forms are universal coverings of unitary groups $\mathbf{SU}_n(D, f)$, where D is a quaternion skew field over K with the canonical involution τ and f is a nondegenerate skew Hermitian form on D^n.

To summarize, for convenience of reference we list the classical simply connected simple algebraic K-groups for the case where K is either a local field or an algebraic number field. First of all, we have the groups $G = \mathbf{SL}_m(D)$, where D is a central skew field over K of index d, that are inner forms of the type A_n, $n = md - 1$. All the remaining groups, with the exceptions of ${}^3D_4$ and ${}^6D_4$, are obtained from the special unitary groups $\mathbf{SU}_m(D, f)$. To be more precise, any simply connected K-group G of such a type is the universal covering of some special unitary group $H = \mathbf{SU}_m(D, f)$, where D is a skew field of index d and center L, with an involution τ such that $L^\tau = K$, and f is a nondegenerate Hermitian or skew Hermitian form (relative to τ) on an m-dimensional space W over D. We have the following possibilities for D, τ and f, in the list of which we shall introduce a number m_0 which comes up in the further study of classical groups:

(1) $[L : K] = 2$, i.e., τ is an involution of the second kind, and f is Hermitian. In this case $G = H$ is of type ${}^2A_n$, where $n = md - 1$ $(m_0 = 2)$.

In the remaining cases $L = K$, i.e., τ is an involution of the first kind. Then D either coincides with K or is a quaternion skew field over K, and the list of classical groups continues as follows:

(2) $D = K$ and f is symmetric. Then $H = \mathbf{SO}_m(f)$ and $G = \mathrm{Spin}_m(f)$; moreover these groups have type $B_{\frac{m-1}{2}}$ for m odd and type $D_{\frac{m}{2}}$ for m even $(m_0 = 4)$.
(3) $D = K$ and f is alternating. Then m is even and $G = H$ is $\mathbf{Sp}_m(f)$, which has type $C_{\frac{m}{2}}$ $(m_0 = 2)$.
(4) D is a quaternion skew field over K, τ is its canonical involution, and f is Hermitian. Then $G = H$ has type C_m $(m_0 = 1)$.
(5) For D and τ as in (4), f is skew Hermitian. Then H is a non-simply connected group of type D_m and $H \simeq \mathbf{SO}_{2m}(\tilde{f})$ over $\bar{K}$ $(m_0 = 3)$.

2.3.5. Witt's Theorem. We keep the notation G, H, f, W, ... introduced above. H acts on $\bar{W} = W \otimes_K \bar{K}$, respecting the natural extension of f. This realization of H induces a realization of G, which we shall use freely without further explication, calling m the degree of G. Below we shall need Witt's Theorem, which describes the orbits of the action of $U_m(D, f)$ on W (relative version) and the orbits of G on $\bar{W}$ (absolute version).

THEOREM 2.10 (WITT'S THEOREM, RELATIVE VERSION). *Let a, $b \in W$ be two nonzero vectors such that $f(a) = f(b)$. Then there exists an element g in $U_m(D, f)$ such that $b = ga$.*

For the proof, see Bourbaki [1, Ch. 9, pp. 396–398]. Note that Witt's Theorem is actually taken to be a more general assertion that any metric isomorphism $\sigma: U_1 \to U_2$ between two subspaces $U_1, U_2 \in W$ extends to an isometry of the entire space W, i.e., is induced by an element of $U_m(D, f)$.

Except for (3) in the above list, there always exists a base of W which is orthogonal with respect to f. In particular, there always exists a vector a in W such that $f(a) \neq 0$ (anisotropic vector).

THEOREM 2.11 (WITT'S THEOREM, ABSOLUTE VERSION). *Let $m \geq 2$ and let a in W be an anisotropic vector. Then for any b in $\bar{W}$ such that $f(b) = f(a)$, there is g in G satisfying $b = ga$.*

PROOF: It suffices to find h in H satisfying $b = ha$. In case (2) the existence of h follows immediately from Theorem 2.10, applied to $\bar{W}$ over $\bar{K}$, and the assumption that $m \geq 2$. Now, let us consider the cases (4) and (5). For this we include a in an orthogonal base $e_1 = a, e_2, \ldots, e_m$ of W and in what follows we shall consider coordinates relative to this base. If $f(e_i) = d_i$, then with respect to this base f can be written as

$$f(x_1, \ldots, x_m) = \tau(x_1)d_1x_1 + \cdots + \tau(x_m)d_mx_m.$$

Next, we choose a skew-symmetric element c in D^*, and pass from τ to σ defined by $\sigma(d) = c\tau(d)c^{-1}$. Then σ is of first type and therefore we can choose an isomorphism $\bar{D} = D \otimes_K \bar{K} \xrightarrow{\sim} M_2(\bar{K})$ in such a way that σ goes over to the matrix transpose. It is easy to see that $\tau(d) = \pm d$ is equivalent to $\sigma(cd) = \mp cd$, for d in D. Therefore the elements cd_i correspond to symmetric (in case (5)) or skew-symmetric (in case (4)) matrices $D_i \in GL_2(\bar{K})$. If $b = (b_1, \ldots, b_m)$, and $b_i \in \bar{D}$ correspond to matrices $B_i \in M_2(\bar{K})$, then

$$ {}^tB_1D_1B_1 + \cdots + {}^tB_mD_mB_m = D_1. \tag{2.23}$$

We know that under the isomorphism $\bar{D} \simeq M_2(\bar{K})$, H goes over respectively to $\tilde{H} = \mathbf{SO}_{2m}(\tilde{f})$ or $\tilde{H} = \mathbf{Sp}_{2m}(\tilde{f})$, where the matrix of $\tilde{f}$ has the form $\mathrm{diag}(D_1, \ldots, D_m)$. Let

$$B_i = \begin{pmatrix} b_{11}^{(i)} & b_{12}^{(i)} \\ b_{21}^{(i)} & b_{22}^{(i)} \end{pmatrix}.$$

Then, it follows from (2.23) that the subspace generated by the vectors $u_1 = (1, 0, \ldots, 0)$ and $u_2 = (0, 1, 0, \ldots, 0)$ in $\bar{K}^{2m}$ is isometric (relative to $\tilde{f}$) to the subspace generated by the vectors $w_1 = (b_{11}^{(1)}, b_{21}^{(1)}, \ldots, b_{11}^{(m)}, b_{21}^{(m)})$ and $w_2 = (b_{12}^{(1)}, b_{22}^{(1)}, \ldots, b_{12}^{(m)}, b_{22}^{(m)})$. Therefore, by Witt's Theorem for

subspaces, it follows that there exists $\tilde{h}$ in $\tilde{H}$ such that $\tilde{h}(u_i) = w_i$ for $i = 1, 2$, or in matrix notation $\tilde{h}(E_2, 0, \dots, 0) = (B_1, \dots, B_m)$. The latter means that the element $h \in H$ corresponding to $\tilde{h}$ satisfies $ha = b$, as required.

For case (1) the argument is analogous but of a somewhat different nature. Again, let $e_1 = a, e_2, \dots, e_m$ be an orthogonal base of W, and $f(e_i) = d_i$, so $f(x_1, \dots, x_m) = \tau(x_1)d_1x_1 + \cdots + \tau(x_m)d_mx_m$. Let us choose the isomorphism $D \otimes_K \bar{K} \simeq M_d(\bar{K}) \oplus M_d(\bar{K})$ in such a way as to have the involution $(X, Y) \to ({}^tY, {}^tX)$ (cf. §2.3.3) corresponding to τ (which we also are going to denote by τ). Let $d_i = (C_i, {}^tC_i)$, $b = (b_1, \dots, b_m)$ and $b_i = (B_i^{(1)}, B_i^{(2)})$. Then $f(b) = f(a)$ can be written as one of the two equivalent matrix equations

$$\begin{aligned} {}^tB_1^{(1)}C_1B_1^{(2)} + \cdots + {}^tB_m^{(1)}C_mB_m^{(2)} &= C_1 \\ {}^tB_1^{(2)}{}^tC_1B_1^{(1)} + \cdots + {}^tB_m^{(2)}{}^tC_mB_m^{(1)} &= {}^tC_1. \end{aligned} \tag{2.24}$$

Furthermore, H corresponds to

$$\tilde{H} = \{\, (X, {}^tC^{-1}\,{}^tX^{-1}\,{}^tC) : X \in SL_n(\bar{K}) \,\},$$

where $n = md$, $C = \mathrm{diag}(C_1, \dots, C_m)$, and $M_m(M_d(\bar{K}))$ is viewed as $M_n(\bar{K})$. Therefore we need to show that if $B_i^{(1)}$, $B_i^{(2)}$ satisfy (2.24), then there is $X \in SL_n(\bar{K})$ satisfying

$$\begin{aligned} X\begin{pmatrix} E_d \\ 0 \\ \vdots \\ 0 \end{pmatrix} &= \begin{pmatrix} B_1^{(1)} \\ \vdots \\ B_m^{(1)} \end{pmatrix} \\ ({}^tC^{-1}\,{}^tX^{-1}\,{}^tC)\begin{pmatrix} E_d \\ 0 \\ \vdots \\ 0 \end{pmatrix} &= \begin{pmatrix} B_1^{(2)} \\ \vdots \\ B_m^{(2)} \end{pmatrix}. \end{aligned} \tag{2.25}$$

The second equation in (2.25) can be rewritten as

$${}^tX\begin{pmatrix} {}^tC_1B_1^{(2)} \\ \vdots \\ {}^tC_mB_m^{(2)} \end{pmatrix} = \begin{pmatrix} {}^tC_1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}. \tag{2.26}$$

The first equation in (2.25) is satisfied exactly by the matrices of the form

$$X = \begin{pmatrix} B_1^{(1)} & X_{12} & \dots & X_{1m} \\ \dots\dots & \dots\dots & \dots\dots & \dots\dots \\ B_m^{(1)} & X_{m2} & \dots & X_{mm} \end{pmatrix}$$

with arbitrary X_{ij}, $2 \le i \le m$, $1 \le j \le m$. In view of (2.24) we see that such a matrix satisfies (2.26) if and only if

$$X_{1i}{}^tC_1B_1^{(2)} + \cdots + X_{mi}{}^tC_mB_m^{(2)} = 0, \quad i = 2, \dots, m. \tag{2.27}$$

In view of the fact that (2.27) actually reduces to m linear equations on each column of X beginning with the $(m+1)$-th, it is easy to see that there is a solution of (2.27) satisfying

$$\mathrm{rank}\begin{pmatrix} X_{12} & \dots & X_{1m} \\ \dots\dots & \dots\dots & \dots\dots \\ X_{m2} & \dots & X_{mm} \end{pmatrix} = n - m.$$

Since C_1 is nondegenerate, then X is also nondegenerate. Moreover, since (2.27) are homogeneous and $m \ge 2$ we may actually find $X \in SL_n(\bar{K})$. Q.E.D.

REMARK: Since $\mathbf{U}_m(D, f) = \mathbf{SU}_m(D, f)$ in case (4) for all $m \ge 1$, Theorem 2.11 also holds in this case for $m = 1$.

Thus, in all the cases we have examined, the "sphere" $X_{(f,a)} = \{\, x \in \bar{W} : f(x) = f(a) \,\}$ is a homogeneous G-space, and therefore may be identified with $G/G(a)$ where $G(a)$ is the stabilizer of a. Below we shall need some information on the stabilizers $G(a)$ and $G(a, b)$ of vectors $a \in W$ and of pairs of vectors $a, b \in W$.

PROPOSITION 2.21. *If $m \ge m_0$ then for any anisotropic vector a in W the stabilizer $G(a)$ is of the same type as G and is a simply connected semisimple group (not excluding the case $G(a) = (e)$). Consequently, if $m \ge m_0 + 1$ then the same conclusion holds for the stabilizer $G(a, b)$ of an arbitrary pair of vectors a, b spanning a nondegenerate 2-dimensional subspace.*

PROOF: It is easy to see that for any anisotropic a in W the stabilizer $H(a)$ is $\mathbf{SU}_{m-1}(D, g)$, where g is the restriction of f to the orthogonal complement of a. On the other hand, $G(a)$ is the pre-image of $H(a)$ under the projection $\pi: G \to H$. From the above review of classical groups it follows that $H(a)$ is semisimple under our condition on m; thus it remains to be shown that $\pi\,|_{G(a)}: G(a) \to H(a)$ is a universal covering. This is obvious

for the classical groups listed in (1) and (4) of §2.3.4, since here H and $H(a)$ are simply connected (recall that we are excluding (3)). For the remaining cases, (2) and (5), it follows from the compatibility of the universal coverings of special orthogonal groups for spaces and subspaces provided by the corresponding spin groups (cf. §2.3.2). The second assertion of Proposition 2.21, regarding stabilizers of vector pairs, follows immediately from the first. Q.E.D.

2.4. Some results from algebraic geometry.

Most of the varieties that we shall work with are either affine or projective, i.e., biregularly isomorphic to a closed subset respectively of n-dimensional affine space $\mathbb{A}^n$ or n-dimensional projective space $\mathbb{P}^n$. We shall assume familiarity with standard concepts ranging from regular and rational functions on a variety, regular and rational maps of varieties, etc., to the concept of dimension (cf. Shafarevich [1], Hartshorne [1], and Borel [8, Ch. AG]). Some more specialized material will be presented below.

2.4.1. The field of definition of an algebraic variety. (Borel [8, Ch. AG, §§11–14].) Let K be a subfield of the universal domain Ω. A closed subvariety $X \subset \mathbb{A}^n$ is said to be *defined over* K if the ideal $\mathfrak{a} \subset \Omega[x_1, \dots, x_n]$ of polynomials vanishing on X is generated by $\mathfrak{a} \cap K[x_1, \dots, x_n]$, where x_i is the standard coordinate function on $\mathbb{A}^n$. A regular (respectively, rational) map $f: X \to Y$ of two K-subvarieties $X \subset \mathbb{A}^n$, $Y \subset \mathbb{A}^n$ is defined over K if there exist polynomials $f_i \in K[x_1, \dots, x_n]$ (respectively, rational functions $f_i \in K(x_1, \dots, x_n)$) for $i = 1, \dots, m$, such that $f(x) = (f_1(x), \dots, f_m(x))$ for all x in X. For a perfect field K the following Galois criterion for being K-defined is known: a closed subvariety $X \subset \mathbb{A}^n$ is defined over K if and only if X is defined over $\bar{K}$ and $X = X^\sigma$ for all σ in $\mathrm{Gal}(\bar{K}/K)$, where X^σ is defined by the ideal $(\mathfrak{a} \cap \bar{K}[x_1, \dots, x_n])^\sigma$ of $\bar{K}[x_1, \dots, x_n]$. An analogous assertion holds for arbitrary varieties and regular (rational) maps.

2.4.2. Dominant morphisms. A morphism $\varphi: X \to Y$ is said to be *dominant* if $\varphi(X)$ is dense in Y in the Zariski topology. For such morphisms, we have

THEOREM 2.12 (DIMENSION OF THE FIBERS OF A MORPHISM). *Suppose $\varphi: X \to Y$ is a dominant morphism of irreducible algebraic varieties, and let $r = \dim X - \dim Y$. Then*

(1) *for any point $y \in \varphi(X)$ we have $\dim \varphi^{-1}(y) \geq r$;*
(2) *$\{y \in Y : \dim \varphi^{-1}(y) = r\}$ is a nonempty open set.*

PROOF: cf. Shafarevich [1, Ch. 1, §6].

2.4.3. Tangent spaces. Simple and singular points. (Shafarevich [1, Ch. 2].) These concepts are of a local nature, i.e., they are independent of whether they are considered with respect to some variety X or with respect to some neighborhood of a given point in X. Therefore, instead of X we may consider an affine neighborhood of a fixed point x in X, and thus we may assume X to be affine. Let $X \subset \mathbb{A}^n$ and let $\mathfrak{a} \subset \Omega[x_1, \dots, x_n]$ be the ideal of all polynomials vanishing on X. For an arbitrary polynomial $f(x_1, \dots, x_n) \in \Omega[x_1, \dots, x_n]$ and a point x in $\mathbb{A}^n$ we let $d_x f(X_1, \dots, X_n)$ denote the linear form $\sum_{i=1}^n \frac{\partial f}{\partial x_i}(x) X_i$, where X_i $(i = 1, \dots, n)$ are the coordinates in the n-dimensional vector space associated with $\mathbb{A}^n$. The *tangent space* of X at a point x in X is the subspace $T_x(X)$ of the n-dimensional vector space, given by

$$d_x f(X_1, \dots, X_n) = 0, \quad f \in \mathfrak{a}. \tag{2.28}$$

By Hilbert's basis theorem, $\mathfrak{a}$ is generated by a finite number of polynomials $f_1, \dots, f_r$; so instead of (2.28) we may consider the equivalent system

$$d_x f_i(X_1, \dots, X_n) = 0, \quad i = 1, \dots, r. \tag{2.29}$$

Now if X is defined over K and $x \in X_K$, then choosing the f_i to be elements of $\mathfrak{a}$ with coefficients from K, we see that $T_x(X)$ is also defined over K. A regular map $\varphi: X \to Y$ of algebraic varieties for any point x in X induces the linear map $d_x\varphi: T_x(X) \to T_{\varphi(x)}(Y)$ of the corresponding tangent spaces, called the *differential* of φ at x; moreover $d_x\varphi$ is defined over K if φ is defined over K and $x \in X_K$.

In (2.28) and (2.29) x was fixed. If we let x run through all of X, i.e., if we consider the set of all points (x, t) in $\mathbb{A}^n \times \mathbb{A}^n$ such that $x \in X$ and $t \in T_x(X)$, then we obtain the *tangent bundle* $T(X)$ of X. (2.29) shows that $T(X)$ is a variety. Assuming X to be irreducible, and applying Theorem 2.12 to the canonical projection $T(X) \to X$, we see that $\dim T_x(X)$ has a constant value, say d, for all points x of some Zariski-open subset $U \subset X$, and moreover $\dim T_x(X) \geq d$ for any point x in X. Furthermore, d turns out to be $\dim X$. Thus $\dim T_x(X) \geq \dim X$ for all x in X, and the points for which the equality is achieved (called *simple* (or non-singular) *points* while the other points are called *singular*) form a nonempty Zariski variety.

For reducible X, a point x in X is simple if it lies on a single irreducible component $Y \subset X$ and is simple on Y.

PROPOSITION 2.22. *A point x of the variety $X \subset \mathbb{A}^n$ is simple if and only if there are polynomials $f_1, \dots, f_r \in \Omega[x_1, \dots, x_n]$, where $r = n - \dim_x X$, and a Zariski-open subset $U \subset \mathbb{A}^n$ such that $x \in Y = \{y \in U : f_i(y) = 0, i = 1, \dots, r\} \subset X$ and the Jacobian*

$$\left(\frac{\partial f_i}{\partial x_j}(x)\right)_{\substack{i=1,\dots,r \\ j=1,\dots,n}}$$

has rank r. If X is defined over K and x is a simple point belonging to X_K, then $f_1, \dots, f_r$ can be chosen to have coefficients in K.

Varieties whose points are all simple are called *smooth*. Since simple points always exist, any homogeneous variety is smooth. In particular, the variety of an arbitrary algebraic group is smooth.

2.4.4. Birational isomorphisms. A rational map $\varphi: X \to Y$ of irreducible varieties is called a *birational isomorphism* if there exists an inverse rational map $\varphi^{-1}: Y \to X$. In this case φ induces a biregular isomorphism of Zariski-open sets $U \subset X$, $V \subset Y$. Varieties that are birationally isomorphic to an affine space are said to be *rational*. A dominant morphism $\varphi: X \to Y$ is a birational isomorphism if its comorphism φ^* induces an isomorphism of the rational function fields $\Omega(X)$ and $\Omega(Y)$. In particular, X is rational if and only if the rational function field $\Omega(X)$ is a purely transcendental extension of Ω. Note that all the definitions and properties listed have obvious analogs for K-varieties.

There is one useful sufficient condition for a dominant morphism $\varphi: X \to Y$ to be a birational isomorphism. To formulate this condition, recall that φ is said to be *separable* if the comorphism φ^* defines a separable field extension $\Omega(X)/\varphi^*\Omega(Y)$ (naturally, the condition of separability is automatically satisfied for char $= 0$).

THEOREM 2.13. *Let $\varphi: X \to Y$ be an injective dominant separable morphism of irreducible varieties. Then φ is a birational isomorphism. If, moreover, φ is a K-morphism of K-varieties, then it is a K-birational isomorphism.*

PROOF: cf. Humphreys [1, Ch. 1, §4.6].

It follows from Theorem 2.13 that to prove that a certain variety X is K-rational it suffices to construct an injective dominant separable K-morphism $\varphi: U \to X$ from some open subset $U \subset \mathbb{A}^n$.

A K-variety X for which there exists a dominant K-morphism $\varphi: U \to X$ from a Zariski-open subset $U \subset \mathbb{A}^n$ is called *unirational*. The question of whether every unirational variety is rational is known as Lüroth's problem. The answer to Lüroth's problem for the relative case (i.e., over a non-closed base field) as well as the absolute case is known now to be negative. The variety of a connected (linear) algebraic K-group G is always unirational over K if either K is perfect or G is reductive (cf. Borel [8, §18]), from which, in particular, the proof of Theorem 2.2 follows. Thus, the question of whether varieties of algebraic K-groups are K-rational is similar to the relative version of Lüroth's problem (for a discussion of this question, cf. §7.3).

The following theorem illustrates the extent to which birational morphisms can differ from biregular morphisms.

THEOREM 2.14. *Let $\varphi: X \to Y$ be a regular map and a birational isomorphism of irreducible varieties, and let $x \in X$. Assume that $y = \varphi(x)$ is a simple point of Y. If the inverse rational map $\psi = \varphi^{-1}$ is not regular at y, then $\dim \varphi^{-1}(y) \geq 1$.*

PROOF: cf. Shafarevich [1, Ch. 2, §4].

From Theorems 2.13 and 2.14 it follows that if $\varphi: X \to Y$ is a bijective regular morphism of irreducible varieties in characteristic zero and Y is a smooth variety, then φ is a biregular isomorphism.

2.4.5. Actions of algebraic groups on varieties. An algebraic group G is said to *act* on an algebraic variety X if there is a morphism $\mu: G \times X \to X$ such that

(1) $\mu(e, x) = x$,
(2) $\mu(gh, x) = \mu(g, \mu(h, x))$.

(We have given the definition of a *left* action. Sometimes, however, it is useful to consider a *right* action $\mu: X \times G \to X$ satisfying $\mu(x, e) = x$ and $\mu(x, gh) = \mu(\mu(x, g), h)$. To shorten the notation, $\mu(g, x)$ is usually written as gx. The action is *defined* over K if G, X and μ are defined over K.

Of the general results on the action of algebraic groups, we shall need only the Closed Orbit Lemma (cf. Borel [8, §1.8]).

PROPOSITION 2.23. *Let G be an algebraic group acting on a variety X. Then each orbit is a smooth variety which is open in its closure in X. Its boundary is a union of orbits of strictly lower dimension. In particular, the orbits of minimal dimension are closed.*

A variety X is a *homogeneous G-space* if there exists a transitive action $G \times X \to X$. Fixing a point x in X, we then have a bijection $G/G(x) \leftrightarrow X$ from the left cosets modulo the stabilizer $G(x)$ to the points of X, which can be used to endow $G/G(x)$ with the structure of an algebraic variety. (Note: it follows from the smoothness of the homogeneous space and the results of §2.4.3 that this structure is uniquely defined, at least for characteristic 0.)

One may ask whether for any (closed) subgroup $H \subset G$ there is some action of G on a suitable algebraic variety X and some point x in X such that $G(x) = H$. The affirmative answer follows from *Chevalley's theorem* (cf. Borel [8, §5.1]; Humphreys [1]): Let G be an arbitrary K-group, H a closed K-subgroup; then there exists a faithful K-representation $\varrho: G \to GL(V)$ and a one-dimensional K-subspace $D \subset V$ such that $H = \{g \in G : gD = D\}$. Then, considering the induced action of G on

the projective space $\mathbb{P}(V)$ and a point x in $\mathbb{P}(V)$ corresponding to D, we obtain a geometric realization of G/H as the orbit Gx, which is a quasiprojective variety, i.e., an open subset of some projective variety. To develop the theory presented in Chapters 4 and 5 we shall need the following result, elaborating Chevalley's theorem (cf. Borel [6, §7]).

THEOREM 2.15 (A STRONGER VERSION OF CHEVALLEY'S THEOREM). *Let G be a connected algebraic group and H a reductive subgroup, both defined over a field K of characteristic 0. Then there exists a K-representation $\varrho: G \to GL(V)$ and a vector x in V_K such that $G(x) = H$ and Gx is closed in V.*

Since this result is not as widely known as Chevalley's theorem, let us sketch its proof. We consider the action of H on G by left translation and the associated representation of H in $\bar{K}[G]$. It is well known that this representation is locally finite, and the classical argument of Nagata [1] from the theory of invariants of reductive groups shows that $A = \bar{K}[G]^H$ is finitely generated and separates the disjoint closed H-invariant subsets of G (in particular, distinct left cosets). Proceeding from these results, we choose a finite set of generators $x_1, \dots, x_r$ of A_K, and let V_i denote a finite-dimensional G-invariant K-subspace in A containing x_i. We shall show that the natural representation in $V = \bigoplus_{i=1}^r V_i$ and the point $x = (x_1, \dots, x_r)$ in V_K will do. Indeed, by our construction $x_i \in A = \bar{K}[G]^H$, whence $G(x) \supset H$. On the other hand, if $gx = x$, then in particular $x_i(g) = x_i(e)$. But since the functions x_i generate A, they must separate distinct cosets; hence $gH = H$ and $g \in H$. It remains to be shown that the orbit of Gx is closed. Put $X = \overline{Gx}$ and consider the comorphism $\eta: \bar{K}[X] \to \bar{K}[G]$, for the morphism $G \to X$ given by $g \mapsto gx$. It follows from our construction that η induces an isomorphism of $\bar{K}[X]$ and A. Moreover, using the bijection from the points of an affine variety to the maximal ideals of the coordinate ring, it is easy to show that the fact that $X = Gx$ is equivalent to the following assertion: $\mathfrak{m}\bar{K}[G]$ is proper for any proper maximal ideal $\mathfrak{m}$ of A. But since H is reductive, there exists an A-linear projection $\bar{K}[G] \to A$; so $\mathfrak{m}\bar{K}[G] = \bar{K}[G]$ would imply that $\mathfrak{m}A = A$, a contradiction.

In applying Theorem 2.15 in Chapters 4 and 5, we shall replace ϱ by the corresponding right representation ϱ^*, given by $\varrho^*(g) = \varrho(g^{-1})$ and shall write the action as $x\varrho^*(g)$; then $x\varrho^*(gh) = (x\varrho^*(g))\varrho^*(h)$.

In proving several results of the arithmetic theory of algebraic groups we shall use a series of concrete varieties, whose construction and whose properties we shall now describe.

2.4.6. Multidimensional conjugacy classes. The orbits of the adjoint action of $G \times G \to G$ given by $(g, h) \mapsto ghg^{-1}$ are the *conjugacy classes* of G. The following fact is well known (cf. Seminar on algebraic groups, p. 191):

The conjugacy class of an element h in the reductive group G is closed if and only if h is semisimple.

Analogously, one can consider the adjoint action of G on the Cartesian product G^d, given by $(g, (h_1, \dots, h_d)) \mapsto (gh_1g^{-1}, \dots, gh_dg^{-1})$. It is natural to call the orbits arising in this way *multidimensional conjugacy classes.* We shall need a certain sufficient condition for a multidimensional conjugacy class to be closed. We shall say that $H \subset G$ (not necessarily closed) is *reduced* if for some faithful representation $\varrho: G \to GL_n(\Omega)$ the image of H is a completely reducible linear group.

THEOREM 2.16. *Let G be a reductive group and let $h_1, \dots, h_d \in G$ generate a reduced subgroup. Then the multidimensional conjugacy class of $(h_1, \dots, h_d)$ over G is closed in G^d.*

PROOF: First we consider the special case where $G = GL_n(\Omega)$ and $H \subset G$, generated by $h_1, \dots, h_d$, is completely reducible. Then the Ω-hull of H, i.e., the subalgebra in $M_n(\Omega)$ generated by H, which we shall denote by A, is semisimple. Let $u_1, \dots, u_m$ be a base of A contained in H, and let $w_i \quad (i = 1, \dots, m)$ be the group of words in d variables, such that $u_i = w_i(h_1, \dots, h_d)$. We have

$$u_iu_j = \sum_{k=1}^m c_{ij}^k u_k$$

for suitable c_{ij}^k in Ω, called the structure constants of A. Moreover, there are d_{ij} in $\Omega \quad (i = 1, \dots, d;\ j = 1, \dots, m)$ such that

$$h_i = \sum_{j=1}^m d_{ij}u_j.$$

We shall let F denote the subvariety in G^d given by

(2.30)
$$w_i(x_1, \dots, x_d)w_j(x_1, \dots, x_d) = \sum_{k=1}^m c_{ij}^k w_k(x_1, \dots, x_d) \quad (i, j = 1, \dots, m),$$

and

(2.31)
$$x_i = \sum_{j=1}^m d_{ij}w_j(x_1, \dots, x_d) \qquad (i = 1, \dots, d),$$

and shall show that F coincides with the multidimensional conjugacy class C of $h = (h_1, \dots, h_d)$. Obviously $C \subset F$. Now let $f = (f_1, \dots, f_d) \in F$.

Let B denote the subspace spanned by $v_i = w_i(f_1, \dots, f_d)$ $(i = 1, \dots, m)$. From (2.30) it follows that B is a subalgebra of $M_n(D)$ and $u_i \to v_i$ (for $i = 1, \dots, m$) extends to a surjective algebra homomorphism $\varphi: A \to B$, and from (2.31) that $\varphi(h_i) = f_j$ $(j = 1, \dots, d)$.

Let $A = \bigoplus_{i=1}^{t} A_i$ be the decomposition of A into the direct sum of simple subalgebras. Then for each $i = 1, \dots, t$, either $\varphi(A_i) = 0$ or the restriction of φ to A_i is an isomorphism onto its image. Then, by the Skolem-Noether theorem (cf. §1.4.1), there exists g in $GL_n(\Omega)$ such that the homomorphism $\psi\varphi$, where $\psi = \operatorname{Int} g$, satisfies the condition that for each $i = 1, \dots, t$ the restriction of $\psi\varphi$ to A_i is either the zero homomorphism or the identity. If $\psi\varphi \mid_{A_i} = 0$ for some i, then $B = \varphi(A)$ consists entirely of degenerate matrices. This contradicts $f_i \in B$. Thus $\psi\varphi \mid_A = \mathrm{id}_A$, hence $f_i = \varphi(h_i) = \psi^{-1}(h_i) = g^{-1}h_i g$ for all $i = 1, \dots, d$, i.e., $f \in C$, as required.

The general case of Theorem 2.16 reduces to the special case. We choose a faithful representation $\varphi: G \to GL_n(\Omega)$ under which H maps to a completely reducible linear group, and view G as a subgroup of $G_0 = GL_n(\Omega)$. Let C_0 (resp., C) denote the multidimensional conjugacy class of $h = (h_1, \dots, h_d)$ with respect to G_0 (resp., G). Clearly $C \subset C_0 \cap G^d$.

LEMMA 2.11. *C is an irreducible component of $C_0 \cap G^d$.*

PROOF: Obtained by generalizing the argument in Richardson [1]. Let Z denote the irreducible component of $C_0 \cap G^d$ containing C; we shall show that $Z = C$. Since G is reductive and $\operatorname{char} K = 0$, each representation in the Lie algebra $\mathfrak{g}_0 = L(G_0)$ is completely reducible (cf. Theorem 2.4), so we can choose a G-invariant complement $\mathfrak{m}$ of $\mathfrak{g} = L(G)$. Consider the map $\pi: G_0 \to D_0$, where $D_0 = C_0 h^{-1}$, given by $\pi(g) = (gh_1g^{-1}h_1{}^{-1}, \dots, gh_dg^{-1}h_d{}^{-1})$. It is easy to see that $\pi(G_0) = D_0$, $d_e\pi(X) = (X - Ad(h_1)(X), \dots, X - Ad(h_d)(X))$, for X in $\mathfrak{g}_0$, and moreover $d_e\pi(\mathfrak{g})$ coincides with $T_e(D_0)$, the tangent space at unity of D_0. We are going to show that

$$\mathfrak{g}^d \cap d_e\pi(\mathfrak{g}_0) = d_e\pi(\mathfrak{g}). \tag{2.32}$$

Indeed, suppose $d_e\pi(X) \in \mathfrak{g}^d$ for X in $\mathfrak{g}_0$. Write X as $X = Y + Z$, where $Y \in \mathfrak{g}$ and $Z \in \mathfrak{m}$. Then for any $i = 1, \dots, d$

$$X - Ad(h_i)(X) = (Y - Ad(h_i)(Y)) + (Z - Ad(h_i)(Z)),$$

from which it follows that $Z - Ad(h_i)(Z) \in \mathfrak{m} \cap \mathfrak{g} = (0)$ by the G-invariance of $\mathfrak{m}$, and $d_e\pi(X) = d_e\pi(Y)$, proving (2.32). Since C is a smooth variety, open in its closure (Proposition 2.13), we may consider the tangent space $T_e(D)$ where $D = Ch^{-1}$. Then, from (2.32) and

$$d_e\pi(\mathfrak{g}) \subset T_e(D) \subset T_e(Zh^{-1}) \subset \mathfrak{g}^d \cap d_e\pi(\mathfrak{g}_0)$$

it follows that $T(Ch^{-1})_e = T(Zh^{-1})_e$, i.e., C is open in Z. This argument can be applied to any multidimensional conjugacy class of elements of G contained in Z. Since Z is irreducible, there exists only one such class, so $C = Z$, proving the lemma.

Since by the lemma the multidimensional conjugacy classes are the irreducible components of the closed subset $C_0 \cap G^d$, which are closed, the proof of Theorem 2.16 is completed.

We shall apply the theorem over fields of characteristic zero in two cases—when H is either a connected reductive group or a finite subgroup.

Note that for $d = 1$ the subgroup generated by an element h in G is reductive if and only if h is semisimple, so we obtain one direction of the above criterion on when the conjugacy class of h is closed. In this regard, it would be interesting to see whether the converse of Theorem 2.16 holds.

2.4.7. Varieties of representations. Let Γ be an arbitrary finitely generated group and let G be some algebraic K-group. We shall show that the set of all homomorphisms (i.e., representations) $\Gamma \to G$ is in one-to-one correspondence with the points of a K-variety $R(\Gamma, G)$ called the *variety of representations* of Γ on G. To do so, consider an arbitrary generating set $\gamma_1, \dots, \gamma_d$ of Γ and the associated surjective homomorphism $\pi: F_d \to \Gamma$ from the free group of rank d with generators $x_1, \dots, x_d$, sending x_i to γ_i $(i = 1, \dots, d)$. Let $N = \ker \pi$ be the set of all relations between $\gamma_1, \dots, \gamma_d$ in Γ. Then put

$$R(\Gamma, G) = \{ (g_1, \dots, g_d) \in G^d : w(g_1, \dots, g_d) = e, \quad \forall w = w(x_1, \dots, x_d) \in N \}.$$

Since the algebraic operations on G are regular K-maps, it follows that $w = e$ defines a K-closed subset of G^d, for each word $w = w(x_1, \dots, x_d)$ in $x_1, \dots, x_d$, and therefore $R(\Gamma, G)$ is a K-closed subset (subvariety) of G^d. On the other hand, for any $(g_1, \dots, g_d)$ in G^d, there is a map $\Gamma \to G$ such that $\gamma_i \mapsto g_i$ if and only if $(g_1, \dots, g_d) \in R(\Gamma, G)$. Since any homomorphism from Γ is uniquely determined by the images of the generators, $R(\Gamma, G)$ thereby provides the parametrization of all representations of Γ in G.

Note that up to isomorphism $R(\Gamma, G)$ is independent of the choice of the original system of generators $\gamma_1, \dots, \gamma_d$. Indeed, if $\delta_1, \dots, \delta_l$ is another system of generators, and

$$\delta_i = w_i(\gamma_1, \dots, \gamma_d), \quad i = 1, \dots, l,$$
$$\gamma_j = \theta_j(\delta_1, \dots, \delta_l), \quad j = 1, \dots, d,$$

then

$$(g_1, \dots, g_d) \mapsto (w_1(g_1, \dots, g_d), \dots, w_l(g_1, \dots, g_d)),$$
$$(\delta_1, \dots, \delta_l) \mapsto (\theta_1(\delta_1, \dots, \delta_l), \dots, \theta_d(\delta_1, \dots, \delta_l))$$

are mutually inverse K-morphisms between the varieties of representations $R_\gamma(\Gamma, G)$ and $R_\delta(\Gamma, G)$ constructed using the generating sets $\gamma_1, \dots, \gamma_d$ and $\delta_1, \dots, \delta_l$. G acts on $R(\Gamma, G)$ in the following natural way:

$$g(g_1, \dots, g_d) = (gg_1g^{-1}, \dots, gg_dg^{-1}).$$

In this context, the orbits of G correspond to the classes of representations that are equivalent relative to G.

Several interesting results have appeared recently on the varieties $R(\Gamma, G)$ and associated varieties of characters (cf. Platonov [22], [23], Platonov, Benyasch-Krivetz [1]). However, we shall limit ourselves here to proving the following assertion.

THEOREM 2.17. *(char $K = 0$.) Let Γ be a finite group. Then there is only a finite number of orbits under the natural action of G on $R(\Gamma, G)$; moreover these orbits are closed.*

PROOF: The fact that the orbits are closed follows from the theorem on the multidimensional conjugacy classes, since $\operatorname{char} K = 0$ implies that the image of any homomorphism $\Gamma \to GL_n(\Omega)$ is completely reducible. Proof of the finiteness of the number of orbits for $G = GL_n(\Omega)$ follows from the classical representation theory of finite groups, according to which there are only a finite number of non-equivalent irreducible representations of Γ. The general case is reduced to the case just considered by using Lemma 2.11. Indeed, if C_0 is the equivalence class of some representation ϱ in $R(\Gamma, G)$ relative to $GL_n(\Omega)$, then the irreducible components of $R(\Gamma, G) \cap C_0$ are the equivalence classes relative to G. On the other hand, there are only a finite number of irreducible components. Q.E.D.

2.4.8. Toric varieties. Let G be a reductive K-group, $T \subset G$ a maximal K-torus, and $N = N_G(T)$ its normalizer. It follows from the conjugacy theorem for maximal tori that the map $T_g = gTg^{-1} \mapsto gN$ gives a bijection between the maximal tori of G and the points of $\mathcal{T} = G/N$, called the *(maximal) toric variety* of G. Moreover, the points of $\mathcal{T}_K$ correspond to the maximal K-tori in G. (Note that up to K-isomorphism $\mathcal{T}$ does not depend on the choice of the original torus T.)

THEOREM 2.18 (CHEVALLEY [3], BOREL-SPRINGER [1]). *If $\operatorname{char} K = 0$, then $\mathcal{T}$ is a rational variety over K.*

PROOF: Let $\mathfrak{g} = L(G)$, $\mathfrak{h} = L(T)$ be the Lie algebras of G and T respectively. Let $\mathfrak{m}$ denote some K-subspace of $\mathfrak{g}$ such that $\mathfrak{g} = \mathfrak{h} \oplus \mathfrak{m}$ and let X be a regular element in $\mathfrak{h}_K$. Let $\mathfrak{m}_0$ denote the subset of $\mathfrak{m}$ consisting of Z such that $X + Z$ is regular semisimple and its centralizer $\mathfrak{z}_\mathfrak{g}(X + Z)$ has zero intersection with $\mathfrak{m}$.

We claim that $\mathfrak{m}_0$ is an open subset of $\mathfrak{m}$. Since it is well known that the set of regular semisimple elements is open (cf. §2.1.11), it suffices to show that $\mathfrak{m}_1 = \{ Z \in \mathfrak{m} : \mathfrak{z}_\mathfrak{g}(X + Z) \cap \mathfrak{m} = (0) \}$ is also open. To do so, we introduce the variety $P = \{ (Y, Z) \in \mathfrak{m} \times \mathfrak{m} : [X + Z,\ Y] = 0 \}$ and consider the projection $P \xrightarrow{\pi} \mathfrak{m}$, given by $(Y, Z) \to Z$. Clearly, we have $(0, Z) \in P$ for any Z in $\mathfrak{m}$; in particular, π is surjective and $\pi^{-1}(0) = (0, 0)$, since by our choice of X, $\mathfrak{z}(X) = \mathfrak{h}$ and $\mathfrak{h} \cap \mathfrak{m} = (0)$. By the theorem on the dimension of the fibers of a morphism, we have $\dim P = \dim \mathfrak{m}$ and $\{ Z \in \mathfrak{m} : \dim \pi^{-1}(Z) = 0 \}$ is open in $\mathfrak{m}$. However, it is easy to see that the latter set coincides with $\mathfrak{m}_1$.

Put $W = \{(Z, g) \in \mathfrak{m} \times G : g^{-1}(X + Z)g \in \mathfrak{h}\}$ and $U = (\mathfrak{m}_0 \times G) \cap W$. Since W is the pre-image of $\mathfrak{h}$ under the K-morphism $\varphi: \mathfrak{m} \times G \to \mathfrak{g}$ given by $\varphi(z, g) = g^{-1}(X + Z)g$, it follows that W is a closed K-subset of $\mathfrak{m} \times G$. On the other hand, $(0, 1) \in U$, so U is a nonempty open subset of W. Consider the projections $\theta: W \to \mathfrak{m}$ and $\delta: W \to G$. Since for any X in $\mathfrak{m}_0$, $\mathfrak{z}_\mathfrak{g}(X + Z)$ is the Lie algebra of some maximal torus, it follows from the conjugacy theorem that there exists g in G such that $g^{-1}(X + Z)g \in \mathfrak{h}$, hence $\theta(U) = \mathfrak{m}_0$. Moreover by our construction we have

$$g\mathfrak{h}g^{-1} \cap \mathfrak{m} = (0), \tag{2.33}$$

and

$$\theta^{-1}(Z) = (Z, gN). \tag{2.34}$$

Furthermore, if $x = (Z, g) \in U$ and $x' = (Z', g') \in \delta^{-1}(\delta(x))$, then $g' \in gN$ and $X + Z,\ X + Z' \in g\mathfrak{h}g^{-1} = g'\mathfrak{h}(g')^{-1}$, from which it follows that $Z - Z' \in \mathfrak{m} \cap (g\mathfrak{h}g^{-1})$ and thus $Z = Z'$ by (2.33). Hence, extending the natural morphism $G \to \mathcal{T} = G/N$ to a map $\psi: \mathfrak{m} \times G \to \mathfrak{m} \times \mathcal{T}$, and taking the respective projections $\theta': \overline{\psi(W)} \to \mathfrak{m}$ and $\delta': \overline{\psi(W)} \to \mathcal{T}$, we see that $\theta' \mid_{\psi(U)}: \psi(U) \to \mathfrak{m}_0$ is a bijection and $\delta' \mid_{\psi(U)}$ is an injection. Then by Theorem 2.13 θ' has a K-defined rational inverse map $\chi: \mathfrak{m}_0 \to \overline{\varphi(W)}$ (recall that $\operatorname{char} K = 0$), and moreover $\xi = \delta' \circ \chi$ is injective on its domain of definition. Since $\dim \mathfrak{m} = \dim \mathcal{T}$, applying Theorem 2.13 again we conclude that ξ is a birational isomorphism from $\mathfrak{m}$ to $\mathcal{T}$, proving the theorem.

PROPOSITION 2.24. *Let G be a connected algebraic group over a field K of characteristic zero, and let $W \subset G$ be the set of regular semisimple elements. Then there exists a regular K-map $\varphi: W \to \mathcal{T}$ such that $x \in T_{\varphi(x)}$ for all x in W, i.e., each element is mapped into the ambient torus.*

PROOF: Fix a maximal K-torus $T \subset G$, which was used to determine the toric variety $\mathcal{T} = G/N$, where $N = N_G(T)$, and put

$$Z = \{(x, g) \in W \times G : g^{-1}xg \in T\},$$

clearly a closed subset of $W \times G$. Let $\theta: W \times G \to W \times \mathcal{T}$ denote the regular map extending the natural morphism $\psi: G \to \mathcal{T}$. It is easy to see that $Z = \theta^{-1}(\theta(Z))$, so since ψ is open (cf. Borel [8, § 6]) it follows that $Y = \theta(Z)$ is closed. Let $\pi_1: W \times \mathcal{T} \to W_1$ and $\pi_2: W \times \mathcal{T} \to \mathcal{T}$ be the natural projections. We claim that $\pi_1 |_Y: Y \to W$ is bijective. Indeed, the conjugacy theorem for maximal tori implies that for any x in W there exists g in G such that $g^{-1}xg \in T$, and moreover, since x is regular then g is unique up to multiplication by an element of N. Since W is open in G and consequently smooth, there exists a regular map $\delta: W \to Y$ which is the inverse of $\pi_1 |_Y$, by the results of §2.4.3. Then $\varphi = \pi_2 \circ \delta$ is the desired map. Q.E.D.

Note that if we let G act on W by conjugation and on $\mathcal{T}$ by translation, then φ as constructed above will be G-equivariant.

2.4.9. Varieties of Borel subgroups. In §2.1.9 we saw that the Borel subgroups of a connected algebraic group G are in one-to-one correspondence with the points of the quotient variety $\mathcal{B} = G/B$, where $B \subset G$ is some fixed Borel subgroup; therefore $\mathcal{B}$ is naturally called the *variety of Borel subgroups*. If a K-group G has a Borel subgroup defined over K then $\mathcal{B}$ is obviously a K-variety, and moreover the action of G on B by left translation is defined over K. However, as we know, K-defined Borel subgroups are relatively rare, and therefore it is natural to ask whether in general $\mathcal{B}$ has a K-structure.

THEOREM 2.19. *Let G be a connected algebraic K-group. Then the variety $\mathcal{B}$ of its Borel subgroups has a K-structure such that points of $\mathcal{B}_K$ correspond to K-defined Borel subgroups, and the action of G on $\mathcal{B}$ is K-defined.*

PROOF: Put $H = G/R(G)$ and $\bar{H} = H/Z(H)$. Then $\bar{H}$ is a semisimple adjoint group. Let $\varphi: G \to \bar{H}$ denote the natural morphism. If B is a Borel subgroup of G, then $\varphi(B)$ is a Borel subgroup of $\bar{H}$ and $G/B \simeq \bar{H}/\varphi(B)$. Thus we are reduced to the case of a semisimple adjoint group. Any such group G can be obtained from some quasisplit group G_0 by twisting using a suitable cocycle $a = \{a_\sigma = \operatorname{Int} g_\sigma\}$, lying in $\operatorname{Int} G_0$. Let $B_0 \subset G_0$ be a K-defined Borel subgroup and $\mathcal{B}_0 = G_0/B_0$ the corresponding K-variety of Borel subgroups. Then the left translations r_σ by g_σ define a cocycle r in the group of K-automorphisms of $\mathcal{B}_0$. Since $\mathcal{B}_0$ is a projective variety, there exists a "twisted" variety ${}_r\mathcal{B}_0$ (cf. the remark following Theorem 2.9) which is the $\mathcal{B}$ we require. Q.E.D.

3. Algebraic Groups over Locally Compact Fields

In Chapter 2 we considered properties of algebraic groups that are determined first and foremost by the group itself, independently of the base field. In this and subsequent chapters we shall study the effect of properties of the base field on the structure of these groups. We begin with groups over locally compact fields for several reasons. First, the group of rational points over such a field is provided naturally with the extra structure of an analytic Lie group, thereby offering the possibility of applying the highly developed structure theory of Lie groups. Second, arithmetic subgroups and generalizations, as well as groups of rational points over number fields—the basic objects in the arithmetic theory of algebraic groups—are embeddable as discrete subgroups of suitable direct products of groups of rational points over appropriate completions; hence the properties of the latter have a significant impact on the properties of our original groups.

In §3.1 we set forth the most straightforward results of a topological and analytic nature, a large number of which remain valid over any field which is complete (or Henselian) with respect to some discrete valuation. In §3.2 we study the classical case where the ground field is either $\mathbb{R}$ or $\mathbb{C}$. The key result here is the Iwasawa decomposition, which plays an important role in Chapter 4. In §§3.3–3.4 we investigate groups over non-Archimedean locally compact fields. Results obtained by applying the theory of profinite groups and the theory of reduction of algebraic varieties are set forth in §3.3, and a survey of the results of the Bruhat-Tits theory needed later on is given in §3.4. Lastly, in §3.5 we present some aspects of measure theory to be used elsewhere in the book.

3.1. Topology and analytic structure.

Throughout this chapter K denotes a non-discrete locally compact field of characteristic zero. It is well known (cf., for example, Bourbaki [5]), that either K is connected (in which case it is either $\mathbb{R}$ or $\mathbb{C}$), or totally disconnected (in which case it is a finite extension of the p-adic number field $\mathbb{Q}_p$). In particular, K is complete with respect to some nontrivial valuation $|\ |_v$, which is either the usual absolute value of the real numbers or the complex numbers, or is discrete, i.e., has a cyclic value group. Then, the open balls $B(a, \varepsilon) = \{ x \in K : |a - x|_v < \varepsilon \}$, where $a \in K$ and $\varepsilon > 0$, form a base for the topology of K. Using the topology on K, one can define naturally a topology on the set of K-points V_K of an arbitrary algebraic K-variety V. To do so, consider a Zariski-open K-subset $U \subset V$ and a finite set $f_1, \ldots, f_r$ of regular K-functions on U, and put

$$V(f_1, \ldots, f_r; \varepsilon) = \{ x \in U_K : |f_i(x)|_v < \varepsilon,\ i = 1, \ldots, r \},$$

where $\varepsilon > 0$. It is easy to see that the $V(f_1, \ldots, f_r; \varepsilon)$ form the base of a topology on V_K, which we call the topology defined by the valuation v, or, more concisely, the v-adic topology. Note that this topology is stronger that the Zariski topology. Unlike the Zariski topology, it has the following natural property: if $V = V_1 \times V_2$ is a K-defined product of two K-varieties, then the topological space V_K is canonically homeomorphic to $V_{1K} \times V_{2K}$ endowed with the direct product topology. If W is an open (respectively, closed) K-subvariety of V, then W_K is an open (respectively, closed) subspace of V_K. If follows that V_K is Hausdorff, for any variety V. Indeed, the diagonal $\Delta \subset V \times V$ is closed in the Zariski topology, and therefore Δ_K is closed in $(V \times V)_K$; since $(V \times V)_K \simeq V_K \times V_K$ under the direct product topology, and since Δ_K is closed then V_K is Hausdorff. Any regular K-morphism $f: V \to W$ induces a continuous map $f_K: V_K \to W_K$. Hence, if G is an algebraic K-group, then G_K is a topological group.

The topology introduced above has a more straightforward description for affine or projective varieties; namely, if $V \subset \mathbb{A}^n$, it is induced from K^n via the inclusion $V_K \subset K^n$. (We take the direct product topology on $K^n = K \times \ldots \times K$; its standard base consists of open n-balls $B(a, \varepsilon) = \{ x \in K^n : \|a - x\|_v < \varepsilon \}$, for $a \in K$, $\varepsilon > 0$, where $\|z\|_v$ is defined as $\max_i |z_i|_v$ for $z = (z_1, \ldots, z_n)$.)

This rather straightforward remark has several corollaries. Firstly, V_K is a locally compact space, for any affine variety V. Since any point of an arbitrary variety has an open affine neighborhood, it follows that this assertion holds for any variety.

Secondly, if $G \subset GL_n(\Omega)$ is an algebraic K-subgroup, then the natural topology on $GL_n(K)$ induces a topology on G_K. In particular, if K is non-Archimedean with respect to $|\ |_v$, then the topology on G_K can be described in the following manner: Let $\mathcal{O} \subset K$ be the ring of integers; then the group of integral points $G_{\mathcal{O}} = G \cap GL_n(\mathcal{O})$ is a "basic" open compact subgroup and its *congruence subgroups* $G_{\mathcal{O}}(\mathfrak{p}^\alpha) = G \cap (E_n + \mathfrak{p}^\alpha M_n(\mathcal{O}))$, where $\mathfrak{p} \subset \mathcal{O}$ is the maximal ideal, constitute a base of the neighborhoods of the identity in G_K.

Now let $V \subset \mathbb{P}^n$ be a projective variety. Then the topology on V_K is induced from $\mathbb{P}^n_K$, the topology on $\mathbb{P}^n_K$ being the quotient topology arising from the canonical map $K^{n+1} \setminus (0) \to \mathbb{P}^n_K$. It is well known (cf., for example, Bourbaki [2]), that $\mathbb{P}^n_K$ is compact with respect to this topology; and therefore V_K is also compact, since V_K is closed in $\mathbb{P}^n_K$.

The question of the compactness of V_K will not be considered here in complete generality; however a compactness criterion will be given for the case where V is a homogeneous space.

THEOREM 3.1. *Let G be an algebraic K-group, and H a K-subgroup.*

G_K/H_K is compact if and only if H contains a maximal connected K-split solvable subgroup of the connected component G^0. In particular, G_K is a compact group if and only if G^0 is reductive and anisotropic over K.

PROOF: The proof reduces easily to the case where G is connected.

($\Leftarrow$) Assume H contains a maximal connected K-split solvable subgroup B of G. We shall show that G_K/B_K is compact, thereby implying that G_K/H_K is also compact. According to Chevalley's theorem (cf. §2.4.4) we can choose a K-representation $G \to GL(V)$ and a one-dimensional subspace $V_1 \subset V$ such that the stabilizer of V_1 in G is B. Since B is split over K, its image in $GL(V/V_1)$ is trigonalizable over K. It follows that in V there is a K-flag $\mathcal{F} = \{ V_1 \subset \ldots \subset V_i \subset \ldots \subset V_n = V \ (\dim V_i = i) \}$ "beginning" with V_1 and invariant with respect to B. Let X denote the closure of the orbit $G\mathcal{F}$ in the flag variety $\mathcal{F}(V)$ (cf. Borel [8]). Since $\mathcal{F}(V)$ is projective, X is also projective, and therefore the above remark asserts that X_K is compact.

Further, as we shall soon see (cf. Corollary 1 of Proposition 3.3), it follows from the Inverse Function Theorem that the G_K-orbits in $(G\mathcal{F})_K$ are open. If we show that $X_K = (G\mathcal{F})_K$, then all the G_K-orbits in X_K are open, and consequently the orbit $G_K\mathcal{F}$, being the complement of the union of the other orbits, is closed, and consequently compact. Since by construction B stabilizes $\mathcal{F}$, the natural map $\varphi: G \to X$ given by $g \mapsto g\mathcal{F}$ induces a continuous bijection $\psi: G_K/B_K \to G_K\mathcal{F}$. But $\varphi_K: G_K \to X_K$ is an open map (Proposition 3.3, Corollary 1), so actually we have a homeomorphism $G_K/B_K \xrightarrow{\sim} G_K\mathcal{F}$, as desired.

Since $(G\mathcal{F})_K \subset X_K$, it remains to show that $X_K \subset G\mathcal{F}$. If not, let $\mathcal{L} \in X_K \setminus G\mathcal{F}$. Then the dimension of $G\mathcal{L}$ must be strictly less than $\dim G\mathcal{F}$ (cf. Proposition 2.23), i.e., the stabilizer $G(\mathcal{L})$ must have dimension strictly greater than $\dim B$. On the other hand, $G(\mathcal{L})$ is clearly trigonalizable over K, so the connected component $G(\mathcal{L})^0$ is split over K. But this contradicts the fact that B is a maximal connected K-split subgroup of G, and thus has maximal dimension, since all maximal connected K-split solvable subgroups of G are conjugate (cf. Borel-Tits [1]).

($\Rightarrow$) Suppose G_K/H_K is compact. Choose a maximal connected solvable K-split subgroup B of G, containing a maximal connected solvable K-split subgroup of H. By the first part of our argument, $H_K/(H \cap B)_K$ is compact. It follows immediately that B_KH_K is closed in G_K, noting $(B_KH_K)^{-1} = H_KB_K$. Therefore $B_K/(B \cap H)_K \simeq B_KH_K/H_K$ is compact. We shall conclude the proof by showing that $B = B \cap H$, i.e., $B \subset H$.

Indeed, it is well known (cf. §2.1.8) that B contains a normal series $B = B_0 \supset B_1 \supset \ldots \supset B_r = (e)$ defined over K, whose composition factors B_i/B_{i+1} are K-isomorphic to $\mathbb{G}_a$ or $\mathbb{G}_m$. If $B \cap H \neq B$, then there is

i such that $B_i(B \cap H) = B$ and $F = B_{i+1}(B \cap H) \neq B$. B_K/F_K is compact since $B_K/(B \cap H)_K$ is compact. Now consider the action of $T = B_i/B_{i+1}$, isomorphic to $\mathbb{G}_a$ or $\mathbb{G}_m$, on B/F. A consequence of Corollary 2 of Proposition 3.3 is the openness of all the orbits of T_K on $(B/F)_K$, from which it follows that $T_K e$ is closed, where e is the class of F in B/F. This means $T_K/\bar{F}_K$ is compact, where $\bar{F}$ is the image of $F \cap B_i$ in T. But $\bar{F}$ is finite since $\dim T = 1$, hence T_K is compact, contradiction. Q.E.D.

REMARK: Applying the finiteness theorem for Galois cohomology over local fields (cf. §6.4), we can show easily that there are a finite number of orbits of G_K in $(G/H)_K$, from which it follows that the spaces G_K/H_K and $(G/H)_K$ are either both compact or both noncompact.

Among other topological properties of V_K we mention the following: if K is totally disconnected then V_K is also totally disconnected. In §3.2 we shall consider when V_K is connected for the case $K = \mathbb{R}, \mathbb{C}$.

Most of the above remarks on the topology of V_K apply equally well to the case where K is a locally compact field of characteristic $p > 0$, i.e., isomorphic to the field $F((t))$ of formal power series over a finite field. However, our assumption $\operatorname{char} K = 0$ cannot be dropped when we study the analytic structure on V_K.

Our next objective is to introduce on V_K (or, more precisely, on its Zariski-open subset) the structure of an analytic variety. Here, from the very outset, it is helpful to assume that V_K is Zariski-dense in V, since the dimension of V_K as an analytic variety will then coincide with $\dim V$ as an algebraic variety. Note that this condition can always be satisfied by passing from V_K to its closure W in V; W is defined over K since $\operatorname{char} K = 0$ and, clearly, $W_K = V_K$.

We aim to show that each simple point x in V_K has a neighborhood which is homeomorphic to an open ball in the space K^m, where $m = \dim_x V$. Replacing V by a suitable affine neighborhood of x, we may assume V is an affine variety, i.e., $V \subset \mathbb{A}^n$. Then Proposition 2.22 and the following version of the Inverse Function Theorem can be applied:

THEOREM 3.2 (INVERSE FUNCTION THEOREM). *Let $U \subset K^n$ be open, $x \in U$, and let $f = (f_1, \dots, f_n): U \to K^n$ be a polynomial (or, more generally, an analytic) map. Put $y = f(x)$ and assume that the Jacobian $\left(\frac{\partial f_i}{\partial x_j}(x)\right)_{i,j=1,\dots,n}$ is nonsingular. Then f is a locally analytic isomorphism at x, i.e., there exists a neighborhood $W \subset U$ of x such that $f(W)$ is a neighborhood of y and f restricts to an analytic isomorphism from W to $f(W)$.*

PROOF: cf. Serre [4, Part II, Chapter 3 §9]. There one can also find the definition of an analytic function and a discussion of the properties pertaining to them. Note that we do not in fact need these properties, since

in most applications it suffices to know that f is a local homeomorphism at x under the hypotheses of Theorem 3.2.

Now let $x = ({x_1}^0, \dots, {x_n}^0)$ be a simple point. (Note that the existence of such an x follows from our assumption on the density of V_K in V in the Zariski topology, since the set of simple points is open.) Also put $m = \dim_x V$. Then, by Proposition 2.22, some neighborhood of x in V is determined by $r = n - m$ equations. More precisely, there are polynomials $f_1, \dots, f_r \in K[x_1, \dots, x_n]$ and a Zariski-open subset $U \subset \mathbb{A}^n$ such that $Y = \{ y \in U : f_i(y) = 0,\ i = 1, \dots, r \}$ is contained in V and the Jacobian

$$\left(\frac{\partial f_i}{\partial x_j}(x)\right)_{\substack{i=1,\dots,r \\ j=1,\dots,n}}$$

has rank n. Also, we may assume that $\det\left(\frac{\partial f_i}{\partial x_j}(x)\right)_{i,j=1,\dots,r} \neq 0$. Consider $g = (g_1, \dots, g_n): K^n \to K^n$ where $g_i = f_i$ for $i \leq r$, and $g_i = x_i$ for $i > r$. Clearly

$$\det\left(\frac{\partial g_i}{\partial x_j}(x)\right)_{i,j=1,\dots,n} = \det\left(\frac{\partial f_i}{\partial x_j}(x)\right)_{i,j=1,\dots,r} \neq 0.$$

By Theorem 3.2 there exists a neighborhood $U \subset K^n$ of x such that $W = g(U)$ is a neighborhood of $g(x)$ and $g: U \to W$ is an analytic isomorphism. Let $h = (h_1, \dots, h_n) = g^{-1}: W \to U$. Then

$$\varphi = (\varphi_i(t_1, \dots, t_{n-r}), \dots, \varphi_r(t_1, \dots, t_{n-r}), t_1, \dots, t_{n-r}),$$

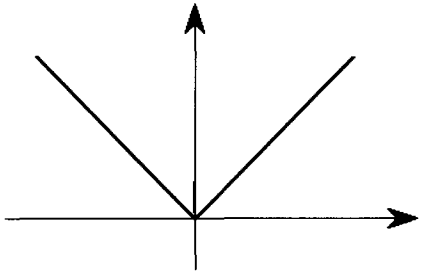
where $\varphi_i(t_1, \dots, t_{n-r}) = h_i(x_1^0, \dots, x_r^0, t_1, \dots, t_{n-r})$ $(i = 1, \dots, r)$ parametrizes the neighborhood of x in V_K by the points of some open set in K^{n-r}. Moreover, the parametrizing map is actually the inverse map for the projection onto the (last) $n-r$ coordinates. From this it follows easily that any two parametrizations of a neighborhood of a given point differ by an analytic isomorphism. Thus, for the case of V affine, the set of simple points of V_K carries the natural structure of an analytic variety (cf. Serre [4]). This structure is respected by the regular maps of affine varieties; namely, any regular K-map $f: V \to W$ of affine K-varieties V and W induces an analytic map $\tilde{f}: V_K \cap f^{-1}(\tilde{W}_K) \to \tilde{W}_K$, where $\tilde{V}_K$ (resp., $\tilde{W}_K$) is the set of simple points of V_K (resp., W_K) provided with the structure introduced above of an analytic variety.

Using affine neighborhoods of points of an arbitrary variety V, it is easy to show that in general $\tilde{V}_K$ carries the structure of an analytic variety, and any regular K-defined map f of algebraic K-varieties induces an analytic

map $\tilde{f}$, as indicated above. Indeed, the coordinates of any two affine neighborhoods of the same point are related to each other by a birational transformation defined at that point. Therefore two neighborhood parametrizations of a given point, constructed via these two affine neighborhoods, differ by an analytic isomorphism. Furthermore, any regular K-map $f: V \to W$ induces a regular map of affine neighborhoods, and therefore an analytic map $\tilde{f}$. We have proven

PROPOSITION 3.1. *Let V be an algebraic K-variety. Then the set $\tilde{V}_K$ of simple points of V_K has the natural structure of an analytic variety over K. Any regular K-map $f: V \to W$ of algebraic K-varieties induces an analytic map $\tilde{f}: \tilde{V}_K \cap f^{-1}(\tilde{W}_K) \to \tilde{W}_K$.*

Thus we can apply the theory of analytic varieties (cf. Serre [4]) to the study of V_K. We call the reader's attention to several concepts needed for our further discussion. Each point x of an analytic variety X has an associated tangent space $T_x(X_{an})$,[1] which is a vector space over K of dimension equal to $\dim X$, i.e., the dimension of the affine space whose domains are used to parametrize the neighborhoods of the points of X. A *morphism $f: X \to Y$ of analytic varieties* is a continuous locally analytic map, in the sense that it induces a usual analytic map of the parametrization domains for the respective points. Any morphism $f: X \to Y$ gives rise to a linear map $d_x f_{an}: T_x(X_{an}) \to T_{f(x)}(Y_{an})$, called the *differential* of f at x. f is called an *immersion* at x if $d_x f_{an}$ is injective, and simply an *immersion* if this condition holds for all points. If a topological subspace X of the variety Y is also provided with the structure of an analytic variety and the inclusion map $X \hookrightarrow Y$ is an immersion, then X is said to be a *subvariety* of Y. To illustrate this concept, take the example of "non-subvariety" of $\mathbb{R}^2$ provided by the set $y = |x|$, as in the following diagram.



[1] The subscript *an* is used in order to distinguish later on between the tangent space of an algebraic variety and the tangent space of the corresponding analytic variety.

(This set is "unsmoothly" embedded in $\mathbb{R}^2$. The subvariety under suitable analytic change of coordinates can be defined by linear equations in the neighborhood of any point.) We shall also need the following criterion of openness of a map.

PROPOSITION 3.2. *Let $f: X \to Y$ be a morphism of analytic varieties, and $x \in X$. If $d_x f_{an}: T_x(X_{an}) \to T_{f(x)}(Y_{an})$ is surjective, then f is an open map at x.*

PROOF: The proof follows easily from the Inverse Function Theorem (3.2), cf. Serre [4, Part II, Chapter 3, §9].

LEMMA 3.1. *Let V be an algebraic K-variety, $x \in \tilde{V}_K$. Then $T_x(\tilde{V}_{K_{an}}) = T_x(V)_K$, i.e., the "analytic" tangent space is the set of K-elements of the "algebraic" tangent space. If $f: V \to W$ is a regular K-map of algebraic K-varieties, $x \in \tilde{V}_K$, and $f(x) \in \tilde{W}_K$, then $d_x f_{an} = (d_x f)\,|_{T_x(\tilde{V}_{K_{an}})}$.*

The proof follows directly from a comparison of the appropriate definitions.

Lemma 3.1 and Proposition 3.2 can be applied to algebraic varieties as follows:

PROPOSITION 3.3. *Let $f: V \to W$ be a dominant K-morphism of irreducible algebraic K-varieties. If x in V_K is a simple point such that $f(x)$ is a simple point on W, and $d_x f: T_x(V) \to T_{f(x)}(W)$ is surjective, then $f_K: V_K \to W_K$ is open at x. Consequently there exists a Zariski-open subset $U \subset V$ such that f_K is open at any point x in U_K.*

PROOF: Consider the analytic map $\tilde{f}: \tilde{V}_K \cap f^{-1}(\tilde{W}_K) \to \tilde{W}_K$ induced by f. The hypothesis and Lemma 3.1 imply $x \in \tilde{V}_K \cap f^{-1}(\tilde{W}_K)$, and $d_x \tilde{f}_{an}$ is a surjective map. Therefore f_K is open at x by Proposition 3.2. Furthermore, since $\operatorname{char} K = 0$, f is automatically a separable morphism, i.e., the corresponding extension $K(V)/K(W)$ of fields of rational functions is separable. It follows (cf. Borel [8, AG §17]) that there exists a Zariski-open subset $U \subset V$ such that for any x in U the hypotheses of the first assertion hold, and the proof is complete.

It should be noted that if V_K is not assumed to be dense in V then U_K could be empty and Proposition 3.3 would become meaningless. Therefore we shall now describe two cases, of particular interest to us further on, for which such degeneracy does not occur.

COROLLARY 1. *Assume V to be smooth and $V_K \neq \emptyset$. Then the image $f_K(F)$ of any nonempty open set $F \subset V_K$ contains a nonempty open subset of W_K. In particular, if $f: G \to H$ is a surjective K-morphism of algebraic K-groups, then $f_K(G_K)$ is an open subgroup of H_K.*

To prove it, we need the following lemma:

LEMMA 3.2. *Let V be an irreducible smooth variety defined over K, such that $V_K \neq \emptyset$. Then, for any nonempty Zariski K-open subset $U \subset V$, the set U_K is dense in V_K in the v-adic topology. Furthermore, any nonempty v-adically open subset $F \subset V_K$ is Zariski-dense in V; in particular, V_K is Zariski-dense in V.*

PROOF: It is easy to see that both assertions of the lemma reduce to proving that $U \cap F$ is nonempty, where $U \subset V$ is Zariski-open and $F \subset V_K$ is open in the topology given by the valuation. Put $X = V \setminus U$. For any x in F, we can find a nonzero regular function $f \in K[W]$ in a neighborhood of $W \subset V$ defined over K, which vanishes on $X \cap W$. Since V is a smooth variety by hypothesis, x is simple and consequently, by the above, there exists an analytic parametrization of some neighborhood of x. If $U \cap F = \emptyset$, i.e., $F \subset X$, then the analytic Taylor series for f must be null; but since the algebraic and analytic Taylor series coincide, this contradicts the injectivity of the map sending a regular function at a simple point to its algebraic Taylor series (cf. Shafarevich [1, Ch. 2]). Q.E.D.

Now let $U \subset V$ be the Zariski-open subset provided by Proposition 3.3. Then $U \cap F \neq \emptyset$ by Lemma 3.2. Since $f_K: V_K \to W_K$ is open at any point x in $U \cap F$, our first assertion follows easily. The second assertion of Corollary 1 follows directly from the first.

COROLLARY 2. *Let $G \times X \to X$ be a K-defined action of a connected algebraic K-group G on a K-variety X. If $x \in X_K$ and Y is the closure of the orbit Gx, then for any open $F \subset G_K$ the set Fx is open in Y_K.*

PROOF: The morphism $\varphi: G \to Y$, given by $\varphi(g) = gx$, is dominant. Therefore, applying Proposition 3.3, we can find a Zariski-open set $U \subset G$ with the properties described. Then φ_K is open at any point g in U_K. Since $\varphi(hg) = h\varphi(g)$ for any h in G, φ_K actually is open at any point h in G_K. It follows at once that $\varphi(F) = Fx$ is open for any open $F \subset G_K$.

Let us give an example of how these results apply to examination of the structure of the groups of rational points over locally compact fields.

THEOREM 3.3 (RIEHM [1,2]). *Let G be a K-simple algebraic group. Then every noncentral normal subgroup of G_K is open.*

PROOF: For each g in G put $W_g = \{ [g,h] = g^{-1}h^{-1}gh : h \in G \}$. All the W_g are irreducible varieties, contain the identity, and together generate the commutator subgroup $[G,G]$ of G. In our case $[G,G] = G$, so, by a straightforward dimension argument (cf. Borel [8, Proposition 2.2]) and taking into account $(W_g)^{-1} = W_{g^{-1}}$, we obtain the existence of a finite set of elements $g_1, \dots, g_n$ in G such that $G = W_{g_1} \dots W_{g_n}$.

Consider the morphism

$$\psi: X = \underbrace{G \times \dots \times G}_{2n} \to \underbrace{G \times \dots \times G}_{n+1} = Y, \text{ given by}$$

$$\psi(x_1, \dots, x_n, y_1, \dots, y_n) = (x_1, \dots, x_n, [x_1, y_1] \dots [x_n, y_n]).$$

By the theorem on the dimensions of the fibers of a morphism (cf. §2.4.2), for any point y in $\psi(X)$ we have $\dim \psi^{-1}(y) \geq (n-1)\dim G$. We claim there is y for which $\dim \psi^{-1}(y) = (n-1)\dim G$. By assumption $\varphi_{g_1,\dots,g_n}: \underbrace{G \times \dots \times G}_{n} \to G$ given by

$$\varphi_{g_1,\dots,g_n}(x_1, \dots, x_n) = [g_1, x_1] \dots [g_n, x_n]$$

is surjective, and therefore there exist points g in G such that

$$\dim \varphi^{-1}_{g_1,\dots,g_n}(g) = (n-1)\dim G.$$

Then y of the form $(g_1, \dots, g_n, g)$ will do.

Again, applying the theorem on the dimensions of the fibers of a morphism, we obtain the existence of a Zariski-open set $U \subset Y$ such that $\dim \psi^{-1}(x) = (n-1)\dim G$ for any x in U. Let V denote the projection of U on the first n components. Then V is open in $\underbrace{G \times \dots \times G}_{n}$ and for any $(x_1, \dots, x_n)$ in V we can find g in G satisfying $\dim \varphi^{-1}_{x_1,\dots,x_n}(g) = (n-1)\dim G$. It follows that $\varphi_{x_1,\dots,x_n}$ is dominant for $(x_1, \dots, x_n)$ in V.

Now let $N \subset G_K$ be a noncentral normal subgroup. Since G_K is dense in G in the Zariski topology (Theorem 2.2; for a local field it also follows from Lemma 3.2), the closure $\bar{N}$ of N in this topology is a noncentral normal K-subgroup of G, and consequently $\bar{N} = G$ since by assumption G is K-simple. Hence it follows from the above argument that there are $x_1, \dots, x_n$ in N such that $\varphi_{x_1,\dots,x_n}$ is a dominant morphism. Applying Corollary 1 of Proposition 3.3 we see that $\varphi_{x_1,\dots,x_n}(G_K \times \dots \times G_K)$ contains an open subset of G_K. But

$$\varphi_{x_1,\dots,x_n}(G_K \times \dots \times G_K) = \{ [x_1, h_1] \dots [x_n, h_n] : h_i \in G_K \} \subset N;$$

hence N is open in G_K. Q.E.D.

REMARK: The proof relies only on Proposition 3.3, which is a formal corollary of the Inverse Function Theorem, and nowhere relied on the local compactness of K. Therefore the assertion of the theorem holds whenever the Inverse Function Theorem is true over K, which is the case if K is complete

with respect to a nontrivial discrete valuation. This more general version will be needed when we investigate the deviation from the weak approximation property for simply connected groups over an arbitrary field (cf. §7.3). Let us also point out that, as we shall show in §§3.2–3.3, Theorem 3.3 yields a stronger result for locally compact fields: under the hypothesis of Theorem 3.3 any noncentral normal subgroup of G_K has finite index.

Thus far, in our exposition of results from the theory of analytic varieties, we have ignored the fact that most of the varieties under consideration have a group structure. Now we shall present several results obtained by utilizing this structure. On the whole, the study of analytic group varieties pertains to classical Lie group theory, expounded for example in Serre [3], Bourbaki [4], and Helgason [1]. We shall limit ourselves to pointing out several results relating mainly to Lie groups arising from algebraic groups. Thus, let G be an algebraic group defined over K. As we know, G is a smooth variety, and therefore G_K has the natural structure of an analytic variety over K. Moreoever, the group operations are analytic maps, so G_K is endowed with the structure of an analytic group or a Lie group (cf. Serre [3]). The *Lie algebra* $\mathfrak{g}^*$ of the analytic group G_K is the tangent space at the identity $T_e^*(G)$. By Lemma 3.1 $\mathfrak{g}^*$ coincides with the subspace of K-elements of the algebraic tangent space $T_e(G)$, i.e., of the Lie algebra $\mathfrak{g} = L(G)$ as an algebraic group; moreoever, the Lie bracket on $\mathfrak{g}^*$ is induced from $\mathfrak{g}$. We can define the exponential and logarithmic maps (cf. Bourbaki [4]) which are mutually inverse, local analytic isomorphisms between $\mathfrak{g}^*$ and G_K. If $G \subset GL_n(\Omega)$ is a matrix realization of G, then exp and log are given by the usual formulas:

$$\exp(X) = E_n + \frac{X}{1!} + \frac{X^2}{2!} + \cdots + \frac{X^m}{m!} + \cdots \quad \text{for } X \in \mathfrak{g}^*$$

$$\log(x) = (x - E_n) - \frac{(x-E_n)^2}{2} + \cdots + (-1)^{m-1}\frac{(x-E_n)^m}{m} + \cdots \quad \text{for } x \in G_K. \tag{3.1}$$

In particular, the exponential map for a group restricts to the exponential map of its subgroups. If $X, Y \in \mathfrak{g}$ (respectively, $x, y \in G$) commute, then

$$\exp(X+Y) = \exp(X)\exp(Y)$$
$$\log(xy) = \log(x) + \log(y)$$

(assuming that all the expressions here are defined, i.e., that the corresponding series converge). Hence, in particular, it follows that G_K always

has a neighborhood of the identity which does not contain nontrivial elements of finite order (cf. Serre [4]). Also note the following formulas:

$$\exp(x^{-1}Xx) = x^{-1}\exp(X)x,$$
$$\log(x^{-1}yx) = x^{-1}\log(y)x, \tag{3.2}$$

i.e., the exponential and logarithmic maps commute with the adjoint action of G_K.

If a subgroup H of G_K is also a subvariety of G_K, then H is said to be a *Lie subgroup* of G_K. It follows from the definition that if $H \subset G_K$ is a Lie subgroup, then there is an analogous inclusion $\mathfrak{h}^* \subset \mathfrak{g}^*$ of the corresponding Lie algebra. A Lie subgroup $H \subset G_K$ need not be closed in the topology of G_K and consequently it need not be closed in the Zariski topology either. Let B be the closure of H in the Zariski topology. Then B_K is a Lie subgroup of G_K containing H. How far can B_K differ from H? We shall answer this question in terms of the corresponding Lie algebras $\mathfrak{b}^*$ and $\mathfrak{h}^*$.

PROPOSITION 3.4. *In the described setting, $\mathfrak{h}^*$ is a Lie ideal of $\mathfrak{b}^*$.*

PROOF: Consider the adjoint representation $\mathrm{Ad}: G \to GL(\mathfrak{g})$, where $\mathfrak{g} = L(G)$ is the Lie algebra of G, as an algebraic group; $\mathfrak{g} = \mathfrak{g}^* \otimes_K \Omega$, where $\mathfrak{g}^*$ is the Lie algebra of G_K, as an analytic group. The space $\mathfrak{h}^*$, and consequently the space $\mathfrak{h} = \mathfrak{h}^* \otimes_K \Omega$, are clearly invariant. On the other hand $S = \{ g \in G : \mathrm{Ad}(g)(\mathfrak{h}) = \mathfrak{h} \}$ is a Zariski-closed subgroup of G. Hence, from $H \subset S$ it follows that $B \subset S$. Taking into account that the differential of the adjoint representation of an algebraic group is the adjoint representation of the corresponding Lie algebra (cf. Borel [8, §3]), for $\mathfrak{b} = L(B)$ we have $[\mathfrak{b}, \mathfrak{h}] \subset \mathfrak{h}$. Since $\mathfrak{b}^* = \mathfrak{b}_K$, $\mathfrak{h}^* = \mathfrak{h}_K$, it follows that $[\mathfrak{b}^*, \mathfrak{h}^*] \subset \mathfrak{h}^*$. Q.E.D.

We conclude our survey of the necessary results from Lie group theory with the statement of a theorem proved by E. Cartan for $K = \mathbb{R}$.

THEOREM 3.4. *Suppose K is either the field of real numbers $\mathbb{R}$ or the field of p-adic numbers $\mathbb{Q}_p$. Then any closed subgroup of a Lie group over K is a Lie group. Every continuous homomorphism of Lie groups over K is analytic.*

PROOF: Cf. Serre [3, pp. 260–263].

We conclude this subsection with a nice application of techniques of Lie groups and analytic varieties to group theory.

PROPOSITION 3.5. *Let $G \subset GL_n$ be a reductive algebraic group defined over a non-Archimedean local field K. Then the group of integral points*

$G_{\mathcal{O}} = G \cap GL_n(\mathcal{O})$ has only a finite number of pairwise nonconjugate finite subgroups. In particular, the number of nonconjugate finite subgroups of $SL_n(\mathbb{Z}_p)$ is finite.

PROOF: From the above remarks about Lie groups it follows that there exists a neighborhood of the identity in $G_{\mathcal{O}}$ which does not contain nontrivial elements of finite order. But the congruence subgroups $G_{\mathcal{O}}(p^\alpha) = \{ x \in G_{\mathcal{O}} : x \equiv E_n \pmod{p^\alpha} \}$,[2] where $p \subset \mathcal{O}$ is the valuation ideal and $\alpha \geq 1$, constitute a base of the neighborhoods of the identity; hence some congruence subgroup (say, $G_{\mathcal{O}}(p^\alpha)$) has this property. It follows that any finite subgroup of $G_{\mathcal{O}}$ is isomorphic to a subgroup of $G_{\mathcal{O}}/G_{\mathcal{O}}(p^\alpha)$, which is finite by virtue of the compactness of $G_{\mathcal{O}}$ and the openness of $G_{\mathcal{O}}(p^\alpha)$.

Therefore $G_{\mathcal{O}}$ contains only a finite number of non-isomorphic finite subgroups, and it suffices to show that the finite subgroups of $G_{\mathcal{O}}$ that are isomorphic to a given group Γ partition into a finite number of conjugacy classes. To do so, we consider the variety of representations $R = R(\Gamma, G)$ (cf. §2.4.7) and shall establish the stronger assertion that the set $R_{\mathcal{O}} = \mathrm{Hom}(\Gamma, G_{\mathcal{O}})$ consists of only a finite number of orbits under the natural action of $G_{\mathcal{O}}$. It follows from Theorem 2.17 that there are only a finite number of orbits in $R(\Gamma, G)$ under the action of G, and these orbits are closed in the Zariski topology. Let X be one of these orbits. It suffices to show that $X_{\mathcal{O}}$ consists of a finite number of $G_{\mathcal{O}}$-orbits. This is obvious if $X_{\mathcal{O}} = \emptyset$. If $X_{\mathcal{O}} \neq \emptyset$, then X is clearly defined over K and for any point x in $X_{\mathcal{O}}$ the orbit $G_{\mathcal{O}}x$ is open in $X_{\mathcal{O}}$ by Corollary 2 of Proposition 3.3. On the other hand, since X is closed in R and $\mathcal{O}$ is compact, then $X_{\mathcal{O}}$ is compact. Hence the open covering $X_{\mathcal{O}} = \bigcup_x G_{\mathcal{O}}x$ has a finite subcovering, yielding a finite number of orbits of $G_{\mathcal{O}}$ on $X_{\mathcal{O}}$. Q.E.D.

3.2. The Archimedean case.

In the previous section several results were obtained concerning elementary topological and analytic properties of the space X_K, where X is an algebraic variety defined over a locally compact field K. Their proofs relied only on the Inverse Function Theorem, which works in both the "classical" case $K = \mathbb{R}$ or $\mathbb{C}$ and in the non-Archimedean case when K is a finite extension of $\mathbb{Q}_p$. In this section we shall present results which are intrinsic only to the Archimedean case. First among these are results pertaining to connectedness.

THEOREM 3.5. *Let X be an irreducible algebraic variety defined over $\mathbb{C}$. Then the space $X_{\mathbb{C}}$ is connected.*

[2] Two matrices over a ring are congruent modulo its ideal if and only if all the respective entries are congruent.

PROOF: Cf. Shafarevich [1, Ch. 7, §2]. However, we shall not need this result.

THEOREM 3.6 (WHITNEY [1]). *Let X be an algebraic variety defined over $\mathbb{R}$. Then the space $X_{\mathbb{R}}$ has only a finite number of connected components.*

PROOF: Replacing X by the closure of $X_{\mathbb{R}}$ in the Zariski topology (which does not affect the $\mathbb{R}$-points), we may assume $X_{\mathbb{R}}$ is dense in X. Then the real points are dense in each irreducible component of X, which thus is defined over $\mathbb{R}$. Hence, we may assume X to be irreducible.

Suppose that the theorem does not hold, and let X be a counterexample of minimal dimension (clearly $\dim X > 0$). Choose an affine open $\mathbb{R}$-defined subset $Y \subset X$. Then $T = X \setminus Y$ is an algebraic $\mathbb{R}$-variety whose dimension is strictly less than $\dim X$. By assumption $T_{\mathbb{R}}$ has a finite number of connected components, so the number of connected components of $Y_{\mathbb{R}}$ must be infinite. Therefore we may assume X to be affine.

Let S be the set of singular points of X (cf. §2.4.3). As we know, S is a proper closed subset of X. Therefore, arguing as above, we see that $V = X_{\mathbb{R}} \setminus S_{\mathbb{R}}$ has an infinite number of connected components $\{V_j\}_{j=1}^{\infty}$, and that almost all of them, say V_j for $j \geq l$, are connected components of $X_{\mathbb{R}}$. In §3.1 we showed that V is an analytic variety and, in particular, a locally connected space. Therefore all V_j are disjoint open-and-closed subsets of V and each V_j for $j \geq l$ is an open-and-closed subset of $X_{\mathbb{R}}$. Suppose that we could find a proper closed $\mathbb{R}$-subset $Z \subset X$ intersecting almost all V_j. Then the number of connected components of $Z_{\mathbb{R}}$ could not be finite, since $Z_{\mathbb{R}} = \bigcup_{j=1}^{\infty}(Z_{\mathbb{R}} \cap V_j)$ and $Z_{\mathbb{R}} \cap V_j$ is a nonempty open-and-closed subset of $Z_{\mathbb{R}}$ for almost all j. But this would contradict our assumption, since $\dim Z < \dim X$.

It remains to construct Z. Suppose X is realized as a Zariski-open subset of the affine space $\mathbb{A}^n$, whose set of real points $\mathbb{R}^n$ is endowed with the usual metric. Fix an arbitrary point $a = (a_1, \ldots, a_n)$ in V_1. The subspace V_j is closed in $\mathbb{R}^n$ for each $j \geq l$, and therefore we can find a point b_j in V_j which is the nearest to a. We shall construct a proper closed algebraic subset $Z \subset X$ containing all b_j's. Its equations are easily obtained by using the fact that the b_j's are points of the conditional extremum for the function $g(X_1, \ldots, X_n) = (X_1 - a_1)^2 + \cdots + (X_n - a_n)^2$. That is, if $r = n - \dim X$ and $\mathfrak{a}$ is the ideal of polynomials that vanish on X, then for any $f_1, \ldots, f_r$ in $\mathfrak{a}_{\mathbb{R}}$ and any j the linear forms

$$d_{b_j} f_1, \ldots, d_{b_j} f_r, d_{b_j} g$$

(cf. §2.4.3) are linearly dependent, which is equivalent to satisfying

$$\Delta_i(f_1, \ldots, f_r, g)(b_j) = 0, \quad i = 1, \ldots, \binom{r+1}{n},$$

where $\Delta_i(f_1,\dots,f_r,g)(x)$ runs through the $(r+1)\times(r+1)$ minors of the matrix

$$\begin{pmatrix} \frac{\partial f_1}{\partial X_1}(x) & \dots & \frac{\partial f_1}{\partial X_n}(x) \\ \dots\dots\dots\dots\dots\dots\dots \\ \frac{\partial f_r}{\partial X_1}(x) & \dots & \frac{\partial f_r}{\partial X_n}(x) \\ \frac{\partial g}{\partial X_1}(x) & \dots & \frac{\partial g}{\partial X_n}(x) \end{pmatrix}.$$

Let Z be the subset of X given by

$$\Delta_i(f_1,\dots,f_r,g)(x)=0, \quad i=1,\dots,\binom{r+1}{n},\ f_1,\dots,f_r\in\mathfrak{a}.$$

By assumption Z contains all the b_j, so it remains merely to show that $Z\neq X$. We shall show that $V_1\not\subset Z$. Since a is simple on X, there exist polynomials $f_1,\dots,f_r$ in $\mathfrak{a}_{\mathbb{R}}$ such that $d_xf_1,\dots,d_xf_r$ are linearly independent forms for $x=a$ (Proposition 2.1), and hence also for all x sufficiently close to a. Furthermore, for $d=\dim X>0$ let the analytic functions $u_1(t_1,\dots,t_d),\dots,u_n(t_1,\dots,t_d)$ realize a parametrization of a neighborhood of a (cf. §3.1). Since g is the distance squared from a, the analytic function

$$\varphi(t_1,\dots,t_d)=g(u_1(t_1,\dots,t_d),\dots,u_n(t_1,\dots,t_d))$$

does not reduce to a constant. Therefore

$$\left(\frac{\partial\varphi}{\partial t_1},\dots,\frac{\partial\varphi}{\partial t_d}\right)\not\equiv(0,\dots,0) \tag{3.3}$$

on any open domain of parameters. The equations

$$f_i(u_1(t_1,\dots,t_d),\dots,u_n(t_1,\dots,t_d))=0, \quad i=1,\dots,r$$

yield

$$(d_xf_i)\left(\frac{\partial u_1}{\partial t_j},\dots,\frac{\partial u_n}{\partial t_j}\right)=\sum_{k=1}^{n}\frac{\partial f_i}{\partial X_k}\cdot\frac{\partial u_k}{\partial t_j}=0 \quad \begin{matrix} i=1,\dots,r\\ j=1,\dots,d\end{matrix}.$$

If $d_xf_1,\dots,d_xf_r,d_xg$ are linearly dependent forms, then d_xg is a linear combination of $d_xf_1,\dots,d_xf_r$ for all x sufficiently close to a, since the latter are linearly independent by construction. Consequently

$$(d_xg)\left(\frac{\partial u_1}{\partial t_j},\dots,\frac{\partial u_n}{\partial t_j}\right)=\sum_{k=1}^{n}\frac{\partial g}{\partial X_k}\cdot\frac{\partial u_k}{\partial t_j}=0, \quad j=1,\dots,d. \tag{3.4}$$

But the left side of (3.4) equals $\frac{\partial\varphi}{\partial t_j}$, so (3.4) contradicts (3.3). We conclude that $d_xf_1,\dots,d_xf_r,d_xg$ can not be linearly dependent at all points x in V_1. Therefore not all the determinants $\Delta_i(f_1,\dots,f_r,g)(x)$ are identically equal to zero on V_1, i.e., $V_1\not\subset Z$. Q.E.D.

COROLLARY 1. *Let G be an algebraic $\mathbb{R}$-group. Then $G_{\mathbb{R}}$ has a finite number of connected components. If G is connected and $G_{\mathbb{R}}$ is compact, then $G_{\mathbb{R}}$ is connected.*

Only the second assertion requires proof. Being compact, $G_{\mathbb{R}}$ consists entirely of semisimple elements. Therefore any of its elements lies in a suitable $\mathbb{R}$-torus $T\subset G$. $T_{\mathbb{R}}$ is also a compact group, and therefore T is isomorphic to a torus of the form $(\mathbf{R}^{(1)}_{\mathbb{C}/\mathbb{R}}(\mathbb{G}_m))^d$, where $d=\dim T$ (cf. §2.2.4). From this it follows that $T_{\mathbb{R}}$ can be identified with the product of d copies of the unit circle, which is connected. Thus, the connected component $G^0_{\mathbb{R}}$ must contain each of the $T_{\mathbb{R}}$, and therefore coincides with $G_{\mathbb{R}}$. An alternate proof of the connectedness of $G_{\mathbb{R}}$ may be obtained by using the fact that a compact linear group of $\mathbb{R}$ is closed in the Zariski topology (cf. Chevalley [1, Vol. 3, p. 296]).

PROPOSITION 3.6. *Let G be a connected $\mathbb{R}$-simple algebraic group. Then any noncentral normal subgroup of $G_{\mathbb{R}}$ has finite index. If $G_{\mathbb{R}}$ is compact, then it is (projectively) simple.*

PROOF: By Theorem 3.3 any noncentral normal subgroup N of $G_{\mathbb{R}}$ is open and therefore must contain the connected component $G^0_{\mathbb{R}}$, which by Corollary 1 has finite index in $G_{\mathbb{R}}$. If $G_{\mathbb{R}}$ is compact, then $G_{\mathbb{R}}=G^0_{\mathbb{R}}$, and therefore $N=G_{\mathbb{R}}$.

We continue with the corollaries of Theorem 3.6.

COROLLARY 2. *Let $G\times X\to X$ be a transitive $\mathbb{R}$-action of an algebraic $\mathbb{R}$-group G on an $\mathbb{R}$-variety X. Then $X_{\mathbb{R}}$ is the union of a finite number of $G_{\mathbb{R}}$-orbits. If $X_{\mathbb{R}}$ is connected, then there is exactly one orbit.*

PROOF: For any point x in $X_{\mathbb{R}}$ the orbit $G_{\mathbb{R}}x$ is open in $X_{\mathbb{R}}$ (Corollary 2 of Proposition 3.4). The complement of $X_{\mathbb{R}}\setminus G_{\mathbb{R}}x$ is the union of the remaining orbits, and therefore also is open. Thus $G_{\mathbb{R}}x$ is an open-and-closed subset of $X_{\mathbb{R}}$ and therefore contains a connected component of the latter. Hence the number of distinct orbits does not exceed the number of connected components of $X_{\mathbb{R}}$, which is finite, and is equal to 1 if $X_{\mathbb{R}}$ is connected.

REMARK: Corollary 2 has an obvious cohomological interpretation. To wit, if $x\in X_{\mathbb{R}}$, then X can be identified with the homogeneous space G/H, where $H=G(x)$ is the stabilizer of x, and then the orbits of $G_{\mathbb{R}}$ on $X_{\mathbb{R}}$ are in one-to-one correspondence with the elements of $\ker(H^1(\mathbb{R},H)\to H^1(\mathbb{R},G))$ (cf. §1.3.2). Thus, by Corollary 2, this kernel is finite. Considering the embedding of any given $\mathbb{R}$-group H in some $\mathbb{R}$-group G with trivial cohomology (for example, using the exact $\mathbb{R}$-representation $H\hookrightarrow G=\mathbf{GL}_n$), we conclude that $H^1(\mathbb{R},H)$ is finite, for any $\mathbb{R}$-group H. In

Chapter 6, §6.4 we shall present another proof of this fact, which also works for the case of non-Archimedean local fields.

COROLLARY 3. *Let $f: G \to H$ be a surjective $\mathbb{R}$-morphism of algebraic groups. Then $[H_{\mathbb{R}} : f(G_{\mathbb{R}})]$ is finite. If $H_{\mathbb{R}}$ is connected, in particular if H is unipotent, then $f_{\mathbb{R}}: G_{\mathbb{R}} \to H_{\mathbb{R}}$ is a surjection.*

The proof follows from Corollary 2, applied to the action $G \times H \to H$ given by $(g, h) \mapsto f(g)h$. The connectedness of the set of $\mathbb{R}$-points of a unipotent group H follows from the fact that the "truncated" logarithmic map defines a homeomorphism between $H_{\mathbb{R}}$ and $L(H)_{\mathbb{R}}$, where $L(H)$ is the Lie algebra of H (cf. §2.1.8).

The subsequent results in this section are aimed at a more precise analysis of the algebraic and topological structure of the groups of real and complex points of reductive algebraic groups. Namely, we wish to obtain the polar decomposition and the Iwasawa decomposition for such groups. To elucidate the matter let us start by considering the simplest case, $\mathbf{GL}_n$. In this case the decompositions under discussion follow easily from well-known facts of linear algebra.

We begin with the polar decomposition of $GL_n(\mathbb{R})$. Let $\mathbf{K}$ designate the subgroup of $GL_n(\mathbb{R})$ consisting of orthogonal matrices, i.e., of matrices x in $GL_n(\mathbb{R})$ satisfying

$$ {}^t x x = E_n, \tag{3.5}$$

where ${}^t x$ is the matrix transpose of x. Clearly $\mathbf{K}$ coincides with the group of $\mathbb{R}$-points $O_n(f)_{\mathbb{R}}$ of the orthogonal group of the standard quadratic form $f = x_1^2 + \cdots + x_n^2$. This form is anisotropic over $\mathbb{R}$, and therefore $O_n(f)$ is also $\mathbb{R}$-anisotropic (cf. Proposition 2.14). But then it follows from Theorem 3.1 that $\mathbf{K} = O_n(f)_{\mathbb{R}}$ is compact. The latter is also easily shown directly by writing out the relations arising from (3.5) in terms of the entries of x. Furthermore, let S denote the set of positive definite symmetric matrices of $GL_n(\mathbb{R})$, i.e., $a = (a_{ij}) \in S$ if $a_{ij} = a_{ji}$ and the quadratic form $f = \sum_{i,j=1}^n a_{ij} x_i x_j$ is positive definite. With this notation, we have

PROPOSITION 3.7. *$GL_n(\mathbb{R}) = \mathbf{K}S$, and for any matrix its factorization on the right is unique. S is connected and simply connected.*

PROOF: Let $x \in GL_n(\mathbb{R})$. Then $a = {}^t x x \in S$, which means that the eigenvalues $\alpha_1, \ldots, \alpha_n$ of a are real and positive. It is well known from linear algebra that there exists b in $\mathbf{K}$ such that bab^{-1} is the diagonal matrix $\operatorname{diag}(\alpha_1, \ldots, \alpha_n)$. Let c denote the matrix $b^{-1} d b$, where $d = \operatorname{diag}(\sqrt{\alpha_1}, \ldots, \sqrt{\alpha_n})$ (taking positive square roots). Then $c \in S$ and ${}^t c c = c^2 = a$. Thus $a = {}^t x x = {}^t c c$, whence ${}^t(x c^{-1})(x c^{-1}) = e_n$, i.e., $z = x c^{-1} \in \mathbf{K}$. Hence $x = zc \in \mathbf{K}S$. If $x = z_1 c_1$ is another such factorization, then applying the transpose to

$$ zc = z_1 c_1 \tag{3.6}$$

we obtain

$$ c z^{-1} = c_1 z_1^{-1}. \tag{3.7}$$

Multiplying (3.6) by (3.7) we have

$$ c^2 = c_1^2, $$

from which it follows that $c = c_1$. There are various ways to prove this, but we prefer to use the following assertion, to which we shall return repeatedly.

LEMMA 3.3. *Let $c \in S$. Then for any integer r the Zariski closure of the cyclic subgroup generated by c^r contains c.*

PROOF: As we have already noted, c can be brought to diagonal form by conjugation, so to begin with we may assume c to be diagonal, i.e., $c = \operatorname{diag}(\gamma_1, \ldots, \gamma_n)$, $\gamma_i > 0$. If $c \notin \overline{\{c^{rn}\}}_{n \in \mathbb{Z}}$, then one can find a character χ of the group of diagonal matrices D_n such that $\chi(c^r) = 1$, but $\chi(c) \neq 1$ (cf. Borel [8]). However $\chi(c) = \gamma_1^{a_1} \ldots \gamma_n^{a_n}$ for suitable integers a_i, and therefore $\chi(c) \in \mathbb{R}^+$. Since $\chi(c^r) = (\chi(c))^r = 1$, it follows that $\chi(c) = 1$, contradiction; and the lemma is proved.

It follows from Lemma 3.3 that the elements c, c_1 in S satisfying $c^2 = c_1^2$ must commute. Then, for $d = c c_1^{-1}$ we have $d^2 = E_n$, so the eigenvalues of d are equal to ± 1. But any eigenvalue of d is a product of the eigenvalues of c and c_1^{-1} and therefore must be positive. Thus $d = E_n$, $c = c_1$ and $z = z_1$, proving the uniqueness of the factorization.

It remains for us to show that S is connected and simply connected. To do so we shall use a method which we shall apply later to an arbitrary reductive group; namely, we shall show that the exponential map induces a homeomorphism from the vector space $\mathfrak{s}$ of symmetric matrices to S. Indeed, it follows from (3.1) that $\exp(X) \in S$ for any matrix X in $\mathfrak{s}$. (It is well known that (3.1) is a convergent series.) Bringing elements of S to diagonal form and using (3.2), we see easily that $\exp: \mathfrak{s} \to S$ is surjective. Furthermore, using the Inverse Function Theorem, it is easy to show that the exponential map actually yields a locally analytic isomorphism of $\mathfrak{s}$ and S. Thus it remains to be shown that exp is injective.

Note that arguing as above one can establish that if c_1, $c_2 \in S$ and $c_1^m = c_2^m$ for some integer m, then $c_1 = c_2$. Hence, from $\exp(X) = \exp(Y)$ for X, Y in $\mathfrak{s}$ it follows that

$$ \exp\left(\frac{1}{m} X\right) = \exp\left(\frac{1}{m} Y\right), $$

for any integer m. Choosing m to be sufficiently large, we can have $\frac{1}{m}X$ and $\frac{1}{m}Y$ arbitrarily close to 0. Then, since exp is a local isomorphism, we have $\frac{1}{m}X = \frac{1}{m}Y$, whence $X = Y$, as required. This completes the proof of Proposition 3.7.

Proposition 3.7 also has the following complex analog. Let $\mathbf{B}$ denote the subgroup of unitary matrices of $GL_n(\mathbb{C})$, i.e., of matrices satisfying ${}^*xx = E_n$, where ${}^*x$ is the conjugate transpose of x. Writing this relation in standard coordinates, we see easily that $\mathbf{B}$ is compact. Let E be the set of positive definite Hermitian matrices, i.e., $a = (a_{ij}) \in E$ if $a_{ij} = \bar{a}_{ji}$ (complex conjugation) and the Hermitian form $f = \sum a_{ij}\bar{x}_i x_j$ is positive definite. Then we have

PROPOSITION 3.8. *$GL_n(\mathbb{C}) = \mathbf{B}E$ and for any matrix its factorization on the right is unique. E is a connected and simply connected space.*

The proof is similar to the proof of Proposition 3.7 and makes use of the following generalization of Lemma 3.3:

LEMMA 3.4. *Let $e \in E$. Then for any integer r the Zariski closure of the subgroup generated by e^r contains e.*

E can be shown to be connected and simply connected as follows. Let $\mathfrak{e}$ denote the space of the Hermitian matrices in $M_n(\mathbb{C})$. Then the exponential map yields a homeomorphism between $\mathfrak{e}$ and E.

The decompositions in Propositions 3.7 and 3.8 are called the *polar decompositions*. We shall establish the existence and uniqueness of the analogous decompositions for an arbitrary reductive $\mathbb{R}$-subgroup $G \subset GL_n(\mathbb{C})$. To do so we must learn to make G well-situated in $GL_n(\mathbb{C})$. More precisely, we say that a subgroup $G \subset GL_n(\mathbb{C})$ is *self-adjoint* if it is invariant relative to the matrix transpose, i.e., if $x \in G$ then ${}^t x \in G$.

THEOREM 3.7 (MOSTOW). *Let $G \subset GL_n(\mathbb{C})$ be a reductive algebraic $\mathbb{R}$-group. There exists a matrix $a \in GL_n(\mathbb{R})$ such that $a^{-1}Ga$ is self-adjoint.*

The proof is based on the following result.

PROPOSITION 3.9. *Let $G \subset GL_n(\mathbb{C})$ be a reductive algebraic $\mathbb{R}$-group. Then there exists a Zariski-dense compact subgroup $\mathbf{K} \subset G$ which is invariant under complex conjugation.*

PROOF OF THEOREM 3.7: Suppose we know the proposition to hold, i.e., let $\mathbf{K} \subset G$ be a Zariski-dense compact subgroup which is invariant under complex conjugation. Put

$$\mathfrak{m} = \int_{\mathbf{K}} {}^*kkdk, \tag{3.8}$$

where the matrix integral is taken with respect to the Haar measure dk of $\mathbf{K}$ (cf. §3.5). Since $\mathbf{K}$ is invariant under complex conjugation, dk is also invariant, from which it follows that $\mathfrak{m}$ is real. Moreover, ${}^*kk$ is positive definite Hermitian, and therefore $\mathfrak{m}$ is actually a symmetric positive definite matrix. In the beginning of the proof of Proposition 3.7 we showed that $\mathfrak{m} = a^2$ for a suitable symmetric positive definite matrix a. It follows from (3.8) that $\mathbf{K}$ lies in the group of matrices which are unitary with respect to $\mathfrak{m}$, and therefore $a^{-1}\mathbf{K}a$ lies in the group $\mathbf{B}$ of usual unitary matrices, i.e., ${}^*xx = e_n$ for x in $a^{-1}\mathbf{K}a$. Thus ${}^t x = {}^*\bar{x} = \bar{x}^{-1} \in a^{-1}\mathbf{K}a$ for any x in $a^{-1}\mathbf{K}a$, where bar denotes complex conjugation. We have shown that $a^{-1}\mathbf{K}a$ is invariant under transpose. Therefore its Zariski closure, $a^{-1}Ga$, has the same property. This completes the proof of Theorem 3.7.

PROOF OF PROPOSITION 3.9: G can be written as an almost direct product $G = TD$, where T is a central $\mathbb{R}$-torus and D is a semisimple group. In case $G = T$, the existence of the required subgroup is clear; indeed, having chosen a $\mathbb{C}$-isomorphism $T \simeq \mathbb{C}^{*d}$, we can take $\mathbf{K}$ to be the subgroup S^d, where S is the set of complex numbers with absolute value 1. This subgroup is the unique maximal compact subgroup of T and therefore is invariant relative to all continuous automorphisms of $\mathbb{C}^*$. If we can construct a subgroup $\mathbf{K}_1 \subset D$ having the desired property, then $\mathbf{K}_0 = \mathbf{K}\mathbf{K}_1$ will be the desired subgroup of G. Thus in what follows we may assume G to be semisimple.

We choose a maximal $\mathbb{R}$-torus $T \subset G$; let $R = R(T, G)$ be the root system of G relative to T, and let $\{X_\alpha\}_{\alpha \in R}$ be the elements of the corresponding Chevalley base in the Lie algebra $L(G)$ (cf. §2.1.13). If we write σ for the involution arising from complex conjugation, then $\sigma(X_\alpha) = c_\alpha X_{\bar{\alpha}}$, where $c_\alpha \in \mathbb{C}$ and $\bar{\alpha}$ is the character of T conjugate to α. Put $\tau(X_\alpha) = |c_\alpha| X_{-\alpha}$, where $|c_\alpha|$ is the absolute value of c_α. Straightforward computation, using the structural relations for a Chevalley base, shows (cf. *Theory of Lie Algebras. Topology of Lie Groups*, (Sophus Lie Seminar), pp. 145–146), that τ extends to an involution of $L(G)$ which commutes with σ. Let f denote the Killing form on $L(G)$ (cf. §2.1.3). By direct computation it is easy to establish (*loc. cit.*) that $f(X, \tau(X)) < 0$ for any $X \neq 0$ in $L(G)$. Therefore, if we let $\mathfrak{h}$ designate the fixed subspace (actually, $\mathbb{R}$-subalgebra) of $L(G)$ under τ, then $f(X, X) = f(X, \tau(X))$ on $\mathfrak{h}$ is a negative definite form. Let $\mathbf{K}$ be the subgroup of those g in G for which $\operatorname{Ad} g$ leaves $\mathfrak{h}$ invariant. Using the $\operatorname{Ad} g$ invariance of f and the fact that $\mathfrak{h} \otimes_{\mathbb{R}} \mathbb{C} = L(G)$, we see easily that $\operatorname{Ad}\mathbf{K}$ is a closed subgroup of the group $\mathbf{O}(g)_{\mathbb{R}}$, the orthogonal group of the form $g = f\,|_{\mathfrak{h}}$. Since g is negative definite, $\mathbf{O}(g)_{\mathbb{R}}$ is compact. Therefore $\mathbf{K}$ is also compact, since Ad has finite kernel. Furthermore, since $\mathfrak{h}$ is a subalgebra, $\exp X \in \mathbf{K}$ for any X in $\mathfrak{h}$. But $\frac{d}{dt}(\exp(tX))_{t=0} = X$, so the Lie algebra of $\mathbf{K}$ contains $\mathfrak{h}$ (note that $\mathbf{K}$ is a Lie group over $\mathbb{R}$ by Theo-

rem 3.1). Therefore, it follows from Lemma 3.1 that the Lie algebra of the closure $\bar{\mathbf{K}}$ of $\mathbf{K}$ in the Zariski topology must contain $\mathbb{C}\mathfrak{h} = L(G)$, whence $\bar{\mathbf{K}} = G$. Lastly, since σ and τ commute, it follows that $\mathfrak{h}$ is σ-invariant and therefore $\mathbf{K}$ is also σ-invariant. Q.E.D.

REMARK: Proposition 3.9 relies on the technical tool generally known as *Weyl's unitary trick*; namely, when working with algebraic groups over fields of characteristic 0, first we reduce the problem to $\mathbb{C}$, then we work with the algebraic group's dense compact subgroup, not with the algebraic group itself. In such a manner it is easy, for example, to establish the complete reducibility of representations of reductive algebraic groups in characteristic 0.

We are now in a position to construct the *polar decomposition* for an arbitrary reductive $\mathbb{R}$-group G. Let $G \subset GL_n(\mathbb{C})$ be a matrix realization of G. Without loss of generality, we may assume G to be self-adjoint by Theorem 3.7. In this case the polar decomposition of $GL_n(\mathbb{R})$ (Proposition 3.7) will yield the polar decomposition of $G_{\mathbb{R}}$.

More precisely, we have

PROPOSITION 3.10.

(1) *Notation as in Proposition 3.7,* $G_{\mathbb{R}} = (G \cap \mathbf{K})(G \cap S)$. *Furthermore* $\mathbf{K}_1 = G \cap \mathbf{K}$ *is a maximal compact subgroup of* $G_{\mathbb{R}}$ *and* $S_1 = G \cap S$ *is a connected and simply connected space. Consequently* $G_{\mathbb{R}}/\mathbf{K}_1$ *is connected and simply connected.*

(2) *Any compact subgroup of* $G_{\mathbb{R}}$ *is contained in a maximal compact subgroup, and all maximal compact subgroups of* $G_{\mathbb{R}}$ *are conjugate.*

PROOF: 1) Let $x \in G_{\mathbb{R}}$ and let $x = kc$ be the polar decomposition in $GL_n(\mathbb{R})$; we shall show that $k \in \mathbf{K}_1$, $c \in S_1$. Since G is self-adjoint, ${}^t x \in G$; consequently $c^2 = {}^t x x \in G$. Applying Lemma 3.3 we obtain $c \in G$, i.e., $c \in S_1$. Thus also $k \in \mathbf{K}_1$. Any subgroup of $G_{\mathbb{R}}$ strictly containing $\mathbf{K}_1$ must contain a nonidentity element of S_1. But since any element of S is conjugate to a diagonal matrix with positive entries, it follows that a nonidentity element of S cannot be contained in a compact subgroup. Thus $\mathbf{K}_1$ is maximal compact. To prove S_1 is connected and simply connected we shall use the same method as in the proof of Proposition 3.7. Let $\mathfrak{s}_1$ designate the subspace of symmetric matrices in the Lie algebra $\mathfrak{g}^*$ of $G_{\mathbb{R}}$. We shall show that the exponential map induces a homeomorphism between $\mathfrak{s}_1$ and S. In the proof of Proposition 3.7 we established that exp induces a homeomorphism from $\mathfrak{s}$ to S; therefore it suffices to show that $\exp(\mathfrak{s}_1) = S_1$. Obviously $\exp(\mathfrak{s}_1) \subset S_1$. Now let $c = \exp X \in S_1$, where $X \in \mathfrak{s}$. It follows from Lemma 3.3 that $\exp(\frac{1}{n}X)$ also lies in S_1, for any

integer n. Therefore $\exp(\mathbb{Q}X) \subset S_1$ and hence $\exp(tX) \in S_1$ for any t in $\mathbb{R}$. But then

$$X = \frac{d}{dt}(\exp(tX))_{t=0} \in \mathfrak{g}^* \cap \mathfrak{s} = \mathfrak{s}_1,$$

as required.

2) The proof, the details of which we omit (cf. Helgason [1]), is along the following lines. The space $X = G_{\mathbb{R}}/\mathbf{K}_1$ is provided with a $G_{\mathbb{R}}$-invariant metric, relative to which it becomes a Riemannian variety of negative curvature. Then, we apply a result of Cartan, according to which any compact subgroup acting by isometries on such a variety must have a fixed point. Thus, if $\mathbf{K}' \subset G_{\mathbb{R}}$ is a compact subgroup, there exists a point $x = g\mathbf{K}_1 \in X$ which is fixed under $\mathbf{K}'$. This means $g^{-1}\mathbf{K}'g \subset \mathbf{K}_1$, thereby yielding the desired result and completing the proof of Proposition 3.10.

We shall also need a complex variant of Proposition 3.10. As before, we assume the given reductive group G to be self-adjoint.

PROPOSITION 3.11.

(1) *Notation as in Proposition 3.8,* $G_{\mathbb{C}} = (G \cap \mathbf{B})(G \cap E)$. *Furthermore* $\mathbf{B}_1 = G \cap \mathbf{B}$ *is a maximal compact subgroup of* $G_{\mathbb{C}}$, *and* exp *yields a homeomorphism from the space* $\mathfrak{e}_1$ *of Hermitian matrices of the Lie algebra* $L(G)$ *to* $E_1 = G \cap E$.

(2) *Any compact subgroup of* $G_{\mathbb{C}}$ *is contained in a maximal compact subgroup, and all maximal compact subgroups are conjugate.*

The proof is analogous to the proof of Proposition 3.10. (Actually Proposition 3.11 could then be deduced from Proposition 3.10 using restriction of scalars.)

We mention one more helpful technical assertion.

LEMMA 3.5. *If* $b \in \mathbf{B}$, $e \in E$ *and* $e^{-1}be \in \mathbf{B}$, *then* $eb = be$.

PROOF: We have ${}^*x = x^{-1}$ for x in $\mathbf{B}$, and ${}^*x = x$ for x in E. Therefore ${}^*(e^{-1}be)^{-1} = e^{-1}be = ebe^{-1}$, i.e., b and e^2 commute. The rest follows from Lemma 3.4.

Now we are in a position to prove the following generalization of Theorem 3.7.

THEOREM 3.8 (MOSTOW). *Let* $G_1 \subset \ldots \subset G_r$ *be a tower of reductive* $\mathbb{R}$*-subgroups of* $GL_n(\mathbb{C})$. *Then there exists a matrix* $a \in GL_n(\mathbb{R})$ *such that all* aG_ia^{-1} *are self-adjoint.*

PROOF: Examining the proof of Theorem 3.7, we see that it suffices to find maximal compact subgroups $\mathbf{K}_i \subset G_{i\mathbb{C}}$ which are Zariski-dense in G_i,

invariant under complex conjugation, and satisfy $\mathbf{K}_1 \subset \ldots \subset \mathbf{K}_r$. Moreover, everything reduces to proving the following assertion for two $\mathbb{R}$-groups $H \subset G$: any maximal compact subgroup $B \subset H_{\mathbb{C}}$ which is invariant under complex conjugation is contained in a maximal compact subgroup $C \subset G_{\mathbb{C}}$ which is also invariant under conjugation. (Since by Proposition 3.9 there exists a Zariski-dense maximal compact subgroup, then any maximal compact subgroup is automatically Zariski-dense.)

Choose a maximal compact subgroup $D \subset G_{\mathbb{C}}$ containing B. It follows from Proposition 3.11 that there exists a unique decomposition $G_{\mathbb{C}} = DF$, where $F = \exp(\mathfrak{f})$ and $\mathfrak{f}$ is an $\mathbb{R}$-subspace of $L(G)$. Let θ denote the automorphism arising from complex conjugation. Then $\theta(D)$ is also a maximal compact subgroup of $G_{\mathbb{C}}$ and therefore $\theta(D) = a^{-1}Da$ for suitable $a = \exp(X)$, $X \in \mathfrak{f}$. Put $b = \exp(\frac{X}{2})$ and, and note $b^2 = a$. We shall show that $C = b^{-1}Db$ is the required group. We have

$$\theta(C) = \theta(b)^{-1}\theta(D)\theta(b) = \theta(b)^{-1}a^{-1}Da\theta(b) = (\theta(b)^{-1}a^{-1}b)C(b^{-1}a\theta(b)).$$

Thus to prove that C is θ-invariant it suffices to show that $b^{-1}a\theta(b)$ lies in the center Z of $G_{\mathbb{C}}$, i.e.,

$$b\theta(b)^{-1} = az, \quad \text{for } z \in Z. \tag{3.9}$$

Since $\theta^2 = \mathrm{id}$,

$$D = \theta^2(D) = \theta(a^{-1}Da) = \theta(a)^{-1}a^{-1}Da\theta(a).$$

Write $a\theta(a) = df$, where $d \in D$ and $f \in F$. Then $f^{-1}Df = D$ and therefore f commutes with D, by Lemma 3.5; since D is Zariski-dense in G, we have $f \in Z$. Let α denote the automorphism of G which is the composite of θ and conjugation by a. Then D is α-invariant; hence F is also α-invariant. (It suffices to use $F = \exp(\mathfrak{f})$ and the property that $\mathfrak{f}$ is the orthogonal complement of $L(D)$ (viewing D as a real Lie group) in $L(G)$, under the Killing form.) Therefore $a\theta(a)a^{-1} \in F$. But $a\theta(a)a^{-1} = dfa^{-1}$; moreover if $f = \exp(Y)$, then $fa^{-1} = \exp(Y - X) \in F$, since $f \in Z$. It follows that $d = 1$ so $a\theta(a) = f$.

Now we compute $\theta(b)$. Put $t = a\theta(b)a^{-1}$. Since $t \in F$, we have $t = \exp(T)$, where $T \in \mathfrak{f}$, implying

$$t^2 = a\theta(a)a^{-1} = \exp(2T) = fa^{-1} = \exp(Y - X),$$

whence $T = \frac{Y-X}{2}$. Therefore T commutes with X, so t commutes with a and $\theta(b) = t = \exp(\frac{Y-X}{2})$. It follows that b commutes with $\theta(b)$ and

$$b\theta(b)^{-1} = \exp(\frac{X}{2} - \frac{Y-X}{2}) = \exp(X - \frac{Y}{2}) = a\exp(-\frac{Y}{2}),$$

so $z = \exp(-\frac{Y}{2}) \in Z$, as required.

It remains to be shown that $B \subset C$. We have $B = \theta(B) \subset \theta(D) = a^{-1}Da$, whence $aBa^{-1} \subset D$. Thus a commutes with B, by Lemma 3.5. Since $b^2 = a$, it follows from Lemma 3.4 that b and B commute. Finally, $B = b^{-1}Bb \subset C$. Q.E.D.

We move on to our last topic—the Iwasawa decomposition, the essence of which is as follows: Let G be a reductive group defined over $\mathbb{R}$, and let $H \subset G$ be a maximal connected solvable $\mathbb{R}$-split subgroup. $G_{\mathbb{R}}/H_{\mathbb{R}}$ is compact, by Theorem 3.1, so $H_{\mathbb{R}}$ has a compact complement in $G_{\mathbb{R}}$. The Iwasawa decomposition asserts that the complement actually can be taken to be a suitable maximal compact subgroup. Moreover, if instead of $H_{\mathbb{R}}$ we consider its connected component of the identity, then the components of the corresponding decomposition are uniquely determined. Thus $G_{\mathbb{R}}$ differs from a compact group by some solvable group. As usual, first we shall prove the Iwasawa decomposition for $GL_n(\mathbb{R})$. To do so, let $\mathbf{K}$ designate the subgroup of orthogonal matrices of $GL_n(\mathbb{R})$, and let A and U be subgroups of $GL_n(\mathbb{R})$ consisting respectively of the diagonal matrices with positive coefficients and the upper triangular unipotent matrices.

PROPOSITION 3.12 (IWASAWA DECOMPOSITION FOR $GL_n(\mathbb{R})$). *The natural map $\varphi: \mathbf{K} \times A \times U \to GL_n(\mathbb{R})$, given by $\varphi(k, a, u) = kau$, is a homeomorphism.*

PROOF: Fix an orthonormal base $e = (e_1, \ldots, e_n)$ of the space $\mathbb{R}^n$ and let $g \in GL_n(\mathbb{R})$. Applying the classical Gram-Schmidt orthogonalization procedure, we obtain an orthonormal base $d = (d_1, \ldots, d_n)$ of $\mathbb{R}^n$ such that $d_1 = \beta_{11}ge_1$, $d_2 = \beta_{12}ge_1 + \beta_{22}ge_2$, $\ldots$, $d_n = \beta_{1n}ge_1 + \cdots + \beta_{nn}ge_n$, where $\beta_{ii} > 0$. Let b denote

$$\begin{pmatrix} \beta_{11} & \ldots & \beta_{1n} \\ \vdots & \ddots & \vdots \\ 0 & \ldots & \beta_{nn} \end{pmatrix} \in B = AU,$$

and let k be the change of base matrix from base e to base d. Then clearly $g = kb^{-1}$, k is an orthogonal matrix, and b^{-1} belongs to B. Thus φ is surjective. $\mathbf{K}$ is defined by ${}^t xx = E_n$, whence $\mathbf{K} \cap B = \{E_n\}$. In view of the fact that B is a group and $B = AU$ is a semi-direct product (as topological groups), we see that φ is a continuous bijection. That the inverse map is continuous follows easily from the compactness of $\mathbf{K}$. Indeed, if the elements $g_m = k_m a_m u_m \underset{m\to\infty}{\longrightarrow} g = kau$ $(k, k_m \in \mathbf{K};\ a, a_m \in A;\ u, u_m \in U)$, then by the compactness of $\mathbf{K}$ we may assume $k_m \underset{m\to\infty}{\longrightarrow} k' \in \mathbf{K}$. Then $b_m = a_m u_m \underset{m\to\infty}{\longrightarrow} b' = a'u' \in B$, since B is closed. Thus $g = k'a'u'$,

whence $k' = k$, $a' = a$, $u' = u$, i.e.,

$$k_m \underset{m\to\infty}{\longrightarrow} k, \quad a_m \underset{m\to\infty}{\longrightarrow} a, \quad u_m \underset{m\to\infty}{\longrightarrow} u,$$

as required. Q.E.D.

The presentation of an element g in $GL_n(\mathbb{R})$ in the form $g = k_g a_g u_g$, where $k_g \in \mathbf{K}$, $a_g \in A$, and $u_g \in U$, is called the *Iwasawa decomposition* of g, and the elements k_g, a_g and u_g are its $\mathbf{K}$-, A- and U-components, respectively. Our objective is to construct a similar decomposition inside an arbitrary reductive $\mathbb{R}$-subgroup $G \subset GL_n(\mathbb{C})$. More precisely, we shall show that, passing from G to a suitable conjugate group, we may ensure that for $g \in G_{\mathbb{R}}$ the components of its Iwasawa decomposition in $GL_n(\mathbb{R})$ also belong to $G_{\mathbb{R}}$. From the outset we may assume G to be self-adjoint, by Theorem 3.7. Then $L(G)$ is invariant under transpose, too. Let $\mathfrak{h}$ (respectively, $\mathfrak{p}$) denote the subspace of skew-symmetric (resp., symmetric) matrices in $\mathfrak{g} = L(G)_{\mathbb{R}}$; clearly $\mathfrak{g} = \mathfrak{h} \oplus \mathfrak{p}$ (this is the infinitesimal analog of the polar decomposition in Proposition 3.10). Let $\mathfrak{a}$ denote a maximal abelian subspace of $\mathfrak{p}$.

LEMMA 3.6. *There exists an $\mathbb{R}$-split torus $T \subset G$ such that $\mathfrak{a} = L(T)_{\mathbb{R}}$. Moreover, T consists of symmetric matrices.*

PROOF: Let T denote the connected component of the Zariski closure of the set $\exp(\mathfrak{a})$. Since any element from $\mathfrak{p}$ is diagonalizable over $\mathbb{R}$ and $\mathfrak{a}$ is an abelian subalgebra of $\mathfrak{g}$, we see $\mathfrak{a}$ is diagonalizable over $\mathbb{R}$, from which it follows that T is a subtorus of G split over $\mathbb{R}$. By construction $\mathfrak{a}$ consists of symmetric matrices; therefore the same is true for $\exp(\mathfrak{a})$, and consequently also for T.

Therefore $L(T)_{\mathbb{R}} \subset \mathfrak{p}$ and commutes with $\mathfrak{a}$, so in fact $L(T)_{\mathbb{R}} = \mathfrak{a}$. Q.E.D.

By construction $T_{\mathbb{R}}$ consists of symmetric matrices, implying $bT_{\mathbb{R}}b^{-1}$ is contained in the group of diagonal matrices D_n, for suitable b in $\mathbf{K}$; thus $bTb^{-1} \subset D_n$. Passing from G to bGb^{-1}, which remains self-adjoint since $b \in \mathbf{K}$, we may assume $T \subset D_n$. Let $R = \{\alpha\}$ denote the set of nonzero weights of T in the adjoint representation on $L(G)$. Since T is $\mathbb{R}$-split, all α are defined over $\mathbb{R}$ and we have the $\mathbb{R}$-decomposition

$$L(G) = L(G)^T \oplus (\oplus_{\alpha\in R}\mathfrak{u}_\alpha), \tag{3.10}$$

where $L(G)^T$ is the centralizer of T and $\mathfrak{u}_\alpha$ is the eigenspace of α. Choose any ordering on $V = \mathbf{X}(T) \otimes_{\mathbb{Z}} \mathbb{R}$, where $\mathbf{X}(T)$ is the character group of T. It is easy to see that there exists an ordering on $V_0 = \mathbf{X}(D_n) \otimes_{\mathbb{Z}} \mathbb{R}$ such that the natural projection $V_0 \to V$, which extends the homomorphism

$\mathbf{X}(D_n) \to \mathbf{X}(T)$ corresponding to $T \subset D_n$, takes positive roots to positive elements. Let R_0 be the root system of $GL_n(\mathbb{C})$ relative to D_n (explicitly $R_0 = \{\varepsilon_i - \varepsilon_j : i,j = 1,\dots,n;\ i \neq j\}$, where $\varepsilon_i(\mathrm{diag}(a_1,\dots,a_n)) = a_i$), and let $\Pi \subset R_0$ be a simple system of roots with respect to V_0 (cf. Bourbaki [4, Ch. 6]). It is well known that the Weyl group $W(R_0)$ contains an element w such that $w\Pi$ coincides with the standard set of simple roots $\Pi_0 = \{\varepsilon_i - \varepsilon_{i+1} : i = 1,\dots,n-1\}$. But $W(R_0)$ is naturally isomorphic to W, the group of permutation matrices. Thus there is c in W for which, taking $T' = cTc^{-1}$, we have an ordering on $\mathbf{X}(T') \otimes_{\mathbb{Z}} \mathbb{R}$ such that the positive roots of $GL_n(\mathbb{C})$ remain positive under restriction to T'. Passing from G to cGc^{-1}, we may assume that this is also true of T (note that $W \subset \mathbf{K}$ and therefore cGc^{-1} remains self-adjoint). Let R_+ be the set of weights of R that are positive under the specified ordering on V. Put $\mathfrak{u} = \sum_{\alpha\in R_+} \mathfrak{u}_\alpha$.

LEMMA 3.7. *$\mathfrak{u}$ is a Lie $\mathbb{R}$-subalgebra of $L(G)$ normalized by T and contained in the algebra of all the upper triangular nilpotent matrices $\mathfrak{u}_n$.*

PROOF: Clearly T normalizes $\mathfrak{u}$, and for $\alpha, \beta \in R_+$ we have

$$[\mathfrak{u}_\alpha, \mathfrak{u}_\beta] = \begin{cases} 0, & \text{if } \alpha+\beta \notin R_+; \\ \mathfrak{u}_{\alpha+\beta}, & \text{if } \alpha+\beta \in R_+. \end{cases}$$

It follows that $\mathfrak{u}$ is a subalgebra. Since $\mathfrak{u}_\alpha$ is defined over $\mathbb{R}$, $\mathfrak{u}$ also is defined over $\mathbb{R}$. To prove $\mathfrak{u} \subset \mathfrak{u}_n$ it suffices to show that $\mathfrak{u}_\alpha \subset \mathfrak{u}_n$ for each α in R_+. If $X = (x_{ij}) \in \mathfrak{u}_\alpha$ and $x_{ij} \neq 0$ for some $i \geq j$, then the restriction to T of $\varepsilon_i - \varepsilon_j$ of D_n is α. $i = j$ is impossible, since it implies $\alpha = 0$. Thus $\varepsilon_j - \varepsilon_i$ is negative with respect to the ordering on V_0, therefore by construction its projection on V (which coincides with α) must also be negative, contradiction; and the lemma is proved.

By a straightforward argument (cf., for example, Borel [8, §7]) we can establish the existence of a unipotent $\mathbb{R}$-subgroup U of G whose Lie algebra is $\mathfrak{u}$. (Actually $U = \exp(\mathfrak{u})$, where exp is taken to be the "truncated" exponential map, cf. §2.1.8, and $U_{\mathbb{R}} = \exp(\mathfrak{u}_{\mathbb{R}})$.) Clearly U is normalized by T and is contained in the group of upper triangular unipotent matrices U_n. Furthermore, let A_1 denote the connected component of $T_{\mathbb{R}}$ and put $\mathbf{K}_1 = G \cap \mathbf{K}$.

THEOREM 3.9 (IWASAWA DECOMPOSITION). *The natural map*

$$\theta: \mathbf{K}_1 \times A_1 \times U_{\mathbb{R}} \to G_{\mathbb{R}}$$

is a homeomorphism.

PROOF: First we establish the infinitesimal analog of the Iwasawa decomposition:

$$\mathfrak{g} = \mathfrak{h} \oplus \mathfrak{a} \oplus \mathfrak{u}_{\mathbb{R}}, \tag{3.11}$$

notation as above. Let τ denote the automorphism of $\mathfrak{gl}_n$ given by $\tau(X) = -{}^tX$ for X in $\mathfrak{gl}_n$. By construction τ induces an automorphism of $\mathfrak{g}$, moreover, $\mathfrak{h}$ is precisely the subalgebra $\mathfrak{g}^\tau$ of fixed points and $\tau(X) = -X$ for X in $\mathfrak{a}$. It follows that $\tau(\mathfrak{u}_\alpha) = \mathfrak{u}_{-\alpha}$ for any α in R. Let $X \in (\mathfrak{u}_{-\alpha})_{\mathbb{R}}$ and write $X = \tau(Y)$, where $Y \in (\mathfrak{u}_\alpha)_{\mathbb{R}}$. Then

$$X = (\tau Y + Y) - Y \in \mathfrak{h} \oplus \mathfrak{a}_{\mathbb{R}}.$$

In view of (3.10), we see that to prove $\mathfrak{g} = \mathfrak{h} + \mathfrak{a} + \mathfrak{u}_{\mathbb{R}}$ we have only to establish that the right side of (3.11) contains the subalgebra $\mathfrak{c} = L(G)^\top_{\mathbb{R}}$ which is the centralizer of $\mathfrak{a}$ in $\mathfrak{g}$. Since $\mathfrak{a}$ is invariant under τ, then so is $\mathfrak{c}$. Any element X in $\mathfrak{c}$ can be written as

$$X = \frac{1}{2}(X + \tau X) + \frac{1}{2}(X - \tau X),$$

where $\frac{1}{2}(X + \tau X) \in \mathfrak{h}$. But $\frac{1}{2}(X - \tau X) \in \mathfrak{p}$ and centralizes $\mathfrak{a}$. Therefore actually $\frac{1}{2}(X - \tau X) \in \mathfrak{a}$, yielding $X \in \mathfrak{h} \oplus \mathfrak{a}$. Thus $\mathfrak{g} = \mathfrak{h} + \mathfrak{a} + \mathfrak{u}_{\mathbb{R}}$. If $X + Y + Z = 0$, where $X \in \mathfrak{h}$, $Y \in \mathfrak{a}$ and $Z \in \mathfrak{u}_{\mathbb{R}}$, then by applying τ we obtain

$$X - Y + \tau Z = 0,$$

whence $Y = \frac{1}{2}(-Z + \tau Z) \in \mathfrak{a} \cap (\sum_{\alpha \in R} \mathfrak{u}_\alpha) = (0)$. Therefore $Z = \tau Z \in (\sum_{\alpha \in R_+} \mathfrak{u}_\alpha) \cap (\sum_{\alpha \in R_+} \mathfrak{u}_{-\alpha}) = (0)$, proving (3.11).

By the Inverse Function Theorem (3.2), there exist connected neighborhoods of the identity $V \subset \mathbf{K}_1$ and $W \subset B = A_1 U_{\mathbb{R}}$ such that the product morphism gives a homeomorphism from $V \times W$ to a neighborhood of the identity in $G_{\mathbb{R}}$. This means that we can find connected neighborhoods of the identity $V_1 \subset V$, $W_1 \subset W$ and continuous functions $\varphi\colon V_1 \times W_1 \to \mathbf{K}_1$, $\psi\colon V_1 \times W_1 \to B$ such that

$$bk = \varphi(b,k)\psi(b,k)$$

for all k in V_1 and b in W_1. By induction it is easy to show that for any set $S = \{k_1, \ldots, k_p\}$ of elements from V_1 we can find a connected neighborhood of the identity $W(S) \subset W_1$ and continuous functions

$$\varphi^S\colon V_1 \times W(S) \to \mathbf{K}_1, \quad \psi^S\colon V_1 \times W(S) \to B,$$

such that

$$bk(S)k = \varphi^S(b,k)\psi^S(b,k)$$

for all k in V_1 and v in $W(S)$, where $k(S) = k_1 \ldots k_p$. V_1 generates the connected component $\mathbf{K}_1^0$ of $\mathbf{K}_1$; therefore the compactness of $\mathbf{K}$ implies the existence of a finite number of sets S, such that $\mathbf{K}_1^0 = \bigcup_S k(S)V_1$. Put $W_2 = \bigcap_S W(S)$. Then $W_2 K_1^0 \subset K_1^0 B$. Since B is a connected group, W_2 generates B and therefore $BK_1^0 = \mathbf{K}_1^0 B$. But $\mathbf{K}_1^0 B$ contains a neighborhood of the identity in $G_{\mathbb{R}}$, and therefore generates the connected component $G_{\mathbb{R}}^0$. Therefore $G_{\mathbb{R}}^0 = \mathbf{K}_1^0 B$. To prove $G_{\mathbb{R}} = \mathbf{K}_1 B$ we need only note that $\mathbf{K}_1 G_{\mathbb{R}}^0 = G_{\mathbb{R}}$, since by Proposition 3.11 $G_{\mathbb{R}} = \mathbf{K}_1 S_1$, where S_1 is a connected set. Thus θ is shown to be surjective.

It follows from our construction that a presentation of $g \in G_{\mathbb{R}}$ in the form $g = kau$, where $k \in \mathbf{K}_1$, $a \in A_1$, $u \in U_{\mathbb{R}}$, is actually its Iwasawa decomposition in $GL_n(\mathbb{R})$. Therefore, since the latter is unique, it follows that θ is bijective. To prove that the inverse map is continuous one argues exactly as in the proof of Proposition 3.13. Q.E.D.

It follows from Theorem 3.9 that $H = TU$ is a maximal connected $\mathbb{R}$-split solvable subgroup of G (and, consequently, T is a maximal $\mathbb{R}$-split torus and U is a maximal unipotent $\mathbb{R}$-subgroup). Indeed, if $H' \supset H$, then by Theorem 3.9 $H'_{\mathbb{R}} = (H' \cap \mathbf{K}_1)H_{\mathbb{R}}$, so $H'_{\mathbb{R}}/H_{\mathbb{R}}$ must be compact, which, as we have seen in the proof of Theorem 3.1, cannot be the case for a connected $\mathbb{R}$-split solvable subgroup H' strictly containing H. As a further corollary (not so much to the theorem as to the argument preceding its proof) we note

PROPOSITION 3.13. *Let $G \subset GL_n(\mathbb{C})$ be a reductive $\mathbb{R}$-group. There exists $a \in GL_n(\mathbb{R})$ such that $H = aGa^{-1}$ satisfies the following:*

(1) *H is self-adjoint;*
(2) *the connected component of the intersection of H with D_n is a maximal $\mathbb{R}$-split torus S in H;*
(3) *there exists an ordering on $V = \mathbf{X}(T) \otimes_{\mathbb{Z}} \mathbb{R}$ such that the restriction of the positive roots $\varepsilon_i - \varepsilon_j$ $(1 \le i < j \le n)$ of $GL_n(\mathbb{C})$ to S are positive with respect to this ordering, and the maximal unipotent $\mathbb{R}$-subgroup corresponding to this ordering lies in the group of upper triangular unipotent matrices U_n;*
(4) *the components in the Iwasawa decomposition in $GL_n(\mathbb{R})$ of any element of $H_{\mathbb{R}}$ lie in $H_{\mathbb{R}}$.*

3.3. The non-Archimedean case.

Throughout this section K denotes a non-Archimedean locally compact field of characteristic 0, i.e., a finite extension of the p-adic number field $\mathbb{Q}_p$.

As we have noted in §3.1, if G is an algebraic group defined over K, then G_K is locally compact and totally disconnected in the p-adic topology. It is well known (cf. Bourbaki [2, Ch. 3, §4]) that such locally compact groups have a base of the neighborhoods of the identity consisting of subgroups. In the case under consideration, they can be described explicitly as the congruence subgroups. Let $G \subset GL_n(\Omega)$ be a matrix realization, let $\mathcal{O}$ be the ring of integers in K, and let $\mathfrak{p}$ be the maximal ideal of $\mathcal{O}$. Then the group of $\mathcal{O}$-points $G_{\mathcal{O}} = G \cap GL_n(\mathcal{O})$ is the "principal" open compact subgroup of G_K (its openness is a consequence of the openness of $\mathcal{O}$ in K, and its compactness follows from the compactness of $GL_n(\mathcal{O})$ since $G_{\mathcal{O}}$ is closed in $GL_n(\mathcal{O})$). The *congruence subgroups* $G_{\mathcal{O}}(\mathfrak{p}^d) \subset G_{\mathcal{O}}$, given by

$$G_{\mathcal{O}}(\mathfrak{p}^d) = \{\, g \in G_{\mathcal{O}} : g \equiv E_n \pmod{\mathfrak{p}^d} \,\}, \quad d > 0,$$

constitute the required base of the neighborhoods of the identity in G_K. Since Lie group theory is less effective here than in the Archimedean case, in order to obtain results on the structure of G_K we shall have to use some other tools.

Several important results, bearing mainly on compact subgroups of G, can be obtained using lattices and orders in semisimple algebras (cf. §1.5.3). If $G \subset GL_n(\Omega)$ is an algebraic K-group and $L \subset K^n$ is a lattice, then throughout the book $G_{\mathcal{O}}^L$ will denote the stabilizer of L in G, i.e.,

$$G_{\mathcal{O}}^L = \{\, g \in G_K : g(L) = L \,\}.$$

(This notation reflects the fact that $G_{\mathcal{O}}^L$ consists of transformations whose matrices with respect to some base of L belong to $GL_n(\mathcal{O})$.)

By Proposition 1.12 any compact subgroup B of $GL_n(K)$ is contained in the stabilizer $G_{\mathcal{O}}^L$ of some lattice $L \subset K^n$. In particular, this means that any compact subgroup of G_K is contained in some open compact subgroup. Moreover, if B is a maximal compact subgroup, then $B = G_{\mathcal{O}}^L$. Another consequence of Proposition 1.12 is that in the case $G = \mathbf{GL}_n$ the same fundamental results hold for maximal compact subgroups as in the Archimedean case: any compact subgroup is contained in some maximal compact subgroup, and all maximal compact subgroups are conjugate. In this regard, it is somewhat surprising that passing from $G = \mathbf{GL}_n$ even to $H = \mathbf{SL}_n$ shatters this harmony.

PROPOSITION 3.14. *Let $H = \mathbf{SL}_n$. Then $H_{\mathcal{O}}^L$ is a maximal compact subgroup of H_K, for any lattice $L \subset K^n$. Any compact subgroup of H_K is contained in some maximal compact subgroup, and the maximal compact subgroups split into n conjugacy classes under H_K.*

PROOF: As an exercise for the reader, we suggest slightly modifying the proof of Propositions 1.11 and 1.12 to establish the maximality of $H_{\mathcal{O}}^L$ for any lattice $L \subset K^n$ and, moreover, to show $H_{\mathcal{O}}^L = H_{\mathcal{O}}^M$ implies that L and M are proportional. To prove the last assertion we construct a surjection φ from the set $\mathcal{B}$ of maximal compact subgroups of $SL_n(K)$ onto K^*/UK^{*n} (where U is the group of v-adic units in K), whose fibers coincide with the conjugacy classes of the maximal compact subgroups. Since the order of K^*/UK^{*n} is n, the desired result follows.

Let us fix some lattice $L \subset K^n$ and let $B \in \mathcal{B}$. Then B has the form $H_{\mathcal{O}}^M$ for a suitable $M \subset K^n$, and then φ is given as follows:

$$\text{If } M = g(L),\ g \in GL_n(K), \text{ then } \varphi(g) = (\det g)UK^{*n}.$$

Since $H_{\mathcal{O}}^{M_1} = H_{\mathcal{O}}^{M_2}$ implies $M_2 = \mu M_1$ for $\mu \in K^*$, clearly φ is well-defined and surjective. Now assume that $\varphi(B_1) = \varphi(B_2)$, where $B_i = H_{\mathcal{O}}^{M_i}$, $M_i \subset K^n$. It follows from the definition of φ that in this case $M_2 = g(M_1)$ for some g in $GL_n(K)$ such that $\det g \in UK^{*n}$, i.e., $\det g = ut^n$ for suitable $u \in U$, $t \in K^*$. Choose an element s from the stabilizer of M_1 satisfying $\det s = u$, and put $h = t^{-1}gs^{-1}$. Then $h \in SL_n(K)$ and $h(M_1) = tM_2$, so $hB_1h^{-1} = H_{\mathcal{O}}^{h(M_1)} = H_{\mathcal{O}}^{M_2} = B_2$, which means that B_1 and B_2 are conjugate in H_K. Conversely, if $B_i = H_{\mathcal{O}}^{M_i}$ $(i = 1,2)$ are conjugate, $B_2 = hB_1h^{-1}$, then $h(M_1)$ and M_2 are proportional lattices, from which it follows easily that $\varphi(B_1) = \varphi(B_2)$. Q.E.D.

The detailed analysis of the properties of maximal compact subgroups in the non-Archimedean case, carried out by Bruhat and Tits [2–4], shows that the last assertion of Proposition 3.14 is a special case of the following general result: if G is a simply connected simple K-group of K-rank l, then G_K has exactly $(l+1)$ conjugacy classes of maximal compact subgroups. We shall set forth some results of Bruhat-Tits' theory in the next section, but for the time being shall give self-contained proofs of several elementary results from which it follows that, for G reductive, any compact subgroup of G_K is contained in some maximal compact subgroup. Moreover, as the following proposition shows, the condition that G be reductive is necessary.

PROPOSITION 3.15. *If G_K contains a maximal compact subgroup, then G is reductive.*

PROOF: Consider the Levi decomposition $G = HU$ of G, where $U = R_u(G)$ is the unipotent radical of G and H is reductive (cf. §2.1.9). Assume $U \neq (1)$. Then the center $Z(U)$ is also nontrivial, and the "truncated" logarithmic map induces a K-isomorphism $\varphi\colon Z(U) \to V$, where $V = L(Z(U))$ is the corresponding Lie algebra, $\dim V > 0$. Since U is a normal subgroup

of G, $Z(U)$ is also a normal subgroup, and for any g in G, z in $Z(U)$ we have

$$\varphi(g^{-1}zg) = (\mathrm{Ad}\, g)\varphi(z). \tag{3.12}$$

Let $\varrho: G \to GL(V)$ be the adjoint representation. If $B \subset G_K$ is a maximal compact subgroup, then by Proposition 1.12 we can find $L \subset V_K$ which is invariant under $\varrho(B)$. Put $Z_i = \varphi^{-1}(\pi^{-i}L)$, where $\pi \in K$ is a uniformizing parameter. Clearly the Z_i's are compact subgroups of $Z(U)_K$ whose union coincides with $Z(U)_K$. Moreover, it follows from (3.12) that B normalizes all Z_i, so any product BZ_i is also a compact subgroup. By the maximality of B we obtain $B = BZ_i$ for each i. Hence $Z(U)_K \subset B$, contradiction, since $Z(U)_K$ is noncompact. Q.E.D.

Now we shall show that if G is reductive then indeed G_K has maximal compact subgroups, and any compact subgroup of G_K lies in some maximal compact subgroup.

PROPOSITION 3.16. *Let G be a reductive K-group. Then*

(1) *any open compact subgroup of G_K is contained in only a finite number of compact subgroups;*
(2) *any compact subgroup of G_K is contained in some maximal compact subgroup.*

Moreover, if G is semisimple, then the normalizer in G_K of any open compact subgroup is compact.

PROOF: Let $G \subset GL_n(\Omega)$. Embedding $GL_n(\Omega)$ in $GL_{n+1}(\Omega)$ by the map $g \to \begin{pmatrix} g & 0 \\ 0 & \det^{-1} g \end{pmatrix}$, we may assume G to be Zariski-closed in $M_n(\Omega)$. Let A denote the Ω-span $\Omega[G]$ of G in $M_n(\Omega)$ (i.e., the set of Ω-linear combinations of the elements of G), and B the K-span $K[G_K]$ of G_K in $M_n(K)$. Since G is reductive, it follows from Theorem 2.4 that A and B are semisimple algebras over Ω and K respectively. Any open compact subgroup $U \subset G_K$ is Zariski-dense in G (Lemma 3.2), implying $\Omega[U] = A$ and $K[U] = B$. In particular, $P = \mathcal{O}[U]$ is an order in B. By Theorem 1.16, P is contained in a finite number of maximal orders $P_1, \ldots, P_r$. Each $P_i \cap G$ is obviously compact and closed under multiplication, so $U_i = (P_i \cap G) \cap (P_i \cap G)^{-1}$ is a compact subgroup of G_K.

Now let $W \subset G_K$ be a compact subgroup containing U. Then $\mathcal{O}[W]$ is an order in B containing P and therefore $\mathcal{O}[W] \subset P_i$ for some i. Consequently, $W \subset P_i \cap G$ and $W = W^{-1} \subset (P_i \cap G)^{-1}$; so $W \subset U_i$. We have shown that any compact subgroup containing U must be contained in one of the groups U_i. The first assertion of Proposition 3.16 follows, since by

the openness of U the index $[U_i : U]$ is finite and therefore the number of intermediate subgroups between U and U_i is also finite. Assertion (1) implies assertion (2) by virtue of the fact mentioned above that any compact subgroup of G_K is contained in some open compact subgroup.

Now let G be semisimple. Consider the adjoint action of G on A, and let $\varphi: G \to \mathrm{Aut}\, A$ be the corresponding representation, given by

$$g \overset{\varphi}{\mapsto} i_g \quad \text{where} \quad i_g(x) = gxg^{-1}.$$

Clearly $\ker\varphi$ is the center of G and therefore is finite. Consider an arbitrary open compact subgroup $U \subset G_K$ and write N for its normalizer in G_K. As we have established above, $P = \mathcal{O}[U]$ is an order in $B = K[G_K]$, so, any $\mathcal{O}$-base $x_1, \ldots, x_m$ in P also is an Ω-base of A. Since clearly $g^{-1}Pg = P$ for any g in N, the entries of the transformation matrix $\varphi(g)$ with respect to $x_1, \ldots, x_m$ lie in $\mathcal{O}$. Thus $\varphi(N) \subset \varphi(G)_{\mathcal{O}}$. Since $\varphi(G)_{\mathcal{O}}$ is compact and $\ker\varphi$ is finite, it follows that $\varphi^{-1}(\varphi(G)_{\mathcal{O}})$ is compact and, consequently, N is relatively compact. On the other hand, since U is closed, N is also closed, and therefore it is indeed compact. Q.E.D.

We shall return to the properties of maximal compact subgroups in the next section, but for now, using the elementary results contained in Proposition 3.16, we shall derive some structural results about G_K. Our arguments will be based on the theory of profinite groups. Since profinite groups will be encountered repeatedly later on, we shall briefly review their definition and basic properties (a more detailed exposition may be found in Serre [2] and Bourbaki [2, Ch. 3, §7]).

Let I be a directed set, i.e., a set with partial order $\leq$, such that for any i, j in I there is k in I satisfying $i \leq k$, $j \leq k$. (In our discussion I will usually be the set $\mathbb{N}$ of positive integers, with its natural ordering.) By a *projective* (or *inverse*) *system* $\mathcal{G} = (G_i, \varphi_i^j)$ over I we mean an aggregate of objects (sets, groups, rings, etc.) G_i, indexed by the elements of I, and of morphisms $\varphi_i^j: G_j \to G_i$ whenever $j \geq i$, where φ_i^i is the identity map and $\varphi_i^k = \varphi_i^j \circ \varphi_j^k$ for $k \geq j \geq i$. The *projective* (or *inverse*) *limit* $\varprojlim G_i$ (more precisely, $\varprojlim(G_i, \varphi_i^j)$) is the subset of $\prod_{i \in I} G_i$ consisting of those $g = (g_i)$ such that $\varphi_i^j(g_j) = g_i$ for all $j \geq i$ in I. Clearly $\varprojlim G_i$ inherits any type of algebraic structure possessed by all the G_i. Moreover, if the G_i are all Hausdorff topological spaces and the φ_i^j are continuous maps, then $G = \varprojlim G_i$ is closed in $\prod_{i \in I} G_i$.

In particular, let all the G_i be finite groups endowed with the discrete topology, and let φ_i^j be group homomorphisms. Then $G = \varprojlim G_i$ is called a *profinite group*. Since G is closed in $\prod_{i \in I} G_i$, which is compact, G itself

is a compact group. Moreover, G is totally disconnected. (This can be shown most easily by using the restriction $\pi_l = p_l \mid_G$ of the canonical projections $p_l\colon \prod_{i\in I} G_i \to G_l$; for the point is that finite intersections of their kernels form a fundamental system of neighborhoods of the identity of G consisting of subgroups.) Conversely, any compact totally disconnected topological group G is profinite, i.e., can be written as a projective limit of finite groups. Such a presentation can be obtained if one has a fundamental system $\{N_i\}_{i\in I}$ of neighborhoods of unity of G, consisting of normal subgroups. (It can be shown that such a system does exist in any compact totally disconnected group, cf. Koch [1, §1.2]). Namely, the natural homomorphism

$$G \to \varprojlim G/N_i, \quad \text{given by} \quad g \mapsto (gN_i)_{i\in I},$$

is an isomorphism of topological groups. Let us apply this result to the group of points $G_{\mathcal{O}}$ of an algebraic K-group G in the ring of integers $\mathcal{O}$. Since the congruence subgroups $G_{\mathcal{O}}(\mathfrak{p}^d)$ (where $\mathfrak{p}$ is the valuation ideal in $\mathcal{O}$, $d > 0$) are obviously normal in $G_{\mathcal{O}}$ and constitute a base of the neighborhoods of the identity,

$$G_{\mathcal{O}} \simeq \varprojlim G_{\mathcal{O}}/G_{\mathcal{O}}(\mathfrak{p}^d). \tag{3.13}$$

We can draw certain specific conclusions about the structure of $G_{\mathcal{O}}$ from this presentation. Recall that the projective limit of finite p-groups is called a *pro-p-group*.

LEMMA 3.8. *$G_{\mathcal{O}}(\mathfrak{p})$ is a pro-p-group.*

PROOF: The prime p is determined by the condition $\mathbb{Q}_p \subset K$ or equivalently by $p \in \mathfrak{p}$. If $G = \varprojlim G/N$ is a presentation of a profinite group G as the projective limit of its finite factors, then for any closed subgroup $H \subset G$ we have $H = \varprojlim H/H \cap N$. It follows that for $G_{\mathcal{O}}(\mathfrak{p})$ we have

$$G_{\mathcal{O}}(\mathfrak{p}) \simeq \varprojlim G_{\mathcal{O}}(\mathfrak{p})/G_{\mathcal{O}}(\mathfrak{p}^d).$$

We shall show that $G_{\mathcal{O}}(\mathfrak{p})/G_{\mathcal{O}}(\mathfrak{p}^d)$ is a p-group. It suffices to show for any $d \geq 1$ that $G_{\mathcal{O}}(\mathfrak{p}^d)/G_{\mathcal{O}}(\mathfrak{p}^{d+1})$ is a p-group. Let $x \in G_{\mathcal{O}}(\mathfrak{p}^d)$. Write $x = E_n + y$, where $y \equiv 0 \pmod{\mathfrak{p}^d}$. Then

$$x^p = E_n + \binom{p}{1} y + \cdots + \binom{p}{p-1} y^{p-1} + y^p$$

where the $\binom{p}{i}$ are the binomial coefficients. Since the $\binom{p}{i}$ are divisible by p for $0 < i < p$, we see that $\binom{p}{i} y^i \equiv 0 \pmod{\mathfrak{p}^{d+1}}$ for any $i \geq 1$. Therefore $x^p \equiv E_n \pmod{\mathfrak{p}^{d+1}}$. Consequently, the order of any element of $G_{\mathcal{O}}(\mathfrak{p}^d)/G_{\mathcal{O}}(\mathfrak{p}^{d+1})$ divides p. Q.E.D.

COROLLARY. *The order of any element of $G_{\mathcal{O}}(\mathfrak{p})$ is either infinite or is a power of p.*

PROOF: It is easy to see that any closed subgroup of a pro-p-group is again a pro-p-group. Therefore if the order of x in $G_{\mathcal{O}}(\mathfrak{p})$ is finite, the cyclic subgroup $H = \langle x \rangle$ generated by x must be a finite pro-p-group, i.e., a usual p-group.

It follows that $G_{\mathcal{O}}$ is a finite extension of the pro-p-group $G_{\mathcal{O}}(\mathfrak{p})$. In the theory of profinite groups, pro-q-subgroups (where q is an arbitrary prime) are the profinite analogs of q-subgroups in the theory of finite groups and retain many properties of the latter. In particular, any pro-q-subgroup is contained in some maximal (Sylow) pro-q-subgroup, and all of the latter are conjugate (cf. Serre [2]).

In the situation under discussion, pro-p-subgroups play a special role, since their properties yield important results on the structure of G_K. Our immediate objective is to establish for G_K the analog of Sylow's theorem on the conjugacy of maximal pro-p-subgroups. (In view of the existence of nonconjugate maximal compact subgroups, such a result is by no means obvious.)

THEOREM 3.10 (MATSUMOTO [1]). *Let G be a semisimple algebraic K-group, and let H be an open subgroup of G_K. Then H contains a maximal open pro-p-subgroup S, and any pro-p-subgroup of H is contained in a conjugate of S.*

PROOF: Since H is an open subgroup it contains a suitable congruence subgroup $G_{\mathcal{O}}(\mathfrak{p}^d)$. $G_{\mathcal{O}}(\mathfrak{p}^d)$ is a pro-p-group by Lemma 3.8. Applying the first assertion of Proposition 3.16, we conclude that $G_{\mathcal{O}}(\mathfrak{p}^d)$ is contained in a maximal pro-p-subgroup $S \subset H$.

Next let $T \subset H$ be a pro-p-subgroup. We shall show that T is contained in a Sylow pro-p-subgroup. Referring again to Proposition 3.16 (1), we see that it suffices to find an open pro-p-subgroup containing T. To find one, note that $[T : T \cap S]$ is finite since T is compact, and therefore there is only a finite number of distinct conjugates $t^{-1}St$ for t in T. Hence $S_0 = \bigcap_{t\in T}(t^{-1}St)$ is open and is normalized by T, so $T_0 = TS_0$ is the desired group.

Therefore, in proving that a pro-p-subgroup T is contained in a subgroup conjugate to S, we may assume T to be Sylow. For technical reasons it is easier for us to prove not only that S and T are conjugate but also the stronger result that there exists x in H such that $xTx^{-1} = S$ and $[S : S \cap T] = [S : x(S \cap T)x^{-1}]$. (Actually, by using the existence of a Haar measure on G_K and its unimodularity (cf. §3.5), we can show that the latter equality is satisfied automatically.)

We proceed by induction on $n = [S : S \cap T]$. If $n = 1$ then $S = T$ and there is nothing to prove. Now take $n > 1$. Let N denote the normalizer of $S \cap T$ in H; by Proposition 3.16 N is a compact subgroup of H and consequently $[N : S \cap T]$ is finite. First we show that $N_1 = N \cap S = N_S(S \cap T)$ and $N_2 = N \cap T = N_T(S \cap T)$ strictly contain $S \cap T$. Since $S \cap T \neq S, T$, this follows from

LEMMA 3.9. *Let P be a pro-p-group, and let H be a proper open subgroup of P. Then the normalizer $N_P(H)$ is distinct from H.*

PROOF: For finite p-groups this assertion is well known. To reduce to the finite case, put $F = \bigcap_{g \in P}(g^{-1}Hg)$. Then F is an open normal subgroup of P, contained in H. Clearly $N_P(H) = \pi^{-1}(N_{P/F}(H/F))$, where $\pi: P \to P/F$ is the natural homomorphism. But P/F is finite, so $N_{P/F}(H/F) \neq H/F$, and hence $N_P(H) \neq H$. The lemma is proved.

To continue the proof of Theorem 3.10, consider the finite group $\bar{N} = N/S \cap T$ and the natural homomorphism $\varphi: N \to \bar{N}$. $\varphi(N_1)$ and $\varphi(N_2)$ are p-subgroups of $\bar{N}$, so by the classic Sylow theorems there is a Sylow p-subgroup P of $\bar{N}$ containing $\varphi(N_1)$ and an element $\bar{x} \in \bar{N}$ such that $\bar{x}\varphi(N_2)\bar{x}^{-1} \subset P$. The inverse image $\varphi^{-1}(P)$ is a pro-p-subgroup of H and therefore is contained in some Sylow pro-p-subgroup V. Note that by assumption N_1, $xN_2x^{-1} \subset V$, where x in N satisfies $\varphi(x) = \bar{x}$. Then $[S : S \cap V] < n$, so by induction $S = yVy^{-1}$ for some y in H such that $[S : S \cap V] = [S : y(S \cap V)y^{-1}]$. Consider $T' = (yx)T(yx)^{-1}$. Clearly $S \cap T' \supset (yx)N_2(yx)^{-1} \supsetneq (yx)(S \cap T)(yx)^{-1}$, and moreover x normalizes $S \cap T$, implying

(3.14)
$$\begin{aligned}[S : (yx)(S \cap T)(yx)^{-1}] &= [S : y(S \cap T)y^{-1}] \\ &= [S : y(S \cap V)y^{-1}][y(S \cap V)y^{-1} : y(S \cap T)y^{-1}] \\ &= [S : S \cap V][S \cap V : S \cap T] = [S : S \cap T].\end{aligned}$$

Thus $[S : S \cap T'] < n$ and again by induction we can find z in H satisfying $S = zT'z^{-1}$ and $[S : S \cap T'] = [S : z(S \cap T')z^{-1}]$. Then $S = (zyx)T(zyx)^{-1}$ and

$$\begin{aligned}[S : (zyx)(S \cap T)(zyx)^{-1}] &= \\ &= [S : z(S \cap T')z^{-1}][z(S \cap T')z^{-1} : (zyx)(S \cap T)(zyx)^{-1}] \\ &= [S : S \cap T'][S \cap T' : (yx)(S \cap T)(yx)^{-1}] \\ &= [S : (yx)(S \cap T)(yx)^{-1}] = [S : S \cap T].\end{aligned}$$

by (3.14). This completes the proof of Theorem 3.10.

REMARK: The original proof of Theorem 3.10 presented by Matsumoto [1] is incomplete: his induction on the pair of indexes $[S : S \cap T]$ and $[T : S \cap T]$ does not work. Our proof is a revision of Matsumoto's argument.

Theorem 3.10 will be used on more than one occasion in this book. In particular, one of its corollaries is the following important structural result:

PROPOSITION 3.17. *Let G be a K-simple algebraic K-group. Then any noncentral normal subgroup of G_K has finite index.*

PROOF: Let H be a noncentral normal subgroup of G_K. By Theorem 3.3 H is open; therefore G_K/H is discrete, and we need only show that it is compact. This follows from

PROPOSITION 3.18. *Let H be an open normal subgroup of G_K, where G is a semisimple K-group. Then there exists a maximal compact subgroup $B \subset G_K$ such that $G_K = BH$.*

PROOF: Let $S \subset H$ be a Sylow pro-p-subgroup, and $g \in G_K$. Then $g^{-1}Sg$ is also a Sylow pro-p-subgroup of $g^{-1}Hg = H$, and consequently $g^{-1}Sg = h^{-1}Sh$ for suitable h in H by Theorem 3.10. Therefore $x = gh^{-1} \in N = N_{G_K}(S)$, i.e., $G_K = NH$. But by Proposition 3.16 N is compact, and by Proposition 3.16 (1) is contained in a maximal compact subgroup B, which is the desired group.

REMARK: Propositions 3.5 and 3.17 together allow one to make the following general conclusion: if K is a locally compact field and G is a K-simple algebraic K-group, then any noncentral normal subgroup of G_K has finite index. (We have not examined explicitly the case $K = \mathbb{C}$, although here, as is well known, $G = G_{\mathbb{C}}$ does not have proper noncentral normal subgroups (cf. §7.2). There is also a topological proof of this fact: any noncentral normal subgroup of $G_{\mathbb{C}}$ is open and therefore necessarily contains the connected component $G^0_{\mathbb{C}}$, but $G_{\mathbb{C}}$ is connected, by Theorem 3.5, i.e., $G_{\mathbb{C}} = G^0_{\mathbb{C}}$). The analogous result for simply connected groups over number fields is far more complicated to prove (cf. §§7.2 and 9.1).

Besides using the theory of profinite groups, the study of algebraic groups over non-Archimedean local fields also uses the trick of reducing the variety under consideration modulo the maximal ideal $\mathfrak{p}$. By means of reduction one can associate to a given algebraic variety X defined over K an algebraic variety $\underline{X}$ defined over the residue field $k = \mathcal{O}/\mathfrak{p}$. Moreover, if some smoothness condition is satisfied, then the points of $\underline{X}_k$ are in one-to-one correspondence with the congruence classes modulo $\mathfrak{p}$ of the points of $X_{\mathcal{O}}$. To avoid weighing down the exposition with technical details, we shall present the basic definitions and results for the case of affine varieties. Later we shall also encounter projective varieties, for which the reasoning

is analogous. (Indeed, the case of arbitrary varieties can be reduced to the affine case by considering a finite affine covering, cf. Weil [3].)

It is convenient to define, more generally, the reduction of an affine algebraic variety $X \subset \mathbb{A}^n$ defined over P, the field of fractions of an integral domain R. Let $\mathfrak{a} \subset P[x_1, \dots, x_n]$ be the ideal of polynomials that vanish on X. By *reduction of* X modulo a maximal ideal $\mathfrak{m} \subset R$ we mean the subvariety $\underline{X}^{(\mathfrak{m})}$ of $\mathbb{A}^n$ over a universal domain containing the residue field $k = R/\mathfrak{m}$, defined by the ideal $\mathfrak{a}^{(\mathfrak{m})}$, which is obtained by reducing all the polynomials of $\mathfrak{a} \cap R[x_1, \dots, x_n]$ modulo $\mathfrak{m}$. (Note that in general $\underline{X}^{(\mathfrak{m})}$ is only k-closed in $\mathbb{A}^n$ but not necessarily defined over k. However, in what follows k is going to be a finite field, which is perfect; hence the concepts of k-closed and k-defined subvarieties will coincide.) Although this definition is quite straightforward, the process of reduction itself is rather delicate and must be used with care. For example, if $P = \mathbb{Q}$, $R = \mathbb{Z}$, and $X \subset \mathbb{A}^1$ consists of a single point $x = p^{-1}$, then $\mathfrak{a} = (px-1)$, $\mathfrak{a} \cap \mathbb{Z}[x] = (px-1)\mathbb{Z}[x]$; so the reduction of X modulo p is given by $0 \cdot x - 1 = 0$, i.e., $\underline{X}^{(p)} = \emptyset$.

Unfortunately there are as yet no books in the literature containing a complete exposition of the theory of reduction of algebraic varieties, although a large number of results pertaining to this subject are referred to as "well known." We too, have decided not to include a fully detailed discussion of these questions, since they require considerably more commutative algebra than the rest of this book. Therefore we shall limit ourselves to the basic definitions and results and shall present several fundamental facts (such as Hensel's lemma) without proofs. On the other hand, below we shall give several simple patterns of arguments which are typical of the theory of reduction, thus enabling the interested reader to reconstruct several of the proofs omitted.

Now we define a *smooth reduction*. As above, let $X \subset \mathbb{A}^n$ be an affine P-variety all of whose irreducible components have the same dimension m, and let $\underline{X}^{(\mathfrak{m})}$ be the reduction of X modulo a maximal ideal $\mathfrak{m}$ of a subring $R \subset P$. We say that a point x in $\underline{X}^{(\mathfrak{m})}$ is a *simple point of reduction* if there exist polynomials $f_1, \dots, f_r \in \mathfrak{a} \cap R[x_1, \dots, x_n]$, with $r = n - m$ (where $\mathfrak{a}$ is the ideal of polynomials of $P[x_1, \dots, x_n]$ that vanish on X), such that the rank of the Jacobian

$$\left(\frac{\partial \bar{f}_i}{\partial x_j}(x) \right)_{\substack{i=1,\dots,r \\ j=1,\dots,n}}$$

equals r (hereafter bar denotes reduction modulo $\mathfrak{m}$). The reduction is said to be *smooth* if all the points of $\underline{X}^{(\mathfrak{m})}$ are simple. Note that the concept of smooth reduction is stronger than the requirements for the variety $\underline{X}^{(\mathfrak{m})}$ to be smooth. Given points $x = (x_1, \dots, x_n)$ and $y = (y_1, \dots, y_n)$ in X_R, we write $x \equiv y \pmod{\mathfrak{m}}$ if $x_i \equiv y_i \pmod{\mathfrak{m}}$ for all $i = 1, \dots, n$.

For any x in X_R there is a corresponding point $\bar{x} \in \mathbb{A}_k^n$ lying in $\underline{X}_k^{(\mathfrak{m})}$, and hence there is a reduction map $\varrho: X_R \to \underline{X}_k^{(\mathfrak{m})}$ whose nonempty fibers are the congruence classes modulo $\mathfrak{m}$ of points of X_R. One may ask what is the image of the reduction map. We shall not discuss all aspects of this problem here (cf. the survey by Parshin [1]), since for our purposes it suffices to present the following result relating to the original case, where K is a finite extension of $\mathbb{Q}_p$, $\mathcal{O}$ is the ring of integers in K, and $\mathfrak{p} \subset \mathcal{O}$ is the maximal ideal.

THEOREM 3.11 (HENSEL'S LEMMA). *If $x \in \underline{X}^{(\mathfrak{p})}$ is a simple point of reduction, then x lies in the image of the reduction map. In particular, if $\underline{X}^{(\mathfrak{p})}$ is a smooth reduction, then the reduction map is surjective.*

Note that in the case of smooth reduction, distinct irreducible components of the variety cannot be "pasted together." In particular, if $\underline{X}$ consists of a finite number of points and the reduction is smooth, then the reduction map is injective.

It is clear that a reduction of a smooth variety need not be smooth. Nevertheless, if $\underline{X}$ is a smooth variety defined over a number field K, then for almost all non-Archimedean valuations v of K the reduction $\underline{X}^{(v)}$ modulo the corresponding maximal ideal $\mathfrak{p}(v)$ of $\mathcal{O} \subset K$ is also smooth.

Another property of an algebraic variety, that of (absolute) irreducibility, behaves in a similar way under reduction. Moreover, if the original variety is an algebraic group, then all of its reductions will be algebraic groups and the corresponding reduction map will be a group homomorphism. The remainder of this subsection is devoted to the precise formulation and partial proof of these facts.

THEOREM 3.12 (NOETHER). *Let X be an irreducible m-dimensional affine variety over a number field K. Then $X^{(v)}$ is also an irreducible m-dimensional variety, for almost all v in V_f^K.*

Let us make one remark regarding the definition of $\underline{X}^{(v)}$. To begin with we can define $\underline{X}^{(v)}$ as the reduction of X modulo the ideal $\mathfrak{p}(v)$ of $\mathcal{O} \subset K$. But it can be shown that we obtain the same variety $\underline{X}^{(v)}$ if we take the ring $\mathcal{O}'$ of S-integers for any subset $S \subset V^K$ such that $v \notin S$, and perform reduction modulo the corresponding maximal ideal $\mathfrak{p}'(v) \subset \mathcal{O}'$. To do so, consider $\mathfrak{b} = \mathfrak{a} \cap \mathcal{O}[x_1, \dots, x_n]$ and $\mathfrak{b}' = \mathfrak{a} \cap \mathcal{O}'[x_1, \dots, x_n]$. Since $\mathcal{O}'$ is a Noetherian ring, $\mathfrak{b}'$ has a finite set of generators $f_1, \dots, f_r$, by Hilbert's basis theorem. Since $v \notin S$, for suitable a in $\mathcal{O} \setminus \mathfrak{p}(v)$ all $af_1, \dots, af_r$ lie in $\mathcal{O}[x_1, \dots, x_n]$ and consequently in $\mathfrak{b}$. Bearing in mind that $\mathcal{O}/\mathfrak{p}(v) = \mathcal{O}'/\mathfrak{p}'(v)$, we see that the images of the ideals $\mathfrak{b}^{(\mathfrak{p}(v))}$ and $(\mathfrak{b}')^{(\mathfrak{p}'(v))}$ coincide, i.e., $\underline{X}^{(\mathfrak{p}(v))} = \underline{X}^{(\mathfrak{p}'(v))}$. Thus the reduction of a K-

variety actually depends only on v rather than on the pair $(\mathcal{O}, \mathfrak{p}(v))$, thereby justifying the notation $\underline{X}^{(v)}$.

Another remark: if $x \in X_K$, then $x \in X_{\mathcal{O}'}$ for the ring of S-integers $\mathcal{O}'$, for S sufficiently large. Then x reduces to $\bar{x}$ of $\underline{X}^{(\mathfrak{p}'(v))}$ when $v \notin S$. But since $\underline{X}^{(\mathfrak{p}(v))}$ and $\underline{X}^{(\mathfrak{p}'(v))}$ are the same, we may regard $\bar{x}$ as belonging to $\underline{X}^{(\mathfrak{p}(v))}$. In this case we say that for $v \notin S$ the point x can be reduced modulo $\mathfrak{p}(v)$ and the result of its reduction is the point $\bar{x}$. Similar terminology is applied to polynomials, regular maps, etc.

In what follows an important, although not so apparent, role is played by the fact that $\underline{X}^{(v)}$ coincides with the reduction $\underline{X}^{(\mathfrak{p}_v)}$ modulo the maximal ideal $\mathfrak{p}_v$ of the ring of integers $\mathcal{O}_v$ of the corresponding completion K_v (in the latter case X is regarded as a K_v-variety).

LEMMA 3.10. *In the given setting,* $\underline{X}^{(v)} = \underline{X}^{(\mathfrak{p}_v)}$.

PROOF: Put $\mathfrak{b} = \mathfrak{a} \cap \mathcal{O}[x_1, \dots, x_n]$ and $\mathfrak{b}' = \mathfrak{a}_v \cap \mathcal{O}_v[x_1, \dots, x_n]$, where $\mathfrak{a}_v$ is the ideal of polynomials in $K_v[x_1, \dots, x_n]$ that vanish on X. Let $f_1, \dots, f_r$ and $g_1, \dots, g_s$ be finite sets of generators of $\mathfrak{b}$ and $\mathfrak{b}'$ respectively. Since X is defined over K, there are h_{ij} in $K_v[x_1, \dots, x_n]$ such that $g_i = \sum_{j=1}^{r} h_{ij} f_j$. If we choose t_{ij} in $K[x_1, \dots, x_n]$ in such a way that their coefficients are sufficiently close to the respective coefficients of h_{ij}, we obtain $g_i' = \sum_{j=1}^{r} t_{ij} f_j$ lying in $\mathcal{O}_v[x_1, \dots, x_n] \cap \mathfrak{a}_v = \mathfrak{b}'$ and satisfying $g_i \equiv g_i' \pmod{\mathfrak{p}_v}$. Furthermore, we can choose a finite subset $S \subset V_f^K$ with $v \notin S$, such that the coefficients of g' lie in the ring of S-integers $\mathcal{O}'$. Then it is easy to see that $\underline{X}^{(\mathfrak{p}'(v))} = \underline{X}^{(\mathfrak{p}_v)}$ for the corresponding ideal $\mathfrak{p}'(v) \subset \mathcal{O}'$, and thus $\underline{X}^{(\mathfrak{p}(v))} = \underline{X}^{(\mathfrak{p}_v)}$.

The same method can be used to prove the following assertion, which shows that reduction relative to a valuation is independent of the base field, for almost all valuations.

LEMMA 3.11. *Let L/K be a finite extension of number fields. Then, for any affine K-variety X, considered also as L-variety, and for almost all v in V_f^K, $\underline{X}^{(v)}$ is the same as $\underline{X}^{(w)}$, for each extension w of v to L.*

The following assertion is often useful in working with reductions of varieties.

LEMMA 3.12. *Let $f_1, \dots, f_r \in K[x_1, \dots, x_n]$. Then if*

$$f_i = 0, \quad i = 1, \dots, r \tag{3.15}$$

is inconsistent, i.e., has no simultaneous solution over $\bar{K}$, then for almost all v in V_f^K the reduction (taken with respect to v)

$$\bar{f}_i = 0, \quad i = 1, \dots, r \tag{3.16}$$

also is inconsistent.

PROOF: Since (3.15) is inconsistent, by Hilbert's Nullstellensatz we can find polynomials $g_1, \dots, g_r$ in $K[x_1, \dots, x_n]$ such that $f_1 g_1 + \dots + f_r g_r = 1$. Then for almost all v the coefficients of g_i are v-integers, and the latter equation can be reduced modulo v. We obtain $\bar{f}_1 \bar{g}_1 + \dots + \bar{f}_r \bar{g}_r = 1$, from which it follows that (3.16) is inconsistent. The lemma is proved.

EXERCISE 1: Using Lemma 3.12, derive a proof of Theorem 3.12 for the basic case (from the birational point of view) of a hyperplane in $\mathbb{A}^n$. In other words, show that if $f \in K[x_1, \dots, x_n]$ is an absolutely irreducible polynomial, then its reduction $\bar{f}$ modulo v is also absolutely irreducible for almost all v in V_f^K. (Hint: note that a factorization $\bar{f} = gh$ can be interpreted as yielding a solution of a certain system of polynomial equations in the coefficients of g and h; on the other hand, using Lemma 3.12 prove that the latter has no solutions for almost all v.)

PROPOSITION 3.19. *Let X be a smooth affine variety over an algebraic number field K, all of whose irreducible components have the same dimension m. Then the reduction $\underline{X}^{(v)}$ is smooth for almost all v in V_f^K.*

PROOF: Let $X \subset \mathbb{A}^n$, let $\mathfrak{a} \subset K[x_1, \dots, x_n]$ be the ideal of polynomials vanishing on X, and let $\mathfrak{b} = \mathfrak{a} \cap \mathcal{O}[x_1, \dots, x_n]$, where $\mathcal{O}$ is the ring of integers of K. Choose a finite set of generators $f_1, \dots, f_l$ of $\mathfrak{b}$ and let $\{D_j\}_{j=1}^{d}$ be the totality of all $r \times r$ minors of the Jacobian

$$\begin{pmatrix} \frac{\partial f_1}{\partial x_x} & \dots & \frac{\partial f_1}{\partial x_n} \\ \dots\dots\dots\dots\dots \\ \frac{\partial f_l}{\partial x_1} & \dots & \frac{\partial f_l}{\partial x_n} \end{pmatrix},$$

where $r = n - m$. Since X is smooth, the system of equations

$$\begin{aligned} f_i &= 0, \quad i = 1, \dots, l \\ D_j &= 0, \quad j = 1, \dots, d \end{aligned}$$

is inconsistent. Therefore, by Lemma 3.12, the reduction of this system is also inconsistent, for almost all v in V_f^K; i.e., the reduced variety does not contain any points for which the Jacobian has rank $< r$. But this means exactly that $\underline{X}^{(v)}$ is smooth. The proposition is proved.

EXERCISE 2: Derive a projective analog of Proposition 3.19.

It remains to be shown that the reduction of an algebraic group is an algebraic group. To do so we first need to discuss some results relating to reduction of morphisms of algebraic varieties. For an arbitrary field P, let $f: X \to Y$ be a regular P-map of two P-varieties $X \subset \mathbb{A}^n$ and $Y \subset \mathbb{A}^m$. This f is described by the m-tuple of "coordinate" polynomials

$f_1, \dots, f_m$ from $P[x_1, \dots, x_n]$. We say that f is defined over a subring $R \subset P$ if it can be given by polynomials from $R[x_1, \dots, x_n]$. In this case, the reduced regular map $f^{(\mathfrak{m})} = (\bar{f}_1, \dots, \bar{f}_m)$ is determined for any maximal ideal $\mathfrak{m} \subset R$. Likewise we obtain the regular map $\underline{f}^{(\mathfrak{m})}: \underline{X}^{(\mathfrak{m})} \to \underline{Y}^{(\mathfrak{m})}$ of the corresponding reductions, as shown by the next result.

LEMMA 3.13. $\underline{f}^{(\mathfrak{m})}(\underline{X}^{(\mathfrak{m})}) \subset \underline{Y}^{(\mathfrak{m})}$.

PROOF: Let $\mathfrak{a}_X$ and $\mathfrak{a}_Y$ be the respective ideals of X and Y in the rings $P[x_1, \dots, x_n]$ and $P[y_1, \dots, y_m]$ respectively, and let $\mathfrak{b}_X = \mathfrak{a}_X \cap \mathcal{O}[x_1, \dots, x_n]$ and $\mathfrak{b}_Y = \mathfrak{a}_Y \cap \mathcal{O}[y_1, \dots, y_m]$. Let $f^*: P[y_1, \dots, y_m] \to P[x_1, \dots, x_n]$ denote the comorphism associated with f, given by $y_j \mapsto f_j(x_1, \dots, x_n)$. Then $f(X) \subset Y$ means $f^*(\mathfrak{a}_Y) \subset \mathfrak{a}_X$. Since f is defined over R, we also have $f^*(\mathfrak{b}_Y) \subset \mathfrak{b}_X$. Reducing modulo $\mathfrak{m}$ yields $(f^*)^{(\mathfrak{m})}(\mathfrak{b}_Y^{(\mathfrak{m})}) \subset \mathfrak{b}_X^{(\mathfrak{m})}$, i.e., $f^{(\mathfrak{m})}(\underline{X}^{(\mathfrak{m})}) \subset \underline{Y}^{(\mathfrak{m})}$, proving the lemma.

Unlike morphisms over a field (cf. §2.4), morphisms over a ring lack explicit criteria of definition. Therefore in general it is difficult to assert that a given P-morphism $f: X \to Y$ is defined over a subring $R \subset P$, i.e., that it can be reduced modulo $\mathfrak{m} \subset R$. We shall deal mainly with morphisms of varieties $f: X \to Y$ defined over some number field K, and then a fortiori for almost all v there is a reduction of f to a regular map $\underline{f}^{(v)}: \underline{X}^{(v)} \to \underline{Y}^{(v)}$. In particular, it follows for almost all v that $\underline{X}^{(v)}$ is independent of the geometric realization of X as a Zariski-closed subset of an affine space. To be more precise, if X and Y are biregularly isomorphic over K, then $\underline{X}^{(v)}$ and $\underline{Y}^{(v)}$ are also biregularly isomorphic over the corresponding residue field, for almost all v.

Using the existence of reductions of morphisms, we can define reductions of arbitrary varieties via affine covers. We give a rough sketch of this technique, and refer the reader to Weil [4] for more detail. Let $X = \bigcup_{i=1}^d X_i$ be a finite affine cover of an arbitrary K-variety X. Fix geometric realizations X_i of closed subsets of affine spaces, i.e., K-isomorphisms $f_i: X_i \to X_i^0$, where X_i^0 is closed in $\mathbb{A}^{n_i}$. Put $Y_{ij} = f_i(X_i \cap X_j) \subset \mathbb{A}^{n_i}$. This gives rise to K-morphisms $g_{ij}: Y_{ij} \to Y_{ij}$ $(i, j = 1, \dots, d)$, and in terms of algebraic geometry the original variety X is obtained by pasting the X_i^0 along the $\{Y_{ij}, g_{ij}\}$ (cf. Shafarevich [1]). By Lemma 3.13, for almost all v there exist reductions $\underline{g}_{ij}^{(v)}$ of the morphisms $\underline{g}_{ij}$; and then, pasting the reductions $(\underline{X}_i)^{(v)}$ along the $\{\underline{Y}_{ij}^{(v)}, \underline{g}_{ij}^{(v)}\}$ (since the necessary conditions for pasting pass from the original morphisms g_{ij} to the reductions), we obtain the variety $\underline{X}^{(v)}$ which is called the reduction of X.

PROPOSITION 3.20. *Let $G \subset \mathbf{GL}_n$ be an algebraic K-group. Then for all v in V_f^K the reduction $\underline{G}^{(v)}$ is an algebraic group defined over the residue field k_v, and the reduction map $G_{\mathcal{O}} \to \underline{G}_{k_v}^{(v)}$ is a group homomorphism. Moreover, $\underline{G}^{(v)}$ is smooth for almost all v, and for these v the corresponding local reduction map $G_{\mathcal{O}_v} \to \underline{G}_{k_v}^{(v)}$ is surjective.*

PROOF: Let $\mu: \mathbf{GL}_n \times \mathbf{GL}_n \to \mathbf{GL}_n$ be the multiplication map $\mu(x, y) = xy$, and let $i: \mathbf{GL}_n \to \mathbf{GL}_n$ be the inverse map $i(x) = x^{-1}$. The fact that G is an algebraic group is described by $\mu(G \times G) \subset G$ and $i(G) \subset G$. Since μ and i are defined over $\mathbb{Z}$, they can be reduced for any v; and by Lemma 3.13 $\underline{\mu}^{(v)}(\underline{G}^{(v)} \times \underline{G}^{(v)}) \subset \underline{G}^{(v)}$ and $\underline{i}^{(v)}(\underline{G}^{(v)}) \subset \underline{G}^{(v)}$, i.e., $\underline{G}^{(v)}$ is an algebraic group. Moreover, the reduction map is the restriction to $G_{\mathcal{O}}$ of $GL_n(\mathcal{O}) \xrightarrow{\varrho} GL_n(k_v)$, given by the homomorphism $\mathcal{O} \to k_v = \mathcal{O}/\mathfrak{p}(v)$. But ϱ is clearly a homomorphism, so the reduction map is also a homomorphism. It remains to be noted that since G is a smooth variety, $\underline{G}^{(v)}$ is a smooth reduction for almost all v, by Proposition 3.19, and so the local reduction map $G_{\mathcal{O}_v} \to \underline{G}_{k_v}^{(v)}$ is surjective by Hensel's lemma. Q.E.D.

PROPOSITION 3.21. *Let $f: G \to H$ be a K-morphism of algebraic K-groups. Then for almost all v in V_f^K the reduction of f exists and the reduced morphism $\underline{f}^{(v)}: \underline{G}^{(v)} \to \underline{H}^{(v)}$ is also a morphism of algebraic groups.*

PROOF: By Lemma 3.13 and its subsequent remark, the reduction of f exists for almost all v in V_f^K, yielding a regular map $\underline{f}^{(v)}: \underline{G}^{(v)} \to \underline{H}^{(v)}$, and we need only establish that it is multiplicative. But the multiplicativity of f can be expressed as a set of polynomial identities on $G \times G$, whose reduction gives the analogous set of polynomial identities on $\underline{G}^{(v)} \times \underline{G}^{(v)}$, as required. Q.E.D.

We conclude this section with

PROPOSITION 3.22. *Let G be a connected algebraic K-group, let H be a connected K-subgroup, and let $X = G/H$. Then $\underline{X}^{(v)}$ coincides with $\underline{G}^{(v)}/\underline{H}^{(v)}$, for almost all v in V_f^K.*

PROOF: Consider the natural action $f: G \times X \to X$ and, for almost all v, its reduction $\underline{f}^{(v)}: \underline{G}^{(v)} \times \underline{X}^{(v)} \to \underline{X}^{(v)}$. We need to show that the following hold for almost all v:

(1) $\underline{f}^{(v)}$ is transitive;
(2) $\underline{H}^{(v)}$ is the stabilizer $\underline{G}^{(v)}(\bar{x})$ of $\bar{x}$ in $\underline{X}^{(v)}$, where $\bar{x}$ is the reduction of the identity coset $x = eH$.

Excluding a finite number of v, we may assume that $\underline{G}^{(v)}$, $\underline{H}^{(v)}$ and $\underline{X}^{(v)}$ are smooth; moreover, these varieties are irreducible and their dimensions coincide respectively with $d = \dim G$, $t = \dim H$ and $s = \dim X$. Put $Y = \{(g, y) \in G \times X : gy = y\}$ and consider the projection $\pi: Y \to X$. Then it

follows from the theorem on the dimension of the fibers of a morphism that $\{ y : \dim \pi^{-1}(y) > t \}$ is a closed subvariety $Z \subset X$. Since in our case $Z = \emptyset$, it follows from Lemma 3.12 that also $\underline{Z}^{(v)} = \emptyset$, i.e., $\underline{X}^{(v)}$ does not contain any y for which $\dim \underline{G}^{(v)}(y) > t$. It follows by a calculation of dimension and from Proposition 2.23 that condition (1) holds. Furthermore, from Theorem 3.12 we obtain that the $\underline{G}^{(v)}(\bar{x})$ must be connected for almost all v. On the other hand, $\underline{G}^{(v)}(\bar{x})$ contains $\underline{H}^{(v)}$ and has the same dimension. Therefore $\underline{G}^{(v)}(\bar{x}) = \underline{H}^{(v)}$, proving the proposition.

3.4. Elements of Bruhat-Tits theory.

Bruhat-Tits, in [2]–[4], constructed a fundamental theory for studying groups of rational points of semisimple algebraic groups over local fields. This theory is based on constructing a B–N pair, which turns out to be related to an affine root system, in the group of points of a simply connected simple group G over a local field K. Furthermore, using B–N pairs we can define a simplicial complex $\mathcal{A}$, called a *building*, acted on by G_K. This complex turns out to be contractible, and by using its properties we can learn about G_K and its subgroups. (Note that a building is actually the natural non-Archimedean analog of the symmetric space $G_{\mathbb{R}}/\mathbf{K}$, where K is a maximal compact subgroup of $G_{\mathbb{R}}$ in the Archimedean case; cf., in particular, Proposition 3.11).

For example, let $B \subset G_K$ be a compact subgroup. It can be shown that the natural action of B on $\mathcal{A}$ leaves a vertex fixed. But the stabilizers of vertices (known as *maximal parahoric subgroups*) themselves are compact, hence the set of maximal compact subgroups of G_K coincides with the set of maximal parahoric subgroups. On the other hand, parahoric subgroups can be described in terms of affine root systems, analogously to the description of parabolic subgroups noted in §2.2.12, thereby enabling us to determine their conjugacy classes and, in particular, to compute how many there are (cf. Theorem 3.13 below). Thus, the Bruhat-Tits theory provides an elegant solution of the problem of describing the maximal compact subgroups of G_K. Unfortunately, we can not go into the details of the Bruhat-Tits theory in the present book and therefore refer the reader to the original works cited above, as well as to Iwahori-Matsumoto [1], MacDonald [1], Satake [2], and Hijikata [2]. An exposition of this theory would require introducing a series of new definitions (none of which are needed later on) and relies on several independent subtheories, thus making a complete exposition as voluminous as this very book. Therefore we shall limit ourselves to describing the basic objects (in so doing, indeed, treating results of the theory as definitions) and to formulating several theorems.

Thus, let G be a simple simply connected algebraic group defined over a finite extension K of $\mathbb{Q}_p$. By an *Iwahori subgroup* $B \subset G_K$ we mean

the normalizer of a Sylow pro-p-subgroup of G_K. Note that since Sylow pro-p-subgroups are conjugate (Theorem 3.10) then Iwahori subgroups are also conjugate. A subgroup $\mathcal{P} \subset G_K$ is *parahoric* if it contains an Iwahori subgroup. A *building* $\mathcal{A}$ of G_K (or of G over K) is a simplicial complex whose vertices are maximal proper parahoric subgroups of G_K, moreover a collection $\{\mathcal{P}_0, \mathcal{P}_1, \dots, \mathcal{P}_s\}$ of such subgroups defines an s-simplex in $\mathcal{A}$ if $\bigcap_{i=0}^{s} \mathcal{P}_i$ is also a parahoric subgroup. G_K acts on $\mathcal{A}$ by conjugation; moreover this action preserves the simplicial structure, and the stabilizers of simplexes are proper parahoric subgroups. Sometimes by a building we mean the geometric realization of the said simplicial complex, which is a contractible geometric complex (Solomon-Tits theorem) whose dimension equals the K-rank of G. In particular, if $\operatorname{rank}_K G = 1$ then the complex constructed is a tree and the structure theory of groups acting on trees can be applied (cf. Serre [10]). Hence, for example, any torsion-free subgroup Γ of G_K is free (for $G = \mathbf{SL}_2$ this theorem was obtained by Ihara [1]; note also that the example of $\mathbf{SL}_2$ is taken up in detail in Humphreys [2]).

Now we shall move on to the construction of a B–N pair in G_K. To begin with, recall (cf. Bourbaki [4, Ch. 4], for more detail) that a B–N *pair* (or *Tits system*) in an abstract group G is a pair of subgroups B, $N \subset G$ such that for some $R \subset N/B \cap N$ the following axioms are satisfied:

(1) $B \cup N$ generates G and $H = B \cap N$ is a normal subgroup of N;
(2) R generates $W = N/H$ and consists of elements of order 2;
(3) $rBw \subset BwB \cup BrwB$ for r in R and w in W;
(4) $rBr \not\subset B$ for any r in R.

$W = N/H$ is the *Weyl group* of (B, N). Although the elements of W are cosets with respect to H, the double coset BgB is independent of the choice of a representative g in the coset w, and therefore is usually designated by BwB, where $w = gH \in W$; the relations expressed in (3) and (4) are to be understood in this sense. Note also that R is uniquely determined by B and N, for it consists of those w in W for which $B \cup BwB$ is a subgroup of G.

Again let G be a simply connected algebraic K-group and let $S \subset G$ be a maximal K-split torus. Write $N_G(S)$ and $Z_G(S)$ respectively for the normalizer and centralizer of S, and put $N = N_G(S)_K$ and

$$H = \{ x \in Z_G(S)_K : \chi(x) \in U \text{ for all } \chi \in \mathbf{X}(Z_G(S))_K \},$$

where U is the group of v-adic units in K. Then there exists an Iwahori subgroup B of G_K for which $B \cap N = H$, such that B, N constitute a B–N pair of G_K. $W = N/H$ then turns out to be the Weyl group of some affine root system R of rank $l = \dim S$ (cf. Bourbaki [4, Ch. 6, §2] for the definition

of an affine Weyl group). In particular, there is a subset R of generators of W, consisting of $(l+1)$ elements $r_1, r_2, \dots, r_{l+1}$ such that $r_1, \dots, r_l$ generate a subgroup $W_0 \subset W$ isomorphic to the Weyl group of some (usual) reduced root system associated with R. W_0 is the relative Weyl group $W(S,G) = N_G(S)/Z_G(S)$; however, in general, R_0 is distinct from the relative root system $R(S,G)$, even if the latter is reduced. Nevertheless, every root of R_0 is proportional to some root of $R(S,G)$ and vice versa. When G is K-split, i.e., when S is a maximal torus in G, then necessarily $R_0 = R(S,G)$.

It follows from the general theory of groups with a B–N pair that any subgroup $P \subset G_K$ containing B has the form $P_S = BW_SB$, for suitable $S \subset R$, where W_S is the subgroup of W generated by S. In addition, if P_{S_1} and P_{S_2} are conjugate in G_K, then $S_1 = S_2$. It follows that a complete system of representatives of the conjugacy classes of the maximal proper parahoric subgroups is given by the $\mathcal{P}_i = P_{S_i}$, where $S_i = R \setminus \{r_i\}$, $i = 1, \dots, l+1$. Since the set of maximal proper parahoric subgroups is the set of maximal compact subgroups, we have the following result.

THEOREM 3.13. *Let G be a simply connected simple algebraic K-group, and $l = \operatorname{rank}_K G$. Then G_K has $(l+1)$ conjugacy classes of maximal compact subgroups.*

A consequence of Theorem 3.13 in particular is that there are only finitely many conjugacy classes of maximal compact subgroups in any simply connected semisimple K-group. The Bruhat-Tits theory shows that this also holds for any reductive K-group.

For groups of rational points there are several decompositions, some of which are non-Archimedean analogs of the decomposition in §3.2. From this body of results we shall only need the non-Archimedean analog of the Cartan decomposition, which we shall discuss in greater detail. Notation as above, let $\mathbf{K} = BW_0B$ be a maximal compact subgroup. It is well known that W is a semidirect product $W = W_0T$, where T is the abelian group generated by roots from R_0; T is a free abelian group of rank $l = \dim S$. Furthermore, we need to introduce the subsemigroup $T^+ \subset T$ of "positive" elements (more precisely, consider the system Π_0 of simple roots in R_0 associated with B; then T^+ consists of those t in T for which $\langle t, \alpha \rangle \geq 0$ for all α in Π_0, where $\langle\ ,\ \rangle$ is a positive definite symmetric bilinear form on $T \otimes_{\mathbb{Z}} \mathbb{R}$ invariant under W_0). Let $\nu: N \to W = N/H$ be the natural homomorphism and put $Z^+ = \nu^{-1}(T^+)$. Note that if $z_1, z_2 \in Z_G(S)_K$ and $\nu(z_1) = \nu(z_2)$, then $z_1 z_2^{-1} \in H$ and therefore $\mathbf{K}z_1\mathbf{K} = \mathbf{K}z_2\mathbf{K}$. Thus, for z in $Z_G(S)_K$ the double coset $\mathbf{K}z\mathbf{K}$ depends only on $t = \nu(z)$, so it can naturally be designated by $\mathbf{K}\nu^{-1}(t)\mathbf{K}$. With this notation, we have

THEOREM 3.14 (CARTAN DECOMPOSITION). *$G_K = \mathbf{K}Z^+\mathbf{K}$, and there is a one-to-one correspondence from T^+ onto the set of double cosets $\mathbf{K} \setminus G_K/\mathbf{K}$ given by $t \mapsto \mathbf{K}\nu^{-1}(t)\mathbf{K}$.*

EXAMPLE: Let $G = \mathbf{SL}_n$ and $K = \mathbb{Q}_p$. It is easy to see that $SL_n(\mathbb{Q}_p)$ has a Sylow pro-p-group consisting of those matrices $x = (x_{ij})$ in $SL_n(\mathbb{Z}_p)$ for which $x_{ii} \equiv 1 \pmod p$ and $x_{ij} \equiv 0 \pmod p$ for all $i, j = 1, \dots, n$, $i > j$. Therefore the corresponding Iwahori subgroup of $SL_n(\mathbb{Q}_p)$ is

$$B = \{x = (x_{ij}) \in SL_n(\mathbb{Z}_p) : x_{ij} \equiv 0 \pmod p \text{ for } i > j\}.$$

This subgroup, together with the normalizer N of the diagonal torus $S \subset G$, constitute the B–N pair described above. A standard set of generators of $R \subset W = N/B \cap N$ consists of the following matrices:

$$r_1 = \begin{pmatrix} 0 & 1 & & & \\ -1 & 0 & & & 0 \\ & & 1 & & \\ & & & \ddots & \\ 0 & & & & 1 \end{pmatrix}, \dots, r_i = \begin{pmatrix} 1 & & & & & & 0 \\ & \ddots & & & & & \\ & & 0 & 1 & & & \\ & & -1 & 0 & & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ 0 & & & & & & 1 \end{pmatrix}, \dots, r_n$$

$$= \begin{pmatrix} 0 & 0 & & & p^{-1} \\ \vdots & 1 & & & 0 \\ & & \ddots & & \vdots \\ 0 & & & 1 & \\ -p & & & & 0 \end{pmatrix}.$$

Let W_0 be generated by $r_1, \dots, r_{n-1}$; then the parahoric subgroup $\mathcal{P} = BW_0B$ is $SL_n(\mathbb{Z}_p)$. Other maximal proper parahoric subgroups are of the form $\mathcal{P}_i = BW_iB$ for $i = 1, \dots, n-1$, where W_i is generated by $R \setminus \{r_i\}$. It is easy to show that $\mathcal{P}_i$ is the stabilizer in $SL_n(\mathbb{Q}_p)$ of the lattice with the base $e_1, \dots, e_{n-i}, pe_{n-i+1}, \dots, pe_n$, where $e_1, \dots, e_n$ is the standard base of $\mathbb{Q}_p^n$. The reader can verify easily that the classification thus obtained of conjugacy classes of maximal compact subgroups of $SL_n(\mathbb{Q}_p)$ is the same as that obtained in the proof of Proposition 3.14.

Finally, let us illustrate the Cartan decomposition for $SL_n(\mathbb{Q}_p)$. As we saw above, here $\mathbf{K}$ coincides with $SL_n(\mathbb{Z}_p)$. T is isomorphic to

$$\{(a_1, \dots, a_n) \in \mathbb{Z}^n : \sum_{i=1}^{n} a_i = 0\};$$

moreover $\alpha_i = (0, \dots, 0, 1, -1, 0, \dots, 0)$ $(i = 1, \dots, n-1)$ constitute the system of simple roots Π_0 (compare with the description of the root system of $G = \mathbf{SL}_n$ in §2.1.3). $W_0 \simeq S_n$ acts on T by permuting coefficients;

hence the usual scalar product is invariant under W_0. It follows that T^+ in the given case consists of $(a_1, \dots, a_n)$ in T such that $a_1 \le a_2 \le \dots \le a_n$. Theorem 3.14 then asserts that in any double coset $\mathbf{K}g\mathbf{K}$, $g \in SL_n(\mathbb{Q}_p)$, we can find a representative g of the form $\mathrm{diag}(p^{a_1}, p^{a_2}, \dots, p^{a_n})$, where $a_1 \le a_2 \le \dots \le a_n$ are uniquely determined. Therefore in the given case Theorem 3.14 essentially reduces to the well known Invariant Factor Theorem for matrices (cf., for example, Curtis and Reiner [1, Ch. 3, §16.5]): if A is a principal ideal domain, then for any matrix X in $M_n(A)$ there are matrices Y_1, Y_2 in $SL_n(A)$ such that $Y_1XY_2 = \mathrm{diag}(d_1, \dots, d_r, 0 \dots 0)$, where $d_i \in A$, $d_i \neq 0$ and d_i divides d_{i+1} for all $i = 1, \dots, r-1$; moreover, d_i (known as the *invariants* of X) are uniquely determined up to multiplication by invertible elements of A.

In the rest of this section, using Theorem 3.14 we shall establish that G_K is compactly presented (this result will be used in §5.4 to prove that S-arithmetic subgroups are finitely presented). To give a precise statement let us fix the following terminology: a subset C of an abstract group Γ is a *defining set* if it generates Γ and if any relation in Γ between the elements of C follows from relations of the form $ab = c$, where $a, b, c \in C$. In other words, this means that the natural homomorphism $f: F(C) \to \Gamma$ from the free group $F(C)$ generated by C is surjective, and its kernel is generated as a normal subgroup of $F(C)$ by elements of the form abc^{-1}, where $a, b, c \in C$. The topological group Γ is said to be *compactly presented* if there exists a compact subset $C \subset \Gamma$ which is a defining set for Γ as an abstract group.

THEOREM 3.15 (BEHR [2]). *Let G be a reductive group defined over a non-Archimedean local field K. Then G_K is compactly presented.*

PROOF: To prove that a topological group Γ is compactly presented it suffices to find a compact subset C of Γ generating Γ as an abstract group, and such that all the relations in Γ, written in terms of elements of C, follow from relations of a bounded length. (This remark will be used repeatedly below.)

First we consider the case where G is a simply connected simple K-group. Here the proof that G_K is compactly presented is obtained from the following assertion.

LEMMA 3.14. *Suppose a topological group Γ has an absolute value $|\ |$, which takes on integral values and has the following properties:*

(a) $|g| \ge 0$, $|1| \neq 0$;
(b) $|g_1 g_2| \le |g_1| + |g_2|$ *for all* g_1, g_2 *in* Γ;
(c) $|g^{-1}| = |g|$ *for all* g *in* Γ;
(d) $\Gamma_n = \{g \in \Gamma : |g| \le n\}$ *is compact, for each* n.

Assume, furthermore, that there are positive integers c, d, and b satisfying the following:

(i) *if $|g| > c$ then there are g_1, g_2 in Γ such that $g = g_1 g_2$ and $|g_1| < c$, $|g_2| < |g| - d$;*
(ii) *if f, g, $h \in \Gamma$ and $fgh = 1$, then there are $g_1, g_2, \dots, g_t$ in Γ such that $g = g_1 g_2 \dots g_t$, $|g_i| \le c$ $(i = 1, \dots, t)$, $t \le |g| + b$ and $|f g_1 \dots g_j| \le \max\{|f|, |h|\} + d$ $(j = 1, \dots, t-1)$.*

Then Γ is compactly presented.

PROOF: It follows from (d) and (i) that Γ_c is a compact generating set for Γ, and therefore it suffices to show that all the relations between the elements of Γ_c are consequences of relations of length l, where:

$$l \le l_0 = \max\left\{3c + b + 3,\ 2\left[\frac{c}{d+1}\right] + 5\right\},$$

where $[\ ]$ denotes the integral part. Since Γ_c contains 1 and is closed under taking inverses, it suffices to consider relations r of the form

$$g_1 g_2 \dots g_n = 1 \quad \text{for } g_i \in \Gamma_c.$$

Put $p_j = g_j g_{j+1} \dots g_n$ and define the norm $\|r\|$ to be $\max\limits_{1 \le j \le n} \{|p_j|\}$. First we shall show that any such r is a consequence of relations r' of the norm $\|r'\| \le 2c$. The proof is by induction on $\|r\|$. Suppose $\|r\| > 2c$ and let j be an index such that $\max\{|p_j|,\ |p_{j+1}|\} = \|r\|$. Then $\min\{|p_j|\ |p_{j+1}|\} > c$, since $|g_j| \le c$; so by (i) we can find g'_j, g'_{j+1} in Γ_c such that

$$|g_j'^{-1} p_j| < |p_j| - d \text{ and } |g_{j+1}'^{-1} p_{j+1}| < |p_{j+1}| - d.$$

Put $f = p_j^{-1} g'_j$, $g = g_j'^{-1} g_j g'_{j+1}$, $h = g_{j+1}'^{-1} p_{j+1}$. Then $fgh = 1$ and $\max\{|f|,\ |h|\} < \|r\| - d$. Applying (ii), we can find $\bar{g}_1, \dots, \bar{g}_t$ in Γ_c such that $g = \bar{g}_1 \dots \bar{g}_t$ for $t \le |g| + b$ and $|f g_1 \dots g_k| \le \max\{|f|,\ |h|\} + d$ for all $k = 1, \dots, t-1$. Since $|g| \le 3c$, we have $t \le 3c + b$. Consider the relations

$$r_j: \quad g_j = g'_j \bar{g}_1 \dots \bar{g}_t g_{j+1}'^{-1},$$

whose length does not exceed l_0. Now we replace g_j in r with the righthand side of r_j, for any j such that $\max\{|p|,\ |p_{j+1}|\} = \|r\|$ (where, of course, in case $|p_j| = \|r\|$ we choose the same g'_j for the pairs $(j-1, j)$ and $(j, j+1)$). Then for any $k \le t$ we have $|\bar{g}_k \dots \bar{g}_t g_{j+1}'^{-1} p_j| = |f \bar{g}_1 \dots \bar{g}_{k-1}| < \|r\|$. Thus we obtain an r' which is equivalent to r modulo the relations r_j, and for

which $\|r'\| < \|r\|$. Repeating this procedure, we eventually arrive at r_0 for which $\|r_0\| \leq 2c$.

Thus we have only to analyze

$$r: \quad g_1 g_2 \dots g_n = 1$$

satisfying $\|r\| \leq 2c$. Then for any $1 \leq j \leq n$ we have $|p_j| \leq 2c$ and therefore by (i) we can write p_j as a product of at most $\left(\left[\frac{c}{d+1}\right] + 2\right)$ elements from Γ_c. Let us write p_j^{-1} as a product of the inverses. Substituting these expressions into $g_j = p_j p_{j+1}^{-1}$ for $1 \leq j \leq n-1$ (respectively, in $g_n = p_n$, for $j = n$) we arrive at the relations whose lengths are bounded by $2\left[\frac{c}{d+1}\right] + 5 \leq l_0$. On the other hand, it is clear that r is a consequence of these relations. This completes the proof of the lemma.

To construct a function $|\ |$ on $\Gamma = G_K$ with the properties described in Lemma 3.14 we proceed as follows. Fix a maximal K-split torus $S \subset G$ (note that if $S = (e)$ then G_K is compact, by Theorem 3.1, so we may take $C = G_K$ as the compact defining set). Notation as above, let $R(S, G)$ be the relative root system. Then for $\mathfrak{g} = L(G)$ we have

$$\mathfrak{g} = \mathfrak{g}_0 \oplus \Big(\bigoplus_{\alpha \in R(S,G)} \mathfrak{g}_\alpha\Big),$$

where $\mathfrak{g}_0$ is the centralizer of $\operatorname{Ad} S$ and $\mathfrak{g}_\alpha$ is the weight space for $\operatorname{Ad} S$ of weight α. Take some lattices $L_0 \subset (\mathfrak{g}_0)_K$, $L_\alpha \subset (\mathfrak{g}_\alpha)_K$ and put $L = L_0 \oplus (\bigoplus_{\alpha \in R(S,G)} L_\alpha)$. Furthermore, let us introduce a distance between any two lattices $L_1, L_2 \subset \mathfrak{g}_K$:

$$d(L_1, L_2) = \min\{\, n : \pi^n L_1 \subseteq L_2 \subseteq \pi^{-n} L_1 \,\},$$

where $\pi \in K$ is a uniformizing parameter. Our objective is to show that all the requirements of Lemma 3.14 are met for the absolute value on $\Gamma = G_K$ given by

$$|g| = d(L, \operatorname{Ad}(g)L).$$

Properties (a)–(d) are immediate. To prove that Γ_n is compact for any $n > 0$ we merely note by restricting to $|\ |$ to Γ_n that $\operatorname{Ad}(\Gamma_n)$ is bounded and hence also compact; on the other hand, the map $\Gamma \to \operatorname{Ad}(\Gamma)$ is open (Proposition 3.3, Corollary 1), has finite kernel, and therefore is proper, i.e., the preimage of a compact subset is itself compact.

To verify (i) and (ii) we need a decomposition of G_K arising from the Cartan decomposition $G_K = \mathbf{K}Z^+\mathbf{K}$. Recall that Z^+ is the preimage of the

semigroup $T^+ \subset W$ under the natural homomorphism $\nu: N \to W = N/H$, where T is an abelian group generated by roots of R_0 and T^+ is the set of all t in T such that $\langle t, \alpha \rangle \geq 0$ for all simple roots α. The constructions from Bruhat-Tits theory imply that $\nu(S_K) \subset T$. But $S_K \simeq (K^*)^l \simeq \mathbb{Z}^l \times U^l$, where $l = \dim S$ and U is the group of units for K. On the other hand, since $H = \ker \nu$ is compact it follows that $\ker(\nu\,|_{S_K})$ is compact and hence $\ker(\nu\,|_{S_K}) \subset U^l$. Therefore $\nu(S_K)$ contains a free abelian subgroup of rank l. But T itself is a free abelian group of rank l, so $m = [T : \nu(S_K)]$ is finite. Hence $\nu(S_K) \supset mT$ and $\nu(S_K) \cap T^+ \supset mT^+$.

We leave it as an exercise for the reader to show that T^+ is a finitely generated semigroup. It follows that $\nu(S_K) \cap T^+$ is also a finitely generated semigroup. Put $S^+ = Z^+ \cap S_K$. We have $\nu(S^+) = \nu(S_K) \cap T^+$, implying $\nu(S^+) \supset mT^+$; consequently there exists a finite subset $E \subset Z^+$ such that $\nu(ES^+) = T^+$. Then $Z^+ = HES^+$ and

$$G_K = \mathbf{K}Z^+\mathbf{K} = \mathbf{K}ES^+\mathbf{K}. \tag{3.17}$$

Furthermore, for s in S_K and α in R_0 we have

$$\langle \nu(s), \alpha \rangle = v(\alpha(s)),$$

where v is the valuation on K. Therefore, taking into consideration that roots from R_0 and $R(S, G)$ are proportional, we obtain that $v(\alpha(s)) \geq 0$ for all s in S^+ and all roots α in $R(S, G)$ which are positive relative to the order pertaining to the system of simple roots $\Pi_0 \subset R_0$.

Now it is clear that for $|s|$ in S^+ we have $|s| = v(\alpha_0(s))$, where $\alpha_0 \in R(S, G)$ is the maximal root; in particular, if $s = s_1 s_2$ $(s, s_1, s_2 \in S^+)$, then $|s| = |s_1| + |s_2|$. As we have seen above, $\nu(S^+)$ is a finitely generated semigroup; therefore there exists an integer $r > 0$ such that the s in S^+ satisfying $|s| \leq r$ generate S^+ as a semigroup.

Let us introduce two more integers from which we shall derive the desired constants c, d and b satisfying Lemma 3.14. Namely, since $\mathbf{K}$ is compact and E finite, it follows that there exist integers c_1, c_2 such that $|k| \leq c_1$, $|e| \leq c_2$ for all k in $\mathbf{K}$ and e in E.

In proving (i), we put $c = 5c_1 + 2c_2 + r + d$, where d will be specified later. If $|g| > c$, and $g = k_1 e s k_2$ is a factorization from (3.17), then

$$|s| = |e^{-1}k_1^{-1} g k_2^{-1}| > 3c_1 + c_2 + r + d.$$

There exist s_1, s_2 in S^+ such that $s = s_1 s_2$ and $3c_1 + c_2 + d < |s_1| \leq 3c_1 + c_2 + r + d$. Then for $g_1 = k_1 e s_1$ and $g_2 = s_2 k_2$ we have

$$|g_1| \leq |s_1| + c_1 + c_2 \leq 4c_1 + 2c_2 + r + d \leq c,$$

$$|g_2| \le |s_2| + c_1 = |s| - |s_1| + c_1$$
$$< |g| + 2c_1 + c_2 + c_1 - (3c_1 + c_2 + d) = |g| - d.$$

Before we move on to prove (ii), one remark is in order. Note that $\pi^n \operatorname{Ad}(s)L \subset L$ for any s in S^+ implies $\pi^n L \subset \operatorname{Ad}(s)L$. It turns out that a somewhat weaker implication holds for any g in G_K. Namely, suppose $\pi^n \operatorname{Ad}(g)L \subset L$ for g in G_K. Choose a factorization $g = k_1 e s k_2$ as in (3.17). Then by properties (b) and (c) of the absolute value function we have $\pi^{n+2c_1+c_2} \operatorname{Ad}(s)L \subset L$, whence $\pi^{n+2c_1+c_2} L \subset \operatorname{Ad}(s)L$, and finally, $\pi^{n+4c_1+2c_2} L \subset \operatorname{Ad}(g)L$.

Now let f, g, h in G_K satisfy $fgh = 1$. Write g as $g = k_1 e s k_2$ and factor s into a product $s = s_1 \dots s_t$, where $s_i \in S^+$ and $|s_i| \le r$. Then, putting $g_1 = k_1 e s_1$, $g_2 = s_2, \dots, g_{t-1} = s_{t-1}$, $g_t = s_t k_2$, we obtain

$$|g_i| \le c_1 + c_2 + r \le c = 5c_1 + 2c_2 + r + d$$

with an arbitrary choice of d. Moreover, we may assume $t \le |s| \le |g| + b$, where $b = 2c_1 + c_2$. Given $j \in \{1, \dots, t-1\}$ we take the segments $u = s_1 \dots s_j$ and $v = s_{j+1} \dots s_t$. Then it follows from the definition of L that

$$\operatorname{Ad}(u)L \subset \operatorname{Ad}(s)L + L,$$

hence $\operatorname{Ad}(f k_1 e u)L \subset \operatorname{Ad}(f k_1 e s)L + \operatorname{Ad}(f k_1 e)L$, i.e., $\pi^n \operatorname{Ad}(f k_1 e u)L \subset L$ for $n = \max\{\, |f k_1 e s|,\ |f k_1 e| \,\}$. Therefore, it follows from our above remark that

$$|f k_1 e u| \le \max\{\, |f k_1 e s|,\ |f k_1 e| \,\} + 4c_1 + 2c_2.$$

On the other hand,

$$|f k_1 e s| \le |f k_1 e s k_2| + |k_2| \le |fg| + c_1 = |h| + c_1$$

and

$$|f k_1 e| \le |f| + |k_1 e| \le |f| + c_1 + c_2.$$

We conclude that

$$|f g_1 \dots g_j| \le \max\{\, |f|,\ |h| \,\} + (5c_1 + 3c_2).$$

Then, setting $d = 5c_1 + 3c_2$ (so that $c = 10c_1 + 5c_2 + r$), we obtain the required constants c, d and b.

We have concluded the proof that G_K is compactly presented when G is a simply connected simple K-group. The remainder of the proof consists of straightforward reductions to this case.

Indeed, suppose G is a simply connected semisimple K-group. Then G can be described as $\prod_{i=1}^{d} \mathbf{R}_{L/K}(G_i)$, where the G_i are simply connected simple groups defined over finite extensions L_i of K $(i = 1, \dots, d)$, so $G_K \simeq \prod_{i=1}^{d} (G_i)_{L_i}$. It is easy to see that a finite product of compactly presented groups is compactly presented; on the other hand, according to the above, all the $(G_i)_{L_i}$ are compactly defined. Therefore G is also compactly defined.

Finally let G be an arbitrary reductive K-group. Then $G = DT$ is an almost direct product, where D is semisimple and T is a maximal central torus in G. Let $\pi\colon \tilde{D} \to D$ denote a K-defined universal covering, and write T as an almost direct product $T = T_1 T_2$, where T_1 is K-split and T_2 is K-anisotropic. Put $H = \tilde{D} \times T_1 \times T_2$, let φ denote the isogeny $H \to G$, obtained from π and the product morphism, and let $F = \ker \varphi$. Then the exact sequence $1 \to F \to H \xrightarrow{\varphi} G \to 1$ yields the exact cohomological sequence

$$H_K \xrightarrow{\varphi} G_K \to H^1(K, F);$$

it follows from Proposition 3.3 and the finiteness theorem for Galois cohomology over local fields (which we shall establish in §6.4) that $\varphi(H_K)$ is an open subgroup of G_K of finite index (for semisimple G this fact also follows from Proposition 3.17).

We claim $\varphi(H_K)$ is a compactly presented group. Indeed, by assumption $H_K = \tilde{D}_K \times (T_1)_K \times (T_2)_K$. We showed above that $\tilde{D}_K$ is compactly presented. It follows from Theorem 3.1 that $(T_2)_K$ is compact, and hence compactly presented. Lastly, $(T_1)_K \simeq K^{*l} \simeq \mathbb{Z}^l \times U^l$, where $l = \dim T_1$ and U is the group of units in K, from which we clearly see that $(T_1)_K$ is compactly presented. Without loss of generality we may assume that the compact defining set $C \subset H_K$ contains F_K. Then it is easy to show that $\varphi(C)$ is a compact defining set for $\varphi(H_K)$. Therefore, the proof of Theorem 3.15 is completed by

LEMMA 3.15. *Let Γ be a locally compact topological group, and Δ an open normal subgroup of finite index. If Δ is compactly presented, then Γ also is compactly presented.*

PROOF: Let $D \subset \Delta$ be a compact defining set. From the outset we may assume that D contains the unit element. Moreover, passing from D to DD^{-1}, we may assume that $D = D^{-1}$. It suffices to construct a compact subset $C \subset \Gamma$ generating Γ and having the property that all the relations in Γ between the elements of C are consequences of relations of a bounded length. Let $\{x_i\}_{i=1}^{n}$ be a set of representatives of cosets Γ/Δ, containing

the unit element. Put $C = \bigcup_{i=1}^{n} x_i D$ and construct a system of defining relations between the elements of C. First of all, since $D \subset C$, we may consider the relations of the form

$$ab = c \tag{3.18}$$

for a, b, c in D which are satisfied in Δ (by our hypothesis, these relations define Δ). Furthermore, for any two indexes i, $j = 1, \dots, n$ there exists a unique index $k = k(i,j)$ such that $E_{ij} = x_k^{-1}((x_iD)(x_jD)) \subset \Delta$. Clearly E_{ij} is compact. By assumption $\Delta = \bigcup_{m=1}^{\infty} D^m$, where $D^m = D \dots D$; so by Baire's theorem (cf. Bourbaki [2, Ch. 9, §5, ¶ 3]) there exists $t \geq 1$ such that D^t contains an open subset U (containing 1) of Δ, and therefore $\Delta = \bigcup_{m=1}^{\infty} UD^m$ is an open covering of Δ. Since E_{ij} is compact it follows that $E_{ij} \subset D^{l(i,j)}$ for some integer $l(i,j) \geq 1$ (noting that $D^{k_1} \subset D^{k_2}$ when $k_1 \leq k_2$), i.e., $(x_iD)(x_jD) \subset x_kD^{l(i,j)}$. Put $l = \max_{i,j=1,\dots,n} l(i,j)$ and consider all the relations satisfied in Γ having the form

$$(x_ia)(x_jb) = x_{k(i,j)}d_1 \dots d_l, \quad \text{for } i, j = 1, \dots, n, \tag{3.19}$$

where a, b, $d_1, \dots, d_l \in D$.

To complete the proof of the lemma we shall show that (3.18) and (3.19) determine Γ. Indeed, let N be the normal subgroup of the free group $F(C)$ generated by (3.18) and (3.19), let $H = F(C)/N$, and let $\kappa: F(C) \to H$ and $\delta: H \to \Gamma$ be the corresponding homomorphisms. Put $L = \kappa(F(D))$. Then (3.18) are satisfied in L, and therefore δ restricts to an isomorphism from L to Δ. This shows that $\ker\delta \cap L$ consists only of the unity element. On the other hand, since (3.19) are satisfied in H, it clearly follows that any element from H has the form x_ky, where $k = 1, \dots, n$ and $y \in L$. Therefore $[H : L] \leq n = [\Gamma : \Delta]$; hence $[H : L] = [\Gamma : \Delta]$ and $\ker\delta = (e)$, proving the lemma.

3.5. Results needed from measure theory.

This section assembles results to be used later on, from the theory of integration over locally compact topological groups and associated spaces. Although concepts relating to integration play a leading role in the study of analytical aspects of the arithmetic theory of algebraic groups (for example, in defining the Tamagawa number) and in its application to the theory of automorphic forms, they play a secondary role in the exposition of the material included in this book (although they are essential at several key points, such as the proof of the strong approximation theorem in

Chapter 7.) For this reason, and also since the theory of integration itself is quite an extensive subject, we do not consider it feasible to give a fairly detailed exposition. As a result, this section recalls only the basic definitions of measure theory and statements of the results needed later on, and also contains some selected examples. A systematic exposition of measure theory and integration (including proofs of the assertions presented below) may be found in Bourbaki [3].

Let X be a locally compact topological space. Recall that $B \subset X$ is a *Borel subset* if it can be presented as a countable union or intersection of open subsets and closed subsets of X (in other words, is an element of the σ-algebra of subsets of X generated by the open and closed subsets). A nonzero measure μ on X is a *Borel measure* if all the Borel subsets are μ-measurable and $\mu(C) < \infty$ for any compact $C \subset X$.

Suppose that a group Γ acts on X by homeomorphisms. Then μ is said to be Γ-invariant if for any measurable subset $M \subset X$ and any γ in Γ the set $\gamma(M)$ is measurable and $\mu(\gamma(M)) = \mu(M)$. The most important example for our purposes is a locally compact topological group G acting on itself by left (or right) translations. In this case a (nonzero) invariant Borel measure on G is called a *left (or right) Haar measure.*

THEOREM 3.16. *Let G be a locally compact group. Then there is a left (right) Haar measure on G, which is unique up to multiplication by a positive constant.*

(Note that if μ is a left Haar measure on G, then $\hat{\mu}$, given by $\hat{\mu}(X) = \mu(X^{-1})$ for all $X \subset G$ such that X^{-1} is μ-measurable, is a right Haar measure on G. Therefore the assertions of the theorem for left and right Haar measures are equivalent.)

We shall take up somewhat later the question of an explicit description of the Haar measure in the cases of special interest to us, but for now we shall list several properties that hold in general.

PROPOSITION 3.23. *Let G be a locally compact group, and μ a (left) Haar measure on G. Then*

(1) *G is discrete if and only if $\mu(\{e\}) > 0$;*
(2) *G is compact if and only if $\mu(G) < \infty$.*

In particular, if G is compact then there is a unique (left) Haar measure μ on G for which $\mu(G) = 1$.

The uniqueness of the Haar measure in Theorem 3.16 allows us to associate with each (topological) automorphism φ of a topological group G a positive number, called the *module* of φ and designated as $\mathrm{mod}_G\varphi$. To be more precise, fix a left Haar measure μ on G, and put $\nu(X) = \mu(\varphi(X))$

for any $X \subset G$ such that $\varphi(X)$ is μ-measurable. Since φ takes Borel sets to Borel sets and compact sets to compact sets, ν will also be a left Haar measure on G. Then, by uniqueness, we must have $\nu = c\mu$, where $c \in \mathbb{R}$ and $c > 0$, and we define $\mathrm{mod}_G \varphi = c$. It is easy to see that $\mathrm{mod}_G \varphi$ is actually independent of the choice of the original Haar measure μ. (Example: if K_v is a locally compact field and $a \in K_v^*$, then the module of the left translation $x \mapsto ax$ regarded as an automorphism of the additive group K_v^+ is equal to the value $\|a\|_v$ of the normalized valuation, cf. §1.2.1.)

For $x \in G$ let $\Delta_G(x)$ denote the module of the corresponding inner automorphism $\varphi = \mathrm{Inn}\, x : g \mapsto xgx^{-1}$. The function $\Delta_G : G \to \mathbb{R}^+$ which then arises is called the *module* of G and is a continuous homomorphism. If $\Delta_G \equiv 1$ then G is said to be *unimodular*. Every left Haar measure μ on a unimodular group G is also a right Haar measure; moreover, $\mu(X) = \mu(X^{-1})$ for any measurable subset X of G.

PROPOSITION 3.24.

(1) *Any Abelian group is unimodular.*
(2) *The module of any automorphism of a discrete or compact group equals 1; hence such groups are unimodular.*

Now we shall consider the question of obtaining a Haar measure for various group-theoretic constructions, given Haar measures on the groups involved.

Clearly, to obtain a Haar measure on a finite direct product it suffices to consider the case of two components. Thus, let $G = G_1 \times G_2$, where each G_i is a locally compact group with Haar measure μ_i. Then G has a unique measure $\mu = \mu_1 \times \mu_2$ such that for any μ_i-measurable subsets M_i of G_i, the set $M = M_1 \times M_2$ is μ-measurable and

$$\mu(M) = \mu_1(M_1)\mu_2(M_2); \tag{3.20}$$

moreover, μ is a Haar measure. More generally, the product measure $\mu = \mu_1 \times \mu_2$ can be defined by (3.20) on any space of the form $X = X_1 \times X_2$, where X_i is a locally compact topological space equipped with measure μ_i $(i = 1, 2)$. We can reformulate (3.20) in terms of integrals with respect to the corresponding measures. Namely, let f_i be a μ_i-integrable function on X_i $(i = 1, 2)$ (i.e., $\int_{X_i} f_i(x_i)d\mu(x_i)$ exists). Then the function f on $X = X_1 \times X_2$, defined by $f(x_1, x_2) = f_1(x_1)f_2(x_2)$, is μ-integrable and

$$\int_X f(x_1, x_2)d\mu(x_1, x_2) = \int_{X_1} f_1(x_1)d\mu_1(x_1) \int_{X_2} f_2(x_2)d\mu_2(x_2).$$

Moreover, for any function f integrable over X we have

$$\int_X f(x_1, x_2)d\mu(x_1, x_2) = \int_{X_1} \left(\int_{X_2} f(x_1, x_2)d\mu_2(x_2) \right) d\mu_1(x_1)$$
$$= \int_{X_2} \left(\int_{x_1} f(x_1, x_2)d\mu_1(x_1) \right) d\mu_2(x_2).$$

Note that in general one cannot extend the definition of the product of measures to an infinite number of factors, since the product of an infinite number of locally compact, but not compact, groups is not a locally compact group. Other constructions must be used here. One of them is the restricted topological product, which formalizes the construction used when we introduced adeles (cf. §1.2).

DEFINITION: Let $\{X_\lambda\}_{\lambda \in \Lambda}$ be a family of locally compact topological spaces, indexed by a countable set of indices Λ. Assume that open compact subsets $K_\lambda \subset X_\lambda$ are fixed for almost all $\lambda \in \Lambda$. Consider the space X whose elements are the families $x = \{x_\lambda\}_{\lambda \in \Lambda}$ where $x_\lambda \in X_\lambda$ and $x_\lambda \in K_\lambda$ for almost all λ. Introduce a topology on X, taking for a fundamental system of open sets all sets of the form ΠU_λ, where $U_\lambda \subset X_\lambda$ is open for all λ and $U_\lambda = K_\lambda$ for almost all λ. The space X with this topology is called the *restricted topological product* of X_λ with respect to the distinguished subsets K_λ.

Let us point out several straightforward properties of this construction.

LEMMA 3.16.

(1) *For any finite subset S of Λ such that K_λ is defined for each $\lambda \in \Lambda \backslash S$, put $X_S = \prod_{\lambda \in S} X_\lambda \times \prod_{\lambda \in \Lambda \backslash S} K_\lambda$; then X_S is open in X and the topology of X induces the direct product topology on X_S.*
(2) *Each X_S is locally compact and $X = \bigcup_S X_S$, where the union is taken over all finite subsets S of Λ such that K_λ is given for each $\lambda \in \Lambda \setminus S$; consequently X is locally compact.*
(3) *If $\{G_\lambda\}_{\lambda \in \Lambda}$ is a family of locally compact topological groups and open compact subgroups K_λ of G_λ are given for almost all λ, then the restricted topological product G of G_λ with respect to the K_λ is a locally compact topological group.*

By (3) there exists a Haar measure on G; we shall show that it can be constructed from the Haar measures μ_λ on G_λ. To do so, let us first assume that μ_λ are normalized in such a way that $\mu_\lambda(K_\lambda) = 1$ for each λ such that K_λ is defined. Then, for any finite subset S of Λ such that K_λ is given for each λ in $\Lambda \setminus S$, one has μ_S on $G_S = \prod_{\lambda \in S} G_\lambda \times \prod_{\lambda \in \Lambda \backslash S} K_\lambda$, which, in

fact, is the "infinite" product of the μ_λ. More precisely, it can be defined as $\mu_1 \times \mu_2$, where μ_1 is the usual finite product of μ_λ on $\prod_{\lambda \in S} G_\lambda$ and μ_2 is the Haar measure on the compact group $K_S = \prod_{\lambda \in \Lambda \setminus S} K_\lambda$, normalized by $\mu_2(K_S) = 1$. It is easy to see that if $S_1 \subset S_2$ then $G_{S_1} \subset G_{S_2}$, and the restriction of μ_{S_2} to G_{S_1} is μ_{S_1}. Therefore, using countable additivity and representing G as the countable union $G = \bigcup_S G_S$, we obtain the desired μ on G extending μ_S. Sometimes, in defining μ on G, it will be useful to waive the condition $\mu_\lambda(K_\lambda) = 1$ and instead to require absolute convergence of $\prod \mu_\lambda(K_\lambda)$ over all λ for which K_λ is defined. Then the measure μ constructed above is replaced by $c\mu$, where $c = \prod \mu_\lambda(K_\lambda)$.

Now we take up the problem of constructing an invariant measure on the quotient space $X = G/H$, where G is a locally compact topological group and H is a closed subgroup (note that here, of course, invariance is with respect to the action of G on X by translations).

THEOREM 3.17. *A nonzero G-invariant Borel measure β on $X = G/H$ exists if and only if the restriction of the module Δ_G to H coincides with Δ_H; if β exists, it is uniquely determined up to a positive scalar.*

In particular, if H is a discrete subgroup of G (the basic case of interest to us in what follows), then an invariant measure on G/H exists if and only if G is unimodular. Note also that the phrase "G/H has finite invariant measure (or volume)" means that there exists an invariant measure on G/H and that the volume of G/H with respect to this measure is finite.

A connection can be found between the "quotient measure" β and the Haar measures μ and ν on G and H respectively. This is best done in terms of integrals of functions with respect to these measures. Thus, consider a function f integrable over G and, fixing g in G, put $\varphi(g) = \int_H f(gh)d\nu(h)$. Then φ is a function on G, constant on cosets modulo H, and therefore it can be regarded as a function on $X = G/H$. In this sense we have the following formula:

$$\int_X \left(\int_H f(gh)d\nu(h) \right) d\beta(gH) = \int_G f(g)d\mu(g). \tag{3.21}$$

On the whole, the definition of β provided by (3.21) is not explicit; however, in the basic case of a discrete subgroup H, which is of interest to us, integration in G/H with respect to β can be reduced to integration over suitable subsets of G with respect to the original measure μ (actually, we then must impose an extra condition on G of the existence of a countable fundamental system of neighborhoods of the identity, although this requirement is automatically satisfied in all the cases of interest to us).

We shall say that a subset $F \subset G$ is a *fundamental domain with respect to H* if the restriction to F of the natural map $\pi: G \to G/H$ is bijective. This can also be stated in the form of the following two conditions:

$$\begin{aligned} &1) \quad G = FH, \\ &2) \quad F \cap Fh = \emptyset \quad \text{for any } h \neq e \text{ in } H. \end{aligned} \tag{3.22}$$

In the given situation there always exists a μ-measurable fundamental domain $F \subset G$; moreover it can actually be extracted from any measurable subset $\Omega \subset G$ satisfying $\pi(\Omega) = G/H$. Then (3.21) yields

$$\int_X f(x)d\beta(x) = \int_F f(\pi(g))d\mu(g), \tag{3.23}$$

for any function f integrable over X.

Sometimes it will be helpful to use a more general definition of the fundamental domain, in which 1) of (3.22) remains the same but 2) is replaced by the following:

$$2') \quad F \cap Fh \text{ has measure 0, for any } h \neq e \text{ in } H.$$

A typical instance of such a situation is the case where F is a closed subset of G with boundary of measure 0, covering G/H, and such that the translations of F have points in common only at the boundary; cf., for instance, the classic example presented in §4.2 of a fundamental domain of $SL_2(\mathbb{R})$ with respect to $SL_2(\mathbb{Z})$). Using the countability of H it is easy to show that (3.23) still holds even under this more general definition of the fundamental domain. If we take $f \equiv 1$ in (3.23), we obtain that $X = G/H$ has finite invariant measure if and only if there exists a measurable fundamental domain $F \subset G$ (relative to H) having finite measure, and then every measurable fundamental domain has a finite measure. Since we can find a fundamental domain in any measurable subset covering X, we can reformulate this criterion in a manner more useful in applications: X has finite measure if and only if it is covered by a set with finite measure.

EXAMPLE 1: let $G = \mathbb{R}^n$. Then the usual Lebesgue measure on G is both a right and left Haar measure. If we view x in $GL_n(\mathbb{R})$ as a topological automorphism of G, then it follows from the change of variables formula in multiple integrals that $\mathrm{mod}_G x = |\det x|$. In particular, the transformations in $SL_n(\mathbb{R})$ are unimodular, i.e., preserve the measure. Now let $e_1, \ldots, e_n$ be a base of $\mathbb{R}^n$, and let H denote the lattice $\mathbb{Z}e_1 \oplus \ldots \oplus \mathbb{Z}e_n$. Then H is a discrete subgroup of $\mathbb{R}^n$, $F = \{t_1e_1 + \cdots + t_ne_n : 0 \leq t_i < 1\}$ is a fundamental domain satisfying 1) and 2), and $F' = \{t_1e_1 + \cdots + t_ne_n : 0 \leq t_i \leq 1\}$ is a fundamental domain satisfying 1) and 2').

The above example is atypical in the sense that attempts to construct a fundamental domain satisfying 1) and 2) or 1) and 2′) explicitly in general do not succeed. For this reason in Chapters 4 and 5 we shall have to resort to a more general treatment of *fundamental sets*, as we shall call (closed) subsets $\Phi \subset G$ for which $G = \Phi H$ and $\Phi^{-1}\Phi \cap H$ is finite. Even if such a fundamental set is available, we may not be able to determine precisely the volume of $X = G/H$; nevertheless, we are in a position to draw qualitative conclusions about its finiteness or infiniteness. Indeed, if Φ has finite measure, then it follows from the above remarks that X has finite measure. Conversely, if X has finite measure, then, by taking a measurable fundamental domain $F \subset \Phi$, we could obtain $\Phi \subset \cup Fh$, where h runs through some finite subset of H, which means that Φ also has finite measure. Thus, G/H has finite measure if and only if there exists a fundamental subset $\Phi \subset G$ of finite measure.

Let us point out one straightforward property of quotient measures: let $H_1 \subset H_2$ be two closed subgroups of a locally compact group G, and suppose G/H_1 has finite G-invariant measure; then G/H_2 also has a finite G-invariant measure. Using this assertion, we have

LEMMA 3.17. *Let $G = G_1 \times G_2$ be the direct product of two locally compact topological groups, G_1 noncompact, and let $p_i: G \to G_i$ be the respective projections. Let $H \subset G$ be a closed subgroup such that G/H has finite invariant measure. Then $p_2(H)$ is non-discrete and there exists a finite invariant measure on $G_2/\overline{p_2(H)}$, where $\overline{\ }$ denotes closure.*

Indeed, suppose that $p_2(H)$ is discrete; then we can find a neighborhood of the identity $U \subset G_2$ such that $U^{-1}U \cap p_2(H) = \{e\}$. Then the restriction to $G_1 \times U$ of the natural map $G \to G/H$ is one-to-one, and therefore $G_1 \times U$ has finite measure. Let μ_i denote the Haar measure on G_i (for $i = 1, 2$), and put $\mu = \mu_1 \times \mu_2$. Then $\mu(G_1 \times U) = \mu_1(G_1)\mu_2(U)$, and since $\mu_2(U) \neq 0$ by the openness of U, we see that $\mu_1(G_1)$ is finite. But then G_1 is compact (Proposition 3.23), a contradiction. The assertion about the existence of a finite invariant measure for $G_2/\overline{p_2(H)}$ follows from the above remark applied to the closed subgroup $\Gamma \subset G_1 \times \overline{p_2(H)}$ of G, noting that $G_2/\overline{p_2(H)} \simeq G/(G_1 \times \overline{p_2(H)})$.

Now we move on to the explicit description of Haar measures in the cases of interest to us. First, we must present a result which applies to real algebraic groups via use of the Iwasawa decomposition (cf. §3.2).

PROPOSITION 3.25. *Let G be a unimodular locally compact topological group and let H, A and U be closed subgroups of G with left Haar measures ν, θ and ω respectively, such that the product morphism $H \times A \times U \to G$ is a homeomorphism. Assume that A normalizes U and that A and U are unimodular. Then $\mu = \varrho(a)\nu(h) \times \theta(a) \times \omega(u)$ is a left Haar measure on G, where $\varrho(a) = mod_U(\mathrm{Inn}\, a\,|_U)$.*

(This notation for μ indicates that the measure of $E \subset G$ is computed by

$$\mu(E) = \int_E \varrho(a)d\nu(h)d\theta(a)d\omega(u).)$$

Other explicit examples of Haar measures can be obtained by integrating differential forms. (The necessary background on differential forms, although only in the context of real varieties, can be found in any book on differential geometry, such as Helgason [1].) Let X be an n-dimensional analytic variety over a complete field K_v, let $x_0 \in X$, and let $x_1, \ldots, x_n$ be local coordinates for a neighborhood of x_0. This means that the x_i are analytic functions such that $\varphi: x \mapsto (x_1(x), \ldots, x_n(x))$ gives an analytic isomorphism of the neighborhood of x_0 onto a domain in K_v^n (i.e., φ is the inverse map of some parametrization of a neighborhood of x_0), or, equivalently, $d_{x_0}\varphi$ realizes an isomorphism from $T_{x_0}(X)$ to K_v^n. A *differential form of degree n in the neighborhood of x_0* is an expression of the form $\omega = f(x)dx_1 \wedge \ldots \wedge dx_n$, where f is an analytic function in the neighborhood of x_0.

Suppose $F: Y \to X$ is an analytic map of two n-dimensional varieties, $y_0 \in Y$ is a point satisfying $F(y_0) = x_0$, and $y_1, \ldots, y_n$ are local coordinates in a neighborhood of y_0. If in coordinate notation F is given by

$$(y_1, \ldots, y_n) \mapsto (F_1(y_1, \ldots, y_n), \ldots, F_n(y_1, \ldots, y_n)),$$

then the image of the differential form ω is defined to be

$$F^*(\omega) = f(F(y))dF_1(y_1, \ldots, y_n) \wedge \ldots \wedge dF_n(y_1, \ldots, y_n),$$

where, as usual, $dF_i(y_1, \ldots, y_n) = \sum_{j=1}^n \frac{\partial F_i}{\partial y_j} dy_j$. In particular, in this way we can define the transformation of a local differential form with respect to change of local coordinates. Now we can define an n-dimensional differential form on the entire variety X as a family of n-dimensional local differential forms in a neighborhood of each point of X, which agree with respect to all the various local coordinates in a neighborhood of the same point. We say that a differential form ω on X is *invariant* with respect to an analytic automorphism $F: X \to X$ if $F^*(\omega) = \omega$.

The discussion which follows below deals, on the whole, with analytic varieties that arise from algebraic varieties; therefore we shall now introduce the algebraic analogs of the corresponding "analytic" definitions. Let X be a smooth n-dimensional algebraic variety defined over K. Then a K-defined

system of local parameters in the neighborhood of x_0 in X is a system of K-rational functions $x_1, \dots, x_n$, defined at x_0, such that the differential $d_{x_0}\varphi$ of the rational map $\varphi: X \to \mathbb{A}^n$ given by $\varphi: x \mapsto (x_1(x), \dots, x_n(x))$ is an isomorphism of tangent spaces. Then an n-dimensional differential form over K in the neighborhood of x_0 is defined as an expression of the form $\omega = f(x)dx_1 \wedge \dots \wedge dx_n$, where f is a K-rational function on X defined at x_0. The concepts of transformation of differential forms under rational maps, of a differential form defined over the entire variety, and of an invariant differential form are analogous to the notions introduced above. Note that if X is defined over a complete field K_v and $x \in X_{K_v}$, then any rational differential K_v-form in a neighborhood of x_0 can also be viewed as an analytic differential form on X_{K_v} in a neighborhood of x_0.

Now let G be a connected algebraic K-group and let $n = \dim G$. Then it is well known that there exists a nonzero n-dimensional rational differential K-form ω on G which is invariant under left translation (i.e., is left-invariant), and moreover this form is uniquely determined up to multiplication by a nonzero element of K. Let us present several examples.

EXAMPLE 2: Let $G = \mathbf{GL}_n$. For a system of local parameters, let us take the functions x_{ij} $(i, j = 1, \dots, n)$, where x_{ij} applied to a matrix is the i-j entry of the matrix. Let $\omega = f(X)dx_{11} \wedge \dots \wedge dx_{nn}$ where $X = (x_{ij})$ be a left-invariant differential form. Fix $A = (a_{ij}) \in \mathbf{GL}_n$. Then the left translation $\lambda_A: X \mapsto AX$ can be written in coordinates as $x'_{ij} = \sum_k a_{ik}x_{kj}$. It follows that the translation λ_A^* of $f(X')dx'_{11} \wedge \dots \wedge dx'_{nn}$ is

$$f(AX)d(\sum_k a_{1k}x_{k1}) \wedge \dots \wedge d(\sum_k a_{nk}x_{kn}) = f(AX)(\det A)^n dx_{11} \wedge \dots \wedge dx_{nn}.$$

Therefore, by the invariance condition, we obtain $f(X) = f(AX)(\det A)^n$. Putting $X = E_n$, we have $f(A) = c(\det A)^{-n}$, where $c = f(E_n)$, i.e.,

$$\omega = \frac{c dx_{11} \wedge \dots \wedge dx_{nn}}{(\det(x_{ij}))^n}.$$

In particular, for $n = 1$ we have $\omega = \frac{cdx}{x}$.

EXAMPLE 3: Let $G = \mathbf{SL}_2$. As a system of local parameters in the neighborhood of 1 let us take the functions x, y, and z which associate the respective components with the matrix $X = \left(\begin{smallmatrix} x & y \\ z & t \end{smallmatrix}\right) \in G$, where $t = \frac{1+yz}{x}$. We look for a left-invariant differential form of the form $\omega = f(X)dx \wedge dy \wedge dz$. The left translation by $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G$ in these coordinates is written as

$$\begin{aligned} x' &= ax + bz, \\ y' &= ay + b\frac{1+yz}{x}, \\ z' &= cx + dz. \end{aligned}$$

Then by the invariance condition, we obtain

$$\begin{aligned} f(X')dx' \wedge dy' \wedge dz' &= f(AX)d(ax + bz) \wedge d(ay + b\frac{1+yz}{x}) \wedge d(cx + dz) \\ &= f(X)dx \wedge dy \wedge dz. \end{aligned}$$

In other words,

$$f(AX)\frac{ax + bz}{x} = f(X).$$

Noting that $ax + bz$ is the element in the 1-1 position of the matrix AX, we obtain

$$f(AX)(AX)_{11} = f(X)(X)_{11},$$

hence ω has the form

$$\omega = \frac{\alpha}{x}dx \wedge dy \wedge dz.$$

Now we obtain an expression for $\omega = \frac{1}{x}dx \wedge dy \wedge dz$ in another system of coordinates. Consider $G_{\mathbb{R}} = SL_2(\mathbb{R})$, and use the polar coordinates on $G_{\mathbb{R}}$, provided by the Iwasawa decomposition (cf. §3.2). In this situation the Iwasawa decomposition asserts that any matrix from $G_{\mathbb{R}}$ can be uniquely presented as a product of three matrices:

$$\begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}, \quad \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix} \ (\alpha > 0), \quad \text{and} \quad \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}.$$

Take φ, α and u as (analytic) coordinates on $G_{\mathbb{R}}$. Then direct computation shows that $x = \alpha\cos\varphi$, $y = \alpha u\cos\varphi - \alpha^{-1}\sin\varphi$, $z = \alpha\sin\varphi$, and therefore $\omega = \alpha d\varphi \wedge d\alpha \wedge du$.

EXAMPLE 4: (Exercise.) Let $\mathbf{U}_n$ be the group of upper triangular unipotent matrices of degree n. Show that the differential form $\prod_{i<j} dx_{ij}$ is a left-invariant form on $\mathbf{U}_n$. Derive a generalization of this result for an arbitrary unipotent group.

Now we move on to the determination of the measure corresponding to a differential form. Again let X be an n-dimensional analytic variety over the field K_v, let $x_0 \in X$, let $x_1, \dots, x_n$ be a system of local coordinates in a neighborhood of x_0, and let $\omega = f(x)dx_1 \wedge \dots \wedge dx_n$ be a nonzero local n-dimensional differential form in some neighborhood of x_0. Then on this neighborhood we can define the measure $\mu = |f(x)|_v|dx_1|_v \times \dots \times |dx_n|_v$ (which means that $\mu(E) = \int_E |f(x)|_v|dx_1|_v \dots |dx_n|_v$), where $|dx|_v$ is the (additive) Haar measure on K_v, which is the ordinary Lebesgue measure if K is $\mathbb{R}$ or $\mathbb{C}$, and in the v-adic case is normalized so that $\mathcal{O}_v$ has measure 1.) Then one proves that this measure is independent of the choice of the

system of local coordinates (in the Archimedean case this follows from the change of variables formula in the definite integral, and in the non-Archimedean case from its v-adic analog, cf. Weil [4]). Lastly, we establish that if ω is a differential form defined over the entire variety and nowhere vanishing, then the local measures extend to a measure on the entire variety. We denote the measure thus obtained by ω_v.

THEOREM 3.18. *Let G be an algebraic K_v-group, let $n = \dim G$, and let ω be an n-dimensional left-invariant differential form defined over K_v. Then ω_v is a left Haar measure on G_{K_v}. The group G_{K_v} is unimodular if and only if ω is also right-invariant.*

This theorem and the examples cited above produce explicit descriptions of Haar measures. Thus, the Haar measure on $GL_n(K_v)$ is given by $\int \frac{dx_{11}\ldots dx_{nn}}{|\det(x_{ij})|_v^n}$. In particular, if we apply this to $n = 1$ we obtain that for an l-dimensional split torus $S = \{\mathrm{diag}(\alpha_1, \ldots, \alpha_l)\}$ the Haar measure on S_{K_v} is defined as $\int \frac{d\alpha_1\ldots d\alpha_l}{\alpha_1\ldots\alpha_l}$. Next, for the group of n-dimensional upper triangular unipotent matrices $\mathbf{U}_n$ the Haar measure of $\mathbf{U}_{nK}$ has the form $\int \prod_{i<j} dx_{ij}$. Therefore if we consider the automorphism φ of $\mathbf{U}_{nK_v}$ given by conjugation by the matrix $s = \mathrm{diag}(\alpha_1, \ldots, \alpha_n)$, then $\mathrm{mod}\varphi = \prod_{i<j} |\alpha_i/\alpha_j|_v$. This example obviously generalizes to the maximal unipotent K_v-subgroup of an arbitrary reductive K_v-group.

Now let $G = \mathbf{SL}_2$. For $SL_2(\mathbb{R})$ we obtain the expression $\int \alpha d\varphi d\alpha du$ for the Haar measure, in the coordinates provided by the Iwasawa decomposition. Since $\frac{d\alpha}{\alpha}$ is the Haar measure on $A = \{\mathrm{diag}(\alpha, \alpha^{-1}) : \alpha \in \mathbb{R}^+\}$, this coincides with the expression for the Haar measure obtained from Proposition 3.25.

Lastly, to give an example of p-adic integration, we compute the volume of $\omega_p(SL_2(\mathbb{Z}_p))$, with respect to the Haar measure ω_p on $SL_2(\mathbb{Q}_p)$ corresponding to the differential form $\omega = \frac{1}{x} dx \wedge dy \wedge dz$ from Example 3. To do so, note that $\omega_p(SL_2(\mathbb{Z}_p)) = |SL_2(F_p)|\omega_p(SL_2(\mathbb{Z}_p, p))$, and all that remains is to compute the volume of the congruence subgroup $\Gamma = SL_2(\mathbb{Z}_p, p)$. But x, y, z map Γ onto $p\mathbb{Z}_p \times p\mathbb{Z}_p \times p\mathbb{Z}_p$ and on Γ we have $|\frac{1}{x}|_p = 1$. Therefore $\omega_p(\Gamma) = (\mu_p(p\mathbb{Z}_p))^3$, where μ_p is the Haar measure on $\mathbb{Q}_p$ normalized by $\mu_p(\mathbb{Z}_p) = 1$. Thus, finally, $\omega_p(\Gamma) = p^{-3}$ and $\omega_p(SL_2(\mathbb{Z}_p)) = p^{-3}|SL_2(F_p)| = p^{-3}p(p^2 - 1) = 1 - \frac{1}{p^2}$.

In conclusion, we note that Theorem 3.18 yields

COROLLARY. *Let G be a semisimple algebraic K_v-group. Then G_{K_v} is unimodular.*

Indeed, let ω be a left-invariant rational K_v-differential form on G of dimension $n = \dim G$. Let ρ_g denote right translation by $g \in G$. Then the fact that left and right translations commute implies that $\rho_g^*(\omega)$ is a left-invariant form; so, since ω is unique, we must have $\rho_g^*(\omega) = \chi(g)\omega$, where $\chi(g)$ is a nonzero constant. Further, it is easy to see that $g \mapsto \chi(g)$ is a rational character of G, and therefore $\chi = 1$, since G is semisimple. Thus, we have shown that ω is also a right-invariant form; therefore the unimodularity of G_{K_v} is an immediate consequence of Theorem 3.18.

4. Arithmetic Groups and Reduction Theory

Arithmetic groups are one of the basic objects studied in the arithmetic theory of algebraic groups. Their properties will be examined or used throughout the remainder of the book. The goal of the present chapter is to expound the theory of reduction for arithmetic groups, which provides the construction of a fundamental set for the group of real points $G_{\mathbb{R}}$ of an algebraic $\mathbb{Q}$-group G with respect to the group of integral points $G_{\mathbb{Z}}$. As a consequence we obtain several basic group-theoretic results on arithmetic subgroups, especially that they are finitely generated and can be defined by finitely many relations. Moreover, we give criteria for $G_{\mathbb{R}}/G_{\mathbb{Z}}$ to be compact or to have finite Haar measure. The final section of this chapter discusses an unsolved problem concerning finite arithmetic groups.

4.1. Arithmetic groups.

We begin with

DEFINITION: Let $G \subset GL_n(\mathbb{C})$ be a linear algebraic group defined over $\mathbb{Q}$. A subgroup $\Gamma \subset G$ is *arithmetic* if it is commensurable with $G_{\mathbb{Z}}$, i.e., if $\Gamma \cap G_{\mathbb{Z}}$ has finite index both in Γ and in $G_{\mathbb{Z}}$.[1]

Henceforth $G_{\mathbb{Z}}$ denotes $G \cap GL_n(\mathbb{Z})$. $G_{\mathbb{Z}}$ can also be viewed as the group of $\mathbb{Z}$-points of G, as a group scheme. That is, the embedding $GL_n(\mathbb{C}) \to GL_{n+1}(\mathbb{C})$, considered in §2.1.1, identifies $GL_n(\mathbb{C})$ with a Zariski-closed subset of $M_{n+1}(\mathbb{C}) = \mathbb{C}^{(n+1)^2}$. Then G is also closed in $M_{n+1}(\mathbb{C})$ and $G_{\mathbb{Z}} = G \cap M_{n+1}(\mathbb{Z})$. This will enable us to avoid cumbersome notation, such as $(\det a)^{-1}$, in the material that follows. Note also, that in accordance with the custom originating with the theory of integral automorphisms of quadratic forms, occasionally we shall call $G_{\mathbb{Z}}$ the group of units of G.

Clearly (cf. Proposition 4.3) groups of integral points may change considerably under rational morphisms. Thus, given an algebraic group G of transformations of a vector space V, in order to obtain a well-defined group of integral points $G_{\mathbb{Z}}$ we must fix a base $e_1, \ldots, e_n$ of $V_{\mathbb{Q}}$ or, equivalently, a lattice $L = \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_n$; then $G_{\mathbb{Z}}$ is the stabilizer $G_{\mathbb{Z}}^L = \{ g \in G_{\mathbb{Q}} : g(L) = L \}$ of L in $G_{\mathbb{Q}}$. Nevertheless, the class of arithmetic subgroups defined via groups of integral points has the following invariance property.

PROPOSITION 4.1. *Let $\varphi: G \to G'$ be a $\mathbb{Q}$-defined isomorphism of linear algebraic $\mathbb{Q}$-groups. If Γ is an arithmetic subgroup of G, then $\varphi(\Gamma)$ is an arithmetic subgroup of G'.*

[1] Note that the concept of commensurability makes sense for arbitrary subgroups of an abstract group.

PROOF: First note the following elementary group-theoretic fact: commensurability is an equivalence relation on the subgroups of a given group (in particular, any two arithmetic subgroups are commensurable). Hence to prove the proposition it suffices to establish the commensurability of $\varphi(G_{\mathbb{Z}})$ and $G'_{\mathbb{Z}}$. Furthermore, since

$$[G'_{\mathbb{Z}} : G'_{\mathbb{Z}} \cap \varphi(G_{\mathbb{Z}})] = [\varphi^{-1}(G'_{\mathbb{Z}}) : \varphi^{-1}(G'_{\mathbb{Z}}) \cap G_{\mathbb{Z}}],$$

where $\varphi^{-1}: G' \to G$ is the inverse rational $\mathbb{Q}$ morphism, the problem reduces to proving $[\varphi(G_{\mathbb{Z}}) : \varphi(G_{\mathbb{Z}}) \cap G'_{\mathbb{Z}}]$ finite for any $\mathbb{Q}$-isomorphism φ. We shall find a subgroup $H \subset G_{\mathbb{Z}}$ of finite index, whose image $\varphi(H)$ lies in $G'_{\mathbb{Z}}$; then $\varphi(G_{\mathbb{Z}}) \cap G'_{\mathbb{Z}} \supset \varphi(H)$, so that

$$[\varphi(G_{\mathbb{Z}}) : \varphi(G_{\mathbb{Z}}) \cap G'_{\mathbb{Z}}] \leq [\varphi(G_{\mathbb{Z}}) : \varphi(H)] < \infty,$$

as required. It turns out that such a subgroup H exists for any rational $\mathbb{Q}$-morphism, and not only for a $\mathbb{Q}$-isomorphism.

LEMMA 4.1. *Let $\varphi: G \to G'$ be a rational $\mathbb{Q}$-morphism. Then there exists a subgroup $H \subset G_{\mathbb{Z}}$ of finite index, such that $\varphi(H) \subset G'_{\mathbb{Z}}$.*

PROOF: Let $G \subset GL_n(\mathbb{C})$ and let $G' \subset GL_m(\mathbb{C})$. Without loss of generality we may assume that G and G' are Zariski-closed in $M_n(\mathbb{C})$ and $M_m(\mathbb{C})$ respectively. Then φ can be written as $\varphi((x_{ij})) = (\varphi_{kl}(x_{11}, \ldots, x_{nn}))$ for $i, j = 1, \ldots, n$ and $k, l = 1, \ldots, m$, where the φ_{kl} are polynomials with rational coefficients. We introduce new variables $y_{ij} = x_{ij} - \delta_{ij}$ (δ_{ij} being the Kronecker delta), and put

$$\psi_{kl}(y_{11}, \ldots, y_{nn}) = \varphi_{kl}(x_{11}, \ldots, x_{nn}) - \delta_{kl}.$$

Since $\varphi(E_n) = E_m$, we have $\psi_{kl}(0, \ldots, 0) = 0$ for $k, l = 1, \ldots, m$, i.e., ψ_{kl} are polynomials with zero constant term. Since the coefficients of ψ_{kl} are rationals, there is an integer d such that all $d\psi_{kl}$ have integral coefficients. Let H denote the congruence subgroup $G_{\mathbb{Z}}(d)$ of level d, i.e., the set of matrices of $G_{\mathbb{Z}}$ congruent to E_n modulo d. Then $H = G_{\mathbb{Z}} \cap GL_n(\mathbb{Z}, d)$, where $GL_n(\mathbb{Z}, d)$ is the congruence subgroup of level d in $GL_n(\mathbb{Z})$. Clearly $GL_n(\mathbb{Z}, d)$ is the kernel of the reduction homomorphism $GL_n(\mathbb{Z}) \to GL_n(\mathbb{Z}/d\mathbb{Z})$, which sends each integral matrix to the matrix whose entries are the residues of the respective entries modulo d, and therefore is a normal subgroup of finite index no greater than the order of the finite group $GL_n(\mathbb{Z}/d\mathbb{Z})$. Consequently H is a normal subgroup of $G_{\mathbb{Z}}$ of finite index. On the other hand, if $h = (h_{ij}) \in H$, then $\varphi_{kl}(h) = \psi_{kl}(h - E_n) + \delta_{kl} \in \mathbb{Z}$, since all $h_{ij} - \delta_{ij}$ are multiples of d. Thus $\varphi(H) \subset G'_{\mathbb{Z}}$. Q.E.D.

COROLLARY 1. *Let Γ be an arithmetic subgroup of an algebraic $\mathbb{Q}$-group G. Then $g\Gamma g^{-1}$ is also an arithmetic group, for any g in $G_{\mathbb{Q}}$.*

COROLLARY 2. *Let $G = HN$ be a semidirect product ($N \lhd G$) defined over $\mathbb{Q}$. Then the subgroup $H_{\mathbb{Z}}N_{\mathbb{Z}}$ has finite index in $G_{\mathbb{Z}}$.*

Indeed, let us consider the rational $\mathbb{Q}$-morphism $\varphi: G \to H$, given by $\varphi: g = hn \mapsto h$. By Lemma 4.1, there is a subgroup $M \subset G_{\mathbb{Z}}$ of finite index such that $\varphi(M) \subset H_{\mathbb{Z}}$. Then $m = \varphi(m)(\varphi(m)^{-1}m) \in H_{\mathbb{Z}}N_{\mathbb{Z}}$ for m in M; so $M \subset H_{\mathbb{Z}}N_{\mathbb{Z}}$, which gives the required result.

The congruence groups $GL_n(\mathbb{Z}, d)$ and $G_{\mathbb{Z}}(d)$, introduced in the proof of Lemma 4.1, play an important role in the arithmetic theory of algebraic groups. We will encounter them time and again, both as a natural technical tool and as an object of study *per se* (cf. §9.5).

It should be noted that the definition of an arithmetic subgroup does not require the condition $\Gamma \subset G_{\mathbb{Q}}$. Some important classes of arithmetic subgroups (such as maximal ones) are not necessarily contained in $G_{\mathbb{Q}}$. On the other hand, arithmetic subgroups contained in $G_{\mathbb{Q}}$ can naturally be described as subgroups of finite index of groups of integral points corresponding to the various possible realizations of G. Namely, we have the following "global" analog of Proposition 1.12.

PROPOSITION 4.2. *Let $G \subset GL_n(\mathbb{C})$ be an algebraic $\mathbb{Q}$-group and let $\Gamma \subset G_{\mathbb{Q}}$ be an arithmetic subgroup. Then there exists a Γ-invariant lattice $L \subset \mathbb{Q}^n$. Moreover, the index of Γ in $G^L_{\mathbb{Z}}$ is finite.*

PROOF: Let $e_1, \ldots, e_n$ be the standard base of $\mathbb{Q}^n$; let M denote the lattice $e_1\mathbb{Z} + \cdots + e_n\mathbb{Z}$. Since by hypothesis $[\Gamma : \Gamma \cap G^M_{\mathbb{Z}}]$ is finite, there are only a finite number of distinct lattices of the form $\gamma(M)$, for γ in Γ. It follows that the $\mathbb{Z}$-submodule $L \subset \mathbb{Q}^n$ generated by $\bigcup_{\gamma \in \Gamma} \gamma(M)$ will be finitely generated, i.e., is a lattice. Obviously, then, $\Gamma \subset G^L_{\mathbb{Z}}$. Furthermore, $G^L_{\mathbb{Z}}$ is a group of integral points relative to some basis $w_1, \ldots, w_n$ of L, and hence is arithmetic by Proposition 4.1. Thus $\Gamma \subset G^L_{\mathbb{Z}}$ are arithmetic subgroups, so $[G^L_{\mathbb{Z}} : \Gamma]$ must be finite. Q.E.D.

REMARK: By the same argument, using Lemma 4.1 we can prove a somewhat more general result: if $\varrho: G \to GL(V)$ is a $\mathbb{Q}$-representation of an algebraic $\mathbb{Q}$-group G and $\Gamma \subset G_{\mathbb{Q}}$ is an arithmetic subgroup, then there exists a lattice $L \subset V_{\mathbb{Q}}$ which is invariant under $\varrho(\Gamma)$. Moreover, we may assume that L contains a given vector v in $V_{\mathbb{Q}}$.

By Proposition 4.2, groups of integral points $G^L_{\mathbb{Z}}$ provide a general example of arithmetic subgroups, in a certain sense. The question naturally arises whether there exist arithmetic subgroups distinct from $G^L_{\mathbb{Z}}$. It turns out that there are, and examples of such subgroups can be constructed by examining the proof of Proposition 4.1. Indeed, we showed that

groups of the form $\varphi^{-1}(\varphi(G)_{\mathbb{Z}})$, where $\varphi: G \to GL_m(\mathbb{C})$ is a rational $\mathbb{Q}$-representation, must contain some congruence subgroup $G_{\mathbb{Z}}(d)$. Yet there are examples of subgroups of finite index, for example, in $SL_2(\mathbb{Z})$, that do not satisfy this property (cf. §9.5). In this connection, it is interesting to note that $G_{\mathbb{Z}}(d)$ itself can be realized as $G_{\mathbb{Z}}^L$. To be more precise, we have the following proposition, which will play an important role in Chapter 8.

PROPOSITION 4.3. *Let $G \subset GL_n(\mathbb{C})$ be an algebraic $\mathbb{Q}$-group, and let $\varrho: G \to GL_{2n}(\mathbb{C})$ be the representation given by*

$$a \mapsto \begin{pmatrix} a & 0 \\ 0 & E_n \end{pmatrix}. \tag{4.1}$$

Then, for any positive integer d, there exists a lattice $L(d) \subset \mathbb{Q}^{2n}$ such that $G_{\mathbb{Z}}(d) = \varrho^{-1}(\varrho(G)_{\mathbb{Z}}^{L(d)})$.

PROOF: Let $e_1, \dots, e_n, f_1, \dots, f_n$ be the base of $\mathbb{Q}^{2n}$ with respect to which ϱ is given by (4.1). Let $L(d)$ denote the lattice having base

$$e_1 + d^{-1}f_1, \dots, e_n + d^{-1}f_n, f_1, \dots, f_n.$$

If $g = (g_{ij}) \in G$, then

$$\begin{aligned} \varrho(g)(e_j + d^{-1}f_j) &= \sum_{i=1}^{n} g_{ij}e_i + d^{-1}f_j \\ &= \sum_{i=1}^{n} g_{ij}(e_i + d^{-1}f_i) - \sum_{\substack{i=1 \\ i\neq j}}^{n} d^{-1}g_{ij}f_i \; + d^{-1}(1 - g_{jj})f_j. \end{aligned}$$

Therefore, for g in $G_{\mathbb{Z}}$, $\varrho(g) \in \varrho(G)_{\mathbb{Z}}^{L(d)}$ if and only if $g_{ij} \equiv \delta_{ij} \pmod{d}$ for all $i, j = 1, \dots, n$. The latter means that $\varrho(G)_{\mathbb{Z}}^{L(d)} = \varrho(G_{\mathbb{Z}}(d))$, as required. Q.E.D.

Proposition 4.3 shows that groups of integral points may change considerably under rational morphisms. In this regard, the class of arithmetic subgroups stands out as a natural invariant class containing them. We have already established a weak form of invariance (invariance under $\mathbb{Q}$-isomorphisms). However, the invariance property turns out to be stronger than might have been expected.

THEOREM 4.1. *Let $\varphi: G \to H$ be a surjective $\mathbb{Q}$-morphism of algebraic groups. If Γ is an arithmetic subgroup of G then $\varphi(\Gamma)$ is an arithmetic subgroup of H.*

The proof here, unlike Proposition 4.1, is not elementary and can be developed only after an exposition of reduction theory (cf. §4.4). Before we move on to this deep subject, let us state several group-theoretic consequences of reduction theory.

THEOREM 4.2. *Let Γ be an arithmetic subgroup of an algebraic $\mathbb{Q}$-group G. Then Γ is finitely presented as an abstract group, i.e., can be defined by a finite number of generators and finitely many defining relations.*

THEOREM 4.3. *Let G be an algebraic group defined over $\mathbb{Q}$. Then there are only finitely many conjugacy classes of finite subgroups of $G_{\mathbb{Z}}$.*

See §4.4 for the proofs of Theorems 4.2 and 4.3. There the reader will also find several other results on arithmetic subgroups (including Borel's density theorem and a description of the commensurability subgroup).

To conclude this section let us indicate some generalizations of arithmetic subgroups. To define the latter we started with the group $G_{\mathbb{Z}}$, defined via some matrix realization $G \subset GL_n(\mathbb{C})$ of an algebraic $\mathbb{Q}$-group G, and then considered the class of all subgroups commensurable with G. We can give an analogous definition for algebraic groups defined over an arbitrary field K, if we fix a subring $\mathcal{O} \subset K$ whose field of fractions is K. Examination of the proof of Proposition 4.1 shows that the class of $\mathcal{O}$-arithmetic subgroups thus obtained is invariant under K-isomorphisms if the following condition is satisfied:

$$\mathcal{O}/a\mathcal{O} \text{ is finite for any } a \text{ in } \mathcal{O} \setminus \{0\}. \tag{4.2}$$

(Note that a consequence of Proposition 4.3 is that (4.2) is a necessary condition for the invariance of the class of $\mathcal{O}$-arithmetic subgroups, for groups G such as GL_n, SL_n, etc.).

The most common example of a ring satisfying (4.2) is $\mathcal{O}(S)$, the ring of S-integers of some algebraic number field (cf. §1.2). The corresponding arithmetic subgroups are said to be *S-arithmetic*. Although the class of S-arithmetic subgroups is much broader than the class of ordinary arithmetic groups, the subgroups corresponding to $S = V_\infty^K$ essentially reduce to arithmetic groups. Indeed, here the ring of S-integers is the ring of algebraic integers $\mathcal{O}$ of K. Therefore, if we choose a $\mathbb{Z}$-base of $\mathcal{O}$ and apply restriction of scalars to G we obtain a $\mathbb{Q}$-group $G' = \mathbf{R}_{K/\mathbb{Q}}G$ for which $G_{\mathcal{O}} \simeq G'_{\mathbb{Z}}$ (cf. §2.1.2). Consequently, when we develop reduction theory we shall consider the basic case of arithmetic subgroups of a $\mathbb{Q}$-group G. For an extension of these results to the general case, cf. §4.7.

4.2. Overview of reduction theory: reduction in $GL_n(\mathbb{R})$.

Most of the results on the structure of arithmetic subgroups, their cohomology, and other properties are obtained by means of a topological

approach, using the realization of $G_{\mathbb{Z}}$ as a discrete subgroup of the group of real points $G_{\mathbb{R}}$. This aspect of the theory of arithmetic groups is closely connected with the theory of discrete subgroups of Lie groups, treated in detail in Raghunathan [5]. Here we confine ourselves to discussing a range of questions relating to the construction of a *fundamental set* in $G_{\mathbb{R}}$ relative to $G_{\mathbb{Z}}$, having certain finiteness properties. Along the way we shall obtain the proofs of Theorems 4.1–4.3 and several other results. Moreover, we shall find necessary and sufficient conditions for $G_{\mathbb{R}}/G_{\mathbb{Z}}$ to be compact (and to have finite volume in the Haar measure).

Since it is impossible to give an explicit description of a fundamental set for an arbitrary algebraic group, we shall use the following approach. First we consider the cases $G = GL_n(\mathbb{C})$, $SL_n(\mathbb{C})$, where we give an explicit construction using the Siegel set Σ. The decomposition $GL_n(\mathbb{R}) = \Sigma GL_n(\mathbb{Z})$ arises, from which we can obtain an analogous decomposition for an arbitrary subgroup $G \subset GL_n(\mathbb{C})$. The formal part of the argument relies on the following elementary assertion.

LEMMA 4.2. *Let $G = \Sigma\Gamma$ be a decomposition of an abstract group G as a product of some subset Σ and a subgroup Γ. Furthermore, given a right action of G on some set X, let $H = G(x)$ denote the stabilizer of a point x in X. Assume that for a suitable a in G the intersection $(xa\Sigma)\cap x\Gamma$ is finite, equal to $\{xb_1, \dots, xb_r\}$ $(b_i \in \Gamma)$. Then $H = \Omega(\Gamma \cap H)$ where $\Omega = \left(\bigcup_{i=1}^{r} a\Sigma b_i^{-1}\right) \cap H$. If, in addition, there is some subgroup D, $\Gamma \subset D \subset G$, for which $\Sigma^{-1}\Sigma \cap g\Gamma h$ is finite for any g, h in D, then $\Omega^{-1}\Omega \cap g(\Gamma \cap H)h$ is also finite for any g, h in $D \cap H$.*

The proof is an easy verification.

Thus, constructing a fundamental domain of $G_{\mathbb{R}}$ with respect to $G_{\mathbb{Z}}$ reduces to two problems:

(1) constructing a fundamental domain for the case $G = GL_n(\mathbb{C})$ and
(2) creating facilities for the application of Lemma 4.2.

In this section we shall handle the first of these.

For the remainder of this section let G denote $GL_n(\mathbb{R})$ and let $\mathbf{K}$, A, U respectively be the subgroups of orthogonal matrices, diagonal matrices with positive entries, and upper triangular matrices with 1 on the diagonal (unipotent matrices). Recall that by Proposition 3.12 on the Iwasawa decomposition in G the product morphism induces a homeomorphism $\mathbf{K} \times A \times U \to G$. Below the components of the Iwasawa decomposition of an element g in G will be denoted as k_g, a_g and u_g. In addition, we shall

assume that a in A, u in U have the form

$$a = \operatorname{diag}(a_1, \dots, a_n), \quad u = \begin{pmatrix} 1 & & u_{ij} \\ & \ddots & \\ 0 & & 1 \end{pmatrix}.$$

DEFINITION: A *Siegel set* in G is the set $\Sigma_{t,v} = \mathbf{K}A_tU_v$ $(t, v > 0)$, where $A_t = \{a \in A : a_i \le ta_{i+1},\ i = 1, \dots, n-1\}$ and $U_v = \{u \in U : |u_{ij}| \le v$ for all $1 \le i < j \le n\}$.

The components in the definition of a Siegel set have been selected in such a way that the following property, used repeatedly in the sequel, will hold.

LEMMA 4.3. *For any t, $v > 0$*

$$\{aua^{-1} : a \in A_t,\ u \in U_v\}$$

is relatively compact.

PROOF: $aua^{-1} = \begin{pmatrix} 1 & & f_{ij} \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$, where $f_{ij} = \frac{a_i}{a_j}u_{ij}$. Moreover

$$|f_{ij}| = \left|\frac{a_i}{a_{i+1}}\frac{a_{i+1}}{a_{i+2}} \cdots \frac{a_{j-1}}{a_j}u_{ij}\right| \le t^{j-i}v;$$

hence the set under consideration is contained in U_{sv}, where

$$s = \max_{1 \le i < j \le n} \{t^{j-i}\},$$

as required.

In what follows we shall treat "relatively compact" and "bounded" as interchangeable terms. Put $\Gamma = GL_n(\mathbb{Z})$. Then we have

THEOREM 4.4. *$G = \Sigma_{t,v}\Gamma$ for $t \ge \frac{2}{\sqrt{3}}$ and $v \ge \frac{1}{2}$.*

PROOF: Fix an orthonormal base $e_1, \dots, e_n$ of $\mathbb{R}^n$, and let $\| \ \|$ denote the corresponding Euclidean norm. Define a continuous function $\Phi: G \to \mathbb{R}^+$ by $\Phi(g) = \|ge_1\|$. Take any g in G. Then $g\Gamma e_1$ is contained in the lattice $g(\mathbb{Z}e_1 + \cdots + \mathbb{Z}e_n)$ and therefore for any $d > 0$ only a finite number of elements w in $g\Gamma e_1$ satisfy $\|w\| \le d$. It follows that Φ reaches its positive minimum on $g\Gamma$. Our objective is to show that this minimum is actually reached at some point in $\Sigma_0 = \Sigma_{\frac{2}{\sqrt{3}}, \frac{1}{2}}$. Then $g\Gamma \cap \Sigma_0 \ne \emptyset$, from which the theorem will follow.

LEMMA 4.4. *If Φ takes on a minimal value on $g\Gamma$ at the point $g = kau$, then*

(1) *there exists $\bar{u}$ in $U_{\frac{1}{2}}$ such that $h = ka\bar{u} \in g\Gamma$ and $\Phi(h) = \Phi(g)$;*
(2) $\frac{a_1}{a_2} \leq \frac{2}{\sqrt{3}}$.

PROOF OF THE LEMMA: First we show that $U = U_{\frac{1}{2}}(U \cap \Gamma)$. Take any element $u = \begin{pmatrix} 1 & & u_{ij} \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \in U$. Direct calculation shows that

$$\begin{pmatrix} 1 & u_{12} & \cdots & u_{1n} \\ & 1 & \cdots & u_{2n} \\ & & \ddots & \vdots \\ & 0 & & u_{n-1,n} \\ & & & 1 \end{pmatrix} \begin{pmatrix} 1 & \alpha_1 & & & \\ & 1 & \alpha_2 & 0 & \\ & & \ddots & \ddots & \\ & 0 & & & \alpha_{n-1} \\ & & & & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & u_{12}+\alpha_1 & & & * \\ & 1 & & & \\ & & \ddots & & \\ & 0 & & \ddots & u_{n-1,n}+\alpha_{n-1} \\ & & & & 1 \end{pmatrix}.$$

Therefore, by selecting α_i suitably in $\mathbb{Z}$ we can make all the elements u_{12}, $\ldots$, u_{ii+1}, $\cdots$, $u_{n-1\,n}$ not exceed $\frac{1}{2}$ in absolute value. We proceed by induction. Assume that $|u_{ij}| \leq \frac{1}{2}$ whenever $0 < j - i \leq l$. If we compute the entries of the product

$$m = \begin{pmatrix} 1 & u_{12} & u_{13} & \cdots & u_{1n} \\ & 1 & u_{23} & \cdots & u_{2n} \\ & & 1 & & u_{3n} \\ & & & \ddots & \vdots \\ & 0 & & & \\ & & & & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & \cdots & \beta_1 & \cdots & 0 \\ & \ddots & \ddots & & \ddots & \vdots \\ & & \ddots & 0 & & \beta_{n-(l+1)} \\ & & & \ddots & \ddots & \vdots \\ & & & & \ddots & 0 \\ & & & & & 1 \end{pmatrix}$$

we see that $m_{ij} = u_{ij}$ for $j - i \leq l$ and $m_{ij} = u_{ij} + \beta_i$ for $i = 1, \ldots, n-(l+1)$, $j = i + l + 1$. Thus, on the $(l+1)$-th step we can satisfy $|u_{ij}| \leq \frac{1}{2}$ for $0 < j - i \leq l + 1$, and finally on the $(n-1)$-th step we obtain a matrix of $U_{\frac{1}{2}}$. Thus $U = U_{\frac{1}{2}}(U \cap \Gamma)$ is proven.

To prove (1) it now suffices to choose $\bar{u}$ in $U_{\frac{1}{2}}$ satisfying $u \in \bar{u}(U \cap \Gamma)$ and to note that for $h = ka\bar{u}$ the equalities

$$\Phi(g) = \|ge_1\| = \|ae_1\| = a_1 = \Phi(h) \tag{4.3}$$

hold, since the a-components of g and h coincide.

Now we move on to the proof of (2). We assume that $g = kau$ and $u \in U_{\frac{1}{2}}$. Put

$$Z = \begin{pmatrix} \begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix} & & 0 \\ & & \\ 0 & & E_{n-2} \end{pmatrix} \in T.$$

By assumption $\Phi(gZ) \geq \Phi(g)$. Computing $\Phi(gZ)$, we obtain

$$gZe_1 = ge_2 = k(a_1 u_{12} e_1 + a_2 e_2);$$

so

$$\Phi(gZ)^2 = \|a_1 u_{12} e_1 + a_2 e_2\|^2 = a_1^2 u_{12}^2 + a_2^2 \leq \frac{1}{4} a_1^2 + a_2^2,$$

since $|u_{12}| \leq \frac{1}{2}$. Since (4.3) gives us $\Phi(g) = a_1$, we have $a_1^2 \leq \frac{1}{4} a_1^2 + a_2^2$, and hence $a_1 \leq \frac{2}{\sqrt{3}} a_2$. This completes the proof of Lemma 4.4.

Now we conclude the proof of the theorem. It follows from Lemma 4.4 that the required assertion holds for $n = 2$. We proceed by induction on n (recall that $\Gamma = GL_n(\mathbb{Z})$). Let $n \geq 3$ and suppose Φ attains a minimum on the coset $g\Gamma$ at $g = kau$. Put $h = bw \in GL_{n-1}(\mathbb{R})$, where

$$b = \operatorname{diag}(a_2, \ldots, a_n), \quad w = \begin{pmatrix} 1 & u_{23} & \cdots & u_{2n} \\ & 1 & & \vdots \\ & & \ddots & u_{n-1\,n} \\ 0 & & & 1 \end{pmatrix}.$$

By induction there exists an element c' in $GL_{n-1}(\mathbb{Z})$ satisfying $hc' = k_0' a' u'$ for a' in $A^{(n-1)}_{2/\sqrt{3}}$ and u' in $U^{(n-1)}_{1/2}$ with the obvious notation. Put

$$c = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & c' & \\ 0 & & & \end{pmatrix} \in \Gamma, \quad \tilde{k} = k \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & k_0' & \\ 0 & & & \end{pmatrix} \in K,$$

$$\tilde{a} = \operatorname{diag}(a_1, a_1', \ldots, a_{n-1}') \in A.$$

Then a direct computation shows that $gc = \tilde{k}\tilde{a}\tilde{u}$ for suitable $\tilde{u}$ in U. Moreover, $ce_1 = e_1$ so $\Phi(gc) = \|gce_1\| = \|ge_1\| = \Phi(g)$ and gc also yields a minimum for Φ on $g\Gamma$. By the lemma we may assume $\tilde{u} \in U_{\frac{1}{2}}$ and $a_1/a_1' \leq \frac{2}{\sqrt{3}}$. But by construction $a' \in A^{(n-1)}_{2/\sqrt{3}}$, so $a_i'/a_{i+1}' \leq \frac{2}{\sqrt{3}}$ for all $i = 1, \ldots, n-2$. Therefore $\tilde{a} \in A_{\frac{2}{\sqrt{3}}}$. Q.E.D.

COROLLARY. *Put* $\Sigma^{(1)}_{t,v} = \Sigma_{t,v} \cap SL_n(\mathbb{R})$. *Then* $SL_n(\mathbb{R}) = \Sigma^{(1)}_{t,v} SL_n(\mathbb{Z})$ *for* $t \geq \frac{2}{\sqrt{3}}$, $v \geq \frac{1}{2}$. *Moreover* $\Sigma^{(1)}_{t,v} = (\mathbf{K} \cap SL_n(\mathbb{R}))(A_t \cap SL_n(\mathbb{R}))U_v$.

PROOF: Let $g \in SL_n(\mathbb{R})$ and $g = \sigma h$, where $\sigma \in \Sigma_{t,v}$ and $h \in GL_n(\mathbb{Z})$. If $\det h = 1$ then $\sigma \in \Sigma^{(1)}_{t,v}$, and we have nothing to prove. If, however, $\det h = -1$ then for $x = \mathrm{diag}(1, \ldots, 1, -1)$ we have $xh \in SL_n(\mathbb{Z})$ and $\sigma x^{-1} \in \Sigma^{(1)}_{t,v}$, since $x \in \mathbf{K}$ and normalizes A_t and U_v. So

$$g = (\sigma x^{-1})(xh) \in \Sigma^{(1)}_{t,v} SL_n(\mathbb{Z}).$$

The decomposition for $\Sigma^{(1)}_{t,v}$ follows from the fact that $\det \mathbf{K} = \pm 1$, $\det U = 1$, and $\det A > 0$.

The study of discrete transformation groups is usually begun by constructing the corresponding fundamental domain. Recall that if Γ acts as a discrete transformation group on a space X then a *fundamental domain of* Γ is an open subset $\Omega \subset X$ such that

(1) $\bar{\Omega}\Gamma = X$, where $\bar{\Omega}$ is the closure of Ω;
(2) $\Omega \cap \Omega\gamma = \emptyset$, if $\gamma \neq e$.

(Sometimes other definitions of a fundamental domain are used.)

N.B. In reduction theory we shall consider the right action of Γ, not the left, as is usually done. The reason for this lies in the nature of the proof of Theorem 4.4. This inconvenience might be avoided by making the standard substitution $x \mapsto x^{-1}$; however that would make the form of the fundamental domain much less elegant.

It follows from Theorem 4.4 that the interior $\Sigma^0_{t,v}$ of any Siegel set with $t > \frac{2}{\sqrt{3}}$, $v > \frac{1}{2}$ satisfies the first condition of the definition of a fundamental domain for the natural action of Γ on G by right translation. The question is whether $\Sigma^0_{2/\sqrt{3},\,1/2}$ is itself a fundamental domain. It turns out that it is not, and this is best seen in the case of $SL_2(\mathbb{R})$, by means of classic geometric arguments.

First of all, note that Siegel sets Σ satisfy $\mathbf{K}\Sigma = \Sigma$; therefore, without loss of generality, instead of Σ we may consider its image in $X = G/\mathbf{K}$. For $SL_2(\mathbb{R})$ there is a classic interpretation of $SL_2(\mathbb{R})/SO_2(\mathbb{R})$ as the upper half-plane of the complex plane. If we then denote the upper half-plane by P, we can define the action of $H = SL_2(\mathbb{R})$ on it by

$$zg = \frac{dz + b}{cz + a}, \quad \text{where } z \in P, \quad g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{R}).$$

Note that this right action differs from the traditional left action $gz = \frac{az+b}{cz+d}$ (cf., for example, Serre [7, Ch. 7]) by the involution

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^t \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} d & b \\ c & a \end{pmatrix}.$$

Direct computation shows that

$$ig = \frac{ab + cd}{a^2 + c^2} + \frac{i}{a^2 + c^2}, \quad \text{where } i = \sqrt{-1}.$$

It follows easily that the action under consideration is transitive and that the stabilizer of i is $SO_2(\mathbb{R})$, which gives the requisite identification

$$SL_2(\mathbb{R})/SO_2(\mathbb{R}) \simeq P.$$

Straightforward computation also shows that the image in P of $\Sigma^{(1)}_{t,v}$ is $\Omega_{t,v} = \{ z \in P : \Im z \geq 1/t,\ |\Re z| \leq v \}$ ($\Im$ and $\Re$ denote respectively the real and imaginary parts). Also consider the domain $D = \{ z \in P : |z| > 1,\ |\Re z| < \frac{1}{2} \}$. We shall show that D in fact is a fundamental domain for the action of $SL_2(\mathbb{Z})$ on P. More precisely, to satisfy the second condition of the definition of fundamental domain we need to pass from $SL_2(\mathbb{Z})$ to $\Gamma = PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z})/\{\pm E\}$, since $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \in SL_2(\mathbb{Z})$ acts on P trivially.

PROPOSITION 4.4. *D is a fundamental domain for Γ in P.*

PROOF: Take arbitrary $z \in P$. We shall show that $zg \in \bar{D} = \{ z \in P : |z| \geq 1,\ |\Re z| \leq \frac{1}{2} \}$ for some g in Γ. Direct computation shows that if $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, then

$$\Im(zg) = \frac{\Im z}{|cz + a|^2}. \tag{4.4}$$

Since $cz + a$ lies in the lattice $\mathbb{Z} \oplus \mathbb{Z}z$, then $|cz + a|$ is bounded from below, and we can find $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $SL_2(\mathbb{R})$ for which $\Im(zg)$ is maximal. Applying a suitable transformation of the form $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ that does not change the imaginary part, we may assume that $|\Re(zg)| \leq \frac{1}{2}$. Let us show that $z' = zg \in \bar{D}$. By assumption $|\Re(z')| \leq \frac{1}{2}$; if $|z'| < 1$, then for $z'' = \frac{-1}{z'}$, obtained from z' by $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, we have $\Im z'' = \frac{\Im z'}{|z'|^2} > \Im z'$, which contradicts the choice of z'.

Now we verify the second condition of the definition of a fundamental domain. Let z, $zg \in D$, with g given by $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$. By symmetry, without loss of generality we may assume that $\Im(zg) \geq \Im(z)$. Then by (4.4) we have $|cz+a| \leq 1$. Since $\Im z > \frac{\sqrt{3}}{2}$, we have $|cz+a| > \left(\frac{\sqrt{3}}{2}\right)|c|$. Switching

from $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ to $\left(\begin{smallmatrix} -a & -b \\ -c & -d \end{smallmatrix}\right)$, if necessary, which does not change g, we may assume $c \geq 0$. Thus, the only possibilities for c are 0, 1.

If $c = 0$, then $a = \pm 1$, so we may assume g has the form $\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)$. Therefore $zg = z + b$, and using $|\Re z| < \frac{1}{2}$ and $|\Re zg| < \frac{1}{2}$, we obtain $b = 0$.

Now suppose $c = 1$, so $|z + a| \leq 1$. We have $|z + a|^2 = |z|^2 + 2a\Re z + a^2$, whence $2a\Re z + a^2 \leq 0$, so $|\Re z| \geq \frac{|a|}{2} \geq \frac{1}{2}$ if $a \neq 0$, in contradiction with the assumption $z \in D$. Thus $a = 0$, and we may assume g has the form $\left(\begin{smallmatrix} 0 & -1 \\ 1 & d \end{smallmatrix}\right)$. Then $zg = d - \frac{1}{z}$. Since $\Re\left(\frac{1}{z}\right) = \frac{\Re z}{|z|^2}$ and $|z|^2 > 1$, we see $|\Re\left(\frac{1}{z}\right)| < |\Re z| < \frac{1}{2}$. But also $|\Re zg| < \frac{1}{2}$, so $d = 0$ and thus $zg = -\frac{1}{z}$. But $|-\frac{1}{z}| = |z|^{-1} < 1$, contradiction. Q.E.D.

Geometrically $\Omega = \Omega_{\frac{2}{\sqrt{3}}, \frac{1}{2}}$ and D (filled in) are related as in Figure 4.1 (below).

Comparing Ω and D, we may conclude two things. First, the bounds $t = \frac{2}{\sqrt{3}}$, $v = \frac{1}{2}$ in Theorem 4.4 are the best possible. Secondly, the interior of a Siegel set is not a fundamental domain, since its translations overlap (the diagram depicts one of the shifts of D', which intersects Ω). It turns out, however, that a Siegel set Σ satisfies a weaker condition of meeting only finitely many Γ-translations.

THEOREM 4.5. *Let $\Sigma = \Sigma_{t,v}$ be a Siegel set of $GL_n(\mathbb{R})$, and let $x, y \in GL_n(\mathbb{Q})$. Then $\Sigma^{-1}\Sigma \cap x\Gamma y$ is a finite set.*

The proof will be deduced from a theorem of Harish-Chandra, whose

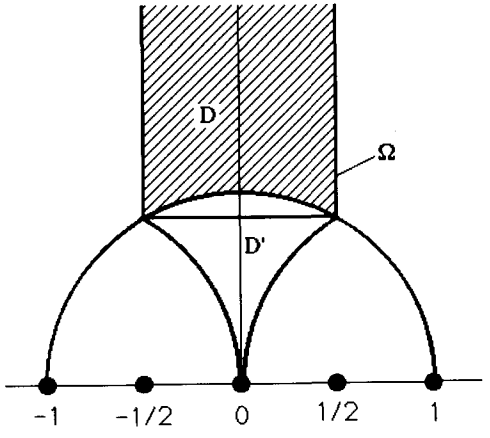


Figure 4.1.

formulation requires some further notation. First, we introduce functions Φ_i, analogous to Φ, by putting $\Phi_i(g) = \|g(e_1 \wedge \ldots \wedge e_i)\|$ for $g \in G$. Here $e_1 \wedge \ldots \wedge e_i$ is viewed as an element of $\wedge^i(\mathbb{R}^n)$, the set of elements of degree i in the exterior algebra, on which $GL_n(\mathbb{R})$ acts in the natural way. The vector norm is taken relative to the orthonormal base $e_{j_1} \wedge \ldots \wedge e_{j_i}$ $(j_1 < \ldots < j_i)$ of the space $\wedge^i(\mathbb{R}^n)$. Clearly $\Phi_1(g) = \Phi(g)$ and $\Phi_n(g) = |\det g|$. Moreover, $\mathbf{K} = O_n(\mathbb{R})$ acts on $\wedge^i(\mathbb{R}^n)$ by orthogonal transformations (an exercise for the reader); in particular, $\Phi_i(kg) = \Phi_i(g)$ for any k in $\mathbf{K}$.

We also need some notation pertaining to the Bruhat decomposition in $G = GL_n(\mathbb{R})$ (cf. §2.1.10 for more detail). Let D be the group of diagonal matrices, and let W be the subgroup of permutation matrices of G, matrices in which every row and every column has exactly one non-zero entry, equal to 1 (obviously $W < \mathbf{K}$). Note that the elements $w = (w_{ij})$ in W can be characterized as follows:

$$w_{ij} = \begin{cases} 1, & \text{for } i = \pi j \\ 0, & \text{for } i \neq \pi j \end{cases}$$

where π is a suitable permutation of the indexes $1, \ldots, n$. Clearly, the map $w \mapsto \pi = \pi(w)$ gives an isomorphism from W to the symmetric group S_n. Both products WD and $B = DU$ are semidirect, the first one being the normalizer of D in G and the second one being the group of upper triangular matrices. A basic result here (cf. Theorem 2.5) is that $G = \bigcup_{w \in W} UwB$, i.e., $G = UWB = UWDU$. Moreover, let U^- denote the group of lower triangular unipotent matrices; then each g in UwB can be represented uniquely in the form $g = v_g^- w t_g v_g$, where $v_g^- \in U_w = w(w^{-1}Uw \cap U^-)w^{-1}$, $t_g \in D$, and $v_g \in U$.

THEOREM 4.6 (HARISH-CHANDRA). *Let $\Sigma = \Sigma_{t,v}$ be a Siegel set of G, and let $M \subset G$ satisfy*

(i) $M = M^{-1}$
(ii) $\Phi_i(t_m) \geq c$ *for all* $i = 1, \ldots, n$ *and all* m *in* M, *for a suitable* $c > 0$.

Then $M_\Sigma = \{ m \in M : \Sigma m \cap \Sigma \neq 0 \}$ is relatively compact in G.

The proof uses several properties of Φ_i, which we formulate as

LEMMA 4.5. *Let $g = k_g a_g u_g = v_g^- w t_g v_g$ respectively be the Iwasawa and Bruhat decompositions of g in G. Then*

(1) $a_g = a_{w^{-1}v_g^- w} a_{t_g}$, *so* $\Phi_i(g) = \Phi_i(w^{-1}v_g^- w) \cdot \Phi_i(t_g) \geq \Phi_i(t_g)$;
(2) *there exists a constant* $d = d(\Sigma) > 0$ *such that* $\|gx\| \geq d\|x\|\Phi_i(g)$ *for all* $g \in \Sigma$ *and* $x \in \wedge^i(\mathbb{R}^n)$, $i = 1, \ldots, n$.

In particular, for g in Σ and h in G we have $\Phi_i(gh) \geq d\Phi_i(g)\Phi_i(h)$.

PROOF: (1) We have $\Phi_i(g) = \|g(e_1 \wedge \ldots \wedge e_i)\| = \|a_g(e_i \wedge \ldots \wedge e_i)\| = \Phi_i(a_g) = a_1 \ldots a_i$, where $a_g = \mathrm{diag}(a_1, \ldots, a_n)$. Furthermore,

$$g = v_g^- w t_g v_g = w w^{-1} v_g^- w t_g v_g$$
$$= (w k_{w^{-1} v_g^- w}) \cdot (a_{w^{-1} v_g^- w} t_g) \cdot t_g^{-1} u_{w^{-1} v_g^- w} t_g v_g,$$

whence $a_g = a_{w^{-1} v_g^- w} a_{t_g}$. Thus

$$\Phi_i(g) = \Phi_i(a_g) = \Phi_i(a_{w^{-1} v_g^- w}) \Phi_i(a_{t_g}) = \Phi_i(w^{-1} v_g^- w) \Phi_i(t_g).$$

It remains to show $\Phi_i(w^{-1} v_g^- w) \geq 1$. But $w^{-1} v_g^- w \in U^-$, and for any u in U^- we have $u(e_1 \wedge \ldots \wedge e_i) = e_1 \wedge \ldots \wedge e_i + b$, where b is a linear combination of elements of the canonical base in $\wedge^i(\mathbb{R}^n)$ distinct from $e_1 \wedge \ldots \wedge e_i$, implying $\|u(e_1 \wedge \ldots \wedge e_i)\| \geq 1$.

(2) We may assume $\|x\| = 1$. The set of all such x is compact, so also

$$\{ ux : u \in U_v, \|x\| = 1 \}$$

is compact. Therefore there exists $\delta_1 > 0$ satisfying $\|ux\| \geq \delta_1$ for all u in U_v and all x such that $\|x\| = 1$. Furthermore, if $f_j = e_{l_1} \wedge \ldots \wedge e_{l_i} (l_1 < \ldots < l_i)$ is an element of the canonical base of $\wedge^i(\mathbb{R}^n)$, then

$$a_g f_j = a_{l_1} \ldots a_{l_i} f_j = (a_1 \ldots a_i) \left(\frac{a_{l_1}}{a_1} \ldots \frac{a_{l_i}}{a_i} \right) f_j.$$

In addition, for any $k = 1, \ldots, i$ we have $l_k \geq k$, so if $g \in \Sigma$, then by definition of the Siegel set $a_{l_k}/a_k \geq t^{k - l_k}$. Thus there exists $\delta_2 > 0$ satisfying $\left| \frac{a_{l_1}}{a_1} \ldots \frac{a_{l_i}}{a_i} \right| \geq \delta_2$ for any $l_1 < \ldots < l_i$, so we have

$$\|gx\| = \|a_g u_g x\| \geq \delta_2 \Phi_i(a_g) \|u_g x\| \geq \delta_1 \delta_2 \Phi_i(g) = d \Phi_i(g) \|x\|,$$

where $d = \delta_1 \delta_2$, as desired. Applying this inequality to the vector $x = h(e_1 \wedge \ldots \wedge e_i)$ yields the second assertion. Q.E.D. for lemma.

An essential part of the continuation of the argument is contained in the following assertion.

LEMMA 4.6. *As m runs through M_Σ, the a-components a_m in the Iwasawa decomposition and the components v_m^- and t_m in the Bruhat decomposition form relatively compact sets.*

PROOF: Let $m \in M_\Sigma$, i.e., $xm = y$ for some $x, y \in \Sigma$. Applying (2) of the previous lemma, we obtain

$$\Phi_i(x) = \Phi_i((xm)m^{-1}) \geq d \Phi_i(xm) \Phi_i(m^{-1}) \geq d^2 \Phi_i(x) \Phi_i(m) \Phi_i(m^{-1}),$$

i.e., $\Phi_i(m) \Phi_i(m^{-1}) \leq \frac{1}{d^2}$ for all i and all m in M_Σ. Since by hypothesis $\Phi_i(m) \geq \Phi_i(t_m) \geq c$ and $M = M^{-1}$, we see Φ_i are bounded on M from above, i.e.,

$$0 < c \leq \Phi_i(t_m) \leq \Phi_i(m) \leq b \tag{4.5}$$

for all m in M_Σ. On the other hand, as we saw in the proof of Lemma 4.5,

$$\Phi_i(m) = \Phi_i(a_m) = a_1 \ldots a_i$$
$$\Phi_i(t_m) = |t_1 \ldots t_i|,$$

where $a = \mathrm{diag}(a_1, \ldots, a_n)$ and $t = \mathrm{diag}(t_1, \ldots, t_n)$. Therefore it follows from (4.5) that $c \leq a_1 \leq b$ and so $cb^{-1} \leq a_i \leq bc^{-1}$, for $i > 1$; i.e., $\{ a_m : m \in M_\Sigma \}$ is a relatively compact set.

Finally, by Lemma 4.5(1), $a_m = a_{w^{-1} v_m^- w} t_m$, so

$$\{ a_{w^{-1} v_m^- w} : m \in M_\Sigma \cap UwB \}$$

is relatively compact. Hence the elements

$$(w^{-1} v_m^- w) u_{w^{-1} v_m^- w}^{-1} = k_{w^{-1} v_m^- w} a_{w^{-1} v_m^- w}$$

also form a relatively compact set. On the other hand $w^{-1} v_m^- w \in U^-$, and we leave it to the reader to show that the product morphism gives a homeomorphism from $U^- \times U$ to a closed subset of G. Therefore the $w^{-1} v_m^- w$, and hence also the v_m^-, form a relatively compact set. This completes the proof of Lemma 4.6.

Now let us take up the proof of Harish-Chandra's theorem. Since W is finite, it suffices to establish that $M_\Sigma \cap UwB$ is relatively compact for all w in W. Therefore, in the discussion which follows we may (and shall) fix w. Let $\pi = \pi_w$ be the corresponding permutation. There are two possible cases:

(1) there exists $\lambda < n$ satisfying $\pi(\{1, \ldots, \lambda\}) = \{1, \ldots, \lambda\}$;
(2) for each $\lambda < n$ there is $j \in \{1, \ldots, \lambda\}$ for which $\pi(j) > \lambda$.

Case 1. Naturally, $n > 1$, and then w, and consequently the entire class UwB, lies in

$$P_\lambda = \begin{pmatrix} GL_\lambda(\mathbb{C}) & * \\ 0 & GL_{n-\lambda}(\mathbb{C}) \end{pmatrix};$$

thus it suffices to establish that $M_\Sigma \cap P_\lambda$ is relatively compact. Furthermore, if $m \in M_\Sigma \cap P_\lambda$, then $xm = y$ for some $x \in AU \subset P_\lambda$; and then also $y \in P_\lambda$. Thus,

$$M_\Sigma \cap P_\lambda = \{\, m \in M : (\Sigma \cap P_\lambda)m \cap (\Sigma \cap P_\lambda) \neq \emptyset \,\}.$$

Now assume Harish-Chandra's theorem has been proven for $GL_r(\mathbb{R})$, for all $r < n$. The Levi decomposition (Theorem 2.3) gives $P_\lambda = SR$, where

$$S = \begin{pmatrix} GL_\lambda(\mathbb{C}) & 0 \\ 0 & GL_{n-\lambda}(\mathbb{C}) \end{pmatrix}$$

is a maximal reductive subgroup and

$$R = \begin{pmatrix} E_\lambda & * \\ 0 & E_{n-\lambda} \end{pmatrix}$$

is the unipotent radical.

Let τ, τ_1 and τ_2 denote the natural projections of P_λ on S, $GL_\lambda(\mathbb{C})$ and $GL_{n-\lambda}(\mathbb{C})$ respectively. Also put $\varrho(x) = \tau(x)^{-1}x$. Since $\mathbf{K} = O_n(\mathbb{R})$ is given by ${}^t g = g^{-1}$, obviously

$$\mathbf{K} \cap P_\lambda = \mathbf{K} \cap S = \begin{pmatrix} O_\lambda(\mathbb{R}) & 0 \\ 0 & O_{n-\lambda}(\mathbb{R}) \end{pmatrix}.$$

Furthermore, $AU \subset P_\lambda$; therefore if $g = k_g a_g u_g$ is the Iwasawa decomposition of g in P_λ, then $k_g \in P_\lambda$, so

$$k_g = \begin{pmatrix} k_{\tau_1(g)} & 0 \\ 0 & k_{\tau_2(g)} \end{pmatrix}, \quad a_g = \begin{pmatrix} a_{\tau_1(g)} & 0 \\ 0 & a_{\tau_2(g)} \end{pmatrix}.$$

Moreover, if $a \in A_t^{(n)}$, then $\tau_1(a) \in A_t^{(\lambda)}$ and $\tau_2(a) \in A_t^{(n-\lambda)}$. By the continuity of τ, which implies that any set of the form $\tau(U_v)$ is compact, it is easy to show that $\tau_1(\Sigma \cap P_\lambda)$ and $\tau_2(\Sigma \cap P_\lambda)$ are contained in suitable Siegel sets $\Sigma_1 \subset GL_\lambda(\mathbb{R})$ and $\Sigma_2 \subset GL_{n-\lambda}(\mathbb{R})$.

It is obvious that $\tau_i(M_\Sigma \cap P_\lambda) \subset (M_i)_{\Sigma_i}$, where $M_i = \tau_i(M \cap P_\lambda)$. In the Bruhat decomposition in $GL_n(\mathbb{C})$ of any g in P_λ, one can easily see that t_g has the form

$$t_g = \begin{pmatrix} t_{\tau_1(g)} & 0 \\ 0 & t_{\tau_2(g)} \end{pmatrix}.$$

Now M_1 and M_2 satisfy the conditions given in the statement of Harish-Chandra's theorem. Indeed, the first condition is obviously satisfied. The second condition is equally evident for M_1. We show that it also holds for M_2. For m in $M \cap P_\lambda$ we have $\Phi_\lambda(m) = |\det \tau_1(m)|$, so $\Phi_\lambda(m^{-1}) = \Phi_\lambda(m)^{-1} \geq c$ by condition (ii). Therefore it remains to note that the functions $\Phi'_1, \ldots, \Phi'_{n-\lambda}$ defined in analogy to Φ_i, but for $GL_{n-\lambda}(\mathbb{R})$, are related to the original Φ_i by the equation $\Phi'_i = \frac{\Phi_{\lambda+i}}{\Phi_\lambda}$, from which the desired result follows. By induction $(M_i)_{\Sigma_i}$ are relatively compact, implying $\tau(M_\Sigma \cap P_\lambda)$ is also relatively compact.

It remains to be shown that $\varrho(M_\Sigma \cap P_\lambda)$ is also relatively compact. Let $m \in M_\Sigma \cap P_\lambda$, so that $xm = y$ for some x, $y \in \Sigma \cap P_\lambda$. Then we have $\tau(x)\varrho(x)\tau(m)\varrho(m) = \tau(y)\varrho(y)$, from which it follows that $\varrho(m) = \tau(m)^{-1}\varrho(x)^{-1}\tau(m)\varrho(y)$. Since x and y were taken from a Siegel set, the $\varrho(x)$ and $\varrho(y)$ run over relatively compact sets. We obtain the required result in view of the relative compactness of $\{\, \tau(m) : m \in M_\Sigma \cap P_\lambda \,\}$, which we have already established.

Case 2. Write $xm = y$ for x, $y \in \Sigma$ and some $m \in M \cap UwB$; also, we may assume $\det x = 1$. Writing the Iwasawa decomposition for x and y and the Bruhat decomposition for m, we obtain

$$k_y a_y u_y = k_x a_x u_x v_m^- w t_m v_m = (k_x w) c w^{-1} a_x w t_m v_m, \tag{4.6}$$

where $c = w^{-1} a_x u_x v_m^- a_x^{-1} w$. Substituting the Iwasawa decomposition of c in (4.6) and equating the a-components, we obtain

$$a_y = a_c (w^{-1} a_x w) a_{t_m}. \tag{4.7}$$

Note that c, and therefore also its a-component a_c, runs through a relatively compact set; this is seen by applying Lemma 4.3 to the fact that the u_x and v_m^- run through relatively compact subsets (u_x, by definition of a Siegel set, and v_m^- by Lemma 4.6). Again by Lemma 4.6, the set of elements of the form a_{t_m} is relatively compact; therefore by (4.7) the $a_y^{-1} w^{-1} a_x w$ are bounded. But if $a_x = \operatorname{diag}(a_1, \ldots, a_n)$ and $a_y = \operatorname{diag}(b_1, \ldots, b_n)$, then $a_y^{-1} w^{-1} a_x w = \operatorname{diag}(b_1^{-1} a_{\pi(1)}, \ldots, b_n^{-1} a_{\pi(n)})$, where π is the permutation corresponding to w. Thus, we can find α, $\beta > 0$ independent of x, y, such that

$$\alpha < b_i^{-1} a_{\pi(i)} < \beta \quad \text{for all } i = 1, \ldots, n. \tag{4.8}$$

It follows from (4.8) that for any i, j the $b_i^{-1}b_j a_{\pi(i)}a_{\pi(j)}^{-1}$ are bounded from above. But for $i < j$ the $b_i b_j^{-1}$ are bounded from above since $a_y \in A_t$. Consequently, we can find a constant $\gamma > 0$ satisfying

$$a_{\pi(i)}a_{\pi(j)}^{-1} < \gamma \quad \text{whenever } i < j, \text{ for all } a_x. \tag{4.9}$$

Next we show $a_k^{-1}a_{k+1}$ are bounded for all $k = 1, \dots, n-1$. By hypothesis we can find $i \le k$ such that $\pi(i) \ge k+1$. Clearly, we can also find $j > k$ satisfying $\pi(j) \le k$. Then $i < j$ and $\pi(j) \le k < k+1 \le \pi(i)$. We have

$$a_{\pi(j)}^{-1}a_{\pi(i)} = (a_{\pi(j)}^{-1}a_{\pi(j)+1}) \dots (a_{\pi(i)-1}^{-1}a_{\pi(i)});$$

moreover, since $a_x \in A_t$, the $a_l^{-1}a_{l+1}$ are bounded from below. Therefore, it follows from (4.9) that $a_k^{-1}a_{k+1}$ for each k is bounded from above (as well as from below). Defining $\varphi: A \to \mathbb{R}^* \times \dots \times \mathbb{R}^*$ by

$$\varphi(\operatorname{diag}(a_1, \dots, a_n)) = \left(\frac{a_1}{a_2}, \frac{a_2}{a_3}, \dots, \frac{a_{n-1}}{a_n}\right),$$

we see the $\varphi(a_x)$ are bounded. But since $x \in SL_n(\mathbb{R})$ we have $a_x \in A \cap SL_n(\mathbb{R})$; on the other hand, $\varphi\,|_{A \cap SL_n(\mathbb{R})}$ is injective, and therefore proper. So we conclude that the a_x also constitute a relatively compact set.

We deduce from (4.8)that the a_y also are bounded. It follows that the $x = k_x a_x u_x$ and the $y = k_y a_y u_y$ are contained in relatively compact sets. Therefore the $m = x^{-1}y$ also constitute a relatively compact set.

PROOF OF THEOREM 4.5: Put $M = (x\Gamma y) \cup (x\Gamma y)^{-1}$, where $\Gamma = GL_n(\mathbb{Z})$. Clearly, M is discrete and closed in G; moreover, the matrix entries of M have bounded denominators. Therefore, to prove the finiteness of the corresponding set M_Σ (the assertion of the theorem), it suffices to establish its relative compactness. The latter follows from Harish-Chandra's theorem once we verify its hypotheses. (i) is given. To verify (ii) we need a preliminary remark.

Let $g = ub$, where $u \in U^-$ and

$$b = \begin{pmatrix} b_{11} & & * \\ & \ddots & \\ 0 & & b_{nn} \end{pmatrix}.$$

Then for any $i = 1, \dots, n$ we have

$$(g_{kl})_{1 \le k,l \le i} = (u_{kl})_{1 \le k,l \le i}(b_{kl})_{1 \le k,l \le i},$$

whence $\det(g_{kl})_{1 \le k,l \le i} = b_{11} \dots b_{ii}$.

Now let $m = v_m^- w t_m v_m \in M$. Then the entries of the matrix $w^{-1}m$ have bounded denominators. On the other hand, $w^{-1}m = w^{-1}v_m^- w t_m v_m$ and $w^{-1}v_m^- w \in U^-$. From the above remark it follows that $\Phi_i(t_m) = |t_1 \dots t_i|$ is the absolute value of the principal $(i \times i)$ minor of $w^{-1}m$, i.e., is a rational number with bounded denominator, from which it follows that (ii) is satisfied. Q.E.D.

This section is best summarized using the concept of a fundamental set, which is a modification (actually, a weakening) of the concept of a fundamental domain, discussed above.

DEFINITION: $\Omega \subset G$ is a *fundamental set* of Γ if

(F0) $\mathbf{K}\Omega = \Omega$, where $\mathbf{K} = O_n$;
(F1) $\Omega\Gamma = G$;
(F2) $\{\gamma \in \Gamma : \Omega g \cap \Omega\gamma \ne \emptyset\}$ is a finite set for each g in $GL_n(\mathbb{Q})$.

At first glance it seems more natural to require, instead of (F2), the weaker condition (F2′), that $\{\gamma \in \Gamma : \Omega \cap \Omega\gamma \ne \emptyset\}$ is finite. However, (F2) has several technical advantages. In particular, if we start with a fundamental set Ω for Γ, it enables us to construct a fundamental set for any subgroup Γ' of $GL_n(\mathbb{Q})$ commensurable with Γ. It suffices to put $\Omega' = \bigcup_\xi \Omega\xi$, where ξ runs through a set of representatives of $\Gamma'/(\Gamma \cap \Gamma')$.

The results of this section can be restated as follows:

THEOREM 4.7. *The Siegel set $\Sigma_{t,v}$ is a fundamental set for $\Gamma = GL_n(\mathbb{Z})$ in $GL_n(\mathbb{R})$ whenever $t \ge \frac{2}{\sqrt{3}}$ and $v \ge \frac{1}{2}$.*

COROLLARY. *There exists an open fundamental set for any arithmetic subgroup $\Gamma \subset GL_n(\mathbb{Q})$.*

Indeed it is easy to see that the interior $\Sigma_{t,v}^0$ of the Siegel set for $t > \frac{2}{\sqrt{3}}$, $v > \frac{1}{2}$ serves as a fundamental set of $\Gamma = GL_n(\mathbb{Z})$. Using this set, with the help of the observation above, we can construct an open fundamental set for an arbitrary Γ.

4.3. Reduction in arbitrary groups.

In this section we shall carry out the second step of the plan outlined in §4.2 and thus shall establish the existence of a fundamental set for an arbitrary connected algebraic $\mathbb{Q}$-group G. Moreover, as the following assertion shows, we may confine ourselves to the case of a reductive group.

LEMMA 4.7.

(1) *Let N be a unipotent $\mathbb{Q}$-group. Then there is an open, relatively compact subset $U \subset N_{\mathbb{R}}$ such that $N_{\mathbb{R}} = UN_{\mathbb{Z}}$ and $U^{-1}U \cap (nN_{\mathbb{Z}}m)$ is finite, for any n, m in $N_{\mathbb{Q}}$.*

(2) *Let $G = HN$ be a Levi decomposition of a connected $\mathbb{Q}$-group G, where H is a maximal reductive $\mathbb{Q}$-subgroup of G and $N = R_u$ is the unipotent radical. Suppose $\Sigma \subset H_{\mathbb{R}}$ satisfies:*

(a) $H_{\mathbb{R}} = \Sigma H_{\mathbb{Z}}$ *and*

(b) $\Sigma^{-1}\Sigma \cap (gH_{\mathbb{Z}}h)$ *is finite for any g, h in $H_{\mathbb{Q}}$.*

If $U \subset N_{\mathbb{R}}$ is as in (1), then $\Omega = \Sigma U$ satisfies:

(α) $G_{\mathbb{R}} = \Omega G_{\mathbb{Z}}$,

(β) $\Omega^{-1}\Omega \cap (xG_{\mathbb{Z}}y)$ *is finite for any x, y in $G_{\mathbb{Q}}$.*

PROOF: (1) It suffices to establish that $N_{\mathbb{R}}/N_{\mathbb{Z}}$ is compact; for then, using elementary topological arguments (cf., for example, Bourbaki [2, Ch. 3]), we can construct an open, relatively compact set U such that $N_{\mathbb{R}} = UN_{\mathbb{Z}}$. Moreover, the finiteness of $U^{-1}U \cap (nN_{\mathbb{Z}}m)$ follows from the fact that $nN_{\mathbb{Z}}m$ is discrete and closed.

The compactness of $N_{\mathbb{R}}/N_{\mathbb{Z}}$ is easily shown by induction on $r = \dim N$ (as in the proof of Lemma 4.4). If $r = 1$ then $N \simeq \mathbb{C}^+$, moreover with this isomorphism $N_{\mathbb{R}} \simeq \mathbb{R}$ and $N_{\mathbb{Z}} \simeq a\mathbb{Z}$ $(a \in \mathbb{Q})$, so $N_{\mathbb{R}}/N_{\mathbb{Z}} \cong \mathbb{R}/a\mathbb{Z}$ is a one-dimensional torus and thus is compact.

Now take $r > 1$. Since $N/[N,N]$ is abelian and unipotent, the logarithmic map yields a $\mathbb{Q}$-isomorphism $N/[N,N] \xrightarrow{\sim} \mathbb{C}^l$, where $l = \dim N/[N,N]$. (Note that in view of the nilpotency of N we automatically have $l \geq 1$.) It follows that there is an $(r-1)$-dimensional normal $\mathbb{Q}$-subgroup $M \lhd N$ and a one-dimensional $\mathbb{Q}$-subgroup $L \subset N$ such that $N = LM$ is a semidirect product over $\mathbb{Q}$. By induction, $L_{\mathbb{R}}/L_{\mathbb{Z}}$ and $M_{\mathbb{R}}/M_{\mathbb{Z}}$ are compact, and therefore (as above) there exist compact $A \subset L_{\mathbb{R}}$ and $B \subset M_{\mathbb{R}}$ such that $L_{\mathbb{R}} = AL_{\mathbb{Z}}$ and $M_{\mathbb{R}} = BM_{\mathbb{Z}}$. We shall show that the compact set $C = AB$ satisfies $N_{\mathbb{R}} = CN_{\mathbb{Z}}$. Indeed, let $n = lm \in N_{\mathbb{R}} = L_{\mathbb{R}}M_{\mathbb{R}}$. Then $l = az$ for suitable a in A and z in $L_{\mathbb{Z}}$, and $zmz^{-1} = bx$ for suitable b in B and x in $M_{\mathbb{Z}}$. Thus $n = lm = azm = azmz^{-1}z = abxz$, whereas $xz \in N_{\mathbb{Z}}$. This completes the proof of (1).

(2) The proof of (α) is obtained by an argument analogous to the final part of the proof of (1). Now we shall demonstrate (β). According to Corollary 2 of Proposition 4.1, $H_{\mathbb{Z}}N_{\mathbb{Z}}$ has finite index in $G_{\mathbb{Z}}$. Therefore, decomposing $G_{\mathbb{Z}}$ into right or left cosets modulo $H_{\mathbb{Z}}N_{\mathbb{Z}}$, we see that ($\beta$) is equivalent to $\Omega^{-1}\Omega \cap (xH_{\mathbb{Z}}N_{\mathbb{Z}}y)$ being finite for arbitrary x, y in $G_{\mathbb{Q}}$. Since $G_{\mathbb{Q}} = H_{\mathbb{Q}}N_{\mathbb{Q}}$, we have $x = ab$ and $y = cd$, for some a, $c \in H_{\mathbb{Q}}$ and b, $d \in N_{\mathbb{Q}}$. Pick $h \in H_{\mathbb{Z}}$ and $n \in N_{\mathbb{Z}}$. Then

$$\Sigma U x h n y = \Sigma U a b h n c d = \Sigma (ahc) U' g,$$

where $U' = (ahc)^{-1}Uabhc$ is compact and contained in $N_{\mathbb{R}}$ and $g = c^{-1}ncd \in N_{\mathbb{R}}$. Therefore the assertion $\Sigma U \cap \Sigma U(xhny) \neq \emptyset$ is equivalent

to the pair of conditions:

$$\Sigma \cap \Sigma(ahc) \neq \emptyset \tag{4.10}$$

$$U'g \cap U \neq \emptyset. \tag{4.11}$$

According to (b) there exist only a finite number of h satisfying (4.10). The finiteness of the number of possible $n = c(gd^{-1})c^{-1}$ in (4.11) follows from the relative compactness of $(U')^{-1}U$ and from the fact that g in (4.11) belongs to the closed discrete set $cN_{\mathbb{Z}}c^{-1}d$. Q.E.D.

Thus we shall assume henceforth that G is a reductive group. The strategy for obtaining a fundamental set in this case has already been discussed (cf. Lemma 4.2): if $G \subset GL_n(\mathbb{C})$, then we need:

(1) to define a (right) action of GL_n on some set X, such that G will be the stabilizer of a suitable point x in X;

(2) to find a in $GL_n(\mathbb{R})$ for which $xa\Sigma \cap xGL_n(\mathbb{Z})$ is finite, where Σ is a Siegel set in $GL_n(\mathbb{R})$.

Then we shall have a fundamental domain for G of the form

$$\Omega = \Big(\bigcup_{i=1}^{r} a\Sigma b_i^{-1}\Big) \cap G, \text{ where } b_i \in GL_n(\mathbb{Z}).$$

For X it is natural to take a vector space V for which there is a $\mathbb{Q}$-representation $\varrho\colon GL_n(\mathbb{C}) \to GL(V)$, and a vector v in $V_{\mathbb{Q}}$ satisfying $G = \{\, g \in GL_n(\mathbb{C}) : v\varrho(g) = v \,\}$. The existence of such ϱ and v is guaranteed by the stronger version of Chevalley's theorem (cf. Theorem 2.15), which also asserts that the orbit $v\varrho(GL_n(\mathbb{C}))$ is Zariski-closed. Then, if we choose a in $GL_n(\mathbb{R})$ such that $a^{-1}Ga$ is self-adjoint, i.e., invariant under transpose (cf. Theorem 3.7), we see that the finiteness of the required intersection follows from

PROPOSITION 4.5. *Let $\varrho\colon GL_n(\mathbb{C}) \to GL(V)$ be a $\mathbb{Q}$-representation and let L be a lattice in $V_{\mathbb{Q}}$. If v in $V_{\mathbb{R}}$ is a point whose stabilizer*

$$G = \{\, g \in GL_n(\mathbb{C}) : v\varrho(g) = v \,\}$$

is a self-adjoint group and $v\varrho(GL_n(\mathbb{C}))$ is closed in the Zariski topology, then $v\varrho(\Sigma) \cap L$ is finite for any Siegel set $\Sigma \subset GL_n(\mathbb{R})$.

PROOF: Choose a base in $V_{\mathbb{Q}}$ consisting of eigenvectors with respect to $\varrho(D_n)$, where D_n is the group of diagonal matrices, and take the Euclidean norm (which we shall denote as $\|v\|$) on $V_{\mathbb{R}}$, with respect to which this base is orthonormal. For a character $\mu \in \mathbf{X}(\varrho(D_n))$, we let $V_\mu = \{ v \in V : gv = \mu(g)v \ \forall g \in \varrho(D_n) \}$ be the weight space of weight μ; below we shall consider only nonzero subspaces. Then V_{μ_1} is orthogonal to V_{μ_2} for $\mu_1 \neq \mu_2$, so $V = \bigoplus_\mu V_\mu$ is an orthogonal direct sum. Let π_μ denote the orthogonal projection of V onto V_μ. Since V_μ is defined over $\mathbb{Q}$, the $\mathbb{Z}$-submodule generated by all intersections $L \cap V_\mu$ has finite index in L. Thus $\pi_\mu(mL) \subset L$ for a suitable integer m, and consequently $\pi_\mu(L) \subset \frac{1}{m}L$ is a lattice in V_μ. Therefore there exists a constant $c_1 > 0$ such that $\|\pi_\mu(w)\| \geq c_1$, for all w in L and all μ such that $\pi_\mu(w) \neq 0$.

Now let $x = k_x a_x u_x \in GL_n(\mathbb{R})$. Put $y_x = x a_x^{-1}$ and $z_x = x a_x^{-2}$ and write vx instead of $v\varrho(x)$. The set of elements of the form $a_x u_x a_x^{-1}$, where $x \in \Sigma$, is relatively compact by Lemma 4.3. Since $y_x = k_x a_x u_x a_x^{-1}$, it follows that there exists $c_2 > 0$ such that $\|vy_x\| \leq c_2$ for all x in Σ. We claim that $\Delta = \{ vz_x : x \in \Sigma,\ vx \in L \}$ is also bounded. Indeed, let $c = c_1^{-1} c_2^2$; then $\pi_\mu(vy_x) = \pi_\mu(vxa_x^{-1}) = \mu(a_x)^{-1}\pi_\mu(vx)$, and similarly $\pi_\mu(vz_x) = \mu(a_x)^{-2}\pi_\mu(vx)$, implying

$$\|\pi_\mu(vz_x)\| = \frac{\|\pi_\mu(vy_x)\|^2}{\|\pi_\mu(vx)\|} \leq \frac{c_2^2}{c_1} = c.$$

Since $vGL_n(\mathbb{C})$ is closed in V in the Zariski topology, $vGL_n(\mathbb{R})$ is closed in $V_{\mathbb{R}}$ in the Euclidean topology (cf. proof of Theorem 3.6, Corollary 2). Therefore

$$W = \{ w \in vGL_n(\mathbb{R}) : \|\pi_\mu(w)\| \leq c \text{ for all } \mu \}$$

is compact, and consequently there is a compact $U \subset GL_n(\mathbb{R})$ such that $W = vU$. Hence $\{ z_x : vz_x \in \Delta \} \subset G_{\mathbb{R}}U$, since $\Delta \subset W$. But

$$z_x = k_x a_x u_x a_x^{-2} = k_x a_x^{-1} a_x^2 u_x a_x^{-2};$$

if $x \in \Sigma = \Sigma_{t,b}$, then $a_x^2 \in A_{t^2}$; so $\{ a_x^2 u_x a_x^{-2} : x \in \Sigma \}$ is relatively compact. Therefore $k_x a_x^{-1} \in G_{\mathbb{R}}U_1$ for a suitable compact U_1. Applying $\theta: g \mapsto {}^t g^{-1}$ and bearing in mind that k_x is an orthogonal matrix and a_x a diagonal matrix, we obtain $k_x a_x \in G_{\mathbb{R}}\theta(U_1)$; so $x = k_x a_x u_x \in GU_2$, where $U_2 = \theta(U_1)U$ is compact. Thus, $v\Sigma \cap L$ is contained in vU_2, and consequently is both compact and discrete, or in other words finite. Proposition 4.5 is proved.

This completes the construction of a fundamental set in a reductive group. The results obtained are formulated in

THEOREM 4.8 (BOREL, HARISH-CHANDRA [2]). *Let $G \subset GL_n(\mathbb{C})$ be a reductive algebraic $\mathbb{Q}$-group, and let $\Sigma = \Sigma_{t,v}$ $(t \geq \frac{2}{\sqrt{3}},\ v \geq \frac{1}{2})$ be a Siegel set of $GL_n(\mathbb{R})$. Then we can find a in $GL_n(\mathbb{R})$, $b_1, \ldots, b_r$ in $GL_n(\mathbb{Z})$ such that $\Omega = \left(\bigcup_{i=1}^r a\Sigma b_i\right) \cap G$ has the following properties:*

(0) $\mathbf{K}\Omega = \Omega$ *for a suitable maximal compact subgroup* $\mathbf{K}$ *of* $G_{\mathbb{R}}$;
(1) $\Omega G_{\mathbb{Z}} = G_{\mathbb{R}}$;
(2) $\Omega^{-1}\Omega \cap xG_{\mathbb{Z}}y$ *is finite for any* x, y *in* $G_{\mathbb{Q}}$.

It remains only to prove (0). Recall that a in $GL_n(\mathbb{R})$ has been chosen to satisfy the requirement that $a^{-1}Ga$ be self-adjoint. But then $a^{-1}Ga \cap O_n(\mathbb{R})$ is a maximal compact subgroup of $a^{-1}G_{\mathbb{R}}a$ (cf. Proposition 3.10), so $\mathbf{K} = G \cap (aO_n(\mathbb{R})a^{-1})$ is a maximal compact subgroup of $G_{\mathbb{R}}$. By construction Σ satisfies $O_n(\mathbb{R})\Sigma = \Sigma$, from which (0) clearly follows.

As in §4.2, the results of this section can be restated more concisely using the concept of a fundamental set. Its definition for the general case is analogous to the definition given in §4.2 for the case of $GL_n(\mathbb{C})$, and is as follows:

DEFINITION: Let G be an algebraic $\mathbb{Q}$-group, and let $\Gamma \subset G_{\mathbb{Q}}$ be an arithmetic subgroup. $\Omega \subset G_{\mathbb{R}}$ is a *fundamental set* for Γ if

(F0) $\mathbf{K}\Omega = \Omega$ for a suitable maximal compact subgroup $\mathbf{K} \subset G_{\mathbb{R}}$;
(F1) $\Omega\Gamma = G_{\mathbb{R}}$;
(F2) $\Omega^{-1}\Omega \cap (xG_{\mathbb{Z}}y)$ is finite for any x, y in $G_{\mathbb{Q}}$.

In view of Lemma 4.7 and the absence of compact subgroups in unipotent groups, Theorem 4.8 yields

COROLLARY. *Let G be a connected $\mathbb{Q}$-group, and let $\Gamma \subset G_{\mathbb{Q}}$ be an arithmetic subgroup. Then there exists an open fundamental set for Γ in $G_{\mathbb{R}}$.*

The structure theorems for arithmetic groups (cf. §4.4) are based on this corollary. There we see the importance of all three conditions (F0)–(F2). In particular, (F1) and (F2) guarantee that Γ is finitely generated. (F0) means that the image of Ω in the symmetric space $X = G_{\mathbb{R}}/\mathbf{K}$ is a fundamental set for the induced action of Γ on X, from which it follows, in view of X being simply connected, that Γ can be defined by a finite number of relations.

Another application of reduction theory lies in the proof of the following finiteness theorem for the orbits of arithmetic groups.

THEOREM 4.9. *Let $\varrho: G \to GL(V)$ be a $\mathbb{Q}$-representation of a reductive $\mathbb{Q}$-group G, and let $\Gamma \subset G_{\mathbb{Q}}$ be an arithmetic subgroup and $L \subset V_{\mathbb{Q}}$ a Γ-invariant lattice. If $X = v\varrho(G)$ is Zariski-closed, then $X \cap L$ is the union of a finite number of orbits of Γ.*

PROOF: Let $G \subset GL_n(\mathbb{C})$. First we consider the special case where ϱ is the restriction of a $\mathbb{Q}$-representation $\pi: GL_n(\mathbb{C}) \to GL(V)$, such that the orbit $Y = v\pi(GL_n(\mathbb{C}))$ is Zariski-closed and the stabilizer of v under π lies in G, i.e., equals the stabilizer H of v under ϱ. $X_{\mathbb{R}}$ is the union of a finite number of orbits of $G_{\mathbb{R}}$ (cf. Theorem 3.6, Corollary 2), i.e., $X_{\mathbb{R}} = \bigcup_i v_i\varrho(G_{\mathbb{R}})$. To prove the theorem one need consider only those i for which $v_i\varrho(G_{\mathbb{R}}) \cap L \neq \emptyset$; thus we may assume $v_i \in L$.

So, it suffices to show that $v\varrho(G_{\mathbb{R}}) \cap L$ consists of a finite number of orbits of Γ. Moreover, without loss of generality, we may assume $\Gamma = G_{\mathbb{Z}}$, and L to be invariant under $\varrho(GL_n(\mathbb{Z}))$ (cf. Proposition 4.2). By Theorem 4.8, we can find a in $GL_n(\mathbb{R})$ and b_i in $GL_n(\mathbb{Z})$ such that

$$G_{\mathbb{R}} = \Big(\Big(\bigcup_i (a\Sigma b_i)\Big) \cap G\Big) G_{\mathbb{Z}} \tag{4.12}$$

for a suitable Siegel set $\Sigma \subset GL_n(\mathbb{R})$. Moreover, for a we can take any element of $GL_n(\mathbb{R})$ for which $a^{-1}Ga$ is self-adjoint. Therefore, by Theorem 3.8, we can choose a such that $a^{-1}Ha$ is also self-adjoint. It follows from (4.12) that it suffices to establish that $v\varrho(a\Sigma b \cap G_{\mathbb{R}}) \cap L$ is finite whenever $b \in GL_n(\mathbb{Z})$. Since L is invariant under $\varrho(GL_n(\mathbb{Z}))$, the latter is equivalent to $w\varrho(\Sigma) \cap L$ being finite, where $w = v\varrho(a)$. But the stabilizer of w equals $a^{-1}Ha$, which is self-adjoint, so the required finiteness follows from Proposition 4.5.

The general case reduces to our special case. Since X is closed, the stabilizer H of v in G is a reductive group. Therefore, by the strong version of the Chevalley theorem (Theorem 2.15), there is a $\mathbb{Q}$-representation $\pi: GL_n(\mathbb{C}) \to GL(W)$ and a point w in $W_{\mathbb{Q}}$ whose stabilizer under π is H, and $Y = w\pi(GL_n(\mathbb{C}))$ is Zariski-closed. In addition, it follows from Proposition 4.2 that w is contained in a $\varrho(GL_n(\mathbb{Z}))$-invariant lattice $M \subset W_{\mathbb{Q}}$. Then the orbit $X' = w\pi(G)$ is also Zariski-closed, since the canonical map $GL_n(\mathbb{C}) \to Y$ (given by $g \mapsto w\pi(g)$) is open. Thus, the set $X' \cap M$ is the union of a finite number of orbits of Γ. Moreover, passing from M to $\frac{1}{d}M$ ($d \in \mathbb{Z}$), which is also $\varrho(GL_n(\mathbb{Z}))$-invariant, we see that $X' \cap (\frac{1}{d}M)$ is the union of a finite number of orbits of Γ, for any d in $\mathbb{Z}$.

It remains to pass from X' to X. To do so, note that each of X and X' is a realization of the homogeneous space G/H, i.e., there exists a G-equivariant isomorphism $\varphi: X \to X'$ defined over $\mathbb{Q}$. Since X is closed in V, φ is given by polynomials $P_i(x_1, \ldots, x_r)$ $(1 \leq i \leq s)$ with rational coefficients, in the coordinates determined by the bases of L and M, respectively. If d is the common denominator of these coefficients, then $\varphi(X \cap L) \subset X' \cap (\frac{1}{d}M)$. Therefore, since the number of orbits of $G_{\mathbb{Z}}$ in $X' \cap (\frac{1}{d}M)$ is finite and φ is G-equivariant, it follows that the number of orbits of $G_{\mathbb{Z}}$ in $X \cap L$ is finite. Q.E.D.

To conclude this section we present a variant of condition (F2) from the definition of a fundamental set, to be used in the next chapter when we develop a reduction theory for adele groups.

LEMMA 4.8. *For $\Omega \subset G_{\mathbb{R}}$, condition (F2) is equivalent to the following:*

(F2)′ *$\Omega^{-1}\Omega \cap xG_r y$ is finite, for any x, y in $G_{\mathbb{Q}}$ and any r in $\mathbb{Z}$, where $G_r = \{ g \in G_{\mathbb{Q}} : rg, rg^{-1} \in M_n(\mathbb{Z}) \}$.*

Indeed, to prove $(F2) \Rightarrow (F2)'$ it suffices to show that G_r is contained in a finite union of cosets of $G_{\mathbb{Z}}$. But if $g \in G_r$, then

$$r\mathbb{Z}^n \subset g(\mathbb{Z}^n) \subset r^{-1}\mathbb{Z}^n.$$

Since there are only finitely many lattices between $r\mathbb{Z}^n$ and $r^{-1}\mathbb{Z}^n$, there are only a finite number of possibilities for $g(\mathbb{Z}^n)$ $(g \in G_r)$. Noting that $g(\mathbb{Z}^n) = h(\mathbb{Z}^n)$ implies $h^{-1}g \in G_{\mathbb{Z}}$, we obtain $G_r \subset \bigcup_i g_i G_{\mathbb{Z}}$, as desired, where the g_i are chosen in such a way that $g_i(\mathbb{Z}^n)$ run through all possible intermediate lattices of the form $g(\mathbb{Z}^n)$ for g in G_r, between $r\mathbb{Z}^n$ and $r^{-1}\mathbb{Z}^n$. The converse $(F2)' \Rightarrow (F2)$ is self-evident.

4.4. Group-theoretic properties of arithmetic groups.

In this section we shall prove several fundamental results (stated in §4.1) on the abstract properties of arithmetic groups. The elegance and relative brevity of the proofs may be viewed as compensation for the effort spent developing reduction theory.

We begin with

THEOREM 4.2. *Let Γ be an arithmetic subgroup of an algebraic $\mathbb{Q}$-group G. Then Γ is finitely presented as an abstract group, i.e., can be defined using a finite number of generators and defining relations.*

PROOF OF THEOREM 4.2: It suffices to establish that Γ has a finitely presented subgroup of finite index. Therefore, we may assume that G is connected and that $\Gamma \subset G_{\mathbb{R}}$. We shall work in the space $X = G_{\mathbb{R}}/\mathbf{K}$, where $\mathbf{K}$ is a maximal compact subgroup of $G_{\mathbb{R}}$. By Proposition 3.10, X is connected and simply connected. If Σ is an open fundamental set for Γ in $G_{\mathbb{R}}$ (cf. §4.3, and Theorem 4.8 and its Corollary), then since $\mathbf{K}\Sigma = \Sigma$, the following two conditions are satisfied for the image Ω of Σ in X:

(i) $\Omega\Gamma = X$;
(ii) $\Delta = \{ \delta \in \Gamma : \Omega\delta \cap \Omega \neq \emptyset \}$ is finite.

(We consider the natural action of Γ on X by right translations.) We shall show that the finite presentability of Γ is a formal consequence of the connectedness, local connectedness and simple-connectedness of X, of the

openness of Ω, and of (i) and (ii). Therefore the same result holds for an arbitrary group of transformations of any topological space X satisfying these hypotheses (note that Behr [1] proves this under somewhat weaker hypotheses, i.e., instead of requiring that Ω be open he requires only that Ω lie in the interior of $\Omega\Delta$).

LEMMA 4.9. *Δ generates the group Γ.*

PROOF: Let Γ_0 be the subgroup generated by Δ. Then (i) implies $X = (\Omega\Gamma_0)\cup(\Omega(\Gamma\backslash\Gamma_0))$. Moreover, if $\Omega\gamma\cap\Omega\delta \neq \emptyset$, where $\gamma \in \Gamma_0$, then $\delta\gamma^{-1} \in \Delta$, implying $\delta \in \Gamma_0$; thus $\Omega\Gamma_0$ and $\Omega(\Gamma \setminus \Gamma_0)$ are disjoint. Since both are open sets and X is a connected space, we conclude $\Omega(\Gamma \setminus \Gamma_0) = \emptyset$, i.e., $\Gamma = \Gamma_0$, proving the lemma.

Now we proceed to construct the defining relations for Γ. Let F denote the free group on a replica $\bar{\Delta}$ of the set Δ, whose elements are in one-to-one correspondence with those of Δ via a bijection $\bar{\delta} \mapsto \delta$, and let $\varphi: F \to \Gamma$ denote the homomorphism determined by this bijection. To obtain the defining relations for Γ, first of all consider the *local* relations, i.e., those of the form

$$\bar{\delta}_1\bar{\delta}_2(\overline{\delta_1\delta_2})^{-1} = e, \tag{4.13}$$

where δ_1, δ_2 run through the elements of Δ for which $\delta_1\delta_2 \in \Delta$.

To understand their role, let L denote the normal subgroup of F generated by the left-hand sides of the local relations. Clearly $\varphi(\bar{\delta}_1\bar{\delta}_2(\overline{\delta_1\delta_2})^{-1}) = 1$, so $\varphi(L) = 1$. Let N be a normal subgroup of F containing L and contained in $K = \ker\varphi$. Consider $H = F/N$ and the natural homomorphisms $\sigma: F \to H$, $\theta: H \to \Gamma$, satisfying $\theta \circ \sigma = \varphi$. Also, endowing H with the discrete topology, we introduce the quotient space S of $\Omega \times H$ under the following relation:

$(x_1, h_1) \sim (x_2, h_2)$ if there is δ in Δ such that $x_2 = x_1\delta$ and $h_1 = \sigma(\bar{\delta})h_2$.

It is (4.13) that assures $\sim$ being an equivalence relation, thus enabling us to define S. Indeed, the reflexivity of $\sim$ is obvious ($1 \in \Delta$) and symmetry follows from the fact that if $\delta \in \Delta$ then $\delta^{-1} \in \Delta$ (since $\Omega\delta \cap \Omega \neq \emptyset \Leftrightarrow \Omega \cap \Omega\delta^{-1} \neq \emptyset$); moreover $\sigma(\bar{\delta})^{-1} = \sigma(\bar{\delta}^{-1})$ by virtue of the local relations. Let us prove transitivity. If $(x_1, h_1) \sim (x_2, h_2)$ and $(x_2, h_2) \sim (x_3, h_3)$, then there are δ_1, δ_2 in Δ such that

$$\begin{aligned} x_2 &= x_1\delta_1, \qquad & h_1 &= \sigma(\bar{\delta}_1)h_2 \\ x_3 &= x_2\delta_2, \qquad & h_2 &= \sigma(\bar{\delta}_2)h_3. \end{aligned}$$

Then $x_3 = x_1\delta_1\delta_2$, so $\delta_1\delta_2 \in \Delta$, and $h_1 = \sigma(\bar{\delta}_1)\sigma(\bar{\delta}_2)h_3 = \sigma(\overline{\delta_1\delta_2})h_3$, by virtue of the local relations.

Now let $\alpha: \Omega \times H \to S$ denote the canonical map, and $\beta: \Omega \times \Gamma \to X$ the "product" map. If $(x_1, h_1) \sim (x_2, h_2)$, then $x_2 = x_1\delta$ and $h_1 = \sigma(\bar{\delta})h_2$ for some δ in Δ, implying

$$\beta(x_1, \theta(h_1)) = x_1\theta(h_1) = (x_1\delta)\theta(\sigma(\bar{\delta})^{-1}h_1) = x_2\theta(h_2) = \beta(x_2, \theta(h_2)),$$

so there exists a unique continuous map $p: S \to X$ making the following diagram commutative:

$$\begin{array}{ccc} \Omega \times H & \xrightarrow{(\mathrm{id},\,\theta)} & \Omega \times \Gamma \\ \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} \\ S & \xrightarrow{\quad p \quad} & X \end{array} \tag{4.14}$$

LEMMA 4.10. *p is a covering map whose multiplicity equals $|\ker\theta|$.*

PROOF: Put $\Psi = \alpha(\Omega \times \{e\})$. Then the inverse image

$$\alpha^{-1}(\Psi) = \bigcup_{\delta\in\Delta} (\Omega \cap \Omega\delta, \sigma(\bar{\delta})^{-1})$$

is an open subset of $\Omega \times H$ and hence Ψ is open in S. The restriction of p to Ψ is injective and yields a homeomorphism $\Psi \xrightarrow{\sim} \Omega$; indeed, if $p(\alpha(x_1, e)) = p(\alpha(x_2, e))$, then $x_1 = x_2$ by the commutativity of (4.14).

Next we show that

$$p^{-1}(\Omega) = \bigcup_h \Psi h,$$

where the union is taken over all $h \in \ker\theta$, and all the Ψh are disjoint. (Henceforth we consider the induced action of H on S; note, in this regard, the useful relation $p(xh) = p(x)\theta(h)$.) If $p(\alpha(x, h)) = y \in \Omega$, then $x\theta(h) = y \in \Omega$, so $\theta(h) = \delta \in \Delta$, i.e. $g = \sigma(\bar{\delta})^{-1}h \in \ker\theta$. But then by definition $(x, h) \sim (y, g)$, as required. Lastly, if $\alpha(x, e) = \alpha(y, h)$, where $h \in \ker\theta$, then $h \in \Delta$; thus $h = e$, since $\varphi|_{\bar{\Delta}}$ is injective. This completes the proof of the lemma.

If Ω is connected then S is also connected. Indeed $S = \bigcup_{h\in H} \Psi h$; since Ψ is connected, it suffices to note that any translate Ψh is connected to Ψ via the chain of pairwise intersecting translates $\Psi_0 = \Psi$, $\Psi_1 = \Psi h_1, \ldots,$ $\Psi_m = \Psi h_m$, (where $h_m = h$). If $h = \sigma(\bar{\delta}_1 \ldots \bar{\delta}_d)$ then we merely put $h_1 = \sigma(\bar{\delta}_d)$, $h_2 = \sigma(\bar{\delta}_{d-1}\bar{\delta}_d)$, $\ldots$, $h_{m-1} = \sigma(\bar{\delta}_2 \ldots \bar{\delta}_d)$, $h_m = \sigma(\bar{\delta}_1 \ldots \bar{\delta}_d)$. Since X is simply connected it follows that p is bijective; hence $\ker\theta$ is

trivial and $N = L$. Thus, for Ω connected, the local relations suffice to define Γ.

In general we work with the connected components of Ω, which we denote by $\{\Omega_i\}_{i\in I}$. Since X is locally connected and Ω is open, all the Ω_i are also open in X. Fix a component $X^0 = \Omega_0$, and let $X^{(1)}$ denote $\bigcup_{i,\gamma} \Omega_i\gamma$, the union taken over all (i,γ) in $I\times\Gamma$ for which $\Omega_i\gamma\cap\Omega_0 \neq \emptyset$. Inductively, given $X^{(1)},\dots,X^{(k)}$, put $X^{(k+1)} = \bigcup_{i,\gamma} \Omega_i\gamma$, the union taken pairwise over all (i,γ) for which $\Omega_i\gamma \cap X^{(k)} \neq \emptyset$. $X' = \bigcup_{k=0}^{\infty} X^{(k)}$ is clearly open in X. Its complement is a union of sets of the form $\Omega_i\gamma$, and therefore is also open. Indeed,

$$X = \Omega\Gamma = \bigcup_{\substack{i\in I\\ \gamma\in\Gamma}} \Omega_i\gamma,$$

however, if $\Omega_{i_1}\gamma_1 \cap \Omega_{i_2}\gamma_2 \neq \emptyset$ for $\Omega_i\gamma_1 \subset X^{(k)}$, then $\Omega_{i_2}\gamma_2 \subset X^{(k+1)} \subset X'$. Since X is connected, it follows that $X' = X$, i.e., any $\Omega_i\gamma$ is connected to Ω_0 by a chain of pairwise intersecting translations in the connected components of Ω.

Now take $\Omega_0\delta$ for δ in Δ. There is a sequence $\{\Omega_{i_j}\gamma_j\}_{j=0}^{m}$ such that $i_0 = i_m = 0$, $\gamma_0 = 1$, $\gamma_m = \delta$ and $\Omega_{i_j}\gamma_j \cap \Omega_{i_{j+1}}\gamma_{j+1} \neq \emptyset$ for all $j = 0,\dots,m-1$. By induction, define ω_j in F such that $\varphi(\omega_j) = \gamma_j$ for all $j = 0,\dots,m$. To do so, put $\omega_0 = e$. If $\omega_0,\dots,\omega_k$ are already defined, then put $\omega_{k+1} = \bar{\delta}_k\omega_k$, where $\delta_k = \gamma_{k+1}\gamma_k^{-1} \in \Delta$. (Thus ω_m depends on δ.) Let N denote the normal subgroup of F generated by the left sides of (4.13) and of

$$\delta^{-1}\omega_m = e \tag{4.15}$$

for all δ in Δ.

LEMMA 4.11. *$N = K$, implying Γ is finitely presented.*

PROOF: Put $\Psi_i = \alpha(\Omega_i \times \{e\})$. We claim that for any δ in Δ and for the corresponding elements ω_j constructed above, we have

$$\Psi_{i_j}\sigma(\omega_j) \cap \Psi_{i_{j+1}}\sigma(\omega_{j+1}) \neq \emptyset. \tag{4.16}$$

Indeed, take $x_j\gamma_j = x_{j+1}\gamma_{j+1} \in \Omega_{i_j}\gamma_j\cap\Omega_{i_{j+1}}\gamma_{j+1}$. Then $\delta_j = \gamma_{j+1}\gamma_j^{-1} \in \Delta$ and $x_j = x_{j+1}\delta_j$, $\sigma(\omega_{j+1}) = \sigma(\bar{\delta}_j)\sigma(\omega_{j+1})$, from which (4.16) follows. Let Φ denote the union of the $\Psi_{i_j}\sigma(\omega_j)$ obtained for all δ in Δ. Since any chain of $\Psi_{i_j}\sigma(\omega_j)$ begins with Ψ_0, we see Φ is connected. Let Y be the connected component of S containing Φ. For any δ in Δ we have $\Psi_0\sigma(\bar{\delta}) = \Psi_{i_m}\sigma(\omega_m) \subset \Phi$, so $\Phi \cap \Phi\sigma(\bar{\delta}) \neq \emptyset$ and therefore $Y\sigma(\bar{\delta}) = Y$. Since the $\sigma(\bar{\delta})$ $(\delta \in \Delta)$ generate H, we have $Yh = Y$ for any h in H. By the local connectedness of S it is easy to show that $p|_Y : Y \to X$ is also a covering map. Since X is simply connected, $p|_Y$ is bijective. On the other hand, all $\Psi_0 h$ $(h \in \ker\theta)$ lie in Y, are disjoint (cf. proof of Lemma 4.10), and their images are in Ω_0. Hence $\ker\theta = \{e\}$, proving the lemma.

Thus the proof of Theorem 4.2 is complete.

In principle the proof of Theorem 4.2 enables us to give an explicit presentation of an arithmetic group in terms of generators and relations, if a "good" fundamental set is known. In this regard, let us take the classical example of $SL_2(\mathbb{Z})$.

EXAMPLE (GENERATORS AND RELATIONS FOR $SL_2(\mathbb{Z})$): As we have seen (cf. §4.2), $X = SL_2(\mathbb{R})/SO_2(\mathbb{R})$ can be identified with the upper half-plane P. $\Gamma = PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z})/\{\pm e\}$ acts on the right on P and its fundamental domain is $D = \{z \in P : |z| > 1,\ |\Re z| < 1/2\}$ (Proposition 4.4). The closure $\bar{D}$ satisfies conditions (i) and (ii) given in the proof of Theorem 4.2, but is not open in P. Nevertheless, we shall consider $\Delta = \Delta_{\bar{D}} = \{\delta \in \Gamma : \bar{D} \cap \bar{D}\delta \neq \emptyset\}$. The translations of $\bar{D}$ by elements of this set are depicted in Figure 4.2 (above).

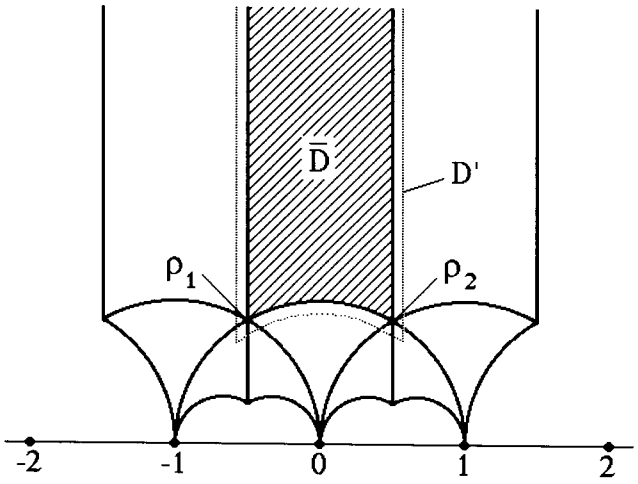


Figure 4.2.

Clearly if we were to pass from $\bar{D}$ to a slightly larger domain D', then $\Delta_{D'} = \{\delta \in \Gamma : D' \cap D'\delta \neq \emptyset\}$ would still be Δ. On the other hand, the proof of Theorem 4.2 can be applied to D'. From this it follows that Δ is a set of generators of Γ, and all the relations are consequences of local relations. It is obvious from Figure 4.2 that $|\Delta| = 10$; therefore, if we were to try to apply the method used in the proof of Theorem 4.2 directly, we would have to work with 10 generators and to analyze $10 \times 10 = 100$ local

relations. To shorten this process we shall apply some additional geometric considerations.

Recall that P is a model of the Lobachevsky geometry, in which rays perpendicular to Ox and semicircles with centers on Ox serve as straight lines. Thus, $\bar{D}$ is a non-Euclidean triangle with two finite vertices (ϱ_1, ϱ_2) and one vertex at infinity. Also, Γ acts on P by isometry, so the translations $\bar{D}\gamma$ $(\gamma \in \Gamma)$ are also triangles which yield a simplicial partitioning of P, i.e., either two triangles do not intersect or they have a common vertex; the proof follows from the fact that the triangles adjacent to $\bar{D}$ intersect $\bar{D}$ as required (cf. Figure 4.2). Then, by a slight modification of the proof of the first part of the theorem, we can show that Γ is generated by those γ for which $\bar{D}$ and $\bar{D}\gamma$ have a common side. (Alternately, one could note that the subgroup generated by such γ contains Δ, cf. below.) In the case under consideration, the set of such γ consists of three elements: $T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ (the transformation corresponding to $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$), $T^{-1} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$ and $S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$. Geometrically, the transformation T is a translation of one unit parallel to the Ox axis, and S is the composition of the inversion with respect to the circle $|z| = 1$ and the reflection relative to the Oy axis. With this description it is easy to show that triangles adjacent to $\bar{D}$ can be obtained from $\bar{D}$ by the transformations shown in Figure 4.3 (below).

The local relations introduced in the proof of Theorem 4.2 have the form

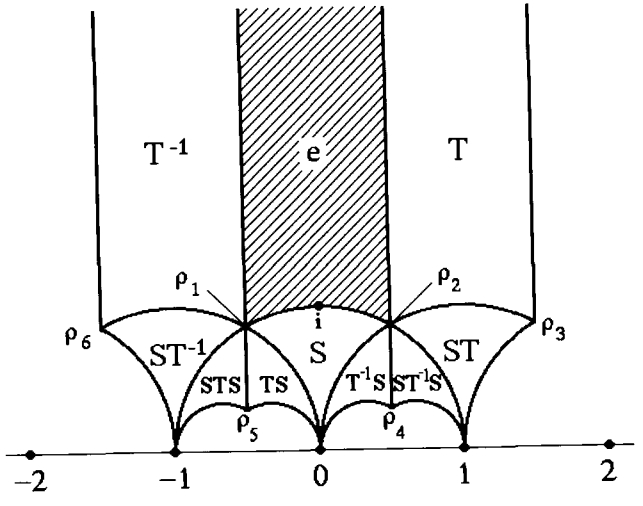


Figure 4.3.

$\bar{\delta}_1\bar{\delta}_2 = \bar{\delta}_3$, where $\delta_3 = \delta_1\delta_2$ and $\delta_1, \delta_2, \delta_3 \in \Delta$. First we shall analyze the local relations in which either δ_1 or δ_2 equals S. A quick glance at the various possible relations shows that they are all consequences of $S^2 = e$.

Before passing to the general case, we must make one remark. If ϱ_1 and ϱ_2 are finite vertices of $\bar{D}$, then for any δ in Δ we have $\{\varrho_1, \varrho_2\}\delta \cap \{\varrho_1, \varrho_2\} \neq \emptyset$, which is a consequence of $\bar{D}\delta \cap \bar{D} \neq \emptyset$ and of the fact that the action of Γ is simplicial. Since $\varrho_1 S = \varrho_2$, $\varrho_2 S = \varrho_1$, then for any δ in Δ the following condition is satisfied: $S\delta$, $\delta S \in \Delta$ and either δ, or $S\delta$ and δS stabilize one of the points ϱ_1, ϱ_2.

Now we shall show that, modulo the relations containing S, any local relation reduces to a relation in which δ_1 and δ_2 stabilize one of the vertices. Indeed, let $\delta_1\delta_2 = \delta_3$ and let $\delta_1, \delta_2, \delta_3 \in \Delta$. Multiplying δ_3 by S if necessary, we may assume that $\varrho_1\delta_3 = \varrho_1$ (or $\varrho_2\delta_3 = \varrho_2$, which can be treated analogously). If $\varrho_1\delta_2 = \varrho_1$, then $\varrho_1\delta_1 = \varrho_1$, and there remains nothing to prove.

Let us show that the case $\varrho_2\delta_2 = \varrho_2$ does not occur. It suffices to establish that under these conditions

$$\{\varrho_1, \varrho_2\}(\delta_3\delta_2^{-1}) \cap \{\varrho_1, \varrho_2\} = \emptyset.$$

Obviously $\delta_3\delta_2^{-1}$ cannot stabilize any of the vertices, so we must show that the following relations are impossible:

$$\varrho_1(\delta_3\delta_2^{-1}) = \varrho_2, \tag{4.17}$$

$$\varrho_2(\delta_3\delta_2^{-1}) = \varrho_1. \tag{4.18}$$

If (4.17) were to hold, then $\varrho_1 = \varrho_1\delta_3 = \varrho_2\delta_2 = \varrho_2$, contradiction. If (4.18) were to hold, then $\varrho_2\delta_3 = \varrho_1\delta_2$; but it is easy to verify that $\{\varrho_1\delta : \varrho_2\delta = \varrho_2\}$ consists of the points ϱ_1, ϱ_3, ϱ_4, and is disjoint from $\{\varrho_2\delta : \varrho_1\delta = \varrho_1\}$, which consists of the points ϱ_2, ϱ_5, ϱ_6.

So, let $\delta_1\delta_2 = \delta_3$ and $\varrho_1\delta_3 = \varrho_1$, but $\varrho_1\delta_2 \neq \varrho_1$. Let us rewrite the corresponding local relation as $(\delta_1 S)(S\delta_2) = \delta_3$. Since $\varrho_2\delta_2 \neq \varrho_2$, then $\varrho_1(S\delta_2) = \varrho_1$ and $\varrho_1(\delta_1 S) = \varrho_1$. Thus, we may assume all δ_1, δ_2, δ_3 stabilize ϱ_1 or ϱ_2.

LEMMA 4.12. *The stabilizer of ϱ_1 (resp., ϱ_2) in Γ is the cyclic group of order three generated by TS (resp., ST).*

PROOF: If $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, then $zg = \frac{dz+b}{cz+a}$. Then $\varrho_1 g = \varrho_1$ can be rewritten as $c\varrho_1^2 + (a-d)\varrho_1 - b = 0$. But $\varrho_1 = \frac{-1+\sqrt{3}i}{2}$ and the minimal polynomial of ϱ_1 over $\mathbb{Q}$ has the form $t^2 + t + 1 = 0$. Therefore, if a, b, c, $d \in \mathbb{Z}$ and

$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = 1$, then either $b = c = a - d = 0$, which corresponds to the identity transformation, or $b = \pm 1$, $c = \mp 1$, $a - d = \mp 1$, which corresponds to $\pm \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$, $\pm \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$. All that remains is to note that

$$TS = \begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix}, \qquad (TS)^2 = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}.$$

The stabilizer of ϱ_2 can then be computed using $\varrho_1 S = \varrho_2$. This completes the proof of the lemma.

It follows from Lemma 4.12 that the local relations in which all letters stabilize one of the vertices reduce to $(ST)^3 = e$. Thus, $PSL_2(\mathbb{Z})$ is given by the generators S, T and the relations $S^2 = (ST)^3 = e$. Likewise, $SL_2(\mathbb{Z})$ is given by the generators S, T, U and the relations $S^2 = (ST)^3 = U$ and $U^2 = e$.

It is clear even from this example that Theorem 4.12 does not completely solve the problem of finding an explicit presentation of arithmetic groups in terms of their generators and relations. For numerous examples of explicit presentations of (arithmetic) groups in terms of generators and relations, see Coxeter and Moser [1]. From the point of view of the theory of algebraic groups, the explicit presentation of the group $G_{\mathbb{Z}}$ for a Chevalley group G found by Behr [5] is of interest. Namely, if G is a simply connected almost simple Chevalley group, constructed using a root system R, then $G_{\mathbb{Z}}$ is generated by $x_\alpha (\alpha \in R)$ and, for the case $R \neq A_1$, is defined by

$$[x_\alpha, x_\beta] = \prod_{j,i>0} x_{i\alpha+j\beta}^{N_{ij}^{\alpha,\beta}}$$

$$(x_\alpha^{-1} x_{-\alpha} x_\alpha^{-1})^4 = 1,$$

where, in the first equation α, β range over all roots $\beta \neq -\alpha$; and in the second equation α is some long root, $[x_\alpha, x_\beta]$ is the commutator of x_α and x_β, and $N_{i,j}^{\alpha,\beta}$ is some integer (about which one can obtain more detailed information from Lemma 15 of Steinberg [2]). For the case $R = A_1$, i.e., $G = \mathbf{SL}_2$, the first of the above relations should be replaced by

$$x_\alpha x_{-\alpha}^{-1} x_\alpha = x_{-\alpha}^{-1} x_\alpha x_{-\alpha}^{-1}.$$

If $G = \mathbf{SL}_n$ then Behr's result gives the well-known generation of $SL_n(\mathbb{Z})$ by elementary matrices. In this connection, we should mention a result of Carter-Keller [1], according to which any element of $SL_n(\mathbb{Z})$ can be written as a product of elementary matrices the number of which does not exceed some constant (the result also holds when $\mathbb{Z}$ is replaced by the ring of integers $\mathcal{O}$ of an algebraic number field). O. I. Tavgen [3] generalized Carter and Keller's result to arbitrary Chevalley groups of rank > 1 (taking "root" generators x_α instead of elementary matrices). An analogous result was obtained by K. Ch. Zakiryanov [1] for the case $G = \mathbf{Sp}_{2n}$ $(n \geq 3)$. He, however, used a larger system of generators and, moreover, asserted erroneously that $Sp_4(\mathbb{Z})$ does not have bounded generation with respect to the elementary symplectic matrices.

In general an abstract, finitely generated group Γ is called a group with *bounded generation* if there is a finite generating set $X \subset \Gamma$ such that any g in Γ can be written as $g = x_1^{\alpha_1} \dots x_l^{\alpha_l}$, where $x_i \in X$, $\alpha_i \in \mathbb{Z}$ and l is bounded by a constant, independent of g.

PROBLEM: What arithmetic groups have bounded generation?

From Tavgen [3] it follows these are, for example, the arithmetic subgroups of $G_{\mathbb{Z}}$, where G is a Chevalley group of rank > 1. On the other hand, he shows there that $SL_2(\mathbb{Z})$ and $SL_2(\mathcal{O}_d)$, where $\mathcal{O}_d$ is the ring of integers of the imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$ $(d > 0)$, do not have bounded generation. A comparison of these facts with known results on the congruence problem (cf. §9.5) suggests that, among the arithmetic subgroups of simply connected simple algebraic groups, the groups with bounded generation are exactly those with the affirmative solution of the congruence problem (i.e., for which the corresponding congruence kernel is finite). Further development of this line of reasoning will most likely lead to a new approach to the congruence problem.

To complete our discussion of generators and relations of arithmetic groups, we must call the reader's attention to the fact that this subject can be treated in terms of the general theory of discrete transformation groups (cf. the survey of Vienberg and Schwarzman [1]). It should also be emphasized that many groups studied in this theory—in particular, discrete groups generated by reflections and groups with a simplicial fundamental domain (cf. the example above)—turn out to be non-arithmetic.

The next result goes back to Jordan's classic work (cf. Debone et al. [1]), which established that $SL_n(\mathbb{Z})$ has only a finite number of non-conjugate finite subgroups.

THEOREM 4.3. *Let G be an algebraic group defined over $\mathbb{Q}$. Then there are finitely many conjugacy classes of finite subgroups of $G_{\mathbb{Z}}$.*

PROOF: Putting $\Gamma = G_{\mathbb{Z}}$, we shall use the notation introduced in proving Theorem 4.2 for this situation. In particular, $\mathbf{K}$ is a maximal compact subgroup of $G_{\mathbb{R}}$, $X = G_{\mathbb{R}}/\mathbf{K}$ and $\Omega \subset X$ is a subset such that

(1) $X = \Omega\Gamma$ and

(2) $\Delta = \{\delta \in \Gamma : \Omega\delta \cap \Omega \neq \emptyset\}$ is finite.

Let $\Theta \subset \Gamma$ be a finite subgroup. By virtue of the fact that any compact subgroup of $G_{\mathbb{R}}$ is conjugate to $\mathbf{K}$ (Proposition 3.10), there is g in $G_{\mathbb{R}}$ satisfying $g\Theta g^{-1} \subset \mathbf{K}$. That means $x = \mathbf{K}g \in X$ is fixed by the transformations of Θ. Write $x = x_0\gamma$, where $x_0 \in \Omega$, $\gamma \in \Gamma$. Then x_0 is fixed by $\gamma\Theta\gamma^{-1}$, so $x_0 \in \Omega \cap \Omega\delta$ for any δ in $\gamma\Theta\gamma^{-1}$, which means $\gamma\Theta\gamma^{-1} \subset \Delta$. Thus, any finite subgroup of Γ is conjugate to a subgroup contained in the finite set Δ. Q.E.D.

REMARK: Theorem 4.3 can also be proved by using Theorem 4.9 and proceeding as in the proof of Proposition 3.5 (cf. also the proof of Theorem 5.10).

Now we are in a position to prove the invariance of the class of arithmetic subgroups under arbitrary surjective morphisms.

THEOREM 4.1. *Let $\varphi: G \to H$ be a surjective $\mathbb{Q}$-morphism of algebraic groups. If Γ is an arithmetic subgroup of G then $\varphi(\Gamma)$ is an arithmetic subgroup of H.*

PROOF: It suffices to show that $\varphi(G_{\mathbb{Z}})$ is arithmetic in H; moreover, if we choose a suitable realization of H, we may assume that $\varphi(G_{\mathbb{Z}}) \subset H_{\mathbb{Z}}$ (cf. remark following Proposition 4.2). We must prove that $[H_{\mathbb{Z}} : \varphi(G_{\mathbb{Z}})]$ is finite.

First we reduce to the case where G is either reductive or unipotent. Let $G = CU$ be the Levi decomposition of G, where $U = R_u(G)$ is the unipotent radical of G and C is a reductive group. Put $D = \varphi(C)$ and $V = \varphi(U)$; then $H = DV$ is the Levi decomposition of H. If we assume $[D_{\mathbb{Z}} : \varphi(C_{\mathbb{Z}})]$ and $[V_{\mathbb{Z}} : \varphi(U_{\mathbb{Z}})]$ are finite, then by an elementary argument (cf. proof of Lemma 4.7) we can establish the finiteness of $[D_{\mathbb{Z}}V_{\mathbb{Z}} : \varphi(C_{\mathbb{Z}}U_{\mathbb{Z}})]$. By Corollary 2 of Proposition 4.1 $[H_{\mathbb{Z}} : D_{\mathbb{Z}}V_{\mathbb{Z}}]$ is finite; hence $[H_{\mathbb{Z}} : \varphi(C_{\mathbb{Z}}U_{\mathbb{Z}})]$ is finite, and thus $[H_{\mathbb{Z}} : \varphi(G_{\mathbb{Z}})]$ is finite.

Now let G be unipotent. Then $G_{\mathbb{R}}/G_{\mathbb{Z}}$ is compact (Lemma 4.7). Since $H_{\mathbb{R}} = \varphi(G_{\mathbb{R}})$ by Theorem 3.6, Corollary 3, $H_{\mathbb{R}}/\varphi(G_{\mathbb{Z}})$ is compact. On the other hand, $H_{\mathbb{Z}}/\varphi(G_{\mathbb{Z}})$ is closed and discrete in $H_{\mathbb{R}}/\varphi(G_{\mathbb{Z}})$, whence $[H_{\mathbb{Z}} : \varphi(G_{\mathbb{Z}})]$ is finite, as required.

It remains to consider the case where G is reductive. Here we appeal to Theorem 4.9. So, let $H \subset GL_n(\mathbb{C})$. Using the embedding $GL_n(\mathbb{C}) \to GL_{n+1}(\mathbb{C})$ given by $A \mapsto \begin{pmatrix} A & 0 \\ 0 & (\det A)^{-1} \end{pmatrix}$ if necessary, we may assume that H is Zariski-closed in $M_n(\mathbb{C})$. Let us define an action of G on $V = M_n(\mathbb{C})$ by $Ag = A\varphi(g)$, the usual matrix product. Then $H = E_n\varphi(G)$ is a closed orbit of G, and $H_{\mathbb{Z}}$ is the union of a finite number of orbits of $G_{\mathbb{Z}}$, by Theorem 4.9. But, as is easily seen, these orbits are the cosets of $\varphi(G_{\mathbb{Z}})$ in $H_{\mathbb{Z}}$, from which it follows that $[H_{\mathbb{Z}} : \varphi(G_{\mathbb{Z}})]$ is finite. Q.E.D.

The above results represent the first step towards the study of the abstract properties of arithmetic groups. In the chapters that follow we shall present deeper results related, in particular, to the description of normal subgroups of arithmetic groups. Note, however, that they are based on far more intricate machinery.

Before formulating the density theorem we shall specify several classes of semisimple groups with basically different arithmetic properties. (These classes will occur in the statements of many theorems in this book.)

DEFINITION: A $\mathbb{Q}$-algebraic group G is said to have *compact type* if the group of real points $G_{\mathbb{R}}$ is compact. For G semisimple, G has *noncompact type* if $G^i_{\mathbb{R}}$ is noncompact for each $\mathbb{Q}$-simple factor G^i of G. If G has neither of the above types, then G is said to have *mixed type*.

THEOREM 4.10 (DENSITY THEOREM; CF. BOREL [5]). *Suppose G is a semisimple $\mathbb{Q}$-group of noncompact type. Then any arithmetic subgroup $\Gamma \subset G$ is Zariski-dense in G.*

PROOF: Suppose we have proven the theorem for $\mathbb{Q}$-simple groups. Then $\bar{\Gamma} \supset \overline{\Gamma \cap G^i} = G^i$ for each $\mathbb{Q}$-simple factor G^i of G; hence $\bar{\Gamma} \supset \prod_i G^i = G$, as desired. Having reduced the theorem to the case G is $\mathbb{Q}$-simple, we need the following fact, to be verified in the next section:

(4.19) For G a semisimple $\mathbb{Q}$-group, if $G_{\mathbb{R}}$ is noncompact then $G_{\mathbb{Z}}$ is infinite.

(Note that the converse is also true, since if $G_{\mathbb{R}}$ is compact, then $G_{\mathbb{Z}}$, being a discrete subgroup, must be finite.)

Note that if $\Gamma_1 \subset \Gamma_2$ are subgroups of G and $[\Gamma_2 : \Gamma_1]$ is finite, then $[\bar{\Gamma}_2 : \bar{\Gamma}_1]$ is also finite, where $\bar{\Gamma}_i$ denotes the closure of Γ_i. Indeed, if $\Gamma_2 = \bigcup_{i=1}^d \Gamma_1\gamma_i$ then $\bar{\Gamma}_2 = \bigcup_{i=1}^d \bar{\Gamma}_1\gamma_i$, i.e., $[\bar{\Gamma}_2 : \bar{\Gamma}_1] \leq d$. It follows that the connected components $(\bar{\Gamma}_1)^0$ and $(\bar{\Gamma}_2)^0$ coincide. More generally, if Γ_1 and Γ_2 are commensurable, then

$$(\bar{\Gamma}_1)^0 = (\overline{\Gamma_1 \cap \Gamma_2})^0 = (\bar{\Gamma}_2)^0.$$

Now we can complete the proof of the theorem. Without loss of generality we may assume that $\Gamma \subset G_{\mathbb{Z}}$. Then it follows from (4.19) and the above remark that $H = \bar{\Gamma}$ is an algebraic $\mathbb{Q}$-group of positive dimension. For any g in $G_{\mathbb{Q}}$, the group $g\Gamma g^{-1}$ is arithmetic (cf. Proposition 4.1, Corollary 1); thus $g\Gamma g^{-1}$ is commensurable with Γ. Hence $H^0 = (\bar{\Gamma})^0 = (\overline{g\Gamma g^{-1}})^0 = gH^0g^{-1}$. Thus, H^0 is normalized by $G_{\mathbb{Q}}$. Since the normalizer $N_G(H^0)$ is a closed subgroup, and $G_{\mathbb{Q}}$ is dense in G (Theorem 2.2), we see $N_G(H^0) = G$,

i.e., H^0 is a normal subgroup of G. Since G does not have any $\mathbb{Q}$-normal subgroup of positive dimension, we conclude $H^0 = G$. Q.E.D.

REMARK: Although the proof of the Density Theorem presented above uses the fact that Γ is arithmetic, and does not carry over to other types of subgroups of G, the result itself holds in far more general cases. Namely, any closed subgroup $\Gamma \subset G_{\mathbb{R}}$ (in the real topology) for which $G_{\mathbb{R}}/\Gamma$ has finite invariant volume is Zariski dense in G (cf. Raghunathan [5, Ch. 5]). In particular, any lattice $\Gamma \subset G_{\mathbb{R}}$, i.e., any discrete subgroup, for which $G_{\mathbb{R}}/\Gamma$ has finite volume, is Zariski dense. (The fact that an arithmetic subgroup of a semisimple $\mathbb{Q}$-group is a lattice will be established in §4.6.)

We conclude this section with an amusing converse of Corollary 1 of Proposition 4.1. For a semisimple $\mathbb{Q}$-group G and its arithmetic subgroup Γ we define

$$C(\Gamma) = \{\, g \in G : \Gamma \text{ is commensurate with } g^{-1}\Gamma g \,\}$$

(treating G as $G_{\mathbb{C}}$). Since commensurability is an equivalence relation, it is easy to obtain that $C(\Gamma)$ is a subgroup of G, which is called the *commensurability subgroup* of Γ. It should be noted that $C(\Gamma)$ is actually independent of Γ, for the same reason. Since clearly $\Gamma \subset C(\Gamma)$, then $C(\Gamma)$ stands out as the universal repository of all the arithmetic subgroups of G. A description of $C(\Gamma)$ is given by the following:

PROPOSITION 4.6. *Let G be a semisimple algebraic group over $\mathbb{Q}$, let N be its largest invariant $\mathbb{Q}$ subgroup of compact type, and let $\pi: G \to G/N$ be the corresponding projection. Then $C(\Gamma) = \pi^{-1}((G/N)_{\mathbb{Q}})$.*

PROOF: Let $G^1, \ldots, G^r$ be the $\mathbb{Q}$-simple factors of G. Then N is generated by those G^i for which $G^i_{\mathbb{R}}$ is compact and by the centers of the remaining factors. Let H be the normal subgroup generated by those G^i for which $G^i_{\mathbb{R}}$ is noncompact. Clearly $G = H \cdot N$ and $H \cap N$ is finite; i.e., $H \times N \to G$ is isogeneous. Since $H \cap \Gamma$ and $N \cap \Gamma$ are arithmetic in H and N respectively, Theorem 4.1 implies $(H \cap \Gamma)(N \cap \Gamma)$ is arithmetic in G. Since $N_{\mathbb{R}}$ is compact, $N \cap \Gamma$ is finite, so $H \cap \Gamma$ is a subgroup of finite index in Γ. As noted above, it follows that $C(\Gamma) = C(\Gamma \cap H)$. In view of the fact that the restriction of π to H is isogeneous, it is easy to see that $C(\Gamma \cap H)$ is the inverse image under π of the commensurability subgroup of $\pi(\Gamma \cap H)$ in G/N.

Thus, we have reduced the proof to the case $N = \{1\}$; in particular, $Z(G) = \{1\}$. We shall show that in this case $C(\Gamma) = G_{\mathbb{Q}}$. The Zariski closure $\bar{\Gamma}$ is G, by the Density Theorem; moreover, without loss of generality we may assume $\Gamma \subset G_{\mathbb{Z}}$. Fix an embedding $G \subset GL_n(\mathbb{C})$ and let $\mathbb{C}[A]$ denote the $\mathbb{C}$-span of $A \subset G$, i.e. the subspace of $M_n(\mathbb{C})$ spanned by A. Then, since $\bar{\Gamma} = G$, we have $\mathbb{C}[\Gamma] = \mathbb{C}[G]$. Moreover, if $g \in C(\Gamma)$, then

$\Gamma \cap g^{-1}\Gamma g$ has finite index in Γ, and therefore also $\overline{\Gamma \cap g^{-1}\Gamma g} = G$, whence $\mathbb{Q}[\Gamma] = \mathbb{Q}[\Gamma \cap g^{-1}\Gamma g]$. Therefore for any g in $C(\Gamma)$

$$g\mathbb{Q}[\Gamma]g^{-1} = g\mathbb{Q}[\Gamma \cap g^{-1}\Gamma g]g^{-1} = \mathbb{Q}[\Gamma]. \tag{4.20}$$

Consider the adjoint representation $\varrho: G \to GL(V)$ in $V = \mathbb{C}[G]$, given by $\varrho(g)v = gvg^{-1}$. Since $V_{\mathbb{Q}} = \mathbb{Q}[\Gamma]$, (4.20) yields $\varrho(C(\Gamma)) \subset \varrho(G)_{\mathbb{Q}}$. But $Z(G) = \{1\}$ by assumption, so ϱ is faithful and $C(\Gamma) \subset G_{\mathbb{Q}}$. The reverse inclusion is obtained from Corollary 1 of Proposition 4.1. Proposition 4.6 is proved.

It follows from Proposition 4.6 that any arithmetic subgroup of a semisimple adjoint group G of noncompact type must be contained in $G_{\mathbb{Q}}$. On the other hand, if $G = SL_n(\mathbb{C})$, then the subgroup Γ generated by $SL_n(\mathbb{Z})$ and $\begin{pmatrix} s & & 0 \\ & \ddots & \\ 0 & & s \end{pmatrix}$, where s is a primitive n-th root of unity, is an arithmetic subgroup of G. Clearly $\Gamma \not\subset G_{\mathbb{Q}}$, for $n > 2$. Here the commensurability subgroup is

$$\left\{ \frac{1}{(\det A)^{1/n}} A : A \in GL_n(\mathbb{Q}) \right\}.$$

4.5. Compactness of $G_{\mathbb{R}}/G_{\mathbb{Z}}$.

The reduction theory set forth in §§4.2–4.3 has already enabled us to derive several structure theorems on arithmetic groups. We shall use time and again the construction of fundamental sets, discussed there. However, this construction does not enable us to answer all the questions that arise in reduction theory. In particular, it does not give a criterion for $G_{\mathbb{R}}/G_{\mathbb{Z}}$ to be compact, which is important in studying cohomology of arithmetic groups. In the present section we examine this problem, beginning with a look at algebraic tori. It turns out that the general case here reduces to norm tori $S = \mathbf{R}^{(1)}_{K/\mathbb{Q}}(\mathbb{G}_m)$, where K is a finite extension of $\mathbb{Q}$ (cf. §2.1.7 for the definition of a norm torus). Constructing fundamental sets for such tori is equivalent to proving Dirichlet's unit theorem. The method which we shall use is of a fairly general nature and is applicable to other groups, arising from division algebras.

PROPOSITION 4.7. *Let K be a finite field extension of $\mathbb{Q}$, and let $S = \mathbf{R}^{(1)}_{K/\mathbb{Q}}(\mathbb{G}_m)$ be the corresponding norm torus. Then $S_{\mathbb{R}}/S_{\mathbb{Z}}$ is compact.*

PROOF: Put $V = K \otimes_{\mathbb{Q}} \mathbb{R}$ and let N denote the natural extension of the norm map $N_{K/\mathbb{Q}}$ to V. It is well known that for any a in V, $N(a)$ coincides with the determinant of the left translation $x \mapsto ax$ $(x \in V)$. It follows (cf. §3.5) that translations by elements of $S_{\mathbb{R}} = \{\, x \in V : N(x) = 1 \,\}$

preserve the Haar measure μ on the additive group V. Let $\mathcal{O}$ be the ring of integers of K. Then $\mathcal{O}$ is a lattice in V; in particular, $V/\mathcal{O}$ is compact and $\mu(V/\mathcal{O}) < \infty$. Choose a compact subset B of V satisfying $\mu(B) > \mu(V/\mathcal{O})$, and put $C = \{ b_1 - b_2 : b_1, b_2 \in B \}$. If $a \in S_{\mathbb{R}}$, then $\mu(aB) = \mu(a^{-1}B) = \mu(B) > \mu(V/\mathcal{O})$; so the restrictions of the natural map $V \to V/\mathcal{O}$ to aB and $a^{-1}B$ cannot be injective. Consequently, there are $c, d \in C$ such that $\alpha = ac$ and $\beta = a^{-1}d$ lie in $\mathcal{O}$. Then $\alpha\beta = cd \in C^2 \cap \mathcal{O}$. Since this intersection is both compact and discrete, it is finite. We shall need the following straightforward assertion:

LEMMA 4.13. *For any $\gamma \neq 0$ in $\mathcal{O}$, there are only finitely many nonassociate factorizations $\gamma = \alpha\beta$ $(\alpha, \beta \in \mathcal{O})$.*

(Recall that two factorizations $\gamma = \alpha_1\beta_1 = \alpha_2\beta_2$ are said to be associate if there exists a unit $\varepsilon \in \mathcal{O}^*$ such that $\alpha_2 = \varepsilon\alpha_1$ and $\beta_1 = \varepsilon\beta_2$.)

Lemma 4.13 implies that if we consider all the possible factorizations $\gamma = \alpha\beta$ of all elements $\gamma \in C^2 \cap \mathcal{O}$, where $\alpha, \beta \in \mathcal{O}$, then there are only finitely many non-associate possibilities for β. Since the norm of any unit $\varepsilon \in \mathcal{O}^*$ is ± 1, there is a finite number of $\beta_1, \ldots, \beta_r \in \mathcal{O}$ such that any of the β under consideration has the form $\beta = \beta_i\varepsilon$ for suitable $\varepsilon \in \mathcal{O}^* \cap S = S_{\mathbb{Z}}$. On the other hand, by definition $\beta = a^{-1}d$, where $d \in C$. Hence $a = d\beta_i^{-1}\varepsilon^{-1}$, and therefore

$$S_{\mathbb{R}} = \left(\bigcup_{i=1}^{r} (C\beta_i^{-1} \cap S_{\mathbb{R}}) \right) S_{\mathbb{Z}}.$$

Since C is compact, it follows from this decomposition that $S_{\mathbb{R}}/S_{\mathbb{Z}}$ is compact. The proposition is proved.

Dirichlet's unit theorem can be derived easily from Proposition 4.7; however we shall present the appropriate argument somewhat later, after first establishing the compactness criterion of $S_{\mathbb{R}}/S_{\mathbb{Z}}$ for an arbitrary torus S.

THEOREM 4.11. *Let S be an algebraic torus over $\mathbb{Q}$. Then the following conditions are equivalent:*

(1) *S is $\mathbb{Q}$-anisotropic,*
(2) *$S_R/S_{\mathbb{Z}}$ is compact.*

PROOF: 2) $\Rightarrow$ 1). Suppose S were not $\mathbb{Q}$-anisotropic. Then there exists a $\mathbb{Q}$-epimorphism $\varphi: S \to \mathbb{G}_m = T$. Since $\varphi(S_{\mathbb{R}})$ has finite index in $T_{\mathbb{R}}$ (Theorem 3.6, Corollary 3), $T_{\mathbb{R}}/\varphi(S_{\mathbb{Z}})$ must be compact if $S_{\mathbb{R}}/S_{\mathbb{Z}}$ is compact. On the other hand, $\varphi(S_{\mathbb{Z}})$ is an arithmetic subgroup of T (Theorem 4.1) and thus is a finite group, since $T_{\mathbb{Z}} \simeq \mathbb{Z}^* = \{\pm 1\}$. Therefore $T_{\mathbb{R}}/\varphi(S_{\mathbb{Z}})$ cannot be compact, since $T_{\mathbb{R}} \cong R^*$ is not compact.

1) $\Rightarrow$ 2). It is well known (cf. Proposition 2.2) that there exists a $\mathbb{Q}$-epimorphism $\varphi: T \to S$, where T is a quasi-split torus, i.e., has the form $T = \prod_{i=1}^{d} \mathbf{R}_{K_i/\mathbb{Q}}(\mathbb{G}_m)$, where K_i are finite field extensions of $\mathbb{Q}$. Since S is $\mathbb{Q}$-anisotropic, the restriction of φ to $T_0 = \prod_{i=1}^{d} \mathbf{R}^{(1)}_{K_i/\mathbb{Q}}(\mathbb{G}_m)$ is surjective. By Proposition 4.7 $(T_0)_{\mathbb{R}}/(T_0)_{\mathbb{Z}}$ is compact, therefore also $\varphi((T_0)_{\mathbb{R}})/\varphi((T_0))_{\mathbb{Z}}$ is compact. But in view of $[S_{\mathbb{R}} : \varphi((T_0)_{\mathbb{R}})]$ being finite and $\varphi((T_0)_{\mathbb{Z}})$ being arithmetic in S, we conclude that $S_{\mathbb{R}}/S_{\mathbb{Z}}$ is compact. Q.E.D.

COROLLARY 1. *(Dirichlet unit theorem) Let S be an algebraic torus over $\mathbb{Q}$. Then $S_{\mathbb{Z}}$ is isomorphic to the direct product of a finite group and a free abelian group of rank equal to* $\operatorname{rank}_{\mathbb{R}} S - \operatorname{rank}_{\mathbb{Q}} S$.

PROOF: Let S_1 and S_2 respectively be maximal split and maximal $\mathbb{Q}$-anisotropic subtori of S. Since $(S_1)_{\mathbb{Z}}$ is a finite group, applying Theorem 4.1 to the isogeny $S_1 \times S_2 \to S$ we obtain that the index of $(S_2)_{\mathbb{Z}}$ in $S_{\mathbb{Z}}$ is finite. However, $\operatorname{rank}_{\mathbb{R}} S - \operatorname{rank}_{\mathbb{Q}} S = (\operatorname{rank}_{\mathbb{R}} S_1 + \operatorname{rank}_{\mathbb{R}} S_2) - (\operatorname{rank}_{\mathbb{Q}} S_1 + \operatorname{rank}_{\mathbb{Q}} S_2) = \operatorname{rank}_{\mathbb{R}} S_2$, since $\operatorname{rank}_{\mathbb{R}} S_1 = \operatorname{rank}_{\mathbb{Q}} S_1 = \dim S_1$. In view of general results on abelian groups, it suffices to establish that $(S_2)_{\mathbb{Z}}$ is the direct product of a finite group by $\mathbb{Z}^r$, where $r = \operatorname{rank}_{\mathbb{R}} S_2$.

Thus, we have reduced the proof to the case S is a $\mathbb{Q}$-anisotropic torus. It follows from the discussion in §2.2.4 that any torus over $\mathbb{R}$ is isomorphic to the product of copies of $\mathbb{G}_m$, $\mathbf{R}_{\mathbb{C}/\mathbb{R}}(\mathbb{G}_m)$ and $\mathbf{R}^{(1)}_{\mathbb{C}/\mathbb{R}}(\mathbb{G}_m)$. Hence there exists an isomorphism $S_{\mathbb{R}} \simeq \mathbb{R}^r \times D$, where $r = \operatorname{rank}_{\mathbb{R}} S$ and D is a compact group. On the other hand, $S_{\mathbb{R}}/S_{\mathbb{Z}}$ is compact, by Theorem 4.11. Therefore our assertion follows from the following well-known fact, which, in view of subsequent applications, we state in a form somewhat more general than necessary to prove the corollary.

LEMMA 4.14. *Let T be an abelian topological group of the form $\mathbb{Z}^a \times \mathbb{R}^b \times D$, where D is a compact group. Then any discrete subgroup Γ of G, such that G/Γ is compact, is isomorphic to $\mathbb{Z}^{a+b} \times F$ for a suitable finite group F.*

PROOF: Reduces easily to the case $G = \mathbb{R}^n$, which is handled in Bourbaki [2, Ch. 7, §1, ¶ 1].

Now take S to be the torus $\mathbf{R}_{K/\mathbb{Q}}(\mathbb{G}_m)$, where K is a finite field extension of $\mathbb{Q}$. Over $\mathbb{R}$ we have $S \simeq \mathbb{G}_m^s \times \mathbf{R}_{\mathbb{C}/\mathbb{R}}(\mathbb{G}_m)^t$, where s and t are the numbers of real valuations and pairwise nonconjugate complex valuations of K, respectively; so $\operatorname{rank}_{\mathbb{R}} S = s + t$. But $\operatorname{rank}_{\mathbb{Q}} S = 1$ and therefore we obtain the classic statement of Dirichlet's unit theorem:

$$U(K) \simeq F \times \mathbb{Z}^{s+t-1},$$

where F is the group of all roots of unity in K. In the next chapter we shall generalize this result for S-units.

Also we can prove the assertion which we used in the previous section.

COROLLARY 2. *Let G be a semisimple $\mathbb{Q}$-group. Then $G_{\mathbb{Z}}$ is infinite if and only if $G_{\mathbb{R}}$ is noncompact.*

PROOF: If $G_{\mathbb{R}}$ is compact, then $G_{\mathbb{Z}}$ is a discrete subgroup of a compact group, and consequently is finite.

To prove the converse, suppose $G_{\mathbb{R}}$ is noncompact. If G is isotropic over $\mathbb{Q}$, then there is a one-dimensional unipotent $\mathbb{Q}$-subgroup U of G, so $U_{\mathbb{Z}}$ is infinite and we are done. Now let G be $\mathbb{Q}$-anisotropic. Since $G_{\mathbb{R}}$ is noncompact, i.e., $\mathbb{R}$-isotropic, there exists a maximal $\mathbb{R}$-defined $\mathbb{R}$-isotropic torus $T \subset G$. By Proposition 7.3, Corollary 3, there is a maximal $\mathbb{Q}$-torus $S \subset G$ which is also isotropic over $\mathbb{R}$. (The proof of that assertion follows from the rationality of maximal toric varieties and does not depend on any results from this chapter.) But then by Corollary 1, $S_{\mathbb{Z}}$ is infinite.

Another proof of Corollary 2 may be found in the next section.

The conditions in Theorem 4.11 (that $S_{\mathbb{R}}/S_{\mathbb{Z}}$ be compact and that S be $\mathbb{Q}$-anisotropic) are actually equivalent for arbitrary algebraic groups, as is shown by the following theorem.

THEOREM 4.12. *Let G be an algebraic group defined over $\mathbb{Q}$. Then the following conditions are equivalent:*

(1) *$G_{\mathbb{R}}/G_{\mathbb{Z}}$ is compact;*
(2) *the reductive part of the connected component of G is anisotropic over $\mathbb{Q}$.*

(Note that (2) may also be formulated as $\mathbf{X}(G^0)_{\mathbb{Q}} = \{1\}$ and each unipotent element of $G_{\mathbb{Q}}$ belongs to the unipotent radical of G.)

PROOF: It suffices to consider the case G connected; let $G = HR_u(G)$ be its Levi decomposition. Then $G_{\mathbb{R}}/G_{\mathbb{Z}}$ being compact is equivalent to $H_{\mathbb{R}}/H_{\mathbb{Z}}$ being compact. The latter assertion follows from Lemma 4.7 combined with

LEMMA 4.15. *Let H be a reductive subgroup of a connected group G, where G and H are defined over $\mathbb{Q}$. Then $H_{\mathbb{R}}/H_{\mathbb{Z}}$ is closed in $G_{\mathbb{R}}/G_{\mathbb{Z}}$.*

PROOF: By the stronger version of Chevalley's theorem, there is a $\mathbb{Q}$-representation $\varrho: G \to GL(V)$ and a vector v in $V_{\mathbb{Q}}$ such that the stabilizer of v under ϱ is H. Thus $W = v\varrho(G_{\mathbb{Z}})$ is contained in a lattice in $V_{\mathbb{Q}}$ (cf. remark following Proposition 4.2), and as a result is closed in $V_{\mathbb{R}}$. Therefore $H_{\mathbb{R}}G_{\mathbb{Z}} = G_{\mathbb{R}} \cap \varrho^{-1}(W)$ is also closed in $G_{\mathbb{R}}$. The lemma is proved.

Thus, it suffices to consider the case where G is reductive. In this case 1) $\Rightarrow$ 2) follows easily from Lemma 4.15. Indeed, if G is $\mathbb{Q}$-isotropic, then it contains a nontrivial $\mathbb{Q}$-split tori S. Then $S_{\mathbb{R}}/S_Z$ is noncompact (cf. Theorem 4.11) and is closed in $G_{\mathbb{R}}/G_{\mathbb{Z}}$; so the latter cannot be compact either.

To prove 2) $\Rightarrow$ 1) we first reduce the problem to the case of a semisimple adjoint group. Let $Z = Z(G)$, the center of G. Then its connected component S is a $\mathbb{Q}$-anisotropic torus, and therefore $S_{\mathbb{R}}/S_{\mathbb{Z}}$ is compact (Theorem 4.11). Since $[Z_{\mathbb{R}} : S_{\mathbb{R}}]$ is finite, $Z_{\mathbb{R}}/Z_{\mathbb{Z}}$ also is compact.

Put $H = G/Z$ and let π denote the canonical projection of G on H. Consider, moreover, the map $\varphi: G_{\mathbb{R}}/G_{\mathbb{Z}} \to \pi(G_{\mathbb{R}})/\pi(G_{\mathbb{Z}})$ induced by π. The compact group $B = Z_{\mathbb{R}}/Z_{\mathbb{Z}}$ acts by translation on $G_{\mathbb{R}}/G_{\mathbb{Z}}$, and it is easy to see that the orbits of B are precisely the fibers of φ. It follows easily that φ is proper. In view of the fact that $[H_{\mathbb{R}} : \pi(G_{\mathbb{R}})]$ is finite and $\varphi(G_{\mathbb{Z}})$ is arithmetic, we see that the compactness of $G_{\mathbb{R}}/G_{\mathbb{Z}}$ is equivalent to the compactness of $H_{\mathbb{R}}/H_{\mathbb{Z}}$. We shall actually prove the latter, but first let us establish a criterion for compactness of a subset of $GL_n(\mathbb{R})/GL_n(\mathbb{Z})$.

PROPOSITION 4.8 (MAHLER'S CRITERION). *A subset $\Omega \subset GL_n(\mathbb{R})$ is relatively compact modulo $GL_n(\mathbb{Z})$ if and only if*

a) *$\det g$ is bounded for all g in Ω,*
b) *$\Omega(\mathbb{Z}^n \setminus \{0\}) \cap U = \emptyset$ for U a suitable a neighborhood of zero in $\mathbb{R}^n$.*

PROOF: If the image of Ω in $GL_n(\mathbb{R})/GL_n(\mathbb{Z})$ is relatively compact, then there is a compact $D \subset GL_n(\mathbb{R})$ such that $\Omega \subset D \cdot GL_n(\mathbb{Z})$. It clearly follows that $\det g$ is bounded for all g in Ω. Furthermore,

$$\Omega(\mathbb{Z}^n \setminus \{0\}) \subset (D \cdot GL_n(\mathbb{Z}))(\mathbb{Z}^n \setminus \{0\}) = D(\mathbb{Z}^n \setminus \{0\});$$

since $\mathbb{Z}^n$ is discrete and D is compact, the right hand side is closed in $\mathbb{R}^n$ and does not contain zero, from which one obtains the required neighborhood U.

Conversely, assume conditions a) and b) hold, and let $\Sigma = \Sigma_{t,v}$ (for $t \geq \frac{2}{\sqrt{3}}$, $v \geq \frac{1}{2}$) be a Siegel set of $GL_n(\mathbb{R})$. We know (Theorem 4.4) that $\Sigma \cdot GL_n(\mathbb{Z}) = GL_n(\mathbb{R})$; therefore there is a subset $\Theta \subset \Sigma$ such that $\Theta GL_n(\mathbb{Z}) = \Omega GL_n(\mathbb{Z})$. Hence, $\Omega(\mathbb{Z}^n \setminus \{0\}) = \Theta(\mathbb{Z}^n \setminus \{0\})$, so that a) and b) also hold for Θ, and it suffices to establish the relative compactness of Θ.

Note that b) means there is $c > 0$ such that $\|g(x)\| \geq c$ for all g in Θ and all x in $\mathbb{Z}^n \setminus \{0\}$, where $\| \ \|$ is the Euclidean norm in $\mathbb{R}^n$. In particular, $\|g(e_1)\| = \|a_g(e_1)\| = a_1 \geq c$, in the notation of §4.2 where $g = k_g a_g u_g$ is the Iwasawa decomposition of g in Θ, and $e_1, \ldots, e_n$ is a fixed orthonormal

base of $\mathbb{R}^n$. Since $a_g \in A_t$, we see that $a_i \geq s a_1$ for all $i = 1, \ldots, n$ and some $s > 0$, and thus all a_i are bounded from below. On the other hand, $|\det g| = |\det a_g| = a_1 \ldots a_n$ is bounded from above; therefore all a_i are also bounded from above. Thus we have shown that the a-components a_g of the elements g in Θ form a relatively compact set. Since $\Theta \subset \Sigma$, it follows that Θ is relatively compact. The lemma is proved.

Now we have all the results needed to prove that $H_{\mathbb{R}}/H_{\mathbb{Z}}$ is compact. Consider the Lie algebra $\mathfrak{h} = L(H)$ and the adjoint representation $\varrho: H \to GL(\mathfrak{h})$. Without loss of generality we may assume that

$$H_{\mathbb{Z}} = \{ h \in H : \varrho(h)L = L \},$$

for a lattice $L \subset \mathfrak{h}_{\mathbb{Q}}$. In view of Lemma 4.15, it suffices to prove that $H_{\mathbb{R}}$ is relatively compact modulo $GL_n(\mathbb{Z})$ $(n = \dim \mathfrak{h})$, where $GL_n(\mathbb{Z})$ is taken relative to some base of L. We can apply Mahler's criteria. Since $\det \varrho(H) = 1$, we only need check condition b). Consider the characteristic polynomial

$$\det(t - \operatorname{ad} x) = t^n + \sum_{i=0}^{n-1} f_i(x) t^i,$$

corresponding to the adjoint action of x in L. Since H is $\mathbb{Q}$-anisotropic, $\mathfrak{h}_{\mathbb{Q}}$ does not contain nilpotent elements, and consequently the $f_i(x)$ cannot vanish simultaneously, i.e. $f(x) = \sum f_i^2(x) > 0$. On the other hand, the f_i are polynomials with rational coefficients of the coordinates of x with respect to a base of L. Therefore $f(x) = \frac{1}{d} g(x)$, where $d \in \mathbb{Z}$ and $g(x)$ is a polynomial with integral coefficients. Since $g(x) \neq 0$ for x in $L \setminus \{0\}$, we have $|f(L \setminus \{0\})| \geq \frac{1}{d}$. But $f_i(x) = f_i(hx)$ for any h in H; hence for any h in $H_{\mathbb{R}}$

$$|f(h(L \setminus \{0\}))| = |f(L \setminus \{0\})| \geq \frac{1}{d}.$$

Thus $|f(x)| < \frac{1}{d}$ defines the required neighborhood U. This completes the proof of Theorem 4.12.

Let us give two examples.

EXAMPLE 1: Let $G = \mathbf{SO}_n(f)$, the special orthogonal group of a nondegenerate quadratic form f in n variables with rational coefficients. Then G is a one-dimensional torus for $n = 2$, and is semisimple for $n \geq 3$ (cf. §2.3). Moreover, by Proposition 2.14, G is $\mathbb{Q}$-anisotropic if and only if f is anisotropic. Thus, Theorem 4.12 gives the following compactness criterion:

$SO_n(f)_{\mathbb{R}}/SO_n(f)_{\mathbb{Z}}$ is compact if and only if
f does not represent zero over $\mathbb{Q}$.

It is interesting to compare our proof of this result with the proof in terms of reduction theory of quadratic forms (cf. Böge [1], Cassels [1]; the adelic version of the argument may be found in Godement [1]).

EXAMPLE 2: Let $G = SL_1(D)$, where D is a finite-dimensional skew field over $\mathbb{Q}$. By Proposition 2.12, G is $\mathbb{Q}$-anisotropic; therefore $G_{\mathbb{R}}/G_{\mathbb{Z}}$ is compact. This result is due to Hey, and its adelic variant to Fudzisaka.

4.6. The finiteness of the volume of $G_{\mathbb{R}}/G_{\mathbb{Z}}$.

Several important structural results on arithmetic groups (cf., in particular, Margulis [2],[3]), rely heavily on the fact that an arithmetic subgroup of a semisimple group G is a lattice in $G_{\mathbb{R}}$, i.e., the volume of $G_{\mathbb{R}}/G_{\mathbb{Z}}$ with respect to the Haar measure is finite. Hardly any commentary is necessary about the significance of this result for developing the analysis of $G_{\mathbb{R}}/G_{\mathbb{Z}}$, in particular, the theory of automorphic functions (cf., for example, Borel [6]). The object of this section is to give a criterion for $G_{\mathbb{R}}/G_{\mathbb{Z}}$ to have finite volume, for arbitrary algebraic groups.

THEOREM 4.13. *Let G be an algebraic $\mathbb{Q}$-group. $G_{\mathbb{R}}/G_{\mathbb{Z}}$ has finite invariant volume if and only if the connected component G^0 does not have non-trivial characters defined over $\mathbb{Q}$.*

This is the most technically intricate result in the entire chapter. The reader who does not wish to labor through all the details of the proof may confine himself to the case $G = \mathbf{SL}_n$. Here, by the corollary to Theorem 4.4, $G_{\mathbb{R}} = \Sigma_{t,v}^{(1)} G_{\mathbb{Z}}$ (for any $t \geq \frac{2}{\sqrt{3}}$, $v \geq \frac{1}{2}$), where $\Sigma_{t,v}$ is a Siegel set of $GL_n(\mathbb{R})$ and $\Sigma_{t,v}^{(1)} = \Sigma_{t,v} \cap G_{\mathbb{R}}$. Since $G_{\mathbb{R}}$ is unimodular (by the corollary to Theorem 3.18), $G_{\mathbb{R}}/G_{\mathbb{Z}}$ carries an invariant measure, and therefore it suffices to establish that $\Sigma_{t,v}^{(1)}$ has finite volume. To do so we shall use an expression for the Haar measure dg of G which follows from the results of §3.5:

$$dg = \varrho(a) dk\, da\, du,$$

where k, a, u are the Iwasawa components of g, and dk, da, and du are the Haar measures on the groups $\mathbf{K}_0 = \mathbf{SO}_n(\mathbb{R})$, $A_0 = A \cap G$, and U, respectively (cf. §4.2 for notation concerning the Iwasawa decomposition); $\varrho(a) = \prod_{i<j} a_i/a_j$ where $a = \operatorname{diag}(a_1, \ldots, a_n)$. We have

$$\int_{\Sigma_{t,v}^{(1)}} dg = \int_{K_0} dk \int_{(A_0)_t} \varrho(a) da \int_{U_v} du, \text{ where } (A_0)_t = A_t \cap G.$$

The first and third integrals on the right hand side are finite by virtue of the compactness of the corresponding domains of integration. Let us show

that the second integral is finite. First of all, we note that via the map

$$\mathrm{diag}(a_1, \dots, a_n) \mapsto (\frac{a_1}{a_2}, \frac{a_2}{a_3}, \dots, \frac{a_{n-1}}{a_n})$$

A_0 is identified with the group $(\mathbb{R}^{>0})^{n-1}$, and $(A_0)_t$ is sent to

$$\{ (x_1, \dots, x_{n-1}) \in (\mathbb{R}^{>0})^{n-1} : x_i \leq t \text{ for all } i \}.$$

Furthermore, we can write ϱ in terms of the coordinates $x_1, \dots, x_n$ as

$$\varrho(a) = \prod_{i=1}^{n-1} x_i^{r_i},$$

where the r_i are positive integers. Since the (multiplicative) Haar measure on $\mathbb{R}^{>0}$ is $\frac{dx}{x}$, we have

$$\int_{(A_0)_t} \varrho(a) da = \int_0^t \dots \int_0^t \prod_{i=1}^{n-1} x_i^{r_i} \frac{dx_1}{x_1} \dots \frac{dx_{n-1}}{x_{n-1}} = \prod_{i=1}^{n-1} \int_0^t x_i^{r_i - 1} dx_i,$$

and each integral $\int_0^t x^{r-1} dx = \frac{1}{r} t^r$ is finite for $r > 0$. Q.E.D.

Broadly speaking, the situation for an arbitrary semisimple group G is similar. Namely, since $G_{\mathbb{R}}$ is unimodular (by the corollary to Theorem 3.18), $G_{\mathbb{R}}/G_{\mathbb{Z}}$ carries an invariant measure; and to prove that the corresponding volume of $G_{\mathbb{R}}/G_{\mathbb{Z}}$ is finite, it suffices to find a measurable subset of $G_{\mathbb{R}}$ which covers $G_{\mathbb{R}}/G_{\mathbb{Z}}$ and has finite volume. We show first that the fundamental set in $G_{\mathbb{R}}$ relative to $G_{\mathbb{Z}}$ constructed in §4.3 is actually contained in the union of a finite number of translations of a suitable Siegel set in $G_{\mathbb{R}}$, and then we establish that any Siegel set has finite volume. (This part of the argument hardly differs from the case of $\mathbf{SL}_n$.)

So, let $G \subset GL_n(\mathbb{C})$ be a semisimple $\mathbb{Q}$-group. In §4.3 we showed that for a fundamental set in $G_{\mathbb{R}}$ relative to $G_{\mathbb{Z}}$ we can take a set of the form

$$\Omega = \left(\bigcup_b a \Sigma b \right) \cap G_{\mathbb{R}},$$

where Σ is a Siegel set in $GL_n(\mathbb{R})$, b runs through a finite set of matrices from $GL_n(\mathbb{Z})$, and $a \in GL_n(\mathbb{R})$ is such that $H = a^{-1} G a$ is self-conjugate. To prove Theorem 4.13 our choice of a must be subject to stricter constraints, namely it should satisfy all the conditions listed in Proposition 3.14. Below we shall use the notation introduced there. In particular, let $S = H \cap D_n$ be a maximal $\mathbb{R}$-split torus of H and $U = H \cap U_n$ a maximal unipotent subgroup. Also, let R denote the root system of H relative to S, and let $\Pi \subset R$ be the system of simple roots corresponding to U. Since $a^{-1}(a \Sigma b \cap G_{\mathbb{R}}) a = \Sigma b a \cap H_{\mathbb{R}}$, the finiteness of the volume of Ω follows from

PROPOSITION 4.9. *$\Sigma x \cap H_{\mathbb{R}}$ has finite volume in the Haar measure of $H_{\mathbb{R}}$, for any Siegel set $\Sigma \subset GL_n(\mathbb{R})$ and any x in $GL_n(\mathbb{R})$.*

The proof is based on the construction of relative Siegel sets for H. Let $H_{\mathbb{R}} = \mathbf{K}^* A^* U^*$ be the Iwasawa decomposition of $H_{\mathbb{R}}$ (cf. Theorem 3.9), in which $\mathbf{K}^*$ is a maximal compact subgroup of $H_{\mathbb{R}}$, A^* is the connected component of $S_{\mathbb{R}}$, and $U^* = U_{\mathbb{R}}$. A *Siegel set* $\Sigma^*_{t,\omega}$ in $H_{\mathbb{R}}$ (where $t > 0$, $\omega \subset U^*$ is a compact subset) is the product $\mathbf{K}^* A^*_t \omega$, where

$$A^*_t = \{ a \in A^* : \alpha(a) \leq t \text{ for all } \alpha \in \Pi \}.$$

Clearly, for $G = \mathbf{SL}_n$ a relative Siegel set amounts to some intersection $G \cap \Sigma$, where Σ is a suitable Siegel set in $GL_n(\mathbb{R})$. An easy argument shows that under our conditions the same statement also holds for H. Indeed, let $h \in \Sigma_{t,v} \cap H$. Then the Iwasawa decompositions of h in $H_{\mathbb{R}}$ and in $GL_n(\mathbb{R})$ coincide. Since condition (iii) of Proposition 3.14 is satisfied, the simple roots of H are of the form $\alpha = d_1 \varepsilon_1 + \dots + d_{n-1} \varepsilon_{n-1}$, where $d_i \geq 0$ and the ε_i are simple roots of $GL_n(\mathbb{C})$. Therefore we can find a constant $s > 0$ such that $\alpha(a_h) \leq s$ for all h in $\Sigma_{t,v} \cap H_{\mathbb{R}}$ and all α in Π; then $\Sigma_{t,v} \cap H_{\mathbb{R}} \subset \Sigma^*_{s,\omega}$, where $\omega = (U_{n\mathbb{R}})_v \cap H_{\mathbb{R}}$. A similar argument also proves the converse (although we shall not need it): any Siegel set of H is contained in a suitable Siegel set of $GL_n(\mathbb{R})$. Proving the analogous assertion for translations of Siegel sets is the most technical and intricate step in the proof of Proposition 4.9.

PROPOSITION 4.10. *Let Σ be a Siegel set of $GL_n(\mathbb{R})$, and let $x \in GL_n(\mathbb{R})$. Then there is a Siegel set $\Sigma^* \subset H_{\mathbb{R}}$ and a finite set of elements $x_i \in H_{\mathbb{R}}$ such that*

$$\Sigma x \cap H_{\mathbb{R}} \subset \bigcup_i \Sigma^* x_i.$$

Given this result, to prove Proposition 4.9 we have only to prove

PROPOSITION 4.11. *The volume of any Siegel set $\Sigma^* = \Sigma^*_{t,\omega}$ under the Haar measure of $H_{\mathbb{R}}$ is finite.*

PROOF OF PROPOSITION 4.11: Relies on the formula for the Haar measure of $H_{\mathbb{R}}$, which is analogous to the formula for $SL_n(\mathbb{R})$ and also can be obtained from the results of §3.5:

$$dh = \varrho(a) dk^* da^* du^*,$$

where dk^*, da^* and du^* are the Haar measures on $\mathbf{K}^*$, A^* and U^*, respectively, and ϱ is the sum of the positive roots of R. As in the case of $SL_n(\mathbb{R})$, we have

$$\int_{\Sigma^*} dh = \int_{\mathbf{K}^*} dk^* \int_{A^*_t} \varrho(a) da^* \int_{\omega} du^*;$$

since the first and third integrals are taken over compact sets, they are finite. To compute the second integral let us consider the map $\varphi: A^* \to (\mathbb{R}^{>0})^d$ for $d = |\Pi|$, given by $\varphi(a) = (\alpha(a))_{\alpha\in\Pi}$. It is easy to see that φ is a group isomorphism; in addition

$$\varphi(A_t^*) = \{\,(x_1,\dots,x_d) \in (\mathbb{R}^{>0})^d : x_i \le t\,\}.$$

Moreover, $\varrho = \Sigma b_\alpha \alpha$ for positive integers b_α. Therefore we have

$$\int_{A_t^*} \varrho(a)da = \prod_{\alpha\in\Pi}\int_0^t x^{b_\alpha - 1}dx = \left(\prod_{\alpha\in\Pi} b_\alpha^{-1}\right) t^{\Sigma b_\alpha} < \infty.$$

The proposition is proved.

Before proving Proposition 4.10 we must first establish an auxiliary assertion on translations of Siegel sets in $GL_n(\mathbb{R})$.

LEMMA 4.16. *Let Σ be a Siegel set of $GL_n(\mathbb{R})$ and let $x \in GL_n(\mathbb{R})$. Then for any $s > 0$, $\Sigma x \cap \mathbf{K}A_sU_{n\mathbb{R}}$ is contained in a Siegel set of $GL_n(\mathbb{R})$.*

The proof does not involve H and its subgroups; therefore, in order not to complicate the notation, we shall return to the notation used in §4.2. In particular, instead of $U_{n\mathbb{R}}$ we shall write simply U, and let $B = AU$. Clearly, for any b in B, Σb and $(\mathbf{K}A_sU)b$ are contained respectively in a suitable Siegel set and in a set of the form $\mathbf{K}A_sU$. Since any x in $GL_n(\mathbb{R})$ has a Bruhat decomposition $x = v_x^- w b_x$ ($v_x^- \in U$, $b_x \in B$, $w \in W$), it suffices to prove the lemma for $x = w \in W$. Let π be the permutation of $\{1,\dots,n\}$ corresponding to w. Put $I = \{\,(i,j) : i < j$, and $\pi i > \pi j\,\}$, and let S denote the torus $\{\,x = \mathrm{diag}(x_1,\dots,x_n) : x_i = x_j$ for all $(i,j) \in I\,\}$. Let F be the commutator group of the centralizer $C_{GL_n}(S)$, let $T = D_n \cap F$, and let $U' = U \cap F$. Also put $A' = (T_{\mathbb{R}})^0$, $A'' = (S_{\mathbb{R}})^0$, $U'' = \{\,u = (u_{ij}) \in U : u_{ij} = 0$ for all $(i,j) \in I\,\}$. We shall need the following simple fact, whose proof is left as an exercise for the reader: the product morphism induces an isomorphism $A' \times A'' \simeq A$ and a homeomorphism $U' \times U'' \simeq U$. Let δ' and δ'' denote the projections of A on A' and A'' respectively.

LEMMA 4.17

(1) *w centralizes S;*
(2) *the set $\delta'(wA_tw^{-1} \cap A_s)$ is compact for any s, $t > 0$.*

PROOF: 1) Let $\{1,\dots,n\} = J_1 \cup \cdots \cup J_r$ be the partitioning into disjoint orbits under π. The set of elements of D_n commuting with w is $\{\,x = \mathrm{diag}(x_1,\dots,x_n) : x_i = x_j$ if i, j lie in the same orbit$\,\}$. Now let $x = \mathrm{diag}(a_1,\dots,a_n) \in S$ and let J be an arbitrary orbit. If $|J| = l$, then without loss of generality we may assume that $J = \{1,\dots,l\}$. Take $f \le l$ such that $a_1 = \cdots = a_{f-1}$, but $a_f \ne a_{f-1}$. Since the subsets $\{\,j \in J : j < f\,\}$ and $\{\,j \in J : j > f\,\}$ can not be invariant under π, we can find j, $k \in J$ such that $j < f < k$ and $\pi k \le f \le \pi j$; in addition $\pi k < \pi j$. Clearly $(j,k) \in I$; therefore $a_j = a_k$, by definition of S. If $\pi(f) > \pi(k)$, then $(f,k) \in I$, whence $a_f = a_k = a_j$; if $\pi(f) \le \pi(k) < \pi(j)$, then $(j,f) \in I$ and again $a_f = a_j$. Thus, in all cases $a_f = a_j$, contradicting our assumption, since $j < f$.

2) Since A' and A'' are invariant under w, we see that $\delta'(wA_tw^{-1} \cap A_s) = w\delta'(A_t \cap w^{-1}A_sw)w^{-1}$; thus we only need to establish that $\delta'(A_t \cap w^{-1}A_sw)$ is bounded. To do so, consider $\varphi: A \to (\mathbb{R}^{>0})^d$, for $d = |I|$, given by

$$\varphi(\mathrm{diag}(a_1,\dots,a_n)) = \left(\frac{a_i}{a_j}\right)_{(i,j)\in I}.$$

Clearly $\ker\varphi = A''$, so $\varphi|_{A'}$ gives an isomorphism $A' \simeq \varphi(A')$. Therefore it suffices to show that $\Phi = \varphi(A_t \cap w^{-1}A_sw)$ is relatively compact. There are constants t_0, $s_0 > 0$ such that $\frac{a_i}{a_j} \le t_0$ (resp., s_0) for all $i < j$ and all $a = \mathrm{diag}(a_1,\dots,a_n) \in A_t$ (resp., A_s). We claim that $\Phi \subset [s_0^{-1}, t_0^{-1}]^d$. Indeed, by our construction $\varphi(A_t) \subset [-\infty, t_0]^d$. But if $a \in w^{-1}A_sw$, then $waw^{-1} = \mathrm{diag}(a_{\pi^{-1}(1)},\dots,a_{\pi^{-1}(u)}) \in A_t$. Let $(i,j) \in I$, $i' = \pi(i)$, and $j' = \pi(j)$. Then $i' > j'$, which means $\frac{a_i}{a_j} = \frac{a_{\pi^{-1}(i')}}{a_{\pi^{-1}(j')}} \ge s_0^{-1}$, as desired, completing the proof of Lemma 4.17.

Now we shall complete the proof of Lemma 4.16. We note at once that the proof only requires the boundedness of the u-component of the elements of $\Sigma w \cap \mathbf{K}A_sU$. Let $g = kau \in \Sigma$. We shall compute the a-component of gw. Put $m = aua^{-1}w$ and let $m = k_m a_m u_m$ be the corresponding Iwasawa decomposition. Then we have

$$gw = kauw = kmw^{-1}aw = (kk_m)a_mu_mw^{-1}aw.$$

Since $w^{-1}aw$ normalizes U, we may equate the a-components to obtain

$$a_{kauw} = a_{aua^{-1}w}w^{-1}aw. \tag{4.21}$$

Now let gw run through $\Sigma w \cap \mathbf{K}A_sU$. Then it follows from Lemma 4.3 that the $a_{aua^{-1}w}$ constitute a relatively compact set. Since $a_{gw} \in A_s$, it follows from (4.21) that $w^{-1}aw \in A_{s'}$ for sufficiently large s'. Applying the second assertion of Lemma 4.17, we obtain that the $\delta'(a)$ are bounded. Let $u = u'u''$, where $u' \in U'$, $u'' \in U''$. Then we have

$$gw = k\delta'(a)\delta''(a)u'u''w = (kw)(w^{-1}\delta'(a)u'w)\delta''(a)w^{-1}u''w.$$

Note that $w^{-1}Fw = F$ since $F = [C_{GL_n}(S), C_{GL_n}(S)]$ and w centralizes with S; hence $h = w^{-1}\delta'(a)u'w \in F_{\mathbb{R}}$. Then the components of the Iwasawa decomposition $h = k_h a_h u_h$ also lie in $F_{\mathbb{R}}$. Indeed, it is easy to verify that if $c = \operatorname{diag}(\varepsilon_1, \dots, \varepsilon_n)$, where $\varepsilon_i = \pm 1$, and if Z_c is the centralizer of c in GL_n and $h \in (Z_c)_{\mathbb{R}}$, then the components of the Iwasawa decomposition of h also lie in $(Z_c)_{\mathbb{R}}$. On the other hand, F can be written as $\bigcap_c Z_c$, where c runs through a suitable set of elements of this form. Taking this into account, we can continue the completions:

$$gw = (kw)h\delta''(a)w^{-1}u''w = (kwk_h)(a_h\delta''(a))(u_h w^{-1}u''w).$$

It follows from the above that h runs through a relatively compact set; therefore its components, in particular the u_h, also run through relatively compact sets. The component u'' is also bounded, since $g \in \Sigma$. It follows that $u_h w^{-1}u''w$ is bounded. It remains to note that as follows from the definition of U'' we have the inclusion $w^{-1}U''w \subset U$; so $u_h w^{-1}u''w$ is exactly the u-component of gw. The lemma is proved.

We also need to generalize the following remark to apply to an arbitrary group. Let $a \in A$; then for a suitable w in W we have $w^{-1}aw \in A_1$ $(= A_t$ for $t = 1)$. In other words

$$A = \bigcup_{w \in W} (w^{-1}A_1 w).$$

Indeed, let $a = \operatorname{diag}(a_1, \dots, a_n)$. We can order a_i: $a_{i_1} \leq \dots \leq a_{i_n}$. Let π denote the transposition $\begin{pmatrix} 1 & \dots & n \\ i_1 & \dots & i_n \end{pmatrix}$ and let w be the corresponding element of W. Then

$$w^{-1}aw = \operatorname{diag}(a_{i_1}, \dots, a_{i_n}) \in A_1.$$

To generalize this to H (at this point we return to the notation introduced in the beginning of this section), recall that the relative Weyl group W^* of H is defined as $N_H(S)/C_H(S)$, where $N_H(S)$ (resp., $C_H(S)$) is the normalizer (resp., centralizer) of S in H; moreover, representatives of all the classes of W^* can be taken from $N_H(S)_{\mathbb{R}}$, so that actually $W^* = N_H(S)_{\mathbb{R}}/C_H(S)_{\mathbb{R}}$. Also note that W^* naturally acts on S by conjugation.

LEMMA 4.18.

(1) *Representatives of all the classes of W^* can be taken from the maximal compact subgroup $\mathbf{K}^*$.*
(2) $A^* = \bigcup_{w \in W^*} w^{-1}A_1^* w$.

PROOF: 1) Let $x \in N_H(S)_{\mathbb{R}}$ and let $x = kau \in \mathbf{K}^*A^*U^*$ be its Iwasawa decomposition. Then for any b in S we have

$$k^{-1}bk = (au)\bar{b}(au)^{-1},$$

where $\bar{b} = x^{-1}bx \in S$. But $k^{-1} = {}^tk$, so $k^{-1}bk = {}^tkbk$ is a symmetric matrix. On the other hand, $(au)\bar{b}(au)^{-1}$ is an upper triangular matrix. Therefore $(au)\bar{b}(au)^{-1}$ is actually a diagonal matrix and $au \in N_H(S)$. Since the centralizer of any torus in a connected solvable group coincides with its normalizer (cf. Borel [8]), in fact $au \in C_H(S)$. It follows that x and k represent the same class in W^*.

2) Let $a \in A^*$. Put $P = \{\alpha \in R : \alpha(a) \geq 1\}$. It is easy to see that if $\alpha, \beta \in P$ and $\alpha + \beta \in R$, then $\alpha + \beta \in P$ and, moreover, $P \cup (-P) = R$. Thus, in the terminology of Bourbaki [4] (cf. Ch. 4, §1.7), P is a parabolic set and therefore contains some system of simple roots Π' of R. Since W^* is naturally isomorphic to $W(R)$, and the latter acts simply transitively on systems of simple roots, then there is a $\tilde{w}$ in $W(R)$ such that $\tilde{w}\Pi' = \Pi$; hence $\tilde{w}P \supset \Pi$. Then, if w is an element of W^* corresponding to $\tilde{w}$, we have $\alpha(w^{-1}aw) \leq 1$ for all α in Π, i.e., $w^{-1}aw \in A_1$. Lemma 4.18 is proved.

The argument continues as follows: let $y = zx \in \Sigma x \cap H_{\mathbb{R}}$, and let $y = k_1 a_1 u_1$ be the corresponding Iwasawa decomposition. By Lemma 4.16 we can find an element w in $N_{H_{\mathbb{R}}}(A^*) \cap \mathbf{K}^*$ satisfying $w^{-1}a_1 w \in A_1^*$. Then $w^{-1}a_1 w \in A_1$, since by assumption, for any $i = 1, \dots, n-1$, the restriction of ε_i to S is positive, i.e., $\varepsilon_i = \sum_{\alpha \in \Pi} c_\alpha^i \alpha$, where $c_\alpha^i \geq 0$. Furthermore, in the proof of Lemma 4.14 we established (cf. (4.21)) that

$$a_{yw} = a_{a_1 u_1 a_1^{-1} w} w^{-1} a_1 w.$$

If we prove that the elements of the form $a_1 u_1 a_1^{-1}$ constitute a relatively compact set, then this formula gives us $a_{yw} \in A_s$ for sufficiently large s, i.e.,

$$yw \in \mathbf{K}A_s(U_n)_{\mathbb{R}} \cap \Sigma xw.$$

It follows from Lemma 4.14 that there exists a Siegel set Σ_1 of $GL_n(\mathbb{R})$, such that $\mathbf{K}A_1(U_n)_{\mathbb{R}} \cap \Sigma xw \subset \Sigma_1$; then $\Sigma_1 \cap H_{\mathbb{R}} \subset \Sigma^*$ for a suitable Siegel set Σ^* of $H_{\mathbb{R}}$. Finally, we have $yw \in \Sigma^*$, i.e.,

$$\Sigma x \cap H_{\mathbb{R}} \subset \bigcup_w \Sigma^* w^{-1},$$

where Σ^* is a sufficiently large Siegel set of H, w runs through a system of representatives of classes of W^*, lying in $\mathbf{K}^*$.

Before showing that the set of elements of the form $a_1u_1a_1^{-1}$ is bounded, we shall reduce the proof of Proposition 4.10 to x's of a more special type. First, let $x = bwu$ be the "inverted" Bruhat decomposition of x, where b is an upper triangular matrix, u is an upper unipotent matrix, and $w \in W$. Since Σb is contained in some large Siegel set of $GL_n(\mathbb{R})$, we may assume that $b = 1$, i.e., $x = wu$. Furthermore, by Lemma 2.1, we can find a Zariski-closed $\mathbb{R}$-set $P \subset U_n$, invariant under the adjoint action of S, such that the product morphism induces the $\mathbb{R}$-isomorphisms $P \times U \xrightarrow{\sim} U_n$ and $U \times P \xrightarrow{\sim} U_n$. Write $u = pv$ where $p \in P_{\mathbb{R}}$ and $v \in U_{\mathbb{R}}$. If we can show that $\Sigma wp \cap H_{\mathbb{R}} \subset \bigcup_i \Sigma^* x_i$, then $\Sigma x \cap H_{\mathbb{R}} \subset \bigcup_i \Sigma x_i v$. Thus, we may assume that $x = wp$, where $p \in P_{\mathbb{R}}$. We shall prove that for x of such a form the set $\{ a_1u_1a_1^{-1} : y = k_1a_1u_1 \in \Sigma x \cap H_{\mathbb{R}} \}$ is bounded, thus completing the proof of Proposition 4.10.

So, let $y = zx \in \Sigma x \cap H_{\mathbb{R}}$; and let $z = kau$ and $y = k_1a_1u_1$ be the corresponding Iwasawa decompositions. We are going to express a_1, u_1 in terms of a, u, and then use the fact that z is taken from Σ. We have

$$y = (kau)wp = (kw)(w^{-1}aua^{-1}w)(w^{-1}aw)p. \tag{4.22}$$

If we set $c = w^{-1}aua^{-1}w$ and then take the Iwasawa decomposition $c = k_ca_cu_c$ and substitute it in (4.22), we obtain

$$y = (kwk_c)a_cu_cw^{-1}awp = (kwk_c)(a_cw^{-1}aw)((w^{-1}aw)^{-1}u_c(w^{-1}aw))p,$$

whence

$$a_1 = a_cw^{-1}aw$$
$$u_1 = (w^{-1}aw)^{-1}u_c(w^{-1}aw)p.$$

Therefore

$$a_1u_1p^{-1}a_1^{-1} = (a_1u_1a_1^{-1})(a_1p^{-1}a_1^{-1}) = a_cu_ca_c^{-1}.$$

Since z was chosen from a Siegel set, Lemma 4.3 shows that the elements of the form aua^{-1} constitute a relatively compact set. This implies that the set $\{c\}$ is bounded, hence so is the set $\{ a_cu_ca_c^{-1} \}$. Now, to obtain that $\{ a_1u_1a_1^{-1} \}$ is bounded we have only to note that $a_1u_1a_1^{-1}$ is the projection of $a_cu_ca_c^{-1}$ on $U_{\mathbb{R}}$ under the isomorphism $U_{\mathbb{R}} \times P_{\mathbb{R}} \simeq (U_n)_{\mathbb{R}}$. This completes the proof of Proposition 4.10.

Thus we have proven

THEOREM 4.14. *Let G be a semisimple $\mathbb{Q}$-group, and let $\Gamma \subset G_{\mathbb{R}}$ be an arithmetic subgroup. Then $G_{\mathbb{R}}/\Gamma$ has finite invariant volume. In other words, Γ is a lattice in $G_{\mathbb{R}}$.*

(Recall that by a *lattice* in a locally compact topological group G we mean a discrete subgroup $\Gamma \subset G$ such that G/Γ has finite invariant volume.)

Theorem 4.14 immediately yields another proof of the infiniteness of an arithmetic subgroup of a semisimple algebraic $\mathbb{Q}$-group G for which $G_{\mathbb{R}}$ is noncompact (Theorem 4.11, Corollary 2). Indeed, if $G_{\mathbb{R}}$ is noncompact, then it has infinite volume with respect to a Haar measure. Consequently $G_{\mathbb{R}}/\Gamma$ also has infinite volume for any finite subgroup Γ of $G_{\mathbb{R}}$. On the other hand, for an arithmetic subgroup Γ this volume must be finite.

The proof of Theorem 4.13 can be derived from Theorem 4.14 by a straightforward argument. Namely, to begin with we may assume G to be connected. If G is a torus, then the quotient space $G_{\mathbb{R}}/G_{\mathbb{Z}}$ is a group, and therefore its having finite volume is equivalent to its being compact (Proposition 3.23). The latter holds if and only if G is $\mathbb{Q}$-anisotropic, i.e., $\mathbf{X}(G)_{\mathbb{Q}} = 1$ (Theorem 4.11). Thus, Theorem 4.13 holds for this case.

Now let G be an arbitrary reductive group. Write G as an almost direct product $G = FS$, where F is a semisimple $\mathbb{Q}$-group and S is a maximal central torus of G; note that $\mathbf{X}(G)_{\mathbb{Q}} = 1$ is equivalent to S being $\mathbb{Q}$-anisotropic. Put $H = F \times S$ and consider the isogeny $\varphi\colon H \to G$. Then $H_{\mathbb{R}} = F_{\mathbb{R}} \times S_{\mathbb{R}}$ is clearly unimodular; therefore the unimodularity of $G_{\mathbb{R}}$ follows from the finiteness of $[G_{\mathbb{R}} : \varphi(H_{\mathbb{R}})]$. Taking into account the finiteness of $\ker\varphi$ and the arithmeticity of $\varphi(H_{\mathbb{Z}})$, we can easily show that $G_{\mathbb{R}}/G_{\mathbb{Z}}$ and $H_{\mathbb{R}}/H_{\mathbb{Z}}$ both have either finite or infinite volume. Since $F_{\mathbb{R}}/F_{\mathbb{Z}}$ has finite volume by Theorem 4.14; then $H_{\mathbb{R}}/H_{\mathbb{Z}}$ has finite volume if and only if $S_{\mathbb{R}}/S_{\mathbb{Z}}$ does, which, as we have seen, is equivalent to S being $\mathbb{Q}$-anisotropic.

As usual, the case of an arbitrary connected group G reduces to the reductive case by means of the Levi decomposition $G = HU$, where U is the unipotent radical of G and H is a reductive group. Then $G_{\mathbb{R}} = H_{\mathbb{R}}U_{\mathbb{R}}$ is a semidirect product, and therefore the Haar measure dg of $G_{\mathbb{R}}$ can be written as the direct product $dg = dh\,du$ of the Haar measures dh and du on $H_{\mathbb{R}}$ and $U_{\mathbb{R}}$, respectively (cf. Bourbaki [3, Ch. 7, §11, Proposition 14]). By Lemma 4.7, $G_{\mathbb{R}}$ contains a fundamental set Ω (relative to $G_{\mathbb{Z}}$) of the form $\Omega = \Sigma\Phi$, where Σ is a fundamental set in $H_{\mathbb{R}}$ relative to $H_{\mathbb{Z}}$ and Φ is a compact subset of $U_{\mathbb{R}}$. Clearly Ω has finite volume if and only if Σ does. On the other hand, it follows from the results in §3.5 that the existence of a finite invariant measure on $G_{\mathbb{R}}/G_{\mathbb{Z}}$ is equivalent to the unimodularity of $G_{\mathbb{R}}$ together with the existence of a fundamental set $F \subset G_{\mathbb{R}}$ relative to $G_{\mathbb{Z}}$ having finite volume; then any fundamental set also has finite volume. If $\mathbf{X}(G)_{\mathbb{Q}} \neq 1$, then $\mathbf{X}(H)_{\mathbb{Q}} \neq 1$, and from our consideration of the reductive case we conclude that Σ has infinite volume. Hence Ω also has infinite volume, which means that $G_{\mathbb{R}}/G_{\mathbb{Z}}$ cannot have finite volume. Conversely, if $\mathbf{X}(G)_{\mathbb{Q}} = 1$, then $\mathbf{X}(H)_{\mathbb{Q}} = 1$; hence Σ and Ω both have finite volume. Thus, it remains to be shown that in this case $G_{\mathbb{R}}$ is unimodular. But this

can be proven in exactly the same way as the corollary of Theorem 3.18. Indeed, let ω be a left-invariant, rational, differential $\mathbb{Q}$-form on G of degree $n = \dim G$. Then, as we have seen in the proof of the above-mentioned corollary, $\varrho_g^*(\omega) = \chi(g)\omega$, where ϱ_g is the right translation by g in G and χ is a character of G. Since ω is defined over $\mathbb{Q}$, it is easy to see that χ is also defined over $\mathbb{Q}$. Therefore, in this case $\chi = 1$, i.e., ω is also a right-invariant form, and consequently $G_{\mathbb{R}}$ is unimodular by Theorem 3.18. This completes the proof of Theorem 4.13.

In those cases where $G_{\mathbb{R}}/G_{\mathbb{Z}}$ has finite volume, we naturally have the problem of its exact computation with respect to some canonical Haar measure. As we shall see in the next chapter, this problem is closely related to computing Tamagawa numbers. For a normed torus $S = \mathbf{R}^{(1)}_{K/\mathbb{Q}}(\mathbb{G}_m)$ the value of $\mu(S_{\mathbb{R}}/S_{\mathbb{Z}})$ can be expressed in terms of the discriminant and regulator of K, if we normalize the Haar measure in such a way that the volume of $K_\infty/\mathcal{O}$ equals 1, where $K_\infty = K \otimes_{\mathbb{Q}} \mathbb{R}$ and $\mathcal{O}$ is the ring of integers in K (cf. Lang [2]).

For a semisimple simply connected $\mathbb{Q}$-split group G the volume of $G_{\mathbb{R}}/G_{\mathbb{Z}}$ can be written as the product of the values of the ζ-function at certain integral points (cf. Langlands [1]). In view of these examples we may say that computation of the volume of $G_{\mathbb{R}}/G_{\mathbb{Z}}$ is a problem of considerable arithmetical interest. On the other hand, as Langlands' work shows, its solution is tied to using a complicated analytic technique (such as the theory of Eisenstein series). Therefore in this book we shall confine ourselves to one example, where the computations can be made explicitly.

EXAMPLE: Let $G = \mathbf{SL}_2$. The Iwasawa decomposition determines coordinates φ, a, u on $G_{\mathbb{R}} = SL_2(\mathbb{R})$ which can be computed for x in $G_{\mathbb{R}}$ from the equation

$$x = \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}.$$

In §3.5 (cf. Example 3) we showed that with respect to these coordinates the Haar measure on $G_{\mathbb{R}}$ can be written as $a\,d\varphi\,da\,du$. Therefore the volume of $G_{\mathbb{R}}/G_{\mathbb{Z}}$ is expressed by $\int_F a\,d\varphi\,da\,du$, where $F \subset G_{\mathbb{R}}$ is a measurable fundamental domain relative to $G_{\mathbb{Z}}$. We shall construct a fundamental domain satisfying conditions 1) and 2) in (3.22), in §3.5. To do so, we return to the considerations of §4.2 and again use the projection of $SL_2(\mathbb{R})$ on the upper half-plane $P = SO_2(\mathbb{R})/SL_2(\mathbb{R})$ of the complex plane given by $\varphi\colon \left(\begin{smallmatrix} x & y \\ u & t \end{smallmatrix}\right) \mapsto \frac{ti+y}{ui+x}$. Furthermore, consider the closed domain

$$\bar{D} = \{\, z \in P : |\Re z| \le \frac{1}{2},\ |z| \ge 1 \,\},$$

which, as we showed in §4.2, is a fundamental domain for the natural action of $PSL_2(\mathbb{Z})$ on P. Then it is easy to see that for F we may take $F = K_0 D_0$, where

$$K_0 = \left\{ \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix} : \varphi \in [0, \pi] \right\},$$

$$D_0 = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} : (a, u) \in \Omega \right\},$$

$$\Omega = \left\{ (a, u) \in \mathbb{R}^{>0} \times \mathbb{R} : \varphi \begin{pmatrix} a & au \\ 0 & a^{-1} \end{pmatrix} \in \bar{D} \right\}.$$

Therefore the volume of $G_{\mathbb{R}}/G_{\mathbb{Z}}$ relative to the given measure is equal to $\int_0^\pi d\varphi \int_\Omega a\,da\,du$. Direct computation shows that

$$\Omega = \left\{ (a, u) \in \mathbb{R}^{>0} \times \mathbb{R} : |u| \le \frac{1}{2},\ 0 \le a \le \frac{1}{\sqrt[4]{1 - u^2}} \right\},$$

and then

$$\operatorname{vol}(G_{\mathbb{R}}/G_{\mathbb{Z}}) = \int_0^\pi d\varphi \int_\Omega a\,da\,du = \int_0^\pi d\varphi \int_{-\frac{1}{2}}^{\frac{1}{2}} du \int_0^{\frac{1}{\sqrt[4]{1-u^2}}} a\,da = \frac{\pi^2}{6}.$$

(Note that this value equals $\zeta(2)$, cf. Serre [8].)

4.7. Concluding remarks on reduction theory.

The plan we outlined for developing a reduction theory of arithmetic subgroups of algebraic groups has been completed. Nevertheless, several interesting concepts, not directly related to the topics chosen for detailed exposition in this book, have been passed over. This section is included in part to remedy this situation. Thus, several supplementary results on reduction theory are collected here (without proofs): another construction of fundamental sets, the connection with reduction theory of quadratic forms, etc. Also, the results obtained are reformulated for $\mathcal{O}$-arithmetic subgroups.

The construction of fundamental sets in §4.3 is based mainly on the properties of $G_{\mathbb{R}}$ and depends relatively little on $G_{\mathbb{Q}}$ and $G_{\mathbb{Z}}$. However, building further on this construction, we can find another, generally better construction, which essentially uses the $\mathbb{Q}$-structure of G. Its advantages become apparent in the theory of automorphic functions, since the behavior at infinity of the fundamental sets thereby obtained is similar to the structure of cusp points for fundamental domains of Fuchsian subgroups of the upper half-plane. This construction also provides a clue to the construction of a compactification of $G_{\mathbb{R}}/G_{\mathbb{Z}}$, which is fundamental to the study of the cohomology of arithmetic groups.

Thus, let G be a semisimple algebraic $\mathbb{Q}$-group. If G is $\mathbb{Q}$-anisotropic, then the situation may be regarded as the best possible: $G_{\mathbb{R}}/G_{\mathbb{Z}}$ is compact (Theorem 4.12), therefore there exists a compact fundamental set with respect to $G_{\mathbb{Z}}$. Now let G be $\mathbb{Q}$-isotropic, let S be a maximal $\mathbb{Q}$-split torus of G and let P be a minimal parabolic $\mathbb{Q}$-subgroup containing S. It is well known that P is a semidirect product of its unipotent radical U and the centralizer $Z_G(S)$ of S. In turn, $Z_G(S)$ can be written as an almost direct product

$$Z_G(S) = M \cdot S, \tag{4.23}$$

where M is the largest connected $\mathbb{Q}$-anisotropic subgroup of $Z_G(S)$. Let $\mathbf{K}$ denote a maximal compact subgroup of $G_{\mathbb{R}}$ and let A be the connected component of $S_{\mathbb{R}}$. Then $G_{\mathbb{R}} = \mathbf{K} \cdot P_{\mathbb{R}}$, so (4.23) yields the following factorization:

$$G_{\mathbb{R}} = \mathbf{K} M_{\mathbb{R}} A U_{\mathbb{R}}$$

(note that, as a rule, this factorization is not unique). Since $M_{\mathbb{R}}/M_{\mathbb{Z}}$ is compact, it makes sense to look for a fundamental set relative to $G_{\mathbb{Z}}$ in the form of a generalized Siegel set

$$\Sigma_{t,y,w} = \mathbf{K}_y A_t w, \quad t > 0$$

where y (resp., w) is a compact subset of $M_{\mathbb{R}}$ (resp., $U_{\mathbb{R}}$) and $A_t = \{ a \in A : \alpha(a) \leq t \ \forall \alpha \in \Pi \}$, and Π is the system of simple roots in the root system of G relative to S, associated with P.

THEOREM 4.15. *Let G be a semisimple algebraic $\mathbb{Q}$-group, and let $\Gamma \subset G_{\mathbb{Q}}$ be its arithmetic subgroup.*

(1) *There exists a generalized Siegel set $\Sigma = \Sigma_{t,y,w}$ and a finite subset C of $G_{\mathbb{Q}}$ such that $\Omega = \Sigma C$ is a fundamental set for Γ in $G_{\mathbb{R}}$. Then C contains at least one representative of each double coset $P_{\mathbb{Q}} \setminus G_{\mathbb{Q}}/\Gamma$ (in particular, there is a finite number of such double cosets).*

(2) *Conversely, if C is a finite subset of $G_{\mathbb{Q}}$ containing a representative of each coset $P_{\mathbb{Q}} \setminus G_{\mathbb{Q}}/\Gamma$, then there exists a Siegel set Σ such that $\Omega = \Sigma C$ is a fundamental set in $G_{\mathbb{R}}$ relative to Γ.*

For the proof, see Borel [6, §§12 and 14]. We note only that the proof of (1) uses the construction of a fundamental set developed in §4.3 and broadly speaking is similar to the proof of Proposition 4.10.

It is easy to show that the generalized Siegel set Σ has finite volume with respect to the Haar measure on $G_{\mathbb{R}}$, so Theorem 4.15 (1) enables us to obtain another proof of Theorem 4.14. Due to Theorem 4.15, one

can introduce a new invariant in the theory—the number of double cosets $P_{\mathbb{Q}} \setminus G_{\mathbb{Q}}/\Gamma$. It turns out to be the smallest number of translates of Σ whose union can form a fundamental set for Γ.

For $G = \mathbf{SL}_2$ we have $P = \left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} : a \in \mathbb{C}^*, b \in \mathbb{C} \right\}$, so $P_{\mathbb{R}}$ is the stabilizer of the point at infinity with respect to the natural left action of $SL_2(\mathbb{R})$ on the upper half-plane $\mathcal{P}$ (cf. §4.2).[2] Then the orbit $SL_2(\mathbb{Q})(\infty)$ is the set of cusp points which is the union of $\{\infty\}$ with the set of points on the real axis having rational coordinates. The number of double cosets $P_{\mathbb{Q}} \setminus G_{\mathbb{Q}}/\Gamma$ in this case is the number of equivalence classes of parabolic points relative to Γ. This number turns out to be equal to the number of points that must be added to the quotient-space $\mathcal{P}/\Gamma$ to obtain its compactification, or the number of vertices of the corresponding fundamental domain at infinity (cf. Figure 4.4, page 226 for the case where Γ coincides with the congruence-subgroup $SL_2(\mathbb{Z}, 2)$; here there are 3 vertices).

In general, the complements to the compact subsets in $\Sigma_{t,y,w}$ have the form $\Sigma_{s,y,w}$ for s sufficiently small, and they may be regarded as analogs of cusps in the case of $\mathbf{SL}_2$. In this manner the number of double cosets $\Gamma \setminus G_{\mathbb{Q}}/\mathcal{P}_{\mathbb{Q}}$ can also be interpreted as the smallest number of cusps of a fundamental domain for Γ. Note that in the next chapter we shall give an adelic interpretation of the number of cosets $\Gamma \setminus G_{\mathbb{Q}}/P_{\mathbb{Q}}$. Hence, in particular, we shall obtain another proof of its finiteness and its connection with the class number of P.

Generalized Siegel sets are functorial in the sense that if $f: G \to H$ is a $\mathbb{Q}$-morphism of semisimple $\mathbb{Q}$-groups and Σ is a generalized Siegel set of G, then $f(\Sigma)$ is contained in a suitable generalized Siegel set of H. This implies that Theorem 4.15 provides a construction of the fundamental sets Ω satisfying the following condition which is stronger than (F2) (on page 193) from the definition of fundamental set:

(F2)$_{bis}$ $\Omega^{-1}\Omega \cap x\Gamma y$ is finite, for any $x, y \in C(\Gamma)_{\mathbb{R}}$, where $C(\Gamma)$- is the commensurability subgroup of Γ.

Indeed, it suffices to show that $\Sigma^{-1}\Sigma \cap x\Gamma y$ is finite, for an arbitrary generalized Siegel set Σ. To do so we use the following description of $C(\Gamma)$ given in Proposition 4.6: $C(\Gamma) = \pi^{-1}((G/N)_{\mathbb{Q}})$, where N is the largest normal $\mathbb{Q}$-subgroup of G of compact type, and $\pi: \Gamma \to G/N$ is the canonical projection. Let $\tilde{\Sigma}$ be a Siegel set of G/N such that $\pi(\Sigma) \subset \tilde{\Sigma}$. Then $\pi(\Sigma^{-1}\Sigma \cap x\Gamma y) \subset \tilde{\Sigma}^{-1}\tilde{\Sigma} \cap \pi(x)\pi(\Gamma)\pi(y)$. But $\pi(x), \pi(y) \in (G/N)_{\mathbb{Q}}$ and $\pi(\Gamma)$ is an arithmetic subgroup of G/N; since $\tilde{\Sigma}$ satisfies the usual condition (F2) (cf. Borel [6, §14]), it follows that the latter intersection is

[2] In §4.2 we denoted the upper half-plane by P. Here we have changed the notation to $\mathcal{P}$ to avoid confusion with the parabolic subgroup.

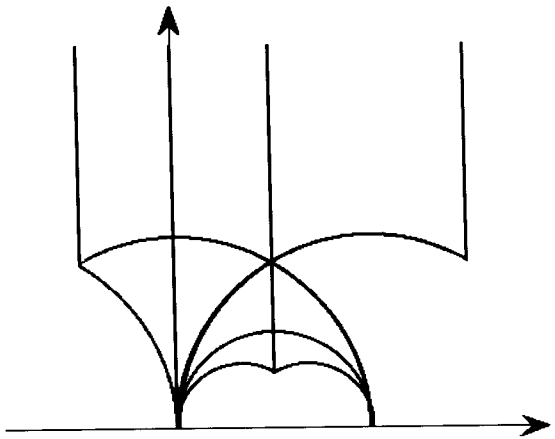


Figure 4.4.

finite. It remains to note that $\Gamma \cap N$ is finite since $N_{\mathbb{R}}$ is compact, and consequently the finiteness of $\pi(\Sigma^{-1}\Sigma \cap x\Gamma y)$ implies that of $\Sigma^{-1}\Sigma \cap x\Gamma y$, as desired.

The fundamental sets from Theorem 4.15 have another noteworthy property. Before introducing its general formulation, let us recall one of the essential steps in the reduction theory for $GL_n(\mathbb{R})$ (cf. §4.2). Having fixed an orthonormal base $e_1, \dots, e_n$ of $\mathbb{R}^n$, we introduced the continuous function $\Phi: GL_n(\mathbb{R}) \to \mathbb{R}^+$, given by $\Phi(g) = \|ge_1\|$. Then the set of values of Φ on any coset $gGL_n(\mathbb{Z})$ is bounded from below, and the minimal value is taken at some point of $\Sigma = \Sigma_{\frac{2}{\sqrt{3}}, \frac{1}{2}}$, implying that $GL_n(\mathbb{R}) = \Sigma GL_n(\mathbb{Z})$. It turns out that a similar minimum principle is satisfied for an arbitrary semisimple algebraic $\mathbb{Q}$-group G. In describing the corresponding φ we shall retain the notation introduced above. Let $\pi: G \to GL(V)$ be an absolutely irreducible $\mathbb{Q}$-respresentation of G for which there exists an eigenvector v in $V_{\mathbb{Q}}$ relative to P. Then put $\varphi_\pi(g) = \|\pi(g)v\|$, the norm being taken with respect to an orthonormal base of $V_{\mathbb{R}}$ consisting of eigenvectors relative to S. A special case of functions of the form φ_π are the Φ_i in §4.2, corresponding to the fundamental representations of $\mathbf{SL}_n$.

THEOREM 4.16. *Let G be a semisimple algebraic $\mathbb{Q}$-group, let $\varphi = \varphi_\pi$ be the function corresponding to some absolute irreducible $\mathbb{Q}$-representation $\pi: G \to GL(V)$, and let C be a set of representatives of double cosets $\Gamma \setminus G_{\mathbb{Q}}/P_{\mathbb{Q}}$, where $\Gamma \subset G_{\mathbb{Q}}$ is an arithmetic subgroup. Then there exists a generalized Siegel set Σ of $G_{\mathbb{R}}$ such that φ reaches its minimum on $x\Gamma C$ at some point of $x\Gamma C \cap \Sigma$, for an arbitrary x in $G_{\mathbb{R}}$, implying that $G_{\mathbb{R}} = \Sigma C^{-1}\Gamma$.*

Note that any semisimple $\mathbb{Q}$-group G has a sufficient supply of representations π with the properties described above. Moreover, as is well known, any absolutely irreducible representation is defined by its highest weight, and any dominant weight can be realized as the highest weight of some representation (cf. Humphreys [1]). Furthermore, it turns out that a suitable multiple of any dominant weight can be realized as the highest weight of the $\mathbb{Q}$-representation satisfying the above requirements.

The φ_π have the same properties as the Φ_i in §4.2. Relying on these properties, we can prove the analogue of Harish-Chandra's theorem for this case, and, as a result, also property (F2) in the definition of a fundamental set. For details, cf. Borel [6, §§13–14].

Although, throughout this chapter, we have been considering algebraic groups defined over $\mathbb{Q}$, the results obtained can be extended to algebraic groups defined over an arbitrary algebraic number field K. Let $\mathcal{O}$ be the ring of integers of K. Then by *$\mathcal{O}$-arithmetic subgroups of G* we mean subgroups of G that are commensurable with the group $G_{\mathcal{O}}$ of points of G over $\mathcal{O}$. The group $G_{\mathcal{O}}$ is a discrete subgroup of $G_\infty = \prod_{v \in V_f^\infty} G_{K_v}$, which is the analogue of the group of real points for $\mathbb{Q}$-groups. Naturally, we have the problem of developing a reduction theory for G_∞ relative to $G_{\mathcal{O}}$. We state the basic results obtained along these lines as

THEOREM 4.17. *Let G be an algebraic group defined over an algebraic number field K. Then the following hold:*

(1) *there exists an open fundamental set $\Omega \subset G_\infty$, relative to $G_{\mathcal{O}}$, i.e.*
   - (F0) $\mathbf{K}\Omega = \Omega$ *for a suitable maximal compact subgroup* $\mathbf{K} \subset G_\infty$,
   - (F1) $\Omega G_{\mathcal{O}} = G_\infty$,
   - (F2) $\Omega^{-1}\Omega \cap xG_{\mathcal{O}}y$ *is finite for any* $x, y \in G_K$;

(2) *$G_{\mathcal{O}}$ is a group with a finite number of generators and defining relations;*

(3) *$G_\infty/G_{\mathcal{O}}$ is compact if and only if the reductive part of the connected component is anisotropic over K;*

(4) *$G_\infty/G_{\mathcal{O}}$ has finite invariant volume if and only if $\mathbf{X}(G^0)_K = 1$.*

To prove this we take a base of $\mathcal{O}$ over $\mathbb{Z}$ and use it to construct $H = \mathbf{R}_{K/\mathbb{Q}}(G)$ (cf. §2.1.2). Then $G_{\mathcal{O}} \simeq H_{\mathbb{Z}}$ and $G_\infty \simeq H_{\mathbb{R}}$, and by applying the appropriate results for $\mathbb{Q}$-groups we can prove (1) and (2). To prove (3) we must note that the reductive part of the connected component of H has the form $\mathbf{R}_{K/\mathbb{Q}}(D)$, where D is the reductive part of the connected component of G; moreover $\mathbf{R}_{K/\mathbb{Q}}(D)$ is $\mathbb{Q}$-anisotropic if and only if D is

K-anisotropic, and then we can use Theorem 4.12. Lastly, (4) follows from Theorem 4.13 in view of the fact that $\mathbf{X}(H^0)_{\mathbb{Q}} = \mathbf{X}(G^0)_K$.

Other results (such as the density theorem, the description of commensurable subgroups, etc.) can also be extended without much effort to $\mathcal{O}$-arithmetic subgroups. We shall not formulate these results, but shall confine ourselves to generalizing the concepts involved in their statements to the $\mathcal{O}$-arithmetic case. An algebraic group G, defined over an algebraic number field K, is said to have *compact type* if $G_\infty = \prod_{v \in V_\infty^K} G_{K_v}$ is compact. Now let G be semisimple. Then G is said to have *noncompact type* if G_∞^i is noncompact for each simple K-subfactor G^i of G. A semisimple group which has neither compact nor noncompact type is said to have *mixed* type.

To conclude our exposition of reduction theory for arithmetic subgroups, we must note that this theory is rooted in the classical reduction theory of quadratic forms (cf., for example, Cassels [1]), which goes back to Hermite and Minkowski. In particular, the construction of fundamental sets as the union of a finite number of translations of a suitable Siegel set is a generalization of the construction used by Hermite [1] for the case of indefinite rational quadratic forms. Paying tribute to these distinguished predecessors, we now present several results on the reduction of positive definite quadratic forms (the case of indefinite quadratic forms is treated by Borel ([6, §5]).

Let us identify the set of positive definite quadratic forms on $\mathbb{R}^n$ with the space H of real symmetric positive definite $n \times n$ matrices. Then $G = GL_n(\mathbb{R})$ acts transitively on H from the right by

$$g\colon F \to F[g] = {}^t g F g.$$

The stabilizer of the unit form is the group $\mathbf{K} = \mathbf{O}_n(\mathbb{R})$, so $H = G/\mathbf{K}$, where the projection $\pi\colon G \to H$ is given by $\pi(g) = {}^t gg$. Clearly π sends $SL_n(\mathbb{R})$ to the set $H^{(1)}$ of elements of H with determinant 1, and $H^{(1)} = SL_n(\mathbb{R})/SO_n(\mathbb{R})$. Notation as in §4.2, we shall call a set of the form

$$\Sigma'_{t,v} = \{\, {}^t uau : a \in A_t,\ u \in U_v \,\}$$

the Siegel set in H. Since ${}^t kk = E_n$ for any k in $\mathbf{K}$, we have

$$\pi(\Sigma_{t,v}) = \Sigma'_{t^2,v}.$$

Since $\pi(g_1 g_2) = \pi(g_1)[g_2]$, Theorems 4.4 and 4.13 yield

THEOREM 4.18.

(i) *(Korkin-Zolotarev). $H = \Sigma'_{t,v}[GL_n(\mathbb{Z})]$ for $t \geq \frac{4}{3}$, $v \geq \frac{1}{2}$.*

(ii) *(Hermite). If F is a positive definite form on $\mathbb{R}^n$, then*

$$\min_{x \in \mathbb{Z}^n \setminus \{0\}} F(x) \leq \left(\frac{4}{3}\right)^{\frac{n-1}{2}} (\det F)^{\frac{1}{n}}.$$

(iii) *(Minkowski). $H^{(1)} = (\Sigma'_{t,v} \cap H^{(1)})[SL_n(\mathbb{Z})]$ for $v \geq \frac{1}{2}$ and $t \geq \frac{4}{3}$, and $H^{(1)}/SL_n(\mathbb{Z})$ has finite invariant volume.*

4.8. Finite arithmetic groups.

The arithmetic theory of algebraic groups is mainly concerned with the analysis of infinite arithmetic groups, since only in this case may one expect a close connection between the properties of an algebraic group G and its arithmetic subgroups. The case of finite arithmetic groups was thought to be of interest primarily for the theory of finite simple groups. Indeed, the group of automorphisms of the 24-dimensional positive definite Leech lattice (more precisely, the quotient-group modulo its center) turned out to be a new simple sporadic group, discovered by Conway (Conway [1]). However, in the past year an interesting collection of purely arithmetic questions have come up regarding finite arithmetic groups. For the most part, these questions focus around the following conjecture.

CONJECTURE 1: Let G be an algebraic $\mathbb{Q}$-defined group of compact type. Then for any totally real extension $K/\mathbb{Q}$, we have $G_{\mathcal{O}} = G_{\mathbb{Z}}$, where $\mathcal{O}$ is the ring of integers of K.

(Recall that $K/\mathbb{Q}$ is said to be totally real if the image of any embedding $K \hookrightarrow \mathbb{C}$ is contained in $\mathbb{R}$. For such an extension, in the case under consideration $G_\infty = \prod_{v \in V_\infty^K} G_{K_v}$ is compact, so $G_{\mathcal{O}}$ is finite.)

In other words, the group of units of a compact algebraic $\mathbb{Q}$-group does not change (is "stable") under extension from ring $\mathbb{Z}$ to the ring of integers $\mathcal{O}$ of a totally real number field K. Since any totally real extension is clearly contained in a totally real Galois extension, we may assume without loss of generality that $K/\mathbb{Q}$ is a Galois extension. This conjecture came up in studying the properties of positive definite quadratic lattices; its proof would enable us to obtain a number of interesting corollaries in the theory of lattices (cf. below). The following proposition shows that its generalization to arbitrary algebraic groups is not essential.

PROPOSITION 4.12. *Let $G \subset GL_n(\mathbb{C})$ be an algebraic $\mathbb{Q}$-group whose group of real points $G_{\mathbb{R}}$ is compact and Zariski dense in G. Then there*

exists an n-dimensional positive definite quadratic form f with rational coefficients, for which $G \subset \mathbf{O}_n(f)$.

PROOF: Let h be an arbitrary n-dimensional positive definite quadratic form. Since $G_{\mathbb{R}}$ is compact, the integral $\int h(gv)dg$ is defined for each v in R^n. We shall denote this integral by $h_0(v)$ (here dg is the Haar measure on $G_{\mathbb{R}}$). Elementary verification shows that the map $\mathbb{R}^n \to \mathbb{R}$, given by $v \mapsto h_0(v)$, yields a positive definite $G_{\mathbb{R}}$-invariant quadratic form on $\mathbb{R}^n$. Since $G_{\mathbb{R}}$ is Zariski-dense in G, the extension of h_0 to $\mathbb{C}^n$ is invariant under G. Let V denote the space of all G-invariant quadratic forms on $\mathbb{C}^n$. Since G is defined over $\mathbb{Q}$, V is also defined over $\mathbb{Q}$. Moreover, the density of $\mathbb{Q}$ in $\mathbb{R}$ implies the density of $V_{\mathbb{Q}}$ in $V_{\mathbb{R}}$. On the other hand, the subset W of $V_{\mathbb{R}}$ of positive definite forms contains h_0 and therefore is a non-empty open subset of $V_{\mathbb{R}}$, its openness being a consequence of the well-known Silvester criterion. Since $V_{\mathbb{Q}}$ is dense in $V_{\mathbb{R}}$, this implies the existence of the desired positive definite form f in $V_{\mathbb{Q}}$. The proposition is proved.

Now we shall show that Conjecture 1 can be restated as follows:

CONJECTURE 1*: Let f be a positive definite quadratic form of dimension n with rational coefficients. Then $\mathbf{O}_n(f)_{\mathcal{O}} = \mathbf{O}_n(f)_{\mathbb{Z}}$ for the ring of integers $\mathcal{O}$ of any totally real extension $K/\mathbb{Q}$.

Conjecture 1* is obviously a special case of Conjecture 1. In order to obtain the converse, we shall fix the ring of integers $\mathcal{O}$ of a totally real Galois extension $K/\mathbb{Q}$, and let H denote the subgroup generated by G^0 and $G_{\mathcal{O}}$. Since $\mathcal{O}$ is invariant under all automorphisms of $\mathbb{C}/\mathbb{Q}$, we see that $G_{\mathcal{O}}$ and hence also $H = G^0 G_{\mathcal{O}}$ are defined over $\mathbb{Q}$. Clearly $H_{\mathbb{R}} = G^0_{\mathbb{R}} G_{\mathcal{O}}$; consequently, since $G^0_{\mathbb{R}}$ is Zariski-dense in G^0 (Theorem 2.2), $H_{\mathbb{R}}$ is dense in H. Therefore, by Proposition 4.12, there exists a positive definite quadratic form f with rational coefficients, such that $H \subset \mathbf{O}_n(f)$, where n is the degree of G as a linear group. Then $G_{\mathcal{O}} = H_{\mathcal{O}} \subset \mathbf{O}_n(f)_{\mathcal{O}} = \mathbf{O}_n(f)_{\mathbb{Z}}$ and $G_{\mathcal{O}} = G_{\mathbb{Z}}$, as required.

In connection with Conjecture 1*, we must mention the following result:

PROPOSITION 4.13. *Let $f(x_1, \dots, x_n) = a_1 x_1^2 + \cdots + a_n x_n^2$ be a diagonal integral positive definite quadratic form. Then $\mathbf{O}_n(f)_{\mathcal{O}} = \mathbf{O}_n(f)_{\mathbb{Z}}$ for the ring of integers $\mathcal{O}$ of any totally real extension $K/\mathbb{Q}$.*

PROOF: We show that for any element $b = (b_{ij})$ in $\mathbf{O}_n(f)_{\mathcal{O}}$, each row and each column has only one non-zero element, which, moreover equals ± 1. Without loss of generality we may assume $a_1 \leq a_2 \leq \cdots \leq a_n$. The fact that $b \in \mathbf{O}_n(f)$ means that ${}^t bFb = F$, where $F = \operatorname{diag}(a_1, \dots, a_n)$, from

which we obtain the following relations:

$$\sum_{i=1}^{n} a_i b_{ij}^2 = a_j \qquad \text{for each } j = 1, \dots, n; \tag{4.24}$$

$$\sum_{i=1}^{n} a_i b_{ij} b_{ik} = 0 \qquad \text{for each } j \neq k \text{ between 1 and } n. \tag{4.25}$$

In the last row of b there will be a nonzero entry b_{nj}. Then, by virtue of (4.24) we have

$$a_n \tau(b_{nj})^2 \leq \sum_{i=1}^{n} a_i \tau(b_{ij})^2 = a_j \leq a_n,$$

for any embedding $\tau: K \hookrightarrow \mathbb{R}$; so $|b_{nj}| \leq 1$ for any real valuation v of K. But

$$\prod_{v \in V_\infty^K} |b_{nj}|_v = |N_{K/\mathbb{Q}}(b_{nj})|,$$

where $N_{K/\mathbb{Q}}$ is the norm map from K to $\mathbb{Q}$. Moreover, since $b_{nj} \in \mathcal{O}$, we have $N_{K/\mathbb{Q}}(b_{nj}) \in \mathbb{Z}$ and $|N_{K/\mathbb{Q}}(b_{nj})| \geq 1$. Therefore $|b_{nj}|_v = 1$ for any $v \in V_\infty^K$, since $|b|_v = |\tau_v(b)|$, where $\tau_v: K \hookrightarrow \mathbb{R}$ is the corresponding embedding and $|\ |$ is the absolute value; in fact $b_{nj} = \pm 1$. Returning to (4.24) and bearing in mind that $a_j \leq a_n$, we obtain $a_j = a_n$ and $b_{ij} = 0$ for $i < n$. Furthermore, applying (4.25) we obtain that $b_{nk} = 0$, for all $k \neq j$. A similar argument can be applied to the j-th row, if $a_j = a_n$. Thus we obtain that b has the block structure

$$b = \begin{pmatrix} b_1 & 0 \\ 0 & b_2 \end{pmatrix},$$

where b_1 is a square $l \times l$ matrix, l being the maximal index for which $a_l < a_n$, and b_2 is a monomial matrix of dimension $(n-l) \times (n-l)$, all of whose nonzero elements equal ± 1. (One can have a situation where all the a_i coincide, but then the above argument completes the proof of the proposition.) The proof of Proposition 4.13 can now be completed by an obvious inductive procedure.

Now we present one more equivalent formulation of Conjecture 1.

CONJECTURE 1**: Let $K/\mathbb{Q}$ be a totally real Galois extension, let $\mathcal{O}$ be the ring of integers of K, and let Γ be a finite subgroup of $GL_n(\mathcal{O})$, invariant (as a whole, but not necessarily elementwise) under $\operatorname{Gal}(K/\mathbb{Q})$. Then $\Gamma \subset GL_n(\mathbb{Z})$.

It is easy to see that Conjectures 1 and 1** are equivalent. Indeed, as we have already noted, we may assume $K/\mathbb{Q}$ in Conjecture 1 to be a Galois extension. If G is an algebraic $\mathbb{Q}$-group of compact type, then $G_{\mathcal{O}}$ is a finite $\mathrm{Gal}(K/\mathbb{Q})$-invariant subgroup of $GL_n(\mathcal{O})$; therefore Conjecture 1 follows from Conjecture 1**. Conversely, if $\Gamma \subset GL_n(\mathcal{O})$ is a finite $\mathrm{Gal}(K/\mathbb{Q})$-invariant subgroup, it can be regarded as an algebraic $\mathbb{Q}$-group G for which $G_{\mathbb{R}} = \Gamma$ is compact.

At present Conjecture 1** has been proved only for some special Galois extensions—namely, for nilpotent extensions and for the extensions whose Galois group has only cyclic Sylow subgroups (cf. Bartels, Kitaoka [1]). The proof for nilpotent extensions contains the most noteworthy aspects of the subject; therefore we shall confine ourselves to this case and refer the reader to Bartels and Kitaoka to supplement the material presented here. We call the reader's attention to two facts which will be used repeatedly in working with Hypothesis 1**. The first is Hermite's theorem on the nonexistence of nontrivial totally unramified extensions of $\mathbb{Q}$ (cf. Theorem 1.3), and the second is the following lemma due to Minkowski [1]:

LEMMA 4.19 (MINKOWSKI). *The congruence subgroup $GL_n(\mathbb{Z}, p)$ is torsion-free, for any $p \neq 2$.*

PROOF: Using the embedding $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ of Lemma 3.8, we obtain that the order of any element of $GL_n(\mathbb{Z}, p)$ is either infinite or is a power of p. Therefore it suffices to show that $GL_n(\mathbb{Z}, p)$ does not contain any elements of order p distinct from E_n. Let $E_n \neq x \in GL_n(\mathbb{Z}, p)$ and suppose that $x^p = E_n$. Write $x = E_n + p^\alpha y$, where $y \in M_n(\mathbb{Z})$ and $y \not\equiv 0 \pmod{p}$. Then

$$x^p = (E_n + p^\alpha y)^p = E_n + \binom{p}{1} p^\alpha y + \cdots + \binom{p}{p-1} p^{\alpha(p-1)} y^{p-1} + p^{\alpha p} y^p = E_n,$$

i.e.,

$$p^{\alpha+1} y = -\binom{p}{2} p^{2\alpha} y^2 - \cdots - \binom{p}{p-1} p^{\alpha(p-1)} y^{p-1} - p^{\alpha p} y^p. \tag{4.26}$$

All the binomial coefficients $\binom{p}{i}$, where $0 < i < p$, are divisible by p; thus we have

$$\binom{p}{i} p^{i\alpha} y^i \equiv 0 \pmod{p^{2\alpha+1}} \text{ for each } i > 1.$$

Since $p > 2$, we have $\alpha p \geq 2\alpha + 1$, and $p^{\alpha p} y^p \equiv 0 \pmod{p^{2\alpha+1}}$ holds. Thus, the right side of (4.26) is congruent to $0 \pmod{p^{2\alpha+1}}$, while, by our construction, this congruence does not hold for the left side, since $\alpha + 1 < 2\alpha + 1$. Lemma 4.19 is proved.

Now let $K/\mathbb{Q}$ be a totally real Galois extension. If $K/\mathbb{Q}$ is unramified at all points, then by Hermite's theorem $K = \mathbb{Q}$, and there is nothing to prove. Thus we may assume that there is at least one ramified prime in $K/\mathbb{Q}$. We shall show that to prove Conjecture 1** is suffices to consider the case when there is only one ramified prime.

PROPOSITION 4.14. *Let $K/\mathbb{Q}$ be a totally real Galois extension with Galois group $\mathcal{G}$ and let Γ be a finite $\mathcal{G}$-invariant subgroup of $GL_n(\mathcal{O})$. Suppose that $\Gamma \cap GL_n(L) \subset GL_n(\mathbb{Z})$ for every proper Galois subextension L of K. If $\Gamma \not\subset GL_n(\mathbb{Z})$, then there is exactly one prime ramified in K.*

PROOF: Let us suppose that two distinct primes p and q ($q \neq 2$) are ramified in $K/\mathbb{Q}$, and show that then $\Gamma \subset GL_n(\mathbb{Z})$. Consider some extensions $w_p \mid p$ and $w_q \mid q$, and let $\mathfrak{p} = \mathcal{O} \cap \mathfrak{p}_{w_p}$ and $\mathfrak{q} = \mathcal{O} \cap \mathfrak{q}_{w_q}$ be the corresponding ideals of $\mathcal{O}$. We shall use the ramification groups $\mathcal{G}^{(i)}$, defined at the end of §1.1. Let $x \in \Gamma$ and $\sigma \in \mathcal{G}^{(1)}(w_q)$. Then $x \equiv \sigma(x) \pmod{\mathfrak{q}}$, and therefore, since Γ is $\mathcal{G}$-invariant, $y = x^{-1}\sigma(x)$ lies in the congruence subgroup $\Gamma(\mathfrak{q})$. Now take an arbitrary τ in $\mathcal{G}^{(1)}(w_p)$. Then, on the one hand, the group commutator $[y, \tau(y)] = y\tau(y)y^{-1}\tau(y)^{-1}$ lies in $\Gamma(\mathfrak{q})$, since $\Gamma(\mathfrak{q})$ is a normal subgroup of Γ; on the other hand, it lies in $\Gamma(\mathfrak{p})$, by virtue of the condition that $y \equiv \tau(y) \pmod{\mathfrak{p}}$. But, embedding $\mathcal{O}$ in $\mathcal{O}_{w_p}$ and $\mathcal{O}_{w_q}$, we obtain that the order of any element of $\Gamma(\mathfrak{p})$ (respectively, $\Gamma(\mathfrak{q})$) is a power of p (respectively, q), by Lemma 3.8; in particular, $\Gamma(\mathfrak{p}) \cap \Gamma(\mathfrak{q}) = \{E_n\}$. Therefore $[y, \tau(y)] = E_n$, i.e., y and $\tau(y)$ commute. Further, since $y \in \Gamma(\mathfrak{q})$, the order of y, and hence also of $z = y^{-1}\tau(y)$, is q. But at the same time $z \in \Gamma(\mathfrak{p})$, and therefore actually $z = E_n$ and $\tau(y) = y$. We have shown that $\tau(y) = y$ for any σ in $\mathcal{G}^{(1)}(w_p)$ where $w_p \mid p$. Let $\mathcal{H}$ be the subgroup of $\mathcal{G}$ generated by the inertia groups $\mathcal{G}^{(1)}(w_p)$ for all $w_p \mid p$, and let $L = K^{\mathcal{H}}$ be the corresponding fixed field. As we noted at the end of §1.1, L is a maximal Galois extension of $\mathbb{Q}$, contained in K and unramified relative to p. Since p is ramified in K, then $L \neq K$ so by hypothesis $\Gamma \cap GL_n(L) \subset GL_n(\mathbb{Z})$. But we established above that $y \in GL_n(L)$, and therefore $y \in GL_n(\mathbb{Z})$. Recalling that $y \in \Gamma(\mathfrak{q})$, we see that y is an element of $GL_n(\mathbb{Z}, q)$ of finite order, which means that $y = E_n$, by Minkowski's lemma. By definition $y = x^{-1}\sigma(x)$, where x is an arbitrary element of Γ and $\sigma \in \mathcal{G}^{(1)}(w_q)$. It follows that indeed $\Gamma \subset GL_n(P)$, where $P = K^{\mathcal{F}}$ is the fixed field of the subgroup $\mathcal{F} \subset \mathcal{G}$ generated by the inertia groups $\mathcal{G}^{(1)}(w_q)$, for all extensions $w_q \mid q$. Proceeding as above, we obtain that $P \neq K$, and hence $\Gamma = \Gamma \cap GL_n(P) \subset GL_n(\mathbb{Z})$. The proposition is proved.

Proposition 4.14 shows that if there are counterexamples to Conjecture 1**, then in terms of field extensions a minimal counterexample corresponds to an extension in which there is exactly one ramified prime. With this observation, we shall prove Conjecture 1** for nilpotent extensions.

THEOREM 4.19 (BARTELS–KITAOKA). *Let $K/\mathbb{Q}$ be a totally real Galois extension with nilpotent Galois group $\mathcal{G}$. If Γ is a finite $\mathcal{G}$-invariant subgroup of $GL_n(\mathcal{O})$, then $\Gamma \subset GL_n(\mathbb{Z})$.*

PROOF: Since any Galois subextension of a nilpotent extension is also nilpotent, it follows from the above remark that we need only consider extensions $K/\mathbb{Q}$ for which there is only one ramified prime p. We shall show that in this case $\mathcal{G}$ is cyclic. To do so, we use induction on $[K:\mathbb{Q}]$. The center Z of $\mathcal{G}$ is nontrivial, and by induction $\mathcal{G}/Z$ is cyclic. But then $\mathcal{G}$ is abelian, and by the Kronecker–Weber theorem (cf., for example, Iwasawa [1, §8.1]) $K \subset \mathbb{Q}(\zeta_{p^d})$ for suitable d, where ζ_{p^d} is a primitive p^d-th root of unity. Since $K/\mathbb{Q}$ is totally real, actually $K \subset \mathbb{Q}(\zeta_{p^d}+\zeta_{p^d}^{-1})$ and $\mathcal{G}$ is a quotient-group of $(\mathbb{Z}/p^d\mathbb{Z})^*/\{\pm 1\}$, which is cyclic. Now, having proven $\mathcal{G}$ is cyclic, by Kronecker's theorem we can assert that in our case always $K \subset \mathbb{Q}(\zeta_{p^d}+\zeta_{p^d}^{-1})$ for a suitable $d>0$, and to prove Theorem 4.19 is suffices to examine the case $K=\mathbb{Q}(\zeta_{p^d}+\zeta_{p^d}^{-1})$.

LEMMA 4.20. *Conjecture 1** is true for $K=\mathbb{Q}(\zeta_{p^d}+\zeta_{p^d}^{-1})$.*

The proof uses a general construction which may also be useful in other situations. Namely, for an arbitrary Galois extension $K/\mathbb{Q}$ with Galois group $\mathcal{G}$ we define the Galois subextension $M/\mathbb{Q}$ as follows: fix some prime p and consider an extension $w_p \mid p$; let $\mathfrak{p}=\mathcal{O}\cap\mathfrak{p}_{w_p}$ be the corresponding ideal in $\mathcal{O}$, and let r be the smallest positive integer for which $p \notin \mathfrak{p}^{r(p-1)}$. Let $\mathcal{H}$ denote the subgroup of $\mathcal{G}$ generated by the r-th ramification groups $\mathcal{G}^{(r)}(w_p)$ for all extensions $w_p \mid p$, and put $M=K^{\mathcal{H}}$. The subextension $M/\mathbb{Q}$ thus obtained depends on the choice of p; however for any p it is a Galois extension, and for any finite $\mathcal{G}$-invariant subgroup Γ of $GL_n(\mathcal{O})$ we have $\Gamma \subset GL_n(\mathcal{O}_M)$, where $\mathcal{O}_M$ is the ring of integers of M. Indeed, for any x in Γ and any σ in $\mathcal{G}^{(r)}_{(w_p)}$, we have $\sigma(x)\equiv x \pmod{\mathfrak{p}^r}$, i.e., $x^{-1}\sigma(x)\in \Gamma(\mathfrak{p}^r)$. Therefore it suffices to establish the triviality of the congruence subgroup $\Gamma(\mathfrak{p}^r)$. To do so, in turn, it suffices to show that the congruence subgroup $GL_n(\mathcal{O},\mathfrak{p}^r)$ is torsion-free, which is equivalent to its having no elements of order p. The latter can be proven by an argument similar to the proof of Minkowski's lemma:

Namely, let $E_n \neq x \in GL_n(\mathcal{O},\mathfrak{p}^r)$ and let $x^p=E_n$. Write $x=E_n+y$, where $y\equiv 0 \pmod{\mathfrak{p}^m}$ $(m\geq r)$, but $y\not\equiv 0 \pmod{\mathfrak{p}^{m+1}}$. Then we have

$$x^p = E_n + py + \binom{p}{2}y^2 + \cdots + \binom{p}{p-1}y^{p-1} + y^p = E_n,$$

i.e.,

$$py = -\binom{p}{2}y^2 - \cdots - \binom{p}{p-1}y^{p-1} - y^p. \tag{4.27}$$

Let e denote the ramification index $e(w_p \mid p)$. Then e is the exponent for $\mathfrak{p}$ in the decomposition of $p\mathcal{O}$; therefore, from the definition of r it follows that $r=\left[\frac{e}{p-1}\right]+1$ (where, as usual, $[a]$ is the integral part of a), and so, $(p-1)r>e$. This estimation enables us to reach a contradiction by computing the power of $\mathfrak{p}$ which divides the left and right sides of (4.27) respectively. By our construction, for the left side of (4.27) we have

$$py\equiv 0 \pmod{\mathfrak{p}^{m+e}}, \text{ but } py\not\equiv 0 \pmod{\mathfrak{p}^{m+e+1}}).$$

Since the $\binom{p}{i}$ are divisible by p $(i\neq 0,p)$, we have $\binom{p}{i}y^i\equiv 0 \pmod{\mathfrak{p}^{im+e}}$ for $1<i<p$ and $imd\geq m+e+1$. Lastly, $y^p\equiv 0 \pmod{\mathfrak{p}^{mp}})$ where $mp=m+m(p-1)\geq m+r(p-1)>m+d$. Thus, the right side of (4.25) equals 0 modulo $\mathfrak{p}^{m+d+1}$, contradiction.

To complete the proof of the lemma it suffices to establish that for $K_d=\mathbb{Q}(\zeta_{p^d}+\zeta_{p^d}^{-1})$ the subextension constructed using p is contained in K_{d-1} (since $K_0=\mathbb{Q}$, this gives the required result). We shall need some information about the ramification of p in the cyclotomic extension $L_d/\mathbb{Q}$, where $L_d=\mathbb{Q}(\zeta_{p^d})$ (cf. ANT, Ch. 3).

It is well known that $L_d/\mathbb{Q}$ is an abelian Galois extension of degree $\varphi(p^d)=p^{d-1}(p-1)$. The ring of integers $\mathcal{O}_d$ of L_d is $\mathbb{Z}[\zeta_{p^d}]$ and $p\mathcal{O}_d=\mathfrak{P}^{\varphi(p^d)}$, where $\mathfrak{P}=(1-\zeta_{p^d})\mathcal{O}_d$; in other words, the p-adic valuation has a unique extension to L_d. Moreover this extension is totally ramified, and the corresponding valuation ideal in $\mathcal{O}_d$ is the maximal ideal generated by $1-\zeta_{p^d}$. In particular, for $d=1$ we see that the valuation ideal $\mathfrak{P}_1\subset\mathcal{O}_1$ is generated by $1-\zeta_p$. On the other hand, since L_d/L_1 is a totally ramified extension of degree p^{d-1}, we must have $\mathfrak{P}_1\mathcal{O}_d=\mathfrak{P}^{p^{d-1}}$, from which it follows that $1-\zeta_p\in\mathfrak{P}^{p^{d-1}}$, i.e., $\zeta_p\equiv 1 \pmod{\mathfrak{P}^{p^{d-1}}}$. This relation is more useful to us when put in a slightly different way. Namely, let σ_a denote the automorphism from $\mathrm{Gal}(L_d/\mathbb{Q})$ given by $\sigma_a(\zeta_{p^d})=\zeta_{p^d}^a$, for any integer a coprime to p. Then the above relation means that

$$\sigma_a(\zeta_{p^d})\equiv\zeta_{p^d} \pmod{\mathfrak{P}^{p^{d-1}}} \quad \text{for} \quad a\equiv 1 \pmod{p^{d-1}}.$$

Since ζ_{p^d} generates $\mathcal{O}_d$, we obtain for such a

$$\sigma_a(x)\equiv x \pmod{\mathfrak{P}^{p^{d-1}}} \quad \text{for all } x \text{ in } \mathcal{O}_d. \tag{4.28}$$

However, computing r for K_d gives us

$$r=\left[\frac{\varphi(p^d)/2}{p-1}\right]+1=\left[\frac{p^{d-1}}{2}\right]+1, \tag{4.29}$$

since the ramification index e of the p-adic valuation in $K_d/\mathbb{Q}$ equals $\varphi(p^d)/2$. Using (4.28) and (4.29), for odd p we obtain

$$\sigma_a(x) \equiv \pmod{\mathfrak{p}^r} \text{ when } a \equiv 1 \pmod{p^{d-1}} \text{ for all integers } x \text{ in } K_d,$$

since the ramification index of L_d/K_d equals 2.

Let $\mathcal{G}$ denote $\mathrm{Gal}(K_d/\mathbb{Q})$ and let w be the (unique) extension of the p-adic valuation to K_d. With this notation, the above congruence means that the r-th ramification group $\mathcal{G}^{(r)}(w)$ contains the subgroup $\mathcal{H}$ of $\mathcal{G}$ consisting of the restrictions of the automorphisms σ_a, for $a \equiv 1 \pmod{p^{d-1}}$. But $K_d^{\mathcal{H}} = K_{d-1}$, so M as defined above is contained in K_{d-1}, as required.

To dispose of the remaining case, $p = 2$, we need to elaborate on (4.28) by showing that $\sigma_a(x) \equiv x \pmod{\mathfrak{P}^{2^{d-1}+2}}$ for $a \equiv 1 \pmod{2^{d-1}}$ and any integer x in K_d. It suffices to show that $\sigma_a(\zeta_{2^d} + \zeta_{2^d}^{-1}) \equiv \zeta_{2^d} + \zeta_{2^d}^{-1} \pmod{\mathfrak{P}^{2^{d-1}+2}}$. The latter follows easily from (4.27) and the following computations,

$$\zeta_{2^d} + \zeta_{2^d}^{-1} = \zeta_{2^d}^{-1}(\zeta_{2^d}^2 + 1) = \zeta_{2^d}^{-1}((\zeta_{2^d} - 1)^2 + 2\zeta_{2^d}),$$

in view of the fact that $(\zeta_{2^d} - 1)^2 + 2\zeta_{2^d} \in \mathfrak{P}^2$. This completes the proof of Lemma 4.20.

In studying special cases of Conjecture 1–1**, we can impose additional conditions of two types—on the totally real extension $K/\mathbb{Q}$, and on Γ in Conjecture 1** or on f in Conjecture 1*, respectively. Conditions of the former type were imposed in Theorem 4.19. Now we present a result illustrating conditions of the latter type, which shows that there is an open subset in the space of real symmetric matrices whose integral matrices (or, more precisely, whose corresponding quadratic forms) satisfy Conjecture 1*.

PROPOSITION 4.15. *Let f be an integral positive definite quadratic form of dimension n with matrix $a = (a_{ij})$. Suppose $a_{ii} \leq 4\lambda$ for all $i = 1, \dots, n$, where λ is the smallest eigenvalue of a. Then we have $\mathbf{O}_n(f)_{\mathcal{O}} = \mathbf{O}_n(f)_{\mathbb{Z}}$ for any totally real extension $K/\mathbb{Q}$, where $\mathcal{O}$ is the ring of integers of K.*

PROOF: Let $x = (x_{ij}) \in \mathbf{O}_n(f)_{\mathcal{O}}$. We shall show that

$$\sum_{i=1}^{n} x_{ij}^2 \leq \frac{a_{jj}}{\lambda} \tag{4.30}$$

under any real embedding of K. Indeed, let v_j denote the vector

$$(0, 0 \dots 0, 1, 0, \dots 0),$$

where 1 is in the j-th position. Then $xv_j = (x_{1j}, \dots, x_{nj}) = w_j$ and $a_{jj} = f(v_j) = f(w_j)$. Also, if we let g denote the quadratic form on $\mathbb{R}^n$ for which $v_1, \dots, v_n$ is an orthonormal base, then the left side of (4.30) becomes $g(w_j)$, and so it suffices to show that $f(w) \geq \lambda g(w)$ for any w in $\mathbb{R}^n$. Putting f into diagonal form using a transformation from $\mathbf{O}_n(g)_{\mathbb{R}}$, we see that it suffices to analyze the case for f diagonal, for which the desired assertion is trivial.

Combining (4.30) with the condition $a_{ii} \leq 4\lambda$, we see that in this case

$$\sum_{i=1}^{n} x_{ij}^2 \leq 4 \quad \text{for all} \quad j = 1, \dots, n.$$

In particular, $|x_{ij}|_v \leq 2$ for all $i, j = 1, \dots, n$ and for any v in V_∞^K. It follows that all the x_{ij} coincide with the real parts of some roots of unity. Indeed, let a be a totally real algebraic number, and let $|a|_v \leq 2$ for any v. Then $b = \sqrt{\frac{a^2}{4} - 1}$ is purely imaginary. Also, $t = \frac{a}{2} + b$ satisfies $t^2 - at + 1 = 0$ and therefore is an algebraic integer all of whose conjugates have absolute value 1. It follows easily that t is a root of unity, so $a = 2\Re(t)$ is its real part. From what we have shown it follows that the coefficients x_{ij} generate an abelian extension of $\mathbb{Q}$; therefore we complete the proof of the proposition by applying Theorem 4.19.

We present two more results, also obtained with the help of a metric argument (Kitaoka [1],[2]).

PROPOSITION 4.16. *For each dimension n there is a finite set of algebraic numbers S such that, if $K \cap S = \emptyset$, then Conjecture 1* holds for $K/\mathbb{Q}$ and any quadratic form of dimension n.*

(Using the reduction theory of quadratic forms one can find S explicitly for small values of n (cf. Kitaoka [1]).)

PROPOSITION 4.17. *If either $[K : \mathbb{Q}]$ or the dimension of f does not exceed 42, then Conjecture 1* holds.*

We have presented virtually all the known results pertaining to the conjectures under consideration. To draw the reader's attention and hopefully stimulate further research, we note several possible applications (cf. Bartels [1], [2]).

PROPOSITION 4.18. *Assume Conjecture 1* holds for a certain extension $K/\mathbb{Q}$ and any positive definite quadratic form. If f and g are integral positive definite quadratic forms which are equivalent over the ring of integers $\mathcal{O}$ of K, then in fact they are equivalent over $\mathbb{Z}$.*

PROOF: Let $a \in GL_n(\mathcal{O})$ realize $f \simeq g$. Take the form $h = f \oplus g$ and let b be the matrix

$$\begin{pmatrix} 0 & a^{-1} \\ a & 0 \end{pmatrix}.$$

Then $b \in \mathbf{O}_{2n}(h)_{\mathcal{O}} = \mathbf{O}_{2n}(h)_{\mathbb{Z}}$, so $a \in GL_n(\mathbb{Z})$, as desired.

The next two theorems involve Galois cohomology and adele groups, which are systematically studied in Chapters 5 and 6. These results are presented here in order to draw together all the material pertaining to the conjectures under consideration. The reader may wish to acquaint himself first with Chapters 5 and 6 and then return to these results.

THEOREM 4.20. *Let $K/\mathbb{Q}$ be a totally real Galois extension, and let G be an algebraic $\mathbb{Q}$-group of compact type. Suppose $G_{\mathcal{O}} = G_{\mathbb{Z}}$. Then the kernel of the natural map of Galois cohomology*

$$H^1(K/\mathbb{Q}, G_{\mathcal{O}}) \to \prod_v H^1(K_v/\mathbb{Q}_p, G_{\mathcal{O}_v})$$

is trivial.

THEOREM 4.21. *Under the above hypotheses and the additional assumption that G be a connected group satisfying the Hasse principle for Galois cohomology, we have*

$$G_{A_{\mathbb{Q}}} \cap G_K G_{A_K(\infty)} = G_{\mathbb{Q}} G_{A_{\mathbb{Q}}(\infty)},$$

i.e., the kernel of

$$G_{\mathbb{Q}} \backslash G_{A_{\mathbb{Q}}} / G_{A_{\mathbb{Q}}(\infty)} \to G_K \backslash G_{A_K} / G_{A_K(\infty)}$$

is trivial.

(Here $G_{A_{\mathbb{Q}}(\infty)}, G_{\mathbb{Q}}$ (resp., $G_{A_K(\infty)}, G_K$) are the subgroups of integral and principal adeles in the adele groups $G_{A_{\mathbb{Q}}}$ and G_{A_K} over $\mathbb{Q}$ and K, respectively. Cf. §5.1.)

For the proofs of Theorems 4.20 and 4.21 and some of their applications, cf. §8.4. Here we wish to note that in the context of quadratic forms Theorem 4.21 means that if two positive definite forms over $\mathbb{Z}$ belong to the same genus and enter the same class under extension of the ring of scalars to $\mathcal{O}$, then they lie in the same class over $\mathbb{Z}$.

To conclude, let us present an example which shows that the relative versions of Conjectures 1, 1* and 1** (i.e., where $\mathbb{Q}$ is replaced by a totally real extension) do not hold.

EXAMPLE: Let E/F be a nontrivial Galois extension of totally real number fields, unramified at all (non-Archimedean) places. Such an extension can be constructed by taking F to be any totally real number field with odd class number > 1 (for example, for $F = \mathbb{Q}(\sqrt{142})$ we have $h_F = 3$) and E to be its Hilbert class field. Our objective is to construct a finite subgroup Γ of $GL_n(E)$, for suitable n, which will be invariant with respect to $\mathcal{G} = \mathrm{Gal}(E/F)$ but will not be in $GL_n(F)$. The key to constructing such a group lies in the proof of Proposition 4.18. Namely, suppose we could construct an n-dimensional vector space V over F provided with a positive definite quadratic form f, and two free latices $L, M \subset V$ over the ring of integers $\mathcal{O}_F$ satisfying

(1) $\mathcal{O}_E L = \mathcal{O}_E M$,
(2) L and M are nonisometric, i.e., there is no g in $\mathbf{O}_n(f)$ for which $g(L) = M$.

Then, arguing as in the proof of Proposition 4.18, we can show that

$$\Gamma = \mathbf{O}_{2n}(f \perp f)_{\mathcal{O}_E}^{\mathcal{O}_E L \perp \mathcal{O}_E M} \subset GL_{2n}(E)$$

is the desired group. To construct free lattices L, M satisfying (1) and (2) we proceed as follows. Let V_0 denote the group ring $F[\mathcal{G}]$; introduce the scalar product on V_0 for which the elements of $\mathcal{G}$ form an orthonormal base. Furthermore, define the action of $\mathcal{G}$ on $EV_0 = E[\mathcal{G}]$ by

$$g(\sum_h a_h h) = \sum_h g(a_h)(gh).$$

Lastly, put $L_0 = \perp_{g \in \mathcal{G}} \mathcal{O}_F g$ and $M_0 = (\mathcal{O}_E L_0)^{\mathcal{G}}$ (the fixed points). L_0 and M_0 have the following properties:

(i) $\mathcal{O}_E L_0 = \mathcal{O}_E M_0$;
(ii) M_0 is $\mathcal{O}_F$-indecomposable, i.e., cannot be written as an orthogonal direct sum of nontrivial $\mathcal{O}_F$-sublattices;
(iii) $L_0^m = L_0 \perp \ldots \perp L_0$ and $M_0^m = M_0 \perp \ldots \perp M_0$ are non-isometric, for any $m \geq 1$.

To prove (i) we must recall several results from ramification theory (cf., for example, Lang [2, Ch. 3]). E/F being unramified at all points is equivalent to the discriminant ideal $D_{E/F}$ being $\mathcal{O}_F$, where $D_{E/F}$ is defined as the ideal in $\mathcal{O}_F$ generated by the discriminants of all bases $a_1, \ldots, a_n$ of E over F (i.e., by the square determinants $\det(g_i(a_j))^2$, where $\mathcal{G} = \{g_1, \ldots, g_n\}$), contained in $\mathcal{O}_E$. Since $D_{E/F} = \mathcal{O}_F$, then for any w in V_f^E there are $a_1, \ldots, a_n$ in $\mathcal{O}_E$ such that $\det(g_i(a_j))$ is the unit of $\mathcal{O}_{E_w}$. Consider the

elements $x_i = \sum_{g\in\mathcal{G}} g(a_i)g \in M_0$ (where $i = 1,\dots,n$). It follows from our construction that all g in $\mathcal{G}$ can be expressed as linear combinations of the x_i with coefficients from $\mathcal{O}_{E_w}$; hence $\mathcal{O}_{E_w}L_0 = \mathcal{O}_{E_w}M_0$. Since this equality holds for any w in V_f^E, necessarily $\mathcal{O}_E L_0 = \mathcal{O}_e M_0$ (cf. §1.5).

Now we prove (ii). Suppose, on the contrary, that $M_0 = M_1 \perp M_2$; then

$$\mathcal{O}_E L_0 = \mathcal{O}_E M_0 = \mathcal{O}_E M_1 \perp \mathcal{O}_E M_2.$$

In particular, each g in $\mathcal{G}$ can be written as $g = g_1 + g_2$, where $g_i \in \mathcal{O}_E M_i$. In this case we obtain the relation

$$1 = f(g) = f(g_1) + f(g_2),$$

from which it follows that $|f(g_i)|_w \leq 1$ for each real valuation w of E $(i = 1, 2)$. But $f(g_i) \in \mathcal{O}_E$; therefore for $f(g_i) \neq 0$ we must have

$$\prod_{w\in V_\infty^E} |f(g_i)|_w = |N_{E/\mathbb{Q}}(f(g_i))| \geq 1.$$

It follows that $f(g_i)$ is always either 0 or 1, i.e., g lies in one of the components $\mathcal{O}_E M_i$. But $M_i \subset M_0 = (\mathcal{O}_E L_0)^{\mathcal{G}}$, so each component must be $\mathcal{G}$-invariant, and eventually one of the components will coincide with M_0 and the other will reduce to zero, proving (ii).

Lastly, let $t\colon L_0^m \to M_0^m$ be an isometry. Fix some element g in $\mathcal{G}$, and put $L_1 = \mathcal{O}_F g$ and $L_2 = (\perp_{h\neq g} \mathcal{O}_F h) \perp L_0^{m-1}$. Then $L_0^m = L_1 \perp L_2$ and therefore we must have $M_0^m = t(L_1) \perp t(L_2)$. Now consider an element $t(g) \in M_0^m$ and write $t(g) = x_1 + \cdots + x_m$, where $x_i \in M_0$. Applying f, we obtain

$$1 = f(t(g)) = f(x_1) + \cdots + f(x_m).$$

Therefore, arguing as above, we conclude that $t(g)$ lies in one of the components M_0 of M_0^m. But then $M_0 = t(L_1) \perp (M_0 \cap t(L_2))$, which contradicts M_0 being indecomposable.

To complete our construction it remains to choose m such that L_0^m and M_0^m will be free. To do so it suffices to set m equal to the exponent of the ideal class group of F. Indeed, any lattice L in K^n can be written as $L = \mathcal{O}x_1 \oplus \cdots \oplus \mathcal{O}x_{n-1} \oplus \mathfrak{a}x_n$, where $\mathfrak{a}$ is an ideal of $\mathcal{O}$ (cf. §1.5.3). Then L^m can be written as $\mathcal{O}y_1 \oplus \cdots \oplus \mathcal{O}y_{mn-1} \oplus \mathfrak{a}^m y_m$. But $\mathfrak{a}^m$ is a principal ideal, and therefore L^m is free.

It is worth noting that this example is based on the existence of extensions unramified at all points. Therefore, by Hermite's theorem, this approach cannot be carried out over $\mathbb{Q}$.

BIBLIOGRAPHICAL NOTE: The basic results of reduction theory are due to Borel and Harish-Chandra [2]. The proof of the criterion for compactness of $G_{\mathbb{R}}/G_{\mathbb{Z}}$ presented here is due to Mostow and Tamagawa [1]. The finite presentability of arithmetic groups (Theorem 4.2) was deduced from the existence of fundamental sets for these groups by Behr [1]. The Density Theorem was proved by Borel in [5]. Our exposition of reduction theory makes no pretentions of being complete. A more comprehensive exposition may be found in Borel [7] and in his lecture notes [6]. Humphreys [2] provides an elementary introduction to reduction theory. As we have mentioned, the origins of the general theory of reduction lie in the reduction theory of quadratic forms, a modern exposition of which may be found in Cassels [1]. The material in §4.8 is less traditional. The main results here are due to Bartels [1], [2], Kitaoka [1], [2] and Bartels-Kitaoka [1].

5. Adeles

In this chapter we introduce adele groups, a concept which plays a central role in the arithmetic theory of algebraic groups. Just as the basic results of class field theory can be expressed in terms of adeles and their cohomology, so too the results of noncommutative arithmetic can be expressed in terms of adele groups of algebraic groups and their related constructions and concepts. Therefore we shall work with adeles for the remainder of the book. This chapter contains basic results on adele groups. In §5.1 we define the adele group G_A of a linear algebraic group G over a number field K, and provide it with the corresponding (adele) topology, with respect to which the group of K-rational points G_K is a discrete subgroup of G_A. The problem arises of constructing a reduction theory for G_A relative to G_K. We solve this problem in §§5.2–5.3. Some of the results here (such as the criterion for compactness of G_A/G_K) are completely analogous to the corresponding results in Chapter 4 and, indeed, essentially rely on those results. Other results have a specifically adelic nature. First and foremost of these is Theorem 5.1, an important theorem asserting the finiteness of the number of cosets $G_{A(\infty)}xG_K$ in the decomposition of G_A modulo the subgroups of integral and principal adeles, respectively. This number, called the *class number* of G, is a very important arithmetic invariant of G, and its computation is closely related to classical number-theoretic problems (cf. Ch. 8). Another invariant that we encounter here—the *Tamagawa number* of G, denoted as $\tau(G)$—equals the volume of G_A/G_K, for G semisimple. In §5.4 we use results from reduction theory to carry over structural results on arithmetic subgroups (cf. §4.4) to arbitrary S-arithmetic groups.

5.1. Basic definitions.

Let us introduce the concept of the adele space X_A of an arbitrary variety X over an algebraic number field K. To do so, we first assume X affine and fix its presentation as a K-closed subset of some affine space $\mathbb{A}^n$. Then, by definition, X_A consists of the points of X over the adele ring $A = A_K$ of K (cf. §1.2). In other words, the elements of X_A are n-tuples $(a_1, \dots, a_n)$ of adeles that satisfy all the equations defining X. It is natural to endow X_A with the topology induced by the direct product topology on $\mathbb{A}^n = \mathbb{A} \times \cdots \times \mathbb{A}$. The same object can be constructed by means of the restricted topological product (cf. §3.5). In fact, considering the projection $\pi_v\colon A \to K_v$ on the v-component and its n-dimensional extension $\pi_v^n\colon A^n \to K_v^n$, we see that the projection $\pi_v^n(x)$ of any point x in X_A lies in X_{K_v}, for any v in V^K; moreover, for all but a finite number of v, this projection actually falls in the set of $\mathcal{O}_v$-points $X_{\mathcal{O}_v}$.

It is easy to see that one can reverse this procedure, i.e., one can define a

point x in X_A by specifying its projections $\pi_v^n(x)$ provided that the latter lie in $X_{\mathcal{O}_v}$ for almost all v. Thus, X_A is a restricted topological product of the spaces X_{K_v} with respect to the distinguished open subspaces $X_{\mathcal{O}_v}$, in the topological as well as the set-theoretic sense. It follows that X_A can be written as the union

$$X_A = \bigcup_S X_{A(S)} \tag{5.1}$$

taken over all finite subsets S of V^K containing V_∞^K, of the spaces of S-integral adeles $X_{A(S)} = \prod_{v\in S} X_{K_v} \times \prod_{v\notin S} X_{\mathcal{O}_v}$. (If $S = V_\infty^K$, then we just have integral adeles, denoted $X_{A(\infty)}$.) Moreover, the topology on $X_{A(S)}$ is the usual direct product topology, and the topology on X_A is the inductive-limit topology.

The diagonal embedding $K \to A$ (cf. §1.2) induces a diagonal embedding of the set of K-points X_K into X_A; the image of this embedding, which as a rule we shall identify with X_K, is called the *space of principal adeles*. Note that since K is discrete in A, it follows that K^n is discrete in A^n; hence X_K is discrete (and closed) in X_A.

The next step in substantiating the construction of adeles is to prove their independence of the choice of a geometric realization of X. To this end we introduce the concept of adelization of a regular K-map $f\colon X \to Y$ of two affine closed K-subsets $X \subset \mathbb{A}^n$, $Y \subset \mathbb{A}^m$. As we know, f induces a continuous map $f_{K_v}\colon X_{K_v} \to Y_{K_v}$, for any v in V^K. Consider the product $\prod_v f_{K_v}$ taken over all v, and let f_A denote its restriction to X_A.

LEMMA 5.1. *$f_A(X_A) \subset Y_A$, and $f_A\colon X_A \to Y_A$ is continuous.*

PROOF: In coordinates f has the form

$$(x_1, \dots, x_n) \mapsto (f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)),$$

where the f_i's are polynomials with coefficients from K. Let S_0 denote a finite subset of V^K containing V_∞^K, such that the coefficients of all the f_i's are v-integers for $v \notin S_0$. Then clearly $f_{K_v}(X_{\mathcal{O}_v}) \subset Y_{\mathcal{O}_v}$ for $v \notin S_0$, and therefore $f_A(X_{A(S)}) \subset Y_{A(S)}$ for any subset S of V^K containing S_0. Furthermore, in view of the fact that $X_{A(S)}$ inherits the direct product topology, we conclude that $f_A\,|_{X_{A(S)}}$ is continuous. It remains to use the fact that X_A and Y_A can be written in the form (5.1). The lemma is proved.

From Lemma 5.1 we easily obtain

PROPOSITION 5.1. *Let $f\colon X \to Y$ be a biregular K-isomorphism of two closed K-subsets $X \subset \mathbb{A}^n$, $Y \subset \mathbb{A}^m$. Then $f_A\colon X_A \to Y_A$ is a homeomorphism.*

Indeed, if $f\colon Y \to X$ is a regular K-map which is the inverse of f, then by Lemma 5.1 $g_A\colon Y_A \to X_A$ is a continuous map which is obviously the inverse of f_A.

The definitions presented above suffice for linear algebraic groups, in most cases. However, we shall need several more paragraphs to define the adele space X_A for an arbitrary K-variety X and to substantiate the definition. This will enable us to give a reasonably complete exposition, while also describing an approach which is used to obtain results of interest even in the affine case.

Thus, let X be an arbitrary K-variety. To define X_A we need to specify an open compact subset $X_{\mathcal{O}_v}$ of X_{K_v} consisting of v-adic integral points for each $v \in V_f^K$, and to construct the restricted topological product of X_{K_v} relative to $X_{\mathcal{O}_v}$. To define $X_{\mathcal{O}_v}$ we use a finite covering $X = \bigcup X_i$ of X by open affine K-sets X_i. (Such a covering exists by definition of a variety.) Furthermore, fix a biregular K-isomorphism $f_i\colon X_i \to X_i^0$ to a K-closed subset X_i^0 of $\mathbb{A}^{n_i}$, for each i. Then, define

$$X_{\mathcal{O}_v} = \bigcup_i f_i^{-1}(X^0_{i\mathcal{O}_v})$$

for any $v \in V_f^K$, and take X_A to be the corresponding restricted product. (Equivalently, one can set $X_A = \bigcup_i f_{iA}^{-1}(X_{iA}^0)$, where $f_{iA}^{-1}(X_{iA}^0)$ is viewed as a subset of $\prod_v X_{K_v}$.) The proof that this construction is invariant rests on generalizing Lemma 5.1 to the case of arbitrary varieties.

LEMMA 5.2. *Let $f\colon X \to Y$ be a K-morphism of arbitrary K-varieties. Then $f_A(X_A) \subset Y_A$ and $f_A\colon X_A \to Y_A$ is continuous.*

(Note that, just as in the affine case, the adelization of f_A of f is defined as the restriction to X_A of $\prod_v f_{K_v}$.)

PROOF: As in the proof of Lemma 5.1, we only need to justify the fact that $f(X_{\mathcal{O}_v}) \subset Y_{\mathcal{O}_v}$ for almost all v. Since by definition $X_{\mathcal{O}_v} = \bigcup_i f_i^{-1}(X^0_{i\mathcal{O}_v})$ is a finite union, it suffices to show that

$$(f \circ f_i^{-1})(X^0_{i\mathcal{O}_v}) \subset Y_{\mathcal{O}_v}$$

for any i and almost all v. Without loss of generality we may assume $i = 1$, i.e., X is affine. Let $Y = \bigcup Y_j$ be the finite affine covering used to define $Y_{\mathcal{O}_v}$. Fix embeddings $X \subset \mathbb{A}^n$ and $Y_j \subset \mathbb{A}^{n_j}$ in the corresponding affine spaces, denoting the corresponding coordinates by $x_1, \dots, x_n$; $y_1^j, \dots, y_{n_j}^j$. Then f can be described by expressing the y_k^j's as rational functions of the x_i's:

$$y_k^j = \varphi_k/\psi, \quad k = 1, \dots, n_j, \tag{5.2}$$

for any j, where φ_k, ψ belong to the ring of regular K-functions $K[X]$. Clearly the presentation in (5.2) is not unique. Therefore, in order to consider all presentations, take the ideal of possible denominators

$$\mathfrak{a}_j = \{\, \psi \in K[X] : \psi y_k^j \in K[X] \quad \text{for all } k = 1, \dots, n_j \,\}$$

for each j. The image $f(x)$ of any point x in X lies in one of the Y_j. This means that for each x in X there is an index j for which all the functions y_k^j $(k = 1, \dots, n_j)$ are defined at x, i.e., there is a presentation $y_k^j = \varphi_{kx}/\psi_x$ of the form (5.2) satisfying $\psi_x(x) \neq 0$. Hence the ideal in $K[X]$ generated by all the $\mathfrak{a}_j$ has no zeros on X, and therefore is $K[X]$ (by virtue of Hilbert's Nullstellensatz, cf. Humphreys [1].) Thus, there exist ψ_j in $\mathfrak{a}_j$ such that $\sum \psi_j = 1$. Choose the corresponding presentation $y_k^j = \varphi_k^j/\psi_j$ of the form (5.2), and let Φ_k^j and Ψ_j be polynomials in $K[x_1, \dots, x_n]$ representing φ_k^j and ψ_j. Then the coefficients of these polynomials are integers relative to v, for almost all $v \in V_f^K$. We claim that $f(X_{\mathcal{O}_v}) \subset Y_{\mathcal{O}_v} = \bigcup Y_{j\mathcal{O}_v}$ holds for such v. Indeed, let $x \in X_{\mathcal{O}_v}$. Since $\psi_j(x) \in \mathcal{O}_v$ for any j, and $\sum \psi_j(x) = 1$, all the $\psi_j(x)$ cannot lie in the maximal ideal $\mathfrak{p}_v$ of $\mathcal{O}_v$. Therefore there is a j for which $\psi_j(x)$ is invertible in $\mathcal{O}_v$. But then the corresponding values of y_k^j clearly lie in $\mathcal{O}_v$, i.e., $f(x) \in Y_{j\mathcal{O}_v}$, as desired, proving the lemma.

PROPOSITION 5.2. *Let $f: X \to Y$ be a K-isomorphism of K-varieties. Then $f_A: X_A \to Y_A$ is a homeomorphism. In particular, X_A is independent of the choice of an affine covering.*

The first assertion follows immediately from Lemma 5.2 (cf. proof of Proposition 5.1). The second assertion follows from the first, if we consider two affine coverings of X and take f to be the identity map between the two copies of X endowed with these respective coverings. It follows, in particular, that our two definitions of the adele space are equivalent for affine varieties.

There is, however, one essential topological difference between the general case and the affine case. A principal adele space X_K, whose definition is perfectly analogous to the one given in the affine case, is not discrete in X_A, in general. For example, X_A is compact for X projective, and therefore X_K cannot be discrete in X_A if it is infinite.

Let us note one other curious corollary of Proposition 5.2.

LEMMA 5.3. *Let $X = \bigcup X_i$ be an arbitrary covering of a K-variety X by open K-varieties X_i. Then $X_A = \bigcup X_{iA}$.*

Indeed, taking a finite subcovering of the given open covering, we may assume without loss of generality that the original covering is finite. It follows from the definition of X_A that the assertion holds for affine varieties X_i. To prove the assertion in general, consider for each i some finite open affine covering $X_i = \bigcup_k X_{ik}$ of X_i. Then $X = \bigcup_{i,k} X_{ik}$ is an open affine covering of X. Since, by Proposition 5.2 the definition of X_A is independent of the choice of affine covering, we have $X_A = \bigcup_{i,k} X_{ikA}$. On the other hand, similarly $X_{iA} = \bigcup_k X_{iKA}$ for each i, hence the desired result follows.

Note that the openness of every X_i is essential for the validity of the lemma. Indeed, consider $\mathbb{A}^1 = X \cup Y$, where $X = \mathbb{A}^1 \setminus (0)$, $Y = \{(0)\}$. Then X is biregularly isomorphic to the hyperbola $\{\, (x, y) \in \mathbb{A}^2 : xy = 1 \,\}$, from which it follows that X_A is the set of all ideles J, and $Y_A = \{(0)\}$. Therefore $\mathbb{A}_A^1 = A \neq X_A \cup Y_Z$. (A helpful exercise, which we recommend to the reader, is to explain what part of the proof of Lemma 5.3 falls through if we do not assume the covering $\{X_i\}$ to be open.)

We shall also need

LEMMA 5.4. *Let Y be a closed K-subvariety of X. Then $Y_A = X_A \cap \prod_v Y_{K_v}$. Moreover, the topology on Y_A is induced from that on X_A.*

PROOF: Let $X = \bigcup_i X_i$ be an open affine covering of X. Then

$$Y = \bigcup_i (Y \cap X_i)$$

is an open affine covering of Y. By the above definition $Y_A = \bigcup_i (Y \cap X_i)_A$. But the lemma clearly holds for a closed subset of an affine variety. (To see this, it suffices to consider an arbitrary embedding of X as a closed subset of an affine space; then we immediately obtain a closed embedding of Y, and the required result follows directly from the definitions.) Therefore

$$(Y \cap X_i)_A = X_{i_A} \cap \prod_v (Y \cap X_i)_{K_v} = X_{i_A} \cap \prod_v Y_{K_v}$$

for any i; hence

$$Y_A = \bigcup_i (Y \cap X_i)_A = \bigcup_i (X_{i_A} \cap \prod_v Y_{K_v}) = (\bigcup_i X_{i_A}) \cap \prod_v Y_{K_v} = X_A \cap \prod_v Y_{K_v}.$$

The proof that the topology on Y_A is induced from X_A is left as an exercise for the reader (cf. proof of the continuity of f_A in Lemma 5.1).

EXERCISE: Show that if $X = Y \times Z$ then $X_A = Y_A \times Z_A$ as a topological space.

When working with adelizations of varieties and their morphisms it is helpful to know which of the most commonly used properties are retained when we pass to adele spaces. It is obvious, for example, that the surjectivity of $f: X \to Y$ is not sufficient for the surjectivity of the corresponding adelization $f_A: X_A \to Y_A$ (example?). Nevertheless, if Y is an irreducible variety and the morphism $f_F: X_F \to Y_F$ of corresponding F-points is surjective for every extension F/K, then f_A is also surjective. Indeed, applying surjectivity to the field $F = K(Y)$ of K-rational functions on Y, we obtain that for any y in Y there is a local section of f defined at y, i.e., a rational K-morphism $g_y: Y \to X$ for which $f \circ g_y = \mathrm{id}_Y$. Then we can use the following assertion:

PROPOSITION 5.3. *Let $f: X \to Y$ be a K-morphism of K-varieties. If there is a local section (over K) of f defined at y, for each y in Y, then $f_A: X_A \to Y_A$ is surjective.*

PROOF: It follows from our assumptions that there exists an open covering $Y = \bigcup Y_j$ and K-subvarieties X_j of X such that f induces a K-isomorphism of X_j onto Y_j. (Indeed, it suffices to take for Y_j the domains of definition of appropriate local sections, and for X_j, their images.) Then, by Proposition 5.2 and Lemma 5.3 we have

$$f_A(X_A) \supset \bigcup_j f_A(X_{j_A}) = \bigcup_j Y_{j_A} = Y_A.$$

Later on we shall encounter various properties of the adelization of morphisms time and again, however for the time being we shall leave off our discussion of adelic points of arbitrary varieties and move on to the more important case (for us) of linear algebraic groups.

Now, let G be a linear algebraic K-group. Then G can be realized as a closed K-subgroup of some full linear group $\mathbf{GL}_n$, and by Lemma 5.4 in order to describe G_A it actually suffices to describe $\mathbf{GL}_{n_A}$. For this, consider the standard realization of $\mathbf{GL}_n$ as a hypersurface in $\mathbb{A}^{n^2+1}$:

$$\mathbf{GL}_n \simeq \{(x_{11}, \ldots, x_{nn}, y) \in \mathbb{A}^{n^2+1} : y \det(x_{ij}) - 1 = 0\}.$$

Then GL_{n_A} is the set of all matrices of $M_n(A)$ whose determinant is invertible in the adele ring A, i.e., is $GL_n(A)$. To view GL_{n_A} in terms of the restricted topological product, note also that $GL_{n_{\mathcal{O}_v}}$ is precisely $GL_n(\mathcal{O}_v)$, so $GL_{n_A} = GL_n(A)$ is the restricted topological product of the $GL_n(K_v)$ with respect to the distinguished subgroups $GL_n(\mathcal{O}_v)$ for $v \in V_f^K$. In other words, GL_{n_A} is the set of all $g = (g_v) \in \prod_v GL_n(K_v)$ for which $g_v \in GL_n(\mathcal{O}_v)$ for almost all $v \in V_f^K$. The topology on GL_{n_A} appears as follows: a base of open sets is comprised of sets of the form

$$U = \prod_{v \in S} U_v \times \prod_{v \notin S} GL_n(\mathcal{O}_v), \tag{5.3}$$

where S is a finite subset of V^K containing V_∞^K whose elements index some open subsets $U_v \subset GL_n(K_v)$. (In order to unify notation, some authors put $\mathcal{O}_v = K_v$ for $v \in V_\infty^K$; we, however, will not do this.) The subgroup $GL_{n_{A(S)}} = GL_n(A(S)) = \prod_{v \in S} GL_n(K_v) \times \prod_{v \notin S} GL_n(\mathcal{O}_v)$ is called the *group of S-integral adeles*; for $S = V_\infty^K$ the group $GL_{nA(S)}$ is denoted by $GL_{n_{A(\infty)}}$ and is called the *group of integral adeles*. GL_{n_K} embeds diagonally in GL_{n_A}, and its image, which we shall usually identify with it, is called the *group of principal adeles*; GL_{n_K} is a discrete subgroup of GL_{n_A}. Our detailed discussion of basic adelic concepts relating to $\mathbf{GL}_n$ is intended for the reader for whom this is the first encounter with adeles of algebraic groups. We recommend that such a reader also see Humphreys [2, Ch. 5], which presents an introduction to the general theory of adelic groups, just using the examples of $\mathbf{GL}_n$ and $\mathbf{SL}_n$.

Now the above definitions can easily be extended to an arbitrary closed subgroup G of $\mathbf{GL}_n$. Namely, the adele group G_A is defined as the restricted topological product of all G_{K_v} with respect to the distinguished subgroups $G_{\mathcal{O}_v} = G \cap GL_n(\mathcal{O}_v)$ for $v \in V_f^K$, i.e., G_A consists of sets of $g = (g_v) \in \prod_v G_{K_v}$ such that $g_v \in G_{\mathcal{O}_v}$ for almost all $v \in V_f^K$. The topology on G_A is induced from GL_{n_A} and therefore its base is comprised of sets analogous to (5.3). G_A is a locally compact topological group under this topology, and the subgroup G_K of principal adeles (i.e., the group of K-rational points of G_K diagonally embedded in G_A) is a discrete subgroup of G_A. The subgroup of S-integral adeles $G_{A(S)} = G_S \times \prod_{v \notin S} G_{\mathcal{O}_v}$, where $G_S = \prod_{v \in S} G_{K_v}$, is defined for any finite subset S of V^K containing V_∞^K. (Obviously $G_{A(S)}$ is open in G_A.) For $S = V_\infty^K$ we write $G_{A(\infty)}$, G_∞ instead of $G_{A(V_\infty^K)}$, $G_{V_\infty^K}$. Note that $G_{\mathcal{O}_v}$, and hence the group $G_{A(\infty)}$ of integral adeles, depend on the choice of matrix realization of G. Therefore, to emphasize that integral points are taken with respect to a lattice $L \subset K^n$, we shall write $G^L_{A(\infty)}$, by which we mean $G_\infty \times \prod_{v \in V_f^K} G^{L_v}_{\mathcal{O}_v}$, where L_v is the corresponding localization of L (cf. §4.5.3).

Sometimes it is useful (and necessary) to consider "truncated" adeles. More precisely, let S be an arbitrary subset of V^K. Then the group of S-adeles G_{A_S} (adeles without S components) of an algebraic K-group G

is defined as the image of G_A under the natural projection of $\prod_v G_{K_v}$ onto $\prod_{v\notin S} G_{K_v}$. Thus G_{A_S} consists of collections of $g=(g_v)\in \prod_{v\notin S} G_{K_v}$ such that $g_v\in G_{\mathcal{O}_v}$ for almost all $v\in V_f^K\setminus(V_f^K\cap S)$, and also is the restricted product of the G_{K_v} for $v\notin S$ with respect to the subgroups $G_{\mathcal{O}_v}$ $(v\in V_f^K\setminus(V_f^K\cap S)$, both in the set-theoretic and the topological sense. As in the case of full adele groups, one can consider for S-adeles the diagonal embedding $G_K\hookrightarrow G_{A_S}$, whose image is called the *group of principal S-adeles*. Moreover, one can define the group of T-integral S-adeles $G_{A_S(T)}=\prod_{v\in T\setminus S} G_{K_v}\times\prod_{v\notin T} G_{\mathcal{O}_v}$ for any subset T of V^K containing S. $G_{A_{V_\infty^K}}$ is denoted by G_{A_f} and is called the *group of finite adeles*; instead of $G_{A_f(V_\infty^K)}$ we shall write $G_{A_f(\infty)}$. With this terminology, we introduce the following important

DEFINITION: G is said to satisfy the *strong approximation property* relative to S (or *absolute strong approximation property* when $S=V_\infty^K$) if the image under the diagonal embedding $G_K\hookrightarrow G_{A_S}$ is dense (in terms of the full adele group this means that G_KG_S, where $G_S=\prod_{v\in S} G_{K_v}$, is dense in G_A).

Similarly, there is the concept of a space of S-adeles and a definition of strong approximation for arbitrary algebraic varieties (moreover, there are analogs to all the above results of this section). However, while the criterion of strong approximation is known for the case of algebraic groups (cf. §7.4), this property has only recently begun to be investigated for arbitrary varieties (cf. Minchev [1], Rapinchuk [8]). Nevertheless, with the concept itself of strong approximation for arbitrary varieties we can obtain several simplifications, as in the proof of the following assertion.

LEMMA 5.5. *Let U be a unipotent group defined over K. Then U satisfies the strong approximation property relative to any nonempty set S.*

The proof rests on the following straightforward remark. If two K-varieties X and Y are biregularly isomorphic over K, then $X_K\simeq Y_K$, $X_{A_S}\simeq Y_{A_S}$ for any S; therefore either both X and Y satisfies the strong approximation property, or neither X nor Y satisfy this property. (Question: is the strong approximation property preserved under birational K-isomorphisms?) In our case U is biregularly isomorphic to an affine space (namely, the corresponding Lie algebra $L(U)$, cf. §2.1.8); therefore it suffices to establish strong approximation for an affine space, where it follows directly from the strong approximation theorem for K (cf. §1.2). The lemma is proved.

Another important concept concerns the subgroups $G_{A(\infty)}$ and G_K of

integral and principal adeles. Consider a decomposition

$$G_A=\bigcup_{i=1}^{h} G_{A(\infty)}x_iG_K$$

of G_A into double cosets modulo these subgroups. We call h the *class number* of G and denote it by $\mathrm{cl}(G)$. The following theorem is one of the most important results in this chapter.

THEOREM 5.1. *$\mathrm{cl}(G)$ is always finite.*

We shall deal with computation and estimation of $\mathrm{cl}(G)$ in Chapter 8. There we shall see, in particular, that most of the well-known finiteness results follow from Theorem 5.1—namely, finiteness of the class number of a field, finiteness of the number of classes in the genus of a quadratic form, etc. Theorem 5.1 is a corollary of the reduction theory for adele groups, which we shall set forth in §§5.2–5.3. In the remainder of this section we shall present several straightforward assertions which enable us to reduce the proof of Theorem 5.1 to the case of a connected reductive group over $\mathbb{Q}$.

PROPOSITION 5.4. *Let $G=HN$ be a semidirect product, where N is a normal subgroup (everything defined over K). Assume N satisfies the absolute strong approximation property. Then $\mathrm{cl}(G)\le\mathrm{cl}(H)$. In particular, the class number for a group with absolute strong approximation is always equal to one.*

The proof uses

LEMMA 5.6. *Under the above assumptions, N_A is a normal subgroup of G_A and $G_A=H_AN_A$ is a semidirect product.*

PROOF: As in Lemma 5.5. Since $G\simeq H\times N$, viewed as a variety, $G_A\simeq H_A\times N_A$, i.e., $G_A=H_AN_A$. The assertion that N_A is normal in G_A is obvious.

The subgroup $x^{-1}N_{A(\infty)}x$ is open in N_A, for any x in G_A. But, since N satisfies absolute strong approximation, $N_\infty N_K$ is dense in N_A. Therefore the open set $(x^{-1}N_{A(\infty)}x)y$ must intersect $N_\infty N_K$, for any y in N_A; hence

$$N_A=(x^{-1}N_{A(\infty)}x)N_\infty N_K=(x^{-1}N_{A(\infty)}x)N_K, \tag{5.4}$$

since N_∞ is a normal subgroup of G_A contained in $N_{A(\infty)}$. Setting $x=1$ we obtain $N_A=N_{A(\infty)}N_K$, so it follows from (5.4) that

$$xN_{A(\infty)}N_K=N_{A(\infty)}xN_K$$

for any x in G_A. Therefore, using Lemma 5.6, we obtain

$$G_A = H_A N_A = H_A N_{A(\infty)} N_K = N_{A(\infty)} H_A N_K.$$

Now if $H_A = \bigcup_i H_{A(\infty)} x_i H_K$, then $G_A = \bigcup_i N_{A(\infty)} H_{A(\infty)} x_i H_K N_K = \bigcup_i G_{A(\infty)} x_i G_K$, which yields the required result, completing the proof of Proposition 5.4.

PROPOSITION 5.5. *Let G be an algebraic K-group, and let G^0 be the connected component of the identity. Then the quotient group G_A/G_A^0 is compact.*

PROOF: Since G^0 has finite index in G, there is a finite subset C_v of G such that $G_{K_v} = C_v G^0_{K_v}$, for any v. Moreover, as we shall show below, such a subset can be found in $G_{\mathcal{O}_v}$ for almost all $v \in V_f^K$. In this case $C = \prod_v C_v$ lies in $G_{A(S)}$ for a suitable finite S, and consequently it is compact in the adele topology, since this topology on $G_{A(S)}$ is precisely the direct product topology. On the other hand, clearly $G_A = C G_A^0$, yielding the desired result.

Thus it remains to be shown that $G_{K_v} = G_{\mathcal{O}_v} G^0_{K_v}$ for almost all $v \in V_f^K$. To do so, we shall use the following result, which we shall prove in §6.2: if H is a connected algebraic group over an algebraic number field K, and L/K is a finite Galois extension, then $H^1(L_w/K_v, H_{\mathcal{O}_{L_w}}) = 1$ for almost all $v \in V_f^K$ and $w|v$, where O_{L_w} is the ring of w-adic integers in L_w. In our case there exists a finite Galois extension L/K and a finite subset C of G_L such that $G = CG^0$. Excluding from consideration a finite number of $v \in V_f^K$, we may assume that $G \xrightarrow{\pi} G/G^0$ is defined over $\mathcal{O}_v$, and for any $w|v$ we have $C \subset G_{\mathcal{O}_{L_w}}$ and $H^1(L_w/K_v, G^0_{\mathcal{O}_{L_w}}) = 1$. In particular, we have the exact sequence

$$1 \to G^0_{\mathcal{O}_{L_w}} \to G_{\mathcal{O}_{L_w}} \to (G/G^0)_{\mathcal{O}_{L_w}} \to 1. \tag{5.5}$$

Using the cohomology sequence derived from (5.5) (cf. (1.12) in §1.3), we obtain $\pi(G_{\mathcal{O}_v}) = (G/G^0)_{\mathcal{O}_v}$. But by assumption $(G/G^0)_{\mathcal{O}_{L_w}} = (G/G^0)_{L_w}$, from which it follows that $(G/G^0)_{\mathcal{O}_v} = (G/G^0)_{K_v}$. Therefore $\pi(G_{K_v}) \subset (G/G^0)_{K_v} = (G/G^0)_{\mathcal{O}_v} = \pi(G_{\mathcal{O}_v})$, and hence $G_{K_v} = G_{\mathcal{O}_v} G^0_{K_v}$, completing the proof of the proposition.

Lastly, we shall look at the way restriction of scalars works for adeles (cf. §2.1.2). Let G be a linear algebraic group defined over K, and let $[K : \mathbb{Q}] = d$. Fix a base $\mathfrak{a} = w_1, \ldots, w_d$ of the ring of integers $\mathcal{O}$ over $\mathbb{Z}$, and using this base construct $H = \mathbf{R}_{K/\mathbb{Q}}(G)$. In § 2.1.2 we noted that for any prime number p we have compatible isomorphisms

$$H_{\mathbb{Q}_p} \simeq \prod_{v|p} G_{K_v}, \tag{5.6}$$

$$H_{\mathbb{Z}_p} \simeq \prod_{v|p} G_{\mathcal{O}_v}, \tag{5.7}$$

and moreover

$$H_{\mathbb{R}} \simeq G_\infty. \tag{5.8}$$

This gives us

PROPOSITION 5.6. *Notation as above, there is a natural isomorphism $H_{A_\mathbb{Q}} \simeq G_{A_K}$ extending $H_\mathbb{Q} \simeq G_K$. Moreover, $H_{A_\mathbb{Q}(\infty)} \simeq G_{A_K(\infty)}$.*

Note that for another choice of base $w_1', \ldots, w_d'$ of K over $\mathbb{Q}$, H is replaced by H', which is K-isomorphic to H, and therefore also $H'_{A_\mathbb{Q}} \simeq G_{A_K}$. This is related to the fact that (5.6) and (5.8) also hold for H', and (5.7) holds for almost all p. It is clear, also, that if $w_1', \ldots, w_d'$ is not a base of $\mathcal{O}/\mathbb{Z}$, then in general $H_{A_\mathbb{Q}(\infty)} \not\simeq G_{A_K(\infty)}$.

5.2. Reduction theory for G_A relative to G_K.

Since G_K is a discrete subgroup of G_A, as we have seen in the previous section, it is natural to ask whether a reduction theory can be developed for G_A relative to G_K. In this section we shall describe construction of the corresponding fundamental sets, from which we shall deduce the proof of Theorem 5.1 as well as criteria for G_A/G_K to be compact or to have finite measure. We begin with the definition of fundamental sets for adele groups.

DEFINITION: We call a subset Ω of G_A a *fundamental set* for G_K if

(F1)$_A$ $\Omega G_K = G_A$;
(F2)$_A$ $\Omega^{-1}\Omega \cap G_K$ is finite.

The reader will undoubtedly notice the total analogy between the adelic conditions and (F1) and (F2) in the definition of a fundamental set for arithmetic groups (cf. §4.3). Indeed, the connection here runs deeper than mere similarity. The fundamental sets constructed for arithmetic groups in Chapter 4 occur as real components of adelic fundamental sets. This is readily seen from the easiest case, $G = \mathbf{GL}_n$ over $\mathbb{Q}$.

PROPOSITION 5.7. *Let $G = \mathbf{GL}_n$ over $\mathbb{Q}$ and let Σ be a fundamental set for $G_\mathbb{Z}$ in $G_\mathbb{R}$. Then $\Omega = \Sigma \times \prod_p G_{\mathbb{Z}_p}$ is a fundamental set for $G_\mathbb{Q}$ in G_A.*

PROOF: First we show that $\mathrm{cl}(G) = 1$, i.e., $G_A = G_{A(\infty)} G_\mathbb{Q}$. G can be written as a semidirect product $G = SH$, where $S = \{ \mathrm{diag}(a, 1, \ldots, 1) \}$ is a one-dimensional torus and $H = \mathbf{SL}_n$. Clearly S_A can be identified with the group $J_\mathbb{Q}$ of ideles of $\mathbb{Q}$; moreover, $S_{A(\infty)}$ corresponds to the group

$J_{\mathbb{Q}}(\infty)$ of integral ideles. Since the class number of $\mathbb{Q}$ is 1, $J_{\mathbb{Q}} = J_{\mathbb{Q}}(\infty)\mathbb{Q}^*$ (cf. §1.2.2), and consequently $S_A = S_{A(\infty)}S_{\mathbb{Q}}$, i.e., $\mathrm{cl}(S) = 1$.

On the other hand, H satisfies the absolute strong approximation property. This follows from the criterion for strong approximation which we shall establish in §7.4; however, one can also give an elementary direct proof. To do so, let U_{ij} $(i, j = 1, \dots, n;\ i \neq j)$ be the subgroup of H consisting of appropriate elementary matrices. Since U_{ij} satisfies absolute strong approximation (Lemma 5.5), the closure $\bar{H}_{\mathbb{Q}}$ of $H_{\mathbb{Q}}$ in H_{A_∞} (where A_∞ is A_S for $S = V_\infty^{\mathbb{Q}}$) contains all the $(U_{ij})_{A_\infty}$. Bearing in mind that the matrices in $(U_{ij})_L$ generate H_L, for any field L, we see that $\bar{H}_{\mathbb{Q}}$ contains all the $H_S = \prod_{p\in S} H_{\mathbb{Q}_p}$, where S is an arbitrary finite set of primes. But from the definition of the adele topology it follows that $\bigcup_S H_S$ is dense in H_{A_∞}, and therefore $\bar{H}_{\mathbb{Q}} = H_{A_\infty}$. The equality $\mathrm{cl}(G) = 1$ now follows from Proposition 5.5. (If we take $G = \mathbf{GL}_n$ over an arbitrary field K, then $\mathrm{cl}(G)$ equals the class number h_K of K; cf. §8.1).

Now we can easily complete the proof. $\Omega G_{\mathbb{Z}} = G_{\mathbb{R}} \times \prod_p G_{\mathbb{Z}_p} = G_{A(\infty)}$, since $\Sigma G_{\mathbb{Z}} = G_{\mathbb{R}}$. Therefore $\Omega G_{\mathbb{Q}} = \Omega G_{\mathbb{Z}} G_{\mathbb{Q}} = G_{A(\infty)} G_{\mathbb{Q}} = G_A$. If $g \in \Omega^{-1}\Omega \cap G_{\mathbb{Q}}$, then $g \in G_{\mathbb{Z}_p}$ for all p, and consequently $g \in G_{\mathbb{Z}}$. However, the projection onto the real component gives $g \in \Sigma^{-1}\Sigma$, and therefore there are only finitely many possibilities for g (cf. condition (F2) in the definition of a fundamental set for arithmetic subgroups, p. 193).

It is evident from the proof of Proposition 5.7 that fundamental sets of the type described there exist whenever $\mathrm{cl}(G) = 1$. Their distinctive feature is the compactness of the projection onto the non-Archimedean part. Later on we shall see that fundamental sets with this property can also be constructed in the general case; this fact is crucial for the proof of the Finiteness Theorem 5.1.

The method of constructing fundamental sets in the adele groups of arbitrary groups is similar to that used in Chapter 4 in the analogous problem for arithmetic subgroups, i.e., it is based on Lemma 4.2. The only difference is that here, instead of working with the action of a group of real points on an appropriate real vector space, we have to work with the action of an adele group on the adelization of a vector space. For this, note that any action of an algebraic K-group G on an algebraic K-variety X, i.e., a morphism $G \times X \to X$, induces a continuous map $(G \times X)_A = G_A \times X_A \to X_A$, i.e., a continuous action of G_A on the adelization X_A. Moreover, for a in $GL_n(\mathbb{R})$, we shall let a^∞ denote the adele from $GL_n(A_{\mathbb{Q}})$ with components

$$(a^\infty)_v = \begin{cases} E_n, & v \neq \infty \\ a, & v = \infty \end{cases}$$

PROPOSITION 5.8. *Let $G \subset \mathbf{GL}_n$ be a reductive $\mathbb{Q}$-group, and let Ω be the fundamental set from Proposition 5.7, corresponding to the Siegel domain $\Sigma = \Sigma_{t,v}$, $t \geq \frac{2}{\sqrt{3}}$, $v \geq \frac{1}{2}$ (cf. §4.2). Then there are a in $GL_n(\mathbb{R})$ and $b_1, \dots, b_r$ in $GL_n(\mathbb{Q})$ for which*

$$\Delta = \left(\bigcup_{i=1}^{r} a^\infty \Omega b_i \right) \cap G_A \tag{5.9}$$

is a fundamental set for $G_{\mathbb{Q}}$ in G_A.

PROOF: By Theorem 2.15 there exist a $\mathbb{Q}$-representation $\varrho\colon \mathbf{GL}_n \to \mathbf{GL}_m$ and a vector v in $\mathbb{Q}^m$ such that the $\mathbf{GL}_n$-orbit of v is closed and the isotropy subgroup is G. Let us choose a in $GL_n(\mathbb{R})$ such that $a^{-1}Ga$ is self-adjoint (Theorem 3.7). Then $v(a^\infty\Omega) \cap vGL_n(\mathbb{Q})$ is finite. (Henceforth we shall consider the action of $GL_n(A)$ on the adele space A^m induced by ϱ.) Indeed, it suffices to show that $M = v(a^\infty\Omega) \cap \mathbb{Q}^m$ is finite. It follows from the definition of Ω and the continuity of ϱ_A that the projections of all elements of $v(a^\infty\Omega)$ onto A_∞^m lie in a suitable compact set. Hence $M \subset \frac{1}{l}\mathbb{Z}^m$ for a suitable integer l. But then $lM \subset (lv)\Sigma \cap \mathbb{Z}^m$, and the latter intersection is finite by Proposition 4.5.

Now if $v(a^\infty\Omega) \cap vGL_n(\mathbb{Q}) = \{vb_1, \dots, vb_r\}$ (where $b_i \in GL_n(\mathbb{Q})$), then, applying Lemma 4.2 and taking into account Proposition 5.7, we conclude that Δ defined as in (5.9) is a fundamental set for $G_{\mathbb{Q}}$ in G_A. Proposition 5.8 is proved.

THEOREM 5.2. *Let G be a reductive algebraic group defined over an algebraic number field K. Then there exists a fundamental set for G_K in G_A having compact projection onto the non-Archimedean part.*

PROOF: Let $H = \mathbf{R}_{K/\mathbb{Q}}(G)$ be the group obtained from G by restriction of scalars. Then, by Proposition 5.8, $H_{A_{\mathbb{Q}}}$ has a fundamental set relative to $H_{\mathbb{Q}}$ of the form (5.9) which has compact projection onto the non-Archimedean part (since Ω, constructed in Proposition 5.7, has this property). Using the isomorphism $H_{A_{\mathbb{Q}}} \simeq G_A$ (cf. Proposition 5.6), we can carry it over to G_A, and this gives the desired fundamental set for G_K in G_A.

PROOF OF THEOREM 5.1, CF. PAGE 251: First, let G be connected. Consider the Levi decomposition $G = HU$, where $U = R_u(G)$ is the unipotent radical of G and H is a reductive K-group (Theorem 2.3). Then it follows from Proposition 5.4, combined with Lemma 5.5, that $\mathrm{cl}(G) \leq \mathrm{cl}(H)$, and it suffices to establish that $\mathrm{cl}(H)$ is finite. To do so we use the fundamental set $\Delta \subset H_A$ constructed in Theorem 5.2. Since Δ has compact projection on the non-Archimedean part, $\Delta \subset \bigcup_{i=1}^r H_{A(\infty)} x_i$ holds for a suitable finite set $x_1, \dots, x_r$ of elements of H_A. But then $H_A = \Delta H_K = \bigcup_{i=1}^r H_{A(\infty)} x_i H_K$ and therefore $\mathrm{cl}(H)$ is finite.

Now let G be arbitrary. Since we have already shown $\mathrm{cl}(G^0)$ to be finite, there is a finite set $x_1, \dots, x_r$ of elements of G_A^0 such that $G_A^0 = \bigcup_{i=1}^r G^0_{A(\infty)} x_i G_K^0$. However, it follows from Proposition 5.5 that there exists a compact set $D \subset G_A$ satisfying $G_A = DG_A^0$. Then D is contained in the union of a finite number of translates of $G_{A(\infty)}$, i.e., $D \subset \bigcup_{j=1}^S G_{A(\infty)} y_j$, where $y_j \in G_A$. We have

$$G_A = DG_A^0 = \bigcup_{i=1}^r \bigcup_{j=1}^S G_{A(\infty)} y_j G^0_{A(\infty)} x_i G_K^0;$$

therefore it suffices to show that for any $x, y \in G_A$ the set

$$G_{A(\infty)} y G_{A(\infty)} x G_K$$

is contained in the union of a finite number of double cosets of the form $G_{A(\infty)} z G_K$ $(z \in G_A)$. We need the following fact.

LEMMA 5.7. *$G_{A(\infty)}$ and $yG_{A(\infty)}y^{-1}$ are commensurable, for any y in G_A.*

PROOF: Let y_∞ (resp., y_f) denote the projection of y onto G_∞ (resp., onto $G_{A_f} = G_{A_{V_\infty^K}}$), and let $U = \prod_{v \in V_f^K} G_{\mathcal{O}_v}$. Then $G_{A(\infty)} = G_\infty \times U$ and $yG_{A(\infty)}y^{-1} = (y_\infty G_\infty y_\infty^{-1}) \times (y_f U y_f^{-1}) = G_\infty \times (y_f U y_f^{-1})$. But U and $y_f U y_f^{-1}$ are open compact subgroups of G_{A_f}, and therefore are commensurable. Therefore $G_{A(\infty)}$ and $yG_{A(\infty)}y^{-1}$ are also commensurable.

Thus, for any y in G_A there exists a finite set of elements $\{ z_l \}_{l=1}^t \subset G_A$ such that $yG_{A(\infty)}y^{-1} \subset \bigcup_{l=1}^t G_{A(\infty)} z_l$. Then

$$G_{A(\infty)} y G_{A(\infty)} x G_K = G_{A(\infty)} (y G_{A(\infty)} y^{-1}) y x G_K \subset \bigcup_{l=1}^t G_{A(\infty)} z_l y x G_K.$$

Q.E.D.

REMARKS: An obvious modification of the argument enables us to prove the following generalization of Lemma 5.7: if $f: G \to G'$ is a K-isomorphism, then $G'_{A(\infty)}$ and $f(G_{A(\infty)})$ are commensurable. Since

$$G_{\mathcal{O}} = G_{A(\infty)} \cap G_K,$$

we can easily obtain another proof, "topological" in nature, of Proposition 4.1 on the invariance of arithmetic subgroups.

Using Theorem 5.1 we can show that the construction of the fundamental sets in Proposition 5.7 is actually universal.

PROPOSITION 5.9. *Let G be an arbitrary K-group. If B is a fundamental set in G_∞ relative to $G_{\mathcal{O}}$ (cf. §4.7), then there is a compact subset C of G_{A_f} such that $B \times C$ is a fundamental set in G_A relative to G_K.*

PROOF: Let $G_A = \bigcup_{i=1}^r G_{A(\infty)} x_i G_K$; moreover, without loss of generality we may assume $(x_i)_\infty = e$ for all i, i.e., $x_i \in G_{A_f}$. Put $U = \prod_{v \in V_f^K} G_{\mathcal{O}_v}$ and $C = \bigcup_{i=1}^r U x_i U$. Then, bearing in mind that $G_\infty = BG_{\mathcal{O}}$, we show easily that for $\Omega = B \times C$ we have $G_A = \Omega G_K$, so $(\mathrm{F1})_A$ is satisfied.

Now we shall verify $(\mathrm{F2})_A$. Let $x \in \Omega^{-1}\Omega \cap G_K$. Projecting onto G_{A_f}, we obtain $x \in D = C^{-1}C$. Fix a matrix realization $G \subset \mathbf{GL}_n$ of G. Then D is a compact subset of $M_n(A_f)$, from which it follows easily that there is an integer d such that $d(D \cap M_n(K)) \subset M_n(\mathcal{O})$; in particular $dx \in M_n(\mathcal{O})$. Moreover, obviously $x^{-1} \in D$, and therefore also $dx^{-1} \in M_n(\mathcal{O})$. Thus, $x \in G_d = \{ g \in G_K : dx, dx^{-1} \in M_n(\mathcal{O}) \}$. Now, taking the projection onto G_∞, we obtain $x \in B^{-1}B \cap G_d$. But this intersection is finite by the obvious generalization of Lemma 4.8 to rings of algebraic integers. Proposition 5.9 is proved.

Besides proving Theorem 5.1, the construction of a fundamental set in G_A relative to G_K enables us to obtain several other important results. The results on when G_A/G_K is compact or has finite volume will be treated in the next section; however, in this section we shall develop an adelic version of Theorem 4.9.

THEOREM 5.3. *Let H be a reductive K-subgroup of a reductive K-group G. Put $X = G/H$, and let σ denote the canonical projection $G \to X$. Then $\sigma_A(G_A) \cap X_K$ consists of a finite number of orbits of G_K.*

PROOF: Consider $G' = \mathbf{R}_{K/\mathbb{Q}} G$ and $H' = \mathbf{R}_{K/\mathbb{Q}} H$, and observe that the variety $X' = \mathbf{R}_{K/\mathbb{Q}} X$ is G'/H'; then, in view of Proposition 5.6, the proof reduces easily to the case $K = \mathbb{Q}$. The rest of the argument is based on what is already a traditional application of the existence of a $\mathbb{Q}$-representation $\varrho: \mathbf{GL}_n \to \mathbf{GL}_m$ (where $G \subset \mathbf{GL}_n$) for which there is a point $v \in \mathbb{Q}^m$ with a closed orbit under $\varrho(\mathbf{GL}_n)$, whose stabilizer in $\mathbf{GL}_n$ is H. Then the orbit $Y = v\varrho(G)$ is also closed and is a geometric realization of X; i.e., there is a G-equivariant K-isomorphism $X \simeq Y$. Hence the problem reduces to proving that $v\varrho_A(G_A) \cap \mathbb{Q}^m$ consists of a finite number of orbits of $G_{\mathbb{Q}}$. But $G_A = \Delta G_{\mathbb{Q}}$, where Δ is the fundamental set obtained in Proposition 5.8; so it suffices to show that $v\varrho_A(\Delta) \cap \mathbb{Q}^m$ is finite. To do so, recall that $\Delta = (\bigcup_{i=1}^r a^\infty \Omega b_i) \cap G_A$, notation as in Proposition 5.8. The matrix a in $GL_n(\mathbb{R})$ was chosen here to satisfy a single condition: $a^{-1}Ga$ must be self-adjoint. Therefore we can make our choice more specific, adding the condition that $a^{-1}Ha$ also be self-adjoint (Theorem 3.8). Since

$b_i \in GL_n(\mathbb{Q})$,

$$v\varrho_A(\Delta) \cap \mathbb{Q}^m = \bigcup_{i=1}^{r} v\varrho_A((a^\infty \Omega b_i) \cap G_A) \cap \mathbb{Q}^m \subset v\varrho_A(a^\infty \Omega) \cap \mathbb{Q}^m.$$

But, in our proof of Proposition 5.8 (substituting H for G), we essentially showed that this intersection is finite. Q.E.D.

In Chapter 6 we shall give a cohomological interpretation of Theorem 5.3, which essentially claims that, given any algebraic K-group G, the canonical Galois cohomology map $H^1(K,G) \to \prod_v H^1(K_v,G)$ has finite kernel (cf. §6.4).

To conclude this section, we shall use Theorem 5.1 to derive an assertion on the finiteness of the number of double cosets of some special kind needed to construct fundamental sets for arithmetic subgroups (cf. §4.7). Let G be a connected K-group, and let P be a parabolic K-subgroup of G. Then $X = G/P$ is a projective variety, implying that the corresponding adele space X_A is compact. Indeed, by Lemma 5.4, it suffices to establish that for n-dimensional projective space $\mathbb{P}^n$ the adele space $\mathbb{P}^n_A$ is compact. To determine $\mathbb{P}^n_A$, take an affine cover $\mathbb{P}^n = \bigcup_{i=0}^n U_i$, where $U_i = \{ x = (x_0, \dots, x_n) \in \mathbb{P}^n : x_i \neq 0 \}$ and the isomorphism $U_i \simeq \mathbb{A}^n$ is given by $(x_0, \dots, x_n) \mapsto (x_0/x_i, \dots, x_{i-1}/x_i, x_{i+1}/x_i, \dots, x_n/x_i)$. If $v \in V_f^K$, $x = (x_0, \dots, x_n) \in \mathbb{P}^n_{K_v}$ and $|x_i|_v = \max_j |x_j|_v$, then clearly $x \in U_{i\mathcal{O}_v}$; hence $\mathbb{P}^n_{K_v} = \mathbb{P}^n_{\mathcal{O}_v}$. Thus $\mathbb{P}^n_A$ is the direct product $\prod_v \mathbb{P}^n_{K_v}$ and therefore is compact, since all $\mathbb{P}^n_{K_v}$ are compact (cf. §3.1). Furthermore, it is well known (cf. Borel-Tits [1]) that the canonical projection $\sigma: G \to X = G/P$ has a rational section over K. Using the density of G_K in G (Theorem 2.2), we easily see that in our set-up all the conditions of Proposition 5.3 are satisfied and therefore $\sigma_A: G_A \to X_A$ is surjective. Thus, X_A can be identified with G_A/P_A just as X_K with G_K/P_K. Now we have all the necessary tools to prove the following

THEOREM 5.4. *Let G be a connected K-group, and let P be a parabolic K-subgroup of G. Then the number $\nu(G,P)$ of double cosets of G_K modulo $G_\mathcal{O}$ and P_K is finite (or, equivalently, there are only finitely many orbits of $G_\mathcal{O}$ on X_K).*

PROOF: First we establish that there are only finitely many distinct double cosets in the decomposition

$$G_A = \bigcup_i G_{A(\infty)} x_i P_K. \tag{5.10}$$

We saw above that X_A (for $X = G/P$) is compact; yet X_A can be identified with G_A/P_A. It follows that $G_A = CP_A$ for a suitable compact subset C of G_A. Furthermore, there are finite sets $y_1, \dots, y_r$ in G_A and $z_1, \dots, z_s$ in P_A such that

$$C \subset \bigcup_{j=1}^{r} G_{A(\infty)} y_j,$$

$$P_A = \bigcup_{l=1}^{s} P_{A(\infty)} z_l P_K,$$

and then $G_A = \bigcup_{j=1}^r \bigcup_{l=1}^s G_{A(\infty)} y_j P_{A(\infty)} z_l P_K$. Therefore it suffices to show that any set of the form $G_{A(\infty)} y P_{A(\infty)} z P_K$ is contained in the union of a finite number of sets of the form $G_{A(\infty)} x P_K$. We have

$$G_{A(\infty)} y P_{A(\infty)} z P_K \subset G_{A(\infty)} y G_{A(\infty)} z P_K = G_{A(\infty)} (y G_{A(\infty)} y^{-1}) y z P_K.$$

But $y G_{A(\infty)} y^{-1}$ is commensurable with $G_{A(\infty)}$ (Lemma 5.7); therefore $y G_{A(\infty)} y^{-1} \subset \bigcup_{i=1}^d G_{A(\infty)} x_i$ for some finite set $\{x_i\}_{i=1}^d \subset G_A$. Then

$$G_{A(\infty)} y P_{A(\infty)} z P_K \subset \bigcup_{i=1}^{d} G_{A(\infty)} x_i y z P_K,$$

as desired. Since there are only finitely many distinct cosets in (5.10), it follows that there is a finite set $\{t_j\}_{j=1}^a \subset G_K$ such that

$$G_K \subset \bigcup_{j=1}^{d} G_{A(\infty)} t_j P_K;$$

therefore $G_K = \bigcup_{j=1}^d (G_{A(\infty)} \cap G_K) t_j P_K = \bigcup_{j=1}^d G_\mathcal{O} t_j P_K$, as desired. Q.E.D.

In §4.7 we noted that, for a connected $\mathbb{Q}$-group G, the number $\nu(G,P)$ of double cosets $G_\mathbb{Z} \backslash G_\mathbb{Q} / P_\mathbb{Q}$, where P is a minimal parabolic $\mathbb{Q}$-subgroup, can be interpreted as the minimal possible number of vertices of a fundamental set in $G_\mathbb{R}$ relative to $G_\mathbb{Z}$. This number turns out to be related to the class number of P.

PROPOSITION 5.10. *Assume $\mathrm{cl}(G) = 1$ and $G_{K_v} = G_{\mathcal{O}_v} P_{K_v}$ for all v in V_f^K. Then $\nu(G,P) = \mathrm{cl}(P)$.*

PROOF: First we show that if $\mathrm{cl}(G) = 1$ then $\nu(G,P)$ equals the number d of double cosets in the decomposition $G_A = \bigcup_{i=1}^d G_{A(\infty)} x_i P_K$, (cf. proof of

Theorem 5.4). Indeed, straightforward verification shows that $G_{\mathcal{O}} x P_K \overset{\theta}{\mapsto} G_{A(\infty)} x P_K$ gives an injection from $G_{\mathcal{O}} \backslash G_K / P_K$ into $G_{A(\infty)} \backslash G_A / P_K$, and the image of θ consists of those cosets $G_{A(\infty)} x P_K$ which intersect G_K. But if $\mathrm{cl}(G) = 1$, i.e., $G_A = G_{A(\infty)} G_K$, then every coset of this form intersects G_K; consequently θ is surjective. Now let us compute d another way. To do so, note that since $G_{K_v} = G_{\mathcal{O}_v} P_{K_v}$ for all $v \in V_f^K$, then we have $G_A = G_{A(\infty)} P_A$, and therefore any coset $G_{A(\infty)} x P_K$ has a representative from P_A. Moreover, if $G_{A(\infty)} x P_K = G_{A(\infty)} y P_K$, where $x, y \in P_A$, then $P_{A(\infty)} x P_K = P_{A(\infty)} y P_K$; consequently $d = \mathrm{cl}(P)$, proving the proposition.

EXAMPLE: Let $G = SL_2$ over a field K. First show that the conditions of Proposition 5.10 hold for G and $P = B$, the Borel subgroup of G consisting of upper triangular matrices. $\mathrm{cl}(G) = 1$ is a consequence of Proposition 5.4 and the strong approximation property for G, which we established in the proof of Proposition 5.7. $G_{K_v} = G_{\mathcal{O}_v} G_{K_v}$ can be verified by direct computation. Indeed, if $x = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(K_v)$ then there are $\gamma, \delta \in \mathcal{O}_v$ not both in $\mathfrak{p}_v$, such that $\gamma a + \delta c = 0$. Furthermore, there are $\alpha, \beta \in \mathcal{O}_v$ for which $y = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ lies in $SL_2(\mathcal{O}_v)$, and then direct computation shows that $yx \in B_{K_v}$. Applying Proposition 5.10, we see that in the case under consideration we have $\nu(G, B) = \mathrm{cl}(B)$.

Writing B as the semidirect product of the 1-dimensional torus $T = \{\mathrm{diag}(a, a^{-1})\}$ by the group U of upper unipotent matrices, and using the obvious equality $B_{A(\infty)} = T_{A(\infty)} U_{A(\infty)}$, we can easily show that $\mathrm{cl}(B) = \mathrm{cl}(S)$ (cf. proof of Proposition 5.4). But $S \simeq \mathbb{G}_m$, and therefore $\mathrm{cl}(S) = [J_K : J_{K(\infty)} K^*]$ is the class number h_K of K. However, by definition $\nu(G, B)$ is the number of orbits of $G_{\mathcal{O}}$ on X_K, where $X = G/B$. Since in our case $X \simeq \mathbb{P}^1$, eventually we arrive at the following result: h_K equals the number of orbits of the natural action of $SL_2(\mathcal{O})$ on $\mathbb{P}^1_K$ over K. (This can also be proven directly; cf. Serre [7].)

5.3. Criteria for the compactness and the finiteness of volume of G_A/G_K.

THEOREM 5.5.

(1) *G_A/G_K is compact if and only if the reductive part of the connected component G^0 is anisotropic over K.*
(2) *G_A/G_K has finite invariant volume if and only if $\mathbf{X}(G^0)_K = 1$.*

PROOF: Since the subgroup G_K is discrete in G_A, an invariant measure on G_A/G_K exists if and only if G_A is unimodular (cf. §3.5). Let us show that the latter is equivalent to G_∞ being unimodular. Since $F = G_A/G_A^0$ is a compact topological group (cf. Proposition 5.4), it has finite G_A-invariant measure; therefore the restriction of the module function Δ_{G_A} to G_A^0 is $\Delta_{G_A^0}$ (Theorem 3.17). In particular, if G_A is unimodular then so is G_A^0. Conversely, if we assume G_A^0 is unimodular, then $\ker \Delta_{G_A}$ contains G_A^0 and therefore Δ_{G_A} induces a continuous homomorphism from F to $\mathbb{R}^{>0}$. But $\mathbb{R}^{>0}$ has no nontrivial compact subgroups; hence $\Delta_{G_A} = 1$. We have shown that the unimodularity of G_A is equivalent to the unimodularity of G_A^0. The same can be said of the unimodularity of G_∞ and G_∞^0, since G_∞/G_∞^0 is finite.

Therefore we may assume from the outset that G is connected. Then the Haar measure on G_A can be constructed using a left-invariant rational differential K-form ω on G of degree $n = \dim G$. More precisely, ω induces a left-invariant measure ω_v on G_{K_v}, for each $v \in V^K$, as described in §3.5. Let us choose numbers λ_v for $v \in V_f^K$ (called *convergence coefficients*) such that $\prod_v \lambda_v \omega_v(G_{\mathcal{O}_v})$ converges absolutely (for example, we can set $\lambda_v = \frac{1}{\omega_v(G_{\mathcal{O}_v})}$). Then, treating G_A as the restricted topological product of the G_{K_v} with respect to the distinguished subgroups $G_{\mathcal{O}_v}$, we can use the construction described in §3.5 to obtain a Haar measure τ on G_A, called the *Tamagawa measure* corresponding to the set of convergence coefficients $\lambda = (\lambda_v)$.

Note that τ is actually independent of the choice of ω. Indeed, any other left-invariant rational differential K-form ω' can be written as $\omega' = c\omega$ for some $c \in K^*$, and then for any $v \in V^K$ the corresponding measures ω_v' and ω_v are related by $\omega_v' = \|c\|_v^n \omega_v$, where $\| \ \|_v$ is the normalized valuation introduced in §1.2.1. Therefore, if we construct τ' by using ω' and the same set of convergence coefficients, then $\tau' = (\prod_v \|c\|_v^n)\tau = \tau$ by the product formula (cf. §1.2.1).

From the construction of τ it follows that G_A is unimodular if and only if all the G_{K_v} are unimodular. But by Theorem 3.18, G_{K_v} being unimodular for some v is equivalent to ω being right-invariant, and then the G_{K_v} are unimodular for all v. It follows that either both G_A and G_∞ are unimodular, or neither is unimodular.

The arguments that follow apply equally to the proof of (1) and of (2). By Proposition 5.9, there always exists a fundamental set in G_A with respect to G_K of the form $\Omega = B \times C$, where $B \subset G_\infty$ is a closed fundamental set with respect to $G_{\mathcal{O}}$ and C is a compact open subset of $G_{A(\infty)}$. The properties of fundamental sets imply that G_A/G_K being compact is equivalent to Ω being compact, i.e., to B being compact. Analogously, the existence of a fundamental set with finite volume is equivalent to B having finite volume. Since the unimodularity of G_∞ is equivalent to that of G_A, we have the

following equivalences:

$$\{G_A/G_K \text{ is compact}\} \Longleftrightarrow \{G_\infty/G_\mathcal{O} \text{ is compact}\}$$

$$\left\{\begin{matrix}G_A/G_K \text{ has finite}\\ \text{invariant volume}\end{matrix}\right\} \Longleftrightarrow \left\{\begin{matrix}G_\infty/G_\mathcal{O} \text{ has finite}\\ \text{invariant volume}\end{matrix}\right\}.$$

Therefore (1) and (2) of Theorem 5.5 follow from the respective assertions in Theorem 4.17. Q.E.D.

It is well known that the convergence coefficients used in the definition of the Tamagawa measure can be chosen canonically; in particular, for G semisimple they are not even necessary (i.e., one can put $\lambda_v = 1$ for all v). With respect to the Tamagawa measure thus obtained, the invariant volume of G_A/G_K (if it exists) is called the *Tamagawa number* of G, denoted $\tau(G)$.

EXAMPLE: Let $G = \mathbf{SL}_2$ over $\mathbb{Q}$. We shall show that $\tau(G) = 1$. Consider the differential form ω on G, which in terms of the coordinates x, y, z of $X = \left(\begin{smallmatrix}x & y\\ z & t\end{smallmatrix}\right) \in G$ can be written as $\omega = \frac{1}{x}dx \wedge dy \wedge dz$. In §3.5 we saw that this is a left-invariant rational form on G. There we computed the volume $\omega_p(SL_2(\mathbb{Z}_p))$ with respect to the corresponding Haar measure ω_p on $SL_2(\mathbb{Q}_p)$ to be equal to $1 - p^{-2}$. Then $\prod_p \omega_p(SL_2(\mathbb{Z}_p))^{-1}$ is exactly the Euler product for the Riemann zeta function $\zeta(s)$ at $s = 2$, and therefore $\prod_p \omega_p(SL_2(\mathbb{Z}_p))$ converges absolutely to $\zeta(2)^{-1}$. (Note that the convergence coefficients, indeed, are not necessary in this case.) Now let Σ be the fundamental domain of $SL_2(\mathbb{R})$ relative to $SL_2(\mathbb{Z})$, as constructed in the example in §4.6. We showed in §3.5 that in terms of the coordinates φ, a, u on $SL_2(\mathbb{R})$ given by the Iwasawa decomposition, ω can be written as $a\,d\varphi\,da\,du$, and therefore the computations in §4.6 for the corresponding Haar measure ω_∞ on $SL_2(\mathbb{R})$ give the value $\omega_\infty(F) = \frac{\pi^2}{6}$. It remains to note that, arguing as in the proof of Proposition 5.7, we see easily that $\Omega = F \times \prod_p SL_2(\mathbb{Z}_p)$ is a fundamental domain in G_A relative to G_K, i.e., it satisfies conditions (1) and (2′) of §3.5. Thus $\tau(G) = \omega_\infty(F) \times \prod_p SL_2(\mathbb{Z}_p) = \frac{\pi^2}{6}\zeta(2)^{-1} = 1$, since $\zeta(2) = \frac{\pi^2}{6}$ (cf. Serre [8]).

In this example we were able to give an explicit description of the fundamental domain in G_A relative to G_K and to compute its volume, thereby leading to the determination of the Tamagawa number $\tau(G)$. Although such constructions are not feasible in general, the problem of computing $\tau(G)$ is itself quite important. This became particularly clear after Kneser and Tamagawa noted independently that, for $G = \mathbf{SO}_n(f)$ where f is a non-degenerate quadratic form in n variables with rational coefficients, the

equality $\tau(G) = 2$ is essentially one of Siegel's basic results in the analytic theory of quadratic forms (the formula for the weight of a genus; cf. Kneser's lecture in ANT). For G semisimple, by Theorem 5.5 $\tau(G)$ is finite, and its computation quickly became a major problem. As Ono has shown [8], [10], it suffices in fact to compute one Tamagawa number for each isogeny class of groups. More precisely, we have the following elegant result: Let G be a semisimple K-group, let $\pi\colon \tilde{G} \to G$ be the universal K-covering, let $F = \ker\pi$ be the fundamental group of G, and let $\mathbf{X}(F)$ be its group of characters. Then $\tau(G) = \tau(\tilde{G})\frac{h^0(\mathbf{X}(F))}{i^1(\mathbf{X}(F))}$, where $h^0(\mathbf{X}(F)) = [H^0(K, \mathbf{X}(F))] = [\mathbf{X}(F)_K]$ and $i^1(\mathbf{X}(F))$ is the order of the kernel of the canonical map $H^1(K, \mathbf{X}(F)) \to \prod_v H^1(K_v, \mathbf{X}(F))$.

Thus it suffices to compute $\tau(G)$ for all the simply connected groups. The Weil conjecture asserts that for G simply connected we have $\tau(G) = 1$. Weil [4], [5] developed a method for computing Tamagawa numbers which uses induction, the residues of some analogs of the zeta function, and the Poisson summation formula. This method allows one to prove his conjecture for many classical groups and some exceptional groups. Later Mars [3], [4] computed the Tamagawa number for unitary groups of type A_n and thereby completed the proof of the Weil conjecture for classical semisimple groups over number fields. A unified proof of the Weil conjecture for Chevalley groups was given by Langlands [1]. Lai [1], [2] computed $\tau(G)$ for G quasisplit. A complete proof of the Weil conjecture was obtained quite recently by Kottwitz [3] modulo the validity of the Hasse principle for Galois cohomology of simply connected semisimple algebraic groups. Chernousov [6], however, completed the proof of the Hasse principle for groups of type E_8 (cf. Chapter 6). Thus the Weil conjecture has recently been proved in general.

The above definition of Tamagawa numbers requires some modification for reductive groups more general than semisimple groups, since for many cases important in applications (such as the 1-dimensional split torus $\mathbb{G}_m$) the volume of G_A/G_K is infinite. This compels us to search for other homogeneous spaces that are closely related to adele groups but have finite invariant volume. Since the obstruction to the finiteness of the volume of G_A/G_K comes from the existence of nontrivial K-characters, or equivalently, of a nontrivial almost direct factor which is a K-split torus, it is natural to begin our analysis with the 1-dimensional K-split torus $S = \mathbb{G}_m$. Here S_A is isomorphic to J_K, the idele group of K. Although J_K/K^* is certainly noncompact, a classical result from algebraic number theory (cf. Lang [2]) asserts that J_K^1/K^* is compact where J_K^1 is the group of what we call special ideles (i.e., the kernel of the homomorphism

$c_K: J_K \to \mathbb{R}^{>0}$ given by $c_K((x_v)) = \prod_v \|x_v\|_v$ (cf. §1.2.1)). In general the analog of J_K^1 can be defined as follows: We associate with each character χ in $\mathbf{X}(G)_K$ the continuous homomorphism $c_K(\chi): G_A \to \mathbb{R}^{>0}$ given by $c_K(\chi)((g_v)) = \prod_v |\chi(g_v)|_v$. Then we define

$$G_A^{(1)} = \bigcap_{\chi \in \mathbf{X}(G)_K} \ker c_K(\chi).$$

Clearly this infinite intersection can be replaced by a finite one, since if $\chi_1, \dots, \chi_r$ constitute a base of $\mathbf{X}_K(G)$, we have $G_A^{(1)} = \bigcap_{i=1}^r \ker c_K(\chi_i)$. As an exercise the reader may show that this relation also holds if $\chi_1, \dots, \chi_r$ generate a subgroup of $\mathbf{X}_K(G)$ of finite index. The product formula implies $G_A^{(1)} \supset G_K$

THEOREM 5.6. *Let G be a connected K-group. Then $G_A^{(1)}$ is unimodular and $G_A^{(1)}/G_K$ has finite invariant volume. $G_A^{(1)}/G_K$ is compact if and only if the semisimple part of G is anisotropic over K.*

Note that the latter requirement can also be formulated as follows: each unipotent element of G_K lies in the unipotent radical of G. Moreover, if G is connected and $\mathbf{X}(G)_K = 1$, then $G_A^{(1)} = G_A$; hence Theorem 5.6 is a generalization of Theorem 5.5 for connected groups.

PROOF: It is convenient to begin by reducing to the case $K = \mathbb{Q}$. Let $H = \mathbf{R}_{K/\mathbb{Q}}(G)$ be the group obtained from G by restriction of scalars. We shall show that the isomorphism $G_{A_K} \overset{\varrho}{\simeq} H_{A_\mathbb{Q}}$ from Proposition 5.6 induces an isomorphism $G_{A_K}^{(1)} \simeq H_{A_\mathbb{Q}}^{(1)}$. To do so, note that any K-character $\chi: G \to \mathbb{G}_m$ induces a morphism $\tilde{\chi} = \mathbf{R}_{K/\mathbb{Q}}(\chi): H \to \mathbf{R}_{K/\mathbb{Q}}(\mathbb{G}_m)$. Composing $\tilde{\chi}$ with the norm map $N: \mathbf{R}_{K/\mathbb{Q}}(\mathbb{G}_m) \to \mathbb{G}_m$, we obtain the character $\kappa = N \circ \tilde{\chi} \in \mathbf{X}(H)_\mathbb{Q}$. Using factorization (2.4) one can show easily that the correspondence $\chi \mapsto \kappa$ defines an isomorphism $\eta: \mathbf{X}(G)_K \to \mathbf{X}(H)_\mathbb{Q}$ of the corresponding groups of characters, which yields the commutative diagram

$$\begin{array}{ccc} G_K & \xrightarrow{\varrho} & H_\mathbb{Q} \\ {\scriptstyle\chi}\downarrow & & \downarrow{\scriptstyle\eta(\chi)} \\ K^* & \xrightarrow{N_{K/\mathbb{Q}}} & \mathbb{Q}^* \end{array}$$

for any χ in $\mathbf{X}(G)_K$. We leave it to the reader to verify that this diagram also extends to the respective adele groups. The formulas in §1.2.3 imply that $c_K(\chi) = c_\mathbb{Q}(\eta(\chi))$; hence ϱ does induce an isomorphism $G_{A_K}^{(1)} \simeq H_{A_K}^{(1)}$.

Therefore $G_{A_K}^{(1)}/G_K$ and $H_{A_\mathbb{Q}}^{(1)}/H_\mathbb{Q}$ are isomorphic, and we may assume that $K = \mathbb{Q}$ from the outset. Simplification of the argument for this case is based on the fact that here we can give a nice description of $G_{A(\infty)}^{(1)} = G_A^{(1)} \cap G_{A(\infty)}$. By definition $G_{A(\infty)} = G_\mathbb{R} \times G_{A_f(\infty)}$, whereas $G_{A_f(\infty)} \subset G_{A(\infty)}^{(1)}$ since $G_{A_f(\infty)}$ is compact and $\mathbb{R}^{>0}$ contains no compact subgroups. Thus $G_{A(\infty)}^{(1)} = L_\mathbb{R} \times G_{A_f(\infty)}$, where $L \subset G$ consists of those g for which $\chi(g) = \pm 1$ for all χ in $\mathbf{X}(G)_\mathbb{Q}$.

LEMMA 5.8. *L is a Zariski-closed $\mathbb{Q}$ subgroup of G, and $\mathbf{X}(L^0)_\mathbb{Q} = 1$. Moreover, the semisimple parts of G and L^0 are the same.*

PROOF: Let $\chi_1, \dots, \chi_r$ be a base of $\mathbf{X}(G)_\mathbb{Q}$, and let $\varphi: G \to \mathbb{G}_m^r$ be the homomorphism defined by $\varphi(g) = (\chi_1(g), \dots, \chi_r(g))$. Then $L = \varphi^{-1}(D)$, where $D \subset \mathbb{G}_m^r$ is the (closed) subgroup consisting of $\{(\pm 1, \dots, \pm 1)\}$; thus the first assertion of the lemma is proved. If $G = HU$ is the Levi decomposition of G, S is the maximal central torus of H, and $S = S_1 S_2$ is its presentation as an almost direct product of a $\mathbb{Q}$-split and a $\mathbb{Q}$-anisotropic torus respectively, then it is easy to see that $L^0 = (BS_2)U$, where $B = [H, H]$ is the semisimple part of G. The rest of the lemma follows immediately.

It follows from Lemma 5.8 and Theorem 4.13 that $L_\mathbb{R}$ is unimodular. Therefore also $G_{A(\infty)}^{(1)} = L_\mathbb{R} \times G_{A_f(\infty)}$ is unimodular, since $G_{A_f(\infty)}$ is compact. Our objective is to show that $G_A^{(1)}$ is unimodular. To do so, let us consider the module function $\Delta = \Delta_{G_A^{(1)}}: G_A^{(1)} \to \mathbb{R}^{>0}$ and show that actually $\Delta = 1$. Since $G_{A(\infty)}^{(1)}$ is open in $G_A^{(1)}$ and unimodular, the restriction of Δ to $G_{A(\infty)}^{(1)}$ equals 1.

We shall show that also $\Delta|_{G_\mathbb{Q}} = 1$. Since $G_A^{(1)}$ is a normal subgroup of G_A, the group $G_A/G_A^{(1)}$ has invariant measure, and therefore Δ is the restriction of Δ_{G_A} to $G_A^{(1)}$. But then the Tamagawa measure can be used to compute Δ. Let ω be a left-invariant rational differential $\mathbb{Q}$-form on G of degree $n = \dim G$, and let ϱ_g be the right translation by the element g of G. Then, as in the proof of Theorem 4.13, $\varrho_g^*(\omega) = \chi(g)\omega$ for some χ in $\mathbf{X}(G)_\mathbb{Q}$. If $v \in V^\mathbb{Q}$ and ω_v is the corresponding Haar measure on $G_{\mathbb{Q}_v}$, then $\Delta_{G_{\mathbb{Q}_v}}(g)$ equals $\|\chi(g)\|_v^n$ for g in $G_{\mathbb{Q}_v}$. Therefore by the product formula $\Delta(g) = \prod_v \|\chi(g)\|_v^n = 1$ for g in $G_\mathbb{Q}$. Furthermore, it follows from Theorem 5.1 that there are only finitely many double cosets $G_{A(\infty)}^{(1)} \backslash G_A^{(1)}/G_\mathbb{Q}$; hence, from the above and the fact that Δ is a homomorphism we obtain that the image $\Delta(G_A^{(1)})$ is finite. Consequently $\Delta(G_A^{(1)}) = 1$, since $\mathbb{R}^{>0}$ has no nontrivial finite subgroups. Thus we have proved the unimodularity of $G_A^{(1)}$.

Now let us consider the finite decomposition

$$G_A^{(1)} = \bigcup_{i=1}^{r} G_{A(\infty)}^{(1)} x_i G_{\mathbb{Q}}.$$

Lemma 5.7 implies that each group $x_i^{-1} G_{A(\infty)}^{(1)} x_i$ is commensurable with $G_{A(\infty)}^{(1)}$; hence there is a finite set $y_1, \dots, y_l$ in $G_A^{(1)}$ such that $G_A^{(1)} = \bigcup_{j=1}^{l} y_j G_{A(\infty)}^{(1)} G_{\mathbb{Q}}$. Therefore it suffices to establish the conditions for $G_{A(\infty)}^{(1)} G_{\mathbb{Q}}/G_{\mathbb{Q}}$ to have finite volume or, respectively, to be compact. But, in view of the factorization $G_{A(\infty)}^{(1)} = L_{\mathbb{R}} \times G_{A_f(\infty)}$ and the fact that $G_{\mathbb{Z}} = L_{\mathbb{Z}}$, we have

$$(G_{A(\infty)}^{(1)} G_{\mathbb{Q}})/G_{\mathbb{Q}} \simeq G_{A(\infty)}^{(1)}/G_{\mathbb{Z}} \simeq L_{\mathbb{R}}/L_{\mathbb{Z}} \times G_{A_f(\infty)};$$

and since $G_{A_f(\infty)}$ is compact, the latter reduces to the condition of $L_{\mathbb{R}}/L_{\mathbb{Z}}$ having finite volume or, respectively, being compact. But Theorems 4.12 and 4.13 imply that $L_{\mathbb{R}}/L_{\mathbb{Z}}$ always has finite volume, and is compact if and only if the semisimple part of L^0, which in view of Lemma 5.8 is the same as the semisimple part of G, is anisotropic over $\mathbb{Q}$. Q.E.D.

As in the case of G_A/G_K, we can define the measure $\tau^{(1)}$ on $G_A^{(1)}/G_K$ canonically, and then the volume of $\tau^{(1)}(G_A^{(1)}/G_K)$ is also called the *Tamagawa number* of G. Note that for G connected, G_A/G_K has finite volume if and only if $\mathbf{X}(G)_K = 1$ and then $G_A^{(1)} = G_A$. Thus this new definition indeed generalizes our former one to arbitrary connected groups.

Ono [6] computed the Tamagawa number of an algebraic K-torus T as $\tau(T) = \frac{[H^1(K,\mathbf{X}(T))]}{[Ш(T)]}$, where $Ш(T) = \ker(H^1(K,T) \to \prod_v H^1(K_v,T))$ is the Shafarevich-Tate group of T. With this result one can construct examples of tori and semisimple groups for which $\tau(T)$ is not an integer. Moreover, one can combine the above formulas for the Tamagawa numbers of semisimple groups and of tori into a single formula (noting that the Tamagawa number of a unipotent group U is always 1), describing the Tamagawa number of any connected K-group G in terms of the cohomology of the Picard module $\operatorname{Pic} G$ (cf. Sansuc [1]).

5.4. Reduction theory for S-arithmetic subgroups.

In this section we shall use the reduction theory which we developed for adele groups to obtain analogous results for S-arithmetic subgroups. In what follows S will denote a finite subset of V^K containing V_∞^K, and $\mathcal{O}(S)$ will denote the ring of S-integers of K. If $G \subset \mathbf{GL}_n$ is an algebraic K-group, then $G_{\mathcal{O}(S)}$ is the group of S-integral points, also called the group of S-units of G.

Recall that a subgroup $\Gamma \subset G$ is said to be *S-arithmetic* if it is commensurable with $G_{\mathcal{O}(S)}$. It can be shown that the set of S-arithmetic subgroups is invariant under K-isomorphisms, either by modifying Proposition 4.2 appropriately or by applying the equality $G_{\mathcal{O}(S)} = G_{A(S)} \cap G_K$ and using the remark following Lemma 5.7. This equality also implies that $G_{\mathcal{O}(S)}$ is a discrete subgroup of $G_{A(S)}$. Since $G_{A(S)} = G_S \times G_{A_S(S)}$ and $G_{A_S(S)}$ is compact, $G_{\mathcal{O}_S}$ is also a discrete subgroup of $G_S = \prod_{v \in S} G_{K_v}$ (which is easily seen also without using adeles). Therefore we may pose the problem of developing a reduction theory for $G_{\mathcal{O}(S)}$ in $G_{A(S)}$ as well as in G_S. It is natural to define fundamental sets here as follows, in analogy to the respective definitions for arithmetic groups and adele groups:

DEFINITION:

(1) A subset Ω of $G_{A(S)}$ is a *fundamental set* for $G_{\mathcal{O}(S)}$ if
  (F1)$_{A(S)}$ $\Omega G_{\mathcal{O}(S)} = G_{A(S)}$,
  (F2)$_{A(S)}$ $\Omega\Omega^{-1} \cap G_{\mathcal{O}(S)}$ is finite.

(2) A subset Ω of G_S is a *fundamental set* for $G_{\mathcal{O}(S)}$ if
  (F1)$_S$ $\Omega G_{\mathcal{O}(S)} = G_S$,
  (F2)$_S$ for any $a, b \in G_K$ the set of x in $G_{\mathcal{O}(S)}$ satisfying $\Omega axb \cap \Omega \neq \emptyset$ is finite.

It is easy to see that, for S finite, the problems of constructing fundamental sets in $G_{A(S)}$ and in G_S respectively are actually equivalent. Namely, if $\Omega \subset G_S$ is a fundamental set as defined in (2), then $\Omega \times G_{A_s(S)} \subset G_{A(S)}$ is a fundamental set as defined in (1). For this reason, below we shall concern ourselves only with constructing fundamental sets in G_S. Note that for S infinite, definition (2) becomes meaningless, whereas all the results for $G_{A(S)}$ remain valid (cf. Borel [1, §8]).

PROPOSITION 5.11. *Let B be a fundamental set for $G_{\mathcal{O}}$ in G_∞. Then there is an open compact subset C of $G_{S \setminus V_\infty^K}$ such that $\Omega = B \times C \subset G_S$ is a fundamental set for $G_{\mathcal{O}(S)}$.*

PROOF: analogous to that of Proposition 5.9. Indeed, Theorem 5.1 implies that there is a finite decomposition

$$G_{A(S)} = \bigcup_{i=1}^{r} G_{A(\infty)} x_i (G_K \cap G_{A(S)}) = \bigcup_{i=1}^{r} G_{A(\infty)} x_i G_{\mathcal{O}(S)}, \text{ for } x_i \in G_{S \setminus V_\infty^K},$$

which leads to the decomposition

$$G_S = \bigcup_{i=1}^{r} Dx_i G_{\mathcal{O}(S)},$$

where $D = G_\infty \times U$, $U = \prod_{v \in S \setminus V_\infty^K} G_{\mathcal{O}_v}$. Put $C = \bigcup_{i=1}^r U x_i U$. Then one can easily verify that for $\Omega = B \times C$ one has $G_S = \Omega G_{\mathcal{O}_S}$, so it remains to verify that $\Sigma = \{ x \in G_{\mathcal{O}(S)} : \Omega \cap \Omega axb \neq \emptyset \}$ is finite for any a, b in G_K. If $x \in \Sigma$, then passing to the projection on the non-Archimedean part, we obtain $x \in a^{-1}C^{-1}Cb^{-1}$; then $x^{-1} \in bC^{-1}Ca$. As we have seen earlier, since $C^{-1}C$ is compact, there is r in $\mathcal{O}$ such that $\Sigma \subset G_r = \{ x \in G_K : rx, rx^{-1} \in M_n(\mathcal{O}) \}$ (assuming $G \subset \mathbf{GL}_n$). Therefore the finiteness of Σ is an immediate consequence of the obvious generalization of Lemma 4.8. The proposition is proved.

Proposition 5.11 easily yields

THEOREM 5.7.

(1) *$G_S/G_{\mathcal{O}(S)}$ has finite invariant volume if and only if $\mathbf{X}(G^0)_K = 1$;*
(2) *$G_S/G_{\mathcal{O}(S)}$ is compact if and only if the reductive part of the connected component of G is anisotropic over K.*

PROOF: In the proof of Theorem 5.5 we established that either all the groups G_{K_v} for $v \in V^K$ are unimodular or neither of them is unimodular, so the unimodularity of G_S is equivalent to the unimodularity of G_∞. Taking a closed fundamental set for $G_{\mathcal{O}}$ in G_∞ in the sense of §3.5 for the B in Proposition 5.11, we obtain that $G_S/G_{\mathcal{O}(S)}$ has finite invariant volume (resp., is compact) if and only if the respective property holds for $G_\infty/G_{\mathcal{O}}$. Therefore our assertions follow from the corresponding parts of Theorem 4.17. Q.E.D.

Applying reduction theory, we obtained theorems on finiteness of orbits both for arithmetic groups and adele groups (cf. Theorems 5.3 and 4.9). A similar theorem also holds for S-arithmetic subgroups. To formulate this theorem let an *S-lattice on K^n* be any finitely generated $\mathcal{O}(S)$-submodule of K^n containing a base.

THEOREM 5.8. *Let G be a reductive algebraic K-group, and let $\varrho: G \to \mathbf{GL}_m$ be a representation of G defined over K. For w in K^m, if the orbit $X = w\varrho(G)$ is Zariski-closed, then for any S-lattice $L \subset K^m$ invariant under $G_{\mathcal{O}(S)}$, $X_S \cap L$ is a union of a finite number of orbits of $G_{\mathcal{O}(S)}$.*

The proof follows directly from the following two propositions.

PROPOSITION 5.12. *X_S consists of a finite number of orbits of G_S.*

PROPOSITION 5.13. *$w\varrho(G_S) \cap L$ is a union of a finite number of orbits of $G_{\mathcal{O}(S)}$.*

PROOF OF PROPOSITION 5.12: Reduces immediately to the case when S consists of a single valuation v (recall that S is always assumed to be finite). If v is complex, then G_{K_v} acts transitively on X_{K_v}, i.e., there is only one orbit. For v real, the desired finiteness is established in Theorem 3.6, Corollary 2. For the non-Archimedean case the only known way to derive the finiteness of the number of orbits is to apply the finiteness theorem for Galois cohomology over locally compact fields, which we shall do in §6.3.

PROOF OF PROPOSITION 5.13: Follows from the construction of fundamental sets, described in Proposition 5.11. More precisely, in §4.7 we showed how to construct a fundamental set $B \subset G_\infty$ relative to $G_{\mathcal{O}}$ by using restriction of scalars and the construction of fundamental sets in $G_{\mathbb{R}}$ relative to $G_{\mathbb{Z}}$ (cf. §4.3). Then it follows from the proof of Theorem 5.9 that B thus obtained has the following property: if $\varrho: G \to \mathbf{GL}_m$ is a K-representation, then $w\varrho(B) \cap \mathcal{O}^m$ is finite, for any w in K^m for which $X = w\varrho(G)$ is closed. Starting with $B \subset G_\infty$ satisfying this property, we then use Proposition 5.11 to find a compact set $C \subset G_{S \setminus V_\infty^K}$ such that $\Omega = B \times C$ is a fundamental set for $G_{\mathcal{O}(S)}$ in G_S. Since L is invariant with respect to $G_{\mathcal{O}(S)}$, it suffices to show that $F = w\varrho(\Omega) \cap L$ is finite. The compactness of C implies the existence of r in $\mathcal{O}$ such that $rF \subset \mathcal{O}^m$. Then, projecting onto the Archimedean component, we see that rF is contained in $(rw)\varrho(B) \cap \mathcal{O}^m$, which is finite by assumption. Q.E.D.

From Theorem 5.8 we can derive that the class of S-arithmetic subgroups is closed under arbitrary epimorphisms, and that there are only finitely many conjugacy classes of finite subgroups of $G_{\mathcal{O}(S)}$.

THEOREM 5.9. *Let $f: G \to H$ be an epimorphism of algebraic groups. Then for any S-arithmetic subgroup Γ of G the image of $f(\Gamma)$ is an S-arithmetic subgroup of H.*

PROOF: Barely differs from the proof of Theorem 4.1. Clearly it suffices to establish that $f(G_{\mathcal{O}(S)})$ is S-arithmetic, and we may assume $f(G_{\mathcal{O}(S)}) \subset H_{\mathcal{O}(S)}$. First we show that the general case reduces to the case of G either reductive or unipotent.

LEMMA 5.9. *Let $G = FU$ be the Levi decomposition. If B and D are subgroups of finite index of $F_{\mathcal{O}(S)}$ and $U_{\mathcal{O}(S)}$, respectively, and if B normalizes D, then BD is a subgroup of $G_{\mathcal{O}(S)}$ having finite index.*

PROOF: Repeating verbatim the proof of Corollary 2 to Proposition 4.2, we obtain that $[G_{\mathcal{O}(S)} : F_{\mathcal{O}(S)} U_{\mathcal{O}(S)}]$ is finite. Now let $F_{\mathcal{O}(S)} = \bigcup_{i=1}^r x_i B$ and $U_{\mathcal{O}(S)} = \bigcup_{j=1}^t y_j D$. Then $F_{\mathcal{O}(S)} U_{\mathcal{O}(S)} = \bigcup_{i=1}^r \bigcup_{j=1}^t x_i y_j BD$. Indeed,

if $x \in F_{\mathcal{O}(S)}$, $y \in U_{\mathcal{O}(S)}$, then writing $x = x_i b$ and $byb^{-1} = y_j d$ for b in B and d in D, we see $xy = x_i by = x_i y_j db = x_i y_j b(b^{-1}db) \in x_i y_j BD$. Thus we have shown that BD has finite index in $F_{\mathcal{O}(S)}U_{\mathcal{O}(S)}$, and consequently also in $G_{\mathcal{O}(S)}$. This proves the lemma.

Let $G = FU$ be the Levi decomposition of G. Then $H = f(F)f(U)$ is the Levi decomposition of H. If we show that $[f(F)_{\mathcal{O}(S)} : f(F_{\mathcal{O}(S)})]$ and $[f(U)_{\mathcal{O}(S)} : f(U_{\mathcal{O}(S)})]$ are finite, then Lemma 5.9 will imply that $[H_{\mathcal{O}(S)} : f(F_{\mathcal{O}(S)}U_{\mathcal{O}(S)})]$ is also finite; hence $[H_{\mathcal{O}(S)} : f(G_{\mathcal{O}(S)})]$ is finite. This gives the reduction to G either unipotent or reductive.

Let us consider the case of G unipotent. Then $G_S/G_{\mathcal{O}(S)}$ is compact, by Theorem 5.7. Setting $U = \ker f$, we have $H^1(K_v, U) = 1$ for any v in V^K (Lemma 2.7); therefore, passing to cohomology in the exact sequence $1 \to U \to G \to H \to 1$, we obtain $f(G_{K_v}) = H_{K_v}$, which yields $f(G_S) = H_S$. It follows that $H_S/f(G_{\mathcal{O}(S)})$ is also compact. Thus $H_{\mathcal{O}(S)}/f(G_{\mathcal{O}(S)})$ is both compact and discrete, so $[H_{\mathcal{O}(S)} : f(G_{\mathcal{O}(S)})]$ must be finite.

Now let G be reductive. If $H \subset GL_n$, then using a well-known trick, we may assume without loss of generality that H is closed in M_n. Then H can be viewed as the (closed) orbit of the identity matrix E_n under the action of G on M_n given by $Ag = Af(g)$, with usual matrix multiplication on the right-hand side. It remains to note that $L = M_n(\mathcal{O}(S))$ is invariant under $G_{\mathcal{O}(S)}$, $H_{\mathcal{O}(S)} = H \cap L$, and the orbits of $G_{\mathcal{O}(S)}$ on $H_{\mathcal{O}(S)}$ are the cosets $H_{\mathcal{O}(S)}/f(G_{\mathcal{O}(S)})$. Thus the finiteness of the number of orbits, assured by Theorem 5.8, is equivalent to the finiteness of the index $[H_{\mathcal{O}(S)} : f(G_{\mathcal{O}(S)}]$. Q.E.D.

THEOREM 5.10. *There are only finitely many conjugacy classes of finite subgroups of $G_{\mathcal{O}(S)}$.*

PROOF: Taking $v \notin S$ and viewing $G_{\mathcal{O}(S)}$ as a subgroup of $G_{\mathcal{O}_v}$, as in the proof of Proposition 3.5 we obtain the finiteness of the number of isomorphism classes of finite subgroups of $G_{\mathcal{O}(S)}$. Therefore it suffices to show that for a given finite group Γ there are only finitely many conjugacy classes of subgroups of $G_{\mathcal{O}(S)}$ isomorphic to Γ. First we consider the case of G reductive. The argument here essentially repeats the proof of Proposition 3.5. Let $R(\Gamma, G)$ be the variety of the representations of Γ in G. Then G acts naturally on $R(\Gamma, G)$ by conjugation, and the assertion is equivalent to the finiteness of the number of orbits of $G_{\mathcal{O}(S)}$ on $R(\Gamma, G)_{\mathcal{O}(S)}$. By Theorem 2.17, G has a finite number of orbits on $R(\Gamma, G)$; moreover, these orbits are Zariski-closed. Let X be one of the orbits for which $X_{\mathcal{O}(S)} \neq \emptyset$. If $G \subset \mathbf{GL}_n$ and $|\Gamma| = d$, then X can be realized as a closed subset of $V = M_n \times \cdots \times M_n$ (d factors), and the action of G extends naturally to V. Therefore, applying Theorem 5.8 to $L = M_n(\mathcal{O}(S)) \times \cdots \times M_n(\mathcal{O}(S))$,

we obtain that there are only finitely many orbits of $G_{\mathcal{O}(S)}$ on $X_{\mathcal{O}(S)}$, as desired.

In general let us consider the Levi decomposition $G = HU$, where U is the unipotent radical of G, and H is reductive. Let $\pi: G \to G/U$ be the canonical projection. We can realize G/U in such a way that $\pi(G_{\mathcal{O}(S)}) \subset (G/U)_{\mathcal{O}(S)}$. Since $[(G/U)_{\mathcal{O}(S)} : \pi(G_{\mathcal{O}(S)})]$ is finite and the reductive case of Theorem 5.10 has already been considered, $\pi(G_{\mathcal{O}(S)})$ has a finite number of conjugacy classes of finite subgroups.

Let us consider an arbitrary finite subgroup $\Gamma = \{\gamma_1, \ldots, \gamma_d\}$ of $G_{\mathcal{O}(S)}$, and define a closed subset $A(\Gamma)$ of G^d as

$$A(\Gamma) = R(\Gamma, G) \cap \{(\delta_1, \ldots, \delta_d) : \pi(\delta_i) = \pi(\gamma_i)\}.$$

Then U acts naturally on $A(\Gamma)$ by conjugation. To complete the proof of the theorem it suffices to show that $A(\Gamma)_{\mathcal{O}(S)}$ consists of a finite number of orbits of $U_{\mathcal{O}(S)}$. Consider the morphism $\varphi: U \to A(\Gamma)$, given by

$$\varphi(g) = g^{-1}\gamma g = (g^{-1}\gamma_1 g, \ldots, g^{-1}\gamma_d g)$$

where $\gamma = (\gamma_1, \ldots, \gamma_d)$. Also, let U_1 denote the centralizer of Γ in U, and choose a K-subvariety $U_2 \subset U$ such that the product morphism $U_1 \times U_2 \to U$ is a K-isomorphism of varieties (cf. Lemma 2.1). (Note that in general it is not possible to choose a subgroup U_2 of U satisfying this property.)

LEMMA 5.10. *The restriction map $\varphi: U_2 \to A(\Gamma)$ is a K-isomorphism of varieties.*

PROOF: First we show that the action of U on $A(\Gamma)$ is transitive. Let $\delta = (\delta_1, \ldots, \delta_d) \in A(\Gamma)$ and $\Delta = \{\delta_1, \ldots, \delta_d\}$. Then Δ is a subgroup of G, and since Γ and Δ are reductive subgroups of G, by Theorem 2.3 there are $x, y \in U$ such that $x^{-1}\Gamma x \subset H$, $y^{-1}\Delta y \subset H$. For any $i = 1, \ldots, d$ we have

$$\pi(x^{-1}\gamma_i x) = \pi(\gamma_i) = \pi(\delta_i) = \pi(y^{-1}\delta_i y),$$

so the injectivity of $\pi\,|_H$ implies that

$$x^{-1}\gamma_i x = y^{-1}\delta_i y, \quad \text{i.e.,} \quad \delta = g^{-1}\gamma g = \varphi(g),$$

where $g = xy^{-1}$. Since the stabilizer of γ is precisely U_1, the restriction map $\varphi: U_2 \to A(\Gamma)$ is one-to-one. It remains to note that since $A(\Gamma)$ is a homogeneous variety and hence is also smooth, then by Zariski's fundamental theorem φ is an isomorphism.

Now let U be an abelian group. Then we can take U_2 to be a suitable subgroup of U (Lemma 2.1). It follows from Lemma 5.10 that the inverse image

$(\varphi\ |_{U_2})^{-1}(A(\Gamma)_{A_S(S)})$ is a compact subset of $U_{2_{A_S}}$ and therefore is contained in the union of a finite number of (left) cosets modulo the subgroup $U_{2_{A_S(S)}}$. But then $\varphi^{-1}(A(\Gamma)_{\mathcal{O}(S)}) = \varphi^{-1}(A(\Gamma)_{A_S(S)}) \cap U_{2_K}$ is contained in the union of a finite number of cosets modulo $U_{2_{\mathcal{O}(S)}} = U_{2_{A_S(S)}} \cap U_{2_K}$, as desired.

In general we use induction on the dimension of U. Let $Z(U)$ be the center of U, and consider $G' = G/Z(U)$. Then in $G'_{\mathcal{O}(S)}$ finite subgroups partition into a finite number of conjugacy classes. Since, by Theorem 5.9, the image of $G_{\mathcal{O}(S)}$ under the canonical morphism $G \to G'$ is an S-arithmetic subgroup, it follows that $G_{\mathcal{O}(S)}$ has only a finite number of conjugacy classes of subgroups of the form $\Gamma Z(U)_{\mathcal{O}(S)}$, where Γ is a finite subgroup of $G_{\mathcal{O}(S)}$. To complete the proof of Theorem 5.10 it suffices to show that finite subgroups of $\Gamma Z(U)_{\mathcal{O}(S)}$ partition into a finite number of conjugacy classes with respect to $G_{\mathcal{O}(S)}$. But Γ is contained in a suitable maximal reductive K-subgroup F of G. Then the unipotent radical of $D = FZ(U)$ is abelian, and $D_{\mathcal{O}(S)} \subset G_{\mathcal{O}(S)}$. Therefore the finite subgroups $D_{\mathcal{O}(S)}$ partition into a finite number of conjugacy classes in $G_{\mathcal{O}(S)}$. Q.E.D.

REMARK: Theorem 5.10 can be proved for G reductive in the same way as the analogous Theorem 4.3 was proved for arithmetic subgroups, using the Bruhat-Tits building for groups over non-Archimedean local fields (cf. §3.4).

We conclude with a result on finite presentability of S-arithmetic groups.

THEOREM 5.11. *Any S-arithmetic subgroup of a reductive group G is a group with a finite number of generators and a finite number of defining relations.*

PROOF: based on Reidemeister-Schreier's method from combinatorial group theory (cf. Lyndon-Schupp [1, Ch. 2, §4]), which we apply to $G_{\mathcal{O}(S)}$, viewed as a subgroup of $\Gamma = G_{S \setminus V_\infty^K}$. In §3.4 (Theorem 3.15) we showed that G_{K_v} is compactly presented for any $v \in V_f^K$; therefore, as one can easily see, $\Gamma = \prod_{v \in S \setminus V_\infty^K} G_{K_v}$ is also compactly presented. (Recall that this means that there exists a compact subset D of Γ which generates Γ and such that the relations $ab = c$, for $a, b, c \in D$, constitute the defining set of relations for Γ. Passing from D to $D \cup D^{-1} \cup \{e\}$, where e is the identity element of Γ, we may assume that $e \in D$ and $D = D^{-1}$.)

Now, let $F(X)$ denote a free group on the set X, and let D^* be the set whose elements are in one-to-one correspondence with the elements of D under the map $d^* \mapsto d$. Then the homomorphism $\varrho\colon F(D^*) \to \Gamma$ defined via the latter bijection is surjective, and $N = \ker \varrho$ is generated by elements of the form $a^* b^* c^{*-1}$, where $a^*, b^*, c^* \in D^*$ and $\varrho(a^* b^*) = \varrho(c^*)$, i.e., $ab = c$.

The system of representatives of cosets $F(D^*)/H$ (where $H = \varrho^{-1}(G_{\mathcal{O}(S)})$), which is needed in order to apply Reidemeister-Schreier's method, can be chosen as follows:

According to Proposition 5.11, there exists a compact subset C of Γ such that $\Gamma = G_{\mathcal{O}(S)} C$; moreover, without loss of generality we may assume that $e \in C$. Choose a system T of representatives of the cosets modulo $G_{\mathcal{O}(S)}$ which consists of elements of C and contains e; let T^* denote a system of representatives of $F(D^*)/H$ containing the identity element e^* of $F(D^*)$, such that ϱ gives a one-to-one correspondence between T^* and T. We introduce a map $F(D^*) \to T^*$, denoted by $x \mapsto \bar{x}$, which sends x to the representative $\bar{x}$ of Hx lying in T^*, i.e., to $\bar{x}$ in T^* such that $Hx = H\bar{x}$. Now take any x in H and write it as $x = d_1, \ldots, d_m$, where $d_i \in D^* \cup D^{*-1}$. Then

$$x = (d_1 \bar{d}_1^{-1})(\bar{d}_1 d_2 (\overline{d_1 d_2})^{-1}) \ldots (\overline{d_1 \ldots d_{m-1}} d_m (\overline{d_1 \ldots d_m})^{-1}),$$

since $\overline{d_1 \ldots d_m} = \bar{x} = e^*$. The $\overline{d_1 \ldots d_{i-1}} d_i (\overline{d_1 \ldots d_i})^{-1}$, provided by the Reidemeister-Schreier method, have x as their product, and lie in $X = (T^*(D^* \cup D^{*-1})T^{*-1}) \cap H$, which thereby is a system of generators for H. Furthermore, by assumption N as a normal subgroup of $F(D^*)$ is generated by abc^{-1} for those $a, b, c \in D^*$ for which $\varrho(ab) = \varrho(c)$. This means that any n in N can be written as

$$n = \prod_{i=1}^{e} g_i (abc^{-1})^{\varepsilon_i} g_i^{-1},$$

where $g_i \in F(D^*)$ and $\varepsilon_i = \pm 1$. Writing $g_i = h_i t_i$, where $h_i \in H$ and $t_i \in T^*$, we see that N as a normal subgroup of H is generated by xyz^{-1}, where $x, y, z \in T^* D^* T^{*-1}$ and $\varrho(xy) = \varrho(z)$. Since $\overline{xyz^{-1}} = e^*$, we have

$$xyz^{-1} = (x\bar{x}^{-1})(\bar{x}y(\overline{\bar{x}y})^{-1})((\overline{xyz^{-1}})z(\overline{\bar{x}y})^{-1})^{-1},$$

implying that N, as a normal subgroup of H, is generated by elements of the form xyz^{-1}, where $x, y, z \in T^{*2} D^* T^{*-2} \cap H$. This suggests that it is helpful to extend the system of generators X to the following set $Y = \varrho^{-1}(BC^2 DC^{-2} B \cap G_{\mathcal{O}(S)})$, where $B = \prod_{v \in S \setminus V_\infty^K} G_{\mathcal{O}_v}$ (from the definition of X, clearly $X \subset Y$). Then N as a normal subgroup of H is generated by xyz^{-1}, where $x, y, z \in Y$ and $\varrho(xy) = \varrho(z)$.

Now we show that Y can be diminished to obtain a finite set of generators of $G_{\mathcal{O}(S)}$. To do so, first we choose a subset Z of Y for which ϱ induces a bijection $Z \to \varrho(Y)$, and we define the projection $\pi\colon Y \to Z$ by the

condition $\varrho(x) = \varrho(\pi(x))$ for any x in Y. Consider the free groups $F(Y)$ and $F(Z)$, and the mutually inverse homomorphisms $F(Z) \underset{\alpha_2}{\overset{\alpha_1}{\rightleftarrows}} F(Y)$ induced by $Z \subset Y$ and π. The commutative diagram

$$\begin{array}{ccc} F(Z) & \underset{\alpha_2}{\overset{\alpha_1}{\rightleftarrows}} & F(Y) \\ & {\scriptstyle \varrho_2} \searrow \quad \swarrow {\scriptstyle \varrho_1} & \\ & G_{\mathcal{O}(S)} & \end{array} \tag{5.11}$$

where $\varrho_2 = \varrho_1 \circ \alpha_1$ and ϱ_1 is obtained as the compositions of ϱ and the homomorphism $\tau\colon F(Y) \to H$, yields $\ker \varrho_2 = \alpha_2(\ker \varrho_1)$. But $\ker \varrho_1$ is generated by $\ker \tau$ and elements of the form xyz^{-1}, for $x, y, z \in Y$ such that $\varrho(xy) = \varrho(z)$. It follows that $\ker \varrho_2$ is generated by $\ker(\tau \circ \alpha_1)$ and elements of the form xyz^{-1}, where $x, y, z \in Z$ and $\varrho(xy) = \varrho(z)$. By assumption ϱ yields a one-to-one correspondence between Y and $E \cap G_{\mathcal{O}(S)}$, where $E = BC^2DC^{-2}B$. But E is a compact subset of Γ and therefore can be covered by a finite number of translations of the open subgroup B. Therefore there exists a finite set of elements $y_1, \dots, y_r$ in $E \cap G_{\mathcal{O}(S)}$ such that

$$E \cap G_{\mathcal{O}(S)} = \bigcup_{i=1}^{r} y_i(G_{\mathcal{O}(S)} \cap B) = \bigcup_{i=1}^{r} y_i G_{\mathcal{O}}.$$

(Since $E = BE = EB$, note that also $E \cap G_{\mathcal{O}(S)} = G_{\mathcal{O}}(E \cap G_{\mathcal{O}(S)}) = (E \cap G_{\mathcal{O}(S)})G_{\mathcal{O}}$.)

By Theorem 4.2 we can choose a finite set $z_1, \dots, z_t$ of generators of $G_{\mathcal{O}}$. Then put $U = \{z_1, \dots, z_t\}$ and $W = \{y_1, \dots, y_r\} \cup U$; and, using the one-to-one correspondence between Z and $E \cap G_{\mathcal{O}(S)}$, identify these sets with the corresponding subsets of Z. By assumption we have an epimorphism $\varphi\colon F(U) \to G_{\mathcal{O}}$. Taking some section $\psi\colon G_{\mathcal{O}} \to F(U)$ for φ which is the identity map on U, we can define the map $Z \xrightarrow{\sigma} F(W)$, sending $y_i g$ to $y_i \psi(g)$ for g in $G_{\mathcal{O}}$. This map induces a homomorphism $\beta_2\colon F(Z) \to F(W)$, which is the inverse of $\beta_1\colon F(W) \to F(Z)$, the homomorphism given by $W \subset Z$. Moreover, we have the commutative diagram

$$\begin{array}{ccc} F(W) & \underset{\beta_2}{\overset{\beta_1}{\rightleftarrows}} & F(Z) \\ & {\scriptstyle \varrho_3} \searrow \quad \swarrow {\scriptstyle \varrho_2} & \\ & G_{\mathcal{O}(S)} & \end{array} \tag{5.12}$$

in which $\varrho_3 = \varrho_2 \circ \beta_1$, where ϱ_2 is taken from (5.11). Diagram (5.12) yields $\ker \varrho_3 = \beta_2(\ker \varrho_2)$. Therefore $\ker \varrho_3$ is generated by $\ker(\tau \circ \alpha_2 \circ \beta_2)$ and elements of the form xyz^{-1} where $x, y, z \in \sigma(Z)$ and $\varrho_3(xy) = \varrho_3(z)$.

We shall show that all the elements of the form xyz^{-1} or, equivalently, the relations $xy = z$ for such x, y, z, can in fact be reduced to a finite number of them. To do so, let us first consider the relations where $x \in \psi(G_{\mathcal{O}})$. Since $G_{\mathcal{O}}(E \cap G_{\mathcal{O}(S)}) = E \cap G_{\mathcal{O}(S)}$, $z_i y_j = y_k w_{ij}$ for all $i = 1, \dots, t$, $j = 1, \dots, r$, with suitable $k \in \{1, \dots, r\}$ and $w_{ij} \in G_{\mathcal{O}}$. Now take the relations

$$z_i y_j = y_k \psi(w_{ij}), \qquad \text{for } i = 1, \dots, t \text{ and } j = 1, \dots, r. \tag{5.13}$$

Adding (5.13) to a finite system of relations among the z_i, defining $G_{\mathcal{O}}$ (cf. Theorem 4.17(2)), we obtain a finite system of relations from which all the relations of the form $xy = z$ for $x \in \psi(G_{\mathcal{O}})$ can be deduced. Indeed, any x in $\psi(G_{\mathcal{O}})$ is a word in z_i's. Therefore, writing $y = y_j b$ and $z = y_k c$, for $b, c \in \psi(G_{\mathcal{O}})$, and using (5.13) an appropriate number of times, we reduce $xy = z$ to the form $y_l ab = y_k c$, where $a \in \psi(G_{\mathcal{O}})$. The equality $\varrho_3(xy) = \varrho_3(z)$ implies that $k = l$; then, canceling y_k, we obtain a relation $ab = c$ between the words in the z_i's, and by assumption all such relations have already been incorporated.

Now, let us take any x in $\sigma(Z)$ and write it as $x = y_i a$, where $a \in \psi(G_{\mathcal{O}})$. By what we proved, any relation of the form $xy = z$ can be reduced to

$$y_i y_j = y_k \psi(r_{ij}), \tag{5.14}$$

where $r_{ij} \in G_{\mathcal{O}}$ is the element of $G_{\mathcal{O}(S)}$ determined by $y_i y_j = y_k r_{ij}$. Thus all the relations of the form $xy = z$, where $x, y, z \in \sigma(Z)$ and $\varrho_3(xy) = \varrho_3(z)$, can be derived from a finite number of relations.

Equivalently, the normal subgroup of $F(W)$ generated by all xyz^{-1} for such x, y, z, is actually generated by a finite number of these elements. Therefore, if we take $\Phi = \alpha_2\beta_2(F(W))$, then our computations of $\ker \varrho_3$ imply that $\ker \varrho \mid_{\Phi} = \Phi \cap W$ is generated as a normal subgroup of Φ by a finite number of elements. It remains to note that since Φ is a finitely generated subgroup of $F(D^*)$, it is a free group of finite rank (by the Nielsen-Schreier Theorem); therefore $G_{\mathcal{O}(S)} \simeq \Phi/\Phi \cap N$ yields the desired finite presentation of $G_{\mathcal{O}(S)}$. Hence any S-arithmetic subgroup of G, being commensurable with $G_{\mathcal{O}(S)}$, is also finitely presented. Q.E.D.

The proof we have given of Theorem 5.11 is a formalized version of the original argument due to Kneser [7]. For the reader familiar with combinatorial group theory, such formalization at times may appear superfluous; in particular, he may prefer not to introduce $F(Y)$, $F(Z)$, etc., but rather to argue directly in Γ (which is possible, and is actually the approach used by Kneser). Nevertheless, even our exposition, aimed at the reader without appropriate background, clearly evinces the basic line of argument, which amounts to a reduction of the general case to the case $S = V_\infty^K$, when

$G_{\mathcal{O}(S)} = G_{\mathcal{O}}$, with finite presentability already proved in Theorem 4.17. This reduction can also be carried out by induction on $|S \setminus V_\infty^K|$, viewing $G_{\mathcal{O}(S)}$ as a subgroup of G_{K_v}, where $v \in S \setminus V_\infty^K$. In some cases appropriate modification of this induction argument makes it possible to determine explicit generators and relations for $G_{\mathcal{O}(S)}$, once one has a representation of $G_{\mathcal{O}}$ (for $G = \mathbf{SL}_2$, cf. Serre [10]).

There is also another proof of Theorem 5.11 in which the case $S = V_\infty^K$ in no way differs from the other cases (cf. Borel-Serre [4]). This proof is similar to the proof of Theorem 4.2 and uses the discrete action of $G_{\mathcal{O}(S)}$ on a suitable simply connected space, which is the product of the quotient space of G_∞ by a maximal compact subgroup, with the Bruhat-Tits buildings for the G_{K_v}, for $v \in S \setminus V_\infty^K$. As we have noted, this approach also yields another proof of Theorem 5.10 for reductive groups.

Note that in Theorem 4.2 we did not require that G be reductive. However, for nonreductive groups Theorem 5.11 generally does not hold. If $S \neq V_\infty^K$, then the additive group of $\mathcal{O}(S)$ is not finitely generated; therefore any S-arithmetic subgroup of the one-dimensional unipotent group $\mathbb{G}_a$ is not finitely generated either. On the other hand, if $B = \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & \alpha^{-1} \end{pmatrix} : \alpha \neq 0 \right\}$ is a Borel subgroup of $\mathbf{SL}_2$, then any S-arithmetic subgroup of B is finitely generated. In this regard, let us point out a criterion (proved by Kneser [7]) for a group to be finitely generated (finitely presented): the S-arithmetic subgroups of G are finitely generated (resp., finitely presented) if and only if G_{K_v} is compactly generated (resp., compactly presented) for every v in $S \setminus V_\infty^K$. Since a reductive group is always compactly presented (Theorem 3.15), the criterion for being compactly generated in general can be formulated in terms of the action of G on the unipotent radical $R_u(G)$. We recommend this as an exercise for the reader.

We conclude this chapter with a description of S-arithmetic subgroups of tori. The theorem below contains as special cases both Dirichlet's classic theorem on the structure of S-units in algebraic number fields, as well as the description of the usual arithmetic subgroups of tori, given in §4.5. (So, this theorem can naturally be called the generalized Dirichlet's theorem.) Its proof, published by Shyr [2], is practically identical to the proof of Theorem 9 in Chapter 4 of Weil [7].

THEOREM 5.12. *Let T be a torus defined over an algebraic number field K, and let S be a finite subset of V^K containing V_∞^K. Then the group of S-units $T_{\mathcal{O}(S)}$ is isomorphic to the product of a finite group and a free abelian group of rank $s = \sum_{v \in S} \operatorname{rank}_{K_v} T - \operatorname{rank}_K T$.*

PROOF: Clearly $T_{\mathcal{O}(S)} = T_{A(S)} \cap T_K$ is a discrete subgroup of $T_{A(S)}$. But, this does not immediately yield results about $T_{\mathcal{O}(S)}$, since $T_{A(S)}/T_{\mathcal{O}(S)}$ in general is noncompact. To obtain a compact quotient space one needs

to reduce $T_{A(S)}$ to $T_{A(S)}^{(1)} = T_{A(S)} \cap T_A^{(1)}$, with $T_A^{(1)}$ defined as in §5.3. Indeed, since $T_K \subset T_A^{(1)}$, we also have $T_{\mathcal{O}(S)} = T_{A(S)}^{(1)} \cap T_K$; and therefore $T_{A(S)}^{(1)}/T_{\mathcal{O}(S)}$ can be identified with an open-and-closed subspace of $T_A^{(1)}/T_K$, which is compact by Theorem 5.6.

Now we shall describe precisely the structure of $T_{A(S)}^{(1)}$. By definition $T_{A(S)} = \prod_{v \in S} T_{K_v} \times \prod_{v \notin S} T_{\mathcal{O}_v}$. We already know the structure of T_{K_v} for v in V_∞^K (cf. proof of Theorem 4.11, Corollary 1): $T_{K_v} \simeq \mathbb{R}^{r_v} \times B$, where $r_v = \operatorname{rank}_{K_v} T$ and B is compact. Now let $v \in S \setminus V_\infty^K$. Consider a decomposition $T = T_1 T_2$, in an almost direct product of a maximal K_v-split torus T_1 and a maximal K_v-anisotropic torus T_2 (cf. §2.1.7). Let B be a maximal compact subgroup of T_{K_v}. Then $T_{2K_v} \subset B$ since T_{2K_v} is compact (Theorem 3.1). Therefore, if $\varphi: T \to T_3 = T/T_2$ is the corresponding quotient map, then $T_{K_v}/B \simeq \varphi(T_{K_v})/\varphi(B)$. But T_3 is K_v-split, so $(T_3)_{K_v} \simeq (K_v^*)^{r_v} \simeq \mathbb{Z}^{r_v} \times U$, where $r_v = \dim T_3 = \operatorname{rank}_{K_v} T$ and U is compact. Since B is maximal, it follows that $\varphi(B) = U \cap \varphi(T_{K_v})$; hence $\varphi(T_{K_v})/\varphi(B) \subset \mathbb{Z}^{r_v}$, implying $\varphi(T_{K_v})/\varphi(B) \simeq \mathbb{Z}^t$ for some $t \leq r_v$. But T_1 is also a K_v-split subtorus of rank r_v, whence $T_{1K_v} \simeq \mathbb{Z}^{r_v} \times U_1$ for some compact subgroup U_1. Also, the subgroup of T_{1K_v} isomorphic to $\mathbb{Z}^{r_v}$ is discrete and therefore does not intersect B; thus T_{K_v}/B contains a free abelian group of rank r_v. Finally, $T_{K_v}/B \simeq \mathbb{Z}^{r_v}$, from which it follows easily that $T_{K_v} \simeq \mathbb{Z}^{r_v} \times B$. Combining our results on the Archimedean and non-Archimedean components, we obtain the following factorization of $T_{A(S)}$:

$$T_{A(S)} \simeq \mathbb{R}^\alpha \times \mathbb{Z}^\beta \times W,$$

where $\alpha = \sum_{v \in V_\infty^K} \operatorname{rank}_{K_v} T$, $\beta = \sum_{v \in S \setminus V_\infty^K} \operatorname{rank}_{K_v} T$, and W is compact.

Now it is easy to describe the structure of $T_{A(S)}^{(1)}$. First, recall that we introduced $T_A^{(1)}$ as the intersection of the kernels of the continuous homomorphisms $c_K(\chi): T_A \to \mathbb{R}^{>0}$ for all χ in $\mathbf{X}(T)_K$ where $c_K(\chi)((g_v)) = \prod_v \|\chi(g_v)\|_v$. Let $\chi_1, \ldots, \chi_r$ $(r = \operatorname{rank}_K T)$ be a base of $\mathbf{X}(T)_K$. Then we have a continuous homomorphism $\theta: T_A \to (\mathbb{R}^{>0})$, given by

$$g \overset{\theta}{\mapsto} (c_K(\chi_1)(g), \ldots, c_K(\chi_r)(g));$$

moreover $T_A^{(1)} = \ker \theta$. We claim that $\theta(T_{A(S)}) = (\mathbb{R}^{>0})^r$ for any $S \supset V_\infty^K$. Indeed, since $\chi_1, \ldots, \chi_r$ is a base of $\mathbf{X}(T)_K$, the morphism $\varphi: T \to \mathbb{G}_m^r$ given by $g \overset{\varphi}{\mapsto} (\chi_1(g), \ldots, \chi_r(g))$ is surjective. Therefore, applying Corollary 1 of Proposition 3.3, we see, for any $v \in V_\infty^K$, that the image of $\varphi(T_{K_v})$ is open and therefore contains the connected component of the

identity in $(K_v^*)^r$, which for v real is $(\mathbb{R}^{>0})^r$ and for v complex is $\mathbb{C}^{*r}$. It remains to note that the restriction of θ to T_{K_v} (appropriately embedded in T_A) is the composite of φ and of the r-th Cartesian power of the normalized valuation map $\| \|_v : K_v^* \to \mathbb{R}^{>0}$, so $\theta(T_{K_v})$ is $(\mathbb{R}^{>0})^r$ for each v in V_∞^K. Since $\mathbb{R}$ and $\mathbb{R}^{>0}$ are isomorphic, we can apply

LEMMA 5.11. *Let $\Gamma = \mathbb{R}^\alpha \times \mathbb{Z}^\beta \times W$, where W is compact. If $\theta : \Gamma \to \mathbb{R}^\gamma$ is a continuous surjective homomorphism, then $\gamma \leq \alpha$ and*

$$\ker \theta \simeq \mathbb{R}^{\alpha-\gamma} \times \mathbb{Z}^\beta \times W.$$

PROOF: Left to the reader as an exercise.

Thus, we can describe $T^{(1)}_{A(S)}$ by

$$T^{(1)}_{A(S)} \simeq \mathbb{R}^{\alpha-r} \times \mathbb{Z}^\beta \times W.$$

Above we showed that $T_{\mathcal{O}(S)}$ is a discrete subgroup of $T^{(1)}_{A(S)}$, and moreover $T^{(1)}_{A(S)}/T_{\mathcal{O}(S)}$ is compact. Therefore Theorem 5.12 follows from Lemma 4.14, noting that $(\alpha - r) + \beta$ is precisely the number s in the statement of the theorem. Q.E.D.

COROLLARY (DIRICHLET'S S-UNITS THEOREM). *Let K be an algebraic number field, and let S be a finite subset of V^K containing V_∞^K. Then the group of S-units $E(S) = \{ x \in K^* : |x|_v = 1 \text{ for all } v \notin S \}$ is isomorphic to the product of the group E of the roots of unity contained in K by a free abelian group of rank $|S| - 1$.*

BIBLIOGRAPHIC NOTE: The basic results of reduction theory for adele groups and S-arithmetic subgroups in the number-theoretic case can be found in Borel [1]. In his exposition, Borel essentially uses the reduction theory for arithmetic groups developed by himself and Harish-Chandra. Later Godement [1] showed how the same theorems can be obtained along different lines, independent of the reduction theorems for arithmetic groups. By elaborating Godement's method, Harder [5] was able to develop a reduction theory for adele groups over global fields of characteristic > 0. The basic theorems here are the same as in the number field case, except for the fact that the analog of Theorem 5.1 looks as follows: If S is a *nonempty* subset of V^K, then there are only finitely many double cosets $G_{A(S)} \setminus G_A / G_K$. However, the question of finite generation and finite presentation of S-arithmetic groups is not so clear-cut for global function fields as for number fields (in particular, there exist infinitely generated S-arithmetic groups). Behr [4] obtained an almost complete answer to the question of finite generation; some classical groups had been examined earlier by O'Meara [2]. The problem of finite presentability of S-arithmetic groups over a function field K has been solved affirmatively in general only for K-anisotropic groups (cf. Borel-Serre [4]). Until recently, the case of K-isotropic groups has not been considered in general. However, it is known that $SL_3(k[t])$, where k is a finite field, is finitely generated but not finitely presented (Behr [6]), and that $SL_2(\mathcal{O}(S))$ is finitely presented if and only if $|S| > 2$ (Stuhler [1]).

6. Galois cohomology

This chapter is devoted to results describing the first Galois cohomology set $H^1(K, G)$ of an algebraic group G over a field K of arithmetic type. Moreover, it includes some indispensable results on the cohomology of groups of v-adic integral points and adele groups. The material in this chapter will be used in Chapters 7 and 8; hence familiarity with it is essential for further reading of this book. However, since Galois cohomology is not generally speaking the emphasis of this book, we do not cover all aspects of cohomology theory, but focus on questions that are either connected with classical number-theoretic concepts (such as the local-global principle) or closely related to other results from the arithmetic theory of algebraic groups. In this sense the present chapter supplements Serre's well-known book [1] on cohomology theory. We shall refer the reader to this book for the proofs of general facts used in our exposition. Several results here have not been published before. For example, this is the first time a complete proof of the Hasse principle for simply connected groups is presented.

6.1. Statement of the main results.

This section assembles the main results describing $H^1(K, G)$, the first Galois cohomology set of an algebraic K-group G, for K a finite, local, or number field. The proofs will be given in the sections that follow. Several applications of these results and their connection with classical facts about the classification of quadratic, Hermitian, and other forms will be described in §§6.5–6.6. For the basic definitions relating to noncommutative Galois cohomology, see §1.3. (The reader may find a more systematic exposition in Serre's book [1]). Note that some proofs of the theorems in this chapter on cohomology of semisimple groups are highly technical and may be omitted in the first reading. (Actually, familiarity with this section suffices for understanding the rest of the book).

We begin with a finite field K, for which a full description of $H^1(K, G)$ is given by

THEOREM 6.1 (LANG [1]). *Let G be a connected algebraic group defined over a finite field K. Then $H^1(K, G) = 1$.*

The proof will be given in §6.2. There we shall also present several corollaries of Theorem 6.1. In particular, we shall show that any connected group over a finite field K is quasisplit, i.e., contains a K-defined Borel subgroup. In view of Hensel's lemma, another important result follows: If G is a connected group defined over a number field K, then it is quasisplit over the completions K_v, for almost all v in V_f^K.

Moreover, Theorem 6.1 has some implications concerning the cohomology of groups of v-adic integral points and adelic groups, which will be used later in our exposition. Note that a result of Steinberg (cf. Theorem 6.23) implies that Theorem 6.1 holds even in the more general case of a field K of cohomological dimension $\mathrm{cd}(K) \leq 1$. In most other cases $H^1(K, G)$ is nontrivial in general; and hence there is the problem of describing it. It follows from Proposition 2.9 that we need only consider the case of a reductive group G. According to Theorem 2.4, such a group is an almost direct product of a torus and a semisimple group, and therefore the computation of $H^1(K, G)$ essentially reduces to two main cases:

(a) G is a torus;
(b) G is a semisimple group.

Note that the results for semisimple groups differ inherently from those for tori, and in fact the latter are actually used in the semisimple case. For this reason we shall first examine the case of algebraic tori.

It is well known (see §2.1.7) that any K-torus T is defined up to isomorphism by assigning to the group of characters $\mathbf{X}(T)$ the structure of a module over the absolute Galois group $Gal(\bar{K}/K)$. (Recall that we always assume K to be perfect; moreover, in most cases $\mathrm{char}\, K = 0$.) Therefore it is natural to try to link the cohomology groups $H^1(K, T)$ and $H^1(K, \mathbf{X}(T))$. Here, first of all, it is helpful to replace the cohomology of the profinite group $\mathrm{Gal}(\bar{K}/K)$ by the cohomology of a finite quotient group. To do so, note (see Lemma 6.8) that $H^1(K, T) = H^1(L/K, T)$ and $H^1(K, T) = H^1(L/K, \mathbf{X}(T))$, where L is a splitting field for T (i.e., a finite Galois extension of K over which T becomes split).

In what follows it is convenient to pass from the usual group cohomology to the modified cohomology groups introduced by Tate. A precise definition of the Tate cohomology groups $\hat{H}^i(G, A)$ of a finite group G with coefficients in a commutative G-module A will be given in §6.3, but for the time being we shall limit ourselves to pointing out that $\hat{H}^i(G, A)$ are defined for all integral values of i, and $\hat{H}^i(G, A) = H^i(G, A)$ for $i \geq 1$. Besides, Tate cohomology retains the basic property of the usual cohomology: a short exact sequence of G-modules $0 \to A \to B \to C \to 0$ gives rise to the following infinite exact sequence going in both directions:

$$\ldots \to \hat{H}^q(G, A) \to \hat{H}^q(G, B) \to \hat{H}^q(G, C) \to \hat{H}^{q+1}(G, A) \to \ldots$$

With this notation we have

THEOREM 6.2 (NAKAYAMA-TATE; LOCAL VERSION). *Let K be a local field. Then for any K-torus T with splitting field L and any integer i, we have the isomorphism*

$$\hat{H}^i(L/K, T) \cong \hat{H}^{2-i}(L/K, \mathbf{X}(T)).$$

In particular, $H^1(L/K, T) \simeq H^1(L/K, \mathbf{X}(T))$.

It should be noted that the isomorphism in Theorem 6.2 arises as an isomorphism of a finite Abelian group with its dual. To obtain a natural isomorphism, instead of using the group of characters $\mathbf{X}(T)$ we ought to consider the dual group of cocharacters (or one-parameter subgroups) $\mathbf{X}_*(T) = \mathrm{Hom}(\mathbb{G}_m, T)$ (cf. §2.1.7), and then $\hat{H}^{i-2}(L/K, \mathbf{X}_*(T)) \simeq \hat{H}^i(L/K, T)$, this isomorphism being induced by the cup product with the generator of $\hat{H}^2(L/K, L^*) = \mathrm{Br}(L/K) \simeq \frac{1}{n}\mathbb{Z}/\mathbb{Z}$ where $n = [4\colon K]$ (for details see §6.3).

It follows from Theorem 6.2 that $H^1(K, T)$ is finite for a local field K. We shall see below that this result still holds if we replace T by an arbitrary algebraic K-group.

The study of $H^1(K, T)$ for a torus T over a number field K is based on analyzing the map $H^1(L/K, T) \to \prod_v H^1(L_w/K_v, T)$ (a single extension $w|v$ is selected for each v). It is easy to see that the image lies in $H^1(L/K, T_{A_L})$, where A_L is the adele ring of L, so that we actually have a map $H^1(L/K, T) \xrightarrow{\varphi} H^1(L/K, T_{A_L})$. To compute its kernel and cokernel, consider the exact sequence

$$1 \to T_L \to T_{A_L} \to C_L(T) \to 1,$$

where $C_L(T) = T_{A_L}/T_L$ is the adele class group of T over L, and the corresponding cohomological sequence

$$H^0(L/K, C_L(T)) \to H^1(L/K, T) \xrightarrow{\varphi} H^1(L/K, T_{A_L}) \to H^1(L/K, C_L(T)).$$

A description of the cohomology groups $\hat{H}^i(L/K, C_L(T))$ is given by

THEOREM 6.3 (NAKAYAMA-TATE; GLOBAL VERSION). *Let K be a number field. Then, for any integer i and any K-torus T with splitting field L, there is an isomorphism*

$$\hat{H}^i(L/K, C_L(T)) \simeq \hat{H}^{2-i}(L/K, \mathbf{X}(T)).$$

The remark following Theorem 6.2 applies equally well to Theorem 6.3. Moreover, it should be noted that notwithstanding the different objects involved in the statement of Theorems 6.2 and 6.3, the proofs of both theorems rest on the same cohomological formalism (i.e., the Tate theorem, cf. §6.3), whose use is justified respectively by local and global class field

theory. Furthermore, note that in §6.3 we shall study the inter-relations between the ismorphisms in Theorems 6.2 and 6.3.

It follows from Theorem 6.3 that the kernel and the cokernel of φ are finite. The group $\ker\varphi$ is called the *Shafarevich-Tate group* of T, denoted by $Ш(T)$. If $Ш(T) = 1$ then T is said to satisfy the local-global, or Hasse, principle; in general $Ш(T)$ expresses the deviation from the local-global principle. This terminology is natural since, for the normed torus $T = \mathbf{R}^{(1)}_{L/K}(\mathbb{G}_m)$ the triviality of $Ш(T)$ is equivalent to the classical Hasse norm principle for L/K. Using Theorems 6.2 and 6.3, Tate showed that, for a Galois extension L/K with Galois group $\mathcal{G}$, and for $T = \mathbf{R}^{(1)}_{L/K}(\mathbb{G}_m)$, the group $Ш(T)$ is isomorphic to the kernel of the canonical homomorphism $H^3(\mathcal{G},\mathbb{Z}) \to \prod_v H^3(\mathcal{G}_v,\mathbb{Z})$, where $\mathcal{G}_v$ is the decomposition group of some extension of v. Until recently, however, no research had been done on $Ш(T)$ for $T = \mathbf{R}^{(1)}_{L/K}(\mathbb{G}_m)$ when L/K is not a Galois extension. Analysis of this case appears in Platonov-Drakokhrust [1], [2], Drakokhrust-Platonov [1] and Drakokhrust [1]; these results are set forth in §6.3.

Qualitatively, Theorems 6.2 and 6.3 provide two basic facts about Galois cohomology of algebraic tori: the finiteness of $H^1(K,T)$ for tori over a local field K, and the finiteness of $Ш(T)$ for tori over a number field K. In §6.4 we establish that these two facts hold for any algebraic group. Of course, the proofs for the general case rely on entirely different arguments from those used to prove Theorems 6.2 and 6.3. To be more precise, it turns out that the finiteness of $H^1(K,G)$ for a local field K (Theorem 6.14) is actually independent of the structure of G and is a consequence of a certain special property of the absolute Galois group $\mathrm{Gal}(\bar{K}/K)$ of K (which we call property (F)). On the other hand, the finiteness of the kernel[1] $Ш(G)$ of the map $H^1(K,G) \to \prod_v H^1(K_v,G)$ (Theorem 6.15) follows from the reduction theory for adele groups, developed in Chapter 5.

Let us consider the problem of the precise computation of the cohomology. As we have noted, we may confine ourselves to the case of reductive groups, which, modulo the results on the cohomology of tori, reduces to the case of semisimple groups.

If G is a semisimple group over a local field K, then, in contrast to the situation for a finite field, $H^1(K,G)$ need not be trivial; however the following is true:

THEOREM 6.4. *Let G be a simply connected semisimple group over a non-Archimedean local field K. Then $H^1(K,G) = 1$.*

[1] Recall that in noncommutative cohomology the kernel is the inverse image of the distinguished element, i.e., of the equivalence class of the trivial cocycle.

To compute $H^1(K,G)$ for any semisimple group G over a local field K, consider the universal K-covering $\tilde{G} \xrightarrow{\pi} G$ (cf. Proposition 2.10). From the exact sequence $1 \to F \to \tilde{G} \xrightarrow{\pi} G \to 1$, where $F = \ker\pi$ is the fundamental group of G, and by the centrality of F, we obtain a map $\delta: H^1(K,G) \to H^2(K,F)$ (cf. §2.2.3), and the main result is that δ is bijective. (Note that injectivity of δ follows from Theorem 6.4, and surjectivity will be established in Theorem 6.20). In particular, the set with a distinguished element $H^1(K,G)$ is endowed with the natural structure of an abelian group. The proof of Theorem 6.4, presented in §§6.7–6.8, uses structural information about semisimple groups and their classification. There is also a uniform proof of Theorem 6.4 based on Bruhat-Tits theory (cf. Bruhat-Tits [2]).

In proving Theorem 6.4 the following important result will also be obtained.

THEOREM 6.5. *Let G be a simply connected simple anisotropic group over a local field K. Then $G = \mathbf{SL}_1(D)$ for some finite dimensional division algebra D over K.*

Although Theorem 6.5 can also be derived from Bruhat-Tits theory, we decided to give the proof of Theorems 6.4 and 6.5 which uses a structural argument, since it also works in the study of cohomology over number fields (where at present there is no alternate proof of the corresponding results). Note the conjecture in Serre [1] that the analogous assertion to Theorem 6.4 must hold whenever the cohomological dimension $\mathrm{cd}(K) \leq 2$. On the other hand, the question of the validity of Theorem 6.20 in this case (i.e., the question of the surjectivity of the coboundary map δ) reduces to the classical question in the theory of simple algebras of whether the exponent and the index of simple K-algebras are the same. Artin [1] presents this as a conjecture for C_2-fields, which are actually those fields having cohomological dimension ≤ 2.

Theorem 6.4 also implies several facts about the classification of simple groups, which we shall need in Chapter 7 to prove the Kneser-Tits conjecture over local fields. For example, any group of type ${}^2E_6$ over a local field is quasisplit, and any group of type E_7 becomes split over any quadratic extension of K.

As in the case of tori, computation of $H^1(K,G)$ over a number field K is based on analysis of a canonical map $H^1(K,G) \xrightarrow{\varrho} \prod_v H^1(K_v,G)$. If ϱ is injective it is natural to say that the Hasse principle holds for G, since the injectivity of ϱ for $G = \mathbf{O}_n(f)$ is equivalent to the validity of the local-global principle for equivalence of quadratic forms. Unfortunately ϱ is not always injective; however, it was conjectured quite a while ago (cf. Serre [1])

that ϱ is injective when G is simply connected. The proof of this fact for the classical groups (cf. Kneser [12]) is closely related to classical results on the classification of quadratic, Hermitian and other forms. Harder [1], [2] studied the exceptional groups of types other than E_8; however, groups of type E_8 remained unexamined for over two decades. The proof presented here was obtained quite recently by Chernousov [6]. Thus §§6.7–6.8 contain the first complete proof of the Hasse principle for simply connected groups.

According to Theorem 6.4, for a simply connected group G we have $H^1(K_v, G) = 1$ if v is non-Archimedean, therefore ϱ actually reduces to the map $H^1(K, G) \xrightarrow{\theta} \prod_{v \in V_\infty^K} H^1(K_v, G)$, which is injective by the Hasse principle. In fact one has the following result:

THEOREM 6.6. *θ is bijective for a simply connected K-group G.*

To complete the picture, it remains to describe the real cohomology $H^1(\mathbb{R}, G)$ of a simply connected simple $\mathbb{R}$-group G. For $G_{\mathbb{R}}$ compact, this has been done in Serre [1, Ch. 3, §4.5]. The general case was recently handled by Borovoi [2].

As in the local case, to compute $H^1(K, G)$ for an arbitrary semisimple group G, one has to consider the exact sequence

$$1 \to F \to \tilde{G} \to G \to 1,$$

where $\tilde{G}$ is simply connected and $F = \ker \pi$ is the fundamental group of G. Then one can show that in the resulting exact cohomological sequence $H^1(K, \tilde{G}) \to H^1(K, G) \xrightarrow{\delta} H^2(K, F)$ the map δ is surjective (Theorem 6.20). Furthermore, one can prove an analog of Theorem 6.5 for totally imaginary number fields.

Using the Hasse principle for simply connected groups, we also prove it for adjoint groups; whence, in turn, several facts follow about the classification of simple groups over number fields. In particular, any simple group of type B_n, C_n, E_7, E_8, F_4, or G_2 over a number field K splits over some quadratic extension of K.

The results described enable us to compute $H^1(K, G)$ for any connected algebraic group G over a local or a number field K. As Borovoi has noted, using his concept of the fundamental group of an arbitrary connected algebraic group and the results of Kottwitz [1], [2] one can formulate these results in a uniform manner similar to Theorems 6.2 and 6.3.

6.2. Cohomology of algebraic groups over finite fields.

We begin with the proof of Lang's theorem that $H^1(K, G) = 1$ for any connected algebraic group G defined over a finite field K (cf. Theorem 6.1).

It suffices to prove that $H^1(L/K, G) = 1$ for any finite extension L/K. It is well known that $\mathrm{Gal}(L/K)$ is cyclic and is generated by the Frobenius automorphism $\varphi: x \mapsto x^q$ for x in L, where $q = |K|$. (Note that the latter formula simultaneously defines an automorphism of $\mathrm{Gal}(\bar{K}/K)$, which we shall also call the Frobenius automorphism and also denote by φ. Clearly φ is a topological generator of $\mathrm{Gal}(\bar{K}/K)$.) Let $g = \{ g_\sigma \} \in Z^1(L/K, G)$ be a cocycle. We claim that to prove that g is trivial it suffices to find x in $G_{\bar{K}}$ satisfying $g_\varphi = x^{-1}\varphi(x)$. Indeed, then

$$g_{\varphi^2} = g_\varphi \varphi(g_\varphi) = x^{-1}\varphi(x)\varphi(x^{-1}\varphi(x)) = x^{-1}\varphi^2(x),$$

and analogously, using straightforward induction, we easily obtain $g_{\varphi^i} = x^{-1}\varphi^i(x)$ for any i. If $n = [L : K]$, then $g_{\varphi^n} = g_e = 1$; but on the other hand, $g_{\varphi^n} = x^{-1}\varphi^n(x)$, from which it follows that $\varphi^n(x) = x$, i.e., $x \in G_L$, thus establishing that g is a trivial cocycle of $Z^1(L/K, G)$. This would complete the proof of Lang's theorem.

LEMMA 6.1. *If G is a connected K-group, then $X = \{ x^{-1}\varphi(x) : x \in G_{\bar{K}} \}$ is precisely $G_{\bar{K}}$.*

PROOF: Based on the interpretation of the action of φ on $G_{\bar{K}}$ as a regular K–morphism of varieties. Namely, for any K-subvariety $V \subset \mathbb{A}^n$ and any point $x = (x_1, \ldots, x_n)$ in $V_{\bar{K}}$, put $x^{(q)} = (x_1^q, \ldots, x_n^q)$. Then $x^{(q)} \in V_{\bar{K}}$, so $f_q: x \mapsto x^{(q)}$ yields a regular K-endomorphism of V, which on the $\bar{K}$-points is the Frobenius automorphism. (Note that f_q is bijective and is independent of the choice of affine realization of V). Direct computation shows that $d_x f_q$ is the zero map for any point x in V. We apply these facts to the connected algebraic K-group G.

LEMMA 6.2. *Let $a \in G$. Then the map $s_a: G \to G$, given by $s_a(g) = g^{-1}ag^{(q)}$, is separable. Its image is open and closed.*

PROOF: We have

$$d_e s_a(X) = -Xa + d_e f_q(X) = -Xa, \quad X \in T_e(G),$$

so the differential map $d_e s_a: T_e(G) \to T_a(G)$ defines an isomorphism of the tangent spaces. It follows that s_a is a dominant separable morphism (cf. Borel [8, Ch. AG, Theorem 17.3]). In particular, the image of $s_a(G)$ contains an open subset of G. But $s_a(G)$ can be interpreted as an orbit under the action $G \times G \to G$ given by $(g, h) \mapsto g^{-1}hg^{(q)}$, so the entire set $s_a(G)$ is open in G. Since this holds for any a, the $s_a(G)$ are also closed, and Lemma 6.2 is proved.

Since G is connected, it follows from Lemma 6.2 that $s_a(G) = G$ for any a in G; in particular, $s_e(G) = G$ and $s_e(G_{\bar{K}}) = G_{\bar{K}}$. On the other hand, it

is easy to see that $s_e(G_{\bar{K}})$ is the set X in Lemma 6.1. This completes the proof of Lemma 6.1 and Lang's theorem.

Notwithstanding its simplicity, Lang's theorem has several important corollaries.

PROPOSITION 6.1. *Let G be a connected algebraic group over a finite field K. Then G is K-quasisplit, i.e., contains a K-defined Borel subgroup. In addition, any two Borel K-subgroups of G are conjugate by an element of G_K.*

PROOF: Let B be a Borel subgroup of G defined over $\bar{K}$, let φ be the Frobenius automorphism in $\mathrm{Gal}(\bar{K}/K)$, and let B^φ be the Borel subgroup obtained by applying φ. By the conjugacy theorem we can find g in $G_{\bar{K}}$ such that $gB^\varphi g^{-1} = B$. However, $g = x^{-1}\varphi(x)$ for some x in $G_{\bar{K}}$, by Lemma 6.1. Then, putting $H = xBx^{-1}$, we obtain a Borel subgroup of G which, by virtue of $H^\varphi = \varphi(x)B^\varphi\varphi(x)^{-1} = xgB^\varphi g^{-1}x^{-1} = H$, is defined over K.

Now let B_1, B_2 be Borel K-subgroups of G. Then $B_2 = gB_1g^{-1}$ for a suitable g in $G_{\bar{K}}$. Since B_i $(i = 1, 2)$ are defined over K, we have $B_i^\varphi = B_i$, implying

$$\varphi(g)B_1^\varphi\varphi(g)^{-1} = gB_1g^{-1};$$

so $g^{-1}\varphi(g)$ lies in the normalizer $N_G(B_1)$, which by Chevalley's theorem (cf. Borel [8, §11]) is B_1. Applying Lemma 6.1 to B_1, we obtain $g^{-1}\varphi(g) = b^{-1}\varphi(b)$ for a suitable b in $(B_1)_{\bar{K}}$. Then, putting $h = gb^{-1}$, we have $\varphi(h) = h$, i.e., $h \in G_K$ and $hB_1h^{-1} = gB_1g^{-1} = B_2$. This completes the proof of the proposition.

COROLLARY 1 (WEDDERBURN'S THEOREM). *Let K be a finite field. Then there are no noncommutative finite-dimensional central division algebras over K.*

Indeed, let D be a finite-dimensional central division algebra over K. Consider $G = \mathbf{SL}_1(D)$ (cf. §2.3). Suppose $D \neq K$; then G is a nontrivial simple K-anisotropic group (Proposition 2.7). But by Proposition 6.1 this group must be quasisplit; in particular, $\mathrm{rank}_K G > 0$; contradiction.

Another proof may be given using the property that the isomorphism classes of central simple algebras over K of dimension n^2 are in one-to-one correspondence with the elements of $H^1(K, H)$, where $H = \mathbf{PGL}_n$. Since $H^1(K, H) = 1$, there exists only one such algebra, viz. $M_n(K)$, which is not a division algebra.

PROPOSITION 6.2. *Let G be a connected group over a finite field K, and let W be a nonempty K-variety with a transitive K-defined action of G. Then $W_K \neq \emptyset$. Moreover, if the stabilizer $G(x)$ of a point x in W is connected, then G_K acts transitively on W_K.*

PROOF: Let $y \in W_{\bar{K}}$. By transitivity, we have g in $G_{\bar{K}}$ such that $g\varphi(y) = y$ (where, as above, φ is the Frobenius automorphism) and, by Lemma 6.1, we may represent it as $g = h^{-1}\varphi(h)$, where $h \in G_{\bar{K}}$. Then $\varphi(hy) = hy$, i.e., $z = hy \in W_K$. If the stabilizer $G(x)$ of some point x in W is connected, then the stabilizer of any point is connected, since W is homogeneous; in particular, $H = G(z)$ is connected. As we know (cf. §1.3.2), the orbits of G_K on W_K are in one-to-one correspondence with the elements of

$$\ker(H^1(K, H) \to H^1(K, G)).$$

But since $H^1(K, H) = 1$, there is in fact only one orbit.

Note that Proposition 6.1 actually is a direct consequence of Proposition 6.2, since by Theorem 2.19 the set of all the Borel subgroups of a connected K-group G is endowed with the natural structure of a K-defined homogeneous space of G. However, we preferred to present a direct proof.

COROLLARY 2. *Let L be a finite extension of a finite field K. Then the norm map $N_{L/K}\colon L^* \to K^*$ is surjective.*

Let $a \in K^*$. Then $W = \{\, x \in L \otimes_K \bar{K} : N_{L/K}(x) = a \,\}$ is a homogeneous space of the norm torus $T = \mathbf{R}^{(1)}_{L/K}(\mathbb{G}_m)$, and therefore $W_K \neq \emptyset$, i.e., $a \in N_{L/K}(L^*)$. One can also use Theorem 6.1 and the fact that $H^1(K, T) = K^*/N_{L/K}(L^*)$ (cf. Lemma 2.5).

COROLLARY 3. *Let f be a nondegenerate quadratic form in $n \geq 2$ variables over a finite field K. Then f represents any element of K. Consequently, any form in $n \geq 3$ variables represents zero over K.*

Indeed, if $a \in K^*$, then by Witt's theorem (cf. Theorem 2.10), for $n \geq 2$ the quadric $W = \{\, x \in \bar{K}^n : f(x) = a \,\}$ is a homogeneous space of the connected group $G = \mathbf{SO}_n(f)$, and therefore the assertion follows from Proposition 6.2. The fact that a nondegenerate quadratic form f in $n \geq 3$ variables is isotropic follows from Proposition 2.14 since $G = \mathbf{SO}_n(f)$ is K-quasisplit (Proposition 6.1) and, in particular, K-isotropic.

To complete the description of the basic properties of quadratic forms over finite fields, recall (cf. Proposition 2.8) that $H^1(K, \mathbf{SO}_n(f))$ classifies the equivalence classes of n-dimensional quadratic forms over K whose discriminants are equal to the discriminant of f. Therefore, Theorem 6.1 yields

COROLLARY 4. *Two nondegenerate n-dimensional quadratic forms over a finite field K are equivalent if and only if they have the same discriminant. Thus, for any n there are precisely 2 equivalence classes of nondegenerate n-dimensional forms.*

Note that the second assertion follows from the first and from the fact that $[K^* : K^{*2}] = 2$, since K^* is cyclic.

PROPOSITION 6.3 (LANG'S ISOGENY THEOREM). *Let G and H be connected K-groups, and let $\pi: G \to H$ be a K-defined isogeny (where K is a finite field). Then G_K and H_K contain the same number of elements.*

PROOF: Put $F = \ker \pi$ and consider the exact sequence

$$1 \to F_{\bar{K}} \to G_{\bar{K}} \to H_{\bar{K}} = 1.$$

Passing to cohomology, we obtain the exact sequence

$$F_K \to G_K \to H_K \to H^1(K, F) \to H^1(K, G)$$

(note that K is perfect). Since $H^1(K, G) = 1$ (Theorem 6.1), we arrive at the following equality:

$$|H_K| = |G_K| \frac{|H^1(K, F)|}{|F_K|},$$

and it suffices to show that $|H^1(K, F)| = |F_K|$. But since $\mathrm{Gal}(\bar{K}/K) \simeq \hat{\mathbb{Z}}$ (the profinite completion of $\mathbb{Z}$), this follows from the following

LEMMA 6.3. *For any finite $\hat{\mathbb{Z}}$-module F, we have $|H^0(\hat{\mathbb{Z}}, F)| = |H^1(\hat{\mathbb{Z}}, F)|$.*

PROOF: The lemma is a direct consequence of the properties of Herbrand's index (cf., for example, ANT, Ch. 4, §8), but it can also be proved directly. Let σ denote a generator of $\hat{\mathbb{Z}}$. Since F is finite, it follows that there is some m such that σ^m acts trivially on F. Thus $\prod_{i=0}^{m-1} \sigma^i(x)$ lies in the group of fixed points F^σ, for any x in F. Therefore, setting $n = mf$, where $f = |F^\sigma|$, we have

$$\prod_{i=0}^{n-1} \sigma^i(x) = \prod_{j=0}^{f-1} \sigma^{jm}\Big(\prod_{i=0}^{m-1} \sigma^i(x)\Big) = \Big(\prod_{i=0}^{m-1} \sigma^i(x)\Big)^f = 1. \tag{6.1}$$

Now we show that the restriction to $n\hat{\mathbb{Z}}$ of any cocycle from $Z^1(\hat{\mathbb{Z}}, F)$ is trivial. Indeed, by assumption the action of $m\hat{\mathbb{Z}}$ on F is trivial, and therefore the restriction of the cocycle $\zeta \in Z^1(\hat{\mathbb{Z}}, F)$ to $m\hat{\mathbb{Z}}$ is a homomorphism from $m\hat{\mathbb{Z}}$ to F. But then the restriction of ζ to $n\hat{\mathbb{Z}} = f(m\hat{\mathbb{Z}})$ is trivial.

The Hochschild-Serre sequence (cf. (1.9)) implies that

$$H^1(\mathbb{Z}, F) = H^1(\mathbb{Z}/n\mathbb{Z}, F),$$

taking the induced action of $\mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}}/n\hat{\mathbb{Z}}$ on F. Moreover, $H^0(\hat{\mathbb{Z}}, F) = H^0(\mathbb{Z}/n\mathbb{Z}, F)$. Let τ be the image of σ in $\mathbb{Z}/n\mathbb{Z}$. Since $H^1(\mathbb{Z}/n\mathbb{Z}, F) = N/(1-\tau)F$, where $N = \{x \in F : \prod_{i=0}^{n-1} \tau^i(x) = 1\}$, in view of (6.1) we obtain:

$$|H^1(\mathbb{Z}/n\mathbb{Z}, F)| = \frac{|F|}{|(1-\tau)F|} = \frac{|F|}{|F|/|F^\tau|} = |F^\tau| = |H^0(\mathbb{Z}/n\mathbb{Z}, F)|.$$

This completes the proof of the lemma.

Theorem 6.1 can also be used to classify simple K-groups (in this regard, it suffices to consider only simply connected groups). Since by Proposition 6.2 any K-group is quasisplit, all the K-forms of a simply connected simple K-group with a root system R can be classified by elements of $H^1(K, \mathrm{Sym}(R))$, where $\mathrm{Sym}(R)$ is the group of symmetries of the Dynkin diagram of R (cf. §2.2.4).

Bearing in mind that $\mathrm{Gal}(\bar{K}/K) = \hat{\mathbb{Z}}$, we obtain that any K-group of type B_n, C_n, E_7, E_8, F_4 or G_2 is split over K; for each of the types A_n (where $n \geq 2$), D_n (where $n \geq 5$), and E_6 there exist precisely two nonisomorphic K-groups—one split and the other nonsplit (note that the latter is quasisplit and splits over a quadratic extension of K); for type D_4 there are three nonisomorphic K-groups—one split and two nonsplit, which become split over a quadratic and a cubic extension of K, respectively.

The following important result for groups over number fields follows from Lang's theorem and Hensel's lemma.

THEOREM 6.7. *Let G be a connected group over a number field K. Then G is K_v-quasisplit for almost all v in V_f^K.*

PROOF: Let $\mathcal{B}$ be the variety of Borel subgroups of G (cf. §2.4.6). Then it follows from Proposition 3.19 that there exist smooth reductions $\underline{G}^{(v)}$ and $\underline{\mathcal{B}}^{(v)}$, for almost all v in V_f^K. We claim that $\underline{\mathcal{B}}^{(v)}$ is the variety of Borel subgroups of $\underline{G}^{(v)}$, for almost all v. (Note that by Theorem 3.12 the reduction $\underline{G}^{(v)}$ is a connected group for almost all v, and therefore the concept of the "variety of Borel subgroups" is meaningful.) Indeed, let L/K be a finite extension for which there exists a Borel L-subgroup B of G. Then over L, $\mathcal{B} = G/B$, and hence we have $\underline{\mathcal{B}}^{(w)} = \underline{G}^{(w)}/\underline{B}^{(w)}$ for almost all w in V_f^L (cf. Proposition 3.22). Since $\underline{\mathcal{B}}^{(w)}$ is projective, it follows that $\underline{B}^{(w)}$, being solvable, is a Borel subgroup of $\underline{G}^{(w)}$. Therefore, for almost all w in V_f^L, $\underline{\mathcal{B}}^{(w)}$ is the variety of Borel subgroups of $\underline{G}^{(w)}$. But it is well-known (cf. Lemma 3.11) that $\underline{G}^{(w)} = \underline{G}^{(v)}$ and $\underline{\mathcal{B}}^{(w)} = \underline{\mathcal{B}}^{(v)}$, for almost all v in V_f^K and the corresponding $w|v \in V_f^L$. By Proposition 6.1,

it follows from the above that $\underline{\mathcal{B}}^{(v)}_{k_v} \neq \emptyset$, where k_v is the residue field of K with respect to v. Since $\underline{\mathcal{B}}^{(v)}$ is smooth, applying the projective analog of Hensel's lemma, we obtain that $\mathcal{B}_{\mathcal{O}_v} \neq \emptyset$; in particular, $\mathcal{B}_{K_v} \neq \emptyset$, i.e., G contains a Borel K_v-subgroup. Q.E.D.

Lastly, using Lang's theorem we shall now obtain some essential results on cohomology of groups of v-adic integral points and adelic groups. Let G be an algebraic group defined over a local field K_v and let L_w/K_v be a finite Galois extension. Then the group of w-adic integral points $G_{\mathcal{O}_w}$ (where $\mathcal{O}_w = \mathcal{O}_{L_w}$) is invariant with respect to $\mathrm{Gal}(L_w/K_v)$, so the first cohomology set $H^1(L_w/K_v, G_{\mathcal{O}_w})$ is defined.

THEOREM 6.8. *If a connected group G has a connected smooth reduction $\underline{G}^{(v)}$ and the extension L_w/K_v is unramified, then $H^1(L_w/K_v, G_{\mathcal{O}_w}) = 1$.*

PROOF: Let $\mathfrak{p}_v$ and $\mathfrak{P}_w$ be the maximal ideals of $\mathcal{O}_v$ and $\mathcal{O}_w$ respectively, and let k_v and l_w be the corresponding residue fields. Since $\underline{G}^{(v)}$ is a smooth reduction, by Hensel's lemma we have the exact sequence

$$1 \to G_{\mathcal{O}_w}(\mathfrak{P}_w) \to G_{\mathcal{O}_w} \to \underline{G}^{(v)}_{l_w} \to 1. \tag{6.2}$$

Since L_w/K_v is unramified, $\mathrm{Gal}(L_w/K_v)$ and $\mathrm{Gal}(l_w/k_v)$ are isomorphic, and their actions on the groups in (6.2) are compatible. Therefore (6.2) yields the exact cohomological sequence

$$H^1(L_w/K_v, G_{\mathcal{O}_w}(\mathfrak{P}_w)) \to H^1(L_w/K_v, G_{\mathcal{O}_w}) \to H^1(l_w/k_v, \underline{G}^{(v)}_{l_w}). \tag{6.3}$$

The last term of (6.3) is trivial by Lang's theorem, so it suffices to establish that $H^1(L_w/K_v, G_{\mathcal{O}_w}(\mathfrak{P}_w))$ is also trivial.

LEMMA 6.4. *For any integer $j \geq 1$ we have*

$$H^1(L_w/K_v, G_{\mathcal{O}_w}(\mathfrak{P}_w^j)/G_{\mathcal{O}_w}(\mathfrak{P}_w^{j+1})) = 1.$$

PROOF: Let $G \subset \mathbf{GL}_n$. Consider the map $GL_n(\mathcal{O}_w, \mathfrak{P}_w^j) \xrightarrow{\theta} M_n(l_w)$ given by $\theta(1 + \pi^j A) = \bar{A}$, where π is a uniformizing parameter in K_v which, since L_w/K_v is unramified, is also a uniformizing parameter in L_w, and where $\bar{A}$ denotes the reduction of a matrix A in $M_n(\mathcal{O}_w)$ modulo $\mathfrak{P}_w$. It is easily verified that θ is a surjective homomorphism and its kernel is the congruence subgroup $\mathbf{GL}_n(\mathcal{O}_w, \mathfrak{P}_w^{j+1})$. Moreover, it is compatible with the natural isomorphism of $\mathrm{Gal}(L_w/K_v)$ and $\mathrm{Gal}(l_w/k_v)$. It follows that there exists an isomorphism

$$H^1(L_w/K_v, G_{\mathcal{O}_w}(\mathfrak{P}_w^j)/G_{\mathcal{O}_w}(\mathfrak{P}_w^{j+1})) \simeq H^1(l_w/k_v, \theta(G_{\mathcal{O}_w}(\mathfrak{P}_w^j)).$$

Below we shall show that $B = \theta(G_{\mathcal{O}_w}(\mathfrak{P}_w^j))$ is the reduction modulo $\mathfrak{P}_w$ of $\mathfrak{g}_{\mathcal{O}_w} = \mathfrak{g} \cap M_n(\mathcal{O}_w)$, where $\mathfrak{g}$ is the Lie algebra of G. This means, in particular, that B is a vector space over l_w, and to prove Lemma 6.4 it remains to note that $H^1(l_w/k_v, W) = 0$ for any finite-dimensional k_v-defined vector space W over l_w. The latter is a consequence of the triviality of $H^1(l_w/k_v, l_w)$ (the additive form of Hilbert's Theorem 90, cf. proof of Lemma 2.7) and the factorization $W = W_0 \otimes_{k_v} l_w$, where $W_0 = W^{\mathrm{Gal}(l_w/k_v)}$ is the subspace of fixed points.

It remains to show that $B = \bar{\mathfrak{g}}_{\mathcal{O}_w}$. To do so, consider the ideal $\mathfrak{a}$ in the coordinate ring $K_v[\mathbf{GL}_n]$ consisting of functions that vanish on G, and take a finite set of generators $f_1(x), \ldots, f_r(x)$ of $\mathfrak{a} \cap \mathcal{O}_v[\mathbf{GL}_n]$ viewed as an ideal of $\mathcal{O}_v[\mathbf{GL}_n]$. Put $F_i(x,t) = t^{-1} f_i(E_n + tx)$. Since $f_i(E_n) = 0$, $F_i(x,t)$ lies in $\mathcal{O}_v[\mathbf{GL}_n][t]$. Hence $G_{\mathcal{O}_w}(\mathfrak{P}_w^j)$ consists of elements of the form $E_n + \pi^j A$, where $A \in M_n(\mathcal{O}_w)$ satisfies

$$F_i(x, \pi^j) = 0, \qquad i = 1, \ldots, r. \tag{6.4}$$

On the other hand, $\mathfrak{g}_{\mathcal{O}_w}$ consists of w-adic integral solutions of

$$d_{E_n} f_i(x) = 0, \qquad i = 1, \ldots, r. \tag{6.5}$$

Since $\underline{G}^{(v)}$ is smooth, the rank of the linear system (6.5) is precisely the rank of the respective reduced system. But it is easy to see that the reductions of (6.4) and (6.5) are the same, from which it follows that the variety defined by (6.4) has a smooth reduction. Therefore, as a result of Hensel's lemma, B and $\bar{\mathfrak{g}}_{\mathcal{O}_w}$ each consist of all the solutions in $M_n(l_w)$ of the same system which is obtained by reduction of either (6.4) or (6.5). Thus $B = \bar{\mathfrak{g}}_{\mathcal{O}_w}$, proving Lemma 6.4.

It follows from Lemma 6.4 that $H^1(L_w/K_v, G_{\mathcal{O}_w}(\mathfrak{P}_w)/G_{\mathcal{O}_w}(\mathfrak{P}_w^j)) = 1$ for any $j \geq 1$. Indeed, for $j = 2$ it is immediate from Lemma 6.4. For larger j one considers the exact sequence

$$1 \to G_{\mathcal{O}_w}(\mathfrak{P}_w^{j-1})/G_{\mathcal{O}_w}(\mathfrak{P}_w^j) \to G_{\mathcal{O}_w}(\mathfrak{P}_w)/G_{\mathcal{O}_w}(\mathfrak{P}_w^j) \to G_{\mathcal{O}_w}(\mathfrak{P}_w)/G_{\mathcal{O}_w}(\mathfrak{P}_w^{j-1}) \to 1$$

and the associated exact cohomological sequence

$$\begin{aligned} H^1(L_w/K_v, G_{\mathcal{O}_w}(\mathfrak{P}_w^{j-1})/G_{\mathcal{O}_w}(\mathfrak{P}_w^j)) \\ \to H^1(L_w/K_v, G_{\mathcal{O}_w}(\mathfrak{P}_w)/G_{\mathcal{O}_w}(\mathfrak{P}_w^j)) \\ \to H^1(L_w/K_v, G_{\mathcal{O}_w}(\mathfrak{P}_w)/G_{\mathcal{O}_w}(\mathfrak{P}_w^{j-1})). \end{aligned} \tag{6.6}$$

Since the left term of (6.6) is trivial by Lemma 6.4, the desired result is obtained by an obvious inductive argument.

Thus, for any cocycle $a = \{ a_\sigma \}$ in $Z^1(L_w/K_v, G_{\mathcal{O}_w}(\mathfrak{P}_w))$ and any $j \geq 1$, there is some b_j in $G_{\mathcal{O}_w}(\mathfrak{P}_w)$ such that $b_j^{-1} a_\sigma b_j^\sigma \in G_{\mathcal{O}_w}(\mathfrak{P}_w^j)$ for all σ in $\mathrm{Gal}(L_w/K_v)$. Since $G_{\mathcal{O}_w}(\mathfrak{P}_w)$ is compact, one can find a subsequence $\{ b_{j_l} \}_{l=1}^\infty$ of $\{ b_j \}_{j=1}^\infty$ which converges to some element b in $G_{\mathcal{O}_w}(\mathfrak{P}_w)$. Then

$$b^{-1} a_\sigma b^\sigma = \lim_{\substack{l \to \infty \\ l \geq l_0}} b_{j_l}^{-1} a_\sigma b_{j_l}^\sigma \in G_{\mathcal{O}_w}(\mathfrak{P}_w^{j_{l_0}})$$

for each $l_0 \geq 1$. Therefore $b^{-1} a_\sigma b^\sigma \in \bigcap_{l=1}^\infty G_{\mathcal{O}_w}(\mathfrak{P}_w^{j_l}) = \{ E_n \}$, hence $a_\sigma = b(b^{-1})^\sigma$ and a is trivial. Q.E.D. for Theorem 6.8.

COROLLARY. *Let G be a connected algebraic group over an algebraic number field K, and let L be a finite extension of K. Then, for almost all v in V_f^K, and any $w|v$ we have $H^1(L_w/K_v, G_{\mathcal{O}_w}) = 1$.*

Theorem 6.8 and several other results on the cohomology of groups of w-adic integral points may be found in Rohlfs [1]. Since the other results are not absolutely necessary here, we shall only state the following *finiteness theorem*: for any extension L_w/K_v and any group G, the cohomology set $H^1(L_w/K_v, G_{\mathcal{O}_w})$ is finite.

Thus far we have considered Galois cohomology with respect to a finite extension L_w/K_v, but one can extend the definition to any Galois extension L_w/K_v by putting

$$H^1(L_w/K_v, G_{\mathcal{O}_w}) = \varinjlim H^1(P/K_v, G_{\mathcal{O}_p}),$$

where the inductive limit is taken over all finite Galois extensions P of K contained in L_w. One can also define $H^1(L_w/K_v, G_{\mathcal{O}_w})$ as the continuous cohomology group of the profinite group $\mathrm{Gal}(L_w/K_v)$ with coefficients in the discrete group $G_{\mathcal{O}_w}$. Bearing this in mind, we can reformulate Theorem 6.8 as follows:

THEOREM 6.8′. *Let G be a connected algebraic group over K_v with a smooth connected reduction. Then*

$$H^1(K_v^{ur}/K_v, G_{\mathcal{O}_{K_v^{ur}}}) = 1,$$

where K_v^{ur} is the maximal unramified extension of K_v. (In other words, any group of integral points has trivial unramified cohomology.)

Now from Theorem 6.8 we shall derive an assertion about the image of the group of v-adic integral points under the coboundary morphism, which we shall need in Chapters 7 and 8. To do so, we begin by looking at a more general case. Let

$$1 \to F \to G \xrightarrow{\pi} H \to 1 \tag{6.7}$$

be an exact sequence of algebraic K_v-groups. Consider the following two conditions:

(1) There exist smooth reductions $\underline{F}^{(v)}$, $\underline{G}^{(v)}$, and $\underline{H}^{(v)}$.
(2) π is a morphism defined over $\mathcal{O}_v$, and the induced sequence

$$1 \to \underline{F}^{(v)} \to \underline{G}^{(v)} \xrightarrow{\pi^{(v)}} \underline{H}^{(v)} \to 1$$

is exact.

LEMMA 6.5. *If (1) and (2) are satisfied, then*

$$1 \to F_{\mathcal{O}_{K_v^{ur}}} \to G_{\mathcal{O}_{K_v^{ur}}} \xrightarrow{\pi} H_{\mathcal{O}_{K_v^{ur}}} \to 1 \tag{6.8}$$

is exact.

We need only verify that $\pi(G_{\mathcal{O}_{K_v^{ur}}}) = H_{\mathcal{O}_{K_v^{ur}}}$. To see this, note that for $a \in H_{\mathcal{O}_{K_v^{ur}}}$, the equality $\pi(x) = a$ defines a subvariety of G which by (1) and (2) has a smooth reduction. Since the reduced equation $\pi^{(v)}(x) = \bar{a}$ has a solution in $\underline{G}^{(v)}_{\bar{k}_v}$, by Hensel's lemma the original equation $\pi(x) = a$ has a solution x in $G_{\mathcal{O}_{K_v^{ur}}}$, since any finite extension l of k_v is the residue field of a suitable finite unramified extension L of K_v.

Verification of (1) and (2) for a specific valuation v can be tedious; however, if the groups in (6.7) are defined over a number field K, then in the cases needed in our further discussion these conditions are satisfied for almost all v.

LEMMA 6.6. *Suppose F, G, H and π of (6.7) are defined over a number field K, and let G be connected. If F is either finite or connected, then (1) and (2) hold for almost all v in V_f^K.*

PROOF: In view of Proposition 3.19 and Theorem 3.12, we see that it suffices to establish condition (2) for almost all v; moreover, we may assume $\underline{G}^{(v)}$ and $\underline{H}^{(v)}$ to be connected.

For F finite, the surjectivity of $\pi^{(v)}$ follows from the fact that $\underline{G}^{(v)}$ and $\underline{H}^{(v)}$ have the same dimension, and the equality $\ker \pi^{(v)} = \underline{F}^{(v)}$ is proved as follows. The variety defined by $\pi(x) = e$ has a smooth reduction for almost all v, and thus by Hensel's lemma one can obtain all the points of $\ker \pi^{(v)}$ by reduction of the points of $\ker \pi = F$; therefore $|\ker \pi^{(v)}| \leq |F|$. On the other hand, $|\underline{F}^{(v)}| = |F|$ and $\underline{F}^{(v)} \subset \ker \pi^{(v)}$ for almost all v; so, finally, $\ker \pi^{(v)} = \underline{F}^{(v)}$.

For F connected the lemma follows immediately from Proposition 3.22.

Next we suppose that conditions (1) and (2) hold for (6.7). Then, considering the natural action of $\mathrm{Gal}(K_v^{ur}/K_v)$ on the groups in (6.8) and passing to cohomology, we obtain the exact sequence

(6.9)
$$G_{\mathcal{O}_v} \xrightarrow{\pi} H_{\mathcal{O}_v} \xrightarrow{\psi_{\mathcal{O}_v}} H^1(K_v^{ur}/K_v, F_{\mathcal{O}_{K_v^{ur}}}) \to H^1(K_v^{ur}/K_v, G_{\mathcal{O}_{K_v^{ur}}}) = 1,$$

where $\psi_{\mathcal{O}_v}$ is the coboundary map.

Now suppose F is finite. Then, since G is connected, F is central and, moreover, $F \subset G_{\mathcal{O}_{K_v^{ur}}}$ for almost all v. On the other hand, $\psi_{\mathcal{O}_v}$, which is a homomorphism since F is central, is the restriction to $H_{\mathcal{O}_v}$ of the coboundary morphism $\psi_{K_v}: H_{K_v} \to H^1(K_v, F)$ obtained by passing to the usual Galois cohomology from the exact sequence $1 \to F \to G \to H \to 1$. Identifying the unramified cohomology group $H^1(K_v^{ur}/K_v, F)$ with a subgroup of $H^1(K_v, F)$ by means of the inflation map, we obtain the following:

PROPOSITION 6.4. *Let $\pi: G \to H$ be an isogeny of connected groups over an algebraic number field K, and let $F = \ker \pi$. Then, for almost all v in V_f^K, we have $\psi_{K_v}(H_{\mathcal{O}_v}) = H^1(K_v^{ur}/K_v, F)$, where $\psi_{K_v}: H_{K_v} \to H^1(K_v, F)$ is the coboundary morphism corresponding to the exact sequence*

$$1 \to F \to G \to H \to 1.$$

Consequently, $\psi_{K_v}(H_{\mathcal{O}_v})$ and F_{K_v} have the same order for almost all v. Moreover, if $F \subset G_{K_v}$, then $\psi_{K_v}(H_{\mathcal{O}_v}) \simeq F$.

The first assertion of the proposition has already been proved. The second follows immediately from the first and from Lemma 6.3. Lastly, to prove the third it suffices to note that $H^1(K_v^{ur}/K_v, F) = \mathrm{Hom}(\hat{\mathbb{Z}}, F) \simeq F$ if $F \subset G_{K_v}$.

Now consider the case where F is connected. Here we have

$$H^1(K_v^{ur}/K_v, F_{\mathcal{O}_{K_v^{ur}}}) = 1$$

for almost all v, and therefore (6.9) yields $\pi(G_{\mathcal{O}_v}) = H_{\mathcal{O}_v}$. Recalling the definition of the adelic topology and applying Proposition 3.3, Corollary 1, we obtain

PROPOSITION 6.5. *Let $\pi: G \to H$ be a surjective morphism of connected algebraic groups over an algebraic number field K. Assume $\ker \pi$ is connected. Then $\pi(G_{\mathcal{O}_v}) = H_{\mathcal{O}_v}$ for almost all v, and hence the corresponding adelic map $\pi_A: G_A \to H_A$ is open.*

We now pass to cohomology of adele groups. Let G be an algebraic group defined over a number field K. For any finite Galois extension L/K, take the ring A_L of adeles of L. It is well known (cf. §1.2.3) that one can identify A_L with $A_K \otimes L$ and via this identification one can define the action of $\mathrm{Gal}(L/K)$ on A_L. Interpreting the adele group G_{A_L} as a group of points G over A_L, and bearing in mind that G is defined over K, we obtain an action of $\mathrm{Gal}(L/K)$ on G_{A_L}.

Thus, we can define the first cohomology set $H^1(L/K, G_{A_L})$. For an arbitrary Galois extension L/K the adelic cohomology admits two equivalent definitions: either as $\varinjlim H^1(P/K, G_{A_P})$ taken over all finite Galois subextensions P/K contained in L, or as the first continuous cohomology set of the profinite group $\mathrm{Gal}(L/K)$ with coefficients in the (discrete) group G_{A_L}. In this regard, the latter group again allows a double description, either as the inductive limit (union) of the G_{A_P} taken over all finite subextensions P of L with respect to the natural embedding $G_{A_{P_1}} \subset G_{A_{P_2}}$ where $P_1 \subset P_2$, or as the group of points G over the ring $A_L = A_K \otimes_K L$.

We shall not study the formalism of adelic cohomology in detail (cf. Kottwitz [1], [2]), since we do not actually need it in this book. However, the main results are as follows: Any exact sequence

$$1 \to F \to G \to H \to 1$$

of connected K-groups and K-homomorphisms gives rise to the exact sequence $1 \to F_{\bar{A}} \to G_{\bar{A}} \to H_{\bar{A}} \to 1$ where $\bar{A}$ denotes the ring $A_{\bar{K}}$ (this follows easily from Proposition 6.5), and one can consider the corresponding derived cohomological sequences. (Note that for F disconnected, and in particular finite, $1 \to F_{\bar{A}} \to G_{\bar{A}} \to H_{\bar{A}} \to 1$ is not, generally speaking, an exact sequence.) In this regard, the adelic cohomology of a connected group G can be described as follows:

PROPOSITION 6.6. *Let G be a connected group over a number field K, and let L be a finite Galois extension of K. Then $H^1(L/K, G_{A_L})$ can be identified with the subset X of the direct product*[2] $\prod_v H^1(L_w/K_v, G)$ *consisting of those $x = (x_v)$ for which x_v is trivial in $H^1(L_w/K_v, G)$ for almost all v in V^K.*

(Using the terminology of group theory, we can say that $H^1(L/K, G_{A_L})$ is a direct sum of the $H^1(L_w/K_v, G)$. Note that for G commutative we actually have the usual direct sum of groups.)

PROOF: For each subset S of V^K let $\bar{S}$ be the aggregate of all extensions to L of valuations from S. Then $G_{A_L} = \bigcup_S G_{A_L(\bar{S})}$, where the union of

[2] The product is taken over all v in V^K, and for each v we choose a single extension w in V^L.

groups of $\bar{S}$-integral adeles $G_{A_L(\bar{S})}$ is taken over all finite subsets S of V^K containing V_∞^K; and therefore

$$H^1(L/K, G_{A_L}) = \bigcup_S H^1(L/K, G_{A_L(\bar{S})}).$$

Let us show that $H^1(L/K, G_{A_L(\bar{S})}) \subset X$ for any S. Without loss of generality we may consider only those S such that, for each $v \notin S$, there exists a smooth reduction $\underline{G}^{(v)}$ and L_w/K_v is unramified. The factorization $G_{A_L(\bar{S})} = G_{\bar{S}} \times \prod_{w \notin \bar{S}} G_{\mathcal{O}_w}$ implies

$$H^1(L/K, G_{A_L(\bar{S})}) = \prod_{v \in S} H^1(L/K, \prod_{w|v} G_{L_w}) \times \prod_{v \notin S} H^1(L/K, \prod_{w|v} G_{\mathcal{O}_w}).$$

But Lemma 1.4 implies that $\prod_{w|v} G_{L_w}$ (resp., $\prod_{w|v} G_{\mathcal{O}_w}$) is induced from G_{L_w} (resp., $G_{\mathcal{O}_w}$) for v in S (resp., $v \notin S$), for some fixed extension $w|v$. Moreover, by assumption Theorem 6.8 holds for $v \notin S$, so $H^1(L_w/K_v, G_{\mathcal{O}_w}) = 1$ for these v. Together these facts imply

$$H^1(L/K, G_{A_L(\bar{S})}) = \prod_{v \in S} H^1(L_w/K_v, G) \times \{1\}.$$

Passing to the union, we obtain $H^1(L/K, G_{A_L}) \subset X$. The reverse inclusion is obvious.

COROLLARY 1. *$H^1(K, G_{\bar{A}})$ can be identified with the subset of the direct product $\prod_v H^1(K_v, G)$ consisting of those $x = (x_v)$ such that x_v is trivial in $H^1(K_v, G)$ for almost all v in V^K.*

If G is commutative, then all the cohomology groups $H^i(L/K, G_{A_L})$ $(i \geq 0)$ are defined. It turns out that they can be described analogously to Proposition 6.6.

PROPOSITION 6.7. *Let G be a commutative algebraic group over a number field K, and let L be a finite Galois extension of K. Then for any $i \geq 1$*

$$H^i(L/K, G_{A_L}) \simeq \bigoplus_v H^i(L_w/K_v, G).$$

PROOF: As is evident from the proof of Proposition 6.6, it suffices to establish that $H^i(L_w/K_v, G_{\mathcal{O}_v}) = 1$ for almost all v. We can confine ourselves to considering those v for which L_w/K_v is unramified. Then $\mathrm{Gal}(L_w/K_v)$ is

cyclic, and by the periodicity of the cohomology of cyclic groups we obtain the isomorphisms

$$H^i(L_w/K_v, G_{\mathcal{O}_w}) \simeq H^1(L_w/K_v, G_{\mathcal{O}_w}) \quad \text{for } i \text{ odd},$$
$$H^i(L_w/K_v, G_{\mathcal{O}_w}) \simeq H^2(L_w/K_v, G_{\mathcal{O}_w}) \quad \text{for } i \text{ even}.$$

From these isomorphisms and Theorem 6.8 we obtain the triviality for i odd of the i-th unramified cohomology groups of the w-adic integral points of any connected commutative group, so to prove the proposition it suffices to establish the triviality of $H^2(L_w/K_v, G_{\mathcal{O}_w})$. To do so, we use a trick which we shall encounter repeatedly.

Put $H = \mathbf{R}_{L/K}(G)$, and consider the "norm" map $\varphi: H \to G$, which is the composite of (2.4) in §2.1 (note that $G^\sigma = G$ for any σ in $\mathcal{G} = \mathrm{Gal}(L/K)$ since G is defined over K) and the product morphism. (It is easy to see that the restriction of φ to $H_K \simeq G_L$ is the usual norm map $N_{L/K}(g) = \prod_{\sigma \in \mathcal{G}} \sigma(g)$.) Clearly, φ is defined over K, and $F = \ker \varphi$ is a connected K-group. Thus, we have the exact sequence of connected K-groups:

$$1 \to F \to H \to G \to 1.$$

It follows from Proposition 6.5 that for almost all v in V_f^K and the corresponding $w|v$ the sequence

$$1 \to F_{\mathcal{O}_w} \to H_{\mathcal{O}_w} \to G_{\mathcal{O}_w} \to 1 \tag{6.10}$$

is exact. Passing in (6.10) to cohomology, we obtain the exact sequence

$$\ldots \to H^2(L_w/K_v, H_{\mathcal{O}_w}) \to H^2(L_w/K_v, G_{\mathcal{O}_w}) \to H^3(L_w/K_v, F_{\mathcal{O}_w}). \tag{6.11}$$

It follows from the above that the last term of (6.11) is trivial for almost all v, and therefore it suffices to establish the triviality of $H^2(L_w/K_v, H_{\mathcal{O}_w})$. But this follows from the fact that by our set-up the $\mathrm{Gal}(L_w/K_v)$-module $H_{\mathcal{O}_w}$ is induced. This proves Proposition 6.7.

The diagonal embedding $L \to A_L$ is compatible with the action of $\mathrm{Gal}(L/K)$; therefore we have a map $H^1(L/K, G) \to H^1(L/K, G_{A_L})$ for any algebraic K-group G. Thus the description of adelic cohomology yields

COROLLARY 2. *Let G be a connected algebraic K-group, and let L/K be a finite Galois extension. Then any cocycle x in $H^1(L/K, G)$ has trivial image in $H^1(L_w/K_v, G)$, for almost all v in V_f^K. In particular, any x in $H^1(K, G)$ has trivial image in $H^1(K_v, G)$, for almost all v in V_f^K.*

Note that if G is commutative, then the analogous assertion holds for all cohomology groups.

EXERCISE: Give examples showing that the connectedness of G in Corollary 2 is essential.

6.3. Galois cohomology of algebraic tori.

As we remarked in §6.1, when working with algebraic tori it is convenient to use the modified cohomology (Tate cohomology) rather than the usual one. We shall briefly review its basic properties and definitions (a systematic exposition may be found in Brown [1, Ch. 6] or [ANT, Ch. 4]).

Let G be a finite group, and let A be a G-module. We introduce the "norm" map $N: A \to A$ given by $N(a) = \sum_{g \in G} ga$. Clearly $N(A) \subset A^G$ and $A' \subset \ker N$, where A' is the submodule of A generated by elements of the form $ga - a$ for all g in G and a in A. Then the Tate cohomology groups $\hat{H}^i(G, A)$ are defined as follows:

$$\begin{aligned} \hat{H}^i(G,A) &= H^i(G,A), && \text{if } i \geq 1, \\ \hat{H}^0(G,A) &= A^G/N(A), \\ \hat{H}^{-1}(G,A) &= \ker N/A', \\ \hat{H}^{-i}(G,A) &= H_{i-1}(G,A), && \text{if } i \geq 2, \end{aligned}$$

where H_i denotes the i-th homology group. It is known that the modified cohomology retains all the basic properties of the usual cohomology, namely:

(1) Shapiro's lemma, in particular, the cohomology of an induced module is trivial;

(2) any exact sequence of G-modules $0 \to A \to B \to C \to 0$ gives rise to the following exact sequence which is infinite in both directions:

$$\ldots \to \hat{H}^i(G,A) \to \hat{H}^i(G,B) \to \hat{H}^i(G,C) \to \hat{H}^{i+1}(G,A) \to \ldots$$

The advantage of passing from the usual cohomology to the modified one is that for the latter we have Tate's theorem (cf. Theorem 6.9 below) which is very useful in our situation.

Having concluded these preliminary remarks, we now proceed directly to the proof of the Nakayama-Tate theorem.

Let us begin with the special case $T = \mathbb{G}_m$. This case, which is trivial from the point of view of the theory of tori, assumes the most significant role in the argument, since, for $i = 0, 1, 2$, the isomorphisms occurring in Theorems 6.2 and 6.3 present the main results of local and global class field theory, respectively. Afterwards the case of arbitrary tori can be considered rather easily with the aid of Tate's theorem.

First we consider the case of a local field K. For $i = 0$ we must obtain the isomorphism $\hat{H}^0(L/K, \mathbb{Z}) \simeq \hat{H}^2(L/K, L^*)$, since here $\mathbf{X}(T) = \mathbb{Z}$ with trivial action of $\mathcal{G} = \mathrm{Gal}(L/K)$. But clearly $\hat{H}^0(L/K, \mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}$, where $n = [L : K]$; and $H^2(L/K, L^*) \simeq \mathrm{Br}(L/K) \simeq \frac{1}{n}\mathbb{Z}/\mathbb{Z}$, where the last isomorphism is realized by the map inv (cf. Theorem 1.7). The inverse image of $\frac{1}{n}$ under this isomorphism is the *fundamental class of* L/K, denoted $u_{L/K}$. If F is an intermediate subfield, then $u_{L/F}$ is the image of $u_{L/K}$ under the restriction map $H^2(L/K, L^*) \to H^2(L/F, L^*)$.

For $i = 1$ both $\hat{H}^1(L/K, \mathbb{Z})$ and $\hat{H}^1(L/K, L^*)$ are trivial.

Lastly, we consider the case $i = 2$. Here $\hat{H}^2(L/K, \mathbb{Z}) \simeq \hat{H}^1(L/K, \mathbb{Q}/\mathbb{Z})$ (cf. Lemma 1.3), and the latter group is the abelianization of $\mathcal{G}$. However, $\hat{H}^0(L/K, L^*) = K^*/N_{L/K}(L^*)$. Thus the isomorphism from Theorem 6.2 assumes the form $\mathcal{G}^{ab} \simeq K^*/N_{L/K}(L^*)$, in particular $\mathcal{G} \simeq K^*/N_{L/K}(L^*)$ if G is abelian. The last fact, supplemented by the existence theorem (any open subgroup of K^* having finite index is a norm one, i.e., has the form $N_{L/K}(L^*)$ for a suitable abelian extension L/K), represents a major result in local class field theory (cf. Serre's lecture in [ANT]). Note that although the basic objects of local class field theory are non-Archimedean local fields, the results still hold formally in the Archimedean case, i.e., when K is $\mathbb{R}$ or $\mathbb{C}$.

Similar results also hold for the global case, although the objects used and the proofs of the basic theorems are more complicated; in particular, the multiplicative group L^* is replaced here by the idele class group $C_L = J_L/L^*$. Again, for $i = 0$ we have $H^2(L/K, C_L) \simeq \frac{1}{n}\mathbb{Z}/\mathbb{Z}$, where $n = [L : K]$ (here the isomorphism is constructed by proceeding from the local inv maps, cf. [ANT, Ch. 7, § 11]), so for $i = 0$ the assertion of Theorem 6.3 holds. As in the local case, the inverse image $u_{L/K}$ of $\frac{1}{n}$ under this isomorphism is called the *fundamental class of* L/K. It also has the property that for any intermediate subfield F the fundamental class $u_{L/F}$ is the restriction of $u_{L/K}$. Since $H^1(L/K, C_L)$ is trivial for $i = 1$, Theorem 6.3 holds here. (Note that the triviality of $H^1(L/K, C_L)$ has several important arithmetic consequences. In particular, passing to the cohomology sequence associated to the exact sequence $1 \to L^* \to J_L \to C_L \to 1$, we see that the map $\mathrm{Br}(L/K) = H^2(L/K, L^*) \to H^2(L/K, J_L) = \sum \mathrm{Br}(L_w/K_v)$ is injective, which is equivalent to the Albert-Brauer-Hasse-Noether theorem in §1.5).

Finally, for $i = 2$ we must obtain $\mathcal{G}^{ab} \simeq C_K/N_{L/K}(C_L)$, and this is the basic isomorphism of global class field theory (cf. Tate's lecture in [ANT]).

We cannot help but note the analogy between the basic results of the

local and the global theories, which finds formal expression in the axiomatic description of *class formations* (cf. Serre [3]).

Now we have all the necessary preliminaries to complete the proof of Theorems 6.2 and 6.3 in the general case. The proof is based on the following

THEOREM 6.9 (TATE [1]). *Let G be a finite group, let M be a G-module, and let u be an element of $H^2(G, M)$. For each prime p denote by G_p a Sylow p-subgroup of G, and assume that the following conditions are satisfied:*

(1) $H^1(G_p, M) = 1$,
(2) $H^2(G_p, M)$ *is a cyclic group of the same order as* G_p, *having generator* $\mathrm{Res}^G_{G_p}(u)$, *where* $\mathrm{Res}^G_{G_p}(u)\colon H^2(G, M) \to H^2(G_p, M)$ *is the restriction morphism.*

Then for any torsion-free finitely generated G-module N and any subgroup H of G and any integer i, the cup-product coupled with u induces an isomorphism $\hat{H}^i(H, N) \to \hat{H}^{i+2}(H, M \otimes N)$.

(The reader may find the definition of the cup product and the proof of Theorem 6.9 in [ANT, Ch. 4, §10]. These results will not be needed later on.)

In order to use Theorem 6.9 for a given K-torus T, split over a finite Galois extension L/K with Galois group $\mathcal{G} = \mathrm{Gal}(L/K)$, consider the group of cocharacters (one-parameter subgroups) $\mathbf{X}_*(T) = \mathrm{Hom}(\mathbb{G}_m, T)$ which is also a $\mathcal{G}$-module (cf. §2.1.7). It turns out that if we know $\mathbf{X}_*(T)$ it is easy to determine the group of L-points T_L. Namely, consider the homomorphism $\theta\colon \mathbf{X}_*(T) \otimes L^* \to T_L$ given by $\theta(\varphi \otimes x) = \varphi(x)$. The action of $\mathcal{G}$ on $\mathbf{X}_*(T) \otimes L^*$ is defined via the action on both factors; and it is easily verified that θ is a $\mathcal{G}$ homomorphism. However, it is easy to show that, for a split torus, θ is an isomorphism of abstract groups. Therefore, in view of the fact that T becomes split over L, we arrive at the following result.

LEMMA 6.7. *The homomorphism $\theta\colon \mathbf{X}_*(T) \otimes L^* \to T_L$ which we have described is an isomorphism of $\mathcal{G}$-modules.*

Now it is quite easy to prove the local version of the Nakayama-Tate theorem. Namely, suppose K is a local field. Then, from our discussion of local class field theory it follows that the conditions of the Tate theorem are satisfied for $M = L^*$ and $u_{L/K} \in H^2(L/K, L^*)$. Therefore, applying it together with Lemma 6.7, we obtain the isomorphisms

$$\hat{H}^i(L/K, \mathbf{X}_*(T)) \simeq \hat{H}^{i+2}(L/K, \mathbf{X}_*(T) \otimes L^*) \simeq \hat{H}^{i+2}(L/K, T_L). \tag{6.12}$$

(Note that this isomorphism is induced by the cup-product on $u_{L/K}$ and therefore has the necessary functorial properties.) On the other hand, the duality theorem for cohomology (cf., for example, Cartan-Eilenberg [1]) implies that the finite abelian groups $\hat{H}^i(L/K, \mathbf{X}_*(T))$ and $\hat{H}^{-i}(L/K, \mathbf{X}(T))$ are dual and hence isomorphic, for any i. Theorem 6.2 follows from this fact and from the sequence of isomorphisms (6.12). Note that this proof of the theorem works for *all* local fields, including Archimedean ones; however, for $K = \mathbb{R}$ there is an easy direct proof using classification of real tori (cf. §2.2.4), which we recommend the reader to work out as an exercise.

It should be pointed out that the isomorphism constructed in the proof of Theorem 6.2 has the nature of an isomorphism of a finite abelian group with its dual. This duality can be described directly, without using $\mathbf{X}_*(T)$. Namely, the cup-product induces a bilinear map

$$\hat{H}^i(L/K, T) \times \hat{H}^{2-i}(L/K, \mathbf{X}(T)) \to \hat{H}^2(L/K, T_L \otimes_{\mathbb{Z}} \mathbf{X}(T)),$$

and the latter group is sent to $\hat{H}^2(L/K, L^*) \simeq \mathbb{Z}/n\mathbb{Z}$, where $n = [L : K]$, by the map $T_L \otimes \mathbf{X}(T) \to L^*$ given by $t \otimes \chi \mapsto \chi(t)$. The resulting bilinear map $\hat{H}^i(L/K, T) \times \hat{H}^{2-i}(L/K, \mathbf{X}(T)) \to \mathbb{Z}/n\mathbb{Z}$ turns out to be a nondegenerate pairing, thereby providing the isomorphism in Theorem 6.2.

The proof of Theorem 6.3 follows the same line as Theorem 6.2, the only difference being that for K global one uses $M = C_L$. The fact that the conditions of the Nakayama-Tate theorem are satisfied for this M and the corresponding fundamental class $u_{L/K}$ in $H^2(L/K, M)$ follows from global class field theory. As an exercise, we recommend the reader show that the $\mathcal{G}$-modules $\mathbf{X}_*(T) \otimes C_L$ and $C_L(T) = T_{A_L}/T_L$ are isomorphic. (Hint: imitate the proof of Lemma 6.7.) Then

$$\hat{H}^i(L/K, \mathbf{X}_*(T)) \simeq \hat{H}^{i+2}(L/K, \mathbf{X}_*(T) \otimes C_L) \simeq \hat{H}^{i+2}(L/K, C_L(T)), \tag{6.13}$$

where the isomorphism is realized by the cup-product with $u_{L/K}$. Again, using the duality between $\hat{H}^i(L/K, \mathbf{X}_*(T))$ and $\hat{H}^i(L/K, \mathbf{X}(T))$, we obtain Theorem 6.3. Note that here, too, we have a nondegenerate bilinear pairing of $\hat{H}^i(L/K, C_L(T))$ and $\hat{H}^{2-i}(L/K, \mathbf{X}(T))$, obtained as the composite map

$$\hat{H}^i(L/K, C_L(T)) \times \hat{H}^{2-i}(L/K, \mathbf{X}(T)) \to \hat{H}^2(L/K, C_L(T) \otimes_{\mathbb{Z}} \mathbf{X}(T)) \to \hat{H}^2(L/K, C_L) \simeq \mathbb{Z}/n\mathbb{Z},$$

where $n = [L : K]$.

One important remark is in order. Since the isomorphisms in Theorems 6.2 and 6.3 involve duality, they are not canonical. Therefore, in

studying functorial properties, instead of the isomorphisms in these theorems one ought to analyze the isomorphisms in (6.12) and (6.13) which involve the cohomology groups $\mathbf{X}_*(T)$, since they are induced by the cup-product and hence are natural. The relations among the cohomology groups of $\mathbf{X}(T)$ itself are then obtained from duality.

As an example, let us consider the connection between the local and the global isomorphisms in the Nakayama-Tate theorems. Thus let K be a number field, $v \in V^K$, let $T_{K_v \otimes_K L} \to T_{A_K \otimes_K L} = T_{A_L}$ be the natural embedding, and let $\tau\colon \hat{H}^i(L/K, T_{K_v \otimes_K L}) \to \hat{H}^i(L/K, C_L(T))$ be the cohomology map induced by this embedding and the projection $T_{A_L} \to C_L(T)$. Since $K_v \otimes_K L \simeq \prod_{w|v} L_w$, the various extensions of v being conjugate with respect to $\mathcal{G}$, we obtain that the group $T_{K_v \otimes_K L} \simeq \prod_{w|v} T_{L_w}$ is induced; therefore by Shapiro's lemma $\hat{H}^i(L/K, T_{K_v \otimes_K L}) = \hat{H}^i(L_w/K_v, T)$. But

$$\hat{H}^i(L/K, C_L(T)) \simeq \hat{H}^{2-i}(L/K, \mathbf{X}(T)),$$
$$\hat{H}^i(L_w/K_v, T) \simeq \hat{H}^{2-i}(L_w/K_v, \mathbf{X}(T)),$$

so naturally one is tempted to describe the map $\hat{H}^{2-i}(L_w/K_v, \mathbf{X}(T)) \to \hat{H}^{2-i}(L/K, \mathbf{X}(T))$, corresponding to τ. But it would be incorrect to put the problem in this way, since the isomorphisms involved are not defined canonically. The correct way to put the problem is as follows: find a homomorphism $\sigma\colon \hat{H}^{i-2}(L_w/K_v, \mathbf{X}_*(T)) \to \hat{H}^{i-2}(L/K, \mathbf{X}_*(T))$ which makes the following diagram commutative:

$$\begin{array}{ccc} \hat{H}^i(L_w/K_v, T) & \xrightarrow{\tau} & \hat{H}^i(L/K, C_L(T)) \\ \uparrow & & \uparrow \\ \hat{H}^{i-2}(L_w/K_v, \mathbf{X}_*(T)) & \xrightarrow{\sigma} & \hat{H}^{i-2}(L/K, \mathbf{X}_*(T)) \end{array} \tag{6.14}$$

(The vertical arrows are isomorphisms obtained from (6.12) and (6.13).)

PROPOSITION 6.8. *σ is the corestriction homomorphism $\mathrm{Cor}^{\mathcal{G}}_{\mathcal{G}(w)}$, where $\mathcal{G}(w) = \mathrm{Gal}(L_w/K_v)$ is the decomposition group of w.*

PROOF: We begin by establishing the connection between the local and global fundamental classes. Put $P = L^{\mathcal{G}(w)}$. Then the results ([ANT, Ch. 7, §11]) imply that $L_w \to C_L$ induces an isomorphism $H^2(L_w/P_w, L_w) \simeq H^2(L/P, C_L)$ (note that $P_w = K_v$); in this regard, the local fundamental class $u_{L_w/P_w} = u_{L_w/K_v}$ passes to the global fundamental class $u_{L/P}$ which, as we know, is $\mathrm{Res}^{\mathcal{G}}_{\mathcal{G}(w)}(u_{L/K})$. Consequently,

$$\begin{array}{ccc} \hat{H}^{i-2}(\mathcal{G}(w), \mathbf{X}_*(T)) & \longrightarrow & \hat{H}^i(\mathcal{G}(w), T) \\ \| & & \downarrow \\ \hat{H}^{i-2}(\mathcal{G}(w), \mathbf{X}_*(T)) & \longrightarrow & \hat{H}^i(\mathcal{G}(w), C_L(T)) \end{array}$$

and

$$\begin{array}{ccc} \hat{H}^{i-2}(\mathcal{G}(w), \mathbf{X}_*(T)) & \longrightarrow & \hat{H}^i(\mathcal{G}(w), C_L(T)) \\ \mathrm{Cor}^{\mathcal{G}}_{\mathcal{G}(w)} \downarrow & & \downarrow \mathrm{Cor}^{\mathcal{G}}_{\mathcal{G}(w)} \\ \hat{H}^{i-2}(\mathcal{G}, \mathbf{X}_*(T)) & \longrightarrow & \hat{H}^i(\mathcal{G}, C_L(T)) \end{array}$$

are commutative. (The proof that the second diagram is commutative uses the following property of the cup-product:

$$\mathrm{Cor}(\mathrm{Res}(x) \cup y) = x \cup \mathrm{Cor}(y), \tag{6.15}$$

which is established in [ANT, Ch. 4, §7].) Comparing these diagrams and bearing in mind the commutativity of

$$\begin{array}{ccc} \hat{H}^i(\mathcal{G}(w), T) & \longrightarrow & \hat{H}^i(\mathcal{G}(w), C_L(T)) \\ i \downarrow & & \downarrow \mathrm{Cor}^{\mathcal{G}}_{\mathcal{G}(w)} \\ \hat{H}^i(\mathcal{G}, \prod_{w|v} T_{L_w}) & \longrightarrow & \hat{H}^i(\mathcal{G}, C_L(T)) \end{array}$$

where i is the isomorphism from Shapiro's lemma, we arrive at the desired result. (We leave it to the reader to work out the details.)

As we noted in §6.1, Theorems 6.2 and 6.3 imply that $H^1(K, T)$ is finite over a local field K and that the kernel $Ш(T)$ of the canonical homomorphism $H^1(K, T) \to \prod_{v \in V^K} H^1(K_v, T)$ is finite for a number field K. Actually these assertions hold not only for the first cohomology group but also for other cohomology groups.

PROPOSITION 6.9. *Let T be an algebraic torus defined over K and split over a finite Galois extension L of K. Then the following hold for all i:*

(1) *$H^i(L/K, T)$ is finite if K is a local field;*
(2) *$P^i(L/K, T) = \ker(\hat{H}^i(L/K, T) \to \prod_v \hat{H}(L_w/K_v, T))$ is finite if K is a number field.*

PROOF: Follows easily from the following remark: $\hat{H}^i(L/K, \mathbf{X}(T))$ is a finitely generated abelian group of finite exponent, for any i (cf. [ANT, Ch. 4, §6]), and therefore is finite. In view of the isomorphism in Theorem 6.2, assertion (1) is a direct consequence of this fact. To prove (2), consider the exact sequence

$$1 \to T_L \to T_{A_L} \to C_L(T) \to 1$$

and the following segment of its corresponding cohomology sequence:

(6.16)
$$\hat{H}^{i-1}(L/K, T_{A_L}) \xrightarrow{g} \hat{H}^{i-1}(L/K, C_L(T)) \to \hat{H}^i(L/K, T) \xrightarrow{f} \hat{H}^i(L/K, T_{A_L}).$$

Then $P^i(L/K, T) = \ker f$ is a quotient group of $\hat{H}^{i-1}(L/K, C_L(T))$, and by Theorem 6.3 this group is isomorphic to $\hat{H}^{3-i}(L/K, \mathbf{X}(T))$ and consequently is finite.

COROLLARY. *Keep the assumptions of Proposition 6.9. Then*

(1) *$H^1(K, T)$ is finite if K is a local field;*
(2) *$Ш(T) = \ker(H^1(K, T) \to \prod_v H^1(K_v, T))$ is finite if K is a number field.*

The proof follows from Proposition 6.9 and the following:

LEMMA 6.8. *If a K-torus T is split over the Galois extension L/K, then $H^1(K, T) = H^1(L/K, T)$.*

Indeed, by Hilbert's Theorem 90 $H^1(L, T) = 1$; therefore, writing the initial segment of the Hochschild-Serre exact sequence

$$1 \to H^1(L/K, T) \to H^1(K, T) \to H^1(L, T),$$

we obtain the desired result.

By refining the argument used in the proof of Proposition 6.8 one can obtain precise formulas for computing $P^i(L/K, T)$. Indeed, (6.16) implies that $P^i(L/K, T) = \ker f$ is isomorphic to $\operatorname{coker} g$. But

$$\hat{H}^{i-1}(L/K, T_{A_L}) = \bigoplus_v \hat{H}^{i-1}(L_w/K_v, T)$$

(Proposition 6.7); thus, using the isomorphisms

$$\hat{H}^{i-1}(L/K, C_L(T)) \simeq \hat{H}^{i-3}(L/K, \mathbf{X}_*(T))$$
$$\hat{H}^{i-1}(L_w/K_v, T) \simeq \hat{H}^{i-3}(L_w/K_v, \mathbf{X}_*(T)),$$

and Proposition 6.8, we obtain that $P^i(L/K, T)$ is isomorphic to the cokernel of

$$\bigoplus_v \hat{H}^{i-3}(L_w/K_v, \mathbf{X}_*(T)) \to \hat{H}^{i-3}(L/K, \mathbf{X}_*(T)) \tag{6.17}$$

induced by $\operatorname{Cor}^{\mathcal{G}}_{\mathcal{G}(w)}$. Passing to the cohomology of $\mathbf{X}(T)$ by duality, and bearing in mind that in this regard the corestriction morphism passes to the restriction, we obtain the following result.

THEOREM 6.10 (TATE).

$$P^i(L/K, T) \simeq \ker(H^{3-i}(L/K, \mathbf{X}(T)) \to \prod_v H^{3-i}(L_w/K_v, \mathbf{X}(T)).$$

(Note that the isomorphism in Theorem 6.10 is not canonical, but instead is induced by duality.)

Most applications involve $Ш(T) = P^1(L/K, T)$, the *Shafarevich-Tate group of T*. The Hasse principle is said to hold for T if $Ш(T) = 1$. Let us show that this concept is a natural generalization of the classical Hasse norm principle for extensions of number fields. Let P be a finite extension of a number field K, let $S = \mathbf{R}_{P/K}(\mathbb{G}_m)$, and let $T = \mathbf{R}^{(1)}_{P/K}(\mathbb{G}_m)$ be the corresponding norm torus. Passing to cohomology, from the exact sequence

$$1 \to T \to S \xrightarrow{N} \mathbb{G}_m \to 1, \tag{6.18}$$

where N is the norm map, we obtain the exact sequence

$$P^* \xrightarrow{N_{P/K}} K^* \to H^1(K, T) \to H^1(K, S).$$

But $H^1(K, S) = 1$ (by Lemma 2.4); therefore $H^1(K, T) \simeq K^*/N_{P/K}(P^*)$. Arguing analogously, we obtain $H^1(K, T_{\bar{A}}) \simeq J_K/N_{P/K}(J_P)$. It follows that

$$Ш(T) \simeq (K^* \cap N_{P/K}(J_P))/N_{P/K}(P^*).$$

Juxtaposing this fact with the classical definition of when the Hasse norm principle holds for P/K (cf. §1.2.3), we see that in the given situation it is equivalent to the validity of the Hasse norm principle for the corresponding normed torus $T = \mathbf{R}^{(1)}_{P/K}(\mathbb{G}_m)$. Thus, Theorem 6.10 gives an effective way of verifying the Hasse norm principle. The relevant computations become quite straightforward when P/K is a Galois extension. In this case, we can take P itself for the splitting field L of $T = \mathbf{R}^{(1)}_{P/K}(\mathbb{G}_m)$. Let $\mathcal{G}$ denote $\operatorname{Gal}(P/K)$. Then $\mathbf{X}(T)$ is given by

$$0 \to \mathbb{Z} \to \mathbb{Z}[\mathcal{G}] \to \mathbf{X}(T) \to 0, \tag{6.19}$$

which is obtained from (6.18). Passing to cohomology in (6.19) we obtain

$$H^2(\mathcal{G},\mathbb{Z}[\mathcal{G}]) \to H^2(\mathcal{G},\mathbf{X}(T)) \to H^3(\mathcal{G},\mathbb{Z}) \to H^3(\mathcal{G},\mathbb{Z}[\mathcal{G}]).$$

But the group ring $\mathbb{Z}[\mathcal{G}]$ is an induced $\mathcal{G}$-module, so $H^i(\mathcal{G},\mathbb{Z}[\mathcal{G}]) = 0$ for $i = 2, 3$; therefore $H^2(\mathcal{G},\mathbf{X}(T)) = H^3(\mathcal{G},\mathbb{Z})$. Analogously, fixing some extension $w|v$ for each v and denoting the respective decomposition group $\mathcal{G}(w)$ by $\mathcal{G}_v$, we have $H^2(\mathcal{G}_v,\mathbf{X}(T)) = H^3(\mathcal{G}_v,\mathbb{Z})$. Thus, applying Theorem 6.10, we obtain the following:

THEOREM 6.11 (TATE). *For the norm torus $T = \mathbf{R}^{(1)}_{P/K}(\mathbb{G}_m)$ corresponding to a Galois extension P/K, $Ш(T)$ is isomorphic to the kernel of the canonical map*

$$H^3(\mathcal{G},\mathbb{Z}) \to \prod_v H^3(\mathcal{G}_v,\mathbb{Z}). \tag{6.20}$$

In particular, the Hasse norm principle holds for P/K if and only if (6.20) is injective.

If $\mathcal{G}$ is cyclic, then $H^3(\mathcal{G},\mathbb{Z}) = H^1(\mathcal{G},\mathbb{Z}) = 0$ and we arrive at the following result due to Hasse [2].

COROLLARY (HASSE NORM THEOREM). *The local-global norm principle always holds for a cyclic extension P/K.*

If P/K is not cyclic, then it may or may not be valid:

EXAMPLE 1: Put $K = \mathbb{Q}$, $P = \mathbb{Q}(\sqrt{13},\sqrt{17})$. Here $\mathcal{G} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and all the $\mathcal{G}_v$ are cyclic. Therefore $H^3(\mathcal{G},\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$, but $H^3(\mathcal{G}_v,\mathbb{Z}) = 0$ for any v. Then $Ш(T) = \mathbb{Z}/2\mathbb{Z}$ and the norm principle does not hold for P/K, which is consistent with what we said in §1.2.3.

EXAMPLE 2: Put $K = \mathbb{Q}$, $P = \mathbb{Q}(\sqrt{2},\sqrt{5})$. Then $\mathcal{G} = \mathcal{G}_2 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, so (6.20) is injective and the norm principle is satisfied for P/K.

The question of the validity of the Hasse principle is theoretically resolved for Galois extensions by Theorem 6.11, but until recently very few results had been found for non-normal extensions. In this situation, of course, Theorem 6.10 can be applied to the corresponding norm torus (see below for the computations); on the other hand, various methods related to the geometry of algebraic tori (cf. Voskresenskiĭ [3] and the latter part of §7.3) can be used. In this regard, however, one is left with the feeling that this solution is inadequate, since the essentially arithmetic question of the Hasse norm principle is answered in a purely homological form which actually does not take into account the arithmetic of the extension itself. An intricate analysis of the Hasse norm principle for

arbitrary extensions, combining homological as well as arithmetic methods, was recently made in Platonov-Drakokhrust [1], [2], Drakokhrust-Platonov [1], and Drakokhrust [1]. The point of departure for this investigation was the following problem of Bartels [3, p. 198]: does the Hasse principle hold for an extension L/K if L is a maximal subfield of a skew field D with center K? Such extensions are said to be *K-adequate* (Shacher [1]). This conjecture seemed quite likely to be true. For example, any extension of prime degree is K-adequate and satisfies the Hasse principle (cf. Proposition 6.10 below). Gurak [2] proved Bartels' conjecture for Galois extensions. (This result can be viewed as an arithmetic interpretation of the criterion in Theorem 6.11.) Bartels [4] himself established the validity of the Hasse principle for K-adequate extensions of degree 4. (As Example 1 shows, for an arbitrary extension of degree 4 the Hasse principle can be violated.) Moreover, the local-global norm principle holds for the ambient skew field D containing L (Eichler's theorem, cf. §1.4).

Nevertheless, it turns out that Bartels' conjecture is false in general. The first counterexample, constructed in Platonov-Drakokhrust [1], was an extension of degree 10. The question naturally arose whether one could find any counterexample of a smaller degree, and what the arithmetic nature is of the possible values of the degree of extension that would satisfy Bartels' conjecture. (Since 10 is the product of two distinct primes, and since the Hasse principle always holds for extensions of prime degree, one may suggest that Bartels' conjecture holds for extensions whose degrees are prime powers. Drakokhrust-Platonov [1] studied these questions in detail. It is shown there, in particular, that Bartels' conjecture holds for extensions L/K of degree p^2 (p prime), while for $[L : K] = p^r$, $r \geq 3$, it does not. It also turns out to hold for extensions of degree 6. Therefore, the smallest counterexamples are extensions of degree 8.

The analysis of the Hasse principle in the works cited above is based on the concept, introduced there, of the *first obstruction*. In our setting, this notion can be described as follows: For a finite extension P/K, the splitting field of the norm torus $T = \mathbf{R}^{(1)}_{P/K}(\mathbb{G}_m)$ can be taken to be any Galois extension L of K containing P. Let $\mathcal{G}$ denote $\mathrm{Gal}(L/K)$ and let $\mathcal{H}$ be the subgroup of $\mathcal{G}$ fixing P. Passing to characters in (6.18), we obtain the following exact sequence containing $\mathbf{X}(T)$:

$$0 \to \mathbb{Z} \to \mathbb{Z}[\mathcal{G}/\mathcal{H}] \to \mathbf{X}(T) \to 0. \tag{6.21}$$

To compute $Ш(T)$ using Theorem 6.10, consider the commutative diagram

obtained from (6.21):

$$
\begin{array}{ccccc}
H^2(\mathcal{G},\mathbb{Z}) & \xrightarrow{\varphi_1} & H^2(\mathcal{G},\mathbb{Z}[\mathcal{G}/\mathcal{H}]) & \xrightarrow{\varphi_2} & H^2(\mathcal{G},\mathbf{X}(T)) \\
\downarrow{\scriptstyle \alpha_1} & & \downarrow{\scriptstyle \alpha_2} & & \downarrow{\scriptstyle \alpha_3} \\
\prod_v H^2(\mathcal{G}_v\mathbb{Z}) & \xrightarrow{\psi_1} & \prod_v H^2(\mathcal{G}_v,\mathbb{Z}[\mathcal{G}/\mathcal{H}]) & \xrightarrow{\psi_2} & \prod_v H^2(\mathcal{G}_v,\mathbf{X}(T))
\end{array}
\tag{6.22}
$$

$$
\begin{array}{ccccc}
\xrightarrow{\varphi_3} & H^3(\mathcal{G},\mathbb{Z}) & \xrightarrow{\varphi_4} & H^3(\mathcal{G},\mathbb{Z}[\mathcal{G}/\mathcal{H}]) \\
& \downarrow{\scriptstyle \alpha_4} & & \downarrow{\scriptstyle \alpha_5} \\
\xrightarrow{\psi_3} & \prod_v H^3(\mathcal{G}_v,\mathbb{Z}) & \xrightarrow{\psi_4} & \prod_v H^3(\mathcal{G}_v,\mathbb{Z}[\mathcal{G}/\mathcal{H}]).
\end{array}
$$

Since $Ш(T) = P^1(L/K,T) \simeq \ker\alpha_3$, by Theorem 6.10, (6.22) implies that there exists an embedding of $\Phi = \alpha_2^{-1}(\operatorname{im}\psi_1)/\operatorname{im}\varphi_1$ in $Ш(T)$. Φ is isomorphic to the first obstruction to the Hasse principle, defined in Platonov-Drakokhrust [1] arithmetically as the quotient group

$$K^* \cap N_{P/K}(J_P)/N_{P/K}(P^*)(K^* \cap N_{L/K}(J_L)).$$

The paper cited describes a method for computing the first obstruction, which can also be obtained from (6.22). To do so, note that $\mathbb{Z}[\mathcal{G}/\mathcal{H}] = \operatorname{Ind}_{\mathcal{H}}^{\mathcal{G}}(\mathbb{Z})$, and therefore $H^2(\mathcal{G},\mathbb{Z}[\mathcal{G}/\mathcal{H}]) = H^2(\mathcal{H},\mathbb{Z})$, by Shapiro's lemma. Similarly, for each v, $\mathbb{Z}[\mathcal{G}/\mathcal{H}] = \bigoplus_{i=1}^{r_v}\mathbb{Z}[K_i^v/\mathcal{H}]$ is a direct sum of $\mathcal{G}_v$-modules, where $K_i^v = \mathcal{G}_v x_i^v \mathcal{H}$ $(i = 1,\dots,r_v)$ are distinct double cosets in the decomposition of $\mathcal{G}$ modulo $\mathcal{G}_v$ and $\mathcal{H}$. In this regard, clearly $\mathbb{Z}[K_i^v/\mathcal{H}] = \operatorname{Ind}_{\mathcal{H}_i^v}^{\mathcal{G}_v}(\mathbb{Z})$, where $\mathcal{H}_i^v = x_i^v\mathcal{H}(x_i^v)^{-1} \cap \mathcal{G}_v$. Thus

$$H^2(\mathcal{G}_v,\mathbb{Z}[\mathcal{G}/\mathcal{H}]) = \bigoplus_{i=1}^{r_v} H^2(\mathcal{H}_i^v,\mathbb{Z}).$$

Applying dimension shifting (cf. Lemma 1.3), we see that the first square in (6.22) is equivalent to

$$
\begin{array}{ccc}
H^1(\mathcal{G},\mathbb{Q}/\mathbb{Z}) & \xrightarrow{\varphi} & H^1(\mathcal{H},\mathbb{Q}/\mathbb{Z}) \\
\downarrow{\scriptstyle \beta_1} & & \downarrow{\scriptstyle \beta_2} \\
\prod_v H^1(\mathcal{G}_v,\mathbb{Q}/\mathbb{Z}) & \xrightarrow{\psi} & \prod_v(\bigoplus_{i=1}^{r_v} H^1(\mathcal{H}_i^v,\mathbb{Q}/\mathbb{Z}))
\end{array}
\tag{6.23}
$$

where all horizontal arrows are induced by the restrictions; in particular, $\Phi \simeq \beta_2^{-1}(\operatorname{im}\psi)/\operatorname{im}\varphi$. But for a finite group $\mathcal{F}$, $H^1(\mathcal{F},\mathbb{Q}/\mathbb{Z})$ is the dual of the abelianization $\mathcal{F}^{ab} = \mathcal{F}/[\mathcal{F},\mathcal{F}]$; therefore (6.23) is the dual of

$$
\begin{array}{ccc}
\mathcal{G}/[\mathcal{G},\mathcal{G}] & \xleftarrow{\mu} & \mathcal{H}/[\mathcal{H},\mathcal{H}] \\
\uparrow{\scriptstyle \gamma} & & \uparrow{\scriptstyle \delta} \\
\bigoplus_v \mathcal{G}_v/[\mathcal{G}_v,\mathcal{G}_v] & \xleftarrow{\eta} & \sum_v(\sum_{i=1}^{r_v}\mathcal{H}_i^v/[\mathcal{H}_i^v,\mathcal{H}_i^v])
\end{array}
\tag{6.24}
$$

where all the arrows are induced by the respective inclusions. By virtue of elementary facts about the duality of abelian groups, (6.24) yields

THEOREM 6.12. *Notation as in (6.24),*

$$\Phi \simeq \ker\mu/\delta(\ker\eta).$$

Theorem 6.12 enables us to compute Φ effectively. In this regard, if $\Phi \neq 1$, then clearly the Hasse principle does not hold for P/K. These facts underlie the construction of the first counterexample to Bartels' conjecture. Namely, first one constructs a Galois extension L/K with Galois group $\mathcal{G} = A_6$, such that there are at least two valuations of K having a noncyclic decomposition group in L and all the noncyclic decomposition groups are isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$. $\mathcal{G}$ contains a subgroup $\mathcal{H}$ of index 10, which is generated by the permutations (123), (456), (1425), (36), and hence is isomorphic to the semidirect product $(\mathbb{Z}/3\mathbb{Z})^2 \rtimes \mathbb{Z}/4\mathbb{Z}$. Put $P = L^{\mathcal{H}}$. Using the criterion from §1.5.1, we infer that P is K-adequate. On the other hand, direct computation shows that the first obstruction in this case is nontrivial, and consequently the Hasse principle does not hold for P/K.

The first obstruction is useful not only for constructing counterexamples, but also for proving the validity of the Hasse principle for extensions of one or another type. This is the case, for example, if the first obstruction is all of $Ш(T)$, which is naturally called the *total obstruction*. Drakokhrust-Platonov [1] established that the first obstruction is precisely the total obstruction for extensions of square-free degree and for K-adequate extensions of degree p^2. From this fact, by computing the first obstruction, they deduced the validity of the Hasse principle for K-adequate extensions whose degree is either 6 or of the form p^2.

The total obstruction is not always the same as the first obstruction; however, as Drakokhrust has shown [1], it can be computed in a similar way with the aid of generalized representation groups. The foundation

for the theory of representation groups was laid down by Schur [1], and a contemporary treatment of the subject may be found in Beyl-Tappe [1].

A finite group $\bar{\mathcal{G}}$ is a *generalized representation group* of a finite group $\mathcal{G}$ if there is a central extension $1 \to M \to \bar{\mathcal{G}} \xrightarrow{\lambda} \mathcal{G} \to 1$, such that $M \cap [\bar{\mathcal{G}}, \bar{\mathcal{G}}]$ is isomorphic to $H^3(\mathcal{G}, \mathbb{Z})$, known as the *Schur multiplier* of $\mathcal{G}$. (Note that $H^3(\mathcal{G}, \mathbb{Z}) = H^2(\mathcal{G}, \mathbb{Q}/\mathbb{Z})$ by Lemma 1.3. For comparison, we point out that the classical definition of a representation group requires that $M \subset [\bar{\mathcal{G}}, \bar{\mathcal{G}}]$.) Let $\bar{\mathcal{G}}$ be an arbitrary generalized representation group for $\mathcal{G}$. Given any subgroup $\mathcal{F}$ of $\mathcal{G}$, let $\bar{\mathcal{F}}$ denote the inverse image $\lambda^{-1}(\mathcal{F})$. Consider the following diagram, analogous to (6.24):

$$\begin{array}{ccc} \bar{\mathcal{G}}/[\bar{\mathcal{G}}, \bar{\mathcal{G}}] & \xleftarrow{\pi} & \bar{\mathcal{H}}/[\bar{\mathcal{H}}, \bar{\mathcal{H}}] \\ \uparrow & & \uparrow \varepsilon \\ \sum_v \bar{\mathcal{G}}_v/[\bar{\mathcal{G}}_v, \bar{\mathcal{G}}_v] & \xleftarrow{\varrho} & \sum_v \Big(\sum_{i=1}^{r_v} \bar{\mathcal{H}}_i^v/[\bar{\mathcal{H}}_i^v, \bar{\mathcal{H}}_i^v]\Big) \end{array}$$

Under this notation, we have

THEOREM 6.13 (DRAKOKHRUST [1]). *$Ш(T) \simeq \ker \pi/\varepsilon(\ker \varrho)$ for the norm torus $T = \mathbf{R}^{(1)}_{P/K}(\mathbb{G}_m)$.*

Drakokhrust [1] provides specific examples of computation of $Ш(T)$ by means of this formula.

We conclude our survey of results related to the Hasse norm principle with the following assertion (cf. Bartels [3], Platonov [20], Platonov-Rapinchuk [4]).

PROPOSITION 6.10. *Let P/K be an extension of prime degree p. Then the Hasse norm principle holds for P/K.*

PROOF: Let L denote the minimal Galois extension containing P, and put $\mathcal{G} = \mathrm{Gal}(L/K)$, $\mathcal{H} = \mathrm{Gal}(L/P)$. Then $\mathcal{G}$ is a subgroup of the symmetric group S_p, and therefore $|\mathcal{G}|$ is divisible only by the first power of p. Consequently, $(|\mathcal{H}|, p) = 1$ and the Sylow p-subgroup $\mathcal{G}_p$ of $\mathcal{G}$ is a cyclic group of order p.

Now let us return to (6.22), set up for $T = \mathbf{R}^{(1)}_{P/K}(\mathbb{G}_m)$. Recall that

$$Ш(T) \simeq K^* \cap N_{P/K}(J_P)/N_{P/K}(P^*).$$

Since $Ш(T) \simeq \ker \alpha_3$ is a group of exponent p, it suffices to show that the p-part of $H^2(\mathcal{G}, \mathbf{X}(T))$ is trivial. But $H^2(\mathcal{G}, \mathbb{Z}[\mathcal{G}/\mathcal{H}]) \simeq H^2(\mathcal{H}, \mathbb{Z})$ is annihilated by multiplication by $|\mathcal{H}|$, and therefore has exponent prime to p.

On the other hand, the p-part of $H^3(\mathcal{G}, \mathbb{Z})$ is isomorphic to $H^3(\mathcal{G}_p, \mathbb{Z}) = 0$, since $\mathcal{G}_p$ is cyclic. Thus, the desired assertion follows from the exactness of the top row of (6.22).

A more arithmetic argument can also be given. Notation as above, also put $F = L^{\mathcal{G}_p}$. Then, clearly, $L = FP$ and $F \cap P = K$. For an arbitrary a in $K^* \cap N_{P/K}(J_P)$ one has $a \in F^* \cap N_{L/F}(J_L)$; and hence $a \in N_{L/F}(L^*)$ by the Hasse norm theorem, since L/F is cyclic. Therefore

$$a^{[F:K]} = N_{F/K}(a) \in N_{L/K}(L^*) = N_{P/K}(N_{L/P}(L^*)) \subset N_{P/K}(P^*).$$

On the other hand, $a^p \in N_{P/K}(P^*)$. Since $[F : K]$ and p are relatively prime, it follows that $a \in N_{P/K}(P^*)$. This proves Proposition 6.10.

In practice, in addition to norm tori one also encounters *multinorm tori* (cf. §2.1.7). Recall that this is what we call the kernel T of the morphism $\varphi\colon \mathbf{R}_{P_1/K}(\mathbb{G}_m) \times \cdots \times \mathbf{R}_{P_l/K}(\mathbb{G}_m) \to \mathbb{G}_m$ which is the product of the norm maps for the finite extensions P_i/K $(i = 1, \ldots, l)$.

EXERCISE: Show that any maximal K-torus of $G = \mathbf{SL}_n$ is multinorm, i.e., corresponds to some collection $P_1, \ldots, P_l$ of finite extensions of K such that $\sum_{i=1}^{l} [P_i : K] = n$.

The exact sequence $1 \to T \to \prod_{i=1}^{l} \mathbf{R}_{P_i/K}(\mathbb{G}_m) \to \mathbb{G}_m \to 1$ easily yields

$$Ш(T) \simeq (K^* \cap N_{P_1/K}(J_{P_1}) \ldots N_{P_l/K}(J_{P_l}))/N_{P_1/K}(P_1^*) \ldots N_{P_l/K}(P_l^*).$$

Hence the validity of the Hasse principle for T means that an element a in K^*, which is representable locally as the product of norms from P_i, can be represented globally in a similar way. Therefore in the given situation the local-global principle naturally is said to be *multinorm*. Although this principle has never before been examined in close detail, it plays an important role here. In particular, it allows considerable simplification of the proof of the Hasse principle for groups of type ${}^2A_n$. Another application has to do with the structure of groups of rational points of simple groups of type ${}^1A_n$ (cf. §9.2). For our purposes, the following sufficiency test for the validity of the multinorm principle (due to Drakokhrust for the case of Galois extensions) is quite adequate.

PROPOSITION 6.11. *Let P_i $(i = 1, 2)$ be finite extensions of K, and let L_i be their normal closures. Assume the following conditions are satisfied:*

(1) *$L_1 \cap L_2 = K$;*
(2) *P_1/K satisfies the Hasse norm principle.*

Then $K^* \cap (N_{P_1/K}(J_{P_1}) N_{P_2/K}(J_{P_2})) = N_{P_1/K}(P_1^*) N_{P_2/K}(P_2^*)$.

PROOF: Put $P = P_1P_2$, $L = L_1L_2$, $\mathcal{G}_i = \mathrm{Gal}(L_i/K)$, $\mathcal{G} = \mathrm{Gal}(L/K) = \mathcal{G}_1 \times \mathcal{G}_2$, $\mathcal{H}_i = \mathrm{Gal}(L_i/P_i)$ and $\mathcal{H} = \mathrm{Gal}(L/P) = \mathcal{H}_1 \times \mathcal{H}_2$. Also, let M_i denote the maximal abelian extension of K contained in P_i. We immediately note that $\mathcal{H}[\mathcal{G},\mathcal{G}] = \mathcal{H}_1[\mathcal{G}_1,\mathcal{G}_1] \times \mathcal{H}_2[\mathcal{G}_2,\mathcal{G}_2]$, whence by Galois theory it follows that the maximal abelian extension M of K contained in P has the form $M = M_1M_2$. Moreover, it follows from

$$[\mathcal{H}_1 \times \mathcal{G}_2, \mathcal{H}_1 \times \mathcal{G}_2](\mathcal{H}_1 \times \mathcal{H}_2) = \mathcal{H}_1 \times (\mathcal{H}_2[\mathcal{G}_2,\mathcal{G}_2])$$

that for $i = 1,2$ the maximal abelian extension of P_i contained in P has the form P_iM_{3-i}.

Consider the map

$$\varphi\colon J_{P_1}/P_1^*N_{P/P_1}(J_P) \times J_{P_2}/P_2^*N_{P/P_2}(J_P) \to J_K/K^*N_{P/K}(J_P),$$

induced by the product of the norm maps $N_{P_1/K}$ and $N_{P_2/K}$. Our goal is to show that φ is injective. We shall do this by showing that φ is surjective and that the image and the domain of φ have the same order. To this end, we consider the analogous map

$$\psi\colon J_{M_1}/M_1^*N_{M/M_1}(J_M) \times J_{M_2}/M_2^*N_{M/M_2}(J_M) \to J_K/K^*N_{M/K}(J_M).$$

Using class field theory isomorphisms $J_{M_i}/M_i^*N_{M/M_i}(J_M) \simeq \mathrm{Gal}(M/M_i)$ and $J_K/K^*N_{M/K}(J_M) \simeq \mathrm{Gal}(M/K)$, and the fact that $\mathrm{Gal}(M/K) \simeq \mathrm{Gal}(M/M_1) \times \mathrm{Gal}(M/M_2)$, we see that ψ is an isomorphism. Therefore ψ is surjective, i.e.,

$$J_K = N_{M_1/K}(J_{M_1})N_{M_2/K}(J_{M_2})K^* \tag{6.25}$$

and the image and the domain of ψ have the same order. Now we can apply the fact that for any finite extension of number fields E/F we have $F^*N_{E/F}(J_E) = F^*N_{N/F}(J_N)$, where N is the maximal abelian extension of F contained in E (cf. [ANT, Exercise 8]). In particular, $K^*N_{P_i/K}(J_{P_i}) = K^*N_{M_i/K}(J_{M_i})$; in view of (6.25) it follows that

$$J_K = N_{P_1/K}(J_{P_1})N_{P_2/K}(J_{P_2})K^*,$$

which means that φ is surjective. Furthermore,

$$\begin{aligned}|J_{P_1}/P_1^*N_{P/P_1}(J_P)| &= |J_{P_1}/P_1^*N_{P_1M_2/P_1}(J_{P_1M_2})| \\ &= [P_1M_2 : P_1] = [M_2 : K] = [M : M_1] \\ &= |J_{M_1}/M_1^*N_{M/M_1}(J_M)|\end{aligned}$$

since P_1M_2 is a maximal abelian extension of P_1 contained in P; similarly

$$\begin{aligned}|J_{P_2}/P_2^*N_{P/P_2}(J_P)| &= |J_{M_2}/M_2^*N_{M/M_2}(J_M)| \\ |J_K/K^*N_{P/K}(J_P)| &= |J_K/K^*N_{M/K}(J_M)|.\end{aligned}$$

It follows from these equations that

$$|J_{P_1}/P_1^*N_{P/P_1}(J_P)||J_{P_2}/P_2^*N_{P/P_2}(J_P)| = |J_K/K^*N_{P/K}(J_P)|,$$

thus completing the proof that φ is injective.

Now let $a \in K^*$ and $a = N_{P_1/K}(x_1)N_{P_2/K}(x_2)$, where $x_i \in J_{P_i}$. Then the pair $(x_1P_1^*N_{P/P_1}(J_P),\ x_2P_2^*N_{P/P_2}(J_P))$ lies in the kernel of φ, so $x_i = y_iN_{P/P_i}(z_i)$, where $y_i \in P_i^*$ and $z_i \in J_P$ (for $i = 1,2$). Under this notation, $a = N_{P_1/K}(y_1)N_{P_2/K}(y_2)N_{P/K}(z_1z_2)$; and therefore

$$\begin{aligned}aN_{P_1/K}(y_1)^{-1}N_{P_2/K}(y_2)^{-1} &\in K^* \cap N_{P/K}(J_P) \\ &\subset K^* \cap N_{P_1/K}(J_{P_1}) = N_{P_1/K}(P_1^*),\end{aligned}$$

since the Hasse principle holds for P_1/K. These computations imply that $a \in N_{P_1/K}(P_1^*)N_{P_2/K}(P_2^*)$. Proposition 6.11 is proved.

Unfortunately the multinorm principle has not yet been analyzed fully.

We conclude this section with a technical assertion about $P^2(L/K,T)$ which we shall need in studying the coboundary map for semisimple groups.

PROPOSITION 6.12 (KNESER [12]). *Let T be a torus defined over a number field K and split over a finite Galois extension L/K. Assume that T is K_{v_0}-anisotropic for some v_0 in V^K. Then $P^2(L/K,T) = 0$.*

PROOF: It might seem natural to use Theorem 6.10; however, closer analysis shows that this approach does not yield the desired result. A preferable approach is to use the dual description of $P^2(L/K,T)$ as the cokernel of the map $\sum_v \hat{H}^{-1}(L_w/K_v, \mathbf{X}_*(T)) \to \hat{H}^{-1}(L/K, \mathbf{X}_*(T))$ induced by $\mathrm{Cor}_{\mathcal{G}_v}^{\mathcal{G}}$. (This result was obtained in the course of proving Theorem 6.10.) Then, to prove the proposition it suffices to establish that

$$\mathrm{Cor}_{\mathcal{G}_v}^{\mathcal{G}}\colon \hat{H}^{-1}(L_{w_0}/K_{v_0}, \mathbf{X}_*(T)) \to \hat{H}^{-1}(L/K, \mathbf{X}_*(T))$$

is surjective. However, $\mathbf{X}_*(T)^{\mathcal{G}_{v_0}} = 0$ since T is K_{v_0}-anisotropic. On the other hand, the image of the norm map $N_{v_0}\colon \mathbf{X}_*(T) \to \mathbf{X}_*(T)$ (given by $N_{v_0}(x) = \sum_{g \in \mathcal{G}_{v_0}} gx$) clearly lies in $\mathbf{X}_*(T)^{\mathcal{G}_{v_0}}$; therefore $\ker N_{v_0} = \mathbf{X}_*(T)$. Let $\mathbf{X}_*(T)'$ (resp., $\mathbf{X}_*(T)'_{v_0}$) denote the subgroup of $\mathbf{X}_*(T)$ generated by

elements of the form $g\chi - \chi$, for χ in $\mathbf{X}_*(T)$ and g in $\mathcal{G}$ (resp., $\mathcal{G}_{v_0}$). By definition $\hat{H}^{-1}(L_{w_0}/K_{v_0}, \mathbf{X}_*(T)) = \ker N_{v_0}/((\mathbf{X}_*(T))'_{v_0}$ and

$$\hat{H}^{-1}(L/K, \mathbf{X}_*(T)) = \ker N/(\mathbf{X}_*)T))',$$

where $N: \mathbf{X}_*(T) \to \mathbf{X}_*(T)$ is the norm map corresponding to $\mathcal{G}$. Then, bearing in mind that in the given situation $\mathrm{Cor}^{\mathcal{G}}_{\mathcal{G}_{v_0}}$ is induced by embedding $\ker N_{v_0}$ in $\ker N$, we conclude that $\mathrm{Cor}^{\mathcal{G}}_{\mathcal{G}_{v_0}}$ is surjective. Proposition 6.12 is proved.

6.4. Finiteness theorems for Galois cohomology.

In this section we shall extend the finiteness results for Galois cohomology, obtained for the case of algebraic tori in §6.3, to arbitrary algebraic groups.

THEOREM 6.14. *Let G be an algebraic group defined over a local field K. Then $H^1(K, G)$ is finite.*

THEOREM 6.15. *For any algebraic group G defined over a number field K, the kernel of the canonical map $H^1(K, G) \to \prod_v H^1(K_v, G)$ is finite.*

Whereas the proofs of these theorems for tori were fairly standard, the proofs in general are totally different. Namely, to prove Theorem 6.15 we shall have to appeal to the reduction theory for adele groups developed in Chapter 5, while Theorem 6.14 is a formal consequence of a certain property of the Galois group of a local field.

DEFINITION: A profinite group $\mathcal{G}$ is said to have type (F) if it has only a finite number of open subgroups of index n, for each integer n. A field K has type (F) if it is perfect and its absolute Galois group $\mathcal{G} = \mathrm{Gal}(\bar{K}/K)$ has type (F).

Clearly a perfect field K has type (F) if and only if for every n it has finitely many extensions of degree n. It follows that examples of fields of type (F) are:

(a) the field of reals,
(b) a finite field,
(c) the field of formal power series $P\langle t\rangle$ in one indeterminate over an algebraically closed field P of characteristic 0.

(In the latter case it is well known (Puiseux' theorem) that $P\langle t\rangle$ has a unique extension of degree n, which has the form $P\langle \sqrt[n]{t}\rangle$, for any n. The fact that the local fields are of type (F) is crucial for our purposes.

PROPOSITION 6.13. *Any finite extension K of $\mathbb{Q}_p$ has type (F).*

PROOF: Since for every n there is a unique unramified extension of K of degree n, and any finite extension of K can be represented as a tower of unramified and totally ramified extensions (cf. [ANT, Ch. 1]), it suffices to show that any local field has finitely many totally ramified extensions. To avoid introducing additional notation, we shall prove this fact for K.

It is well known (cf. Proposition 1.4) that any totally ramified extension of K of degree n is given by the root of an Eisenstein polynomial

$$t^n + a_{n-1}t^{n-1} + \cdots + a_0 = 0.$$

But the set M of coefficients $(a_{n-1}, \ldots, a_0)$ of all possible Eisenstein polynomials is obviously a compact subset of K^n. Therefore the standard argument shows that the desired assertion is a consequence of the following result, known as *Krasner's lemma*: if f is an irreducible monic polynomial over K of degree n, then any polynomial g over K whose coefficients are sufficiently close to those of f is also irreducible; moreover, f and g define isomorphic extensions of K.

The reader may find the usual proof of Krasner's lemma in Lang [2]. We shall show how this assertion is obtained in our context. For $f(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_0$ let $a(f)$ denote the companion matrix

$$\begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & 0 & \ldots & 0 & \vdots \\ 0 & 1 & 0 & \ldots & 0 & \vdots \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 1 & -a_{n-1} \end{pmatrix}.$$

It is easily verified that $f(a(f)) = 0$. If, in addition, f is irreducible, then $K[a(f)]$, the K-algebra generated by $a(f)$, is isomorphic to the extension K_f of degree n over K given by f. In this regard, the multiplicative group $K[a(f)]^*$ is the set of K-points of $T = \mathbf{R}_{K_f/K}(\mathbb{G}_m)$. Put $G = \mathbf{GL}_n$ and let U denote the open subvariety of T consisting of regular elements in G (cf. §2.1.11). Also, consider the map $\varphi: G \times U \to G$ given by $\varphi(g, u) = gug^{-1}$. Then the image of φ is precisely the set of semisimple regular elements of G, and therefore is Zariski-open in G; in particular, φ is a dominant morphism. Therefore, it follows from Proposition 3.3 that $W = \varphi(G_K \times U_K)$ is an open subset of G_K under the v-adic topology. On the other hand, it is clear that, for any x in W, $K[x]$ is conjugate to $K[a(f)]$ under G_K. Since $a(f) \in U_K \subset W$, clearly $a(g) \in W$ for all g sufficiently close to f, and therefore $K[a(f)]$ and $K[a(g)]$ are conjugate; hence K_f and K_g are isomorphic. Proposition 6.13 is proved.

Theorem 6.14 is a consequence of the following general result.

THEOREM 6.16. *Let K be a field of type (F), and let G be a linear algebraic group defined over K. Then $H^1(K,G)$ is finite.*

PROOF: First we prove the theorem for G finite. Let $\mathcal{H}$ denote an open normal subgroup of $\mathcal{G} = \mathrm{Gal}(\bar{K}/K)$ which acts trivially on $G = G_{\bar{K}}$. By the definition of group of type (F), there are only a finite number of open subgroups of $\mathcal{G}$ contained in $\mathcal{H}$ and having index in $\mathcal{H}$ not exceeding $n = |G|$. Their intersection, which we denote by $\mathcal{F}$, is an open normal subgroup of $\mathcal{G}$ contained in $\mathcal{H}$. We claim that the restriction map $\varphi: H^1(\mathcal{G}, G_{\bar{K}}) \to H^1(\mathcal{F}, G_{\bar{K}})$ is trivial. Indeed, if $f: \mathcal{G} \to G_{\bar{K}}$ is a continuous 1-cocycle, then $g = f\,|_{\mathcal{H}}$ is a continuous homomorphism from $\mathcal{H}$ to $G_{\bar{K}}$, since $\mathcal{H}$ acts trivially on $G_{\bar{K}}$. Then $[\mathcal{H} : \ker g] \leq n$, so by assumption $\mathcal{F} \subset \ker g$, i.e., $g(\mathcal{F}) = \{e\}$, as desired.

Now let us consider the noncommutative analog of the Hochschild-Serre exact sequence (cf. 1.3.2):

$$1 \to H^1(\mathcal{G}/\mathcal{F}, G_{\bar{K}}) \xrightarrow{\varepsilon} H^1(\mathcal{G}, G_{\bar{K}}) \xrightarrow{\varphi} H^1(\mathcal{F}, G_{\bar{K}}). \tag{6.26}$$

Since φ is trivial and (6.26) is exact, ε is surjective. But $H^1(\mathcal{G}/\mathcal{F}, G_{\bar{K}})$ is obviously finite; therefore $H^1(\mathcal{G}, G_{\bar{K}}) = H^1(K,G)$ is also finite.

The following lemma, applied to $N = G^0$, together with the fact just proved, enables us to reduce Theorem 6.16 to the case of connected groups.

LEMMA 6.9. *Let G be an algebraic K-group, and let N be a normal K-subgroup. Assume $H^1(K, G/N)$ is finite, and that $H^1(K, {}_\mu N)$ is finite for each μ in $Z^1(K,G)$, where ${}_\mu N$ is the group obtained from N by twisting using μ.[3] Then $H^1(K,G)$ is also finite.*

Indeed, the exact sequence of K-groups $1 \to N \to G \to G/N \to 1$ induces the map of the first cohomology $H^1(K,G) \xrightarrow{\pi} H^1(K, G/N)$, which has the following property: $H^1(K, {}_\mu N)$ maps onto the fiber $\pi^{-1}(\pi(\mu))$, for any μ in $H^1(K,G)$ (cf. §1.3.2). Therefore if $\pi(H^1(K,G)) = \pi(\{\mu_1, \dots, \mu_r\})$, then $H^1(K,G) = \bigcup_{i=1}^r \pi^{-1}(\pi(\mu_i))$ is finite, since each of the $\pi^{-1}(\pi(\mu_i))$ is finite by the assumption that $H^1(K, {}_{\mu_i} N)$ is finite.

Thus we may assume G to be connected. In this case, as Proposition 2.9 shows, $H^1(K,G) = H^1(K,H)$ for a maximal reductive K-subgroup H of G; hence we need only consider the case of G connected and reductive. First we take the case $G = T$, an algebraic torus. (Note that the finiteness of $H^1(K,T)$ for a local field K was established in §6.3, however here we shall obtain a general proof, good for all fields of type (F).) Let L denote a finite Galois extension of K over which T becomes split, and put $n = [L : K]$. Then $H^1(K,T)$ is precisely $H^1(L/K, T)$ (by Lemma 6.8), and therefore is a

[3] We have in mind G acting naturally on N by conjugation.

group of exponent n. Consider the morphism $\eta: T \to T$ given by $\eta(t) = t^n$, and let S denote its kernel. We have the exact sequence of cohomology groups $H^1(K,S) \to H^1(K,T) \xrightarrow{\theta} H^1(K,T)$, where θ is the homomorphism induced by η. It follows from the above that θ is trivial, therefore $H^1(K,T)$ is precisely the image of $H^1(K,S)$. But $H^1(K,S)$ is clearly finite; so we conclude that $H^1(K,T)$ is also finite.

The case of arbitrary connected reductive groups in Theorem 6.16 can be reduced easily to the case of tori. To this end, note that by combining Lemma 6.9 with the results obtained on the finiteness of H^1 for finite groups and tori, we obtain the finiteness of H^1 for any group whose connected component is a torus. This result can be applied, in particular, to the normalizer $N = N_G(T)$ of an arbitrary K-torus T in a given connected reductive K-group G. Therefore, the proof of Theorem 6.16 is completed by

LEMMA 6.10. *The natural map $H^1(K,N) \to H^1(K,G)$ is surjective.*

PROOF: Let $\mathcal{T} = G/N$ be the variety of maximal tori of G (cf. §2.4.5). For an arbitrary cocycle g in $Z^1(K,G)$, take the group ${}_gG$ and the variety ${}_g\mathcal{T}$, obtained by twisting (noting that G acts on itself by conjugation and on $\mathcal{T}$ by translation). Clearly there is a K-action of ${}_gG$ on ${}_g\mathcal{T}$, moreover the stabilizer of a point is the normalizer of a maximal torus. Then, using the fact that ${}_gG$ always has a maximal K-torus (cf. §2.1.9), we can show easily that $({}_g\mathcal{T})_K \neq \emptyset$; therefore Lemma 1.6 implies that g lies in the image of $H^1(K,N) \to H^1(K,G)$. Lemma 6.10 is proved.

COROLLARY 1. *Let K be a field of type (F). Then any given semisimple K-group G has only a finite number of K-forms, up to K-isomorphism.*

Indeed, we know (cf. §2.2) that, up to K-isomorphism, the K-forms of a given K-group G are classified by the elements of $H^1(K, \mathrm{Aut}_{\bar{K}}(G))$. On the other hand, for a semisimple group G, $\mathrm{Aut}_{\bar{K}}(G)$ is a finite extension of the group of inner automorphisms, which is isomorphic to the adjoint group, and therefore can be viewed as an algebraic K-group. Then, by Theorem 6.14, $H^1(K, \mathrm{Aut}_{\bar{K}}(G))$ is finite; hence the number of nonisomorphic K-forms of G is also finite.

EXERCISE: Find out whether the corollary also holds for an arbitrary connected group G. (Note that the above proof does not work for an algebraic torus T of dimension $n > 1$, since here $\mathrm{Aut}_{\bar{K}}(T) \cong GL_n(\mathbb{Z})$ is not an algebraic group.)

COROLLARY 2. *Let X be a homogeneous space of a linear algebraic group G, both defined over a field K of type (F). Then X_K is the union of a finite number of orbits of G_K.*

For $X_K = \emptyset$ we have nothing to prove. For $X_K \neq \emptyset$ let $x \in X_K$, and let $H = G(x)$ be the stabilizer of x. Since K is perfect, H is defined over K, and it suffices to establish that there are only finitely many orbits of G_K on $(G/H)_K$. It is well known, however, that these are in one-to-one correspondence with the elements of the kernel of $H^1(K,H) \to H^1(K,G)$; therefore the desired result follows from Theorem 6.16.

In particular, taking X to be the variety $\mathcal{T}$ of tori of a given connected group G, we obtain

COROLLARY 3. *Let G be a connected linear group over a field K of type (F). Then the maximal K-tori of G form a finite number of conjugacy classes with respect to G_K.*

A special case of Theorem 6.16 is the assertion on the finiteness of the first set of real cohomology $H^1(\mathbb{R},G)$, for any algebraic $\mathbb{R}$-group G. Actually this follows from Whitney's theorem (cf. §3.2, Theorem 3.6). Indeed, in §3.2, using Whitney's theorem we gave a proof of Corollary 2 for $K = \mathbb{R}$, independent of Theorem 6.16. Now let G be a real algebraic group, and let $G \subset \mathbf{GL}_n$ be a matrix realization of G defined over $\mathbb{R}$. Applying Corollary 2 to $X = \mathbf{GL}_n/G$, we see that there are only finitely many orbits of $\mathbf{GL}_n(\mathbb{R})$ on $X_{\mathbb{R}}$; hence also the finiteness of the kernel of $H^1(\mathbb{R},G) \to H^1(\mathbb{R},\mathbf{GL}_n)$ (cf. proof of Corollary 2). But $H^1(R,\mathbf{GL}_n) = \{1\}$ (Lemma 2.2); therefore, we thus obtain the finiteness of all $H^1(\mathbb{R},G)$. (This argument shows that Corollary 2 is indeed equivalent to Theorem 6.16 itself. Below we shall use the adelic version of this observation in the proof of Theorem 6.15.) Actually, for real cohomology there are much more precise results. For instance, Serre [1, Ch. 3, §4.5] proved the following assertion for the case of $\mathbb{R}$-anisotropic G:

THEOREM 6.17. *Let G be a connected algebraic $\mathbb{R}$-group with $G_{\mathbb{R}}$ compact. Then $H^1(\mathbb{R},G)$ is in one-to-one correspondence with S/W, where S is the set of elements of a fixed maximal $\mathbb{R}$-torus $T \subset G$ satisfying $x^2 = 1$, and W is the Weyl group of T acting on T by conjugation.*

(In classical terms, the theorem means that the elements of $H^1(\mathbb{R},G)$ are in one-to-one correspondence with the conjugacy classes of involutions in $G_{\mathbb{R}}$.)

The cohomology of an arbitrary connected reductive real group G was recently described by Borovoi [2]. To formulate his result we need to introduce some notation. Let T_0 be a maximal $\mathbb{R}$-anisotropic torus of G, and let T be its centralizer $C_G(T_0)$. Then T is a maximal $\mathbb{R}$-torus of G, and one can consider the corresponding Weyl group $W = W(T,G) = N/T$, where $N = N_G(T)$ is the normalizer of T in G. We define the action of W on $H^1(\mathbb{R},T)$ as follows. Let $\sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ be the complex conjugation. Any

cocycle ξ in $Z^1(\mathbb{R},T)$ can be defined by an element $z = \xi_\sigma \in T_{\mathbb{C}}$ satisfying $z\sigma(z) = 1$. If w in W is represented by an element n in $N_{\mathbb{C}}$, then we define $w\xi$ as the cocycle given by $n^{-1}z\sigma(n)$. It is easy to verify that this action is well defined. With this notation we have

THEOREM 6.18. *The embedding $T \subset G$ induces a bijection*

$$H^1(\mathbb{R},T)/W \xrightarrow{\sim} H^1(\mathbb{R},G).$$

The proof of Theorem 6.18 and several of its applications can be found in Borovoi [2].

Let us proceed to an analysis of finiteness properties for cohomology of groups defined over a number field K. Here K does not have type (F) (why?), and actually $H^1(K,G)$ now can be infinite. Therefore in this situation the finiteness theorems are of a different nature (cf. Theorem 6.15 and Theorem 6.19 below), and their proofs are based on other arguments.

Let us begin the proof of Theorem 6.15 by considering a finite group.

LEMMA 6.11. *Let G be a finite K-group. Then the kernel $Ш(G)$ of the canonical map $H^1(K,G) \to \prod_v H^1(K_v,G)$ is finite.*

PROOF: Let $\mathcal{H}$ be an open normal subgroup of $\mathcal{G} = \mathrm{Gal}(\bar{K}/K)$ acting trivially on $G = G_{\bar{K}}$, and put $L = \bar{K}^{\mathcal{H}}$. We shall show that the kernel of $H^1(L,G) \xrightarrow{\theta} \prod_w H^1(L_w,G)$ is trivial. It will follow that the image of $Ш(G)$ under the restriction map $H^1(K,G) \to H^1(L,G)$ is trivial, so we can conclude from the exact sequence

$$1 \to H^1(L/K,G) \to H^1(K,G) \to H^1(L,G)$$

that $Ш(G)$ is covered by the finite set $H^1(L/K,G)$ and hence is itself finite.

To analyze the kernel of θ, note that in the given situation the 1-cocycles are continuous homomorphisms $\alpha\colon \mathcal{H} \to G$, and there is only one trivial cocycle, which is defined by the unity homomorphism. Now if $\alpha \in \ker\theta$, then $\alpha(\mathcal{H}_w) = \{1\}$ for any valuation w in V^L, where $\mathcal{H}_w = \mathrm{Gal}(\bar{L}_w/L_w)$ is identified with the decomposition subgroup of $\mathcal{H} = \mathrm{Gal}(\bar{L}/L)$ of a fixed extension $\bar{w}$ of w to $\bar{L}$. Note that any two extensions $\bar{w}'$ and $\bar{w}''$ are conjugate with respect to $\mathcal{H}$, so the corresponding subgroups $\mathcal{H}'_w$ and $\mathcal{H}''_w$ are conjugate in $\mathcal{H}$; thus $\alpha(\mathcal{H}'_w) = \{1\}$ if and only if $\alpha(\mathcal{H}''_w) = \{1\}$. Hence it suffices to show that the closed normal subgroup $\mathcal{P}$ of $\mathcal{H}$ generated by all $\mathcal{H}_w$ is $\mathcal{H}$. Consider the fixed field $P = \bar{L}^{\mathcal{P}}$. Then P is a normal extension of L having the following property: $P \subset L_w$ for all w in V^L. If we suppose $P \neq L$, then there is a nontrivial finite normal extension F/L which also satisfies $F \subset L_w$ for all w in V^L. But this obviously contradicts the Chebotarev density theorem. The lemma is proved.

To reduce Theorem 6.15 to the case of a connected group we also need

LEMMA 6.12. *Let G be an algebraic K-group, and let G^0 be its connected component. Then $G_{K_v}/G^0_{K_v} = (G/G^0)_{K_v}$ for almost all v. Hence, the kernel of $H^1(K_v, G^0) \to H^1(K_v, G)$ is trivial for almost all v.*

PROOF: Consider the exact sequence $1 \to G_0 \to G \xrightarrow{\pi} G/G_0 \to 1$ and its associated exact cohomological sequence

$$G_{K_v} \xrightarrow{\pi} (G/G_0)_{K_v} \to H^1(K_v, G^0) \xrightarrow{\psi} H^1(K_v, G). \tag{6.27}$$

In the proof of Proposition 5.5 we showed that $\pi(G_{\mathcal{O}_v}) = (G/G^0)_{K_v}$ for almost all v in V_f^K; in particular $\pi(G_{K_v}) = (G/G^0)_{K_v}$. Therefore (6.27) implies that $\ker\psi$ is trivial for these v. The lemma is proved.

Now let us suppose we can prove that Ш of a connected group is finite; we shall show that $Ш(G)$ then is finite for any K-group G. Consider the commutative diagram

$$\begin{array}{ccc} H^1(K,G) & \xrightarrow{\varrho} & \prod_v H^1(K_v,G) \\ \downarrow{\scriptstyle\sigma} & & \downarrow{\scriptstyle\tau} \\ H^1(K,G/G^0) & \xrightarrow{\theta} & \prod_v H^1(K_v,G/G^0) \end{array}$$

By Lemma 6.11 $\ker\theta$ is finite, whence it follows that $\sigma(Ш(G))$ is finite. Let $\sigma(Ш(G)) = \sigma(\{\mu_1, \dots, \mu_r\})$, for $\mu_i \in Ш(G)$. It follows by a twisting argument that $Ш(G)$ is covered by the union of the images of $Ш_i = \ker(H^1(K, G_i^0) \to \prod_v H^1(K_v, G_i))$, where $G_i = {}_{\mu_i}G$ and $G_i^0 = {}_{\mu_i}G_i^0$ are the respective twisted groups. But by Lemma 6.12 the kernel of $H^1(K_v, G_i^0) \to H^1(K_v, G_i)$ is trivial for almost all v, and, as Theorem 6.14 implies, is finite in the remaining cases. Therefore $\prod_v H^1(K_v, G_i^0) \to \prod_v H^1(K_v, G_i)$ has finite kernel, so the image of $Ш_i$ in $\prod_v H^1(K_v, G_i^0)$ is finite. But by assumption the kernel of $H^1(K,H) \to \prod_v H^1(K_v, H)$ is finite for any connected group H; therefore by a twisting argument it follows that the inverse image of any element under $H^1(K, G_i^0) \to \prod_v H^1(K_v, G_i^0)$ is finite. In view of the above, we obtain that each of the $Ш_i$ is finite, which means that $Ш(G)$ is also finite.

It remains to consider the basic case of a connected K-group G which, by Proposition 2.9, may also be assumed to be reductive. To do so, let us fix a matrix realization of $G \subset \mathbf{GL}_n$ and the homogeneous space $X = \mathbf{GL}_n/G$. We saw above that the elements of $H^1(K,G)$ are in one-to-one correspondence with the orbits of $GL_n(K)$ on X_K; moreover, proceeding from this interpretation, one can establish the finiteness of real cohomology. Our proof of the finiteness of $Ш(G)$ is based on an analogous interpretation.

LEMMA 6.13. *Let $\pi: \mathbf{GL}_n \to X$ be a canonical projection. Then the elements of $Ш(G)$ are in one-to-one correspondence with the orbits of $GL_n(K)$ on $\pi_A(GL_n(A)) \cap X_K$, where A is the adele ring of K.*

PROOF: For each extension P/K we have a map $\psi_P: X_P \to H^1(P,G)$ whose fibers are in one-to-one correspondence with the orbits of G_P on X_P. Then we may conclude from the commutative diagram

$$\begin{array}{ccc} X_K & \xrightarrow{\psi_K} & H^1(K,G) \\ \downarrow & & \downarrow{\scriptstyle\varrho} \\ \prod_v X_{K_v} & \xrightarrow{\prod_v \psi_{K_v}} & \prod_v H^1(K_v,G) \end{array}$$

that the elements of $Ш(G)$ are in one-to-one correspondence with the orbits of $GL_n(K)$ on $B = (\prod \pi_{K_v}(GL_n(K_v))) \cap X_K$. Therefore it suffices to show that B is the intersection $\pi_A(GL_n(A)) \cap X_K$ given in the statement of the lemma. But this follows easily from the fact that $\pi(GL_n(\mathcal{O}_v)) = X_{\mathcal{O}_v}$ for almost all v in V_f^K, the proof of which is analogous to the proof of Proposition 6.7 and is left to the reader as an exercise. The lemma is proved.

Combining Lemma 6.13 and Theorem 5.3, we obtain the proof of Theorem 6.15.

Theorem 6.15 can also be put in the following, sometimes more convenient, way:

THEOREM 6.19. *Let G be a linear algebraic group defined over a number field K, and let S be a finite subset of V^K. Then the natural map $\varrho_S: H^1(K,G) \to \prod_{v \notin S} H^1(K_v, G)$ is proper, i.e., the inverse image of any finite set is finite.*

Indeed, by the finiteness of local cohomology (Theorem 6.14) everything reduces easily to the case $S = \emptyset$, and it suffices to establish the finiteness of the inverse image of any element under $\varrho = \varrho_\emptyset$. But by twisting, it follows that for any μ in $H^1(K,G)$ the fiber $\varrho^{-1}(\varrho(\mu))$ is covered by $Ш({}_\mu G)$, which is finite by Theorem 6.15.

$Ш(G)$ can be defined not only for a linear algebraic group, but also, for instance, for an abelian variety, where it is an abelian group known as the *Shafarevich-Tate group*. Here, however, the finiteness of $Ш(G)$ is a far more complicated issue. For a long time not a single elliptic curve was known for which Ш could be proven to be finite. Quite recently some progress has been made on this problem by Rubin [1] and Kolyvagin [1], [2], who

established the finiteness of Ш for large families of elliptic curves. (Note that one of the reasons the proof given for Theorem 6.15 does not work for an abelian variety is that in general it cannot be embedded in an algebraic group with trivial cohomology, while for linear groups such an embedding is provided by any matrix realization $G \subset \mathbf{GL}_n$.)

We conclude this section with an example of a semisimple K-group G with $Ш(G)$ nontrivial. Let us begin with an extension L/K, where $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{13}, \sqrt{17})$, for which the Hasse principle does not hold (cf. §6.3, Example 1). Let μ_n denote the algebraic group of the n-th roots of unity, and let us use the construction described in the proof of Proposition 6.7. Namely, take the norm map $N: \mathbf{R}_{L/K}(\mu_n) \to \mu_n$ and let F denote its kernel. (Clearly F is the set of elements of order n in the norm torus $S = \mathbf{R}^{(1)}_{L/K}(\mathbb{G}_m)$.)

The cohomology group of F can be computed from the exact sequence

$$1 \to F \to \mathbf{R}_{L/K}(\mu_n) \to \mu_n \to 1, \tag{6.28}$$

which induces the following commutative diagram with exact rows:

(6.29)
$$\begin{array}{ccccc} H^1(K, \mathbf{R}_{L/K}(\mu_n)) & \xrightarrow{\alpha_1} & H^1(K, \mu_n) & \xrightarrow{\alpha_2} & H^2(K, F) \\ \downarrow{\scriptstyle \gamma_1} & & \downarrow{\scriptstyle \gamma_2} & & \downarrow{\scriptstyle \gamma_3} \\ \prod_v H^1(K_v, \mathbf{R}_{L/K}(\mu_n)) & \xrightarrow{\beta_1} & \prod_v H^1(K_v, \mu_n) & \xrightarrow{\beta_2} & \prod_v H^2(K_v, F) \end{array}$$

Note that

$$H^1(K, \mu_n) = K^*/K^{*n},$$
$$H^1(K, \mathbf{R}_{L/K}(\mu_n)) = H^1(L, \mu_n) = L^*/L^{*n};$$

moreover, α_1 is induced by $N_{L/K}: L^* \to K^*$. It follows that α_2 induces an embedding of $K^*/K^{*n}N_{L/K}(L^*)$ in $H^2(K, F)$. We shall assume that $n = 4l$ and then $K^{*n} \subset N_{L/K}(L^*)$, i.e., we have an embedding of $K^*/N_{L/K}(L^*)$ in $H^2(K, F)$.

Let $x \in K^*/K^{*n}$ be an element whose image in $K^*/N_{L/K}(L^*)$ defines a nontrivial element of $Ш(S) \cong (K^* \cap N_{L/K}(J_L))/N_{L/K}(L^*)$, and let $y = \alpha_2(x)$. Then the definitions and the commutativity of diagram (6.29) yield

LEMMA 6.14. *y in $H^2(K, F)$ is nontrivial and lies in $\operatorname{im}\alpha_2 \cap \ker\gamma_3$.*

Now we can easily complete the construction of our example. Put $\tilde{G} = \mathbf{R}_{L/K}(\mathbf{SL}_n)$. Then $Z(\tilde{G}) = \mathbf{R}_{L/K}(\mu_n)$ and we can consider the embedding

$F \subset Z(\tilde{G})$. Let $G = \tilde{G}/F$. We have the commutative diagram with exact rows

$$\begin{array}{ccccc} H^1(K, \tilde{G}) & \xrightarrow{\delta_1} & H^1(K, G) & \xrightarrow{\delta_2} & H^2(K, F) \\ \downarrow{\scriptstyle \varrho_1} & & \downarrow{\scriptstyle \varrho_2} & & \downarrow{\scriptstyle \varrho_3} \\ \prod_v H^1(K_v, \tilde{G}) & \xrightarrow{\zeta_1} & \prod_v H^1(K_v, G) & \xrightarrow{\zeta_2} & \prod_v H^2(K_v, F) \end{array}.$$

Since $Z(G) = \mathbf{R}_{L/K}(\mu_n)/F \simeq \mu_n$, $H^1(K, Z(G))$ can be identified with K^*/K^{*n}. Viewing x as an element of $H^1(K, Z(G))$, let z be the image of x in $H^1(K, G)$. Then $z \neq 1$, since $\delta_2(z) = y \neq 1$. On the other hand, $\zeta_2(\varrho_2(z)) = 1$ since ϱ_3 is γ_3; and $\varrho_2(z) = 1$ since $H^1(K_v, \tilde{G}) = \prod_{w|v} H^1(L_w, SL_n) = 1$ for any v. Thus, $z \in Ш(G)$, proving $Ш(G) \neq 1$.

As above, the Hasse principle is said to hold for G when $Ш(G) = 1$. Thus, the above example can be viewed as a counterexample to the Hasse principle for semisimple groups. The objective of the sections that follow is to show that the Hasse principle always holds in the extreme cases of simply connected groups and adjoint groups.

6.5. Cohomology of semisimple algebraic groups over local fields and number fields.

As we mentioned in §6.1, the basic cohomological results for a simply connected semisimple K-group G are: $H^1(K, G) = 1$ if K is a non-Archimedean local field (Theorem 6.4), and $H^1(K, G)$ is isomorphic to $\prod_{v \in V_\infty^K} H^1(K_v, G)$ if K is a number field (Theorem 6.6). Sections 6.7 and 6.8 are devoted to the proofs of these deep theorems. In this section, assuming these results, we shall learn how to compute the cohomology of any semisimple group and shall obtain some applications of these results (in particular, we shall establish the validity of the Hasse principle for adjoint groups and shall prove that groups of types B_n, C_n, E_7, E_8, F_4, G_2 over a number field K are split over a suitable quadratic extension L/K). In the next section, using these results, we shall obtain a local-global classification of various types of sesquilinear forms and shall prove Theorem 6.5, that any anisotropic group over a local field is of type $\mathbf{SL}_1(D)$ and the analogous assertion over a totally imaginary number field.

Computation of the cohomology of a nonsimply connected semisimple K-group G is based on a universal K-covering $1 \to F \to \tilde{G} \xrightarrow{\pi} G \to 1$ and the corresponding exact cohomological sequence

$$H^1(K, \tilde{G}) \to H^1(K, G) \xrightarrow{\delta} H^2(K, F).$$

The basic result, which, together with Theorems 6.4, 6.6 and 6.18, enables us to compute $H^1(K,G)$ is as follows:

THEOREM 6.20. *If K is a non-Archimedean local field or a number field, then δ is surjective.*

COROLLARY. *If K is a local field, then δ is bijective.*

Indeed, it follows from Theorem 6.4 that $H^1(K,{}_\xi\tilde{G}) = 1$ for any ξ in $Z^1(K,G)$; hence δ is injective.

The proof of Theorem 6.20 is based on the following result, which is interesting in its own right.

THEOREM 6.21. *Let G be a semisimple algebraic group over a non-Archimedean local field K. Then G contains a maximal K-torus S, which is anisotropic over K.*

Before proving Theorem 6.21, let us note that it does not hold over $K = \mathbb{R}$. Indeed, consider the quadratic form

$$f(x_1,\dots,x_6) = g(x_1,x_2,x_3) - g(x_4,x_5,x_6),$$

where $g(x,y,z) = x^2+y^2+z^2$. Then the maximal compact subgroup of $G_{\mathbb{R}} = \mathbf{SO}_6(f)$ has the form $\mathbf{SO}_3(g)\times\mathbf{SO}_3(g)$, i.e., is a group of rank 2. Hence, since G has rank 3, it does not contain a 3-dimensional $\mathbb{R}$-anisotropic torus.

PROOF OF THEOREM 6.21: We use the cohomological characterization of all possible K-tori of G. Assuming G adjoint (which may always be done in the proof of this theorem), we fix a maximal K-torus T of G and take its normalizer $N = N_G(T)$. Let T' be another maximal K-torus of G. Then $T' = gTg^{-1}$ for suitable g in $G_{\bar K}$. Since T and T' are defined over K it follows that the cocycle $\xi = \{\xi_\sigma\}$, where $\xi_\sigma = g^{-1}\sigma(g)$ for σ in $\mathrm{Gal}(\bar K/K)$, takes on values in N and determines an element of $M = \ker(H^1(K,N)\to H^1(K,G))$. In this regard, T' is obtained from T by twisting with ξ, where N acts on T by conjugation. Conversely, for any ξ in $Z^1(K,N)$ the twisted torus ${}_\xi T$ is a maximal K-torus of ${}_\xi G$. Therefore ${}_\xi T$ will obviously be a maximal K-torus of G if ${}_\xi G = G$, i.e., $\xi\in M$. In this way the proof reduces to finding ξ in M such that ${}_\xi T$ is K-anisotropic.

Let $W = N/T$ be the corresponding Weyl group. Viewing W as a subgroup of $\mathrm{Aut}_{\bar K}(T)$, the group of all automorphisms of T, we can define ${}_\xi T$ for any ξ in $Z^1(K,W)$.

LEMMA 6.15. *There is a cocycle ξ in $Z^1(K,W)$ for which ${}_\xi T$ is anisotropic over K.*

PROOF: First we reduce the proof to the quasisplit case. Let G_0 be a quasisplit K-group of the same inner type as G, let $T_0\subset G_0$ be a maximal K-torus containing a maximal K-split torus, and let $f: G\to G_0$ be a $\bar K$-isomorphism such that $f(T) = T_0$. Then the cocycle $\alpha = \{\alpha_\sigma\}$, where $\alpha_\sigma = f^{-1}\circ\sigma(f)$ for $\sigma\in\mathrm{Gal}(\bar K/K)$ with values in $\mathrm{Int}\,G\simeq G$, actually assumes values in N. Clearly $G_0 = {}_\alpha G$, $T_0 = {}_\alpha T$ and $W_0 = {}_\beta W$, where β is the image of α in $Z^1(K,W)$. This being the case, the properties of twisting imply that "multiplication" by β induces a bijection $Z^1(K,W_0)\simeq Z^1(K,W)$ and the set of tori obtained from T_0 by twisting with cocycles from $Z^1(K,W_0)$ coincides with the set of tori obtained from T by twisting with cocycles from $Z^1(K,W)$; this observation yields the desired reduction.

Now we take the case where G is split and T is a maximal K-split torus. Then $\mathcal{G} = \mathrm{Gal}(\bar K/K)$ acts on $\mathbf{X}(T)$ and W trivially; in particular, the cocycles in $Z^1(K,W)$ are simply the (continuous) homomorphisms $\xi:\mathcal{G}\to W$. We shall interpret $\mathbf{X}({}_\xi T)$ as the group of characters $\mathbf{X}(T)$, on which an element σ in $\mathcal{G}$ acts as the automorphism ξ^*_σ of $\mathbf{X}(T)$ corresponding to ξ_σ. Thus, it suffices to construct a cocycle $\xi = \{\xi_\sigma\}$ such that all the ξ^*_σ have no nonzero fixed points on $\mathbf{X}(T)$. (Then $\mathbf{X}({}_\xi T)^{\mathcal{G}} = 0$, so ${}_\xi T$ is K-anisotropic.) To do so, take a system $\Pi = \{\alpha_1,\dots,\alpha_r\}$ of simple roots in the root system $R = R(T,G)$ and construct the Coxeter element $w = w_{\alpha_1}\dots w_{\alpha_r}$ where w_{α_i} is the reflection associated to α_i; it is well known (cf. Bourbaki [4, Ch. 5, §6]) that w has no nonzero fixed points on $\mathbf{X}(T)$. Let d be the order of w (the Coxeter number of R), let L/K be an unramified extension of degree d, and let $\mathrm{Gal}(L/K) = \langle\sigma\rangle$. Then the desired cocycle ξ in $Z^1(L/K,W)$ is given by $\xi_{\sigma^i} = w^i$.

In analyzing the case of a quasisplit but not split group, let L/K denote a Galois extension whose Galois group acts faithfully on the Dynkin diagram of R. For types ${}^2A_n$, ${}^2D_{2n+1}$, ${}^2E_6$ this L is a quadratic extension of K. Let σ be a generator of $\mathrm{Gal}(L/K)$. By the fact that for groups of these types $-1\notin W$ and at the same time $\sigma^*\notin W$ (where σ^* denotes the action of σ on $\mathbf{X}(T)$), we can define ξ in $Z^1(L/K,W)$ by $\xi^*_\sigma = -\sigma^*$. Then σ acts on $\mathbf{X}({}_\xi T)$ as $\xi^*_\sigma\circ\sigma^* = -1$, and consequently it has no nonzero fixed points.

For the remaining type D_{2n} (including ${}^3D_4$, ${}^6D_4$) we construct a quadratic extension P/K such that $P\cap L = K$ (this is always possible, since K has at least two quadratic extensions, and $\mathrm{Gal}(L/K)$ is isomorphic to a subgroup of S_3), and let $\mathrm{Gal}(P/K) = \langle\sigma\rangle$. It is easy to see that the desired cocycle will be $\xi\in Z^1(P/K,W)$ such that $\xi_\sigma = -1$ (here $-1\in W$). The lemma is proved.

In view of Lemma 6.15, the proof of Theorem 6.21 reduces to proving the following: let $\varrho: H^1(K,N)\to H^1(K,W)$ be the canonical projection; then there exists θ in $\ker(H^1(K,N)\xrightarrow{\tau}H^1(K,G))$ satisfying $\varrho(\theta) = \xi$. For

this, let us consider the universal covering $1 \to F \to \tilde{G} \xrightarrow{\pi} G \to 1$ and the corresponding coboundary morphism $\delta: H^1(K,G) \to H^2(K,F)$, and construct the following commutative diagram

$$\begin{array}{ccccc} H^1(K,\tilde{G}) & \longrightarrow & H^1(K,G) & \xrightarrow{\delta} & H^2(K,F) \\ & & \uparrow{\scriptstyle \tau} & & \| \\ & & H^1(K,N) & \xrightarrow{\delta} & H^2(K,F). \end{array}$$

Since $H^1(K,\tilde{G}) = 1$ (Theorem 6.4), it suffices to establish that there exists θ in $\varrho^{-1}(\xi)$ such that $\delta(\theta) = 1$. Thus, the proof is completed by

LEMMA 6.16. *Let ξ in $Z^1(K,W)$ be a cocycle such that ${}_\xi T$ is anisotropic. Then δ maps $\varrho^{-1}(\xi)$ onto $H^2(K,F)$.*

PROOF: Since ${}_\xi T$ is anisotropic over K, Theorem 6.2 implies that

$$H^2(L/K, {}_\xi T) = \hat{H}^0(L/K, \mathbf{X}({}_\xi T)) = 0$$

for any finite extension L of K containing a splitting field of ${}_\xi T$; hence $H^2(K, {}_\xi T) = 1$. Therefore, passing to cohomology in the exact sequence $1 \to T \to N \to W \to 1$, we see that ξ lies in the image of $\varrho: H^1(K,N) \to H^1(K,W)$, i.e., $\varrho^{-1}(\xi) \neq \emptyset$. Let $\theta \in \varrho^{-1}(\xi)$, and consider the twisted groups ${}_\theta N$, ${}_\theta T = {}_\xi T$, and ${}_\xi W$. It follows from the twisting argument that the assertion of the lemma is equivalent to the surjectivity of

$$\delta: \ker(H^1(K, {}_\theta N) \xrightarrow{\varrho'} H^1(K, {}_\xi W)) \to H^2(K,F).$$

(Clearly ${}_\theta F = F$ and therefore we use the same letter to denote the coboundary morphism.) We have the commutative diagram with exact upper row:

$$\begin{array}{ccccc} H^1(K, {}_\theta T) & \longrightarrow & H^1(K, {}_\theta N) & \xrightarrow{\varrho'} & H^1(K, {}_\xi W) \\ \downarrow{\scriptstyle \delta} & & \downarrow{\scriptstyle \delta} & & \\ H^2(K,F) & = & H^2(K,F) & & \end{array}$$

Clearly, it suffices to establish that $H^1(K, {}_\theta T) \xrightarrow{\delta} H^2(K,F)$ is surjective. But this follows from the exact sequence

$$H^1(K, {}_\theta T) \to H^2(K,F) \to H^2(K, {}_\theta \tilde{T}),$$

where $\tilde{T} = \pi^{-1}(T)$; indeed ${}_\theta \tilde{T}$, as well as ${}_\theta T$, is K-anisotropic, and consequently $H^2(K, {}_\theta \tilde{T}) = 1$. The lemma is proved.

PROOF OF THEOREM 6.20 (FOR A LOCAL FIELD): Let S be a maximal K-anisotropic torus of G, the existence of which is given by Theorem 6.21, and let $\tilde{S} = \pi^{-1}(S)$. The commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & F & \longrightarrow & \tilde{G} & \longrightarrow & G & \longrightarrow & 1 \\ & & \| & & \uparrow & & \uparrow & & \\ 1 & \longrightarrow & F & \longrightarrow & \tilde{S} & \longrightarrow & S & \longrightarrow & 1 \end{array}$$

induces the commutative cohomological diagram

$$\begin{array}{ccccc} H^1(K,S) & \xrightarrow{\delta} & H^2(K,F) & \longrightarrow & H^2(K,\tilde{S}) \\ \downarrow & & \| & & \\ H^1(K,G) & \xrightarrow{\delta} & H^2(K,F) & & \end{array}$$

Since $\tilde{S}$, as well as S, is K-anisotropic, we have $H^2(K,\tilde{S}) = 1$, and hence the map $\delta: H^1(K,S) \to H^2(K,F)$ is surjective. Consequently, $\delta: H^1(K,G) \to H^2(K,F)$ is surjective.

To analyze the case of a number field, we need several additional assertions.

LEMMA 6.17. *Let G be a semisimple algebraic group defined over an arbitrary field K of characteristic 0 and containing a Borel subgroup over a quadratic extension L/K, and let σ be a generator of $\mathrm{Gal}(L/K)$. Then there exists a Borel L-subgroup B of G such that $B \cap B^\sigma$ is a maximal K-torus of G.*

PROOF: Consider the K-variety $\mathcal{B}$ of Borel subgroups of G (cf. §2.4.6), and put $H = \mathbf{R}_{L/K}(G)$, $X = \mathbf{R}_{L/K}(\mathcal{B})$. Over L, we can identify X with the direct product $\mathcal{B} \times \mathcal{B}$; moreover, the elements of X_K correspond to pairs of the form (B, B^σ), where $B \in \mathcal{B}_L$. Then $X_K \neq \emptyset$ since $\mathcal{B}_L \neq \emptyset$ by assumption. On the other hand, X is the variety of Borel subgroups of H; in particular, it is a homogeneous space of H. Since H_K is dense in H (Theorem 2.2), it follows that X_K is dense in X.

Now we show that the subset U of X, consisting of pairs (B_1, B_2) such that $B_1 \cap B_2$ is a maximal torus of G, contains an open subset of X. Then $U \cap X_K$ is nonempty, and any of its elements having the form (B, B^σ) clearly provides the desired Borel subgroup B.

To prove that U contains an open subset, we take the subvariety $Y \subset G \times \mathcal{B} \times \mathcal{B}$ consisting of points (g, b_1, b_2) such that $gb_1 = b_1$, $gb_2 = b_2$, and show that U can be characterized as the set of those y in $\mathcal{B} \times \mathcal{B}$ for which the fiber $\pi^{-1}(y)$ of the natural projection $\pi: Y \to \mathcal{B} \times \mathcal{B}$ has minimal dimension; the necessary result will then follow from the theorem on the dimension of the fibers of a morphism. If $y = (b_1, b_2) \in \mathcal{B} \times \mathcal{B}$ then $\pi^{-1}(y) = (B_1 \cap B_2, b_1, b_2)$, where B_i is the Borel subgroup of G corresponding to b_i. But it is well known (cf. corollary to Theorem 2.5) that $B_1 \cap B_2$ always contains a maximal torus T of G; therefore if $\dim \pi^{-1}(y)$ is minimal, then the connected component $(B_1 \cap B_2)^0$ is a torus. On the other hand, writing $B_1 = TU_1$ as a semidirect product yields $B_1 \cap B_2 = T(U_1 \cap B_2)$. Here $U_1 \cap B_2$ is unipotent and therefore is connected; hence $B_1 \cap B_2$ is also connected. The lemma is proved.

LEMMA 6.18. *Let G be a simply connected semisimple algebraic group over $\mathbb{R}$. Then there exists a maximal $\mathbb{R}$-torus T of G such that $H^2(\mathbb{R}, T) = 1$.*

PROOF: Using Lemma 6.17, we choose a Borel $\mathbb{C}$-subgroup B of G such that $T = B \cap B^\sigma$ is a maximal $\mathbb{R}$-torus of G, where σ denotes complex conjugation. Our objective is to show that $H^2(\mathbb{R}, T) = 1$. To do so, let us consider the root system $R = R(T, G)$ and fix a system of simple roots $\Pi \subset R$ associated with B (cf. §2.1.10). Since G is simply connected, the group $\mathbf{X}_*(T)$ of cocharacters of T has a base $\Pi^\vee$ consisting of the dual roots $\alpha^\vee$ for α in Π. Since $B \cap B^\sigma$ is T, B^σ is the opposite of B, and hence $\sigma^*(\Pi) = -\Pi$, $\sigma^*(\Pi^\vee) = -\Pi^\vee$ (where σ^* denotes the induced action of σ on characters and cocharacters). Thus for $\alpha^\vee \in \Pi^\vee$ we have either $\sigma^*(\alpha^\vee) = -\alpha^\vee$ or $\sigma^*(\alpha^\vee) = -\beta^\vee$ for some $\beta^\vee \neq \alpha^\vee$ in $\Pi^\vee$. With these properties of the base of $\mathbf{X}_*(T)$ it is easy to obtain that $\hat{H}^0(\mathbb{R}, \mathbf{X}_*(T)) = 0$. But then, by the Nakayama-Tate theorem, it follows that $H^2(\mathbb{R}, T) = 1$. The lemma is proved.

PROOF OF THEOREM 6.20 (FOR A NUMBER FIELD): First we establish that, for almost all v in V_f^K, the image $\varrho_v(x)$ of a given element x in $H^2(K, F)$ under the restriction map $\varrho_v: H^2(K, F) \to H^2(K_v, F)$ is trivial. Indeed, x lies in the image of the inflation map $H^2(L/K, F) \to H^2(K, F)$, where L/K is a suitable finite extension of K. Then L_w/K_v is unramified for almost all v in V_f^K, and thus $\varrho_v(x)$ falls in the image of the inflation map $H^2(K_v^{ur}/K_v, F) \to H^2(K_v, F)$. But $H^2(K_v^{ur}/K_v, F) = 1$, since $\mathrm{Gal}(K_v^{ur}/K_v) \simeq \hat{\mathbb{Z}}$ is the group of cohomological dimension L; therefore $\varrho_v(x) = 1$, as desired.

Now fix x in $H^2(K, F)$ and let S be a finite subset of V^K containing at least one non-Archimedean valuation and all those v for which $\varrho_v(x) \neq 1$. For each v in S we can find a maximal K_v-torus $\tilde{T}_v$ of $\tilde{G}$ such that $H^2(K_v, \tilde{T}_v) = 1$. Indeed, if v is non-Archimedean, it suffices to take a maximal K_v-anisotropic torus $\tilde{T}_v$ of $\tilde{G}$ (cf. Theorem 6.21), and if v is Archimedean one uses Lemma 6.18. By the weak approximation property for varieties of tori (cf. §7.1, Corollary 3) we obtain a K-torus $\tilde{T}$ of $\tilde{G}$ which over K_v is isomorphic to $\tilde{T}_v$. (Note that the proof in Chapter 7 of the existence of such a torus does not rely on any results from Chapter 6.) Put $T = \pi(\tilde{T})$. Clearly it suffices to show that x lies in the image of the coboundary morphism $\delta: H^1(K, T) \to H^2(K, F)$ corresponding to the exact sequence

$$1 \to F \to \tilde{T} \to T \to 1.$$

We have the commutative diagram with exact rows

$$\begin{array}{ccccc} H^1(K,T) & \xrightarrow{\delta} & H^2(K,F) & \xrightarrow{\tau} & H^2(K,\tilde{T}) \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \varrho} & & \downarrow{\scriptstyle \gamma} \\ \prod_v H^1(K_v,T) & \xrightarrow{\mu} & \prod_v H^2(K_v,F) & \xrightarrow{\eta} & \prod_v H^2(K_v,\tilde{T}) \end{array}$$

Since $x \in \mathrm{im}\,\delta$ and $x \in \ker \tau$ are equivalent conditions, we shall verify the latter. We have $\gamma(\tau(x)) = \eta(\varrho(x)) = 1$, since by assumption $H^2(K_v, \tilde{T}) = 1$ for those v for which $\varrho_v(x) \neq 1$. But S contains a non-Archimedean valuation v_0 and $\tilde{T}$ is K_{v_0}-anisotropic; it follows from Proposition 6.13 that $\ker \gamma$ is trivial; therefore $\tau(x) = 1$. Q.E.D.

Note that Theorem 6.20 includes some essential arithmetic results. Thus, for $G = \mathbf{PSL}_n$, the fundamental group F is the group μ_n of the n-th roots of unity. Then, by Lemma 2.6, $H^2(K, F) = \mathrm{Br}(K)_n$ is the subgroup of elements of $\mathrm{Br}(K)$ which are annihilated under multiplication by n. However, it is easy to see that the image of $H^1(K, G) \xrightarrow{\delta} H^2(K, F)$ consists of the elements of $\mathrm{Br}(K)_n$ represented by simple n^2-dimensional algebras. Therefore, the assertion on the surjectivity of δ for local fields and number fields is actually equivalent to the deep assertion that over these fields the exponent of a simple algebra equals its index (cf. §1.4.1).

For what follows we shall need an explicit computation of the cohomology of the centers of simply connected groups. Clearly the structure of the center as a module over the Galois group is the same for all groups of the same inner type; and, for simple groups we have the following table, where L/K denotes a Galois extension of K, whose Galois group acts effectively on the corresponding Dynkin diagram:

Type of G	$Z(G)$	Type of G	$Z(G)$
${}_1A_{n-1}$	μ_n	${}^3D_4$	$\mathbf{R}^{(1)}_{L/K}(\mu_2)$
${}^2A_{n-1}$	$\mathbf{R}^{(1)}_{L/K}(\mu_n)$	${}^6D_4$	$\mathbf{R}^{(1)}_{P/K}(\mu_2)$
B_n, C_n, E_7	μ_2	${}^1E_6$	μ_3
${}^1D_n$	μ_4, $n=2k+1$ $\mu_2\times\mu_2$, $n=2k$	${}^2E_6$	$\mathbf{R}^{(1)}_{L/K}(\mu_3)$
${}^2D_n$	$\mathbf{R}^{(1)}(\mu_4)$, $n=2k+1$ $\mathbf{R}_{L/K}(\mu_2)$, $n=2k$	E_8, F_4, G_2	1

(Here, for type ${}^6D_4$, P denotes a subfield of L having degree 3 over K.)

We are already familiar with the cohomology of μ_n (Lemma 2.6):

$$H^1(K,\mu_n)=K^*/K^{*n},\qquad H^2(K,\mu_n)=\mathrm{Br}(K)_n.$$

The cohomology of $\mathbf{R}^{(1)}_{L/K}(\mu_n)$ is computed starting from the exact sequence $1\to\mathbf{R}^{(1)}_{L/K}(\mu_n)\to\mathbf{R}_{L/K}(\mu_n)\xrightarrow{N}\mu_n\to 1$. Passing to cohomology, we obtain the exact sequence

$$\begin{aligned}\mathbf{R}_{L/K}(\mu_n)_K &\xrightarrow{N}(\mu_n)_K\\ &\to H^1(K,\mathbf{R}^{(1)}_{L/K}(\mu_n))\\ &\to H^1(K,\mathbf{R}_{L/K}(\mu_n))\to H^1(K,\mu_n)\\ &\to H^2(K,\mathbf{R}^{(1)}_{L/K}(\mu_n))\to H^2(K,\mathbf{R}_{L/K}(\mu_n))\to H^2(K,\mu_n).\end{aligned}$$

Thus the $H^i(K,\mathbf{R}^{(1)}_{L/K}(\mu_n))$ $(i=1,2)$ enter into the exact sequences

$$\begin{aligned}1\to(\mu_n)_K/N_{L/K}((\mu_n)_L)\to &H^1(K,\mathbf{R}^{(1)}_{L/K}(\mu_n))\\ &\to\ker(L^*/L^{*n}\xrightarrow{N}K^*/K^{*n})\to 1\end{aligned}\tag{6.30}$$

and

$$\begin{aligned}1\to K^*/K^{*n}N_{L/K}(L^*)\to &H^2(K,\mathbf{R}^{(1)}_{L/K}(\mu_n))\\ &\to\ker(\mathrm{Br}(L)_n\xrightarrow{N}\mathrm{Br}(K)_n)\to 1.\end{aligned}\tag{6.31}$$

Using (6.31) we can compute explicitly $H^2(K,Z)$, where Z is the center of a simply connected group of one of the types ${}^{3,6}D_4$, ${}^2E_6$, i.e., when $Z=\mathbf{R}^{(1)}_{L/K}(\mu_2)$, $\mathbf{R}^{(1)}_{P/K}(\mu_2)$, or $\mathbf{R}^{(1)}_{L/K}(\mu_3)$, notation as in the table above.

Note that if n is prime to the degree of L/K then $K^*=K^{*n}N_{L/K}(L^*)$, and therefore the corresponding term in (6.31) is trivial. (This is exactly so in the cases under consideration.)

Now we shall show that for K a local field, $B=\ker(\mathrm{Br}(L)_n\xrightarrow{N}\mathrm{Br}(K)_n)$ is trivial. First we analyze the case of types ${}^{3,6}D_4$, i.e., when $Z=\mathbf{R}^{(1)}_{L/K}(\mu_2)$, where L/K is any extension of degree 3, and show that in this case $\mathrm{Br}(L)_2\xrightarrow{N}\mathrm{Br}(K)_2$ is an isomorphism. The composite map

$$\mathrm{Br}(K)_2\xrightarrow{i}\mathrm{Br}(L)_2\xrightarrow{N}\mathrm{Br}(K)_2,$$

where i is induced by extension of the base field, is multiplication by 3, and therefore is the identity map. Since $|\mathrm{Br}(K)_2|=|\mathrm{Br}(L)_2|=2$, i is an isomorphism; hence N is also an isomorphism, as desired.

Now take the case of a group of type ${}^2E_6$, i.e., $Z=\mathbf{R}^{(1)}_{L/K}(\mu_3)$, where L/K is a quadratic extension. The elements of B correspond to those classes of simple algebras over L of exponent 3, which have involution τ of second kind such that the field of fixed elements L^τ is K. It is well known (cf. Albert [1, Ch. 10]), that there are no nontrivial simple algebras with involution of second kind over local fields, and therefore in the given case again $B=1$. Thus, over local fields $H^2(K,Z)=1$ for the types under consideration.

Now let K be a number field. We shall show that here, for any x in $H^2(K,Z)$, there is an extension E/K of degree 2 for types ${}^{3,6}D_4$ and of degree 3 for ${}^2E_6$, such that the image of x under the restriction map $H^2(K,Z)\to H^2(E,Z)$ is trivial. Consider an element y in B corresponding to x, and let D in $\mathrm{Br}(L)$ be the division algebra representing this element. Let $\bar S$ denote the finite subset of V^L consisting of those w for which $D_w=D\otimes_L L_w$ is nontrivial, and let S consist of the restrictions of the valuations from $\bar S$ to K.

First consider the groups of type ${}^{3,6}D_4$. Then $[L:K]=3$ and therefore $[L_w:K_v]\le 3$ for any v in V^K. Hence it follows easily that there exists a quadratic extension E/K such that $[EL_w:L_w]=2$ for all w in $\bar S$. Then §1.5.1 implies that EL is a splitting field for D and therefore E is the desired extension.

For type ${}^2E_6$, D is an algebra over L with involution of second type; so by the absence of such algebras over local fields it follows that $L\subset K_v$ for v in S. It is easy to see that there exists a cubic extension $E=K(\sqrt[3]{d})$ satisfying $[E_w:K_v]=3$ for all v in S. Then, as above, we conclude that E is the desired extension. Moreover, using the Grünwald-Wang theorem from class field theory (cf. Artin-Tate [1]), one can show that there always exists a cyclic extension of K of degree 3 satisfying this property.

Let us gather the results just obtained.

PROPOSITION 6.14. *Let Z be the center of a simply connected simple K-group of type ${}^3D_4$, ${}^6D_4$, or ${}^2E_6$. Then*

(1) *$H^2(K, Z) = 1$ if K is a local field;*
(2) *if K is a number field, then for any x in $H^2(K, Z)$ there is an extension E/K having degree 2 for types ${}^{3,6}D_4$ and degree 3 for type ${}^2E_6$, such that the image of x under the restriction map $H^2(K, Z) \to H^2(E, Z)$ is trivial (moreover, for type ${}^2E_6$ one can choose a cyclic extension E/K of degree 3 having this property).*

Now we show how Proposition 6.14 can be applied to elucidate the structure of groups of the types mentioned. Let G_0 be the corresponding simply connected quasisplit group, let $Z = Z(G_0)$ be its center, and let $\bar{G}_0 = G_0/Z$ be the adjoint group. Then the elements of $H^1(K, \bar{G}_0)$ classify the simply connected simple groups belonging to the same inner type as G_0, up to K-isomorphism. In particular, the group $G = {}_\xi G_0$ corresponding to ξ in $H^1(K, \bar{G}_0)$, is quasisplit over K if and only if ξ is trivial, and becomes quasisplit over an extension E of K if the image of ξ under the restriction map $H^1(K, \bar{G}_0) \to H^1(E, \bar{G}_0)$ is trivial. $H^1(K, \bar{G}_0)$ is a term in the exact sequence

$$H^1(K, G_0) \to H^1(K, \bar{G}_0) \xrightarrow{\delta} H^2(K, Z).$$

Now assume K is a local field and $H^1(K, G_0)$ is trivial (we deliberately are not using Theorem 6.4 to its fullest extent). Then the kernel of δ is trivial. On the other hand, $H^2(K, Z) = 1$ by Proposition 6.14 (1). Therefore $H^1(K, \bar{G}_0) = 1$, which means that any group of one of the types ${}^{3,6}D_4$, ${}^2E_6$ is quasisplit over K.

Now let K be a number field. Assume $H^1(P, G_0)$ is known to be trivial for any totally imaginary extension P/K (again, we are not using Theorem 6.6 fully). Then, noting that for E in Proposition 6.14 (2) we can choose a totally imaginary extension for types ${}^{3,6}D_4$, we arrive at the following

PROPOSITION 6.15. *Let G_0 be a simply connected quasisplit group of type ${}^3D_4$, ${}^6D_4$, or ${}^2E_6$ over a non-Archimedean local field or number field K. Assume for K a local field that $H^1(K, G_0)$ is known to be trivial, or for K a number field that $H^1(P, G_0)$ is known to be trivial for each totally imaginary extension of K. Then*

(1) *for K a local field, any K-group belonging to one of the above types is quasisplit;*
(2) *for K a number field, any K-group belonging to type ${}^3D_4$ or ${}^6D_4$ becomes quasisplit over a quadratic extension of K;*
(3) *for K a totally imaginary number field, any K-group of type ${}^2E_6$ becomes quasisplit over some (cyclic) extension of K of degree 3.*

Next we establish an important structural result which will play a key role in §9.4 in studying the normal structure of groups of rational points.

PROPOSITION 6.16. *Let G_0 be a simply connected split group of type B_n, C_n, E_7, E_8, F_4, or G_2 over a non-Archimedean local field or a number field K. Assume for K a local field that $H^1(K, G_0)$ is known to be trivial, and for K a number field that $H^1(P, G_0)$ is trivial for any totally imaginary extension P of K. Then*

(1) *any K-group of type E_8, F_4, or G_2 is K-split if K is a local field, and split over every totally imaginary extension of K if K is a number field;*
(2) *any K-group of type B_n, C_n, or E_7 is split over a suitable totally imaginary quadratic extension L/K which we may assume to be totally imaginary in the number field case.*

In particular, any group belonging to one of the types mentioned in the proposition is split over a suitable quadratic extension L/K.

PROOF: The Dynkin diagrams of the above-mentioned groups do not have any nontrivial symmetries; therefore their K-forms are classified by the elements of $H^1(K, \bar{G}_0)$, where $\bar{G}_0$ is the corresponding adjoint group. Since $G_0 = \bar{G}_0$ for the types in (1), the desired assertion follows easily. For groups of the remaining types, $Z(G_0) = \mu_2$, so $H^2(K, Z) = \mathrm{Br}(K)_2$; thus any x in $H^2(K, Z)$ becomes trivial over some quadratic extension L/K, which in the case of a number field we can assume is totally imaginary. Then the exact sequence

$$H^1(L, G_0) \to H^1(L, \bar{G}_0) \to H^2(L, Z)$$

yields the desired assertion.

The reader might be perplexed by the seeming inconsistency of Propositions 6.15 and 6.16, in that throughout this section we have assumed Theorems 6.4 and 6.6 to hold, whereas in these two propositions, for some reason, we restricted ourselves to the weaker assumption that $H^1(K, G_0)$ be trivial for a quasisplit group G_0 over a local or totally imaginary number field K. This is because Propositions 6.15 and 6.16 are actually intertwined in the complicated scheme of the proofs of Theorems 6.4 and 6.6, and will be used in precisely the situation described in their formulation. Needless to say, after Theorems 6.4 and 6.6 are proved, Propositions 6.15 and 6.16 turn from conditional statements to unconditional ones.

Now we return to our discussion of the Hasse principle for semisimple groups. In the preceding section we saw that it does not always hold; however, Theorem 6.6 claims it to hold for simply connected groups. We shall show that it also holds for another special case—adjoint groups.

THEOREM 6.22. *Let G be a semisimple adjoint group over a number field K. Then $Ш(G) = 1$.*

PROOF: Clearly it suffices to consider the case when G is simple. Let $\pi: \tilde{G} \to G$ denote the universal covering, and let $Z = \ker \pi$. We have the following commutative diagram with exact rows:

(6.32)

$$\begin{array}{ccccccc} H^1(K,Z) & \xrightarrow{\alpha_1} & H^1(K,\tilde{G}) & \xrightarrow{\alpha_2} & H^1(K,G) & \xrightarrow{\alpha_3} & H^2(K,Z) \\ \downarrow{\scriptstyle \gamma_1} & & \downarrow{\scriptstyle \gamma_2} & & \downarrow{\scriptstyle \gamma_3} & & \downarrow{\scriptstyle \gamma_4} \\ \prod_v H^1(K_v,Z) & \xrightarrow{\beta_1} & \prod_v H^1(K_v,\tilde{G}) & \xrightarrow{\beta_2} & \prod_v H^1(K_v,G) & \xrightarrow{\beta_3} & \prod_v H^2(K_v,Z) \end{array}$$

LEMMA 6.19. $\ker \gamma_4 = 1$.

PROOF: If $Z = \mu_n$ then γ_4 is the canonical map $\mathrm{Br}(K)_n \to \prod_v \mathrm{Br}(K_v)_n$, which is injective by the Hasse-Brauer-Noether theorem (cf. Theorem 1.12, §1.5). Now let $Z = \mathbf{R}^{(1)}_{L/K}(\mu_n)$. Then (6.31) yields the following commutative diagram with exact rows:

$$\begin{array}{ccccc} 1 & \longrightarrow & K^*/K^{*n}N_{L/K}(L^*) & \xrightarrow{\varepsilon_1} & H^2(K,Z) \\ & & \downarrow{\scriptstyle \eta_1} & & \downarrow{\scriptstyle \eta_2 = \gamma_4} \\ 1 & \longrightarrow & \prod_v K_v^*/K_v^{*n}N_{L/K}((L\otimes_K K_v)^*) & \xrightarrow{\theta_1} & \prod_v H^2(K_v,Z) \end{array}$$

$$\begin{array}{ccccc} & \xrightarrow{\varepsilon_2} & \ker(\mathrm{Br}(L) \xrightarrow{N_{L/K}} \mathrm{Br}(K)) & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \eta_3} & & \\ & \xrightarrow{\theta_2} & \prod_v \ker(\sum_{w|v} \mathrm{Br}(L_w) \xrightarrow{N_{L/K}} \mathrm{Br}(K_v)) & \longrightarrow & 1 \end{array}$$

Again, $\ker \eta_3 = 1$ by the Hasse-Brauer-Noether theorem. It follows that if $x \in \ker \eta_2$ then $x = \varepsilon_1(y)$ for some $y \in \ker \eta_1$. Therefore it remains to show that in our case $\ker \eta_1 = 1$. First let L/K be a quadratic extension. Then, for n odd $K^*/K^{*n}N_{L/K}(L^*)$ is trivial, and there is nothing to prove. On the other hand, for n even, $K^{*n} \subset N_{L/K}(L^*)$, so η_1 reduces to $K^*/N_{L/K}(L^*) \to \prod_v K_v^*/N_{L/K}((L\otimes_K K_v)^*)$, which is injective, since the Hasse norm principle holds for L/K (cf. Corollary to Theorem 6.11). From the table above, we see that it remains to consider the case $n = 2$ for L/K an extension of degree 3. But then again $K^*/K^{*n}N_{L/K}(L^*) = 1$, and the proof of Lemma 6.19 is complete.

Now let $x \in \ker \gamma_3$, notation as in (6.32). Then $\alpha_3(x) \in \ker \gamma_4$, so $\alpha_3(x)$ is trivial by Lemma 6.19. Since the top row of (6.32) is exact, it follows that $x \in \mathrm{im}\,\alpha_2$, i.e., $x = \alpha_2(y)$ for y in $H^1(K,\tilde{G})$. Consider $\gamma_2(y)$. From the exactness of the bottom row of (6.32), its commutativity, and the stipulation that $x \in \ker \gamma_3$, it is easy to see that $\gamma_2(y) \in \mathrm{im}\,\beta_1$, i.e., $\gamma_2(y) = \beta_1(z)$, $z = (z_v) \in \prod_v H^1(K_v,Z)$. Now we use the fact that $H^1(K,Z) \xrightarrow{\psi} \prod_{v\in V_\infty^K} H^1(K_v,Z)$ is surjective (cf. Proposition 7.7, Corollary 2; of course the proof of this assertion from Chapter 7 does not depend on Theorem 6.22). Then we can choose a in $H^1(K,Z)$ satisfying $\varphi(a) = (z_v)_{v\in V_\infty^K}$. Since $H^1(K_v,\tilde{G})$ is trivial for v in V_f^K (Theorem 6.4), by our construction it follows that $\gamma_2(\alpha_1(a)) = \gamma_2(y)$. But then, applying Theorem 6.6 (the Hasse principle for $\tilde{G}$), we get $y = \alpha_1(a)$, and hence $x = \alpha_2(y) = \alpha_2(\alpha_1(a)) = 1$. Q.E.D.

REMARK: Actually we have shown that the Hasse principle holds for G semisimple if $H^2(K,F) \to \prod_v H^2(K_v,F)$ is injective, where F is the fundamental group of G. In particular, this is always the case for $F = \mu_2$. We shall use this remark in the next section with respect to orthogonal and unitary groups.

To avoid overloading the next section, devoted to proving the Hasse principle, here we shall reduce Theorem 6.6 to the matter of proving $Ш(G) = 1$ for a simply connected semisimple group G over a number field K. This reduction is given by the following

PROPOSITION 6.17. *Let G be a connected group over a number field K. Then $H^1(K,G) \to \prod_{v\in V_\infty^K} H^1(K_v,G)$ is surjective.*

PROOF: In Chapter 7 (cf. Corollary 2 in §7.3) we shall establish this result for tori, of course without using results from this section. Therefore now we show how the general case reduces to the case of tori. To this end, we begin by establishing that for any connected real algebraic group G, any given element ξ in $H^1(\mathbb{R},G)$ lies in the image of $H^1(\mathbb{R},T) \to H^1(\mathbb{R},G)$, for a suitable maximal $\mathbb{R}$-torus T of G. Indeed, the cocycle $\xi = \{\xi_\tau\}$ is determined by fixing $z = \xi_\sigma \in G_{\mathbb{C}}$, where σ denotes complex conjugation, satisfying $z\sigma(z) = 1$. Consider the Jordan decomposition $z = z_s z_u$. It is easy to see that $z_s\sigma(z_s) = 1$ and $z_u\sigma(z_u) = 1$, i.e., the semisimple and unipotent parts of z also define cocycles. It is well known that the minimal

algebraic group U generated by z_u (of course, if $z_u \neq 1$) is isomorphic to $\mathbb{G}_a$; moreover, $z_u\sigma(z_u) = 1$ obviously implies that this group is defined over $\mathbb{R}$. Since $H^1(\mathbb{R}, U) = 1$ (Lemma 2.7) and every element of U commutes with z_s, it is easy to show that ξ is equivalent to θ, given by $t = z_s$.

Furthermore, consider the connected component H^0 of the centralizer $H = Z_G(t)$. Both H and H^0 are defined over $\mathbb{R}$, since $\sigma(t) = t^{-1}$. It is well known (cf. Borel [8, Ch. 2]), that $t \in H^0$. On the other hand, H^0 contains a maximal $\mathbb{R}$-torus T which is also maximal in G. But then $t \in T$ since t is central in H^0, and hence θ lies in the image of $H^1(\mathbb{R}, T) \to H^1(\mathbb{R}, G)$.

Now let $\xi = (\xi_v) \in \prod_{v \in V_\infty^K} H^1(K_v, G)$. By what we have already shown, for each v in V_∞^K one can choose a maximal K_v-torus T_v of G such that $\xi_v \in \mathrm{im}(H^1(K_v, T_v) \to H^1(K_v, G))$. As noted before, we are entitled to use Corollary 3 of Proposition 7.3 here, as a result of which we can find a maximal K-torus T of G which, over each K_v ($v \in V_\infty^K$), is G_{K_v}-conjugate to T_v. It is easy to see that if θ in $H^1(\mathbb{R}, G)$ is defined by z in $G_{\mathbb{C}}$, then for any g in $G_{\mathbb{R}}$, gzg^{-1} defines an equivalent cocycle. It follows that the images of $H^1(K_v, T) \to H^1(K_v, G)$ and $H^1(K_v, T_v) \to H^1(K_v, G)$ are the same for any v in V_∞^K. But then ξ lies in the image of the composite map $H^1(K, T) \xrightarrow{\alpha} \prod_{v \in V_\infty^K} H^1(K_v, T) \to \prod_{v \in V_\infty^K} H^1(K_v, G)$, since we assume that the surjectivity of α has already been established. This proves the proposition.

In §§6.7–6.8 we shall present the proofs of Theorems 6.4 and 6.6. The arguments in these sections involve several stages and use diverse tools, ranging from the arithmetic properties of sesquilinear forms to quite subtle results from algebraic group theory and algebraic number theory. §6.6 is devoted specifically to the properties of forms, but here we present some cohomological corollaries of Steinberg's theorem which we shall need later on.

THEOREM 6.23 (STEINBERG [1]). *Let G_0 be a simply connected semisimple group defined and quasisplit over a (perfect) field K. Then any K-defined conjugacy class of semisimple elements of G_0 contains a K-rational point.*

We shall not actually use Steinberg's theorem, but rather its cohomological corollaries.

PROPOSITION 6.18. *Let G_0 be a semisimple quasisplit K-group (not necessarily simply connected), let $\xi \in Z^1(K, G_0)$ and let $G = {}_\xi G_0$ be the corresponding twisted group. Then for any maximal K-torus T of G there is a cocycle μ in $Z^1(K, T)$ such that $G_0 = {}_\mu G$.*

PROOF: The assertion is trivial for K finite, by Lang's theorem, so we shall assume henceforth that K is infinite. Let $\pi_0: \tilde{G}_0 \to G_0$ be the universal K-covering. Twisting by means of ξ, we obtain a universal K-covering $\pi: \tilde{G} \to G$. We shall interpret $\tilde{G}_{\bar{K}}$ as $(\tilde{G}_0)_{\bar{K}}$ with twisted action of $\mathrm{Gal}(\bar{K}/K)$: $\sigma^*(x) = \tilde{a}_\sigma \sigma(x) \tilde{a}_\sigma^{-1}$ for any σ in $\mathrm{Gal}(\bar{K}/K)$ and x in $(\tilde{G}_0)_{\bar{K}} = \tilde{G}_{\bar{K}}$, where $\xi = \{a_\sigma\}$ and $\tilde{a}_\sigma$ is any inverse image of a_σ. Put $\tilde{T} = \pi^{-1}(T)$, and fix an arbitrary regular element x in $\tilde{T}_K$. Then $\sigma^*(x) = x$ for all σ in $\mathrm{Gal}(\bar{K}/K)$, i.e., $\sigma(x) = \tilde{a}_\sigma^{-1} x \tilde{a}_\sigma$. It follows that the conjugacy class

$$C = \{\, gxg^{-1} : g \in \tilde{G}_0 \,\}$$

is defined over K. Therefore, by Steinberg's theorem $C_K \neq \emptyset$, i.e., there is y in $(\tilde{G}_0)_{\bar{K}}$ such that $\sigma(yxy^{-1}) = yxy^{-1}$. Then we have $yxy^{-1} = \sigma(y)\tilde{a}_\sigma^{-1} x \tilde{a}_\sigma \sigma(y)^{-1}$, whence we obtain $y^{-1}\sigma(y)\tilde{a}_\sigma^{-1} \in \tilde{T}_{\bar{K}}$, since x is regular; hence $z^{-1}\sigma(z)a_\sigma^{-1} \in T_{\bar{K}}$, where $z = \pi_0(y)$. Clearly G_0 can be obtained from G by twisting by $\{a_\sigma^{-1}\}$ in $Z^1(K, G)$. Let us take the equivalent cocycle, $\mu = \{b_\sigma\}$, where $b_\sigma = z^{-1}a_\sigma^{-1}\sigma^*(z)$, and show that $b_\sigma \in T_{\bar{K}}$ for all σ in $\mathrm{Gal}(\bar{K}/K)$. Indeed,

$$b_\sigma = z^{-1}a_\sigma^{-1}\sigma^*(z) = z^{-1}a_\sigma^{-1}(a_\sigma\sigma(z)a_\sigma^{-1}) = z^{-1}\sigma(z)a_\sigma^{-1} \in T_{\bar{K}},$$

and the proposition is proved.

Sometimes the following (essentially equivalent) restatement of Proposition 6.18 is helpful:

PROPOSITION 6.19. *Let G_0, ξ and G be as in Proposition 6.18. Then any maximal K-torus T of G admits a K-embedding in G_0 such that ξ lies in the image of $H^1(K, T) \to H^1(K, G_0)$.*

PROOF: Notation remains as in Proposition 6.18. We have established the existence of y in $(\tilde{G}_0)_{\bar{K}}$ such that $yxy^{-1} = \sigma(y)\tilde{a}_\sigma^{-1} x \tilde{a}_\sigma \sigma(y)^{-1}$. Then for $z = \pi_0(y)$ we have $a'_\sigma = z a_\sigma \sigma(z)^{-1} \in T' = Z_{G_0}(yxy^{-1})$. Since T', being the centralizer of the regular semisimple element yxy^{-1} in $(G_0)_K$, is a maximal K-torus of G_0, and $\xi' = \{a'_\sigma\}$ is equivalent to the original cocycle, it remains to show that the isomorphism $T \simeq T'$ given by $\varphi: t \mapsto ztz^{-1}$ is defined over K. To do so it suffices to establish that φ commutes with any σ in $\mathrm{Gal}(\bar{K}/K)$ which acts as σ on T' and as σ^* on T. Since $a'_\sigma = z a_\sigma \sigma(z)^{-1} \in T'$, we have:

$$\begin{aligned}\varphi(\sigma^*(t)) &= z a_\sigma \sigma(t) a_\sigma^{-1} z^{-1} \\ &= z a_\sigma \sigma(z)^{-1} \sigma(ztz^{-1}) \sigma(z) a_\sigma^{-1} z^{-1} = \sigma(ztz^{-1}) = \sigma(\varphi(t)),\end{aligned}$$

for any t in $T_{\bar{K}}$, as desired.

The following curious observation stems from Propositions 6.18 and 6.19: If G is a semisimple K-group, and G_0 a quasisplit K-group of the same inner type, then any maximal K-torus T of G is K-embeddible in G_0. (In other words, any quasisplit group is a universal repository for all the K-tori that occur in all K-groups of the given inner type.) Indeed, let $\varrho: G \to \bar{G}$ be an isogeny onto the corresponding adjoint group. Since G is obtained from G_0 by twisting with ξ in $H^1(K, \bar{G}_0)$, Proposition 6.18 yields a cocycle μ in $H^1(K, \varrho(T))$ such that $G_0 = {}_\mu G$. But the components of μ act on T trivially, and therefore $T = {}_\mu T$ is a maximal K-torus of $G_0 = {}_\mu G$.

The following application of this statement will be needed below. Let L be either a quadratic extension of K or the algebra $K \oplus K$. Let $*$ denote an involution of L, which in the first instance is a nontrivial automorphism of L/K and in the second switches the components. Furthermore, consider the algebra $A = M_n(L)$ and let τ denote the involution of A given by

$$\tau((x_{ij})) = f(x_{ji}^*)f^{-1},$$

where $f = \begin{pmatrix} 0 & E_{\frac{n}{2}} \\ E_{\frac{n}{2}} & 0 \end{pmatrix}$ for n even, and $f = \begin{pmatrix} 0 & E_{\frac{n-1}{2}} & 0 \\ E_{\frac{n-1}{2}} & 0 & \vdots \\ 0 & \dots & 1 \end{pmatrix}$ for n odd, $E_l = \begin{pmatrix} 1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 1 \end{pmatrix}$ denoting the unit matrix of the appropriate dimension; 1 is understood as $(1,1)$ when $L = K \oplus K$. Then the corresponding special unitary group $G_0 = \mathbf{SU}(A, \tau)$ is a quasisplit group of type ${}^2A_{n-1}$ in the first case ($[L : K] = 2$) and is isomorphic to $\mathbf{SL}_n$ if $L = K \oplus K$ (cf. §2.3). We shall show that any commutative semisimple algebra B over L of degree n, equipped with involution σ whose restriction to L is $*$, can be embedded in (A, τ) as an algebra with involution. Indeed, using the regular representation, we embed B in A as an algebra without involution. Furthermore, let σ also denote the extension of the involution to all A (cf. Albert [1, Ch. 10]). Let $G = \mathbf{SU}(A, \sigma)$ be the corresponding unitary group. Then $T = (B \otimes_K \bar{K}) \cap G$ is a maximal K-torus of G. From the above it follows that $G_0 = {}_\mu G$ for a suitable μ in $Z^1(K, \bar{G})$ acting trivially on T. Clearly the elements of $\bar{G} = \operatorname{Int} G$ act as automorphisms of (A, σ) and $(A, \tau) = {}_\mu(A, \sigma)$. In this regard, μ acts trivially on B, so $(B, \sigma) = {}_\mu(B, \sigma) \hookrightarrow (A, \tau)$.

Proposition 6.19 will be used in combination with some results on cohomological dimension. We shall mention only the basic results relating to this subject and refer the reader to Serre [1] for the proofs and relevant details. Let p be a prime. The cohomological dimension of a profinite group $\mathcal{G}$ with respect to p is said not to exceed 1 ($\operatorname{cd}_p(\mathcal{G}) \leq 1$) if $H^2(\mathcal{G}, A)$ is p-torsion free, for any finite $\mathcal{G}$-module A. Moreover, $\operatorname{cd}(\mathcal{G}) \leq 1$ if $\operatorname{cd}_p(\mathcal{G}) \leq 1$ for each p. Analogously, for K perfect, $\operatorname{cd}_p(K) \leq 1$ if $\operatorname{cd}_p(\mathcal{G}) \leq 1$, for the absolute Galois group $\mathcal{G} = \operatorname{Gal}(\bar{K}/K)$ and $\operatorname{cd}(K) \leq 1$ if $\operatorname{cd}_p(K) \leq 1$ for any p. For $\operatorname{char} K \neq p$ (here generally $\operatorname{char} K = 0$), the condition $\operatorname{cd}_p(K) \leq 1$ can be restated purely in terms of fields: it is equivalent to the triviality of the p-component $\operatorname{Br}(L)_p$ of the Brauer group of any finite extension L/K. This provides important examples of fields satisfying $\operatorname{cd}_p(K) \leq 1$.

PROPOSITION 6.20. *Let K be either a local field or a number field, and let Π be a set of primes. Let K_Π denote the field obtained by adjoining to K all the roots of unity whose degrees are divisible only by elements of Π. Then $\operatorname{cd}_p(K_\Pi) \leq 1$ for any p in Π.*

The proof follows from the fact that any division algebra of index n over a finite extension L of K has a splitting field of the form $L(\zeta_{n^\alpha})$, where ζ_m is the m-th root of unity (cf. proof of Proposition 9 on p. II-11 of Serre [1]).

LEMMA 6.20. *Let $\operatorname{cd}_p(K) \leq 1$. Then $H^1(K, T)$ is p-torsion free, for any K-torus T. In particular, if $\operatorname{cd}(K) \leq 1$, then $H^1(K, T) = 0$.*

PROOF: First we show that $H^2(K, S)$ is p-torsion free, for an arbitrary K-torus S. To do so, consider the exact sequence

$$1 \to S_p \to S \xrightarrow{[p]} S \to 1,$$

where $[p]$ denotes raising to the p-th power and $S_p = \ker[p]$. This sequence has a corresponding exact cohomological sequence

$$\dots \to H^2(K, S_p) \to H^2(K, S) \xrightarrow{[p]} H^2(K, S),$$

whence it follows that $H^2(K, S_p)$ covers all the elements of order p in $H^2(K, S)$. But $H^2(K, S_p) = 1$, since $H^2(K, S_p)$ is annihilated by multiplication by p and at the same time is p-torsion free by the condition $\operatorname{cd}_p(K) \leq 1$; hence $H^2(K, S)_p = 1$.

Now we put the original torus T in the exact sequence

$$1 \to S \to F \to T \to 1,$$

where S and F are K-tori, and F is quasisplit (cf. Proposition 2.2). Then $H^1(K, T)_p = 1$ follows from the previous remark and the exact sequence

$$1 = H^1(K, F) \to H^1(K, T) \to H^2(K, S).$$

Thus the lemma is proved.

The results set forth above enable us to extend Lang's theorem on the triviality of the cohomology of connected groups over finite fields (which, obviously, satisfy $\operatorname{cd}_p(K) \leq 1$) to fields of cohomological dimension ≤ 1.

THEOREM 6.24 (STEINBERG [1]). *If* $\mathrm{cd}(K) \leq 1$, *then* $H^1(K,G) = 1$ *for any connected algebraic* K*-group* G.

PROOF: Indeed, we may confine ourselves to the case where G is reductive. Let $H = [G,G]$ be its semisimple part. Then $T = G/H$ is a torus, and using Lemma 6.20 and the exact sequence $H^1(K,H) \to H^1(K,G) \to H^1(K,T)$, we conclude that the triviality of $H^1(K,G)$ follows from the triviality of $H^1(K,H)$.

Thus the proof of Theorem 6.24 is reduced to the semisimple case. Let G_0 denote a quasisplit K-group of the same inner type as G. Proposition 6.19 and Lemma 6.20 imply the triviality of $H^1(K,B)$ for any semisimple group B quasisplit over K. Applying this assertion to the corresponding adjoint group $\bar{G}_0$, we see that there exists only one K-form of a given inner type, i.e., $G = G_0$ is quasisplit. But then, as we have observed, $H^1(K,G) = 1$. Q.E.D.

6.6. Galois cohomology and quadratic, Hermitian, and other forms.

In this section we shall set forth results, to be used later on, relating to some arithmetic properties of sesquilinear forms, and shall give an interpretation of these results in terms of Galois cohomology. We shall also show how the Hasse principle can be used to give a local-global classification of forms. The basic results of this section include the proof of Theorem 6.5 and the analogous result for a totally imaginary number field.

We begin by analyzing the most well-known and intuitive case, that of quadratic forms. Let f be a nondegenerate quadratic K-form on an n-dimensional vector space W. Then f represents 0 over K, i.e., $f(x) = 0$ has a nonzero solution x in W_K, if and only if it represents 0 over all completions K_v, where $v \in V^K$ (the Minkowski-Hasse theorem, cf. §2.2.3). Moreover, if $n \geq 5$ then f automatically represents 0 over all non-Archimedean completions K_v, where $v \in V_f^K$ (Meyer's theorem). Thus, in particular, we have the following

CLAIM 6.1. *Let* f *be a nondegenerate* n*-dimensional quadratic form over a local field or number field* K, *where* $n \geq 5$. *Then* f *represents 0 if:*

(1) K *is a local field, or*
(2) K *is a number field and* f *represents 0 over* K_v *for all* $v \in V_\infty^K$.

Sometimes the following equivalent restatement is useful:

CLAIM 6.1′. *Let* f *be as in Claim 6.1, let* $n \geq 4$ *and let* $a \in K^*$. *Then* f *represents* a *over* K, *i.e.,* $f(x) = a$ *has a solution* x *in* W_K, *if and only if* f *represents* a *over* K_v *for all* $v \in V_\infty^K$.

For future reference, we also formulate the respective claims for the case of Hermitian forms over a quadratic extension L/K or over a quaternion skew field D/K, which immediately reduce to the case of quadratic forms. Namely, let W be an n-dimensional vector space over L (respectively, D), and let f be a nondegenerate σ-Hermitian form on W, where σ is the nontrivial automorphism of L/K (respectively, the canonical involution of D). We shall say that f represents 0 over K if $f(x) = 0$ has a nonzero solution in W, and over K_v if a solution exists in $W \otimes_K K_v$. The representability of a Hermitian element $a \in L^*, D^*$ by a form f is defined analogously. (Note that in our case the set of Hermitian elements is K^*.) Then we have

CLAIM 6.2. *The situation being as above, assume in addition that* $n \geq 3$ *for a quadratic extension* L/K *and* $n \geq 2$ *for a quaternion skew field* D. *Then* f *represents 0 if:*

(1) K *is a local field, or*
(2) K *is a number field and* f *represents 0 over* K_v *for all* $v \in V_\infty^K$.

Indeed, there is an orthogonal base of W with respect to which f has the form

$$f(x_1, \ldots, x_n) = a_1 N_{L/K}(x_1) + \cdots + a_n N_{L/K}(x_n)$$

or

$$f(x_1, \ldots, x_n) = a_1 \,\mathrm{Nrd}_{D/K}(x_1) + \cdots + a_n \,\mathrm{Nrd}_{D/K}(x_n),$$

where $a_i \in K$, i.e., the values of f are those of a quadratic form of dimension $2n$ (resp. $4n$); therefore everything follows from Claim 6.1. Note also that there is an obvious analog for Claim 6.1′ on the representability by f of an element a in K^*, in which the lower bounds on n in 6.1′ are reduced by 1.

It remains to consider the case of a skew-Hermitian form f defined on an n-dimensional vector space W over a quaternion skew field D. As before, we shall say that a skew-Hermitian element a in D^* is represented by f over K (resp., over K_v), if $f(x) = a$ has a solution x in W (resp., in $W \otimes_K K_v$). Note that the concept of representability of 0 for forms of this type has some delicate points: if $D \otimes_K K_v \simeq M_2(K_v)$, then one should require that there exist not merely a nonzero solution of $f(x) = 0$, but in fact a solution x in $W \otimes_K K_v$ which can be included in a base of $W \otimes_K K_v$ as a module over $D \otimes_K K_v$; this condition is equivalent to the quadratic form $\tilde{f}$, corresponding to f, having rank ≥ 2 over K_v. We shall not go into detail here, but refer the reader to Scharlau [1, Ch. 10].

CLAIM 6.3. *Let* f *be a nondegenerate skew-Hermitian form of dimension* $n \geq 3$ *over a quaternion skew field* D *with center* K. *Then* f *represents a skew-Hermitian element* a *in* D^* *if:*

(1) *K is a local field, or*
(2) *K is a number field and f represents a over all completions K_v, where $v \in V_\infty^K$.*

For the usual proof of this assertion, see Scharlau [1, Ch. 10]). We shall show that it actually follows from Theorems 6.4 and 6.6 for groups of type $A_1 \times A_1$ and type A_3. Since, in the next section, these theorems will be proved for groups of type A_n without using Claim 6.3, this gives a complete proof of the assertion, independent of other sources.

First we consider the case of a local field K, where, without loss of generality, we may assume that $n = 3$. We begin by constructing a 3-dimensional skew-Hermitian form g over D, which *a fortiori* represents a and has the same discriminant as f. We shall look for a matrix of g having the form $\operatorname{diag}(a, b, c)$. Claim 6.1 (cf. also §1.4.3) implies that $\operatorname{Nrd}_{D/K}(D^*) = K^*$; in particular, one can find an element d in D^* such that $\operatorname{Nrd}_{D/K}(d) = d(f)\operatorname{Nrd}_{D/K}(a)$, where $d(f)$ is the discriminant of f. Also, let us consider the space $P = \{ x \in D : \sigma(x) = -x \}$ of "pure" quaternions. It is easy to see that $\dim_K P = 3$, from which it follows that $dP \cap P \neq (0)$. Then there are $b, c \in P$ satisfying $db^{-1} = c$, which will be the desired elements.

By Proposition 2.16, f can be obtained from g by twisting using ξ in $H^1(K, G)$, where $G = \mathbf{SU}_3(g)$. Let H denote the stabilizer in G of the vector $t = (1, 0, 0) \in D^3$, on which g is defined. Then it follows from Witt's theorem (cf. §2.4.5) that the quotient space G/H can be identified with the sphere $S_g = \{ x \in D^3 \otimes_K \bar{K} : g(x) = a \}$. By definition, it also follows easily that the twisted space ${}_\xi(G/H)$ under the action of G on G/H by left translation is $S_f = \{ x \in W \otimes_K \bar{K} : f(x) = a \}$. Therefore, as follows from Lemma 1.6, $(S_f)_K \neq \emptyset$ if and only if ξ lies in the image of $\varepsilon\colon H^1(K, H) \to H^1(K, G)$, and it suffices to show that in our case ε is surjective. To do so, note that G and H are semisimple groups of type $D_3 = A_3$ and $D_2 = A_1 \times A_1$ respectively (cf. §2.3), and their universal coverings $\tilde{G}$ and $\tilde{H}$ are compatible in the sense that we have the commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & F & \longrightarrow & \tilde{G} & \longrightarrow & G & \longrightarrow & 1 \\ & & \| & & \uparrow & & \uparrow & & \\ 1 & \longrightarrow & F & \longrightarrow & \tilde{H} & \longrightarrow & H & \longrightarrow & 1, \end{array} \tag{6.33}$$

where $F = \{\pm 1\}$. Diagram (6.33) yields the commutative cohomological

diagram

$$\begin{array}{ccc} H^1(K, G) & \xrightarrow{\delta_G} & H^2(K, F) \\ \uparrow{\scriptstyle \varepsilon} & & \| \\ H^1(K, H) & \xrightarrow{\delta_H} & H^2(K, F). \end{array}$$

Since we assume Theorem 6.4 to be proved for groups of type D_3 and D_2, if we also take Theorem 6.20 into account we see that δ_G and δ_H are bijections. Therefore ε is also bijective, as desired.

The argument for K a number field is analogous, but differs in several details related to the presence of real valuations. (For totally imaginary number fields the above argument requires no modification.) First we reduce to the case $n = 3$. By our assumptions, for each v in V_∞^K we can find x_v in $W \otimes_K K_v$ such that $f(x_v) = a$. The weak approximation theorem for K implies that the weak approximation property also holds for W, so by a continuity argument there exists x in W such that $f(x) \in \{ ya\sigma(y) : y \in D_v^* \}$ for all v in V_∞^K. Let W' denote a 3-dimensional subspace of W containing x, for which the restriction f' of f to W' is nonsingular. Then clearly the existence of a solution of $f'(x) = a$ implies the existence of a solution of $f(x) = a$.

Thus, henceforth we may assume $\dim f = 3$. Furthermore, in constructing g representing a and having the same discriminant as f, it should be noted that on the one hand $\operatorname{Nrd}_{D/K}(D^*) = K^* \cap (\bigcap_{v \in V_\infty^K} \operatorname{Nrd}_{D_v/K_v}(D_v^*))$ (which follows from Claim 6.1 or Theorem 1.13), but on the other hand $d(f)/\operatorname{Nrd}_{D/K}(a) \in \operatorname{Nrd}_{D_v/K_v}(D_v^*)$ for v in V_∞^K. Finding d in D^* such that $\operatorname{Nrd}_{D/K}(d) = d(f)/\operatorname{Nrd}_{D/K}(a)$ and arguing as above, we can obtain a matrix realization of the desired g as $\operatorname{diag}(a, b, c)$.

Again let ξ in $H^1(K, G)$ (where $G = \mathbf{SU}_3(g)$) be a cocycle which, by twisting, transforms g into f. It follows from the argument for the local case that our task can be restated in terms of Galois cohomology as follows: let $\xi \in H^1(K, G)$. Whereas, by what we have seen, the image ξ_v of ξ in $H^1(K_v, G)$ lies in $\operatorname{im}(H^1(K_v, H) \xrightarrow{\varepsilon_v} H^1(K_v, G))$, for every v in V_∞^K; we must show that $\xi \in \operatorname{im}(H^1(K, H) \xrightarrow{\varepsilon} H^1(K, G))$. To do so, again consider the commutative cohomological diagram with exact rows, obtained from (6.33),

$$\begin{array}{ccccccc} H^1(K, \tilde{G}) & \xrightarrow{\gamma} & H^1(K, G) & \xrightarrow{\delta_G} & H^2(K, F) \\ \uparrow{\scriptstyle \beta} & & \uparrow{\scriptstyle \varepsilon} & & \| \\ H^1(K, \tilde{H}) & \xrightarrow{\alpha} & H^1(K, H) & \xrightarrow{\delta_H} & H^2(K, F). \end{array} \tag{6.34}$$

Since δ_H is surjective (Theorem 6.20), one can find a cocycle η in $H^1(K,H)$ such that $\delta_H(\eta) = \delta_G(\xi)$. Twisting (6.34) by means of η, we reduce the proof to the case where $\delta_G(\xi) = 1$, which we shall assume below without change of notation (i.e., without replacing H by ${}_\eta H$, etc.). Then $\xi = \gamma(\theta)$ for suitable θ in $H^1(K,\tilde{G})$. Furthermore, in this set-up, for each v in V_∞^K one can find a cocycle μ_v in $H^1(K_v,H)$ such that $\xi_v = \varepsilon_v(\mu_v)$. Writing a diagram analogous to (6.34) but for K_v, and using the condition $\delta_G(\xi) = 1$, we obtain that $\mu_v = \alpha_v(\omega_v)$, where $\omega_v \in H^1(K_v,\tilde{H})$.

Since $\gamma_v(\theta_v) = \gamma_v(\beta_v(\omega_v))$, we can write $\beta_v(\omega_v) = f_v\theta_v$ for suitable f_v in $H^1(K_v,F)$. Using the surjectivity of

$$K^*/K^{*^2} = H^1(K,F) \to \prod_{v\in V_\infty^K} H^1(K_v,F) = \prod_{v\in V_\infty^K} K_v^*/K_v^{*^2},$$

we can find f in $H^1(K,F)$ which is mapped onto $(f_v)_{v\in V_\infty^K}$. Modifying θ by f, without loss of generality we may assume that $\beta_v(\omega_v) = \theta_v$ for all v in V_∞^K.

Now consider the commutative diagram

$$\begin{array}{ccc} H^1(K,\tilde{G}) & \xrightarrow{\varrho_{\tilde{G}}} & \prod_{v\in V_\infty^K} H^1(K_v,\tilde{G}) \\ \uparrow\beta & & \uparrow\prod\beta_v \\ H^1(K,\tilde{H}) & \xrightarrow{\varrho_{\tilde{H}}} & \prod_{v\in V_\infty^K} H^1(K_v,\tilde{H}). \end{array}$$

Applying Theorem 6.6 to $\tilde{G}$ and $\tilde{H}$, which pertain to types A_3 and $A_1\times A_1$, respectively, we obtain that $\varrho_{\tilde{G}}$ and $\varrho_{\tilde{H}}$ are bijections. In particular, one can find a (unique) element ω in $H^1(K,\tilde{H})$ such that $\varrho_{\tilde{H}}(\omega) = (\omega_v)_{v\in V_\infty^K}$. Then $\varrho_{\tilde{G}}(\beta(\omega)) = \varrho_{\tilde{G}}(\theta)$, and therefore $\beta(\omega) = \theta$. Returning to (6.34), we have $\xi = \gamma(\theta) = \gamma(\beta(\omega)) = \varepsilon(\alpha(\omega))$, i.e., $\xi \in \operatorname{im}\varepsilon$. This completes the proof of Claim 6.3.

The argument used to prove Claim 6.3 can be reversed. More precisely, if we start from the properties of sesquilinear forms, we can derive proofs of Theorems 6.4 and 6.6 for the simply connected algebraic groups associated with them. The proof of these theorems for the classical groups, other than A_n, which we shall present in the next section, is based precisely on this approach. Groups of type A_n will be considered separately. In particular, in proving Theorems 6.4 and 6.6 for groups of type D_n, we are entitled to use Claim 6.3, since its proof relies on the validity of these theorems only for groups of type A_3 and $A_1\times A_1$.

Now we shall discuss one other aspect of the relationship between the arithmetic of sesquilinear forms and Galois cohomology of algebraic groups over local and number fields—the problem of the equivalence of forms of the same type. This problem can be subdivided naturally into two:

(1) classifying forms over local fields (including $\mathbb{R}$ and $\mathbb{C}$);
(2) justifying the transition from the local to the global, i.e., deducing the equivalence of two K-forms f and g over K from their equivalence over all completions K_v.

When (2) holds we say that forms of the given type satisfy the weak Hasse principle, as opposed to the strong Hasse principle which consists of a local-global treatment of the question of the representability of 0 (or of another element). Note that, in general, the strong Hasse principle does not have a direct, unified cohomological interpretation, as is attested, in particular, by the ad hoc cohomological proof of Claim 6.3. From the point of view of algebraic group theory, the problem is one of analyzing the Hasse principle for homogeneous spaces of algebraic groups by using cohomological methods. Unfortunately, although this is a problem of long standing, it has not yet been fully solved. We note only that the Hasse principle for one class of homogeneous spaces (known as *symmetric spaces*) has been studied by Rapinchuk [5].

Unlike the strong Hasse principle, the weak principle has a precise and explicit interpretation: Since K-forms of the same type as f are classified by elements of $H^1(K,G)$, where G is the corresponding orthogonal (unitary) group (Proposition 2.16), the validity of the local-global principle in this situation is equivalent to the injectivity of $H^1(K,G) \to \prod_v H^1(K_v,G)$. To illustrate concrete computations (and results) we analyze the case of quadratic forms and of skew-Hermitian forms over quaternion algebras.

Let f be a nondegenerate n-dimensional quadratic form over a number field K. Then the set of K-equivalence classes of nondegenerate n-dimensional quadratic forms over K is in one-to-one correspondence with $H^1(K,\mathbf{O}_n(f))$, where $\mathbf{O}_n(f)$ is the corresponding orthogonal group. Since $\mathbf{O}_n(f)$ is not connected, the results which we have obtained are not immediately applicable. To pass to the connected group $\mathbf{SO}_n(f)$, consider the exact sequence

$$1 \to \mathbf{SO}_n(f) \to \mathbf{O}_n(f) \xrightarrow{\det} \mu_2 \to 1, \tag{6.35}$$

where det denotes the determinant and $\mu_2 = \{\pm 1\}$. The above sequence gives rise to the corresponding exact cohomological sequence

$$\mathbf{O}_n(f) \xrightarrow{\det} \mu_2 \to H^1(K,\mathbf{SO}_n(f)) \xrightarrow{\varphi} H^1(K,\mathbf{O}_n(f)) \xrightarrow{\psi} H^1(K,\mu_2).$$

Clearly $\det: \mathbf{O}_n(f) \to \mu_2$ is surjective, from which we can infer that $\ker \varphi$ is trivial. Since this is true for all quadratic forms, we see by standard twisting arguments that φ is injective.

Furthermore, identifying $H^1(K, \mu_2)$ with K^*/K^{*2}, the reader can easily obtain the following description of ψ: if $\xi \in H^1(K, \mathbf{O}_n(f))$ and $[g]$ is the corresponding equivalence class of nondegenerate n-dimensional quadratic forms, then $\psi(\xi)$ is the image in K^*/K^{*2} of $d(g)/d(f)$, where d denotes the discriminant. Thus, a typical fiber of ψ consists of the classes of forms having a given fixed discriminant. In particular, again we obtain that $H^1(K, \mathbf{SO}_n(f))$ classifies the equivalence classes of n-dimensional nondegenerate forms having the same discriminant as f.

Clearly if f and g are equivalent over all K_v, then $d = d(g)/d(f)$ everywhere locally is a square, and therefore also is a square in K. Thus, locally equivalent forms have the same discriminant. A cohomological interpretation of this fact is given in the following diagram:

$$\begin{array}{ccc} H^1(K, \mathbf{O}_n(f)) & \xrightarrow{\quad\psi\quad} & H^1(K, \mu_2) \\ \Big\downarrow \varrho & & \Big\downarrow \theta \\ \prod\limits_v H^1(K_v, \mathbf{O}_n(f)) & \longrightarrow & \prod\limits_v H^1(K_v, \mu_2). \end{array}$$

Then θ is injective; so $\varrho(\xi_1) = \varrho(\xi_2)$ implies $\psi(\xi_1) = \psi(\xi_2)$, as desired. This argument shows that to establish the weak Hasse principle it suffices to analyze the injectivity of $\mu: H^1(K, G) \to \prod\limits_v H^1(K_v, G)$, where $G = \mathbf{SO}_n(f)$. For $n = 2$, G is a 1-dimensional torus; moreover $G \simeq \mathbb{G}_m$ if f is isotropic over K (i.e., $-d(f) \in K^{*2}$), and $G \cong \mathbf{R}^{(1)}_{L/K}(\mathbb{G}_m)$ if f is anisotropic over K (i.e., $-d(f) \notin K^{*2}$), where $L = K(\sqrt{-d(f)})$. Therefore, the Hasse norm principle implies that μ is injective.

Now let $n \geq 3$. Then G is semisimple, and its fundamental group F is isomorphic to μ_2. Therefore the remark following the proof of Theorem 6.22 implies that μ is also injective. Thus, the Hasse principle holds for the quadratic forms; to complete their classification, it remains to solve the analogous local problem. We shall consider forms having the same discriminant d over K_v, whose equivalence classes correspond to the elements of $H^1(K_v, G)$.

First assume $n = 2$. If $-d \in K_v^{*2}$, then $G = \mathbb{G}_m$ and $H^1(K_v, G) = 1$, i.e., in this case all the forms are equivalent to, let us say, $f(x, y) = xy$. Now suppose $-d \notin K_v^{*2}$. Then $G = \mathbf{R}^{(1)}_{L/K}(\mathbb{G}_m)$ where $L = K(\sqrt{-d})$; so $H^1(K_v, G) = K_v^*/N_{L/K_v}(L^*)$ has order 2. The representatives of the two

equivalence classes are the forms $f_1 = x^2 + dy^2$, $f_2 = ax^2 + \frac{d}{a}y^2$, where $a \in K_v^*$ and the Hilbert symbol $(a, -d)_v = -1$. Thus, here a complete system of invariants of the quadratic form f consists of its discriminant $d(f)$ and the Hasse-Witt invariant $\varepsilon_v(f)$, which by definition equals the Hilbert symbol $(a, b)_v$ if $f = ax^2 + by^2$. (Note that $\varepsilon(f_1) = (1, d)_v = 1$, and $\varepsilon(f_2) = (a, \frac{d}{a})_v = (a, -d)_v = -1$.)

Now assume $n \geq 3$, and take $v \in V_f^K$. Then Theorem 6.20 implies that there is a one-to-one correspondence $H^1(K_v, G) \xrightarrow{\delta_v} H^2(K_v, \mu_2)$. If one identifies $H^2(K_v, \mu_2) = \mathrm{Br}(K_v)_2$ with $\{\pm 1\}$, then one can show that δ_v is given by $\delta_v([g]) = \varepsilon_v(g)/\varepsilon_v(f)$, where $\varepsilon_v(f)$ and $\varepsilon_v(g)$ are the Hasse-Witt invariants of f and g, respectively. (Recall that by definition $\varepsilon_v(h) = \prod\limits_{i<j}(a_i, a_j)_v$, for $h = a_1x_1^2 + \cdots + a_nx_x^2$.) The proof of this formula can be found in Springer [1]). It turns out that also for $n \geq 3$ the equivalence class of a quadratic form f is completely determined by $d(f)$ and $\varepsilon_v(f)$. On the other hand, given any values of d in K_v^*/K_v^{*2} and $\varepsilon = \pm 1$ which satisfy the sole condition $\varepsilon = 1$, if $n = 2$ and $-d \in K_v^{*2}$, there exists an n-dimensional quadratic form f over K_v with these invariants.

It remains to interpret the elements of $H^1(\mathbb{R}, G)$. For the sake of simplicity, we shall confine ourselves to forms having positive discriminant, and then we may assume that $f = x_1^2 + \cdots + x_n^2$. In this case the description of $H^1(\mathbb{R}, G)$ can be deduced easily from Theorem 6.17. Namely, assume for convenience that $n = 2l$ is even, and for a maximal $\mathbb{R}$-torus T of G take $T = \mathbf{SO}_2(g_1) \times \cdots \times \mathbf{SO}_2(g_l)$, where $g_i = x_{2i-1}^2 + x_{2i}^2$. Then the set T_2 of elements of order 2 in T can be identified with $D = \{\, \mathrm{diag}(\varepsilon_1, \ldots, \varepsilon_l) : \varepsilon_i = \pm 1 \,\}$. Moreover, the orbits of the action of the Weyl group $W = W(T, G)$ on T_2 are the orbits of the natural action of the symmetric group S_l on D. Thus, the equivalence classes in D/S_l are determined by the numbers r and s of those ε_i which equal -1 and $+1$ respectively (clearly $r+s = l$). On the other hand, it is easy to see that the form corresponding to the class with representative $\mathrm{diag}(\varepsilon_1, \ldots, \varepsilon_l)$, where $\varepsilon_1 = \cdots = \varepsilon_r = -1$, $\varepsilon_{r+1} = \cdots = \varepsilon_l = 1$ is $f_r = -x_1^2 - \cdots - x_{2r}^2 + x_{2r+1}^2 + \cdots + x_n^2$, which brings us to the well-known classification of real forms by means of signatures.

(EXERCISE: Using Theorem 6.18, derive the analogous interpretation for the elements of $H^1(\mathbb{R}, \mathbf{SO}_n(f))$ when the discriminant of f is -1.)

To summarize our discussion, we may say that the equivalence class of an n-dimensional quadratic form over a number field K is characterized by

(1) the discriminant $d(f)$;
(2) the Hasse-Witt invariants $\varepsilon_v(f)$ for v in V_f^K;
(3) the signatures (r_v, s_v) for real v in V_∞^K.

Note that not all these invariants are independent; in particular, it follows from Theorem 1.12 that $\varepsilon_v(f) = 1$ for almost all v in V_f^K and $\prod_v \varepsilon_v(f) = 1$ (the product taken over all v, including the Archimedean ones), but for any set of invariants obeying these and several other straightforward conditions one can find a quadratic form with the prescribed invariants. O'Meara [1] and Scharlau [1] give a detailed exposition of this theory, and Serre [8, Ch. 4] provides a brilliant introduction to the subject.

Now we move on to an analysis of skew-Hermitian forms over a quaternion skew field D. Let f be an n-dimensional nondegenerate skew-Hermitian form, and let $G = \mathbf{SU}_n(f)$ be the corresponding special unitary group. Then, for $n = 1$, G is the one-dimensional torus of the form $\mathbf{R}^{(1)}_{L/K}(\mathbb{G}_m)$, where L is a maximal subfield of D; and, for $n \geq 2$, G is a semisimple group whose fundamental group is isomorphic to μ_2. In both cases the Hasse principle holds for G. It follows that in this case the weak Hasse principle holds for proper equivalence: two skew-Hermitian forms f and g are properly equivalent (i.e., transform to one another by a matrix from $SL_n(D)$) if and only if they are properly equivalent for all completions K_v. However, we are interested in the usual equivalence of forms, and therefore must pass from the cohomology of $\mathbf{SU}_n(f)$ to the cohomology of the full unitary group $\mathbf{U}_n(f)$. We shall need the following well-known assertion (cf. Kneser [12]).

LEMMA 6.21. *$U_n(f) = SU_n(f)$.*

Consider the exact sequence $1 \to \mathbf{SU}_n(f) \to \mathbf{U}_n(f) \overset{\mathrm{Nrd}}{\to} \mu_2 \to 1$ and its corresponding cohomological sequence

$$U_n(f) \overset{\mathrm{Nrd}}{\to} \mu_2 \overset{\varepsilon}{\to} H^1(K, \mathbf{SU}_n(f)) \overset{\varphi}{\to} H^1(K, \mathbf{U}_n(f)) \overset{\psi}{\to} H^1(K, \mu_2). \tag{6.36}$$

It follows from Lemma 6.21 that $\varepsilon(\mu_2) = \ker\varphi$ consists of two elements; in particular, φ is never injective. Nevertheless, using (6.36) we can obtain a complete classification of skew-Hermitian forms over a local field K. Namely, since for $n \geq 2$, G is a semisimple group with fundamental group μ_2, and for $n = 1$, is the one-dimensional torus $\mathbf{R}^{(1)}_{L/K}(\mathbb{G}_m)$, where L/K is a quadratic extension, we see that $H^1(K, \mathbf{SU}_n(f))$ consists of two elements and therefore is precisely $\ker\varphi$. Hence, applying twisting, we obtain that ψ is injective. Thus, over a local field the equivalence class of a skew-Hermitian form is uniquely determined by its discriminant; moreover, if $n \geq 2$, the discriminant can take on any value and, if $n = 1$, a value not belonging to $-K^{*2}$.

Now we show that the weak Hasse principle for equivalence of skew-Hermitian forms does not hold in general; moreover, from a cohomological

point of view, this is due to the fact that $H^1(K, \mathbf{SU}_n(f)) \to H^1(K, \mathbf{U}_n(f))$ is not injective. Consider the commutative diagram with exact rows

$$\begin{array}{ccccccc}
1 & \longrightarrow & \mu_2 & \xrightarrow{\alpha_1} & H^1(K, \mathbf{SU}_n(f)) & \xrightarrow{\alpha_2} & H^1(K, \mathbf{U}_n(f)) \\
 & & \downarrow{\scriptstyle \gamma_1} & & \downarrow{\scriptstyle \gamma_2} & & \downarrow{\scriptstyle \gamma_3} \\
1 & \longrightarrow & \prod_{v\in S} \mu_2 \times \prod_{v\notin S} \{1\} & \xrightarrow{\beta_1} & \prod_v H^1(K_v, \mathbf{SU}_n(f)) & \xrightarrow{\beta_2} & \prod_v H^1(K_v, \mathbf{U}_n(f))
\end{array}$$

where $S = \{ v \in V^K : D_v = D \otimes_K K_v \text{ is a skew field} \}$. It follows from this diagram that $\alpha_2(\gamma_2^{-1}(\operatorname{im}\beta_1)) \subset \ker\gamma_3$; moreover, clearly

$$|\alpha_2(\gamma_2^{-1}(\operatorname{im}\beta_1))| = \frac{1}{2}|\gamma_2^{-1}(\operatorname{im}\beta_1)|.$$

LEMMA 6.22. *$|\gamma_2^{-1}(\operatorname{im}\beta_1)| \geq 2^{t-1}$, where $t = |S \cap V_f^K|$.*

PROOF: Consider the commutative diagram induced by the universal covering $\tilde{G} \to G$ of $G = \mathbf{SU}_n(f)$:

$$\begin{array}{ccccc}
H^1(K, \tilde{G}) & \longrightarrow & H^1(K, G) & \xrightarrow{\delta} & H^1(K, \mu_2) \\
\downarrow & & \downarrow{\scriptstyle \gamma_2} & & \downarrow{\scriptstyle \tau} \\
\prod_{v\in V^K} H^1(K_v, \tilde{G}) & \longrightarrow & \prod_{v\in V^K} H^1(K_v, G) & \xrightarrow{\theta} & \prod_{v\in V^K} H^2(K_v, \mu_2).
\end{array}$$

Since ε in (6.36), taken for K_v where $v \in S \cap V_f^K$, is a bijection we see that it suffices to establish the equality

$$|\gamma_2^{-1}(\prod_{v\in S\cap V_f^K} H^1(K_v, G) \times \prod_{v\notin S\cap V_f^K} \{1\})| = 2^{t-1}.$$

But for v in V_f^K the restriction of θ to $H^1(K_v, G)$ is bijective onto $H^2(K_v, \mu_2)$; therefore, in view of the surjectivity of δ (Theorem 6.20) and Theorem 6.6, with a standard twisting argument we can reduce the problem to proving

$$|\tau^{-1}(\prod_{v\in S\cap V_f^K} H^2(K_v, \mu_2) \times \prod_{v\notin S\cap V_f^K} \{1\})| = 2^{t-1}.$$

(We leave it to the reader to work out the details.) But in view of the identifications $H^2(K, \mu_2) = \operatorname{Br}(K)_2$ and $H^2(K_v, \mu_2) = \operatorname{Br}(K_v)_2$, this equality follows from Theorem 1.12. The lemma is proved.

Thus, $|\ker\gamma_3| \geq 2^{t-2}$ and therefore γ_3 is not injective in general. A somewhat more precise computation (cf. Kneser [12], Bartels [2]) shows that $|\ker\gamma_3| = 2^{s-2}$, where $s = |S|$. Notwithstanding the violation of the weak Hasse principle, a local-global classification of skew-Hermitian forms is possible (cf. Bartels [2], Scharlau [1]). The reader who wishes to pursue the subject is referred to Bartels [1], [2] for a detailed exposition of the cohomological approach to the classification of skew-Hermitian forms.

Using results from the arithmetic of sesquilinear forms, we obtain a proof of Theorem 6.5, that any simple simply connected anisotropic group over a local field is of type $\mathbf{SL}_1(D)$, and the following analog for a totally imaginary field.

THEOREM 6.25. *Let G be a simple anisotropic group over a totally imaginary number field K. Then G is of type A_n.*

(The difference between Theorems 6.5 and 6.25 is that over local fields only inner forms of type A_n can be anisotropic, whereas, over totally imaginary number fields, outer forms also can be anisotropic.)

The fact that the groups of type B_n $(n \geq 2)$, C_n $(n \geq 2)$, and ${}^{1,2}D_n$ $(n \geq 4)$ are isotropic follows from the description of these groups as connected components of the groups of automorphisms of quadratic, Hermitian, or skew-Hermitian forms (cf. §2.3) and from the fact that a group is isotropic if and only if the corresponding form is isotropic (cf. Proposition 2.15 and Claims 6.1–6.3). Note, also, that over local fields there are no noncommutative skew fields with involution of the second kind, so the outer forms of type ${}^2A_n$ $(n \geq 2)$ correspond to Hermitian forms of degree ≥ 3 over a quadratic extension L/K, which are isotropic by Claim 6.2.

For exceptional groups the proofs of Theorems 6.5 and 6.25 use Propositions 6.15 and 6.16, and thus in the final analysis depend on Theorems 6.4 and 6.6. However, Theorems 6.5 and 6.25 will be used in proving Theorems 6.4 and 6.6. Therefore, to avoid circular reasoning, we shall prove the following conditional statement, which automatically completes the proof of Theorems 6.5 and 6.25 after Theorems 6.4 and 6.6 are proved.

THEOREM 6.26. *Let G be a simply connected simple group belonging to one of the exceptional types and defined over a local or a totally imaginary number field K, and let G_0 be a quasisplit group of the same inner type. If $H^1(K, G_0) = 1$, then G is K-isotropic.*

PROOF: If G belongs to one of the types E_8, F_4, G_2, then $H^1(K, G_0) = 1$ implies that G is K-split (Proposition 6.16 (1)), and there is nothing to prove.

Consider the remaining types ${}^{3,6}D_4$, ${}^{1,2}E_6$, E_7. If K is a local field then groups of types ${}^{3,6}D_4$ and ${}^2E_6$ are quasisplit over K (Proposition 6.15); therefore it remains to consider only types ${}^1E_6$ and E_7. Over a totally imaginary number field all these types must be considered.

GROUPS OF TYPE E_7: This is the easiest case to analyze. Proposition 6.16 implies that G is split over some quadratic extension L/K. Furthermore, one can apply

LEMMA 6.23. *Let G be a connected K-group splitting over a quadratic extension L/K. Then G has a maximal K-torus T which is split over L.*

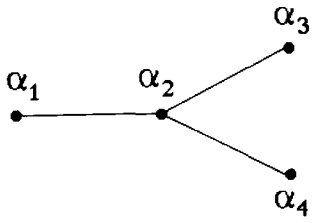
Indeed, G has a Borel subgroup defined over L, and hence by Lemma 6.17 there exists a Borel L-subgroup B of G such that $T = B \cap \sigma(B)$ is a maximal K-torus of G, where σ is the generator of $\mathrm{Gal}(L/K)$. It remains to note that since G is split over L, any L-torus of B is L-split.

Now suppose G is K-anisotropic, and consider the root system $R = R(T, G)$, where T is the torus from Lemma 6.23. Since T is K-anisotropic, we have $\mathbf{X}(T)^{\sigma^*} = \{0\}$, where σ^* denotes the action of σ on the group of characters. Since $(\sigma^*)^2 = \mathrm{id}$, it follows that $\sigma^*\chi = -\chi$ for any χ in $\mathbf{X}(T)$. In particular, $\sigma^*\alpha = -\alpha$ for any α in R, and therefore the root subgroup G_α generated by the one-dimensional unipotent subgroups U_α and $U_{-\alpha}$ (cf. §2.1.10) is defined over K. Hence, for any subset Σ of the system of simple roots $\Pi \subset R$, the group G_Σ generated by G_α, for all α in Σ, is defined over K. (This argument works for any anisotropic group split by a quadratic extension and will be used repeatedly.)

Take Σ to be a subset consisting of two adjacent roots in the Dynkin diagram. Then $H = G_\Sigma$ is a K-subgroup of G of type A_2, split by a quadratic extension L/K. Therefore, from the description of groups of this type (cf. §2.3) it follows that H must be a group isogenous to $\mathbf{SU}_3(f)$, where f is a Hermitian form over L/K. But Claim 6.2 implies that over local fields or totally imaginary number fields such a form is isotropic. Therefore H, and certainly G, are isotropic.

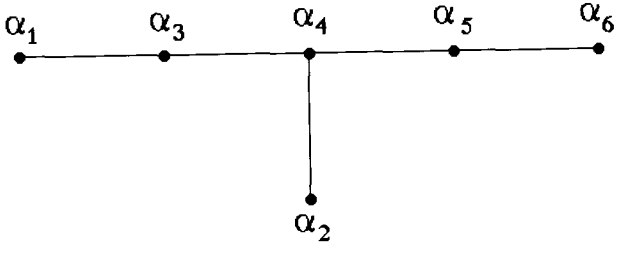
GROUPS OF TYPE ${}^{3,6}D_4$: By Proposition 6.15 (2), any group G of one of these types contains a Borel subgroup B defined over a quadratic extension L/K. Suppose G is K-anisotropic and σ generates $\mathrm{Gal}(L/K)$. Then $T = B \cap \sigma(B)$ is a maximal K-torus of G contained in B. Consider the root

system $R = R(T, G)$, and label the simple roots as follows:
(6.37)



The explicit description of roots (cf. Bourbaki [4, Table 4]) implies that $\beta = \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4$ is a root. Moreover, $\alpha = \alpha_2$ and β are invariant with respect to all the symmetries of (6.37), and therefore are defined over L. Then, as above, since G is K-anisotropic we obtain $\sigma^*\alpha = -\alpha$ and $\sigma^*\beta = -\beta$; so H, generated by G_α and G_β, is defined over K. The description of the roots implies that H is a group of type A_2, split over L/K. Therefore, the argument can be concluded as in the previous case.

GROUPS OF TYPE ${}^1E_6$: We know that $Z(G) = \mu_3$, therefore, arguing as in the proof of Proposition 6.16, we obtain that G is split by some cyclic extension L/K of degree 3. Let σ be a generator of $\mathrm{Gal}(L/K)$. To apply the above method here, one would consider $B \cap \sigma(B) \cap \sigma^2(B)$, where B is a Borel L-subgroup of G; however this trick does not work, since this intersection might be trivial. Therefore, instead one should use a modification of this trick which essentially amounts to taking parabolic subgroups rather than Borel subgroups. Namely, consider a root system $R = R(T, G)$ with respect to a maximal L-split torus T of G, and label the simple roots in the following manner:
(6.38)



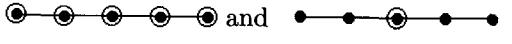
Notation as in §2.1.12, put $P = P_\Delta$, where $\Delta = \{\alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6\}$. Then P is a maximal parabolic L-subgroup of G having codimension 16 ($\dim G = 78$, $\dim P = 62$); the central torus of the reductive part of P is one-dimensional, and the semisimple part is a group of type D_5. Put $H = P \cap \sigma(P) \cap \sigma^2(P)$. From the dimension theorem it follows that

$\operatorname{codim} H \leq 3 \cdot 16 = 48$, i.e., $\dim H \geq 78 - 48 = 30$. If we assume G to be K-anisotropic, then H is a reductive K-subgroup of G. We shall show that its semisimple part D contains a simple component of type other than A_n. Then the fact that D is isotropic follows immediately, since we have already proved that the groups of all types other than A_n and E_6 are isotropic.

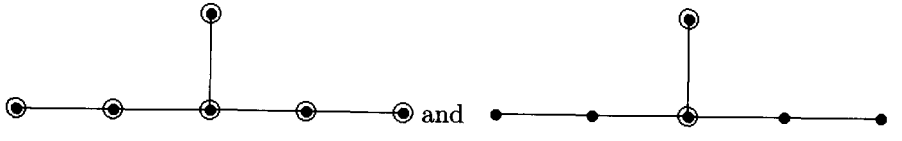
Suppose on the contrary that D has type $A_{d_1} \times \cdots \times A_{d_n}$. Then $d_1 + \cdots + d_n \leq 5$ and $d_1 + \cdots + d_n + m \leq 6$, where m is the dimension of the central torus of H. Moreover, the case $d_i = 5$ is impossible, since D must be contained in a group of type D_5 (the semisimple part of P) and a group of type A_5 is not embeddable in D_5 (since the order of the Weyl group $W(A_5)$, which equals 6!, does not divide the order of $W(D_5)$, which equals $2^4 \cdot 5!$). With elementary estimates one obtains that $\dim H = d_1^2 + \cdots + d_n^2 + 2(d_1 + \cdots + d_n) + m \leq 28$, which is impossible, since we have seen $\dim H \geq 30$.

GROUPS OF TYPE ${}^2E_6$: Let L/K be a quadratic extension over which G becomes an inner form. Then by the previous arguments G is L-isotropic. We claim that at least one of the end points α_i ($i = 1, 2, 6$) in (6.38) is distinguished in the L-index of G. Indeed, if not, the L-anisotropic kernel of G has a simple component of type A_1. But the anisotropic kernel must split over an extension L of degree 3, contradiction. Then the corresponding parabolic subgroup $P = P_\Delta$, where $\Delta = \{\alpha_j : j \neq i\}$ is defined over L and has codimension 16 for $i = 1, 6$, and 21 for $i = 2$. If we assume G to be K-anisotropic, then $H = P \cap \sigma(P)$, where σ is the generator of $\mathrm{Gal}(L/K)$, is a reductive K-subgroup. In case $\operatorname{codim} P = 16$ we have $\operatorname{codim} H \leq 32$, i.e., $\dim H \geq 78 - 32 = 46$ and, as above, it is easy to see that all the simple components cannot have type A_n, thereby yielding the desired result.

Therefore the only remaining case where G *a priori* might be K-anisotropic is the case where the vertex α_2 is distinguished and the semisimple part D of H is a group of type A_5. (Clearly in this case D is the semisimple part of P.) Furthermore, D must split over an extension L of degree 3, from which it follows that for the L-index of D there are two possibilities:



Then the L-index of G appears as



respectively. In the first instance, G is split over L, and the proof that it is K-isotropic follows as in the case of groups of type E_7.

Now we consider the second possibility. Put $P' = P_{\Delta'}$, where $\Delta' = \{\alpha_j : j \neq 2,4\}$. Then $\dim P' = 48$, hence for $F = P' \cap \sigma(P')$ we obtain the estimate $\dim F \geq 18$. Since F is a reductive K-group whose semisimple part S is embeddible in a group of type $A_2 \times A_2$, a dimension analysis shows that S has type $A_2 \times A_2$ and hence is the semisimple part of P. The centralizer $C = Z_G(S)$ is a semisimple K-group of type A_2 which becomes isotropic over L, since even the centralizer of D is L-isotropic. It follows that C must be a group of type $\mathbf{SU}_3(f)$, where f is an Hermitian form over the extension L of K. Since groups of this kind are K-isotropic, the proof of Theorem 6.26 is complete.

6.7. Proof of Theorems 6.4 and 6.6: Classical groups.

Representing a semisimple simply connected K-group G as

$$G = \prod_{i=1}^{r} \mathbf{R}_{L_i/K}(G_i),$$

where G_i is a simply connected simple group over a finite extension L_i of K, we can easily reduce the proof of Theorems 6.4 and 6.6, with the help of Shapiro's lemma, to the case of simple groups.

In this section we shall look at groups of type ${}^{1,2}A_l$, B_l, C_l and ${}^{1,2}D_l$. The section is organized as follows: first we take up groups of type ${}^1A_l$. Theorem 6.4 in this case turns out to be equivalent to the surjectivity of the reduced norm in a simple algebra over a local field (cf. §1.4.3), and Theorem 6.6 to Eichler's norm theorem. Furthermore, in view of Claims 6.1–6.3 of the previous section, the proof of Theorems 6.4 and 6.6 for groups of type B_l, C_l and ${}^{1,2}D_l$, as well as $\mathbf{SU}_n(f)$ arising from a Hermitian form over a quadratic extension L/K, reduces to groups of type $B_1 = C_1 = A_1$ and $D_2 = A_1 \times A_1$, which have already been analyzed. Thus, it remains to consider forms of type ${}^2A_l$ associated with noncommutative skew fields with involution of the second kind. (Note that over local fields, i.e., in the proof of Theorem 6.4, this case does not occur.) The argument here is based on a relatively little known theorem due to Landherr, presented here with its proof. Note also that in proving Theorem 6.6 for groups of all types we only check the triviality of the kernel of

$$H^1(K,G) \to \prod_{v \in V_\infty^K} H^1(K_v, G),$$

since its surjectivity has already been proved (Proposition 6.17).

GROUPS OF TYPE ${}^1A_l$: Here $G = \mathbf{SL}_n(D)$, where D is a finite-dimensional skew field over K. Then by Lemma 2.9

$$H^1(K,G) \simeq K^*/\operatorname{Nrd}_{A/K}(A^*) = K^*/\operatorname{Nrd}_{D/K}(D^*),$$

where $A = M_n(D)$. If K is a local field, then $\operatorname{Nrd}_{D/K}(D^*) = K^*$ (cf. §1.4.3), and hence $H^1(K,G) = 1$, i.e., Theorem 6.4 is proved in this case.

Now let K be a number field. Then $H^1(K,G) \xrightarrow{\delta} \prod_{v \in V_\infty^K} H^1(K_v, G)$ is equivalent to $K^*/\operatorname{Nrd}_{A/K}(A^*) \to \prod_{v \in V_\infty^K} K_v^*/\operatorname{Nrd}_{A_v/K_v}(A_v^*)$, where $A_v = A \otimes_K K_v$; therefore the triviality of $\ker \delta$ is equivalent to

$$\operatorname{Nrd}_{A/K}(A^*) = \bigcap_{v \in V_\infty^K} (K^* \cap \operatorname{Nrd}_{A_v/K_v}(A_v^*)). \tag{6.39}$$

It is easy to see for v in V_∞^K that $\operatorname{Nrd}_{A_v/K_v}(A_v^*)$ is K_v^* if A_v is a full matrix algebra over K_v (in particular if $K_v = \mathbb{C}$), and is the set of positive elements of K_v^* if $K_v = \mathbb{R}$ and A_v is a full matrix algebra over the skew field of the real quaternions. Therefore (6.39) follows from the Eichler norm theorem (cf. Theorem 1.13).

GROUPS OF TYPE B_l, C_l, ${}^{1,2}D_l$: Since $H^1(K, \mathbf{Sp}_{2n}) = 1$ for the symplectic group $\mathbf{Sp}_{2n}$ over any K (cf. Proposition 2.7), we can exclude symplectic groups from further analysis. The remaining groups pertaining to one of the above types are the universal coverings G_n of $\mathbf{SO}_n(f)$ (resp., $\mathbf{SU}_n(f)$), where f is a nondegenerate n-dimensional quadratic form (resp., Hermitian or skew-Hermitian form over a skew field D of quaternions). At the same time we shall also consider $\mathbf{SU}_n(f)$ corresponding to Hermitian forms over a quadratic extension L/K which belong to type ${}^2A_{n-1}$.

Let W denote an n-dimensional space over K (resp., D or L) on which f is defined. Moreover, we shall designate by m_0 the integer appearing in the list of classical groups (cf. §2.3.4) for each type. Its arithmetic interpretation, which follows from Claims 6.1′, 6.2 and 6.3 in §6.6, is that, for $n \geq m_0$, f automatically represents a given a in K^* (resp., Hermitian or skew-Hermitian a in D^* or L^*) if K is a local field or a number field, and the representability holds over K_v for all v in V_∞^K. Note that $m_0 = 1$ for quaternionic groups of type C_n, and in this case, for the sake of uniformity it is convenient to view the group of type C_0 as the unit group. For the remaining types of groups, G_{m_0-1} belongs to types $B_1 = A_1$ and $D_2 = A_1 \times A_1$, which we have already analyzed.

First we take K a local field and apply induction. Supposing $n \geq m_0$, we show that the triviality of $H^1(K, G_n)$ follows from the triviality of $H^1(K, G_{n-1})$. Fix an anisotropic vector x in W. Its stabilizer in G_n is a group of type G_{n-1} (cf. Proposition 2.21). We shall show that $H^1(K, G_{n-1}) \xrightarrow{\varphi} H^1(K, G_n)$ is surjective. To do so, note that by Witt's theorem the homogeneous space G_n/G_{n-1} can be identified with the sphere

$$X = \{ y \in W \otimes_K \bar{K} : f(y) = f(x) \}.$$

Now let $\xi \in H^1(K, G)$. Then the twisted space $\xi(G_n/G_{n-1})$ is isomorphic to the sphere $Y = \{ y \in W \otimes_K \bar{K} : g(y) = f(x) \}$, where $g = \xi f$ is the corresponding twisted form. We have $Y_K \neq \emptyset$ since $n \geq m_0$, and therefore $\xi \in \operatorname{im} \varphi$ (cf. Lemma 2.6), as desired.

Now let us take the case where K is a number field. For K totally imaginary, no modification is needed in the above argument in order to establish the triviality of $H^1(K, G_n)$. In general one needs an additional result on weak approximation, which we shall prove in §7.1. Namely, let x in W be an anisotropic vector and let $X = \{ y \in W \otimes_K \bar{K} : f(y) = f(x) \}$ be the corresponding sphere; then X has the weak approximation property with respect to any finite set $S \subset V^K$, i.e., $X_K \to X_S = \prod_{v \in S} X_{K_v}$ is dense. We shall use this fact in the following context. Since X is a homogeneous space of G_n, the orbit $(G_n)_{K_v} x_v$ is open in X_{K_v} for any v in V^K and any x_v in X_{K_v} (Proposition 3.3, Corollary 2), and therefore one can find x in X_K such that $x \in (G_n)_{K_v} x_v$ for all v in S. In other words, the map $X_K/(G_n)_K \to \prod_{v \in S} (X_{K_v}/(G_n)_{K_v})$ of the corresponding orbit spaces is surjective. Now consider the "exact sequence"

$$1 \to G_{n-1} \to G_n \xrightarrow{\alpha} X \to 1,$$

where $\alpha(g) = gx$, from which one obtains the following commutative diagram:

(6.40)

$$\begin{array}{ccccc} X_K/(G_n)_K & \xrightarrow{\beta_1} & H^1(K, G_{n-1}) & \xrightarrow{\beta_2} & H^1(K, G_n) \\ \downarrow \alpha_1 & & \downarrow \alpha_2 & & \downarrow \alpha_3 \\ \prod_{v \in V_\infty^K} X_{K_v}/(G_n)_{K_v} & \xrightarrow{\gamma_1} & \prod_{v \in V_\infty^K} H^1(K_v, G_{n-1}) & \xrightarrow{\gamma_2} & \prod_{v \in V_\infty^K} H^1(K_v, G_n). \end{array}$$

Now let $\xi \in \ker \alpha_3$. As in the local case, $\xi(G_n/G_{n-1})$ can be identified with $Y = \{ y \in W \otimes_K \bar{K} : g(y) = f(x) \}$, where $g = \xi f$ is the twisted form. Since $\xi \in \ker \alpha_3$, it follows that f and g are equivalent over K_v for each v in V_∞^K; in particular, $g(y) = f(x)$ has a solution, i.e., $Y_{K_v} \neq \emptyset$. But by assumption $n \geq m_0$, and therefore $Y_K \neq \emptyset$. This means that $\xi = \beta_2(\zeta)$ for a suitable ζ in $H^1(K, G_{n-1})$. By assumption the cocycle

$$\gamma_2(\alpha_2(\zeta)) = \alpha_3(\beta_2(\zeta)) = \alpha_3(\xi)$$

is trivial; therefore, since the bottom row of (6.40) is exact, we obtain $\alpha_2(\zeta) = \gamma_1(z)$, where $z \in \prod_{v \in V_\infty^K} X_{K_v}/(G_n)_{K_v}$. But above we established

that α_1 is surjective, which means that $z = \alpha_1(a)$ for some $a \in X_K/(G_n)_K$. Since (6.40) is commutative, it follows that $\alpha_2(\zeta) = \alpha_2(\beta_1(a))$; and therefore $\zeta = \beta_1(a)$, since by the induction hypothesis α_2 is injective. (The induction hypothesis consists of the fact that the kernel of α_2 is trivial for all groups of the given type of degree $n-1$, which by twisting arguments is equivalent to α_2 being injective for the same class of groups.) Finally we obtain that $\xi = \beta_2(\zeta) = \beta_2(\beta_1(a))$ is trivial.

GROUPS OF TYPE ${}^2A_l$: The case of special unitary groups associated with a quadratic extension L/K was discussed together with the groups of type B_l and D_l; therefore now we shall consider special unitary groups $G = \mathbf{SU}_n(f)$ of Hermitian forms f over a (noncommutative) skew field D with involution σ of the second kind, whose center L is a quadratic extension of the ground field K (where K is always a number field). The argument is quite intricate and long, therefore we shall break it down into two main stages: first we shall prove the Hasse principle for the corresponding unitary group $H = \mathbf{U}_n(f)$; then we deduce the Hasse principle for G from the Hasse principle for H. In the preliminaries to the proof we shall reduce these assertions to several properties of algebras with involution, and afterwards we shall prove these properties.

Take the algebra $A = M_n(D)$ and define an involution τ by putting $\tau((x_{ij})) = F(\sigma(x_{ji}))F^{-1}$, where F is the matrix of f. Let B denote $\mathbf{GL}_n(D)$, and let Σ denote the set of τ-symmetric elements of B. Then $\varphi: B \to \Sigma$ given by $\varphi(x) = x\tau(x)$ is surjective and has H as its kernel; therefore Σ can be identified with the homogeneous space B/H. The exact sequence $1 \to H \to B \xrightarrow{\varphi} \Sigma \to 1$ gives rise to the following diagram:

(6.41)

$$\begin{array}{ccccccc} A^* & \xrightarrow{\beta_1} & \Sigma_K & \xrightarrow{\beta_2} & H^1(K, H) & \xrightarrow{\beta_3} & H^1(K, B) = 1 \\ \downarrow \alpha_1 & & \downarrow \alpha_2 & & \downarrow \alpha_3 & & \downarrow \alpha_4 \\ \prod_{v \in V^K} (A \otimes_K K_v)^* & \xrightarrow{\gamma_1} & \prod_{v \in V^K} \Sigma_{K_v} & \xrightarrow{\gamma_2} & \prod_{v \in V^K} H^1(K_v, H) & \xrightarrow{\gamma_3} & \prod_{v \in V^K} H^1(K_v, B) = 1 \end{array}$$

Let $\xi \in \ker \alpha_3$. Since $H^1(K, B) = 1$, we have $\xi = \beta_2(x)$ for some $x \in \Sigma_K$. By assumption $\gamma_2(\alpha_2(x)) = \alpha_3(\xi)$ is trivial, which, in view of the exactness of the bottom row of (6.41), means that $\alpha_2(x) \in \operatorname{im} \gamma_1$. However, the triviality of ξ is equivalent to $x \in \operatorname{im} \beta_1$. Thus, the Hasse principle for the unitary group H is equivalent to the following

THEOREM 6.27 (LANDHERR [1]). *Suppose $y \in A^*$ is symmetric. Assume for each v in V^K the equation $y = x \cdot \tau(x)$ has a solution x_v in $A \otimes_K K_v$. Then this equation has a solution x in A^*.*

Now assume the Hasse principle has already been proved for H. Put $S = \mathbf{R}^{(1)}_{L/K}(\mathbb{G}_m)$. The reduced norm $\mathrm{Nrd}_{A/L}$ induces the exact sequence $1 \to G \to H \to S \to 1$, which yields:

(6.42)

$$\begin{array}{ccccccc} H_K & \xrightarrow{\theta_1} & S_K & \xrightarrow{\theta_2} & H^1(K,G) & \xrightarrow{\theta_3} & H^1(K,H) \\ \downarrow{\scriptstyle \delta_1} & & \downarrow{\scriptstyle \delta_2} & & \downarrow{\scriptstyle \delta_3} & & \downarrow{\scriptstyle \delta_4} \\ \prod_{v\in V^K} H_{K_v} & \xrightarrow{\varrho_1} & \prod_{v\in V^K} S_{K_v} & \xrightarrow{\varrho_2} & \prod_{v\in V^K} H^1(K_v,G) & \xrightarrow{\varrho_3} & \prod_{v\in V^K} H^1(K_v,H). \end{array}$$

As before, for any ξ in $\ker \delta_3$, the injectivity of δ_4 implies that $\xi = \theta_2(x)$, for suitable $x \in S_K$; moreover, the commutativity of (6.42) yields that $\delta_2(x) \in \operatorname{im} \varrho_1$. To prove ξ trivial we need to show that $x \in \operatorname{im} \theta_1$. Thus, the proof is completed by the following unitary version of Eichler's theorem.

THEOREM 6.28. *Let $y \in L^*$ and $N_{L/K}(y) = 1$. Assume that for all v in V^K the equation $\mathrm{Nrd}_{A/L}(x) = y$ has a solution x_v in $A \otimes_K K_v$ such that $x_v \tau(x_v) = 1$. Then this equation has a solution x in A^* such that $x\tau(x) = 1$.*

The rest of this section is devoted to proving Theorems 6.27 and 6.28. We begin the proof of Theorem 6.27 by reducing it to the case $\mathrm{Nrd}_{A/L}(y) = 1$. We have $a = \mathrm{Nrd}_{A/L}(y) \in L^\tau = K$; moreover, for any v in V^K, setting $t_v = \mathrm{Nrd}_{A\otimes_K K_v/L\otimes_K K_v}(x_v)$, we obtain

$$a = t_v \tau(t_v) \in N_{L\otimes_K K_v/K_v}((L \otimes_K K_v)^*).$$

Since the Hasse principle holds for L/K, it follows that $a \in N_{L/K}(L^*)$, i.e., $a = t\tau(t)$ for suitable t in L^*.

We shall show that t can be chosen in such a way that $t \in \mathrm{Nrd}_{A/L}(A^*)$. Indeed, by Eichler's theorem it suffices to show that

$$t \in \mathrm{Nrd}_{A\otimes_L L_w/L_w}((A \otimes_L L_w)^*)$$

for each w in V^L_∞, or, equivalently,

$$t \in U_v = \mathrm{Nrd}_{A\otimes_K K_v/L\otimes_K K_v}((A \otimes_K K_v)^*)$$

for each v in V^K_∞. We have $a = t\tau(t) = t_v\tau(t_v)$, where

$$t_v \in \mathrm{Nrd}_{A\otimes_K K_v/L\otimes_K K_v}(x_v) \in U_v.$$

Then $z_v = tt_v^{-1} \in S_{K_v}$, where $S = \mathbf{R}^{(1)}_{L/K}(\mathbb{G}_m)$, and therefore by the weak approximation theorem for S one can find z in $S_K \cap \prod_{v\in V^K_\infty} z_v(S_{K_v} \cap U_v)$. Putting $t' = tz^{-1}$, we obtain $a = t\tau(t) = t'\tau(t')$ and $t' \in U_v$ for all v in v^K_∞, as desired.

Thus, let $t = \mathrm{Nrd}_{A/L}(b)$, for some $b \in A^*$. Then, taking $y' = b^{-1}y\tau(b^{-1})$, we have $\mathrm{Nrd}_{A/L}(y') = \mathrm{Nrd}_{A/L}(b^{-1}y\tau(b^{-1})) = t^{-1}a\tau(t^{-1}) = 1$. If we can show that $y' = x\tau(x)$ for some x in A^*, then $y = tx\tau(x)\tau(t) = (tx)\tau(tx)$, so we have the desired reduction.

The next step in the argument is to look for a solution of $y = x\tau(x)$ not in A but in $L(y)$. Thus the problem reduces to establishing that y belongs to $N_{L(y)/K(y)}(L(y)^*)$. But $L(y)/K(y)$ has degree 2, and therefore satisfies the Hasse norm principle; hence it suffices to establish that y is a norm over all completions with respect to all w in $V^{K(y)}$. This, as one easily sees, is equivalent to $y \in N_{L(y)\otimes_K K_v/K(y)\otimes_K K_v}(L(y) \otimes_K K_v)$ for all v in V^K. To realize this situation we must pass from y to $y' = ty\tau(t)$, for suitable t in $SL_1(A)$, which is permissible since either y and y' can both be written as $x\tau(x)$, for suitable $x \in A^*$, or neither can be written in this form.

LEMMA 6.24. *Suppose $y \in SL_1(A)$ is symmetric. If $y = x\tau(x)$ has a solution x_v in $A \otimes_K K_v$ $(v \in V^K_f)$, then this equation also has a solution z_v in $SL_1(A \otimes_K K_v)$.*

PROOF: It suffices to find t_v in $A \otimes_K K_v$ such that $t_v\tau(t_v) = 1$ and $\mathrm{Nrd}_{A\otimes_K K_v/L\otimes_K K_v}(t_v) = \mathrm{Nrd}_{A\otimes_K K_v/L\otimes_K K_v}(x_v^{-1})$. To do so, we shall consider separately the two cases $L \otimes_K K_v \simeq K_v \oplus K_v$ and $L \otimes_K K_v$ is a field.

In the first case $A \otimes_K K_v \simeq A_1 \oplus A_2$ is the direct sum of two simple algebras, where there is an anti-isomorphism $\varphi\colon A_1 \to A_2$ between them; moreover, we may assume that the K_v-linear extension of τ is given by

$$\tau((a,b)) = (\varphi^{-1}(b), \varphi(a)).$$

It follows that the t_v in $A \otimes_K K_v$ satisfying $t_v\tau(t_v) = 1$ have the form $t_v = (a, \varphi(a)^{-1})$, $a \in A_1^*$, and by §1.4.3 the values of the reduced norm on such elements comprise $X = \{(s, s^{-1}) : s \in K_v^*\}$. It remains to note that $\mathrm{Nrd}_{A\otimes_K K_v/L\otimes_K K_v}(x_v)$ lies in X, by virtue of the conditions $y \in SL_1(A)$ and $y = x_v\tau(x_v)$.

In the second case $A_w = A \otimes_K K_v$ is a full matrix algebra over $L_w = L \otimes_K K_v$, and one can choose an isomorphism $A_w \xrightarrow{\sim} M_n(L_w)$ such that τ can be written as $\tau((x_{ij})) = a\tau(x_{ji}))a^{-1}$, where $a = \mathrm{diag}(a_1, \ldots, a_n)$, $a_i \in K_v^*$. Then for t_v we can take a matrix of the form $\mathrm{diag}(d, 1, \ldots, 1)$, where $d = \mathrm{Nrd}_{A_w/L_v}(x_v)^{-1}$. Note that since $y \in SL_1(A)$ and $y = x_v\tau(x_v)$, we have $d\tau(d) = 1$; hence $t_v\tau(t_v) = 1$, proving the lemma.

Now we shall complete the proof of Theorem 6.27. Let us fix some τ-invariant order in A, so that one can speak properly of integral points. Let S_0 be a finite subset of V^K containing all the Archimedean valuations, as well as those non-Archimedean valuations for which either y is not a unit or L/K is ramified. For each v in S_0 fix a solution z_v in $SL_1(A \otimes_K K_v)$ of $y = x\tau(x)$.

We claim that there are open subsets W_v of $SL_1(A \otimes_K K_v)$ such that $t_v y \tau(t_v)$ is a square in $K_v[t_v y \tau(t_v)]$ for each t_v in W_v. Indeed, let us consider the algebraic group $F = SL_1(A \otimes_K \bar{K})$ (noting that $F = \mathbf{R}_{L/K}(\mathbf{SL}_1(A))$), and let Φ denote the set of τ-symmetric elements of F. Clearly Φ contains regular semisimple elments, and the subset Φ_0 of such elements is a nonempty Zariski-open subset of Φ Since $F \xrightarrow{\varphi} \Phi$, given by $\varphi(t) = t\sigma(t)$, is obviously surjective, it follows that $F_0 = \{ t \in F : ty\tau(t) \in \Phi_0 \}$ is a nonempty Zariski-open subset of F. However, Proposition 3.3 implies that the map $\Phi_{K_v} \to \Phi_{K_v}$, given by $p \mapsto p^2$, is open; in particular, there exists a neighborhood of the identity $U_v \subset \Phi_{K_v}$ contained in $\Phi_{K_v}^2$. We shall show that the $W_v = F_0 \cap (\varphi^{-1}(U_v) z_v^{-1})$ are the desired sets. (Lemma 3.2 implies that W_v are nonempty.) By construction we have $y' = t_v y \tau(t_v) \in U_v \cap \Phi_0$, for t_v in W_v. Thus $y' = s^2$ for some s in Φ_{K_v}, and $(L \otimes_K K_v)[y']$ is a maximal semisimple commutative subalgebra of $A \otimes_K K_v$. It follows that $s \in (L \otimes_K K_v)[y']$; and since $\tau(s) = s$, indeed $s \in K_v[y']$, as desired.

With the Chebotarev density theorem, we now choose a valuation $v_0 \notin S_0$ for which $L \otimes_K K_{v_0} \simeq K_{v_0} \oplus K_{v_0}$ and, moreover, $A \otimes_K K_{v_0}$ is the direct sum of two matrix algebras over K_{v_0}. Then $F_{K_{v_0}}$ is noncompact, and therefore one can apply strong approximation (Theorem 7.13) to F and $\{v_0\}$. (Note that the proof of Theorem 7.13, given by Platonov [4] and presented here in §7.4, does not use any results from cohomology over number fields.) It follows from this theorem that there exists t in F such that $t \in W_v$ for $v \in S_0$, and $t \in F_{\mathcal{O}_v}$ for $v \notin S_0 \cup \{v_0\}$.

We shall show that t is the desired element, i.e., for $y' = ty\tau(t)$ and all v in V^K the condition

$$y' \in N_{L(y') \otimes_K K_v / K(y') \otimes_K K_v}(L(y') \otimes_K K_v) \tag{6.43}$$

is satisfied; which, as we noted above, enables us to complete the proof of Theorem 6.27. If $v \in S_0$, then by assumption y' is a square in $K(y') \otimes_K K_v$ and (6.43) is obvious. To verify the remaining cases, note that $L(y') \otimes_K K_v$ is a composite of L and $K(y') \otimes_K K_v$. Hence (6.43) is satisfied automatically if $L \otimes_K K_v \simeq K_v \oplus K_v$, in particular for $v = v_0$. Now suppose $v \notin S_0 \cup \{v_0\}$. Then, on the one hand, the extension $L(y') \otimes_K K_v / K(y') \otimes_K K_v$ evidently is unramified; but, on the other hand, y' is a unit with respect to v, and again condition (6.43) holds. This completes the proof of Theorem 6.27.

REMARK: The following observation greatly simplifies the verification of the conditions of Landherr's theorem: for v in V_f^K, a symmetric element y can be written as $y = x_v \tau(x_v)$, where $x_v \in A \otimes_K K_v$, if and only if $\mathrm{Nrd}_{A/L}(y) \in N_{L \otimes_K K_v / K}((L \otimes_K K_v)^*)$. To prove sufficiency, suppose $\mathrm{Nrd}_{A/L}(y) = N_{L \otimes_K K_v / K_v}(z)$, where $z \in L \otimes_K K_v$. We take t in $A \otimes_K K_v$ such that $\mathrm{Nrd}_{A \otimes_K K_v / L \otimes_K K_v}(t) = z$ and consider $y' = t^{-1} y \tau(t)$. It suffices to show that y' can be written as $y' = x_v \tau(x_v)$, where $x_v \in A \otimes_K K_v$. But this follows from the result, which we have already established, that $H^1(K_v, G) = 1$ for $G = \mathbf{SU}_n(f)$. Indeed, the map $\varphi: F \to \Phi$, introduced above, induces the exact sequence $1 \to G \to F \xrightarrow{\varphi} \Phi \to 1$ and the corresponding cohomological sequence

$$F_{K_v} \xrightarrow{\varphi} \Phi_{K_v} \to H^1(K_v, G).$$

Since $H^1(K_v, G) = 1$, it follows that $\varphi(F_{K_v}) = \Phi_{K_v}$, as desired.

PROOF OF THEOREM 6.28: The unitary version of the proof of Eichler's theorem can be found in Weyl [7]. Namely, one constructs an irreducible polynomial $f(t) = t^n + a_{n-1} t^{n-1} + \cdots + a_0$, over L, whose degree equals $\deg(A)$ (the square root of $\dim_L A$), $a_0 = (-1)^n y$, and such that the extension $P = L(x)$, where x is a root of f, can be embedded in A so that $x\tau(x) = 1$; then $\mathrm{Nrd}_{A/L}(x) = y$. The reader can easily see for himself that, without loss of generality, one can assume the local solutions x_v of $\mathrm{Nrd}_{A/L}(x) = y$ are semisimple regular elements of $\mathbf{R}_{L/K}(\mathbf{GL}_1(A))$. The required $f(t)$ can be constructed by taking a sufficiently close approximation of the characteristic polynomials $f_v(t)$ of the x_v for some finite set of valuations S. To clarify what we mean by "sufficiently close" some preliminary arguments are needed.

Let $\chi: \mathbb{A}^n \to \mathbb{A}^n$ be the regular map that sends $x = (x_1, \ldots, x_n)$ to the n-tuple of coefficients of $f(x,t) = \prod_{i=1}^{n} (t - x_i)$ (which, up to the sign, coincide with the elementary symmetric functions of $x_1, \ldots, x_n$).

LEMMA 6.25. *If all the coordinates of $x = (x_1, \ldots, x_n)$ are distinct, then the differential $d_x\chi$ is a linear isomorphism.*

PROOF: We must show that $d_x\chi$ is injective. Suppose $d_x\chi(X_1, \ldots, X_n) = 0$. In terms of dual numbers this means that

$$\prod_{i=1}^{n} (t - (x_i + \delta X_i)) = \prod_{i=1}^{n} (t - x_i), \quad \text{where } \delta^2 = 0.$$

Putting $t = x_i$, we obtain $\delta X_i \prod_{j \neq i} ((x_i - x_j) - \delta X_j) = 0$; and since $x_j \neq x_i$ for $i \neq j$, it follows that $X_i = 0$. The lemma is proved.

Now let us fix v in V^K and consider the K_v-variety

$$W = ((L \otimes_K K_v)[x_v]) \otimes_{K_v} \bar{K}_v$$

together with the regular map $\chi: W \to B = (L \otimes_K \bar{K}_v)^n$, which sends an element to the coefficients of the corresponding characteristic polynomial. It follows from Lemma 6.25 that $d_z\chi$ is a linear isomorphism at a regular point z in W, which by Proposition 3.3 implies that

$$\chi_v: (L \otimes_K K_v)[x_v] \to (L \otimes_K K_v)^n$$

is open at any regular point.

An alternate proof of Krasner's lemma (cf. §6.4) is easily obtained along these lines. For our purposes we need its unitary version. Let X denote the subvariety of W consisting of unitary elements with respect to τ, and let Y denote the subvariety of B consisting of n-tuples $(a_0, \dots, a_{n-1})$ satisfying

$$\tau(a_0)a_0 = 1, \qquad a_0\tau(a_i) = a_{n-i}, \qquad i = 1, \dots, n-1. \tag{6.44}$$

If the characteristic polynomial of x has the form

$$f(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_0,$$

then the characteristic polynomials of x^{-1} and $\tau(x)$ have the form

$$t^n + a_1a_0^{-1}t^{n-1} + \cdots + a_0^{-1} \quad \text{and}$$
$$t^n + \tau(a_{n-1})t^{n-1} + \cdots + \tau(a_0),$$

respectively. It follows that χ induces a morphism $\chi^*: X \to Y$, and it is easy to compute that X and Y both have dimension n. Clearly X is a (multiplicative) algebraic group, and in particular, a smooth variety. Also, straightforward verification shows that Y is smooth. Furthermore, for z in X, $d_z\chi^*$ is the restriction of $d_z\chi$ to the tangent space T_zX and hence is a linear isomorphism to $T_{\chi^*(z)}Y$, in case z is regular. Applying Proposition 3.3, we see that $\chi_v^*: X_{K_v} \to Y_{K_v}$ is open at any regular point. In particular, one can find a neighborhood $U_v \subset Y_{K_v}$ of $a_v = \chi_v^*(x_v)$ such that for any a in U_v there is a regular element x in X_{K_v} for which $\chi_v^*(x) = a$.

This can be restated in the spirit of Krasner's classic lemma, in terms of characteristic polynomials. Let the characteristic polynomial of x_v have the form $f_v(t) = t^n + a_{n-1}^v t^{n-1} + \cdots + a_0^v$. Then if $f(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_0$ is sufficiently close to f_v, in the sense that its corresponding n-tuple $a = (a_0, \dots, a_{n-1})$ lies in the neighborhood U_v of $a_v = (a_0^v, \dots, a_{n-1}^v)$ constructed above, and if the conditions in (6.44) are satisfied, then there exists a root $x \in (L \otimes_K K_v)[x_v]$ of f such that $(L \otimes_K K_v)[x] = (L \otimes_K K_v)[x_v]$ and $x\tau(x) = 1$.

Now we choose a finite set S with respect to which we shall make an approximation of the f_v.

LEMMA 6.26. *There exists a finite subset S_0 of V^K containing V_∞^K such that, for $v \notin S_0$, any n-dimensional commutative semisimple $L \otimes_K K_v$-algebra B_v with involution, whose restriction to L is τ, can be embedded in $A \otimes_K K_v$ as the algebra with involution.*

PROOF: It is well known (cf. Theorem 6.7), that $G = \mathbf{SU}_n(f) = \mathbf{SU}(A, \tau)$ is K_v-quasisplit for almost all v in V_f^K. Then, as Proposition 6.19 and the above arguments imply, any algebra with involution of degree n over $L \otimes_K K_v$ can be embedded in $(A \otimes_K K_v, \tau)$. Therefore, for S_0 we can take the union of V_∞^K with the set of those non-Archimedean v for which G is not K_v-quasisplit. The lemma is proved.

Let us take two more valuations, v_1, v_2 in $V^K \setminus S_0$, having the properties that $L \otimes_K K_{v_i}$ is a field for $i = 1, 2$, and $L \otimes_K K_{v_1}/K_{v_1}$ is unramified. Let B_{v_1} denote the algebra $L \otimes_K E$, where E is an unramified extension of K_{v_1} of degree n, endowed with involution σ_1 defined by $\sigma_1 \mid_L = \tau \mid_L$ and $\sigma_1 \mid_E = \mathrm{id}$. Let us also take the algebra $B_{v_2} = (L \otimes_K K_{v_2})^n$, endowed with involution σ_2, which on each component is induced by τ. We shall show that there exist x_i in B_{v_i} $(i = 1, 2)$ satisfying the following:

$$N_{B_{v_i}/L\otimes_K K_{v_i}}(x_i) = y, \quad B_{v_i} = (L \otimes_K K_{v_i})[x_i] \quad \text{and} \quad \sigma_i(x_i)x_i = 1.$$

This is obvious for $i = 2$, so we consider the case $i = 1$. Using Hilbert's Theorem 90, we can write $y = \tau(z)z^{-1}$, where, since $L \otimes_K K_{v_1}$ is unramified over K_{v_1}, without loss of generality we may take z to be a v_1-unit in $(L \otimes_K K_{v_1})^*$. Since E/K_{v_1} is unramified, one can find t in B_{v_1} such that $N_{B_{v_1}/L\otimes_K K_{v_1}}(t) = z$. Then $s = \sigma_1(t)t^{-1}$ will satisfy $N_{B_{v_1}/L\otimes_K K_{v_1}}(s) = y$ and $\sigma_1(s)s = 1$. To obtain x_{v_1} it remains to multiply s by a unitary element with norm 1 to make it regular. Since $v_i \notin S_0$, there exist embeddings of the B_{v_i} in $A \otimes_K K_{v_i}$ as algebras with involutions, so henceforth we may view the B_{v_i} as subalgebras of $A \otimes_K K_{v_i}$.

Now we can easily complete our construction of f. Put $S = S_0 \cup \{v_1, v_2\}$, and for each v in S take the corresponding x_v, where for $v = v_i$ we assume that x_v is the x_i constructed above; and let

$$f^v(t) = t^n + a_{n-1}^v t^{n-1} + \cdots + a_0^v$$

be its characteristic polynomial. Then (6.44) holds for its coefficients; moreover, $a_0^v = (-1)^n y$. Put $a_0 = (-1)^n y$ in (6.44); then for the remaining coefficients we obtain a system of linear equations with coefficients in K. Therefore, using the weak approximation property for K, one can find a tuple $(a_0, \dots, a_{n-1})$ in L^n satisfying (6.44), with $a_0 = (-1)^n y$, which for each v in S is sufficiently close to $(a_0^v, \dots, a_{n-1}^v)$ in the sense indicated above.

Let $P = L[t]/(f(t))$, where $f(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_0$, and let x denote the image of t in P. Define an involution σ of P as follows: the restriction of σ to L is τ, and $\sigma(x) = x^{-1}$. (Such an involution exists, by virtue of the conditions in (6.44).) It remains to show there is an L-embedding $\theta: P \to A$ as an algebra with involution, since then $\theta(x)$ will be the desired element.

To do so, note that our construction implies, firstly, that for all v in V^K there exist embeddings $\theta_v: P \otimes_K K_v \to A \otimes_K K_v$ as algebras with involution; and secondly, that there exists an embedding $\varepsilon: P \to A$ as an algebra without involution. Indeed, the existence of θ_v for $v \notin S_0$ follows from Lemma 6.26. To establish the existence of θ_v for $v \in S_0$, it suffices to find x'_v in $A \otimes_K K_v$ such that $f(x'_v) = 0$, $[(L \otimes_K K_v)[x'_v] : L \otimes_K K_v] = n$, and $\tau(x'_v)x'_v = 1$. But by our set-up such an element can already be found in $(L \otimes_K K_v)[x_v]$. Using the criterion for embeddibility of a field as a maximal subfield in a simple algebra (cf. §1.5.1), we can show easily that the existence of ε follows from the existence of θ_v, once it is established that P is a field.

Consider the K-algebra of fixed points $F = P^\sigma$. By assumption

$$P \otimes_K K_{v_1} \overset{\theta_{v_1}}{\xrightarrow{\sim}} (L \otimes_K K_{v_1})[x_1] \simeq L \otimes_K E,$$

from which it follows that $F \otimes_K K_{v_1} \simeq E$ is an unramified extension of degree n of K_{v_1}; in particular, F is a field. Let us embed F in the algebraic closure $\bar{K}$ of K and show that the normal closure M of F satisfies $M \cap L = K$. To do so we use v_2. By assumption

$$\begin{aligned} P \otimes_K K_{v_2} &= (F \otimes_K L) \otimes_K K_{v_2} \\ &= (F \otimes_K K_{v_2}) \otimes_{K_{v_2}} (L \otimes_K K_{v_2}) \simeq (L \otimes K_{v_2})^n; \end{aligned}$$

hence $F \otimes_K K_{v_2} \simeq K_{v_2}^n$, yielding $M \subset K_{v_2}$, while $[L \otimes_K K_{v_2} : K_{v_2}] = 2$. In particular $P = F \otimes_K L = FL$ is a field.

Let us identify P with a subalgebra of A by means of ε, and extend σ to an involution of all of A, which we also denote as σ. Then there exists a symmetric element t in A^* such that $\sigma(z) = t\tau(z)t^{-1}$ for all z in A (cf. Lemma 2.10). By the Skolem-Noether theorem, any other embedding of P in A has the form $x \mapsto s^{-1}xs$, $s \in A^*$, so our problem reduces to realizing the choice of s in such a manner that the embedding obtained be compatible with the involutions, i.e., $s\sigma(z)s^{-1} = \tau(szs^{-1})$ for all z in P. Easy computation shows that the last condition is equivalent to $s\tau(s)t^{-1} \in Z_A(P) = P$. Thus, we must find b in P^* for which $s\tau(s) = bt$ has a solution s in A^*. To do so, according to Landherr's theorem it suffices

to choose b in P^* such that there exist local solutions s_v in $(A \otimes_K K_v)^*$. In this regard, as we noted after the proof of Landherr's theorem, for v in V_f^K, the condition for the solvability of $s\tau(s) = bt$ in $A \otimes_K K_v$ (assuming that $\tau(bt) = bt$) can be written as $\mathrm{Nrd}_{A/L}(bt) \in N_{L \otimes_K K_v/K_v}((L \otimes_K K_v)^*)$. Thus, it remains to find b in P, such that

$$\mathrm{Nrd}_{A/L}(bt) \in N_{L/K}(L^*) \tag{6.45}$$

$$\tau(bt) = bt \tag{6.46}$$

are satisfied and, in addition, $s\tau(s) = bt$ is solvable in $A \otimes_K K_v$ for v in V_∞^K. Condition (6.46) is equivalent to $\sigma(b) = b$, i.e., $b \in F$. Then (6.45) can be rewritten as

$$r = \mathrm{Nrd}_{A/L}(t) \in N_{F/K}(b)^{-1}N_{L/K}(L^*). \tag{6.47}$$

In this regard, the existence of θ_v implies that the corresponding local problem can be solved throughout, i.e., for any v in V^K one can find b_v in $(F \otimes_K K_v)^*$ for which $s\tau(s) = b_v t$ has a solution s_v in $(A \otimes_K K_v)$. In particular,

$$r \in N_{F \otimes_K K_v/K_v}((F \otimes K_v)^*)N_{L \otimes_K K_v/K_v}((L \otimes K_v)^*). \tag{6.48}$$

Now we shall use the fact that the multinorm Hasse principle holds for the pair of fields F, L, since the conditions of Proposition 6.11 are satisfied. (The fact that the normal closure of F intersects L in K was established above, and the validity of the norm principle for L/K follows from Hasse's theorem.) Therefore (6.48) implies that

$$r = N_{F/K}(b_0)^{-1}N_{L/K}(l_0) \tag{6.49}$$

for suitable b_0 in F^* and l_0 in L^*.

To complete the argument it remains to construct b in F^* and l in L^* such that again $r = N_{F/K}(b)N_{L/K}(l)$ but also $s\tau(s) = bt$ be solvable in $(A \otimes_K K_v)^*$ for v in V_∞^K. For each v in V^K the set Φ_v of elements of the form $s\tau(s)$, where $s \in (A \otimes_K K_v)^*$, is open in the set Σ_v of symmetric elements. Therefore, if $s\tau(s) = b_v t$ is solvable, then also $s\tau(s) = bt$ is solvable, for b in $F \otimes_K K_v$ sufficiently close to b_v. It is also clear that $r = N_{F \otimes_K K_v/K_v}(b_v)N_{L \otimes_K K_v/K_v}(l_v)$ for suitable l_v in $L \otimes_K K_v$. Thus, it suffices to prove the following

LEMMA 6.27. *Let*

$$X_v = \{\,(b_v, l_v) \in (F \otimes_K K_v)^* \times (L \otimes_K K_v)^* : r = N_{F\otimes_K K_v/K_v}(b_v)^{-1} \cdot N_{L\otimes_K K_v/K_v}(l_v)\,\}.$$

Then $X = \{\,(b,l) \in F^* \times L^* : r = N_{F/K}(b)^{-1} N_{L/K}(l)\,\}$ *is dense in* $\prod_{v\in V_\infty^K} X_v$.

PROOF: The lemma asserts that the weak approximation property holds with respect to $S = V_\infty^K$ for the variety

$$C = \{\,(b,l) \in \mathbf{R}_{F/K}(\mathbb{G}_m) \times \mathbf{R}_{L/K}(\mathbb{G}_m) : r = N_{F/K}(b^{-1}) N_{L/K}(l)\,\}.$$

We have $c = (b_0, l_0) \in C_K$ (cf. (6.49)) and $C = cT$, where T is the subtorus of $\mathbf{R}_{F/K}(\mathbb{G}_m) \times \mathbf{R}_{L/K}(\mathbb{G}_m)$ given by $N_{F/K}(b) = N_{L/K}(l)$. In this regard, C_K being dense in C_S is equivalent to T_K being dense in T_S, i.e., to the weak approximation property holding for T. However, when $S = V_\infty^K$ this property holds for any torus (cf. Proposition 7.8). This completes the proof of Lemma 6.27, and along with it also Theorem 6.28.

EXERCISE:

(1) Modify the above arguments, given for the unitary case, to derive a proof of Eichler's norm theorem.
(2) Obtain the Hermitian analog of Theorem 6.28. More precisely, for y in K^*, show that $\mathrm{Nrd}_{A/L}(x) = y$ has a solution x in A^* such that $\tau(x) = x$, if for each v in V^K it has a solution x_v in $A \otimes_K K_v$ such that $\tau(x_v) = x_v$.

6.8. Proof of Theorems 6.4 and 6.6: Exceptional groups.

In this section we shall complete the proof of Theorems 6.4 and 6.6 for groups of type ${}^{3,6}D_4$, ${}^{1,2}E_6$, E_7, E_8, F_4 and G_2. Throughout this section G denotes a simply connected simple K-group of one of the above types, and G_0 denotes a quasisplit K-group of the same inner type as G.

First we look at the easiest case, groups of type G_2, and then reduce the case of groups of type F_4 to groups of type D_4.

GROUPS OF TYPE G_2: We begin by showing that if K is a local field or a totally imaginary number field, then $H^1(K, G_0) = 1$. Let $\xi \in H^1(K, G_0)$. Then by Proposition 6.19 there is a maximal K-torus T of G_0 such that ξ lies in the image of $H^1(K,T) \xrightarrow{\varphi} H^1(K, G_0)$. Let us show that this map is actually trivial. Let $R = R(T, G)$ be the corresponding root system, and let R_0 be the subset of long roots of R. The description of the root system of type G_2 (Table 9 in Bourbaki [4, Ch. 4–6]) implies that R_0 comprises a

closed subsystem of roots in R of type A_2. It follows that the subgroup H of G_0 generated by the root groups G_α, for α in R_0, is a simple group of type A_2. Furthermore, R_0 is clearly invariant under all automorphisms of R; therefore the automorphisms σ in $\mathrm{Gal}(\bar{K}/K)$ permute the groups G_α, $\alpha \in R_0$, and thus H is defined over K. Finally, an easy computation with the roots, omitted here, establishes that H satisfies the criterion for being simply connected (cf. Theorem 2.6), so H is simply connected.

The validity of Theorems 6.4 and 6.6 for the classical groups (cf. §6.7) implies that $H^1(K, H) = 1$. But φ clearly can be written as the composition of maps $H^1(K,T) \to H^1(K,H) \to H^1(K, G_0)$, and therefore is trivial. Thus $H^1(K, G_0) = 1$. Since G_0 is both simply connected and adjoint, this means that G_0 is a unique K-form of type G_2, i.e., any K-group of this type is split over K. Therefore, actually $H^1(K, G) = 1$ for any K-group G of type G_2.

It remains to show that the kernel of $H^1(K,G) \xrightarrow{\varrho} \prod_{v\in V_\infty^K} H^1(K_v, G)$ is trivial, for any number field K. This part of the argument is repeated, to one or another extent, for groups of all types except E_6 and is based on the following lemma, which we shall prove in general.

LEMMA 6.28. *Let G be a semisimple algebraic group defined over an arbitrary field K. Assume G contains a Borel subgroup B defined over a quadratic extension L/K, such that $T = B \cap \sigma(B)$ is a maximal K-torus of G (where σ is the generator of $\mathrm{Gal}(L/K)$). Then any cocycle ξ in $Z^1(L/K, G)$ is equivalent to some ξ' in $Z^1(L/K, T)$. Moreover, if K is a number field and ξ in $Z^1(L/K, G)$ represents an element of $\ker(H^1(K,G) \to \prod_{v\in V_\infty^K} H^1(K_v, G))$, then also ξ' in $Z^1(L/K, T)$ can be chosen to represent an element of $\ker(H^1(K,T) \to \prod_{v\in V_\infty^K} H^1(K_v, T))$.*

PROOF: ξ is given by a_σ in G_L such that $a_\sigma \sigma(a_\sigma) = 1$. Let H denote $\mathbf{R}_{L/K}(G)$. Then σ induces a K-automorphism of $H \simeq \mathbf{R}_{L/K}(G)$, which we shall also designate as σ. Consider the K-subvariety Z of H, given by $h\sigma(h) = 1$. Then the ξ in $Z^1(L/K, G)$ correspond to points from Z_K, and H acts on Z by $(h, z) \mapsto h^{-1} z \sigma(h)$; moreover this action is transitive and is defined over K. Since H_K is dense in H (Theorem 2.2), it follows that the set of cocycles equivalent to ξ comprises a Zariski-dense subset of Z. On the other hand, $T = B \cap \sigma(B)$ implies that $\sigma(B)$ is B^-, the opposite Borel subgroup for B.

Let U and U^- denote the unipotent radicals of B and B^- respectively. The Bruhat decomposition implies that the product morphism

$$\mu: U \times T \times U^- \to G$$

is an L-isomorphism onto an open subset W of G. It follows that some cocycle equivalent to ξ is given by b_σ in W_L. Let $b_\sigma = u_1 t u_2$, where $u_1 \in U_L$, $t \in T_L$, and $u_2 \in U_L^-$. Then the condition $\sigma(b_\sigma) = b_\sigma^{-1}$, the uniqueness of the Bruhat decomposition, and the fact that $\sigma(U) = U^-$ and $\sigma(U^-) = U$ imply the relations $\sigma(u_1) = u_2^{-1}$, $\sigma(u_2) = u_1^{-1}$ and $\sigma(t) = t^{-1}$. We shall show that the cocycle ξ' given by $a'_\sigma = t$ is the desired cocycle. Indeed, $a'_\sigma = t = u_1^{-1} u_1 t u_2 u_2^{-1} = u_1^{-1} b_\sigma \sigma(u_1)$, i.e., ξ' is equivalent to ξ in $Z^1(L/K, G)$.

A slight revision of this argument is necessary in order to obtain the ξ' in $Z^1(L/K, T)$ which gives an element of $\ker(H^1(K,T) \to \prod_{v \in V_\infty^K} H^1(K_v, T))$ for K a number field. Namely, let S denote the set of real v of K satisfying $L_w = LK_v \neq K_v$. By assumption, for each v in S there is a g_v in G_{L_w} satisfying $a_\sigma = g_v^{-1} \sigma(g_v)$. Let us consider $B = \mathbf{R}_{L/K}(T)$, a subvariety D of B giving cocycles of $Z^1(L/K, T)$, and an action of B on D analogous to the action described above of H on Z. Proposition 3.3 implies that there exists an open subset $\Delta_v \subset T_{L_w} \simeq B_{K_v}$ such that, for any $t \in \Delta_v$ with $t\sigma(t) = 1$, the cocycle in $Z^1(L_w/K_v, T)$ determined by t is trivial. It follows from the Bruhat decomposition that $F_v = U_{L_w} \Delta_v U_{L_w}^-$ is open in G_{L_w} in the w-adic topology. G_L is dense in $\prod_{v \in S, w|v} G_{L_w}$ by Proposition 7.9. However, if one chooses g sufficiently close to g_v^{-1}, then one can make $g^{-1} a_\sigma \sigma(g)$ arbitrarily close to 1. It follows that there exists g in G_L such that $b_\sigma = g^{-1} a_\sigma \sigma(g) \in F_v$ for all v in S. If $b_\sigma = u_1 t u_2$ is the corresponding Bruhat decomposition, then, as we saw above, the cocycle ξ' given by $a'_\sigma = t$ is equivalent to ξ. Moreover, by our construction $t \in \Delta_v$, so ξ' becomes trivial in $H^1(L_w/K_v, T)$. It remains to note that $L \subset K_v$ for v in $V_\infty^K \setminus S$, and ξ' is automatically trivial in $H^1(K_v, T)$. The lemma is proved.

Now we return to our K-group G of type G_2. Let $\xi \in \ker \varrho$ and $L = K(\sqrt{-1})$, $\mathrm{Gal}(L/K) = \langle \sigma \rangle$. As we have shown, ξ becomes trivial in $H^1(L, G)$, i.e., $\xi \in H^1(L/K, G)$, and G is L-split. Using Lemma 6.16, choose a Borel L-subgroup B of G such that $T = B \cap \sigma(B)$ is a maximal K-torus of G. By Lemma 6.25, passing to an equivalent cocycle, without loss of generality we may assume that $\xi \in \ker(H^1(K,T) \xrightarrow{\theta} \prod_{v \in V_\infty^K} H^1(K_v, T)$. But above we saw that any K-torus T of G is contained in a simply connected K-subgroup H of G of type A_2. Therefore, the validity of the Hasse principle for H implies that ξ is a trivial cocycle of $H^1(K, H)$, and hence also of $H^1(K, G)$.

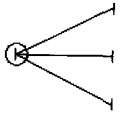
Note that a proof of Theorems 6.4 and 6.6 for G of type G_2 could have been obtained using a geometric realization of G as a group of automorphisms of the Cayley K-algebra of octonions; however we preferred to use a structural approach, especially since it contains several typical points.

GROUPS OF TYPE F_4: This type can be reduced to groups of type D_4, just as G_2 was reduced to A_2. First, let K be a local or totally imaginary number field, and let $\xi \in H^1(K, G_0)$. With Proposition 6.19 we find a maximal K-torus T of G_0 such that ξ lies in the image of $H^1(K,T) \to H^1(K, G_0)$. Now let us assume that Theorems 6.4 and 6.6 have been proved for groups of type D_4 (including outer forms of types ${}^3D_4$ and ${}^6D_4$). To prove that ξ is trivial it suffices to show G has a simply connected K-subgroup $H \supset T$ of type D_4. But the explicit description of the root system of type F_4 (cf. Bourbaki [4, Table 8]), implies that these requirements are met by the subgroup generated by the root subgroups G_α, where α runs through all the long roots of $R(T, G)$. Here, too, G_0 is both simply connected and adjoint; therefore the triviality of $H^1(K, G_0)$ implies that any K-group G of type F_4 is split, and consequently $H^1(K, G) = 1$.

The proof of the Hasse principle for a group G of type F_4 over a number field K which is not totally imaginary is a verbatim repetition of the corresponding argument for groups of type G_2.

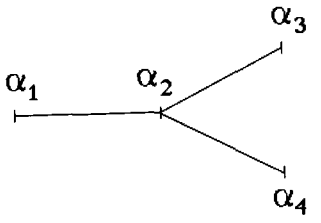
GROUPS OF TYPES ${}^{3,6}D_4$: As before, we show first that $H^1(K, G_0) = 1$ if K is a local field or a totally imaginary number field. Let $\xi \in H^1(K, G_0)$ and $G = {}_\xi G_0$. We wish to establish that G is K-quasisplit, i.e., that $G \simeq G_0$. Suppose the contrary. Then there are two possibilities: G is isotropic over K, and G is anisotropic over K.

In the first case the only possible index for G is the following:



(cf. Tits [2]). Let S denote a maximal K-split torus of G, and let T be a maximal K-torus of its centralizer $C = C_G(S)$. By Proposition 6.18, $G_0 =_\mu G$ for a suitable μ in $H^1(K, T)$. Therefore it suffices to show that $H^1(K, C) = 1$. But the semisimple part $H = [C, C]$ is a simply connected K-group of type $A_1 \times A_1 \times A_1$, and therefore $H^1(K, H) = 1$. On the other hand, C/H is a one-dimensional K-split torus, so $H^1(K, C/H) = 1$. Therefore, the exact sequence $H^1(K, H) \to H^1(K, C) \to H^1(K, C/H)$ implies that $H^1(K, C) = 1$, as desired.

Now suppose G is K-anisotropic. Let L denote the minimal Galois extension of K over which G_0 becomes an inner form. Then $\mathcal{G} = \mathrm{Gal}(L/K)$ is either cyclic of order 3, or the symmetric group S_3. Let us examine the first case. Since G_0 becomes a group of type ${}^1D_4$ over L, by what we have already proved $H^1(L, G_0) = 1$; hence $G \simeq G_0$ is a split group over L. Let us label the simple roots of an L-split torus in the following way:



and let P denote the parabolic L-subgroup P_Δ where $\Delta = \{\alpha_2, \alpha_3, \alpha_4\}$. Simple calculation shows that $\dim G = 28$ and $\dim P = 22$, i.e., P has codimension 6. Let σ be a generator of $\mathcal{G}$. Put $C = P \cap \sigma(P) \cap \sigma^2(P)$. Clearly C is a K-subgroup and is reductive, since G is K-anisotropic. Moreover, $\dim C \geq \dim G - 3 \operatorname{codim} P = 10$.

Let us describe the structure of C. Let $H = [C, C]$ be the semisimple part of C. By assumption H must be contained in the semisimple part P' of P, which is a simple L-split group of type A_3. Moreover, since Theorems 6.4 and 6.6, and hence also Theorems 6.5 and 6.25, have already been proved for groups of smaller dimension, it follows in view of H being K-anisotropic that all its simple components have type A_l, and therefore the only possible types for H are: A_1, $A_1 \times A_1$, A_2, and A_3. The first two cases cannot occur because of the dimensions of the groups involved, and the last because H here must be P' and consequently is a K-anisotropic group of type A_3 which becomes split over a cubic extension of K, which is impossible. Thus, H must have type A_2, so $\dim H = 8$, which means $C = HS$ is an almost direct product, where S is a 2-dimensional K-torus.

We claim S is L-split. Otherwise let S_0 denote a maximal L-split subtorus of S. It follows from our set-up that $S_0 \neq (e)$, and therefore it remains to exclude the possibility of $\dim S_0 = 1$. Since L/K is a Galois extension, S_0 is defined over K and consequently has the form $S_0 = \mathbf{R}^{(1)}_{E/K}(\mathbb{G}_m)$, where E/K is a quadratic extension. But such a torus remains anisotropic over L, contradiction.

Now, embedding S in a maximal L-split torus and noting that $H \subset Z_G(S)$, we also obtain that H is L-split. In particular, H is an inner form over K, since $[L : K] = 3$, i.e., $H = \mathbf{SL}_1(D)$, where D is a skew field of index 3 over K such that $D \otimes_K L = M_3(L)$. The latter implies that L can be embedded in D and consequently defines a maximal L-split K-torus $S' = \mathbf{R}^{(1)}_{L/K}(\mathbb{G}_m) \subset H$. Then $T = SS'$ is a maximal K-torus of C and G which is anisotropic over K and split over L. It follows that for any character χ in $\mathbf{X}(T)$ we have $\chi + \sigma(\chi) + \sigma^2(\chi) = 0$. Therefore, for any root α in $R(T, G)$, the group G_{Σ_α}, generated by the root groups G_γ for γ in $\Sigma_\alpha = \{\alpha, \sigma(\alpha)\}$, is a simply connected K-group of type A_2. Put $T_{\Sigma_\alpha} = T \cap G_{\Sigma_\alpha}$, and take two roots α, β in $R(T, G)$ such that $T = T_{\Sigma_\alpha} \times T_{\Sigma_\beta}$.

(The reader should verify that such roots exist.) We have $G_0 = {}_\mu G$ for suitable $\mu = \{a_\tau\}$ in $H^1(K, T)$, by Proposition 6.18. We wish to show that μ is trivial in G. Let $\mu_\alpha = \{a^\alpha_\tau\} \in H^1(K, T_{\Sigma_\alpha})$ and $\mu_\beta = \{a^\beta_\tau\} \in H^1(K, T_{\Sigma_\beta})$ be the projections of μ on T_{Σ_α} and T_{Σ_β}, respectively. Since $H^1(K, G_{\Sigma_\beta}) = 1$, it follows that $a^\beta_\tau = g^{-1}\tau(g)$ for suitable g in G_{Σ_β}. We have $b_\tau = g a_\tau \tau(g)^{-1} = g a^\alpha_\tau g^{-1} \in F = g G_{\Sigma_\alpha} g^{-1}$. It remains to establish that F is defined over K, since then $H^1(K, F) = 1$ and $\{b_\tau\}$ is trivial in G. For an arbitrary τ in $\operatorname{Gal}(\bar{K}/K)$ we have

$$\tau(F) = \tau(g) G_{\Sigma_\alpha} \tau(g)^{-1} = g a^\beta_\tau G_{\Sigma_\alpha} (a^\beta_\tau)^{-1} g^{-1} = F,$$

since a^β_τ in T_{Σ_β} normalizes G_{Σ_α}. Thus, the isomorphism $G \simeq G_0$ is established for $[L : K] = 3$.

Now assume $\mathcal{G} = \operatorname{Gal}(L/K) \simeq S_3$. Let E denote a quadratic extension of K contained in L. By what has been shown, G becomes quasisplit over E. But then, as in the proof of Theorem 6.26, it can be established that G is isotropic over K, and the isotropic case has already been handled.

Thus, in all cases $G = {}_\xi G_0 \simeq G_0$. This means that ξ projects onto the trivial cocycle in the corresponding adjoint group, i.e., ξ lies in $H^1(K, Z)$, where Z is the center of G_0. But then $\xi \in H^1(K, T_0)$, where T_0 is a maximal torus of a Borel K-subgroup of G_0. Analysis of the index

of G_0 shows that T_0 has the form $\mathbb{G}_m \times \mathbf{R}_{M/K}(\mathbb{G}_m)$, where $M \subset L$ is a subfield of degree 3 over K; so $H^1(K, T_0) = 1$ and, therefore, ξ is trivial in $H^1(K, G_0)$. This completes the proof that $H^1(K, G_0)$ is trivial.

Now let K be a local field. Since $H^1(K, G_0)$ has been proved trivial, Proposition 6.15 implies that any simply connected simple K-group G of type ${}^3D_4$ or ${}^6D_4$ is quasisplit over K, i.e., $G \simeq G_0$. Therefore $H^1(K, G) = H^1(K, G_0) = 1$, and Theorem 6.4 is proved.

To prove Theorem 6.6 we shall need

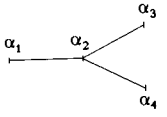
LEMMA 6.29. *Let G be a simply connected simple group of type ${}^{3,6}D_4$ over a number field K, and let E/K be the minimal Galois extension over which G becomes an inner form. Then there exists a quadratic extension L/K with the following properties:*

(1) *L and E are linearly disjoint over K;*
(2) *L is totally imaginary;*
(3) *G becomes quasisplit over L.*

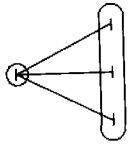
PROOF: Obtained by a straightforward modification of the argument in the proof of Proposition 6.15, and left to the reader as an exercise.

Now let $\xi \in \ker(H^1(K,G) \xrightarrow{\varrho} \prod_{v\in V_\infty^K} H^1(K_v,G))$, and let L/K be the extension given in Lemma 6.29. Since $G \simeq G_0$ over L, by what we have shown $H^1(L,G) = 1$; therefore $\xi \in H^1(L/K,G)$. Let B be a Borel L-subgroup of G such that $T = B \cap \sigma(B)$ is a maximal K-torus of G, where σ is the generator of $\mathrm{Gal}(L/K)$ (cf. Lemma 6.17). Applying Lemma 6.28, we see that by passing to an equivalent cocycle, we may assume that $\xi = \{a_\tau\} \in \ker(H^1(K,T) \to \prod_{v\in V_\infty^K} H^1(K_v,T))$. We shall need a description of the action of σ on the roots in $R(T,G)$.

More precisely, since the splitting field for T is LE, one should speak of the action of $\mathrm{Gal}(LE/K)$ on $\mathbf{X}(T)$, rather than the action of $\mathrm{Gal}(L/K)$. So, to define the action of σ first we have to extend σ to LE; and, since L and E are linearly disjoint, we may assume that this extension acts trivially on E, and we shall also denote it by σ. Since G becomes an inner form over E, it follows that σ must act on $\mathbf{X}(T)$ as an element of the Weyl group $W(T,G)$. On the other hand, since $T = B \cap \sigma(B)$, σ takes the positive roots associated with B to negative ones. But the only element in the Weyl group of the root system of type D_4 with this property is -1 (cf. Bourbaki [4, Table 4]). Therefore σ acts on $\mathbf{X}(T)$ by multiplication by -1. Let us label the simple roots of $R(T,G)$ as follows:



Since the index of G under L has the form



the description of the action of σ implies that the subgroups $G_1 = G_{\alpha_2}$ and G_2 generated by G_{α_i} $(i = 1,3,4)$ are defined over K. Put $T_i = T \cap G_i$. Then $T = T_1 \times T_2$, and one can apply the trick, used before, of "componentwise" trivialization of ξ. Namely, let $\xi_i = \{a_\tau^i\} \in H^1(K,T_i)$ be the projection of ξ on T_i. Clearly $\xi_i \in \ker(H^1(K,T_i) \to \prod_{v\in V_\infty^K} H^1(K_v,T_i))$.

Since G_2 is a group of type $A_1 \times A_1 \times A_1$, it satisfies the Hasse principle. This implies that ξ_2 defines a trivial cocycle in $H^1(K,G_2)$, i.e., $a_\tau^2 = g^{-1}\tau(g)$ for suitable g in G_2. Then $b_\tau = g a_\tau \tau(g)^{-1} = g a_\tau^1 g^{-1} \in F = gG_1g^{-1}$. As above, one can show that F and $T_1' = gT_1g^{-1}$ are defined over K. Furthermore, we claim that the morphism $\varphi: T_1 \to T_1'$ given by $t \mapsto gtg^{-1}$ is defined over K. Indeed, for any t in T_1 and any τ in $\mathrm{Gal}(\bar{K}/K)$ we have

$$(\tau\varphi)(t) = \tau(g)t\tau(g)^{-1} = g(g^{-1}\tau(g))t(g^{-1}\tau(g))^{-1}g^{-1} = gtg^{-1} = \varphi(t),$$

since $g^{-1}\tau(g) = a_\tau^2 \in T_2$; hence $\tau\varphi = \varphi$. It follows that $\xi_1' = \{b_\tau\} = \varphi(\xi_1)$ lies in $\ker(H^1(K,T_1') \to \prod_{v\in V_\infty^K} H^1(K_v,T_1'))$, and since the Hasse principle holds for F (F belongs to type A_1), ξ_1' is trivial in $H^1(K,F)$. But then ξ is trivial in $H^1(K,G)$, as desired.

GROUPS OF TYPE E_6, E_7, E_8 (PRELIMINARIES): The analysis of the preceding types was based on the fact that for the given group one can easily pick a maximal torus which can be embedded either entirely or componentwise in a group of smaller rank, for which Theorems 6.4 and 6.6 have already been proved. For groups of type E this method runs into considerable difficulty, since *a priori* one cannot find a splitting field having a relatively small degree over K. At best, in this situation, one can construct a splitting field in the form of a tower of 2-, 3- and 5- extensions. To do so, we need

PROPOSITION 6.21. *Let G be an arbitrary K-group of type E_6, E_7 or E_8, and let T be a maximal K-torus of G. Then the order of any element of $H^1(K,T)$ is of the form $2^\alpha 3^\beta$ if G is a group of type E_6 or E_7, and the form $2^\alpha 3^\beta 5^\gamma$ if G is a group of type E_8.*

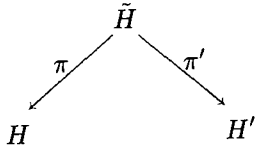
PROOF: Let L be a minimal splitting field of T, and let $\mathcal{G} = \mathrm{Gal}(L/K)$. Then $\mathcal{G}$ acts on $R = R(T,G)$ by automorphisms, thereby yielding a homomorphism from $\mathcal{G}$ to $\mathrm{Aut}(R)$ which is an embedding since the roots generate the vector space $\mathbf{X}(T) \otimes_{\mathbb{Z}} \mathbb{R}$. In our case $\mathrm{Aut}\, R$ is $W(R)$ if R is a system of type E_7 or E_8, and contains $W(R)$ as a subgroup of index 2 if R is a system of type E_6. The Weyl groups of these types of root systems have the following orders (cf. Bourbaki [4, Tables 5–7]): $|W(E_6)| = 2^7 \cdot 3^4 \cdot 5$, $|W(E_7)| = 2^{10} \cdot 3^4 \cdot 5 \cdot 7$, and $|W(E_8)| = 2^{14} \cdot 3^5 \cdot 5^2 \cdot 7$. Therefore one can assert immediately that the order of any element of $H^1(K,T)$ has the form $2^\alpha \cdot 3^\beta \cdot 5^\gamma$ for type E_6 and form $2^\alpha \cdot 3^\beta \cdot 5^\gamma \cdot 7^\delta$ for types E_7 and E_8. Our objective is to eliminate from these expressions the power of 5 for E_6 and E_7, and the power of 7 for E_7 and E_8. To this end, first we prove

LEMMA 6.30. *Let H be a K-group of type ${}^{1,2}D_n$ $(n \geq 4)$, and let S be a maximal K-torus of H. Then $H^1(K,S)$ is a 2-group.*

PROOF: It suffices to prove the lemma in the case where H is either $\mathbf{SO}_{2n}(f)$ or $\mathbf{SU}_n(D,f)$, i.e., is isomorphic over $\bar{K}$ to the special orthogonal

group; indeed, any H' of one of the given types occurs in a diagram

(6.50)



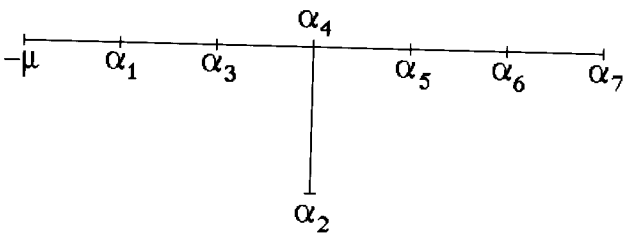
where π and π' are isogenies whose kernels are 2-groups; and then, for any K-torus S' of H' and any $p \neq 2$, the p-components of $H^1(K, S')$ and $H^1(K, S)$ are isomorphic, where $S = \pi((\pi')^{-1}(S'))$. In this case, S over $\bar{K}$ can be reduced to the form $\{ s = \mathrm{diag}(s_1, s_1^{-1}, \dots, s_n, s_n^{-1}) \}$, and therefore $\mathbf{X}(T) = \mathbb{Z}\varepsilon_1 \oplus \cdots \oplus \mathbb{Z}\varepsilon_n$, where $\varepsilon_i(s) = s_i$. In this situation $R(S, H)$ consists of $\pm\varepsilon_i \pm \varepsilon_j$ $(i \neq j)$, and $\mathrm{Aut}(R(S, H))$ consists of the transformations that send ε_i to $\pm\varepsilon_j$, i.e., is the semidirect product $A \cdot B$, where $B = \prod_{i=1}^{n} \{\pm 1\}$ and $A = S_n$ acts on ε_i by permuting indexes. We saw above that the Galois group $\mathcal{H} = \mathrm{Gal}(E/K)$ of the minimal splitting field E of S can be embedded in $\mathrm{Aut}(R(S, H))$; on the other hand, the lemma is equivalent to the claim that $H^1(\mathcal{H}_p, S)$ is trivial for any $p \neq 2$, where $\mathcal{H}_p$ is a Sylow p-subgroup of $\mathcal{H}$. Put $F = E^{\mathcal{H}_p}$. Since $p \neq 2$, $\mathcal{H}_p$ is conjugate in $\mathrm{Aut}(R(S, H))$ to a subgroup of A, and therefore there exists a base of $\mathbf{X}(S)$ on which $\mathcal{H}_p$ acts by permutation. It follows that S is quasisplit over F and therefore $H^1(\mathcal{H}_p, S) = H^1(E/F, S) = 1$. The lemma is proved.

Now we return to the proof of Proposition 6.21. We need to show that $H^1(\mathcal{G}_5, T) = 1$ for the systems of type E_6 and E_7, where $\mathcal{G}_5$ is a Sylow 5-subgroup of $\mathcal{G}$. Analysis of the Dynkin diagrams shows that in this case R contains a closed subsystem R_0 of type D_5. We have $[W(D_5)] = 2^8 \cdot 3 \cdot 5$; therefore, analyzing the orders given above of $W(E_6)$ and $W(E_7)$ we conclude that any Sylow 5-subgroup of $W(R_0)$ is simultaneously a Sylow subgroup of $W(R)$. It follows that $\mathcal{G}_5$ is conjugate to a subgroup of $W(D_5)$, which means one can always find a system $R_0 \subset R$ of type D_5 which is invariant with respect to $\mathcal{G}_5$. Let H be the subgroup of G of type D_5, generated by the root groups G_α for α in R_0. Clearly H is defined over $E = L^{\mathcal{G}_5}$. Put $S = T \cap H$. Then it follows from Lemma 6.30 that $H^1(L/E, S)$ is simultaneously a 2-subgroup and a 5-subgroup, and therefore is trivial. However $T_1 = T/S$ must either be one-dimensional or two-dimensional. Since $GL_1(\mathbb{Z})$ and $GL_2(\mathbb{Z})$ have no subgroups of order 5, T_1 is E-split. Therefore $H^1(L/E, T_1) = 1$, and we conclude from the exact sequence $H^1(L/E, S) \to H^1(L/E, T) \to H^1(L/E, T_1)$ that $H^1(L/E, T) = 1$, as desired.

Any root system of type E_8 contains a subsystem of type D_7; moreover $|W(E_8)_7| = |W(D_7)_7| = 7$, and by the analogous argument one can establish that $H^1(K, T)$ has no 7-elements.

A different argument is needed for the groups of type E_7. The extended Dynkin diagram for the system of type E_7 is as follows:

(6.51)



(where μ is the maximal root; cf. Bourbaki [4, Table 6]), and $-\mu$ and α_i $(i \neq 2)$ generate a closed subsystem R_0 of type A_7. Since $|W(E_7)_7| = |W(A_7)_7| = 7$, we may assume without loss of generality that R_0 is invariant with respect to $\mathcal{G}_7$. But then the root groups G_α for α in R_0 generate a subgroup H of type A_7 which contains T, is defined over $E = L^{\mathcal{G}_7}$, and is split over L. Now one can easily see from the description of groups of type A_n (cf. §2.3) that $H \simeq \mathbf{SL}_8$ over E, and consequently T is isomorphic to the multinorm torus associated with a set $P_1, \dots, P_l$ of extensions of K such that $\sum_{i=1}^{l} [P_i : E] = 8$. Since T becomes split over L, the only such torus which is not split over E is associated with the extensions L, E in the case where $[L : E] = 7$, and then $T \simeq \mathbf{R}_{L/E}(\mathbb{G}_m)$. In all cases $H^1(L/E, T) = 1$. This completes the proof of the proposition.

COROLLARY. *Let K be a perfect field and let $\mathrm{cd}_p(K) \leq 1$ for $p = 2, 3$. Then $H^1(K, G_0) = 1$ for any simply connected quasisplit K-group G_0 of type E_6 or E_7. If furthermore $\mathrm{cd}_5(K) \leq 1$, then also $H^1(K, G_0) = 1$ for G_0 of type E_8.*

Indeed, by Proposition 6.19, for any ξ in $H^1(K, G_0)$ one can find a maximal K-torus T of G_0 such that ξ lies in the image of $H^1(K, T) \to H^1(K, G_0)$. However, as we have just shown, the order of any element of $H^1(K, T)$ has the form $2^\alpha \cdot 3^\beta$ for types E_6 and E_7, and the form $2^\alpha \cdot 3^\beta \cdot 5^\gamma$ for type E_8. But, the conditions on cohomological dimension imply that $H^1(K, T)$ does not contain any nontrivial elements of this order (Lemma 6.20). Thus $H^1(K, T) = 1$, and hence $H^1(K, G_0) = 1$.

Let us apply the corollary to K_Π, where $\Pi = \{2, 3\}$ for types E_6, E_7, and $\Pi = \{2, 3, 5\}$ for type E_8. (Recall, that for a set Π of prime numbers, K_Π is the field obtained by adjoining to K the n-th roots of unity ζ_n for all n which are divisible only by primes from Π; cf. Proposition 6.20.) Then $\mathrm{cd}_p(K_\Pi) \leq 1$ for p in Π, by Proposition 6.20; and therefore any ξ in $H^1(K, G_0)$ becomes trivial over K_Π. In particular, there exists a finite

abelian extension L/K of degree $2^\alpha 3^\beta$ for types E_6, E_7, and of degree $2^\alpha 3^\beta 5^\gamma$ for type E_8, such that ξ becomes trivial in $H^1(L, G_0)$, i.e., lies in $H^1(L/K, G_0)$. One can arrange L/K in a tower $L = L_m \supset L_{m-1} \supset \cdots \supset L_1 \supset L_0 = K$, where each floor L_{i+1}/L_i has degree p, $p \in \Pi$. Therefore the triviality of $H^1(K, G_0)$ over a local or totally imaginary number field is obtained by iterative application of the following

THEOREM 6.29. *Let G_0 be a simply connected quasisplit simple group of type E_6, E_7 or E_8 over a field K, which is either a local or a totally imaginary number field. If L/K is a cyclic extension of degree p, where $p = 2, 3$ for types E_6 and E_7, and $p = 2, 3, 5$ for type E_8, then $H^1(L/K, G_0) = 1$.*

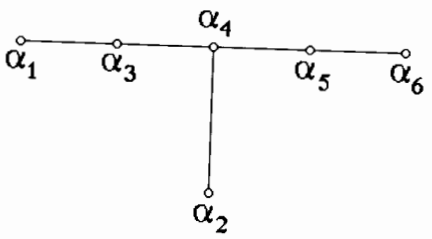
Now we shall analyze the cases $p = 2, 3$, thereby completing the proof of the triviality of $H^1(K, G_0)$ for groups of type E_6 and E_7. The case $p = 5$ for groups of type E_8 requires special consideration and will be taken up later. We argue by induction on the rank of the group. The induction is based on the following

PROPOSITION 6.22. *Hypotheses as in Theorem 6.29, let $\xi \in H^1(K, G_0)$ and let $G = {}_\xi G_0$. Assume G is K-isotropic and $H^1(K, H) = 1$ for any simply connected semisimple quasisplit K-subgroup H of G_0 of lower rank. Then $\xi = 1$.*

PROOF: First we suppose that G is an inner form, i.e., that G_0 has type other than ${}^2E_6$. Let S be a maximal K-split torus of G, and let T be a maximal K-torus of G containing S. Then by Proposition 6.19 there exists an embedding $T \to G_0$ defined over K, such that ξ lies in the image of $H^1(K, T) \to H^1(K, G_0)$. The latter map can be factored into the composition $H^1(K, T) \to H^1(K, C_0) \to H^1(K, G_0)$, where $C_0 = Z_{G_0}(S)$; therefore it suffices to show that $H^1(K, C_0) = 1$. To do so note that the K-embedding $T \to G_0$ constructed in Proposition 6.19 is induced by a $\bar{K}$-isomorphism $G \to G_0$; in particular C_0 and $C = Z_G(S)$ are isomorphic over $\bar{K}$. But the connected component of the center of C is S, since G is an inner form; thus the connected component of the center of C_0 also is S. Therefore $C_0 = HS$ is an almost direct product, where $H = [C, C]$ is the semisimple part of C_0, which is a simply connected semisimple split K-group. By hypothesis $H^1(K, H) = 1$. But C_0/H is a split torus, and therefore $H^1(K, C_0/H) = 1$. Thus, the exact sequence $H^1(K, H) \to H^1(K, C_0) \to H^1(K, C_0/H)$ yields $H^1(K, C_0) = 1$, as desired.

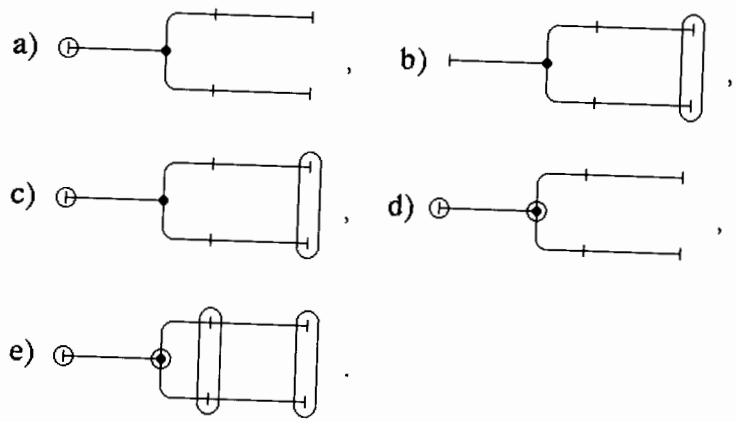
For groups of type ${}^2E_6$ this argument requires slight modification. In fact, it suffices to find a K-split torus S of G such that the connected component of the center of $C = Z_G(S)$ is S. Let S_0 be a maximal K-split torus of G and let T be a maximal K-torus of G containing S_0. Let us

label the simple roots of $R = R(T, G)$ as follows:
(6.52)



and list all the possibilities for the index of G (cf. Tits [2]):

(6.53)



In case (b) the anisotropic kernel has type D_4. But for groups of this type Theorems 6.4 and 6.6, and hence also Theorems 6.5 and 6.25, have already been proved; therefore such a group cannot be K-anisotropic. In other words, case (b) does not occur in the given situation. In the remaining cases put $S = (\bigcup_{i \neq 2} \ker \alpha_i)$. Since α_2 is a distinguished vertex throughout, S is a one-dimensional K-split torus; moreover, the semisimple part H of its centralizer C is a simple group of type A_5, so computation of the ranks yields $C = HS$, which means that the connected component of the center of C is S. The proposition is proved.

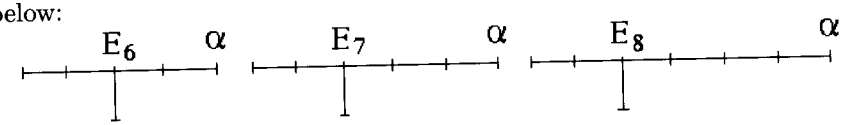
To apply Proposition 6.22 to our situation we need two lemmas.

LEMMA 6.31. *Let G be a simply connected simple group of type E_6, E_7 or E_8, defined over K and split over a quadratic extension L of K. Then G is K-isotropic.*

PROOF: Using Lemma 6.23, we choose a maximal L-split K-torus T of G. If we assume G is K-anisotropic, then the nonidentity automorphism σ of $\mathrm{Gal}(L/K)$ acts on $\mathbf{X}(T)$ by multiplication by -1. It follows that any root subgroup G_α generated by one-dimensional unipotent subgroups U_α and $U_{-\alpha}$ is defined over K. Let F be the subgroup generated by two root subgroups G_α and G_β for two adjacent roots α and β in a Dynkin diagram. Then F is a simply connected simple K-group of type A_2, split over L. The description of groups of type A_n implies that $F = \mathbf{SU}_3(f)$, where f is a nondegenerate three-dimensional Hermitian form associated with L/K. But since K by assumption is either local or totally imaginary, F is isotropic over K (cf. proof of Theorem 6.26), and hence G is K-isotropic.

LEMMA 6.32. *Let G be a simply connected simple group of type E_6, E_7 or E_8, defined over K and split over L, a cyclic extension of degree 3 of K. Then G is either K-isotropic or contains a proper semisimple K-subgroup of a type other than $A_{l_1} \times A_{l_2} \times \cdots \times A_{l_t}$.*

PROOF: Let T be a maximal L-split torus of G, let $R = R(T, G)$ be the corresponding root system, and let $\Pi \subset R$ be a system of simple roots. In each of the respective Dynkin diagrams we choose one root, as shown below:



Let P denote the standard parabolic L-subgroup P_Δ, where $\Delta = \Pi \setminus \{\alpha\}$, and put $C = P \cap \sigma(P) \cap \sigma^2(P)$. Clearly $\dim C \geq \dim G - 3\,\mathrm{codim}_G P$; therefore direct computation using the tables of root systems in Bourbaki [4] yields the following table:

Type R	$\dim G$	$\dim P$	$\dim C$
E_6	78	62	≥ 30
E_7	133	106	≥ 52
E_8	248	191	≥ 77

Now let us suppose G is K-anisotropic. Then C is reductive, since it is defined over K; i.e., $C = HS$, where $H = [C, C]$ is the semisimple part of C and S is its central torus. Let $H_1, \ldots, H_t$ be the absolutely simple components of H. We must show that not all the H_i have type A_n. We shall show that otherwise the estimates of $\dim C$ given in the table do not hold. Put $l_i = \mathrm{rank}\, H_i$, $s = \dim S$, and $r = \mathrm{rank}\, G$. Then clearly

$$\dim C = \sum_{i=1}^{t}((l_i + 1)^2 - 1) + s, \tag{6.54}$$

moreover

$$\sum_{i=1}^{t} l_i \leq \min(r - s, r - 1) := f. \tag{6.55}$$

Let d be the number of H_i's for which $l_i = 1$. Then, with (6.54) and (6.55), it is easy to obtain the following inequality:

$$\dim C \leq s + 3d + (f - d)^2 + 2(f - d) - 4(f - d)(t - d - 1). \tag{6.56}$$

For E_6, we have $f \leq 5$; so, in particular, (6.56) should yield

$$s + 3d + (5 - d)^2 + 2(5 - d) = s + d^2 - 9d + 35 \geq 30.$$

For $0 < d \leq 5$ we have $d^2 - 9d \geq -8$, hence $s \geq 3$. But then $f \leq 3$ and $s + 3d + (f - d)^2 + 2(f - d) < 30$. Thus $d = 0$ and (6.56) assumes the form $35 + s - 4t(t - 1) \geq 30$. If $t > 1$, then $s \geq 3$ and (6.56) narrows down to $s + 15 - 4t(t - 1) \geq 30$, which is impossible. Thus $t = 1$ and the only case that satisfies (6.54) furnishes a simple group of type A_5 for H. But H must be isomorphically embeddible in the semisimple part of P, which is a group of type D_5. However a group of type D_5 cannot contain a group of type A_5, since $|W(A_5)| = 2^4 \cdot 3^2 \cdot 5$ does not divide $|W(D_5)| = 2^7 \cdot 3 \cdot 5$.

For E_7, we have $f \leq 6$; then

$$s + 3d + (6 - d)^2 + 2(6 - d) = s + d^2 - 11d + 48 \geq 52$$

is possible only if $d = 0$ and $s \geq 4$. But then $f \leq 2$ and $s + 3d + (2 - d)^2 + 2(2 - d) \leq 15$, contradiction.

Lastly, for E_8, we have $f \leq 7$; then

$$s + 3d + (7 - d)^2 + 2(7 - d) = s + d^2 - 13d + 63 \geq 77$$

has no integral solutions satisfying $0 \leq s, d \leq 8$. The lemma is proved.

Now we conclude the analysis for $p = 2, 3$ in Theorem 6.29. Let $\xi \in H^1(L/K, G_0)$, where $[L : K] = p$ and $G = {}_\xi G_0$. Consider the case where G_0 has type ${}^1E_6$. If $p = 2$ then G is K-isotropic, by Lemma 6.31. If $p = 3$ and G is K-anisotropic, then by Lemma 6.32 G must contain a semisimple K-subgroup H of a type other than $A_{l_1} \times \cdots \times A_{l_t}$. But Theorems 6.4 and 6.6, and hence also Theorems 6.5 and 6.25, have already been proved for simply connected groups of lower rank; hence H is K-isotropic. Thus, G is K-isotropic for $p = 3$ as well; therefore Proposition 6.22 and the validity of Theorems 6.4 and 6.6 for groups of lower rank imply that $\xi = 1$, i.e., $H^1(L/K, G_0) = 1$. But, as we have seen, this implies that $H^1(K, G_0) = 1$.

Now let G_0 have type ${}^2E_6$, and let E/K be a quadratic extension over which G_0 becomes an inner form. What we have already shown implies that $H^1(E, G_0) = 1$, from which it follows that $G = {}_\xi G_0$, where $\xi \in H^1(K, G_0)$, becomes split over E. Therefore, G is K-isotropic by Lemma 6.31, and $\xi = 1$ by Proposition 6.22, i.e., $H^1(K, G_0) = 1$.

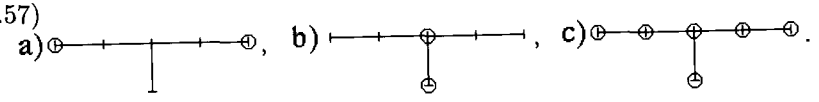
Now we analyze type E_7. Since $H^1(K, H)$ has already been proved trivial for all quasisplit simply connected groups H of lower rank, Theorem 6.26 shows that any semisimple K-group of lower rank having type other than $A_{l_1} \times \cdots \times A_{l_t}$, is K-isotropic. Therefore, it follows from Lemmas 6.31 and 6.32 that $G = {}_\xi G_0$, where $\xi \in H^1(L/K, G_0)$, is K-isotropic, and by Proposition 6.22 $\xi = 1$. Thus, $H^1(L/K, G_0) = 1$, implying $H^1(K, G_0) = 1$.

For groups of type E_8 the argument is analogous.

Let us proceed directly to the proof of Theorems 6.4 and 6.6 for groups of the E series.

GROUPS OF TYPE ${}^1E_6$: First we shall show that $H^1(K, G) = 1$ for any simply connected K-group of type ${}^1E_6$, if K is a local number field or a totally imaginary number field. Let $\xi \in H^1(K, G)$, and let $G_1 = {}_\xi G$. Since the triviality of $H^1(K, G_0)$ has already been established, G and G_1 are K-isotropic (Theorem 6.26). Let $T \subset G$ and $T_1 \subset G_1$ be maximal K-tori containing maximal K-split tori. All the possible indexes for isotropic groups of type ${}^1E_6$ are as follows (cf. Tits [2]):

(6.57)



In case (a) the anisotropic kernel must have type D_4, which is impossible, since all groups of this type are K-isotropic. In the remaining diagrams α_2 is a distinguished vertex (labelling as in (6.52)). Put

$$S = (\bigcap_{i \neq 2} \ker \alpha_i)^0, \qquad S_1 = (\bigcap_{i \neq 2} \ker \alpha_i^1)^0,$$

where $\Pi = \{\alpha_1, \ldots, \alpha_6\}$ and $\Pi_1 = \{\alpha_1^1, \ldots, \alpha_6^1\}$ are systems of simple roots in $R = R(T, G)$ and $R_1 = R(T_1, G_1)$, respectively. Then there exists a $\bar{K}$-isomorphism $\varphi: G \to G_1$ sending S to S_1.

Consider the cocycle $\theta = \{a_\sigma = \varphi^{-1}\sigma(\varphi)\}$ in $Z^1(K, \bar{G})$, where $\bar{G}$ is the corresponding adjoint group, which, as usual, we identify with the group of inner automorphisms. Clearly θ is equivalent to the image of ξ in $Z^1(K, \bar{G})$; so, replacing ξ by an equivalent cocycle, one may assume that θ is precisely the image of ξ. Since S and S_1 are K-split, $\varphi|_S: S \to S_1$ is defined over K, and therefore a_σ acts trivially on S. It follows that $\xi \in H^1(K, C)$, where

$C = Z_G(S)$. But $C = HS$, where H is a simply connected simple group of type A_5. Therefore $H^1(K, H) = 1$, and the exact sequence

$$H^1(K, H) \to H^1(K, C) \to H^1(K, \bar{S}) = 1,$$

where $\bar{S} = C/H = S/S \cap H$ is a split torus, yields $H^1(K, C) = 1$, and thus ξ is trivial in $H^1(K, G)$.

It remains to show that the Hasse principle holds for groups of type ${}^1E_6$ over a number field K. To do so we shall need two lemmas, generalizing Lemmas 6.17 and 6.28. Before we formulate them, recall that $\mathcal{P}$, a conjugacy class of the parabolic subgroups of G, is said to be *reflexive* if, for P in $\mathcal{P}$, the opposite parabolic subgroup P^- also lies in $\mathcal{P}$ (cf. Borel-Tits [1, §4]. Also note that $P^- \cap P$ is the reductive part of P.) For example, all Borel subgroups constitute a reflexive class.

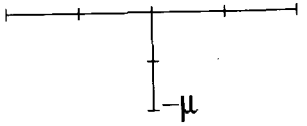
LEMMA 6.17′. *Let G be a semisimple algebraic group defined over an arbitrary infinite perfect field K and having a parabolic subgroup P_0 over a quadratic extension L of K such that its conjugacy class $\mathcal{P}$ is reflexive. Then there exists a parabolic L-subgroup P of G, $P \in \mathcal{P}$, such that $C = P \cap \sigma(P)$ is the reductive part of P, where σ is a generator of* $\mathrm{Gal}(L/K)$.

LEMMA 6.28′. *Notation as in Lemma 6.17′, assume in addition that K is a number field. If ξ is a cocycle in $Z^1(L/K, G)$ representing an element of* $\ker(H^1(K, G) \to \prod_{v \in V_\infty^K} H^1(K_v, G))$, *then there exists ξ' in $Z^1(L/K, C)$ which is equivalent to ξ in $Z^1(L/K, G)$ and represents an element of* $\ker(H^1(K, C) \to \prod_{v \in V_\infty^K} H^1(K_v, C))$.

The proof of Lemmas 6.17′ and 6.28′ is completely analogous to that of Lemmas 6.17 and 6.28. We leave it to the reader to work out the details of the argument, and note only that in proving Lemma 6.28′, instead of the usual Bruhat decomposition one uses a generalized decomposition (cf. Borel-Tits [1, §5]).

Now let $\xi \in \ker(H^1(K, G) \to \prod_{v \in V_\infty^K} H^1(K_v, G))$. Put $L = K(\sqrt{-1})$. It has been shown that $H^1(L, G) = 1$, and therefore one may assume that $\xi \in Z^1(L/K, G)$. G is isotropic over L; moreover its index is either (b) or (c) in (6.57). Let P_0 denote the standard parabolic subgroup P_Δ, where $\Delta = \Pi \backslash \{\alpha_2, \alpha_4\}$, notation as in (6.52). Since $\{\alpha_2, \alpha_4\}$ is invariant with respect to the symmetries of the Dynkin diagram, the conjugacy class of P_0 is reflexive (cf. Borel-Tits [1, §4.9]). The semisimple part of P_0 is a simply connected semisimple group of type $A_2 \times A_2$, and the simple components correspond to the systems $\{\alpha_1, \alpha_3\}$ and $\{\alpha_5, \alpha_6\}$. Using Lemma 6.17′ we can find a parabolic L-subgroup P of G which is conjugate to P_0 and for which

$C = P \cap \sigma(P)$ is the reductive part of P. By Lemma 6.28′, ξ can be replaced by an equivalent cocycle in $Z^1(L/K, G)$, such that $\xi \in \ker(H^1(K, C) \to \prod_{v \in V_\infty^K} H^1(K_v, C))$. To prove ξ trivial we construct a certain semisimple K-subgroup of G containing C. To wit, let $H = [C, C]$ be the semisimple part of C. Then we see from analysis of the extended Dynkin diagram



of the system of type E_6, where μ is the maximal root (cf. Bourbaki [4, Table 5]), that the centralizer $B = Z_G(H)$ is a simply connected simple group of type A_2 corresponding to the system $\{\alpha_2, \mu\}$. Put $D = HB$. Clearly $C \subset D$, and therefore the proof is completed by

LEMMA 6.33. *If* $\xi \in H^1(L/K, D)$ *and*

$$\xi \in \ker(H^1(K, D) \to \prod_{v \in V_\infty^K} H^1(K_v, D)),$$

then $\xi = 1$ *in* $H^1(L/K, D)$.

PROOF: Put $F = H \cap B$ and consider the commutative diagram

$$\begin{array}{ccc} H^1(K,F) & \xrightarrow{\alpha_1} & H^1(K, H\times B) \\ \downarrow{\scriptstyle \gamma_1} & & \downarrow{\scriptstyle \gamma_2} \\ \prod_{v\in V_\infty^K} H^1(K_v,F) & \xrightarrow{\beta_1} & \prod_{v\in V_\infty^K} H^1(K_v, H\times B) \end{array}$$

$$\begin{array}{ccccc} \xrightarrow{\alpha_2} & H^1(K,D) & \xrightarrow{\alpha_3} & H^2(K,F) \\ & \downarrow{\scriptstyle \gamma_3} & & \downarrow{\scriptstyle \gamma_4} \\ \xrightarrow{\beta_2} & \prod_{v\in V_\infty^K} H^1(K_v,D) & \xrightarrow{\beta_3} & \prod_{v\in V_\infty^K} H^2(K_v,F) \end{array}$$

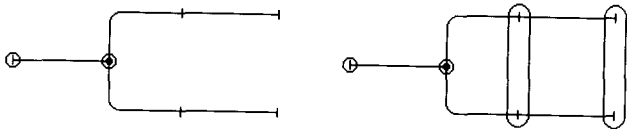
corresponding to the universal covering $1 \to F \to H \times B \to D \to 1$. Clearly $\alpha_3(\xi)$ lies in the kernel of $H^2(K, F) \xrightarrow{\text{Res}} H^2(L, F)$. Using the map $\text{Cor}: H^2(L, F) \to H^2(K, F)$ and the fact that $\text{Cor} \circ \text{Res}$ coincides with multiplication by $[L : K] = 2$, we obtain that $\alpha_3(\xi) = 1$, since $|F|$ divides $|Z(B)| = 3$. Then $\xi = \alpha_2(\zeta)$, where $\zeta \in H^1(K, H \times B)$. We have

$\beta_2(\gamma_2(\zeta)) = \gamma_3(\alpha_2(\zeta)) = 1$, so $\gamma_2(\zeta) \in \operatorname{im}\beta_1$. But again, by the fact that $|F|$ divides 3 and $[\text{Gal}(\bar{K}_v/K_v)] \leq 2$ for $v \in V_\infty^K$, we obtain that $H^1(K_v, F) = 1$, i.e., $\operatorname{im}\beta_1 = (1)$. Therefore $\zeta \in \ker\gamma_2$ and hence $\zeta = 1$, since the Hasse principle has already been proved for groups of type A_2. Finally, $\xi = \alpha_2(\zeta) = 1$, and the lemma is proved.

GROUPS OF TYPE ${}^2E_6$: If K is a local field, then by Proposition 6.15 any K-group G of type ${}^2E_6$ is quasisplit, i.e., $G \simeq G_0$, since $H^1(K, G_0)$ has already been proved trivial. But then $H^1(K, G) = H^1(K, G_0) = 1$.

The proof of the triviality of $H^1(K, G)$ for a totally imaginary number field K is analogous to the respective argument for ${}^1E_6$. Indeed, the triviality of $H^1(K, G_0)$ implies that G is K-isotropic (Theorem 6.26). Then its index is one of those indicated in (6.53); moreover, as we noted in the proof of Proposition 6.22, case (b) does not occur over a totally imaginary number field. In the remaining cases α_2 is a distinguished vertex. The argument continues as in the case of type ${}^1E_6$.

The Hasse principle can also be proved similarly to the case of ${}^1E_6$ if one knows that the index of G over a totally imaginary number field L must be one of the following:



i.e., α_2 and α_4 must be distinguished vertices. We shall now prove this. Let S_0 denote the two-dimensional L-split torus $(\bigcap_{i \neq 2,4} \ker\alpha_i)^0$ of G_0, let C be its centralizer in G_0, and let $H = [C, C]$ be its semisimple part. Put $\bar{H} = \pi(H)$, where $\pi: G_0 \to \bar{G}_0$ is an isogeny on the adjoint group. Since G is obtained from G_0 by twisting using a cocycle θ in $H^1(L, \bar{G}_0)$, it suffices to show that $H^1(L, \bar{H}) \to H^1(L, \bar{G}_0)$ is surjective. It is easy to show that the center Z of G_0 is contained in H. We have the commutative diagram with exact rows

$$\begin{array}{ccccc} H^1(L,H) & \xrightarrow{\alpha_1} & H^1(L,\bar{H}) & \xrightarrow{\alpha_2} & H^2(L,Z) \\ \downarrow{\scriptstyle \gamma_1} & & \downarrow{\scriptstyle \gamma_2} & & \downarrow{\scriptstyle \gamma_3} \\ H^1(L,G_0) & \xrightarrow{\beta_1} & H^1(L,\bar{G}_0) & \xrightarrow{\beta_2} & H^2(L,Z). \end{array}$$

By Theorem 6.20, α_2 is surjective. It follows that for a given θ in $H^1(L, \bar{G}_0)$ there is a ζ in $H^1(L, \bar{H})$ such that $\beta_2(\theta) = \beta_2(\gamma_2(\zeta))$. But since the triviality of the cohomology of simply connected groups of type ${}^2E_6$ over a totally imaginary number field has already been proved, β_2 is injective by a twisting argument. Therefore $\theta = \gamma_2(\zeta)$, as desired.

GROUPS OF TYPE E_7: Since $H^1(K, G_0) = 1$, then by Proposition 6.16, for any K-group G of type E_7 there is a quadratic extension L/K, totally imaginary in the case of a number field, over which G becomes split. With Lemma 6.17 we find a Borel L-subgroup B of G such that $T = B \cap \sigma(B)$ is a maximal K-torus of G, split over L (where σ is the generator of $\mathrm{Gal}(L/K)$).

Let us show that T is K-anisotropic, i.e., that σ acts on $\mathbf{X}(T)$ by multiplication by -1. Indeed, since $B \cap \sigma(B) = T$, it follows that σ translates the positive roots of $R(T, G)$ associated with B to negative roots. But since the Dynkin diagram has no nontrivial symmetries, the only automorphism with this property is -1. It follows that any root subgroup G_α is defined over K, and hence H constructed in the proof of Proposition 6.21, a simply connected subgroup of G of type A_7 containing T, is also defined over K.

Now let $\xi \in H^1(K, G)$, where K is a local field. Since $G \simeq G_0$ over L, it follows that $H^1(L, G) = H^1(L, G_0) = 1$, and therefore $\xi \in H^1(L/K, G)$. By Lemma 6.28 there exists a cocycle ξ' in $H^1(L/K, T)$ which is equivalent to ξ. But since Theorem 6.4 has already been proved for H, the composite map $H^1(K, T) \to H^1(K, H) \to H^1(K, G)$ is trivial and $\xi = 1$.

For K a number field, take ξ in $\ker(H^1(K, G) \to \prod_{v \in V_\infty^K} H^1(K_v, G))$. As above, one can prove that $\xi \in H^1(L/K, G)$; so by Lemma 6.28, replacing ξ by an equivalent cocycle, we may assume that

$$\xi \in \ker\left(H^1(K, T) \to \prod_{v \in V_\infty^K} H^1(K_v, T)\right).$$

Then, applying Theorem 6.6 for H, we conclude that $\xi = 1$.

GROUPS OF TYPE E_8: For groups of this type we actually need only consider the case $p = 5$ in Theorem 6.29, since $H^1(K, G) = 1$ over a local or totally imaginary number field K. It follows that any group G of type E_8 over such a field splits; one concludes from this that $H^1(K, G) = 1$ for all G. The Hasse principle can then be derived exactly as in the case of E_7.

So, let L be a cyclic Galois extension of degree 5 over a local or a totally imaginary number field K, and let G_0 be a simple split K-group of type E_8. Our objective is to show that $H^1(L/K, G_0) = 1$. Let E denote the compositum of all the finite solvable Galois extensions of K having degree of the form $2^\alpha 3^\beta$ (a maximal solvable $\{2, 3\}$ extension of K; note that any group of order $2^\alpha 3^\beta$ is solvable (Burnside's theorem), so one could actually omit "solvable"). It suffices to show that $H^1(LE/E, G_0) = 1$, since then any ξ in $H^1(L/K, G_0)$ lies in $H^1(E/K, G_0)$ and hence in $H^1(P/K, G_0)$ for some finite solvable extension P/K of degree $2^\alpha 3^\beta$. There exists a tower $P = P_0 \supset P_1 \cdots \supset P_{n-1} \supset P_n = K$, every floor P_i/P_{i+1} of which is a cyclic extension of degree 2 or 3. But the cases $p = 2, 3$ in Theorem 6.29 have already been considered; applying this theorem to each floor in turn, we obtain that $H^1(P/K, G_0) = 1$, which means $\xi = 1$. In this manner we shall prove the triviality of $H^1(L/E, G_0)$, where L/E is any cyclic extension of E of degree 5. We shall need the following property of E (for which we actually have to pass from K to E): E has no extensions of degree 2, 3, or 4; in particular, if $a \in E$, then $\sqrt{a}, \sqrt[3]{a} \in E$. The following theorem plays a key role in the proof.

THEOREM 6.30 (CHERNOUSOV [6]). *Let G be an anisotropic group of type E_8 defined over E and split over a cyclic extension L of E of degree 5. Then G has a proper semisimple E-subgroup H which is isotropic over L.*

PROOF: Let σ be a generator of $\mathrm{Gal}(L/E)$. We shall establish the existence of a one-dimensional unipotent subgroup $U = U_\alpha$ corresponding to a root α in $R(T, G)$ with respect to a suitable maximal L-split torus T of G such that the subgroup H_0 of G generated by $\sigma^i(U)$ $(i = 0, 1, 2, 3, 4)$ is proper. Such an H_0 is obviously defined over E and, in particular, is reductive since G is E-anisotropic. By construction, H_0 over L contains unipotent elements; therefore H_0 does not reduce to a torus and its commutator subgroup $H = [H_0, H_0]$ is the desired group.

To verify that $H_0 \neq G$, we shall show that its Lie algebra $\mathfrak{h}_0 = L(H_0)$ is distinct from $\mathfrak{g} = L(G)$. To do so note that since $\mathrm{char}\, K = 0$, $\mathfrak{h}_0$ is generated as a Lie algebra by $\sigma^i(X)$, $(i = 0, 1, 2, 3, 4)$, where $X \in L(U)_L$ is any nonzero element (cf. Borel [8, §7]). Therefore our task reduces to finding X in $\mathfrak{g}_L$ that generates the Lie algebra of some root unipotent subgroup U and for which the subalgebra of $\mathfrak{g}$ generated by $\sigma^i(X)$ $(i = 0, 1, 2, 3, 4)$ is proper. We call the elements satisfying the first condition *root* elements; more precisely, X in $\mathfrak{g}_L$ is a root element if there exists a maximal L-split torus T of G such that X is an eigenvector with respect to $\mathrm{Ad}\, T$, i.e., $\mathrm{Ad}(t)(X) = \alpha(t)X$ for suitable $\alpha \neq 1$ in $\mathbf{X}(T)$ and all t in T. If $X \neq 0$, then α turns out to be a root of G with respect to T, and the one-dimensional space spanned by X has the form $L(U_\alpha)$, where U_α is the unipotent root subgroup corresponding to α. Thus, it suffices to find a nonzero root element X in $\mathfrak{g}_L$ all of whose translations $\sigma^i(X)$ generate a proper subalgebra of $\mathfrak{g}$.

We begin by establishing some properties of root elements needed later on. Let $X \in L(U_\alpha)_L$, where $\alpha \in R = R(T, G)$. Since all the roots in a system of type E_8 have the same length, without loss of generality we may assume that α is the maximal root under the ordering associated with a given system of simple roots $\Pi \subset R$. Let $\{H_\alpha, \alpha \in \Pi; X_\alpha, \alpha \in R\}$ be a Chevalley base of $\mathfrak{g}_L$ (cf. §2.1.13). Then $[X_\alpha, X_{-\alpha}] = H_\alpha$, $[X_\alpha, X_\beta] = 0$ or $\pm X_{\alpha+\beta}$, and the maximality of α implies that for any Y in $\mathfrak{g}_L$ the expression $[X_\alpha, [X_\alpha, Y]]$ is proportional to X_α. Since X in turn is proportional to X_α,

we see that for any Y in $\mathfrak{g}_L$ we have

$$[X,[X,Y]] = \langle X,Y\rangle X$$

for suitable $\langle X,Y\rangle$ in L (putting $\langle X,Y\rangle = 0$ if $X = 0$). This property of root elements is crucial in later computations. It is easy to see that $\langle X,Y\rangle$ is linear in the second argument. Now suppose that both X and Y are root elements of $\mathfrak{g}_L$. Then, multiplying the equations

$$\begin{aligned} [X[X,Y]] &= \langle X,Y\rangle X \\ [Y,[Y,X]] &= \langle Y,X\rangle Y \end{aligned} \tag{6.58}$$

on the left by Y and X respectively, and using

$$[Y[X,[X,Y]]] = -[X,[Y,[Y,X]]],$$

which follows from the Jacobi identity, we easily obtain that $\langle X,Y\rangle = \langle Y,X\rangle$. Thus $\langle X,Y\rangle$ is linear in X, for a root element Y, where X runs through a linear space consisting of root elements.

Let us establish several other properties of root elements.

LEMMA 6.34. *Let X, Y, $Z \in \mathfrak{g}_L$, where X is a root element. Then*

(1) *The following identities hold:*

$$2[[X,Z],[X,Y]] = \langle X,Y\rangle[X,Z] - \langle X,Z\rangle[X,Y] - \langle X,[Y,Z]\rangle X \tag{6.59}$$

$$2[X,[Y,[Z,X]]] = \langle X,Z\rangle[X,Y] + \langle X,Y\rangle[X,Z] + \langle X,[Z,Y]\rangle X; \tag{6.60}$$

(2) *If $[X,Y] = 0$ then $\langle X,[Y,Z]\rangle = 0$.*

PROOF: The Jacobi identity implies that

$$\begin{aligned} [[X,Z],[X,Y]] &= [Y,[X,[X,Z]]] - [X,[Y,[X,Z]]] \\ &= \langle X,Z\rangle[Y,X] + [X,[Y,[Z,X]]]. \end{aligned} \tag{6.61}$$

Analogously, one obtains that

$$[[X,Y],[X,Z]] = \langle X,Y\rangle[Z,X] + [X,[Z,[Y,X]]]. \tag{6.62}$$

Moreover,

$$[X,[Y,[Z,X]]] = -\langle X,[Y,Z]\rangle X + [X,[Z,[Y,X]]]. \tag{6.63}$$

(6.59) and (6.60) follow easily from (6.61)–(6.63). If $[X,Y] = 0$ and $X \neq 0$, then (2) follows immediately from (6.59). The lemma is proved.

The point of departure for finding the requisite root element X in $\mathfrak{g}_L$ is

PROPOSITION 6.23. *Let X be a root element of $\mathfrak{g}_L$ such that $[X,\sigma(X)] = 0$. Then the subalgebra $\mathfrak{h}_0$ of $\mathfrak{g}$ generated by the $\sigma^i(X)$ $(i = 0,\dots,4)$ has dimension ≤ 25, and therefore is proper.*

PROOF: Put $X_i = \sigma^{2i-2}(X)$. Then $\mathfrak{h}_0$ is generated by the X_i; furthermore $[X,\sigma(X)] = 0$ implies that $[X_i,X_j] = 0$, except when $i \equiv j \pm 1 \pmod 5$. For the sake of simplicity put

$$(i_1,\dots,i_s) = [X_{i_1},[X_{i_2},\dots,[X_{i_{s-1}},X_{i_s}]\dots]],$$

where $1 \leq i_l \leq 5$, $1 \leq l \leq s$; we call such an expression a *monomial of length s*. Clearly $\mathfrak{h}_0$ is the linear space spanned by all possible monomials. A monomial is said to be *reducible* if it is a linear combination of monomials having strictly smaller length. Also, $(i_1,\dots,i_l)$ is called a *standard monomial* if $i_{h+1} \equiv i_h + 1 \pmod 5$, $h = 1,\dots,l-1$. There are 5 standard monomials of any given length; therefore there are 25 standard monomials of length ≤ 5. Thus, the estimate given for the dimension of $\mathfrak{h}_0$ is obtained from the following two assertions:

(*) any monomial of length ≤ 5 is a linear combination of standard monomials;

(**) any monomial of length 6 is reducible.

To prove (*) consider a monomial $m = (i_1,\dots,i_l)$ of length $l \leq 5$, and suppose that (*) has already been proved for monomials of smaller length. Then we may assume $(i_2,\dots,i_l)$ is a standard monomial; without loss of generality we can suppose that $i_h = h$, for $2 \leq h \leq l$. If $i_1 = 1$, then m is standard. If $i_2 = 2$, then it follows from the basic properties of root elements that m is proportional to X_{i_2}, and there is nothing to prove. If $2 < i_1 \leq l$, then using the fact that $[X_i,X_j] = 0$ for $i \not\equiv j \pm 1 \pmod 5$ and the Jacobi identity, it is easy to show that

$$m = (i_2,2,\dots,l) = (2,3,\dots,i_1,i_1-1,i_1,\dots,l),$$

and the reducibility of this monomial follows from (6.60). If $i_1 = l+1$, then $m = (l+1,2,\dots,l) = (2,\dots,l-1,l+1,l) = -(2,\dots,l-1,l,l+1)$ is a standard monomial. Lastly, if $i_1 > l+1$, then $m = 0$.

To prove (**) it suffices to establish that $(i,1,2,\dots,5)$ is reducible, which can be done by a similar argument. The proposition is proved.

The most technically intricate part of the proof of Theorem 6.30 is to construct a nonzero root element X of $\mathfrak{g}_L$ for which $[X,\sigma(X)] = 0$. To do so, first one constructs a root element Y in $\mathfrak{g}_L$ satisfying the following:

$$\langle Y,\sigma(Y)\rangle = 0, \qquad \langle \sigma(Y),[Y,\sigma^2(Y)]\rangle = 0. \tag{6.64}$$

If in addition $[Y,\sigma(Y)]=0$, then $X=Y$ is the desired element. If not, put $X=[Y,\sigma(Y)]$. Then (6.64) and (6.59) imply that

$$\begin{aligned}[X,\sigma(X)] &= [[Y,\sigma(Y)],[\sigma(Y),\sigma^2(Y)]]\\ &= -\frac{1}{2}(\langle\sigma(Y),\sigma^2(Y)\rangle[\sigma(Y),Y]-\langle\sigma(Y),Y\rangle[\sigma(Y),\sigma^2(Y)]\\ &\qquad -\langle\sigma(Y),[\sigma^2(Y),Y]\rangle\sigma(Y))=0.\end{aligned}$$

It remains to show that X is a root element.

LEMMA 6.35. *Let X and Y be root elements of $\mathfrak{g}_L$. There exists a maximal L-split torus T of G such that both X and Y are eigenvectors with respect to $\operatorname{Ad}T$. In addition, if $\langle X,Y\rangle=0$ then $[X,Y]$ is also a root element.*

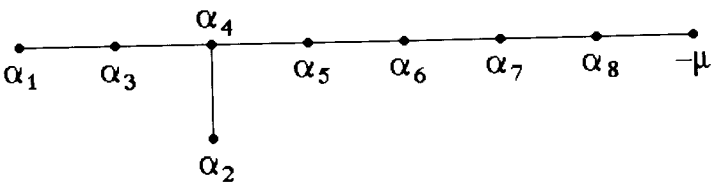
PROOF: Let T_X be a maximal L-split torus of G, such that X is an eigenvector for $\operatorname{Ad}T_X$. We saw above that without loss of generality we may assume X to be proportional to X_α, where $\alpha\in R_X=R(T_X,G)$ is the maximal root with respect to the ordering on R_X given by a system of simple roots Π_X. Let $B_X=T_XU_X$ be the Borel subgroup corresponding to Π_X. Since α is maximal, the unipotent part of U_X centralizes X, and therefore X is an eigenvector for $\operatorname{Ad}B_X$. Similarly, we can find a Borel subgroup B_Y of G such that Y is an eigenvector for $\operatorname{Ad}B_Y$. Then $B_X\cap B_Y$ contains a maximal torus T of G, which is the desired torus.

Let $X\in L(U_\alpha)$, $Y\in L(U_\beta)$, where $\alpha,\beta\in R(T,G)$. If $\beta\neq-\alpha$, then either $[X,Y]=0$ or $\alpha+\beta$ is a root and $[X,Y]\in L(U_{\alpha+\beta})$. We claim that $\beta\neq-\alpha$ if $\langle X,Y\rangle=0$. Indeed, if $\beta=-\alpha$, then $[X,Y]$ is proportional to H_α and nonzero. Then $[X,[X,Y]]=cX$, where $c=\langle X,Y\rangle\neq0$, contradiction. The lemma is proved.

The proof of the theorem is completed by

PROPOSITION 6.24. *There exists a nonzero root element Y in $\mathfrak{g}_L$ satisfying (6.64).*

PROOF: First we show how to find a root element Z in $\mathfrak{g}_L$ satisfying the first condition of (6.64). To do so, temporarily fix a maximal L-split torus T of G, a root system $R=R(T,G)$, and a system of simple roots $\Pi=\{\alpha_1,\dots,\alpha_8\}$, and let μ in R be the corresponding maximal root. Recall that the extended Dynkin diagram here appears as follows:



The elements $X_{\pm\alpha}$, $\alpha\in\{\alpha_i : i\neq2\}\cup\{\mu\}$, generate a subalgebra $\mathfrak{b}_L$ of $\mathfrak{g}_L$ of type A_8. Identifying $\mathfrak{b}_L$ with the Lie algebra $\mathfrak{sl}_9(L)$ of matrices in $M_9(L)$ with zero trace, we see that $\mathfrak{b}_L$ contains an 8-dimensional subspace V consisting entirely of root elements (for example, the subspace

$$V=\{(z_{ij}) : z_{ij}=0 \text{ if } i=j=1 \text{ or } i\neq1\};$$

note that since $\mathfrak{b}$ and $\mathfrak{g}$ have the same rank and the elements of V are obviously root elements of $\mathfrak{b}_L$, these elements will also be root elements of $\mathfrak{g}_L$). We show that there exists an element Z in $V\setminus(0)$ such that

$$\langle Z,\sigma(Z)\rangle=0. \tag{6.65}$$

Since V is 8-dimensional over L, it has dimension 40 over E. In this respect, (6.59) is equivalent to a system of five homogeneous quadratic equations for the E-coordinates of Z. Therefore the existence of a nonzero Z satisfying (6.65) is a consequence of the following straightforward assertion:

EXERCISE: Let $f_1,\dots,f_l$ be quadratic forms in n variables, with coefficients from E. If $n>\frac{1}{2}l(l+1)$, then $f_1(x)=\dots=f_l(x)=0$ has a nonzero solution over E. (Proof is by induction on l and uses the feasibility of extracting square roots of elements of E.)

Fix a nonzero root element Z in $\mathfrak{g}_L$ satisfying (6.65). To construct a root element Y in $\mathfrak{g}_L$ satisfying both equalities in (6.64) one must reconstruct the original T. Namely, by Lemma 6.35, passing to another torus, one may assume that Z and $\sigma(Z)$ are eigenvectors with respect to $\operatorname{Ad}T$, i.e., that they generate algebras $L(U_\alpha)$ and $L(U_\beta)$ for suitable roots $\alpha,\beta\in R(T,G)$. If $[Z,\sigma(Z)]=0$, then the Jacobi identity implies that $[\sigma(Z),[Z,\sigma^2(Z)]]=0$, and $Y=Z$ is the desired element. Therefore, henceforth we shall assume that $[Z,\sigma(Z)]\neq0$. Then, in view of (6.65), we obtain $\beta\neq-\alpha$, and hence $\alpha+\beta$ is also a root.

We have already noted that one can choose a subsystem Π of $R(T,G)$ of simple roots such that α is the maximal root with respect to the corresponding ordering. We show that by changing Π one can also satisfy $\beta=-\alpha_8$, where $\Pi=\{\alpha_1,\dots,\alpha_8\}$, with the roots labelled as above. To do so, consider the set $\{\tilde\Pi\}$ of all systems of simple roots $\tilde\Pi\subset R(T,G)$ in which α is the maximal root, and make the choice of Π subject to the condition $\operatorname{ht}_\Pi\beta=\max_{\tilde\Pi}\operatorname{ht}_{\tilde\Pi}\beta$, where $\operatorname{ht}_\Pi\beta=\sum_{i=1}^8 n_i$ is the height of $\beta=\sum_{i=1}^8 n_i\alpha_i$ with respect to $\Pi=\{\alpha_1,\dots,\alpha_8\}$. Since $\alpha+\beta$ is a root and α is maximal, β must be negative. However, if $\gamma\in\{\alpha_1,\dots,\alpha_7\}$, then necessarily the scalar product $(\gamma\cdot\beta)\geq0$, since otherwise the height of β with respect to $\Pi'=w_\gamma(\Pi)\in\{\tilde\Pi\}$ (where w_γ is the corresponding reflection) would be greater than $\operatorname{ht}_\Pi\beta$. It is clear from the description of the root system

of type E_8 (cf. Bourbaki [4, Table 7]) that $\beta = \delta - \alpha_8$, where δ is a linear combination of $\alpha_1, \dots, \alpha_7$ with non-positive integral coefficients. Then $(\beta\cdot\beta) = (\delta\cdot\delta) - 2(\delta\cdot\alpha_8) + (\alpha_8\cdot\alpha_8)$, from which it follows that $(\delta\cdot\delta) = 2(\delta\cdot\alpha_8)$ since $(\beta\cdot\beta) = (\alpha_8\cdot\alpha_8)$; therefore $(\delta\cdot\delta) = (\delta\cdot\beta + \alpha_8) = (\delta\cdot\beta) + (\delta\cdot\alpha_8) \leq \frac{1}{2}(\delta\cdot\delta)$, implying finally $(\delta\cdot\delta) = 0$, i.e., $\delta = 0$, as desired.

Thus, replacing Z by a proportional element, one can assume that $Z = X_\alpha$, where α is a maximal root, and $\sigma(Z) = cX_{-\alpha_8}$.

LEMMA 6.36. *There exists a 6-dimensional subspace W of $\mathfrak{g}_L$ such that $LZ + W$ consists of root elements and for any S in W the following relations hold:*

$$\begin{aligned} \langle Z, \sigma(S)\rangle = \langle S, \sigma(S)\rangle = 0 \\ [Z, S] = [Z, \sigma(S)] = 0. \end{aligned} \tag{6.66}$$

PROOF: Let W_1 denote the subspace of $\mathfrak{g}_L$ spanned by

$$X_{\alpha_7}, X_{\alpha_7+\alpha_6}, \dots, X_{\alpha_7+\dots+\alpha_3}, X_{\alpha_7+\dots+\alpha_3+\alpha_1};$$

$\dim W_1 = 6$. If, as above, we identify the algebra of type A_8 generated by X_γ $(\gamma \in \{\alpha_i : i \neq 2\} \cup \{\alpha\})$ with $\mathfrak{sl}_9(L)$, we can easily show that $LX_{-\alpha_8} + W_1$ consists of root elements. The relations for elements of a Chevalley base yield the following properties:

$$W_1 \subset [X_{-\alpha_8}, \mathfrak{g}_L], \qquad [X_{-\alpha_8}, W_1] = 0, \qquad [X_\alpha, W_1] = 0. \tag{6.67}$$

Put $W = \sigma^{-1}(W_1)$. Then $LX_\alpha + W$ consists of root vectors. All the relations in (6.66) follow from (6.67) except for $\langle S, \sigma(S)\rangle = 0$ for S in W. But $[X_\alpha, S_1] = 0$ for any S_1 in W_1, according to (6.67). Therefore, applying Lemma 6.34(2), we obtain $\langle S_1, [X_\alpha, \mathfrak{g}_L]\rangle = 0$. But now (6.67) implies that $[X_\alpha, \mathfrak{g}_L]$ contains W, therefore $\langle W_1, W\rangle = 0$, whence $\langle W, \sigma(W)\rangle = 0$. The lemma is proved.

With the properties of W given above, it is now easy to finish constructing the desired nonzero element Y, satisfying (6.64). First we find a nonzero S in W satisfying the following:

$$\langle \sigma(Z), S\rangle = \langle \sigma(Z), [S, \sigma^2(Z)]\rangle = 0, \tag{6.68}$$

$$\langle \sigma(S), [S, \sigma^2(Z)]\rangle = 0. \tag{6.69}$$

The S in W satisfying (6.68) form a subspace of dimension ≥ 4 over L, i.e., dimension ≥ 20 over E. In this respect, (6.69) is equivalent to a

system of 5 homogeneous quadratic equations for the E-coordinates of S. Therefore, again applying the assertion in the exercise, we obtain the existence of S. Furthermore, we may assume that $z = \langle \sigma(Z), [Z, \sigma^2(Z)]\rangle \neq 0$, $s = \langle \sigma(S), [S, \sigma^2(S)]\rangle \neq 0$.

Let us put $q = -zs^{-1}$, $r = \sqrt[3]{N_{L/E}(q)} \in E$, and $t = rq\sigma^3(q)$, and show that $Y = Z + tS$ is the desired root element.

We have

$$\langle Y, \sigma(Y)\rangle = \langle Z + tS, \sigma(Z) + \sigma(t)\sigma(S)\rangle = 0$$

by conditions (6.66) and (6.68). To avoid cumbersome notation in computing

$$y = \langle \sigma(Y), [Y, \sigma^2(Y)]\rangle = \langle \sigma(Z) + \sigma(t)\sigma(S), [Z + tS, \sigma^2(Z) + \sigma^2(t)\sigma^2(S)]\rangle,$$

note that by Lemma 6.34(2) and (6.66), all the terms vanish except for

$$\langle \sigma(Z), [Z, \sigma^2(Z)]\rangle, \quad \langle \sigma(S), [S, \sigma^2(S)]\rangle, \quad (\sigma(Z), [S, \sigma^2(Z)]\rangle$$

and

$$\langle \sigma(S), [S, \sigma^2(Z)]\rangle;$$

moreover, these last two terms also vanish by virtue of conditions (6.68) and (6.69). It follows that $y = z - t\sigma(t)\sigma^2(t)s = 0$. This completes the proof of Proposition 6.24, and along with it Theorem 6.30.

We now proceed directly to proving that $H^1(L/E, G_0)$ is trivial. Take any $\xi \in H^1(L/E, G_0)$, and let $G = {}_\xi G_0$. If G is isotropic over E, then by applying Proposition 6.22 and bearing in mind that Theorems 6.4 and 6.6 have been proved for all groups except type E_8, we obtain $\xi = 1$. Therefore, below we can (and shall) always assume that G is E-anisotropic. Then, by Theorem 6.30 there exists a proper semisimple subgroup H of G which is L-isotropic and defined over E. Without loss of generality, we may assume that H is E-simple. Then H is isogenous to a group of the form $\mathbf{R}_{P/E}(F)$. Since Theorem 6.29 has been proved for all groups except those of type E_8, it follows that F belongs to type A_n because G is E-anisotropic. Since by construction E does not have any extensions of degree ≤ 4, *a priori* the only possible cases are:

(1) $[P : E] \geq 5$, $n = 1$;
(2) $P = E$.

In view of the fact that H is E-anisotropic and L-isotropic, it is easy to show that actually the only possible case is $P = E$, $n = 4$, i.e., H is a simple group of type A_4. Since E has no quadratic extensions, H automatically is an inner form; in other words, $H = \mathbf{SL}_1(D)$, where D is a skew field over

E of index 5. Moreover, $D \otimes_E L \simeq M_5(L)$, so L embeds in D as a maximal subfield. Let $T_1 = \mathbf{R}^{(1)}_{L/E}(\mathbb{G}_m)$ be the corresponding norm E-torus of G. Since G is L-split, the centralizer $C_1 = Z_G(T_1)$ is also an L-split E-group. If the semisimple part $H_1 = [C_1, C_1]$ is nontrivial, then by applying the same argument as we used for H we can establish the existence of a torus T_2 of H_1 having the form $T_2 = \mathbf{R}^{(1)}_{L/E}(\mathbb{G}_m)$. Then $T = T_1T_2$ is an L-split E-torus of G. On the other hand, if $H_1 = 1$, then $T = C_1$ will be such a torus.

By Proposition 6.19 there exists an E-embedding $T \to G_0$ such that ξ lies in the image of $\varphi\colon H^1(E,T) \to H^1(E,G_0)$; therefore the proof that $H^1(L/E,G_0)$ is trivial is completed by

PROPOSITION 6.25. *φ is trivial.*

PROOF: For each root α in $R = R(T,G)$, let $G(\alpha)$ denote the subgroup of G generated by the root subgroups $G_{\sigma^i(\alpha)}$ $(i = 0,1,2,3,4)$. We claim that $G(\alpha)$ is a simply connected simple E-group of type A_4. It is easy to see that $T(\alpha) = T \cap G(\alpha)$ is a maximal torus of $G(\alpha)$ and $R(T(\alpha), G(\alpha))$ is precisely the subsystem Σ_α of R of all the roots that are integral linear combinations of $\sigma^i(\alpha)$ $(i = 0,1,\dots,4)$. Since T is E-anisotropic, $\alpha+\sigma(\alpha)+\cdots+\sigma^4(\alpha) = 0$, and hence $\operatorname{rank}\Sigma_\alpha \leq 4$. On the other hand, σ induces an automorphism of Σ_α of order 5. But the only root system of rank ≤ 4 having this property is A_4. In the proof of Proposition 6.24 we showed that any two roots α, β in R for which $\alpha + \beta \in R$ are respectively the maximal root and $-\alpha_8$ with respect to a suitable base. By an analogous argument it is easy to show that, in a suitable base $\Pi \subset R$, $G(\alpha)$ is the group generated by the root subgroups G_γ, where $\gamma \in \{\alpha_8, \alpha_7, \alpha_6, \mu\}$ and μ is the maximal root. It follows that $G(\alpha)$ is simply connected.

Now form the direct product $T_0 = \prod_{\alpha \in R} T(\alpha)$, and consider the map $\theta_0\colon H^1(E,T_0) \to H^1(E,T)$ induced by $\theta_\alpha\colon H^1(E,T(\alpha)) \to H^1(E,T)$. Later we shall show that θ_0 is surjective, but meanwhile we use this fact to complete the proof of Proposition 6.25.

Let $\xi \in H^1(E,T)$ and write $\xi = \prod_{i=1}^{n} \theta_{\alpha_i}(\xi_i)$, where $\xi_i \in H^1(E,T(\alpha_i))$. We argue by induction on n. If $n = 1$, then $\xi = \theta_{\alpha_1}(\xi_1)$, and $\xi \in H^1(E,G(\alpha_1)) = 1$. In general we shall use our familiar procedure of componentwise trivialization of ξ. Namely, since $H^1(E,G(\alpha_n)) = 1$, we have $\xi_n = \{a_\tau\}$, where $a_\tau = g^{-1}\tau(g)$ for $\tau \in \operatorname{Gal}(\bar{E}/E)$ and suitable g in $G(\alpha_n)$. Consider the torus $T' = gTg^{-1}$ and the isomorphism $\psi\colon T \to T'$ given by $\psi(x) = gxg^{-1}$. In view of the fact that $g^{-1}\tau(g) \in T$, it is easy to show that T' and ψ are defined over E. Put $\xi' = \psi(\theta_{\alpha_1}(\xi_1)\dots\theta_{a_n-1}(\xi_{n-1})) \in H^1(E,T')$. One can immediately verify that

$\xi' = g\xi\tau(g)^{-1}$, and therefore it suffices to establish that ξ' is trivial. However, $\xi' = \psi(\theta_{\alpha_1}(\xi_1))\dots\psi(\theta_{\alpha_n-1}(\xi_{n-1}))$, and moreover $\psi(\theta_{\alpha_i}(\xi_i)) \in \theta_{\alpha_i'}(H^1(E,T'(\alpha_i')))$ where $\alpha_i' = \psi(\alpha_i)$, so the triviality of ξ' follows from the induction hypothesis.

To prove θ_0 surjective we give a method of computing $H^1(L/E,S)$ for an arbitrary E-anisotropic L-split torus S in terms of the group cohomology of the group of one-parameter subgroups $\mathbf{X}_*(S)$.

LEMMA 6.37. *The isomorphism $\mathbf{X}_*(S) \otimes L^* \to S_L$ and the cup-product induce an isomorphism*

$$\Phi_S\colon \hat{H}^{-1}(L/E, \mathbf{X}_*(S)) \otimes \hat{H}^2(L/E, L^*) \to \hat{H}^1(L/E,S).$$

PROOF: Put $\Gamma = \langle\sigma\rangle$ and let ε denote the element $1 + \sigma + \cdots + \sigma^4$ of the group ring $\mathbb{Z}[\Gamma]$. Now take the Γ-module $I = \mathbb{Z}[\Gamma]/\mathbb{Z}\varepsilon$. First we handle the special case $\mathbf{X}_*(S) = I$. The module $\mathbf{X}_*(S)$ occurs in the exact sequence

$$0 \to \mathbb{Z} \xrightarrow{[\varepsilon]} \mathbb{Z}[\Gamma] \to I \to 0,$$

where $[\varepsilon]$ denotes multiplication by ε, and S is a term in the exact sequence

$$1 \to \mathbb{G}_m \to \mathbf{R}_{L/E}(\mathbb{G}_m) \to S \to 1.$$

These sequences yield the isomorphisms

$$H^1(L/E,S) \simeq H^2(L/E,L^*),$$
$$\hat{H}^{-1}(L/E,I) \simeq \hat{H}^0(L/E,\mathbb{Z}) = \mathbb{Z}/5\mathbb{Z},$$

which can be combined in the commutative diagram

$$\begin{array}{ccccc} \hat{H}^{-1}(L/E,I) & \otimes & \hat{H}^2(L/E,L^*) & \xrightarrow{\Phi_S} & H^1(L/E,S) \\ \simeq\downarrow & & \| & & \simeq\downarrow \\ \hat{H}^0(L/E,\mathbb{Z}) & \otimes & \hat{H}^2(L/E,L^*) & \longrightarrow & H^2(L/E,L^*). \end{array}$$

Since the bottom row is obviously an isomorphism, Φ_S is also an isomorphism.

Thus it follows that Φ_S is an isomorphism in the case $\mathbf{X}_*(S) = I^n$. However I can be identified with the ring $\mathbb{Z}[\zeta_5]$ (where ζ_5 is a primitive 5-th root of unity) which is a principal ideal domain. But for any E-anisotropic torus S we have $\varepsilon\mathbf{X}_*(S) \subset \mathbf{X}_*(S)^{\operatorname{Gal}(L/E)} = (0)$, so $\mathbf{X}_*(S)$ can

be viewed as a module over $\mathbb{Z}[\Gamma]/\mathbb{Z}\varepsilon = I \simeq \mathbb{Z}[\zeta_5]$, and therefore $\mathbf{X}_*(S)$ has the form $\mathbf{X}_*(S) = \mathbb{Z}[\zeta_5]^n = I^n$, proving the lemma.

The lemma shows that to prove θ_0 surjective it suffices to establish that $\hat{H}^{-1}(L/E, \mathbf{X}_*(T_0)) \to \hat{H}^{-1}(L/E, \mathbf{X}_*(T))$ is surjective. But by definition $\hat{H}^{-1}(L/E, \mathbf{X}) = \ker N/(1-\sigma)\mathbf{X}$, where $N\chi = \varepsilon\chi$ is the norm map. Therefore, for the E-anisotropic torus S we have

$$\hat{H}^{-1}(L/E, \mathbf{X}_*(S)) = \mathbf{X}_*(S)/(1-\sigma)\mathbf{X}_*(S);$$

hence, in our case, everything follows from the surjectivity of the map $\oplus_{\alpha\in R}\mathbf{X}_*(T(\alpha)) \to \mathbf{X}_*(T)$, which is self-evident. Q.E.D.

This completes the proof of Theorems 6.4 and 6.6.

The validity of Theorem 6.6 for groups of type E_8 remained an open question for a long time. Theorem 6.30, which made it possible to complete the proof of Theorem 6.6, was obtained by Chernousov [6]. (Initially, Chernousov, in collaboration with Premet, tried to show that in fact any five root elements in the Lie algebra of type E_8 must generate a proper subalgebra; however, it turned out that five root elements in the generic position do generate the full algebra. Subsequently, Chernousov found the conditions on a root element X under which the subalgebra generated by $\sigma^i(X)$ $(i = 0, \ldots, 4)$ (notation as in the proof of Theorem 6.30) is proper, and then showed that these can be realized over a certain extension of the ground field. Ubdoubtedly, the argument given above was influenced to some extent by the initial joint work of Chernousov and Premet, which eventually did not prove successful. Note that Premet claims he was able to obtain some steps of the proof independently.) Theorem 6.4 for groups of type E_8, however, was known earlier (Kneser [9]). The crucial difference between the local case and the global one lies in the existence of the local Nakayama-Tate duality, which, combined with a detailed analysis of subgroups of the Weyl group, makes it possible to prove Proposition 6.25 for practically any torus, not only for the special tori which we have used.

BIBLIOGRAPHICAL NOTE: Much of the material set forth in §§6.2–6.3 is traditional (cf. Borel [8, §16], Voskresenskiĭ [3, Ch. 6]); and practically all of §6.4 is taken from Borel-Serre [1]. In contrast, this is the first complete exposition of results on precise computation of the cohomology of semisimple groups over local and number fields. The triviality of $H^1(K, G)$ for simply connected groups over a local field was established by Kneser [9]. In his lectures [12] he showed that Theorems 6.4 and 6.6 for the classical groups are equivalent to the well-known results on the properties and classification of quadratic, Hermitian, and other forms. (Since these results can be obtained without using cohomological techniques, we thereby obtain a proof

of Theorems 6.4 and 6.6 for the classical groups.) Our exposition uses only one result from the theory of quadratic forms—the Minkowski-Hasse theorem. We must also point out certain modifications in the proof of the Hasse principle for groups of type ${}^2A_n$, based on using the multinorm principle. Theorem 6.6 for the exceptional groups, excluding type E_8, was obtained by Harder [1], [2]; the case of type E_8 was analyzed by Chernousov [6]. (Note that for global function fields the triviality of $H^1(K, G)$ for semisimple simply connected groups of all types was established by Harder [11].) Several of the results on Galois cohomology are contained in Sansuc [1]. We did not take up the question of Galois cohomology of finite commutative groups, which are described by the Poitou-Tate theorems (cf. Serre [1]). A detailed exposition of these results may be found in a recent book by Milne [2].

In studying cohomology of semisimple groups we repeatedly used some results on approximation in algebraic groups and varieties, which will be treated in detail in the next chapter. Here we provide a complete list of these results:

(1) weak approximation for varieties of tori;
(2) weak approximation for spheres defined by quadratic, Hermitian, and other forms;
(3) weak approximation for any torus with respect to $S = V_\infty^K$;
(4) the surjectivity of $H^1(K, T) \to \prod_{v\in V_\infty^K} H^1(K_v, T)$ for any torus T;
(5) strong approximation for $G = \mathbf{SL}_n(D)$.

The reader may verify that these results do not rely on any results from Galois cohomology of semisimple groups, and therefore it was permissible to use them in this chapter.

7. Approximation in Algebraic Groups

This chapter is concerned with the quantitative aspect of the local-global principle—the question of when the elements of local groups G_{K_v} and their products can be approximated with any given accuracy by the elements of G_K. When such approximation is feasible, G is said to have *weak approximation*. Although this concept is meaningful for any field K, naturally we shall concern ourselves primarily with number fields (note, however, the remark at the end of §7.3). In contrast, strong approximation (i.e., approximation using elements which in addition satisfy certain integral conditions) applies only to global fields. We shall define weak, as well as strong, approximation for arbitrary algebraic varieties, although the most substantial results on approximation have been obtained so far only for algebraic groups. The existing methods are essentially based on analysis of the group structure on the set of rational points; therefore, before our exposition of approximation results, we discuss the well-known Kneser-Tits hypothesis on isotropic groups (cf. §7.2). Note, also, that beginning with this chapter the "synthetic" nature of the arithmetic theory of algebraic groups will become clearer still, both vis-à-vis basic ideas as well as applications. In particular, this chapter uses most of the results of the previous chapters.

7.1. Strong and weak approximation in algebraic varieties.

Let X be an algebraic variety defined over a number field K. The possibility of arbitrarily close approximation of the elements of the local spaces X_{K_v} by the elements of X_K actually means that X_K is dense under embedding in certain topological spaces constructed from X_{K_v}. Thus, from the topological point of view, it is natural to consider the topological direct product $\underline{X} = \prod_{v \in V^K} X_{K_v}$ or a part of it, $X_S = \prod_{v \in S} X_{K_v}$, where S is a subset of V^K; whereas, from the arithmetic point of view, one should look at the space of S-adeles X_{A_S} with its appropriate topology (cf. §5.1). In both cases there is a natural diagonal embedding $X_K \hookrightarrow \underline{X}$ ($X_K \hookrightarrow X_S$) and $X_K \hookrightarrow X_{A_S}$. With this terminology, we introduce the following

DEFINITION:

(1) We say that X satisfies the *weak approximation* property (resp. weak approximation with respect to $S \subset V^K$) if the diagonal embedding $X_K \hookrightarrow \underline{X}$ (resp., $X_K \hookrightarrow X_S$) is dense.

(2) X satisfies the *strong approximation* property with respect to a finite subset S of V^K if the diagonal embedding $X_K \hookrightarrow X_{A_S}$ is dense.[1]

[1] Note that when X is an algebraic group one may say equivalently that $X_S X_K$ must

When $S = V_\infty^K$ one speaks of *absolute strong approximation*.

We begin by describing the functorial properties of these concepts.

PROPOSITION 7.1.

(1) *If X and Y are biregularly isomorphic varieties over K, then either both have strong (resp., weak) approximation, or neither have.*
(2) *If $X = X_1 \times X_2$ over K, then the existence of strong (resp., weak) approximation in X is equivalent to the existence of the same type of approximation in both factors.*
(3) *If $X = R_{L/K}(Y)$, then the existence of strong (resp., weak) approximation in X over K with respect to a subset S of V^K is equivalent to the existence of the same type of approximation in Y over L with respect to the subset $\bar{S}$ of V^L consisting of all the extensions of valuations from S.*

The proof follows from the existence of natural homeomorphisms between the spaces involved in the definition of approximation. For example, $X_S \simeq Y_S$ under the conditions of (1), and $X_S \simeq Y_{\bar{S}}$ for any $S \subset V^K$ under the conditions of (3). (We leave it to the reader to work out the details.)

It should be noted that for the case $X = \mathbb{A}^1$ the definitions given above pass to the classical definitions of strong and weak approximation for K. In particular, Proposition 7.1 (2) and the relevant approximation theorems (cf. Theorems 1.4 and 1.5) imply that the affine space $\mathbb{A}^n$ has weak approximation and strong approximation with respect to any nonempty S. Since the variety of any unipotent K-group U is biregularly isomorphic over K to $\mathbb{A}^n$, where $n = \dim U$, parts (1) and (2) yield

COROLLARY. *Let $G = HR_u(G)$ be the Levi decomposition of a connected group G. The existence of strong (resp., weak) approximation for G is equivalent to the existence of the same type of approximation for H.*

For convenient reference we now present several elementary facts about strong and weak approximation.

PROPOSITION 7.2.

(1) *The existence of weak approximation in X with respect to an arbitrary subset S of V^K is equivalent to the existence of weak approximation with respect to all finite subsets S' of S.*
(2) *X satisfies strong approximation with respect to a finite subset S of V^K if and only if, for each finite subset T of V^K containing $S \cup V_\infty^K$, the set $X_{\mathcal{O}(T)}$ of T-integral points is dense in $X_{T\setminus S}$ (under the diagonal embedding). In particular, if G has strong approximation with respect to S, then it has weak approximation with respect to $V^K \setminus S$. If X is projective, then also the converse is true: weak approximation with respect to $V^K \setminus S$ implies strong approximation with respect to S.*
(3) *If X satisfies weak (resp., strong) approximation with respect to an arbitrary (resp. finite) subset S of V^K, then X satisfies the same type of approximation for any $S_1 \subset S$ (resp., finite $S_1 \supset S$).*
(4) *If X satisfies weak approximation with respect to S, then any open K-subvariety U of X also has weak approximation with respect to S.*

PROOF: (1) follows from the definition of the topology on the direct product.

To prove (2) recall that a base of open sets in X_{A_S} consists of sets of the form $W = \prod_{v\in T\setminus S} U_v \times \prod_{v\notin T} X_{\mathcal{O}_v}$, where T is a finite subset of V^K containing $S \cup V_\infty^K$ and U_v is an open subset of X_{K_v} for v in $T\setminus S$. Therefore strong approximation for X with respect to S amounts to the condition $X_K \cap W \neq \emptyset$ for such W, which, obviously, is equivalent to $X_{\mathcal{O}(T)} \cap \prod_{v\in T\setminus S} U_v$ being nonempty, i.e., to $X_{\mathcal{O}(T)}$ being dense in $X_{T\setminus S}$. In §3.1 we saw that $\mathbb{P}^n_{\mathcal{O}_v} = \mathbb{P}^n_{K_v}$ for all v in V_f^K; therefore for any realization of a projective variety X one has $X_{\mathcal{O}_v} = X_{K_v}$ for almost all v in V_f^K. Thus, taking the topological space X_{A_S} to be precisely $X_{V^K\setminus S}$ yields the second assertion.

(3) follows from the fact that for $S_1 \subset S$ (resp., $S_1 \supset S$) there is a natural continuous projection $X_S \to X_{S_1}$ (resp., $X_{A_S} \to X_{A_{S_1}}$) which agrees with the corresponding diagonal embeddings of X_K.

Lastly, to prove (4) it suffices to note that since the v-adic topology on X_{K_v}, defined in §3.1, is stronger than the Zariski topology, any open subset W of U_S is also open in X_S; therefore $W \cap X_K$ is nonempty and obviously is contained in U_K. This completes the proof of Proposition 7.2.

Strong approximation has a manifestly arithmetic character. In the basic case where $S \supset V_\infty^K$, the validity of strong approximation is equivalent to the solvability of a certain system of congruences in integral points of X. More precisely, let $X \subset \mathbb{A}^n$. Then any open subset of X_{A_S} contains a subset of the form

$$W = \prod_{i=1}^{r} \left(X_{K_{v_i}} \cap \left((a_1^i + \mathfrak{p}_{v_i}^{m_i}) \times \ldots \times (a_n^i + \mathfrak{p}_{v_i}^{m_i})\right)\right) \times \prod_{v\in S_1} X_{\mathcal{O}_v},$$

where $v_1, \ldots, v_r \notin S$, $S_1 = S \cup \{v_1, \ldots, v_r\}$, $m_1, \ldots, m_r$ are positive integers, and $a^i = (a_1^i, \ldots, a_n^i) \in X_{K_v}$. Therefore $X_K \cap W$ is nonempty if

be dense in X_A.

and only if there is a solution in $X_{\mathcal{O}(S_1)}$ for the system of congruences

$$x \equiv a^i \pmod{\mathfrak{p}_{v_i}^{m_i}}, \tag{7.1}$$

where $a \equiv b \pmod{\mathfrak{p}_v^m}$, for $a = (a_1, \dots, a_n)$ and $b = (b_1, \dots, b_n)$ lying in K_v^n but not necessarily in $\mathcal{O}_v^n$, means that $a_i - b_i \in \mathfrak{p}_v^m$ for all $i = 1, \dots, n$.

Therefore the question of strong approximation for X is the algebro-geometric version of the Chinese Remainder Theorem. In view of the fundamental role the latter plays in classical arithmetic, it is natural to expect the strong approximation theorem for algebraic groups, which we shall prove in §7.4, to lie at the foundation of important results in our theory. In the chapters that follow we shall see that this is indeed the case.

With this we conclude our discussion of questions of approximation with respect to arbitrary varieties. Most of the results which follow apply only to algebraic groups. It is completely natural to restrict the subject in this way, since if one were to examine the solvability of (7.1) only from the point of view of Diophantine geometry, i.e., without using group structure, the problem would become exceedingly complicated. Thus, we shall show below that absolute strong approximation holds for $G = \mathbf{SL}_2$, and therefore (7.1) must have a solution. On the other hand, G as an algebraic variety is defined by $xy - zt = 1$, and we highly recommend that the reader ascertain that it is not easy to lift the solutions of the congruences (7.1) to an integral solution satisfying those congruences. This example illustrates that it is not so much the geometric properties of G, but rather its group structure, that holds the key to strong approximation. Weak approximation, in contrast, is more closely related to geometry.

PROPOSITION 7.3. *Let X be an irreducible, smooth K-rational variety. Then X satisfies the weak approximation property.*

PROOF: The K-rationality of X means there exists a biregular K-isomorphism $\varphi: U \to W$ between open subsets $U \subset \mathbb{A}^l$ $(l = \dim X)$ and $W \subset X$. Propositions 7.1 and 7.2 imply that W has weak approximation, i.e., W_K is dense in $\prod_v W_{K_v}$. However, W_{K_v} is dense in X_{K_v} for any v, by Lemma 3.2. It follows that W_K, and thus certainly X_K, are dense in $\prod_v X_{K_v}$.

This proposition is the first example of the connection between the geometry and the arithmetic of linear algebraic groups. This interrelationship embraces a wide range of questions such as weak approximation, the validity of the Hasse principle, computation of the Tamagawa number, etc. A detailed analysis of all these questions would take us beyond the scope of this book, therefore we shall confine ourselves to some brief remarks in §7.3.

For our purposes, it suffices to present the corollaries that follow directly from Proposition 7.3.

COROLLARY 1. *Let X be a quadric; i.e., a surface in $\mathbb{A}^n$ $(n \geq 1)$ defined by an equation of the form $f(x_1, \dots, x_n) = a$, where f is a nondegenerate quadratic form over K and $a \in K^*$. If $X_K \neq \emptyset$, then X has weak approximation.*

Indeed, it is well known that X is smooth and, when $X_K \neq \emptyset$, is also a K-rational variety. Note that the question of strong approximation for X is more subtle (cf. Rapinchuk [8]).

The proposition just proved partially fills in the gap left in the previous chapter, where we used the validity of weak approximation for "spheres" related to all types of forms, i.e., for varieties given by $f(x) = a$, where f is a quadratic, Hermitian, or other form. As we saw in §6.6, the "spheres" corresponding to Hermitian forms over a quadratic extension L/K or over a quaternion skew field D/K, are in fact equivalent to quadrics in higher dimension, and therefore one may assume weak approximation to be proved for them. On the other hand, for skew-Hermitian forms over a quaternion skew field D, the rationality of the corresponding spheres is still an open question, so Proposition 7.3 is not directly applicable here. For this reason one must take a somewhat different approach which enables one to analyze all types of forms simultaneously. This approach is based on the following generalization of Proposition 7.3.

PROPOSITION 7.3′. *Let X be a smooth irreducible K-variety such that $X \times Y$ is rational over K, for a suitable K-variety Y. Then X satisfies weak approximation.*

The proof follows easily from Proposition 7.3 and Proposition 7.1 (2).

Now let f be a nondegenerate n-dimensional Hermitian (skew-Hermitian) form over D, provided with involution τ such that K is the fixed subfield under τ of the center of D.

PROPOSITION 7.4. *Let G be the connected component of the unitary group $\mathbf{U}_n(f)$. Then G is a rational variety over K. In particular, G has weak approximation.*

PROOF: Obtained using the well-known Cayley-Dickson parametrization. Namely, let $\mathfrak{g} = L(G)$ be the Lie algebra of G, and consider the correspondence

$$\varrho: X \mapsto \frac{E_n - X}{E_n + X}, \quad X \in \mathfrak{g}. \tag{7.2}$$

It turns out that ϱ gives a birational K-isomorphism between $\mathfrak{g}$ and G. For the proof, note that $\mathfrak{g} = \{X \in M_n(D) \otimes_K \bar{K} : {}^*XF + FX = 0\}$, since $\mathbf{U}_n(f) = \{x \in M_n(D) \otimes_K \bar{K} : {}^*xFx = F\}$, where we put ${}^*x = (\tau(x_{ji}))$ for $x = (x_{ij})$, and F is the matrix of f. Therefore, a direct computation using (7.2) shows that the image of ϱ falls in $\mathbf{U}_n(f)$, and hence also in G, since $\varrho(0) = E_n \in G$ and G is the component of the identity in $\mathbf{U}_n(f)$. In addition, the inverse map for ϱ is given by the same formula (7.2). Thus the rationality of G is established. It remains to note that group varieties are smooth, and therefore for such varieties weak approximation follows automatically from rationality.

Now we have all the necessary results to complete the proof of weak approximation for "spheres".

COROLLARY 2. *Let f be a nondegenerate n-dimensional $(n \geq 2)$ Hermitian (skew-Hermitian) form, and let $a \in D^*$ be a Hermitian (skew-Hermitian) element, respectively. Put $X = \{x \in D^n \otimes_K \bar{K} : f(x) = a\}$. If $X_K \neq \emptyset$, then X has weak approximation.*

Indeed, let $x \in X_K$. Consider the map $\varphi: G \to X$ given by $\varphi(g) = gx$, where, as above, G is the identity component of $\mathbf{U}_n(f)$. It follows from Witt's theorem that φ is surjective; i.e., X can be identified with the homogeneous space G/H, where $H = G(x)$ is the stabilizer of x; in particular, X is smooth. Moreover, by Witt's theorem one can show that $\varphi(G_L) = X_L$ for any extension L of K. Applying this to the field of rational functions $L = K(X)$, we obtain a rational section $\psi: X \to G$ defined over K, so $G \simeq X \times H$ birationally. But G is rational by Proposition 7.4; therefore the proof is completed by applying Proposition 7.3′.

A propos the question of rationality, unfortunately the groups described in Proposition 7.4 and the K-split groups basically exhaust the list of group varieties for which rationality is known. In particular, the question of rationality of the spinor varieties $\mathbf{Spin}_n(f)$ was open for a long time. These varieties are 2-fold covers of $\mathbf{SO}_n(f)$, whose rationality follows from Proposition 7.4. It is easy to show that $\mathbf{Spin}_n(f)$ is K-rational for $n \leq 5$ (cf. Platonov [18]); but, as Platonov [18],[19] has shown, over a suitable field K there exist nonrational spinor varieties for n of the form $4k+2$, for any $k \geq 1$. This result was obtained thanks to the development of methods in reduced K-theory which, at the time, made it possible to establish the existence of nonrational varieties of type $\mathbf{SL}_1(D)$ (cf. Platonov [17], Voskresenskiĭ [3]). However, if K is locally compact, then any spinor variety over K is always K-rational (cf. Platonov [18], Platonov-Chernousov [1]); moreover for $K = \mathbb{R}$, most group K-varieties are known to be rational. For number fields, the rationality of $\mathbf{Spin}_n(f)$ is known only over $\mathbb{Q}$ (cf. Chernousov [1]).

Nevertheless, the question of weak approximation for algebraic groups over number fields is solved by other methods (cf. §7.3).

One more important application of Proposition 7.3 is

COROLLARY 3. *Let G be a reductive algebraic group over a number field K, and let $\mathcal{T}$ be the variety of its maximal tori. Then $\mathcal{T}$ has weak approximation. In particular, if S is a finite subset of V^K and, for each v in S, $T(v)$ is a given maximal K_v-torus of G, then there exists a maximal K-torus T of G which, for any v in S, is conjugate to $T(v)$ via an element of G_{K_v}.*

Indeed, $\mathcal{T}$ is smooth since it is a homogeneous space of G. Its rationality over K was established in Theorem 2.18. Therefore $\mathcal{T}$ satisfies weak approximation. Furthermore, if x_v is the point in $\mathcal{T}$ $(v \in S)$ corresponding to $T(v)$, then the tori from the conjugacy class $\{gT(v)g^{-1} : g \in G_{K_v}\}$ correspond exactly to the points of the orbit $U_v = G_{K_v}x_v$. But U_v is open in $\mathcal{T}_{K_v}$ (cf. Proposition 3.3, Corollary 2), therefore by the weak approximation property for $\mathcal{T}$ one can find a point x in $\mathcal{T}_K \cap \prod_{v \in S} U_v$. Its corresponding maximal torus $T \subset G$ is the desired torus. (We call the reader's attention to the fact that weak approximation for the variety of tori always holds, independently of the validity of weak approximation for G. This is not typical, since usually weak approximation in a homogeneous space is deduced from weak approximation in the group (cf. proof of Corollary 2), and not the other way around.)

7.2. The Kneser-Tits conjecture.

As we remarked above, one cannot make much progress on approximation questions for algebraic groups without using the group structure. Therefore in this chapter on approximation we must devote a section exclusively to analysis of group structure. Since the exposition of such questions could fill an entire volume, this section necessarily presents no more than an overview of the subject. However, we shall give a complete proof of the basic result, validity of the Kneser-Tits conjecture over local fields (Theorem 7.6), which is needed later on.

The structure theory of linear algebraic groups provides a virtually exhaustive description of the structure of an algebraic group G over an algebraically closed field. However, the situation changes drastically when one considers groups of rational points G_K over a field K which is not algebraically closed. The basic difficulties in this regard arise in the case of G simple, which we shall take up here.

Also, one must distinguish between the cases where G is K-anisotropic and K-isotropic, respectively. In the former case the structure of G_K essentially depends not only on the structure of G itself, but also on the

arithmetic of K. In particular, choosing G and K appropriately, one can have G_K residually finite or even prosolvable (cf. §1.4.4). On the other hand, in the isotropic case, G_K always contains a "large" normal subgroup which does not contain any proper noncentral normal subgroups. More precisely, for an absolutely simple group G defined and isotropic over K, let G_K^+ denote the subgroup (in fact, a normal subgroup of G_K) generated by the K-rational elements of the unipotent radicals of its parabolic subgroups defined over K (note, that in the basic case where K is perfect, G_K^+ can be defined simply as the subgroup generated by the K-rational unipotent elements). Then one has the following

THEOREM 7.1 (TITS [1]). *Suppose K contains at least 4 elements. Then any subgroup of G_K normalized by G_K^+ either contains G_K^+ or is central. In particular, G_K^+ does not have any nontrivial noncentral normal subgroups.*

The proof of this theorem, which we will not present here, involves constructing a BN-pair (cf. §3.4) in G_K. Note that for the classical groups the theorem can be obtained using methods of geometric algebra (cf. Artin [1], Dieudonné [2]).

Theorem 7.1 tells us the structure (at least of the normal subgroups) of G_K when $G_K^+ = G_K$. This result has been known for some time when the simply connected group G is K-split (Chevalley [4]) or K-quasisplit (Steinberg [2]). In particular, by virtue of Proposition 6.1 this gives a complete picture in case K is finite.

PROPOSITION 7.5. *If G is simply connected and K is finite, then $G_K^+ = G_K$. In particular, if $|K| \geq 4$, then G_K does not have any nontrivial noncentral normal subgroups.*

(The exceptional cases of the fields F_2 and F_3 are analyzed in Tits [1].)

Below we shall discuss results on when G_K^+ coincides with G_K, for other types of fields. It is well-known that $G_K^+ = G_K$ if G is a group of type B_n, C_n $(n \geq 1)$, or a special form of one of the exceptional groups (cf. Tits [4]). These results evidently motivated the formulation of the following natural conjecture (cf. Tits [1]).

CONJECTURE (KNESER-TITS). *$G_K^+ = G_K$ for any simply connected K-simple group G defined and isotropic over an arbitrary field K.*

The assumption that G is simply connected is essential and obviously cannot be omitted. First of all, we note that if $\pi\colon \tilde{G} \to G$ is the universal K-covering and K is perfect, then $\pi(\tilde{G}_K^+) = G_K^+$. Indeed, let g be a unipotent element of G_K, and write $g = \pi(x)$ for $x \in \tilde{G}$. If $x = x_s x_u$ is the Jordan decomposition, then clearly $\pi(x_s) = 1$ and $\pi(x_u) = g$, so we may assume x to be unipotent. For any $\sigma \in \mathrm{Gal}(\bar{K}/K)$ we have $\pi(\sigma(x)) = \sigma(g) = g = \pi(x)$,

so $\sigma(x) = fx$, where $f \in F = \ker\pi$. But F consists of semisimple elements; therefore it follows from the unipotency of x and $\sigma(x)$ that $f = 1$, i.e., $x \in \tilde{G}_K$. We have shown that any unipotent element of G_K is the image of a unipotent element of $\tilde{G}_K$. Since K is perfect, any unipotent element of G_K lies in the unipotent radical of a suitable parabolic K-subgroup, it follows that $\pi(\tilde{G}_K^+) = G_K^+$, as desired. There is, however, an extensive class of K for which $\pi(\tilde{G}_K) \neq G_K$ when $\ker\pi \neq 1$.

THEOREM 7.2 (PLATONOV [10]). *Let K be a finitely generated infinite field, and let $\pi\colon \tilde{G} \to G$ be a nontrivial central K-isogeny of connected algebraic K-groups. Then $\pi(\tilde{G}_K) \neq G_K$. In particular, if G is not simply connected but is isotropic over an infinite, finitely generated field K, then $G_K \neq G_K^+$.*

The Kneser-Tits conjecture is obviously true for K algebraically closed. However, even the case of the field of real numbers requires a more subtle analysis.

PROPOSITION 7.6 (E. CARTAN [1]). *Let G be a simply connected simple algebraic group over $\mathbb{R}$. Then $G_{\mathbb{R}}$ does not have any nontrivial noncentral normal subgroups. In particular, $G_{\mathbb{R}}$ is connected, and if in addition G is $\mathbb{R}$-isotropic, then $G_{\mathbb{R}}^+ = G_{\mathbb{R}}$.*

PROOF: The case where G is $\mathbb{R}$-anisotropic, i.e., if G is $G_{\mathbb{R}}$ compact, was treated in §3.2 (cf. Proposition 3.6). For the isotropic case the proof uses several structural results about G which hold over any K and which we shall need again later on (cf. Borel-Tits [1]). Let S be a maximal K-split torus of G, let $H = Z_G(S)$ be its centralizer, and let U and U^- be the unipotent radicals of two opposite minimal parabolic K-subgroups containing S. Then the product morphism gives a K-isomorphism $U \times H \times U^-$ on a Zariski-open subset W of G. Since G is connected, $V = W \cap gW^{-1}$ is nonempty and open for any g in G_K; therefore $V \cap G_K = W_K \cap gW_K^{-1} \neq \emptyset$, since G_K is dense in G (cf. Theorem 2.2). Thus, $g \in W_K W_K$; in particular, W_K generates G_K. It follows that

$$G_K/G_K^+ \simeq H_K/(H_K \cap G_K^+),$$

so $G_K^+ = G_K$ if and only if $H_K \subset G_K^+$.

Furthermore, let us split H into its components. Let S' be the connected component of the center of H (note that generally $S' \neq S$). Then S' is a torus and S is a maximal K-split subtorus of S'. Therefore S' can be written as the almost direct product $S' = S \cdot S''$, where S'' is the maximal K-anisotropic subtorus of S'. In turn, $H = D \cdot S'$, where $D = [H, H]$ is a semisimple K-anisotropic group. Put $B = D \cdot S''$. Then $H = B \cdot S$ is an

almost direct product, and B is anisotropic over K. It is well known (cf. Borel-Tits [2]), that S is contained in a simply connected K-split semisimple subgroup of G, and consequently $S_K \subset G_K^+$.

Now we shall use specific properties of $\mathbb{R}$. Let us consider the commutative diagram

$$\begin{array}{ccc} H & \longrightarrow & H/S \\ \uparrow & & \uparrow \simeq \\ B & \xrightarrow{\alpha} & B/B\cap S \end{array}$$

and show that $\alpha(B_{\mathbb{R}}) = (B/B\cap S)_{\mathbb{R}}$. The group $B/B\cap S$ is anisotropic over $\mathbb{R}$; therefore $(B/B\cap S)_{\mathbb{R}}$ is compact and hence also connected (Theorem 3.6, Corollary 1). Therefore, by Theorem 3.6, Corollary 1, $\alpha(B_{\mathbb{R}}) = (B/B\cap S)_{\mathbb{R}}$. Hence $H_{\mathbb{R}} = B_{\mathbb{R}}S_{\mathbb{R}}$. Since $S_{\mathbb{R}} \subset G_{\mathbb{R}}^+$, it suffices to establish that $B_{\mathbb{R}} \subset G_{\mathbb{R}}^+$. However, since $B_{\mathbb{R}}$ is also compact, and hence connected, the desired inclusion follows from the openness of $G_{\mathbb{R}}^+$ (Theorem 3.3). This completes the proof of Proposition 7.6.

The case $K = \mathbb{R}$ is apparently the only one in which the proof of the Kneser-Tits conjecture is based on general structural considerations. In all the remaining cases, as a rule, one has to examine each type of simple group separately. This becomes evident in the case of a non-Archimedean locally compact field K (which is the most important case when considering approximation problems). In this case the first proof of the Kneser-Tits conjecture is due to Platonov. It is based on the classification of simple algebraic groups over local fields and consists of reduction to the case of classical groups, for which the proof is obtained by other considerations. We begin our exposition of the proof with a review of the necessary results on the classical groups.

Groups of type A_n hold the dominant place in the classical groups. If G is an inner form of type A_n, then $G = \mathbf{SL}_m(D)$, where D is a finite-dimensional central skew field over K (cf. §2.3). Then G is K-isotropic if and only if $m \geq 2$; and in this case we let $SL'_m(D)$ denote the subgroup of $G_K = SL_m(D)$ generated by transvections, i.e., by those matrices x in $SL_m(D)$ which in a suitable base of D^m have the form of an elementary matrix $e_{ij}(\alpha)$, $\alpha \in D$, $i \neq j$. It is easy to see that each elementary matrix is unipotent (and, moreover, lies in the unipotent radical of a suitable parabolic K-subgroup), and therefore $SL'_m(D) \subset G_K^+$. On the other hand, $SL'_m(D)$ is a normal subgroup of $SL_m(D)$ (and even of $GL_m(D)$), so $G_K^+ = SL'_m(D)$, by Theorem 7.1. Thus

$$G_K/G_K^+ \simeq SL_m(D)/SL'_m(D).$$

But the Dieudonné determinant (cf. Artin [1], Dieudonné [2]) induces an isomorphism of the latter quotient group on the reduced Whitehead group $SK_1(D) = SL_1(D)/[D^*, D^*]$ of D. Thus, for $G = \mathbf{SL}_m(D)$ $(m \geq 2)$ the Kneser-Tits conjecture is equivalent to the Tanaka-Artin conjecture on the triviality of $SK_1(D)$, formulated in 1943 (cf. also Bass [2, p. 222]).

Similarly, if G is an outer form of type A_n, then $G = \mathbf{SU}_m(f)$, where f is a nondegenerate m-dimensional Hermitian form over D with involution τ of the second kind, and K is the subfield of τ-invariant elements of the center L of D. Then G is K-isotropic if and only if f is isotropic (cf. §2.3) and in this case G_K^+ is precisely the subgroup $TU_m(f)$ generated by the unitary transvections. Furthermore, the Wall norm induces an isomorphism of $SU_m(f)/TU_m(f)$ on the reduced unitary Whitehead group $SUK_1(D)$. The latter is defined as Σ'/Σ, where Σ is the subgroup of D^* generated by all τ-symmetric elements, and Σ' consists of elements with symmetric reduced norm (for details, cf. Yanchevskiĭ [2]).

THEOREM 7.3. *Let D be a finite-dimensional skew field (resp., a finite-dimensional skew field with involution of the second kind) over a local or global field. Then the reduced Whitehead group $SK_1(D)$ (resp., the reduced unitary Whitehead group $SUK_1(D)$) is trivial.*

The triviality of $SK_1(D)$ was proved in Chapter 1 (cf. §1.4–1.5). The triviality of $SUK_1(D)$ over a local field is obvious, since here $D = L$. The case for a global field is treated in Platonov-Yanchevskiĭ [1].

Theorem 7.3 ceases to be true over an arbitrary field, i.e., in general the Kneser-Tits conjecture is false. We shall discuss this matter at the end of the section, but for now we point out a class of groups for which the Kneser-Tits conjecture does hold over an arbitrary field. First of all, there are the spinor groups $G = \mathbf{Spin}_n(f)$, $n \geq 3$, where f is a nondegenerate quadratic form over K. Then G is K-isotropic if and only if f is K-isotropic (cf. §2.3), and then well-known results from geometric algebra (cf. Artin [1], Dieudonné [2]) provide a complete picture of the structure of the corresponding special orthogonal group $\mathbf{SO}_n(f)$. Namely, the image of $\mathbf{Spin}_n(f)_K$ in $\mathbf{SO}_n(f)_K$ under the natural 2-fold covering $\pi\colon \mathbf{Spin}_n(f) \to \mathbf{SO}_n(f)$ (which is the kernel of the spinor norm) has no proper noncentral normal subgroups, and

$$\mathbf{SO}_n(f)_K/\pi(\mathbf{Spin}_n(f)_K) \simeq K^*/K^{*2}.$$

However, $\ker\pi = \{\pm 1\}$ embeds in $\mathbf{Spin}_3(g)$, where g is a three-dimensional isotropic subform of f; and since $\mathbf{Spin}_3(g) \simeq \mathbf{SL}_2$ over K,

$$-1 \in \mathbf{Spin}_3(g)_K^+ \subset \mathbf{Spin}_n(f)_K^+,$$

thereby yielding $\mathbf{Spin}_n(f)_K^+ = \mathbf{Spin}_n(f)_K$.

It remains to examine unitary groups over skew fields with involution of the first kind. Thus, let D be a skew field over K with involution τ of the first kind and the first type (the latter means that if $[D : K] = m^2$, then $\dim D^\tau = \frac{m(m+1)}{2}$). If a nondegenerate sesquilinear form f of degree n is skew-Hermitian, then, as shown in §2.3, $G = \mathbf{SU}_n(f)$ is a simply connected simple group of type C_l, and the Kneser-Tits conjecture always holds for it, as Dieudonné [1] has shown. For f a Hermitian form, $G = \mathbf{SU}_n(f)$ is a non-simply connected group of type D_l, and the Kneser-Tits conjecture is known to hold for the simply connected cover $\tilde{G}$ when D is a quaternion skew field (cf. Seip-Hornix [1]). Thus, the Kneser-Tits conjecture holds over an arbitrary field for all groups of type B_l and C_l, and for groups of type D_l arising from either a field or a quaternion skew field. Since over local and global fields these exhaust all the classical groups (cf. §2.3), we can sum up our discussion of the Kneser-Tits conjecture for such groups.

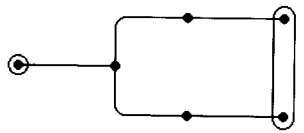
PROPOSITION 7.7. *Let K be a local or global field. Then the Kneser-Tits conjecture holds for any simple simply connected K-group G of one of the types A_l, B_l, C_l or D_l (possibly excluding ${}^3D_4$ and ${}^6D_4$).*

The proof of the Kneser-Tits conjecture for arbitrary groups can be reduced to the case of the classical groups as follows: Suppose a simply connected simple K-group G is isotropic over K, and let S be a maximal K-split torus of G. In proving Proposition 7.6 we saw that $G_K^+ = G_K$ is equivalent to $H_K \subset G_K^+$, where $H = Z_G(S)$ is the centralizer of S. To establish this inclusion one constructs simply connected simple K-isotropic subgroups G_i of G normalized by S, for which the Kneser-Tits conjecture has already been proved (such as G_i of classical type), and such that the groups H_{i_K}, where $H_i = Z_{G_i}(S \cap G_i)^0$, generate H_K. (Note that $(S \cap G_i)^0$ is a maximal K-split torus of G and $H_i \subset H$.) If such a construction is possible, then $H_{i_K} \subset G_{i_K} = G_{i_K}^+ \subset G_K^+$, and hence $H_K \subset G_K^+$, as desired.

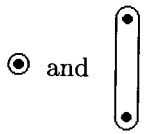
This method was first applied by Platonov [4] to prove the Kneser-Tits conjecture over a local field. There the G_i's were constructed by discarding one or more distinguished vertices in the Tits index of G; therefore this method was called the *vertex elimination procedure*. This method was later elaborated by Prasad and Raghunathan [3], who showed that for the G_i's one could always take groups of K-rank 1. Thus the proof of the Kneser-Tits conjecture over arbitrary fields was reduced to groups of rank 1. For a precise statement of these results we need to recall several definitions and introduce some additional notation.

Take a maximal K-torus T of G, containing a maximal K-split torus S. Let $R = R(T, G)$ be the corresponding root system, and let Π be a subsystem of simple roots which is (uniquely) defined by fixing a Borel subgroup B of G which contains T and is contained in a minimal parabolic K-subgroup. Let Π_0 denote the subset of Π consisting of those roots whose restriction to S is trivial; then $\Pi \setminus \Pi_0$ is precisely the set of distinguished vertices in the Tits index of G. In §2.1.14 we defined the natural action of $\mathcal{G} = \mathrm{Gal}(\bar{K}/K)$ on Π (called the *-action). It turns out that Π_0 and $\Pi \setminus \Pi_0$ are invariant under this action; moreover, the number of $\mathcal{G}$-orbits on $\Pi \setminus \Pi_0$ equals the K-rank of G.

For an arbitrary subset Θ of Π, put $T(\Theta) = \left(\bigcap_{\theta \in \Theta} (\ker \theta)\right)^0$ and $H(\Theta) = Z_G(T(\Theta))$, and let $G(\Theta)$ denote the commutator subgroup of $H(\Theta)$. (In particular, $H = H(\Pi_0)$ is the centralizer of a maximal K-split torus, and $G_0 = G(\Pi_0)$ is the anisotropic kernel of G.) For the most part we shall work with $\mathcal{G}$-invariant subsets Θ containing Π_0. The corresponding group $G(\Theta)$ is a simply connected semisimple (but not necessarily simple) K-group (Borel-Tits [2], 43), and its K-simple components can be easily found using the Tits index: they correspond to the orbits of $\mathcal{G}$ on the set of connected components of the subdiagram of Π in which only the vertices of Θ and the adjacent edges remain. (For example, if the index looks like



and $\Theta = \Pi_0$, then $G(\Theta)$ has two K-simple components,



of which one has type A_1 and the other is obtained from a group of type A_1 by restriction of scalars from a quadratic field extension of K.) Let $\Theta_1, \ldots, \Theta_r$ be all the $\mathcal{G}$-orbits on $\Pi \setminus \Pi_0$. Then $G(\Theta_i \cup \Pi_0)$ has K-rank equal to 1, and consequently has a unique K-simple K-isotropic component G_i. With this notation, we have

THEOREM 7.4 (PRASAD-RAGHUNATHAN [3]). *Suppose G has K-rank ≥ 2. Then H_K is generated by H_{i_K}, where $H_i = H \cap G_i$. In particular, if the Kneser-Tits conjecture holds for all the G_i, then it also holds for G.*

The proof is obtained by reducing to the following cohomological assertion, which is interesting in its own right.

THEOREM 7.5. *Let $\Pi_1, \ldots, \Pi_d$ be $\mathcal{G}$-invariant subsets of $\Pi \setminus \Pi_0$ such that*

$\bigcap_{i=1}^{d} \Pi_i = \emptyset$. *Then the kernel of the natural map*

$$H^1(K, G_0) \to \prod_{i=1}^{d} H^1(K, G(\Pi_i \cup \Pi_0))$$

is trivial.

The proof of Theorem 7.5, which we omit here, referring the reader to Prasad-Raghunathan [3], becomes trivial in the case of non-Archimedean local fields, of primary interest to us here, since then $H^1(K, G_0) = 1$ (Theorem 6.4).

PROOF OF THEOREM 7.4: Let Π_i denote the complement of Θ_i in $\Pi \setminus \Pi_0$, and put $C_i = H(\Pi_i \cup \Pi_0)$ and $D_i = G(\Pi_i \cup \Pi_0)$. Note that $H \subset C_i$, $G_0 \subset D_i$ for any $i = 1, \ldots, r$.

LEMMA 7.1. *The canonical map*

$$H/G_0 \to \prod_{i=1}^{r} C_i/D_i$$

is an isomorphism.

PROOF: Put $T_\alpha = T \cap G_\alpha$, where G_α is the root subgroup coinciding in our notation with $G(\{\alpha\})$. It is well known (cf. Steinberg [2]) that $T = \prod_{\alpha \in \Pi} T_\alpha$, and consequently, for any subset Θ of Π, the subgroup T_Θ generated by T_α ($\alpha \in \Theta$) is the direct product $\prod_{\alpha \in \Theta} T_\alpha$. It is easy to see that $T_\Theta \subset G(\Theta)$. But

$$\text{(7.3)} \quad \operatorname{rank} G(\Theta) = \dim T - \dim Z(H(\Theta)) \leq \dim T - \dim T(\Theta) = \dim T_\Theta,$$

so T_Θ is in fact a maximal torus of $G(\Theta)$, and $T \cap G(\Theta) = T(\Theta)$. Hence the inequality (7.3) is actually an equality, and as a result $Z(H(\Theta))^0 \subset T(\Theta) \subset T$. Since $H(\Theta) = G(\Theta)Z(H(\Theta))^0$, it follows that $H(\Theta) = G(\Theta)T$. But $T = T_\Theta \times T_{\Pi \setminus \Theta}$ and $T_\Theta \subset G(\Theta)$; therefore $H(\Theta) = G(\Theta)T_{\Pi \setminus \Theta}$. On the other hand,

$$T_{\Pi \setminus \Theta} \cap G(\Theta) = T_{\Pi \setminus \Theta} \cap (T \cap G(\Theta)) = T_{\Pi \setminus \Theta} \cap T_\Theta = 1,$$

so $H(\Theta)$ is actually the semidirect product of $G(\Theta)$ and $T_{\Pi \setminus \Theta}$. It follows that in the commutative diagram

$$\begin{array}{ccc} H/G_0 & \xrightarrow{\alpha} & \prod_{i=1}^{r} C_i/D_i \\ \uparrow & & \uparrow \\ T(\Pi \setminus \Pi_0) & \longrightarrow & \prod_{i=1}^{r} T(\Theta_i) \end{array}$$

induced by the respective embeddings, all the arrows other than α are isomorphisms. Therefore also α is an isomorphism. Lemma 7.1 is proved.

Now the commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & G_0 & \longrightarrow & H & \longrightarrow & H/G_0 & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \prod_{i=1}^{r} D_i & \longrightarrow & \prod_{i=1}^{r} C_i & \longrightarrow & \prod_{i=1}^{r} (C_i/D_i) & \longrightarrow & 1 \end{array}$$

induces the following commutative diagram of Galois cohomology with exact rows:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & G_{0K} & \longrightarrow & H_K & \longrightarrow & (H/G_0)_K & \longrightarrow & H^1(K, G_0) \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow \beta \\ 1 & \longrightarrow & \prod_{i=1}^{r} D_{iK} & \longrightarrow & \prod_{i=1}^{r} C_{iK} & \longrightarrow & \prod_{i=1}^{r} (C_i/D_i)_K & \longrightarrow & \prod_{i=1}^{r} H^1(K, D_i). \end{array}$$

Since $D_i = G(\Pi_i \cup \Pi_0)$ and $\bigcap_{i=1}^{r} \Pi_i = \emptyset$, Theorem 7.5 implies that the kernel of β is trivial. Therefore the natural homomorphism

$$H_K/G_{0K} \to \prod_{i=1}^{r} C_{iK}/D_{iK}$$

is an isomorphism. It follows that H_K is generated by the subgroups

$$F_i = H_K \cap \Big(\bigcap_{j \neq 1} D_{iK}\Big) = (H \cap G(\Theta_i \cup \Pi_0))_K.$$

We have $H \cap G(\Theta_i \cup \Pi_0) = A_i \times H_i$, where the A_i are the products of the K-anisotropic factors of $G(\Theta_i \cup \Pi_0)$, so $F_i = A_{i_K} H_{i_K}$. It remains to note that $A_i \subset G_0$, for each i; and since the Tits index of G is connected, every K-simple component of G_0 lies in a suitable G_j and consequently also in an H_j. Q.E.D.

Now we can easily complete the proof of the main result in this section.

THEOREM 7.6 (PLATONOV [4]). *Let K be a non-Archimedean locally compact field. Then the Kneser-Tits conjecture holds for any simple simply connected K-isotropic group G, i.e $G_K^+ = G_K$.*

PROOF: Since groups of type ${}^3D_4$ and ${}^6D_4$ are quasisplit (cf. Proposition 6.15) and hence do not require special consideration, in view of Proposition 7.7 and Theorem 7.4 it suffices to establish that there are no exceptional groups of K-rank 1. Let us apply Propositions 6.15 and 6.16. Then all the groups of type E_8, F_4, G_2 are split over K, so they need not be considered. Any group of type E_7 is split over a quadratic extension of K, so its anisotropic kernel also has this property. On the other hand, as Theorem 6.5 implies, the anisotropic kernel is the product of groups which are inner forms of type A_n. Therefore the anisotropic kernel must have type $A_1 + \cdots + A_1$. But the diagram of such a type cannot be obtained from the diagram of type E_7 by discarding one vertex, so the K-rank of the original group of type E_7 must be greater than 1.

An analogous argument can be applied to inner forms of type E_6. These forms are split over an extension of K of degree 3, so it follows that the anisotropic kernel must have type $A_2 + \cdots + A_2$. But in order to obtain a diagram of such a type from E_6 one must discard at least two vertices. Any outer form of type ${}^2E_6$ is quasisplit over K and has rank 4. Q.E.D.

Thus, there are a significant number of results verifying the Kneser-Tits conjecture for various groups and for various classes of fields. These results led to the opinion that the conjecture ought to hold in general. In 1975, however, the first author disproved this conjecture. First, in [13] he gave examples of skew fields defined over a rational function field $\mathbb{Q}(x, y)$ for which $SK_1(D) \neq 1$, and then in subsequent papers (cf. [14]–[16]) he developed reduced K-theory for computing $SK_1(D)$. It turned out that $SK_1(D)$ can be any finite, or even infinite, abelian group of finite exponent, for suitable D and K. Following papers [13]–[16], intensive work on reduced K-theory was begun by others (cf. Draxl-Kneser [1]). The results obtained in these subsequent papers generalize the original theorems somewhat and go into greater detail. A survey of the basic results of reduced K-theory may be found in Platonov's talk [17] at the Helsinki International Congress of Mathematicians, Tits' lecture [4] at the Bourbaki seminar, and in the papers of the Draxl-Kneser seminar [1].

Analogous results have also been obtained for the reduced unitary Whitehead group. Platonov-Yanchevskiĭ [3] showed that $SUK_1(D)$ can be nontrivial; later Yanchevskiĭ [2] developed reduced unitary K-theory, which is the analog of reduced K-theory for the unitary case and in many instances makes it possible to compute $SUK_1(D)$.

In conclusion, we note that examples have recently been constructed of simply connected K-isotropic groups G of type D_n for which $G_K^+ \neq G_K$ (cf. Monastyrni-Yanchevskiĭ [1]). Thus, we have quite a complete picture of the Kneser-Tits conjecture for the classical groups. Several of the exceptional groups are examined in Tits [4].

7.3. Weak approximation in algebraic groups.

In this section we shall show that weak approximation almost always holds for a connected algebraic group G. Namely, we have

THEOREM 7.7. *Let G be a connected algebraic group defined over an algebraic number field K. Then there exists a finite subset S_0 of V_f^K such that G has the weak approximation property with respect to $V^K \setminus S_0$. In particular, G always satisfies the weak approximation property with respect to $S = V_\infty^K$.*

There are examples which show that in general one cannot let $S_0 = \emptyset$, even when G is semisimple. However, weak approximation always holds in the "extreme" cases of simply connected and adjoint groups.

THEOREM 7.8. *Let G be a semisimple group, either simply connected or adjoint, defined over a number field K. Then G satisfies the weak approximation property.*

The proof of this result is based on reduction theory, the validity of the Kneser-Tits conjecture for local fields, the Hasse principle for simply connected groups, and a single sufficient condition for weak approximation in algebraic tori, first noted by Serre (unpublished).

PROPOSITION 7.8. *Let T be an algebraic K-torus, split over a Galois extension L/K, let $\mathcal{G} = \mathrm{Gal}(L/K)$, and let S be a finite subset of V^K. Assume that for each v in S the following condition holds:*

(7.4) *There exists $v' \notin S$ for which the decomposition groups $\mathcal{G}(w)$ and $\mathcal{G}(w')$ of suitable extensions $w|v$ and $w'|v'$ coincide.*

Then T has weak approximation with respect to S. Condition (7.4) is automatically satisfied if the local Galois group $\mathrm{Gal}(L_w/K_v)$ is cyclic for $w|v$.

PROOF: Put $H = \mathbf{R}_{L/K}(T)$ and let $\varphi: H \to T$ be the norm map (cf. proof of Proposition 6.7). It is easy to see that $N = \ker\varphi$ is also an algebraic K-torus. We have $H^1(K,H) = H^1(L,T) = 1$, since T is L-split. Analogously, $H^1(K_v,H) = 1$ for any v in V^K. The exact sequence

$$1 \to N \to H \xrightarrow{\varphi} T \to 1 \tag{7.5}$$

for any finite subset S of V^K induces the following commutative diagram of Galois cohomology with exact rows:

$$\begin{array}{ccccccc} H_K & \xrightarrow{\varphi} & T_K & \longrightarrow & H^1(K,N) & \longrightarrow & 1 \\ \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\gamma} & & \\ H_S & \xrightarrow{\Phi} & T_S & \longrightarrow & \prod_{v\in S} H^1(K_v,N) & \longrightarrow & 1 \end{array}$$

in which α, β are diagonal embeddings, γ is the product of the restriction maps $H^1(K,N) \to H^1(K_v,N)$, and Φ is induced by φ. Since T is split over L, we have

$$H_K \simeq T_L \simeq L^{*d}, \quad \text{and}$$
$$H_S \simeq T_{\bar{S}} \simeq \prod_{w\in\bar{S}} L_w^{*d},$$

where $d = \dim T$ and $\bar{S}$ is the aggregate of all the extensions to L of valuations from S; so weak approximation for L implies that α is dense. It follows that $\beta(\varphi(H_K))$ is dense in $\Phi(H_S)$; and since $\Phi(H_S)$ is open in T_S (cf. Proposition 3.3, Corollary 1), we obtain that weak approximation for T relative to S is equivalent to

$$T_S = \beta(T_K)\Phi(H_S).$$

This equation, as one easily sees, is precisely equivalent to the surjectivity of γ. To compute the image of γ let us consider the exact sequence

$$1 \to N_L \to N_{A_L} \to C_L(N) \to 1,$$

where N_{A_L} is the adele group of N over L, and $C_L(N) = N_{A_L}/N_L$ is the corresponding adele class group. Passing to cohomology, we obtain the exact sequence

$$H^1(L/K,N_L) \to H^1(L/K,N_{A_L}) \xrightarrow{\delta} H^1(L/K,C_L(N)).$$

Furthermore, let us write N_{A_L} as $N_{\bar{S}} \times N_{(A_L)_{\bar{S}}}$ and note that

$$H^1(L/K,N_{\bar{S}}) = \prod_{v\in S} H^1(L/K,\prod_{w|v} N_{L_w}) = \prod_{v\in S} H^1(L_w/K_v,N).$$

Therefore, in terms of these identifications

$$\operatorname{Im}\gamma = \{\, x \in H^1(L/K,N_{\bar{S}}) : \exists y \in H^1(L/K,N_{(A_L)_{\bar{S}}}) \text{ with } \delta(x+y) = 0 \,\}.$$

It follows that γ is surjective if and only if

$$\delta(H^1(L/K,N_{\bar{S}})) \subset \delta(H^1(L/K,N_{(A_L)_{\bar{S}}})). \tag{7.6}$$

Now we apply the Nakayama-Tate theorems (cf. §6.3), which imply that there exist natural isomorphisms

$$H^1(L_w/K_v,N) \simeq \hat{H}^{-1}(L_w/K_v,\mathbf{X}_*(N))$$
$$H^1(L/K,C_L(N)) \simeq \hat{H}^{-1}(L/K,\mathbf{X}_*(N)),$$

where $\mathbf{X}_*(N)$ is the group of cocharacters of N. In addition, as Proposition 6.8 shows, the composition map

$$\begin{aligned}\hat{H}^{-1}(L_w/K_v,\mathbf{X}_*(N)) &\simeq \hat{H}^1(L_w/K_v,N)\\ &= H^1(L/K,\prod_{w|v} N_{L_w}) \to H^1(L/K,C_L(N)) \simeq \hat{H}^{-1}(L/K,\mathbf{X}_*(N))\end{aligned}$$

induced by the composition $\prod_{w|v} N_{L_w} \to N_{A_L} \to C_L(N)$ is the corestriction map $\mathrm{Cor}^{\mathcal{G}}_{\mathcal{G}(w)}$, which we shall denote as $\varrho(w)$. Taking into account the description of the cohomology of adele groups (cf. Proposition 6.6), we obtain that (7.6) is equivalent to

$$\sum_{v\in S} \operatorname{Im}\varrho(w) \subset \sum_{v\notin S} \operatorname{Im}\varrho(w) \tag{7.7}$$

(where a single extension $w|v$ is chosen for each v). Now if condition (7.4) holds, then for each v in S one can find a v' not in S and extensions $w|v$ and $w'|v$ such that $\operatorname{Im}\varrho(w) = \operatorname{Im}\varrho(w')$; and then, clearly, (7.7) holds. Consequently, T has weak approximation with respect to S. It remains to note that if $\mathcal{G}(w) = \mathrm{Gal}(L_w/K_v)$ is a cyclic group, say $\mathcal{G}(w) = \langle\sigma\rangle$, then by the Chebotarev density theorem there exist infinitely many v' in V_f^K for which $L_{w'}/K_{v'}$ is unramified and the Frobenius automorphism $\mathrm{Fr}(L_{w'}/K_{v'}) = \sigma$; in particular, such v' can be chosen not in S. Then $\mathcal{G}(w') = \langle\sigma\rangle = \mathcal{G}(w)$. This completes the proof of Proposition 7.8. (Note: a different proof of Proposition 7.8 may be found in Voskresenskiĭ [3, Theorem 3.36].)

COROLLARY 1. *Let T be a K-torus. Then there exists a finite subset S_0 of V_f^K such that T has weak approximation with respect to $V^K \setminus S_0$.*

Indeed, let L be a splitting field of T. For S_0 take the set of valuations v in V_f^K which are ramified in L; it is well-known that S_0 is finite. Then any v in $V^K \setminus S_0$ is either Archimedean or unramified on L; and in either case the local extension L_w/K_v (for $w|v$) is cyclic. Therefore Proposition 7.8 implies that T has weak approximation with respect to any finite subset S of $V^K \setminus S_0$, and hence with respect to the entire set $V^K \setminus S_0$ (cf. Proposition 7.1).

COROLLARY 2. *Let F be a diagonalizable K-group. For v in V^K, let $\mathcal{G}(F,v)$ denote the kernel of the action of $\mathcal{G}(v) = \mathrm{Gal}(\bar{K}_v/K_v)$ on the group of characters $\mathbf{X}(F)$; and let S_0 be the set of non-Archimedean valuations v for which $\mathcal{G}(v)/\mathcal{G}(F,v)$ is not cyclic. Then S_0 is a finite set, and for any finite subset S of $V^K \setminus S_0$ the canonical map $H^1(K,F) \to \prod_{v\in S} H^1(K_v,F)$ is surjective. In particular, $H^1(K,F) \to \prod_{v\in V_\infty^K} H^1(K_v,F)$ is always surjective.*

PROOF: Let $\mathcal{G}(F)$ denote the kernel of the natural action of $\mathcal{G} = \mathrm{Gal}(\bar{K}/K)$ on $\mathbf{X}(F)$, and let P be the fixed field under $\mathcal{G}(F)$. Then P is a minimal splitting field for F; in particular, P/K is finite. Clearly $\mathcal{G}/\mathcal{G}(F)$ is $\mathrm{Gal}(P/K)$; and, for v in V^K, clearly $\mathcal{G}(v)/\mathcal{G}(F,v)$ is the Galois group $\mathrm{Gal}(P_w/K_v)$ of the corresponding local extension. In view of these remarks, the arguments used to prove Corollary 1 allow us to assert that S_0 finite. Now we use Proposition 2.1 and insert F in the exact sequence

$$1 \to F \to T_1 \to T_2 \to 1, \tag{7.8}$$

where T_1 and T_2 are tori split over P, and T_1 is quasisplit over K. Then for any extension L of K, we have $H^1(L,T_1) = 1$, so, for any finite subset S of V^K, (7.8) yields the following commutative diagram with exact rows:

$$\begin{array}{ccccccc} T_{1K} & \xrightarrow{\alpha} & T_{2K} & \xrightarrow{\beta} & H^1(K,F) & \longrightarrow & 1 \\ \downarrow & & \downarrow & & \downarrow{\scriptstyle \chi} & & \\ T_{1S} & \xrightarrow{\theta} & T_{2S} & \xrightarrow{\varphi} & \prod_{v\in S} H^1(K_v,F) & \longrightarrow & 1. \end{array} \tag{7.9}$$

Now, if we suppose that $S \subset V^K \setminus S_0$, then Proposition 7.8 implies that weak approximation holds for T_2 relative to S. In particular, since $\theta(T_{1S})$ is open in T_{2S}, we obtain that

$$T_{2S} = \varrho(T_{2K})\theta(T_{1S}).$$

To prove that χ is surjective it remains to apply φ to both parts of this equation and to use the commutativity of (7.9).

Having analyzed the case of algebraic tori, we now turn to the proof of Theorems 7.7 and 7.8. The first step consists of proving Theorem 7.8 for simply connected groups.

PROPOSITION 7.9. *Let G be a semisimple simply connected K-group. Then G has the weak approximation property with respect to any finite subset S of V^K.*

PROOF: Using Propositions 7.1 and 7.2, we can easily reduce the proof to the case of a simple simply connected K-group G. As we noted in §2.4.3, G is a unirational variety over K, i.e., there exists a dominant K-morphism $f: U \to G$, where U is an open subset of a suitable affine space $\mathbb{A}^d$. It follows from Proposition 3.3 that $f(U_S)$ contains an open subset of G_S. But by Proposition 7.2 (4), U has weak approximation, so the closure $\bar{G}_K$ of G_K in G_S contains $\overline{f(U_K)} \supset f(\bar{U}_K) = f(U_S)$, and therefore is an open subgroup. However, by Theorem 5.5, G_A/G_K has finite volume; so, writing $G_A = G_S \times G_{A_S}$ and using Lemma 3.17, we obtain that $G_S/\bar{G}_K$ also has finite volume. It follows that $[G_S : \bar{G}_K]$ must be finite. (Since in our proof we did not assume G to be simple and/or simply connected, this fact holds for any semisimple K-group.)

Now let G be a simply connected simple K-group of type other than A_n. Then G is K_v-isotropic for all non-Archimedean v (Theorem 6.5), and therefore it follows from Proposition 7.6 and Theorem 7.6 that, for any v in V^K, G_{K_v} does not have any proper noncentral normal subgroups. This implies that G_S does not have any proper subgroups of finite index, which means that $G_S = \bar{G}_K$.

The case for groups of type A_n requires special consideration.

LEMMA 7.2. *Let G be a simple simply connected K-group of type A_n. Then G has the weak approximation property with respect to any finite S.*

PROOF: There are two possibilities here: $G = \mathbf{SL}_m(D)$ or $G = \mathbf{SU}_m(f)$, where f is a nondegenerate m-dimensional Hermitian form over a skew field D with involution τ of the second kind, and the field of τ-fixed elements of the center of D is K. For these cases, put $H = \mathbf{GL}_m(D)$ or $H = \mathbf{U}_m(f)$, respectively. We claim that $G_{K_v} = [H_{K_v}, H_{K_v}]$ for any v in V^K. If G is isotropic over K_v or $v \in V_\infty^K$, then this follows from Theorem 7.6 and Proposition 7.6. If not, then $G_{K_v} \simeq \mathbf{SL}_1(A)$ and $H_{K_v} \simeq \mathbf{GL}_1(A)$, where A is a division algebra over K_v, and the desired result is exactly equivalent to the triviality of $SK_1(A)$ (cf. §1.4.3). Since $\mathbf{GL}_m(D)$ is obviously a rational variety, as is $\mathbf{U}_m(f)$ by Proposition 7.4, we see that H is always

rational over K. Therefore Proposition 7.3 implies that H has weak approximation; i.e., $\bar{H}_K = H_S$. Thus $[H_K, H_K]$ is dense in $[H_S, H_S] = G_S$, and consequently $G_S = \overline{[H_K, H_K]} \subset \bar{G}_K$. This completes the proof of Lemma 7.2 and Proposition 7.9.

Now we establish a cohomological criterion (due to Kneser [5]) for weak approximation in an arbitrary semisimple group G. As one might expect after Proposition 7.9, this criterion is stated in terms of the corresponding fundamental group F, i.e., the kernel of the universal K-covering $\pi\colon \tilde{G} \to G$. However, since we wish to prove Theorem 7.7, we shall present a somewhat more general assertion involving *special coverings* $\pi\colon \tilde{H} \to H$ of arbitrary reductive groups (cf. §2.2.4), i.e., isogenies with $\tilde{H}$ being a direct product of a semisimple simply connected group and a quasisplit torus.

PROPOSITION 7.10. *Let $\pi\colon \tilde{H} \to H$ be a special K-covering of a reductive group H, and let $\ker \pi = F$. Then H has weak approximation with respect to a finite subset S of V^K containing V_∞^K if an only if the canonical map $H^1(K, F) \to \prod\limits_{v \in S} H^1(K_v, F)$ is surjective.*

PROOF: We have the following familiar diagram:

$$
\begin{array}{ccccccc}
\tilde{H}_K & \xrightarrow{\pi} & H_K & \xrightarrow{\psi} & H^1(K,F) & \xrightarrow{\theta} & H^1(K,\tilde{H}) \\
\downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\gamma} & & \downarrow{\scriptstyle\delta} \\
\tilde{H}_S & \xrightarrow{\Pi} & H_S & \xrightarrow{\Psi} & \prod\limits_{v\in S} H^1(K_v,F) & \xrightarrow{\Theta} & \prod\limits_{v\in S} H^1(K_v,\tilde{H}).
\end{array}
\tag{7.10}
$$

Since $\tilde{H} = D \times T$, where D is a semisimple simply connected K-group, and T is a quasisplit torus, Proposition 7.9 and Proposition 7.2 (4) imply that α is a dense embedding. It follows that weak approximation for H is equivalent to $H_S = \beta(H_K)\Pi(\tilde{H}_S)$, which in turn reduces to the surjectivity of the induced map $\gamma'\colon \ker\theta \to \ker\Theta$. Note that for any extension P/K we have $H^1(P, \tilde{H}) = H^1(P, D)$. Therefore, Theorems 6.4 and 6.6 imply that $H^1(K_v, \tilde{H}) = 1$ for non-Archimedean v, and $H^1(K, \tilde{H}) \to \prod\limits_{v \in V_\infty^K} H^1(K_v, \tilde{H})$ is bijective. In particular, δ is injective since $S \supset V_\infty^K$. From this we see easily that if γ is surjective, then γ' is also surjective, which means that H has weak approximation relative to S. Conversely, weak approximation for H implies the surjectivity of γ'. But then

$$
\prod_{v \in V_\infty^K} \{0\} \times \prod_{v \in S \setminus V_\infty^K} H^1(K_v, F) \subset \ker\Theta = \operatorname{Im}\gamma' \subset \operatorname{Im}\gamma.
$$

Since $H^1(K, F) \to \prod\limits_{v \in V_\infty^K} H^1(K_v, F)$ is always surjective (Proposition 7.8, Corollary 2), it follows that γ is surjective, and Proposition 7.10 is proved.

We can now prove Theorem 7.7 easily. If G is semisimple, then its universal covering $\pi\colon \tilde{G} \to G$ is special, and the required assertion follows immediately from Proposition 7.9 and Proposition 7.8, Corollary 2. The case of an arbitrary connected group easily reduces to the reductive case (cf. corollary of Proposition 7.1). Unfortunately, not every reductive group G has a special covering, and Proposition 7.10 cannot be used directly. However, by Proposition 2.11 one can find a positive integer m and a quasisplit torus T such that $H = G^m \times T$ has a special covering $\pi\colon \tilde{H} \to H$. Then, applying Proposition 7.10 and Proposition 7.8, Corollary 2, we obtain the existence of a finite exceptional subset $S_0 \subset V_f^K$ for H. However, it follows from Proposition 7.1 (2) that this set also works for G, thus completing the proof of Theorem 7.7.

The proof of Theorem 7.7 enables us to obtain additional information about weak approximation in a reductive group G. To do so, we return to the special covering $\pi\colon \tilde{H} \to H$ of $H = G^m \times T$ and the corresponding diagram (7.10). It follows from the weak approximation property for $\tilde{H}$ that the closure $\bar{H}_K$ in H_S contains $\pi(\tilde{H}_S) \supset [H_S, H_S]$ and therefore is a normal subgroup of H_S. Moreover,

$$
[H_S : \bar{H}_K] \le |\operatorname{coker}\gamma| \le \sum_{v \in S_0} |H^1(K_v, F)|,
$$

where S_0 is the exceptional subset from Corollary 2 of Proposition 7.8, i.e., $[H_S : \bar{H}_K]$ is bounded by a number which does not depend on S. It follows that the closure $\bar{H}_K$ in $\underline{H} = \prod_v H_{K_v}$ is also a normal subgroup, and the (abelian) group $A(H) = \underline{H}/\bar{H}_K$, measuring the deviation from weak approximation, is finite. Using the canonical projection $H \to G$, one can easily show that this assertion remains valid for an arbitrary reductive group G. Then it is fairly easy to extend the result to an arbitrary connected group (cf. corollary of Proposition 7.1). Thus, one obtains

THEOREM 7.9. *For an arbitrary connected K-group G, the closure $\bar{G}_K$ of G_K in $\underline{G} = \prod\limits_{v \in V^K} G_{K_v}$ is a normal subgroup, and the corresponding quotient group $A(G) = \underline{G}/\bar{G}_K$, measuring the deviation from weak approximation, is a finite abelian group.*

We have yet to complete the proof of Theorem 7.8. To do so, first we present two corollaries, of interest in their own right.

COROLLARY 3. *Let G be a semisimple K-group, for which the automorphism group of the fundamental group F is cyclic. Then G has the weak approximation property.*

Indeed, notation as in Corollary 2, for any v in V^K, one can embed $\mathcal{G}(v)/\mathcal{G}(F,v)$ in $\operatorname{Aut}\mathbf{X}(F) \simeq \operatorname{Aut} F$, and therefore $\mathcal{G}(v)/\mathcal{G}(F,v)$ is cyclic. Then $H^1(K,F) \to \prod_{v\in S} H^1(K_v,F)$ is surjective, for any finite subset S of V^K; so G has weak approximation with respect to any such S.

COROLLARY 4. *Let G be a semisimple K-group and let S be a finite subset of V^K. Assume, for each v in S, that G has a maximal K_v-torus which is split over a cyclic extension of K_v (this is true, for example, if G is split over K_v). Then G has weak approximation with respect to S.*

PROOF: Without loss of generality, we may assume that $S \supset V_\infty^K$; so, as above, it suffices to show that $\mathcal{G}(v)/\mathcal{G}(F,v)$ is cyclic, for any v in S. Let T be the maximal K_v-torus of G whose minimal splitting field L is cyclic over K_v. Letting $\mathcal{G}(T,v)$ denote the kernel of the action of $\mathcal{G}(v)$ on $\mathbf{X}(T)$, we see $\mathcal{G}(v)/\mathcal{G}(T,v)$ is isomorphic to $\operatorname{Gal}(L/K_v)$, and consequently is cyclic. On the other hand, it follows from $F \subset T$ that $\mathcal{G}(T,v) \subset \mathcal{G}(F,v)$ and therefore $\mathcal{G}(v)/\mathcal{G}(F,v)$ is also cyclic.

PROPOSITION 7.11. *Any simple K-group G has weak approximation.*

PROOF: Groups of type E_8, F_4, G_2 are simply connected, and therefore for these groups weak approximation follows from Proposition 7.9. The center of a simply connected group belonging to type B_n, C_n, E_6, or E_7 has order ≤ 3; therefore, for any fundamental group F arising here, $\operatorname{Aut} F$ is cyclic, and one can use Corollary 3. The center of a simply connected group of type D_{2n+1} is isomorphic to $\mathbb{Z}/4\mathbb{Z}$, so again $\operatorname{Aut} F$ is cyclic.

It remains to consider types D_{2n} and A_n. For G of type A_n one can use Corollary 4, since for each v in V^K it is easy to find a K_v-torus T of G with a splitting field which is cyclic over K_v. Indeed, if $G \simeq \mathbf{SL}_m(D)$ over K_v, then the desired torus will have the form

$$T = (\mathbf{R}_{L/K}(\mathbb{G}_m) \times \cdots \times \mathbf{R}_{L/K}(\mathbb{G}_m)) \cap \mathbf{SL}_m(D),$$

where $L \subset D$ is a maximal subfield which is cyclic over K. Note that such an L always exists. This is obvious if D is a quaternion skew field over $K_v = \mathbb{R}$, while for non-Archimedean v one can take a maximal subfield L of D which is unramified over K_v.

It remains to consider the case of $G \simeq \mathbf{SU}_m(f)$ over K_v, where f is a nondegenerate m-dimensional Hermitian form over a quadratic extension L/K_v. But here G is L-split, and therefore has a maximal K_v-torus T which is split over L (Lemma 6.23). Thus we need consider only groups G of type D_{2n}. Here special attention is needed only for the case where $F = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $\mathcal{G}/\mathcal{G}(F) = \operatorname{Aut} F \simeq S_3$.

Let P denote a subfield of $L = \bar{K}^{\mathcal{G}(F)}$ having degree 3 over K. Then the composite

$$H^1(K,F) \overset{\text{Res}}{\to} H^1(P,F) \overset{\text{Cor}}{\to} H^1(K,F)$$

coincides with multiplication by 3, and hence is identical to $H^1(K,F)$, since the exponent of F is 2. In particular, Cor is surjective. Analogously, for any v in V^K, the composite

$$H^1(K_v,F) \overset{\alpha_v}{\to} \prod_{w|v} H^1(P_w,F) \overset{\beta_v}{\to} H^1(K_v,F),$$

where α_v is induced by the appropriate restriction map and β_v by the corestriction map, is also multiplication by 3; hence β_v is surjective. On the other hand, L is a cyclic extension of P, so $H^1(P,F) \to \prod_{w\in\bar{S}} H^1(P_w,F)$ is surjective, for any finite subset $\bar{S}$ of V^P. Then, the surjectivity of γ follows from the commutative diagram

$$\begin{array}{ccc} H^1(P,F) & \longrightarrow & \prod_{\substack{w|v \\ v\in S}} H^1(P_w,F) \\ \Big\downarrow \text{Cor} & & \Big\downarrow \beta \\ H^1(K,F) & \xrightarrow{\gamma} & \prod_{v\in S} H^1(K_v,F), \end{array}$$

where $\beta = \prod_{v\in S} \beta_v$, and from the surjectivity of β. Proposition 7.11 is proved.

Since any adjoint K-group is a direct product of its K-simple components, which are obtained from absolutely simple groups by restriction of scalars, it follows that Proposition 7.11 completes the proof of Theorem 7.8.

All the above results have been positive, which might give the impression that weak approximation always holds. This, however, is not the case; counterexamples exist for algebraic tori as well as for semisimple groups.

The examples which we present here start with the extension L/K, where $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{-1}, \sqrt{2})$, which has the following property: any prime $p \neq 2$ is unramified on L/K, but $p = 2$ is totally ramified; moreover, the local degree for $p \neq 2$ (including $p = \infty$) is 1 or 2, but for $p = 2$ it is 4. Now we put $T = \mathbf{R}^{(1)}_{L/K}(\mathbb{G}_m)$ and show that T_K is not dense in T_{K_2}. To

do so, let us show that (7.7), which is a necessary and sufficient condition for weak approximation, does not hold here. To this end, we construct the exact sequence

$$1 \to N \to H \xrightarrow{\varphi} T \to 1,$$

where $H = \mathbf{R}_{L/K}(T)$ and φ is the norm map (cf. proof of Proposition 7.8). This sequence has a corresponding exact sequence of cocharacter modules

$$0 \to \mathbf{X}_*(N) \to \mathbf{X}_*(H) \to \mathbf{X}_*(T) \to 0.$$

Since $\mathbf{X}_*(H)$ is of the form $\mathbf{X}_*(T) \otimes_{\mathbb{Z}} \mathbb{Z}[\mathcal{G}]$, where $\mathcal{G} = \mathrm{Gal}(L/K) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, it is induced. Therefore $\hat{H}^i(L/K, \mathbf{X}_*(H)) = 0$ for any i. Hence from the exact cohomological sequence

$$0 = \hat{H}^{-2}(L/K, \mathbf{X}_*(H)) \to \hat{H}^{-2}(L/K, \mathbf{X}_*(T)) \to \hat{H}^{-1}(L/K, \mathbf{X}_*(N)) \to \hat{H}^{-1}(L/K, \mathbf{X}_*(H)) = 0$$

we obtain a natural isomorphism

$$\hat{H}^{-1}(L/K, \mathbf{X}_*(N)) \simeq \hat{H}^{-2}(L/K, \mathbf{X}_*(T)).$$

In turn $\mathbf{X}_*(T)$ enters the exact sequence

$$0 \to \mathbf{X}_*(T) \to \mathbb{Z}[\mathcal{G}] \to \mathbb{Z} \to 0,$$

which corresponds to $1 \to T \to \mathbf{R}_{L/K}(\mathbb{G}_m) \to \mathbb{G}_m \to 1$; and by a similar argument we obtain that

$$\hat{H}^{-2}(L/K, \mathbf{X}_*(T)) \simeq \hat{H}^{-3}(L/K, \mathbb{Z}).$$

Performing the same computations locally, we arrive at the isomorphism

$$\hat{H}^{-1}(L_w/K_v, \mathbf{X}_*(N)) \simeq \hat{H}^{-3}(L_w/K_v, \mathbb{Z}).$$

Then (7.7) reduces to the following:

$$(7.11) \qquad \sum_{\substack{v \in S \\ w|v}} \mathrm{Cor}^{\mathcal{G}}_{\mathcal{G}(w)}(\hat{H}^{-3}(L_w/K_v, \mathbb{Z})) \subset \sum_{\substack{v \notin S \\ w|v}} \mathrm{Cor}^{\mathcal{G}}_{\mathcal{G}(w)}(\hat{H}^{-3}(L_w/K_v, \mathbb{Z})).$$

In our case $S = \{2\}$, $\mathcal{G}(2) = \mathcal{G}$; so the left side of (7.11) is

$$\hat{H}^{-3}(\mathcal{G}, \mathbb{Z}) \simeq H^3(\mathcal{G}, \mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z}.$$

On the other hand, all the local Galois groups on the right side of (7.11) are cyclic; so $\hat{H}^{-3}(L_w/K_v, \mathbb{Z}) \simeq H^1(L_w/K_v, \mathbb{Z}) = 0$, and the right side of (7.11) is trivial. Thus, (7.11) does not hold, which means T_K is not dense in T_{K_2}. (Note that this argument shows, in fact, that $T_{K_2}/\bar{T}_K$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.)

Using the construction of T, now we construct a finite diagonalizable K-group F for which $H^1(K, F) \to H^2(K_2, F)$ is not surjective. Since $\bar{T}_K \neq T_{K_2}$, there is a positive integer l such that $T_{K_2} \not\subset T_K \cdot L_2^{*l}$. Then put $n = 4l$, $F = \mathbf{R}^{(1)}_{L/K}(\mu_n)$, where μ_n is the group of the n-th roots of unity (note that F is the set of elements in T which have order dividing n).

LEMMA 7.3. *$H^1(K, F) \xrightarrow{\chi} H^1(K_2, F)$ is not surjective.*

PROOF: By Lemma 2.6 one has the following isomorphisms:

$$H^1(K, \mu_n) \simeq K^*/K^{*n}$$
$$H^1(K, \mathbf{R}_{L/K}(\mu_n) \simeq H^1(L, \mu_n) \simeq L^*/L^{*n};$$

so $H^1(K, F)$ enters the exact sequence

$$H^1(K, F) \to L^*/L^{*n} \xrightarrow{\alpha} K^*/K^{*n},$$

where α is induced by the norm map $N_{L/K}$. In particular, $H^1(K, F)$ maps surjectively onto $\ker \alpha$. Analogously, $H^1(K_2, F)$ maps surjectively onto the kernel of $\beta\colon L_2^*/L_2^{*n} \to K_2^*/K_2^{*n}$ induced by N_{L_2/K_2}. Therefore, if χ were surjective, then the canonical map $\ker \alpha \xrightarrow{\gamma} \ker \beta$ would also be surjective. But clearly

$$\ker \alpha = T_K K^{*l} L^{*n}/L^{*n}$$
$$\ker \beta = T_{K_2} K_2^{*l} L_2^{*n}/L_2^{*n};$$

hence the surjectivity of γ would mean in particular that

$$T_{K_2} \subset T_K K^{*l} L_2^{*n} \subset T_K L_2^{*l},$$

contradiction. Lemma 7.3 is proved.

Now, to obtain an example of a semisimple group G which does not have weak approximation, it suffices to take $H = \mathbf{R}_{L/K}(\mathbf{SL}_n)$ and, in view of the natural embedding $F \subset \mathbf{R}_{L/K}(\mu_n) = Z(H)$, to put $G = H/F$. Then, for $S = \{\infty, 2\}$, we see $H^1(K, F) \to \prod_{v \in S} H^1(K_v, F)$ is not surjective; consequently G does not have weak approximation with respect to S (and even with respect to $\{2\}$). It should be noted that the first examples of this sort were constructed by Serre (cf. ANT, ex. 5).

Regarding weak approximation for simply connected groups and Serre's counterexamples, Kneser [5] put forward a conjecture on the validity of weak approximation for simply connected semisimple groups over an arbitrary infinite field. In particular, he conjectured that the algebraic group $G = \mathbf{SL}_n(D)$, where D is a finite-dimensional skew field over K, always satisfies the weak approximation property. Here we have the following

PROPOSITION 7.12. *Let $G = \mathbf{SL}_n(D)$, and let v be a discrete valuation of K. Then:*

(1) *$\bar{G}_K$ is a normal subgroup of G_{K_v} (bar denotes closure in the v-adic topology);*
(2) *$G_{K_v}/\bar{G}_K \simeq SK_1(D \otimes_K K_v)/\varphi(SK_1(D))$, where φ is induced by $D \hookrightarrow D \otimes_K K_v$.*

PROOF: The group variety $H = \mathbf{GL}_n(D)$ is rational over K and therefore H_K is dense in H_{K_v} (the proof is the same as for the case of a number field). Since $[H_K, H_K] \subset G_K$, the closure $\bar{G}_K$ of G_K contains $\overline{[H_K, H_K]} \supset [H_{K_v}, H_{K_v}]$, implying (1). Note that this inclusion is actually an equality, since $[H_{K_v}, H_{K_v}]$ contains $[H_K, H_K]$ and is open by the remark following Theorem 3.3; consequently it is also closed in G_{K_v}. This also implies that $\bar{G}_K = G_K[H_{K_v}, H_{K_v}]$; so

$$G_{K_v}/\bar{G}_K = G_{K_v}/G_K[H_{K_v}, H_{K_v}] \simeq SK_1(M_n(D \otimes_K K_v))/\psi(SK_1(M_n(D))),$$

where ψ is induced by $M_n(D) \hookrightarrow M_n(D \otimes_K K_v)$. It remains to note that the Dieudonné determinant induces an isomorphism

$$SK_1(M_n(D \otimes_K K_v))/\psi(SK_1(M_n(D)) \simeq SK_1(D \otimes_K K_v)/\varphi(SK_1(D)).$$

Proposition 7.12 is proved.

Now we apply the following result from reduced K-theory.

THEOREM 7.10 (PLATONOV [16]). *There exist skew fields D over a field K for which $SK_1(D)$ is finite (and even trivial); but the orders of $SK_1(D \otimes_K K_{v_i})$ are not bounded, for some infinite set $V = \{v_i\}$ of discrete valuations of K.*

Theorem 7.10 and Proposition 7.12 imply the following result, which, in particular, provides a negative answer to Kneser's conjecture, stated above.

THEOREM 7.11 (PLATONOV [16]). *There exist skew fields D over a field K for which the orders of $G_{K_{v_i}}/\bar{G}_K$ (where $G = \mathbf{SL}_n(D)$), expressing the deviation from weak approximation, are not bounded, for some infinite set $V = \{v_i\}$ of discrete valuations of K.*

(The unitary analog of Theorem 7.11 was obtained by Yanchevskiĭ [2].)

Despite the fact that most of the conjectures regarding algebraic groups over an arbitrary field have recently been refuted, we shall be so bold as to advance a new conjecture. Namely, several examples show that regarding rationality, and in particular regarding weak approximation, the groups which behave "well" are those which are adjoint and not, as previously thought, simply connected.

CONJECTURE: Let G be a semisimple adjoint group over an arbitrary infinite field K. Then G is a rational variety over K. In particular, G has the weak approximation property with respect to any finite set S of valuations of K.

It is easy to show that this conjecture holds for $G = \mathbf{PGL}_n(D)$. However, to verify the conjecture for $\mathbf{PSO}_{2n}(f)$, where $f = x_1^2 + \cdots + x_{2n}^2$ (Chernousov, unpublished) one must use the machinery of the algebraic theory of quadratic forms. The general case of $\mathbf{PSO}_{2n}(f)$ has not yet been studied.

We conclude with several remarks on the connection between the geometric and arithmetic properties of linear algebraic groups. Apparently this connection was first explicitly formulated for algebraic tori by Voskresenskiĭ [1],[3]. To state his result, let us consider a K-defined embedding $T \hookrightarrow V(T)$ in a smooth projective variety (the existence of such an embedding follows easily from Hironaka's theorem on the resolution of singularities), and the corresponding Picard group $\operatorname{Pic} V(T)$; then, for a number field K, one has the exact sequence

$$0 \to A(T) \to H^1(K, \operatorname{Pic} V(T)) \to Ш(T) \to 0, \tag{7.12}$$

where $Ш(T)$ is the Shafarevich-Tate group of T and $A(T)$ is the group expressing the deviation from weak approximation. (As Sansuc [1] noted, to have a functorial sequence one should replace the middle term of (7.12) with the dual group.) Afterwards Sansuc [1] showed that a sequence similar to (7.12) holds for any connected K-group.

7.4. The strong approximation theorem.

The object of this section is to establish a criterion for strong approximation in connected groups over number fields (for the case of global function fields, cf. the remark at the end of this section). If $G = HR_u(G)$ is the Levi decomposition of a connected K-group G, then by Proposition 7.1 strong approximation for G is equivalent to strong approximation for H (with respect to the same finite subset S of V^K); therefore, below we may assume G to be reductive. Then we have

THEOREM 7.12. *Let G be a reductive algebraic group over an algebraic number field K, and let S be a finite subset of V^K. Then G has the strong approximation property with respect to S if and only if*

(1) *G is simply connected (in particular, G is semisimple);*
(2) *G does not contain any K-simple component G^i with G^i_S compact.*

In particular, for a K-simple simply connected group G, strong approximation with respect to S is equivalent to G_S being noncompact.

That (1) and (2) are necessary conditions is implied by the following more precise assertion.

PROPOSITION 7.13. *Let G be an algebraic K-group and let S be a non-empty finite subset of V^K. Assume one of the following conditions holds:*

(1) *G is not connected;*
(2) *G is connected but not simply connected;*
(3) *G is connected, and its semisimple part D has a K-simple component D^i with D^i_S compact.*

Then the closure $\bar{G}_K$ of G_K in G_{A_S} has infinite index.

PROOF: First we assume that G is not connected. Let P be a finite Galois extension of K such that $G = G_P G^0$. By the Chebotarev density theory, $V_0 = \{ v \in V_f^K \setminus S : P \subset K_v \}$ is infinite. Fix an integer $l > 0$, and choose $v_1, \dots, v_l$ in V_0. Furthermore, put $T = \{ v_1, \dots, v_l \}$ and let $\bar{G}_K^{(T)}$ denote the closure of G_K in G_T. Since $G_{A_S} = G_T \times G_{A_{S \cup T}}$, the projection of $\bar{G}_K$ on G_T is contained in $\bar{G}_K^{(T)}$; hence

$$[G_{A_S} : \bar{G}_K] \geq [G_T : \bar{G}_K^{(T)}]. \tag{7.13}$$

However, $G_T^0 \subset G_T$ is a closed normal subgroup of finite index, from which it follows easily that $B = G_K G_T^0$ contains $\bar{G}_K^{(T)}$. Therefore

$$[G_T : \bar{G}_K^{(T)}] \geq [G_T : B] = \frac{[G_T : G_T^0]}{[G_K : G_K^0]} \geq [G : G^0]^{l-1}, \tag{7.14}$$

since by our choice of P we have $G = G_{K_v} G^0$, implying $[G_{K_v} : G^0_{K_v}] = [G : G^0]$ and consequently $[G_T : G_T^0] = \prod_{v \in T} [G_{K_v} : G^0_{K_v}] = [G : G^0]^l$. If one chooses l sufficiently large, then (7.13) and (7.14) yield that $[G_{A_S} : \bar{G}_K]$ cannot be finite.

Next, assume G is connected. If $G = HR_u(G)$ is the Levi decomposition, then clearly conditions (2) and (3) for G are equivalent to the respective conditions for H, and $[G_{A_S} : \bar{G}_K] = [H_{A_S} : \bar{H}_K]$. Thus we may assume G to be reductive. Put $S_1 = S \cup V_\infty^K$ and consider the open subgroup

$$W = \prod_{v \in V_\infty^K \setminus (V_\infty^K \cap S)} G_{K_v} \times \prod_{v \notin S_1} G_{\mathcal{O}_v} \subset G_{A_S}.$$

Then the closure $\bar{\Gamma}$ of $\Gamma = G_K \cap W$ in W is $\bar{G}_K \cap W$; therefore if $[G_{A_S} : \bar{G}_K]$ is finite, then $[W : \bar{\Gamma}]$ is also finite. In particular, for any finite subset T of $V^K \setminus S_1$ and the respective closure $\bar{\Gamma}^{(T)}$ of Γ in $W_T = \prod_{v \in T} G_{\mathcal{O}_v}$, we see that $[W_T : \bar{\Gamma}^{(T)}]$ is bounded from above by some number c, independent of T.

Now assume that G is not simply connected, i.e., that there is a K-covering $\pi: H \to G$, where H is connected and $F = \ker \pi \neq 1$. Then for any v in V^K one can take the exact cohomological sequence

$$H_{K_v} \xrightarrow{\pi} G_{K_v} \xrightarrow{\psi_{K_v}} H^1(K_v, F),$$

where ψ_{K_v} is the appropriate coboundary morphism. Since $\pi(H_{K_v})$ is open in G_{K_v} (cf. Proposition 3.3, Corollary 1), it follows that $U = \prod_{v \in T} \pi(H_{K_v})$ is open in G_T, for any finite $T \subset V^K \setminus S_1$; thus $\bar{\Gamma}^{(T)} \subset \Gamma U$. Hence, letting $\psi_T = \prod_{v \in T} \psi_{K_v}$, we obtain

$$\psi_T(\Gamma) = \psi_T(\bar{\Gamma}^{(T)}).$$

But since we have seen that $[W_T : \bar{\Gamma}^{(T)}] \leq c$ for any T, we obtain

$$[\psi_T(W_T) : \psi_T(\Gamma)] \leq c. \tag{7.15}$$

We note now that Γ is the group of S_1-units $G_{\mathcal{O}(S_1)}$, and therefore is finitely generated (Theorem 5.11); say $\Gamma = \langle \gamma_1, \dots, \gamma_r \rangle$. Let P denote a finite Galois extension of K generated by the coefficients of the matrix F and of the matrices $\delta_1, \dots, \delta_r$ in $H_{\bar{K}}$ such that $\pi(\delta_i) = \gamma_i$, $(i = 1, \dots, r)$. Clearly in this case $\pi^{-1}(\Gamma) \subset H_P$, i.e., $\Gamma \subset \pi(H_P)$. Furthermore, by Proposition 6.4 there is a finite subset S_0 of V_f^K such that $\psi_{K_v}(G_{\mathcal{O}_v}) = H^1(K_v^{ur}/K_v, F)$ for each v in $V_f^K \setminus S_0$. By the Chebotarev density theorem $V_0 = \{ v \in V_f^K \setminus (S_1 \cup S_0) : P \subset K_v \}$ is infinite, and therefore one can choose a finite subset T of V_0 with an arbitrarily large number of elements. Then by construction $\Gamma \subset \pi(G_{K_v})$ for any v in T, and consequently $\psi_T(\Gamma) = \{1\}$. On the other hand, $\psi_{K_v}(G_{\mathcal{O}_v}) \simeq F$ by Proposition 6.4, since $F \subset G_{K_v}$; so $\psi_T(W_T) \simeq F^l$, where $l = |T|$. Thus $[\psi_T(W_T) : \psi_T(\Gamma)] = |F|^l$, and we reach a contradiction with (7.15), having chosen l sufficiently large.

Lastly, we show that condition (3) also implies that $[G_{A_S} : \bar{G}_K]$ is infinite. By what we have already shown, we may assume G to be reductive and simply connected and, in particular, semisimple. Then G is a direct product of its K-simple components G^i. Now if $[G_{A_S} : \bar{G}_K]$ were finite, it would follow that all the $[G^i_{A_S} : \bar{G}^i_K]$ were finite. On the other hand, (3) implies there is a component G^i with G^i_S compact. Since G^i_K is discrete in $G^i_A = G^i_{A_S} \times G^i_S$, the fact that G^i_S is compact implies that G^i_K is discrete in $G^i_{A_S}$, and consequently $\bar{G}^i_K = G^i_K$. But then $[G^i_{A_S} : \bar{G}^i_K]$ obviously cannot be finite (or even countable). The proposition is proved.

Proving that (1) and (2) in Theorem 7.12 are sufficient conditions for strong approximation is far more difficult; the proof of this assertion constitutes the bulk of the proof of this theorem. Condition (1) implies that G

is a direct product of its K-simple components, and by Proposition 7.1 the problem reduces to the case of K-simple groups. In turn, a K-simple group can be obtained from a simple group by restriction of scalars, so Proposition 7.2(3) gives a reduction to the case of simple groups, which we now consider. The following straightforward assertion will be used repeatedly.

LEMMA 7.4. *Let Γ be a subgroup of the direct product $B = B_1 \times B_2$ of two topological groups B_1 and B_2, and let $\pi_i: B \to B_i$ $(i = 1, 2)$ be the respective projections. Assume the following conditions hold:*

(1) *$\pi_1(\Gamma)$ is dense in B_1;*
(2) *B_1 has a base $\mathcal{U} = \{U\}$ of the neighborhoods of 1 consisting of subgroups, such that for any U in $\mathcal{U}$ the projection $\pi_2(\Gamma \cap (U \times B_2))$ is dense in B_2.*

Then Γ is dense in B.

PROOF: Almost self-evident. Suppose $\bar{\Gamma} \neq B$. Then there exists an open subset $W = W_1 \times W_2 \subset B$ disjoint from Γ. By condition (1) one can find an element γ in Γ for which $\pi_1(\gamma) \in W_1$. Furthermore, by (2) there is an open subgroup U of B_1 contained in $\pi_1(\gamma)^{-1}W_1$. Since $\Gamma \cap W = \emptyset$ and $\gamma^{-1}W \supset U \times \pi_2(\gamma)^{-1}W_2$, one has $\pi_2(\Gamma \cap U) \cap \pi_2(\gamma)^{-1}W_2 = \emptyset$, which contradicts (2).

Let us begin by considering the case where S contains all Archimedean valuations and those non-Archimedean valuations v for which G is K_v-anisotropic (the latter, as we know, can exist only for groups of type A_n). By Proposition 7.2(2) we must show that $\Gamma = G_{\mathcal{O}(S \cup S_1)}$ is dense in G_{S_1} for any finite subset S_1 of $V^K \setminus S$. Let S_2 be a maximal (possibly empty) subset of S_1 such that Γ is dense in G_{S_2} (always taking the diagonal embedding of Γ). Our objective is to show that $S_1 = S_2$. Let $S_2 \neq S_1$, and let $v \in S_1 \setminus S_2$. Put $S_3 = S_2 \cup \{v\}$, write $G_{S_3} = G_{S_2} \times G_{K_v}$, and apply Lemma 7.3. Since Γ is not dense in G_{S_3}, there is an open subgroup U of G_{S_2} such that $\Delta = \Gamma \cap U$ is not dense in G_{K_v} (moreover, making U smaller if necessary, we may assume it to be compact). We shall show that actually this is not the case.

Since Γ is a discrete subgroup of $G_{S \cup S_1}$ and $G_{S \cup S_1}/\Gamma$ has finite measure (Theorem 5.7), then Δ is a discrete subgroup of $D = G_{(S \cup S_1) \setminus S_2} \times U$ and D/Δ also has finite measure. Writing $D = (G_{(S \cup S_1) \setminus S_3} \times U) \times G_{K_v}$, and applying Lemma 3.17, which is possible since G_S is noncompact, we obtain that Δ is not discrete in G_{K_v}, and $G_{K_v}/\bar{\Delta}$ has finite measure.

Furthermore, let p denote the prime corresponding to v. Then $\mathbb{Q}_p \subset K_v$ and G_{K_v} can be viewed as a p-adic Lie group (cf. §3.1). Its Lie algebra over $\mathbb{Q}_p$ is $L(G)_{K_v}$. Since G is simple, it does not contain any nontrivial ideals. By Cartan's theorem (cf. Theorem 3.4), $\bar{\Delta}$ is a Lie subgroup of

G_{K_v}; moreover, since Δ is not discrete, its Lie algebra $\mathfrak{h} \neq 0$. Furthermore, it follows from Theorem 5.7 on the finiteness of the volume of $G_S/G_{\mathcal{O}(S)}$ that $G_{\mathcal{O}(S)}$ is infinite, since G_S is noncompact. Then, repeating the proof of Theorem 4.10 verbatim, we obtain that $G_{\mathcal{O}(S)}$ is Zariski-dense in G. Since U is open and compact, it is commensurable with $\prod_{v \in S_2} G_{\mathcal{O}_v}$; hence $[G_{\mathcal{O}(S)} : G_{\mathcal{O}(S)} \cap U]$ is finite. It follows that $G_{\mathcal{O}(S)} \cap U$ is also Zariski-dense in G. Since clearly $\Delta \supset G_{\mathcal{O}(S)} \cap U$, it follows finally that Δ is Zariski-dense in G. Applying Proposition 3.4, we obtain that $\mathfrak{h}$ is a Lie ideal of $L(G)_{K_v}$ and consequently $\mathfrak{h} = L(G)_{K_v}$, since $\mathfrak{h} \neq 0$. Then Proposition 3.2 implies that $\bar{\Delta}$ is open in G_{K_v}. However, we established above that $G_{K_v}/\bar{\Delta}$ has finite measure. Therefore $\bar{\Delta}$ has finite index in G_{K_v}; consequently $\bar{\Delta} = G_{K_v}$, since G_{K_v} does not have any nontrivial subgroups of finite index, as follows easily from Theorem 7.6. Thus we obtain a contradiction, which completes the proof of Theorem 7.12 for the case under consideration.

Now we shall weaken the constraints on S, keeping only the requirement that S contain all Archimedean valuations. Put

$$S_0 = \{ v \in V_f^K \setminus S : G \text{ anisotropic over } K_v \}.$$

S_0 is finite, by Theorem 6.7. It follows from what we have proved above that G has strong approximation with respect to $S \cup S_0$, i.e., G_K is dense in $G_{A_{S_0 \cup S}}$. On the other hand, G has weak approximation with respect to S_0 (Proposition 7.9), i.e., G_K is dense in G_{S_0}. Since $G_{A_S} = G_{S_0} \times G_{A_{S \cup S_0}}$, in order to use Lemma 7.4 it suffices to show that $G_K \cap U$ is dense in $G_{A_{S \cup S_0}}$ for any open subgroup U of G_{S_0}.

Since G_{K_v} is compact for any v in S_0 (Theorem 3.1), G_{S_0} is also compact, which implies that U has finite index in G_{S_0}. It follows that $G_K \cap U$ has finite index in G_K; thus its closure has finite index in $G_{A_{S \cup S_0}}$, and it remains to show that $G_{A_{S \cup S_0}}$ does not have any nontrivial closed subgroups of finite index. As we noted above, it follows from Theorem 7.6 that G_{K_v} does not have any proper normal subgroups of finite index, for any v in $V^K \setminus (S \cup S_0)$; consequently, the same is true for G_{S_1}, where S_1 is any finite subset of $V^K \setminus (S \cup S_0)$. Therefore, any closed subgroup $B \subset G_{A_{S \cup S_0}}$ of finite index must contain the images of all embeddings $\delta_{S_1}: G_{S_1} \to G_{A_{S \cup S_0}}$. But it follows easily from the definition of the adele topology that the union $\bigcup \delta_{S_1}(G_{S_1})$, taken over all finite subsets $S_1 \subset V^K \setminus (S \cup S_0)$, is dense in $G_{A_{S \cup S_0}}$ as desired.

The last remaining constraint to be removed is $S \supset V_\infty^K$. Put

$$S_1 = V_\infty^K \setminus (S \cap V_\infty^K) \quad \text{and} \quad S_2 = S \cup S_1;$$

then $G_{A_S} = G_{A_{S_2}} \times G_{S_1}$. By what we have proved, G_K is dense in $G_{A_{S_2}}$. Therefore, to use Lemma 7.4 it suffices to verify that $G_K \cap U$ is dense

in G_{S_1}, for any open subgroup U of $G_{A_{S_2}}$. Without loss of generality, U may be assumed compact. Then it is commensurable with $G_{A_{S_2}(S_2)}$, and hence $G_K \cap U$ is commensurable with $G_{\mathcal{O}(S_2)}$. On the other hand, by Proposition 7.6 G_{K_v} is connected for each v in V_∞^K; thus also G_{S_1} is connected. It follows that we actually need only establish that $G_{\mathcal{O}(S_2)}$ is dense in G_{S_1}. Let Λ denote the connected component of the closure of $G_{\mathcal{O}(S_2)}$ in G_{S_1}. We claim that Λ is a normal subgroup of G_{S_1}. Indeed, $G_{\mathcal{O}(S_2)}$ and $g^{-1}G_{\mathcal{O}(S_2)}g$ are commensurable, for any g in G_K; therefore their closures are also commensurable, and consequently the connected components of the closures coincide, i.e., $\Lambda = g^{-1}\Lambda g$. But G has weak approximation with respect to S_1, by Proposition 7.9; it follows that $\Lambda = g^{-1}\Lambda g$ for any g in G_{S_1}. Thus, Λ is a connected normal subgroup of G_{S_1}, so $\Lambda = G_{S_3}$ for some $S_3 \subset S_1$.

Assume that $S_4 = S_1 \setminus S_3 \neq \emptyset$, and let $\pi: G_{S_1} \to G_{S_4}$ be the corresponding projection. Since $\ker \pi = G_{S_3}$ is contained in the closure of $G_{\mathcal{O}(S_2)}$ in G_{S_1}, the connected component of the closure Φ of $G_{\mathcal{O}(S_2)}$ in G_{S_4} is $\pi(\Lambda) = \{1\}$. Now let us view G_{S_4} as a real Lie group. Then by Cartan's theorem Φ is a Lie subgroup of dimension zero, since Φ is totally disconnected. Hence Φ is discrete in G_{S_4}. To obtain a contradiction here, it suffices to view $G_{\mathcal{O}(S_2)}$ as a discrete subgroup of $G_{S_2} = G_{(S_2 \setminus S_4)} \times G_{S_4}$, whose quotient space has finite measure, and to invoke Lemma 3.17, in view of the fact that $G_{S_2 \setminus S_4}$ is noncompact (since $S \subset S_2 \setminus S_4$ and G_S is noncompact). This completes the proof of Theorem 7.12. Q.E.D.

Combining Theorem 7.12 and Proposition 7.13, we arrive at the following interesting observation: an algebraic K-group G either has strong approximation with respect to a nonempty subset S of V^K, or the closure $\bar{G}_K$ of G in G_{A_S} has infinite index.

The problem of strong approximation in algebraic groups has a long history. The first important result was the theorem of Eichler [1] on strong approximation in $\mathbf{SL}_n(D)$, where D is a finite-dimensional division algebra over K. Later various special cases of this problem over a number field K were studied by Eichler [2], Shimura [1] and Weil [3]. Next Kneser [10], [11] solved the problem of strong approximation for the classical groups, obtained the necessary conditions for its validity in the general case, and showed that the strong approximation theorem for arbitrary groups can be obtained when the Hasse principle holds. A complete solution of the strong approximation problem was obtained by Platonov [3]–[5] via a different approach. It is evident from the proof of Theorem 7.12 presented above that a central role is played by reducing the problem of strong approximation to the Kneser-Tits' conjecture over local fields, which was proved by Platonov (Theorem 7.6).

The strong approximation theorem is also valid for a global field of positive characteristic. The proof, however, requires considerable modification, not only to prove that conditions (1) and (2) are necessary (cf. Behr [2]), but especially to prove that they are sufficient. A crucial reason for this is that the key part of the above argument (which is close to the original version given in Platonov [4], [5])—the theory of analytic groups—cannot be applied in the case of positive characteristic. Prasad [1] refined Platonov's method and obtained a complete proof in the function field case; the proof uses Theorem 7.6 and relies on the following assertion, which is interesting in its own right.

THEOREM 7.13. *Let G be a K_v-simple K_v isotropic algebraic group. If H is a closed nondiscrete subgroup of G_{K_v} such that G_{K_v}/H has finite invariant measure, then $H \supset G_{K_v}^+$.*

A different proof of Theorem 7.13, based on the ergodic properties of G_{K_v}/H, was obtained by Margulis [1]. It should be noted that for characteristic zero the proof of Theorem 7.13 actually follows the same argument as the first part of the proof of sufficiency in Theorem 7.12.

7.5. Generalization of the strong approximation theorem.

Several mathematicians (cf. Mathews et al. [1], Nori [2]) have recently obtained results which in a certain sense generalize the strong approximation theorem. The point of departure for this generalization is the following straightforward observation: in proving strong approximation for a simply connected group G with respect to a finite set $S \supset V_\infty^K$, an important role is played by the assertion that the closure $\bar{G}_{\mathcal{O}(S)}$ of $G_{\mathcal{O}(S)}$ is open in G_{A_S}.

Indeed, the second part of the proof of sufficiency in Theorem 7.12 shows that, without loss of generality, one may assume all the v in V_f^K for which G is K_v-anisotropic to be contained in S; and it suffices to establish that for any finite subset S_1 of $V^K \setminus S$, the image of the natural embedding $\delta_{S_1}: G_{S_1} \to G_{A_S}$ is contained in $\bar{G}_K$. It follows from the openness of $\bar{G}_K$ that $W = \delta_{S_1}^{-1}(\operatorname{Im} \delta_{S_1} \cap \bar{G}_K)$ is an open subgroup of G_{S_1}, which is obviously normalized by G_K. But by the weak approximation property for G (Proposition 7.9), G_K is dense in G_{S_1}, and hence $W = G_{S_1}$ by Theorem 7.6. Thus we arrive at the question, investigated in the works mentioned above: if Γ is a finitely generated subgroup of G_K, when is its closure $\bar{\Gamma}$ open in G_{A_S}? We shall not state the results obtained in their most general form but, to visualize the approach, shall limit ourselves to the case $K = \mathbb{Q}$. Then one has

THEOREM 7.14. *Let G be a simply connected simple $\mathbb{Q}$-group, let S be a finite set of prime numbers, and let $\Gamma \subset G_{\mathbb{Z}(S)}$ be a Zariski-dense subgroup of G. Then $\bar{\Gamma}$ is open in G_{A_S}.*

The proof of Theorem 7.14 follows easily from the next assertion, which is of interest in its own right.

THEOREM 7.15. *Let π_p denote the reduction map modulo p. Then, under the assumptions of Theorem 7.14, for almost all $p \notin S$ we have $\pi_p(\Gamma) = \underline{G}^{(p)}_{F_p}$, where $\underline{G}^{(p)}$ is the reduction of G modulo p and F_p is the field of p elements.*

The proof of this result, found in Mathews et al. [1], unfortunately relies on the classification of the finite simple groups. In contrast, the proof presented in Nori [2] is self-contained and is based on several nice observations dealing with the properties of the exponential and logarithmic maps for characteristic $p > 0$.

Theorem 7.14 implies that any infinite arithmetic subgroup Γ of a simply connected simple algebraic $\mathbb{Q}$-group G contains many subgroups $\Phi \subset \Gamma$ of infinite index which are dense in Γ in the adelic topology. Indeed, Margulis-Soifer [2] showed that in Γ there is a continuum of maximal subgroups of infinite index which are the desired ones. On the other hand, in several cases, such as $\Gamma = SL_n(\mathbb{Z})$ $(n \geq 3)$, the adelic topology coincides with the profinite one (note that this assertion is equivalent to a positive solution of the congruence problem for Γ, cf. §9.5); this yields examples of proper subgroups $\Phi \subset \Gamma$ which are dense in the profinite topology. Then the corresponding homomorphism $\hat{\Phi} \to \hat{\Gamma}$ of profinite completions is surjective. Naturally one might ask whether there exist proper subgroups $\Phi \subset \Gamma$ for which the homomorphism $\hat{\Phi} \to \hat{\Gamma}$ is an isomorphism.

This question was put forward by Grothendieck [1], in 1970, for arbitrary finitely generated residually finite groups Γ. As Platonov and Tavgen have shown [1], the answer to the general Grothendieck problem is negative. A relevant example has already been found in the group $\Gamma = F \times F$, where F is a free group with generators x_1, x_2, x_3, and x_4. It suffices to consider the normal subgroup $N \lhd F$ generated by $x_2x_1x_2^{-1}x_1^{-2}$, $x_3x_2x_3^{-1}x_2^{-2}$, $x_4x_3x_4^{-1}x_3^{-2}$, and $x_1x_4x_1^{-1}x_4^{-2}$ (note that F/N is the remarkable Higman group) and to take $(N,1)F^{\Delta}$ for Φ, where F^{Δ} is the diagonal in $F \times F$. For further results on the Grothendieck problem, see Tavgen [1], [2]. In particular, a counterexample in the class of solvable groups was constructed in Tavgen [1]. We call the reader's attention to the fact that the above group, $\Gamma = F \times F$, is an arithmetic subgroup of $\mathbf{SL}_2 \times \mathbf{SL}_2$, so the Grothendieck conjecture is also false for the class of arithmetic groups. Nevertheless, the following remains an open

PROBLEM: Let Γ be an S-arithmetic subgroup of G having a finite congruence kernel $C^S(G)$ (for example $\Gamma = SL_n(\mathbb{Z})$, $n \geq 3$). Do there exist proper subgroups Φ of Γ for which the homomorphism $\hat{\Phi} \to \hat{\Gamma}$ of profinite completions is an isomorphism?

This problem is closely related to an interesting conjecture which came up in studying the representations of finitely generated groups. In §2.4.7 we defined the variety of representations $R(\Gamma, G)$ of a finitely generated group Γ in an algebraic group G. Instead of $R(\Gamma, \mathbf{GL}_n)$, we shall write $R_n(\Gamma)$, and call the latter the *variety of n-dimensional representations of* Γ. It is well known (cf. van der Waerden [1]) that a completely reducible representation $\varrho \in R_n(\Gamma)$ is uniquely defined up to equivalence by its character, i.e., by the function $\chi_\varrho(g) = \operatorname{tr} \varrho(g)$, $g \in \Gamma$; on the other hand, for an arbitrary ϱ there exists a completely reducible representation ϱ_0 with the same character: $\chi_\varrho = \chi_{\varrho_0}$. Thus, a natural one-to-one correspondence arises between the set of equivalence classes of completely reducible n-dimensional representations of Γ and the set $\mathbf{X}_n(\Gamma)$ of all n-dimensional characters. It turns out that $\mathbf{X}_n(\Gamma)$ also has the natural structure of an algebraic variety. Computing $\mathbf{X}_n(\Gamma)$ for concrete groups and studying the impact of the geometry of $\mathbf{X}_n(\Gamma)$ on the properties of Γ and its representations are the main problems related to the geometric approach to representation theory of finitely generated groups, which has its origins in the classical works of Poincaré, Klein, Vogt and Fricke.

One of the first questions arising here is what are the Γ for which $\dim \mathbf{X}_n(\Gamma) = 0$, for any n? (This condition is equivalent to the finiteness of $\mathbf{X}_n(\Gamma)$; hence the groups satisfying it are naturally called groups of finite representation type.) Clearly all finite groups are groups of finite representation type; but there are also infinite groups with this property, such as $\Gamma = SL_m(\mathbb{Z})$, $m \geq 3$. The finiteness of the representation type here follows from a general theorem of Margulis on the almost algebraicity of finite-dimensional representations of irreducible lattices in semisimple Lie groups of rank ≥ 2 (cf. Margulis [5]). However, Margulis' argument does not reveal the connection between finiteness of the representation type and the structure of Γ. Therefore we shall show how the finiteness of type of $\Gamma = SL_m(\mathbb{Z})$, $m \geq 3$, can be deduced from a result of Carter and Keller [1] on the bounded generation of Γ with respect to the set of elementary matrices (cf. §4.4).

PROPOSITION 7.14. *Let $\Gamma = SL_m(\mathbb{Z})$, $m \geq 3$. Then $\dim \mathbf{X}_n(\Gamma) = 0$ for any n.*

PROOF (RAPINCHUK): The essence of Carter and Keller's result mentioned above consists of proving the existence of an integer $d > 0$ such that any element x in Γ can be written as $x = x_1^{\alpha_1} \dots x_d^{\alpha_d}$, where $\alpha_i \in \mathbb{Z}$ and x_i is one of the elementary matrices $e_{jk}(1)$, the set of which we shall denote by X. Now let $\varrho\colon \Gamma \to GL_n(\mathbb{C})$ be an n-dimensional representation. If $U \subset \Gamma$ is the subgroup of upper unipotent matrices, then $\varrho(U)$ is a nilpotent subgroup of $GL_n(\mathbb{C})$. By the Malcev-Kolchin theorem $\varrho(U)$ has a triangulizable normal

subgroup N of finite index l. Then, obviously, $\varrho(e_{ij}(l)) = \varrho(e_{ij}(1))^l \in N$ for all $i < j$; consequently

$$\varrho(e_{13}(l^2)) = \varrho([e_{12}(l), e_{23}(l)]) \in [N, N];$$

in particular $\varrho(e_{13}(l^2))$ is a unipotent matrix. Since all the $e_{ij}(1)$ in Γ are conjugate, we obtain that $\varrho(e_{ij}(l^2))$ is a unipotent matrix for any $i \neq j$. In other words,

$$(\varrho(e_{ij}(1)))^{l^2} - E_n)^n = 0, \tag{7.16}$$

where E_n is the identity matrix. Let $f(t)$ denote the polynomial $(t^{l^2} - 1)^n$ of degree $\delta = l^2 n$. Then (7.16) means that $f(\varrho(x)) = 0$ for any x in X. We let Y denote the (finite) set $\{ x_1^{\alpha_1} \dots x_d^{\alpha_d} : x_i \in X,\ 0 \leq \alpha \leq \delta \}$ and show that the $\mathbb{Q}$-hull $\mathbb{Q}[\varrho(\Gamma)]$ is precisely the $\mathbb{Q}$-space spanned by $\varrho(Y)$; in particular, $\dim_{\mathbb{Q}} \mathbb{Q}[\varrho(\Gamma)] < \infty$. Indeed, since $f(\varrho(x)) = 0$ for any x in X, any power $\varrho(x)^\alpha$ can be expressed linearly in the $\varrho(x)^\beta$, $0 \leq \beta \leq \delta$, with integral coefficients. Now, writing any z in Γ as $z = x_1^{\alpha_1} \dots x_d^{\alpha_d}$, where $x_i \in X$ and $\alpha_i \in \mathbb{Z}$, and plugging in the expression already obtained for $\varrho(x_i)^{\alpha_i}$ in the corresponding expression for $\varrho(z)$, we obtain a presentation for $\varrho(z)$ as a linear combination of the elements of $\varrho(Y)$, as desired.

It follows, for any z in Γ, that the powers $\varrho(z)^i$ cannot be linearly independent over $\mathbb{Q}$, so $\varrho(z)$ satisfies some polynomial equation with rational coefficients. All the eigenvalues $\lambda_1, \dots, \lambda_n$ of the matrix of $\varrho(z)$ satisfy this equation and thus are algebraic numbers. Therefore $\operatorname{tr} \varrho(z) = \sum_{i=1}^n \lambda_i$ will also be algebraic. The proof of the proposition is completed by

LEMMA 7.5. *Suppose that for any representation $\varrho \in R_n(\Gamma)$ all the $\operatorname{tr} \varrho(x)$ are algebraic numbers. Then $\dim \mathbf{X}_n(\Gamma) = 0$.*

PROOF: Suppose $\dim \mathbf{X}_n(\Gamma) > 0$. Then there exists an irreducible curve $C \subset R_n(\Gamma)$, defined over a finitely generated field k, whose image under the map $\mu: R_n(\Gamma) \to \mathbf{X}_n(\Gamma)$ does not reduce to a point. Let K denote the function field $k(C)$ and, embedding k in $\mathbb{C}$, construct a representation $\pi: \Gamma \to GL_n(\mathbb{C})$, defining $\pi(x)$ for x in Γ as the matrix (a_{ij}), where a_{ij} is the function on C such that $a_{ij}(\varrho) = \varrho(x)_{ij}$ for ϱ in C. Since the image of C in $\mathbf{X}_n(\Gamma)$ does not reduce to a point, it follows that there exists x_0 in Γ for which $\chi_\pi(x_0) = \operatorname{tr} \pi(x_0)$ is a nonconstant function of $k(C)$, in particular $\chi_\pi(x_0) \notin \bar{\mathbb{Q}}$. We obtain a contradiction to the algebraicity of the traces of all the ϱ in $R_n(\Gamma)_{\mathbb{C}}$. Thus Lemma 7.5 and Proposition 7.14 are proved.

In §4.4 we noted that Tavgen [3] generalized the result of Carter-Keller [1] for all Chevalley groups of rank ≥ 2. In this connection, we wish to point out that the proof of Proposition 7.14 also extends to these groups. (More precisely, if all the roots have the same length, then the proof goes through as is. For a system having roots of different lengths, some modifications are required due to the fact that the analog of (7.16) must be proved separately for long and short roots.)

In analyzing the known examples of groups of finite representation type, Platonov [22], [23] has set forth the following conjecture:

CONJECTURE (ON ARITHMETICITY): Assume Γ is a finitely generated linear group, such that $\dim \mathbf{X}_n(\Gamma) = 0$ for any n. Then Γ is a group of arithmetic type.

(By a group of arithmetic type we mean a group which is commensurable with a direct product of suitable S-arithmetic subgroups (possibly for different S), where the commensurability in this situation means there exist isomorphic subgroups of finite index.)

Unfortunately, this conjecture is still far from being proved. However, even preliminary investigation has brought to light a surprising connection with the Grothendieck problem stated above (cf. Platonov-Tavgen [2]). Namely, if, for example, one could find a proper subgroup Φ in $\Gamma = SL_n(\mathbb{Z})$, $n \geq 3$, for which the natural homomorphism $\hat{\Phi} \to \hat{\Gamma}$ of the profinite completions is an isomorphism, then the representations of Φ and Γ would be the same for each dimension. Consequently, Proposition 7.14 would imply that Φ has finite representation type. However, Grothendieck proved in fact that Φ cannot be an arithmetic group. Therefore, for subgroups of most arithmetic groups, the Platonov conjecture would imply an affirmative answer to the Grothendieck problem stated above.

8. Class numbers and class groups of algebraic groups

In this chapter we study an important arithmetic invariant of an algebraic K-group G—its class number $\mathrm{cl}(G)$ (cf. §5.1). In §8.1 we present results which allow the problem of computing $\mathrm{cl}(G)$ to be interpreted as the problem of computing the number of classes in the genus of various arithmetical objects. In particular, we establish that the class number $\mathrm{cl}(\mathbf{O}_n(f))$ of the orthogonal group of a quadratic form f is precisely the number of classes in the genus of f, and the class number $\mathrm{cl}(\mathbf{GL}_n)$ of $\mathbf{GL}_n$ $(n \geq 1)$ over K equals the class number of K.

These examples suggest that computation of class number is a difficult, even hopeless, problem in its most general formulation. Naturally, we cannot pay equally close attention to all aspects of the problem, so we have decided to focus on studying the possible values of $\mathrm{cl}(\varphi(G))$, the class number of a fixed algebraic K-group G under various realizations φ, depending on the arithmetic properties of the group. The most complete results are obtained for G a semisimple group of noncompact type. It turns out that $\mathrm{cl}(G)$ in this case is the order of some finite abelian group $\mathcal{G}\mathrm{cl}(G)$, called the *class group*, whose exponent is always a divisor of the exponent of f of the fundamental group F of G. In particular, if the canonical factorization of f can be written as $f = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, then the class number with respect to any realization can be written as $p_1^{\beta_1} \dots p_r^{\beta_r}$. In §8.2 we prove the realization theorem, according to which any number of such a form can be obtained as a class number of G in a suitable realization. In §8.3 we study the class number of semisimple groups of compact type. The main result of this section asserts that the class number here takes on values which are divisible by any given number. In §8.4 we prove a general theorem on the unboundedness of the class numbers of nonsimply connected groups and study the relationship between the class number of a group and the class numbers of its most important subgroups (parabolic subgroups and maximal tori).

Several classical arithmetic problems can be solved with the results obtained here. In particular, in §§8.2–8.3 we look at problems of the number of classes in the genus of a quadratic form and the number of classes in the genus of a lattice under conjugation. In §8.5 we investigate the genus problem in arithmetic groups and for integral representations of finite groups.

8.1. Class numbers of algebraic groups and number of classes in a genus.

Let K be an algebraic number field. Recall (cf. §5.1) that by definition

the *class number* $\mathrm{cl}(G)$ of an algebraic K-group G is the number of double cosets $G_{A(\infty)}xG_K$ of the adele group G_A modulo the subgroups $G_{A(\infty)}$ and G_K of integral and principal adeles respectively. In §1.2 we saw that for the idele group J_K of K (which is the adele group of the one-dimensional K-split torus $\mathbb{G}_m$) the index $[J_K : J_K^\infty K^*]$ is equal to the class number h_K of K. Below we shall show that for the orthogonal group $G = \mathbf{O}_n(f)$ of a nondegenerate n-dimensional quadratic form f over K, $\mathrm{cl}(G)$ is equal to the number of classes in the genus of f. Thus, the definition of class number is a natural generalization of the classical arithmetic invariants introduced by Lagrange and Gauss. Moreover, we shall see that this definition works in other situations as well, enabling us to achieve new results by means of general methods.

The following remark should always be born in mind when working with class numbers of algebraic groups. While J_K has a uniquely determined subgroup J_K^∞ of integral ideles, in an arbitrary algebraic K-group G the group $G_{A(\infty)}$ of integer adeles is well-defined only when there is a fixed realization of G as a matrix group. Below, by a realization of G we mean a specified K-representation $\varphi\colon G \to \mathbf{GL}_r$ and lattice $L(\varphi) \subset K^r$. Then one can put $G_{A(\infty)}^{L(\varphi)} = \varphi_A^{-1}(\varphi(G)_{A(\infty)}^{L(\varphi)})$, where

$$\varphi(G)_{A(\infty)}^{L(\varphi)} = \prod_{v \in V_\infty^K} \varphi(G)_{K_v} \times \prod_{v \in V_f^K} \varphi(G)_{\mathcal{O}_v}^{L(\varphi)_v};$$

here $\varphi(G)_{\mathcal{O}_v}^{L(\varphi)_v} = \{\, g \in \varphi(G)_{K_v} : gL(\varphi)_v = L(\varphi)_v \,\}$ is the group of v-adic integral points under the localization $L(\varphi)_v$ of $L(\varphi)$, i.e., the aggregate of those g in $\varphi(G)_{K_v}$ which are given by a matrix in $GL_r(\mathcal{O}_v)$ with respect to a base of the lattice $L(\varphi)_v$. Equivalently, $\varphi(G)_{A(\infty)}^{L(\varphi)}$ can be viewed as the stabilizer in $\varphi(G)_A$ of $L(\varphi)$ under the action of $GL_r(A)$ on lattices in K^r, defined as follows: if $g = (g_v) \in GL_r(A)$ and $L \subset K^r$ is a lattice, then we have $g_v \in GL_r(\mathcal{O}_v)$ and $L_v = \mathcal{O}_v^r$ for almost all v in V_f^K (cf. §1.5.3); so $g_v L_v = L_v$. Therefore by Theorem 1.15 there exists a unique lattice $M \subset K^r$ satisfying $M_v = g_v L_v$ for all v in V_f^K, and by definition we put $M = gL$.

We shall write the class number of G corresponding to the representation φ as $\mathrm{cl}(\varphi(G)^{L(\varphi)})$, but shall also use the notation $\mathrm{cl}(G^{L(\varphi)})$, $\mathrm{cl}(\varphi(G))$, or simply $\mathrm{cl}(G)$ when this does not lead to ambiguity. Note that Theorem 5.1 implies that $\mathrm{cl}(\varphi(G))$ is finite for any φ. Indeed, Theorem 5.1 itself actually asserts the finiteness of $\mathrm{cl}(\varphi(G))$ for any φ defined by a free lattice $L(\varphi)$. On the other hand, for two arbitrary representations $\varphi_i\colon G \to \mathbf{GL}_{r_i}$ $(i = 1, 2)$, the $G_{A(\infty)}^{L(\varphi_i)}$ are commensurable. Indeed, $G_{A(\infty)}^{L(\varphi_i)} = G_\infty \times G_{A_f(\infty)}^{L(\varphi_i)}$, where the Archimedean part G_∞ of the adele group is independent of the choice of the

representation and the finite parts $G_{A_f(\infty)}^{L(\varphi_1)}$ and $G_{A_f(\infty)}^{L(\varphi_2)}$ are commensurable as two open compact subgroups of G_{A_f}. It follows that $\mathrm{cl}(\varphi_1(G))$ and $\mathrm{cl}(\varphi_2(G))$ are either both finite or both infinite. In view of the above, this remark implies

THEOREM 8.1. *$\mathrm{cl}(\varphi(G))$ is finite for any representation φ of an algebraic K-group G.*

As we noted, the basic objective of this chapter is to study the values that $\mathrm{cl}(\varphi(G))$ can assume, depending on the arithmetic and structural properties of G. In this regard, recall that $\mathrm{cl}(\varphi(G))$ is 1 for any representation φ if G has absolute strong approximation (cf. Proposition 5.4).

Above we saw that h_K, the class number of K, can be interpreted as the class number of the one-dimensional K-split torus $T \simeq \mathbf{GL}_1$. It turns out that h_K is also the class number of the full linear group of arbitrary dimension.

PROPOSITION 8.1. *Let $G = \mathbf{GL}_n$ be the full linear group over K, in its natural realization. Then $\mathrm{cl}(G) = h_K$.*

PROOF: We use an approach widely applied in computing class numbers: essentially, the "noncommutative" problem of calculating the number of double cosets is reduced to the computation of an index of commutative groups. In the case at hand, this can be done using the homomorphism $\det\colon G \to \mathbb{G}_m$, which, for the sake of brevity, we denote by f. Clearly the image of $f(G_A)$ is the idele group J_K of K, $f(G_{A(\infty)})$ is the subgroup of integral ideles J_K^∞, and $f(G_K)$ is the subgroup K^* of principal ideles. We shall show that the map $\theta\colon G_{A(\infty)} \setminus G_A/G_K \to J_K^\infty \setminus J_K/K^*$, induced by f, is one-to-one. Then

$$\mathrm{cl}(G) = [J_K : J_K^\infty K^*] = h_K,$$

as desired. In view of what we have just observed, we need only prove that θ is injective, i.e.,

$$J_K^\infty f(g)K^* = J_K^\infty f(h)K^* \Rightarrow G_{A(\infty)}gG_K = G_{A(\infty)}hG_K \tag{8.1}$$

for $g, h \in G_A$. If $f(g) = xf(h)y$, where $x \in J_K^\infty$, $y \in K^*$, then choosing a in $G_{A(\infty)}$ and b in G_K such that $f(a) = x$ and $f(b) = y$, we obtain $f(g) = f(ahb)$; and it suffices to show that g and $t = ahb$ determine the same double coset modulo $G_{A(\infty)}$ and G_K. Obviously

$$s = t^{-1}g \in H_A,$$

where $H = \mathbf{SL}_n$. $U = t^{-1}H_{A(\infty)}t$ is an open subgroup of H_A, and therefore $Us \cap H_\infty H_K$ is nonempty, since absolute strong approximation holds for

H. In view of the fact that $H_\infty \subset U$, it follows that there exist u in $H_{A(\infty)}$ and v in H_K such that

$$s = t^{-1}g = t^{-1}utv.$$

Then $g = utv$, as desired. Proposition 8.1 is proved.

When $G = \mathbf{GL}_n$, one can push the equality $\mathrm{cl}(G) = h_K$ further by applying an argument analogous to that used to show $h_K = [J_K : J_K^\infty K^*]$ and replacing fractional ideals of K (i.e., lattices in K^1) by n-dimensional lattices. To do so, let us fix the lattice $L = \mathcal{O}^n$ in K^n and use the action of G_A on lattices, defined above. We claim that the orbit $G_A(L)$ is precisely the entire set $\mathcal{L}$ of all n-dimensional lattices. Indeed, $L_v = M_v$ for any lattice M of K^n and almost all v in V_f^K. However, each localization M_v is $\mathcal{O}_v$-free (cf. §1.5) and therefore one can find g_v in G_{K_v} such that $M_v = g_v(L_v)$. It follows easily that there exists an adele g in G_A such that $M = g(L)$. Since $G_{A(\infty)}$ is the stabilizer of L, the set of double cosets $\{ G_{A(\infty)} \backslash G_A/G_K \}$ is in one-to-one correspondence with the set of orbits $G_K \backslash \mathcal{L}$, i.e., the set of classes of isomorphic lattices. Therefore, Proposition 8.1 implies that the number of isomorphism classes of n-dimensional lattices is h_K, the class number of K. This can also be proved directly by methods from lattice theory. To do so we use the concept of the pseudobase of a lattice, introduced in §1.5.3. Recall that any lattice M of K^n has a pseudobase, i.e., there exists a presentation of the form $M = \mathcal{O}x_1 \oplus \mathcal{O}x_2 \oplus \cdots \oplus \mathcal{O}x_{n-1} \oplus \mathfrak{a}x_n$, where $\mathfrak{a} \subset \mathcal{O}$ is an ideal whose class in the ideal class group depends only on M. Furthermore, one can show that two lattices $M = \mathcal{O}x_1 \oplus \ldots \mathcal{O}x_{n-1} + \mathfrak{a}x_n$ and $N = \mathcal{O}y_1 \oplus \cdots \oplus \mathcal{O}y_{n-1} \oplus \mathfrak{b}y_n$ are isomorphic if and only if the classes of $\mathfrak{a}$ and $\mathfrak{b}$ are the same. This implies that the classes of isomorphic n-dimensional lattices are in one-to-one correspondence with the classes of the fractional ideals of K, and so we obtain again $\mathrm{cl}(G) = [G_K \backslash \mathcal{L}] = h_K$. This example readily illustrates that the adelic interpretation offers a faster and more direct proof. Moreover, it enables us to formulate the following useful *criterion for a lattice to be free.*

LEMMA 8.1. *Fix a lattice $L = \mathcal{O}^n$ and consider an arbitrary lattice M in K^n. Then M is free if and only if $f(g) \in J_K^\infty K^*$, where g in G_A is an element satisfying $M = g(L)$.*

PROOF: It follows from what we have seen above that M is free if and only if $g \in G_K G_{A(\infty)}$, which by (8.1) reduces to the condition $f(g) \in J_K^\infty K^*$.

This implies

PROPOSITION 8.2. *Let K be an algebraic number field with the Hilbert class field $\tilde{K}$, and let L be a free lattice in K^n. Then a lattice M in K^n is free if there exists $v_0 \in V_f^K$ such that $L_v = M_v$ for $v \in V_f^K$, $v \neq v_0$ and $\tilde{K} \subset K_{v_0}$.*

PROOF: To begin with, recall that by the Hilbert class field for K we mean a maximal abelian extension of K which is unramified at all points. In terms of global class field theory, $\tilde{K}$ is defined as the field corresponding to the norm subgroup $J_K^\infty K^*/K^*$ of C_K; so $\mathrm{Gal}(\tilde{K}/K)$ is isomorphic to the ideal class group of K. In this connection, $\tilde{K} \subset K_{v_0}$ is equivalent to the principal class $J_K^\infty K^*$ containing all the ideles $i^{v_0}(\alpha)$ $(\alpha \in K_{v_0}^*)$, given componentwise by

$$i_v = \begin{cases} 1, & v \neq v_0 \\ \alpha, & v = v_0. \end{cases}$$

(All of these results can be found in [ANT].)

Now let M satisfy the conditions of the proposition. Then for g in G_A which sends L to M we can take an adele of the form $g^{v_0}(a)$ $(a \in G_{K_{v_0}})$, so $f(g) = i^{v_0}(\det a) \in J_K^\infty K^*$, and by Lemma 8.1 M is free. Proposition 8.2 is proved.

To prove the theorem on one-class lattices (cf. §8.2) we shall need another result which also follows from Lemma 8.1.

PROPOSITION 8.3. *Let S be a finite subset of V^K containing V_∞^K, such that $J_K = J_K^S K^*$, where J_K^S is the group of S-integral ideles. Then for any lattice M in K^n there exists a free lattice N in K^n such that $M_v = N_v$ for all v in $V^K \setminus S$. In other words, any lattice can be made free by changing its localization only for v in $S \setminus V_\infty^K$.*

PROOF: Put $L = \mathcal{O}^n$, and let g be an adele in G_A such that $M = g(L)$. Then $f(g) \in J_K = J_K^S K^*$; and therefore $f(g) = xyz$, where $x_v = 1$ for $v \notin S \setminus V_\infty^K$, $y \in J_K^\infty$, and $z \in K^*$. For v in $S \setminus V_\infty^K$ take a_v in G_{K_v} such that $f(a_v) = x_v$, and construct the adele h with components

$$h_v = \begin{cases} 1, & v \notin S \setminus V_\infty^K, \\ a_v, & v \in S \setminus V_\infty^K. \end{cases} \tag{8.2}$$

We claim that $N = h^{-1}(M)$ is the desired lattice. Indeed, $N = h^{-1}g(L)$ and $f(h^{-1}g) = f(h)^{-1}f(g) = x^{-1}(xyz) = yz \in J_K^\infty K^*$, so N is free. However, (8.2) implies that $N_v = M_v$ for v in $V^K \setminus S$. The proposition is proved.

Now we can conclude our discussion of questions dealing with the computation of the class number of $G = \mathbf{GL}_n$, in its natural realization, and with various interpretations of $\mathrm{cl}(G) = h_K$. This discussion, however, does not cover all the relations between the class numbers of algebraic groups and classical arithmetic invariants. In particular, we now show that the number of classes in the genus of a nondegenerate quadratic form f is precisely the class number of the corresponding orthogonal group $G = \mathbf{O}_n(f)$.

We deduce this from a general result which has several other interesting applications.

So, let G be a linear algebraic K-group acting on an affine K-variety X. Let us fix realizations of $G \subset \mathbf{GL}_n$ and $X \subset \mathbb{A}^m$, such that the action of G on X is defined over the ring of integers $\mathcal{O}$ of K, i.e., is given by polynomials with coefficients in $\mathcal{O}$. We say that two elements x, y in $X_\mathcal{O}$ are equivalent (with respect to $G_\mathcal{O}$) if there exists an element g in $G_\mathcal{O}$ such that $y = gx$. As we shall see in the examples below, this definition includes the classical concepts of the equivalence of integral matrices, integral quadratic forms, integral representations of finite groups and other arithmetical objects.

The basic problem which arises here is to determine necessary and sufficient conditions for the equivalence of two elements. In this regard, one can readily point out a series of very natural necessary conditions: if x, y in $X_\mathcal{O}$ are equivalent with respect to $G_\mathcal{O}$, then they are equivalent with respect to G_K and $G_{\mathcal{O}_v}$ for all non-Archimedean valuations v of K, i.e., there exist g_K in G_K and g_v in $G_{\mathcal{O}_v}$ $(v \in V_f^K)$ such that $g_K x = y$ and $g_v x = y$. The question of the sufficiency of these conditions comes down to a question of the validity of the local-global principal holds in the given situation. This is a very complicated question, and in most instances the answer is negative. In order to discuss the question quantitatively (i.e., to characterize the deviation from the local-global principal) we introduce the following

DEFINITION: Let $x \in X_\mathcal{O}$. The *genus* $\operatorname{gen}(x)$ of x is the collection of all elements y in $X_\mathcal{O}$ such that x and y are equivalent with respect to G_K and $G_{\mathcal{O}_v}$ for all v in V_f^K. The *class* $\operatorname{cl}(x)$ of x is the orbit $G_\mathcal{O} x$, i.e., the aggregate of those y which are equivalent to x with respect to $G_\mathcal{O}$. Each $\operatorname{gen}(x)$ partitions into the union of disjoint classes:

$$\operatorname{gen}(x) = \bigcup_{i \in I} \operatorname{cl}(x_i), \quad \operatorname{cl}(x_i) \cap \operatorname{cl}(x_j) = \emptyset \quad (i \neq j);$$

the order of I is called the *number of classes in the genus* of x (under the action of G) and is denoted as $f_G(x)$.

Thus, we see that the local-global principal for equivalence holds if and only if $f_G(x) = 1$. In general $f_G(x) \neq 1$, and this naturally raises the question of computing $f_G(x)$. The results in this vein will be discussed in the sections that follow; for the time being, we point out the connections with the class numbers of algebraic groups.

THEOREM 8.2 (ON THE STABILIZER). *Let $x \in X_\mathcal{O}$ and let $G(x) = \{ g \in G : gx = x \}$, the stabilizer of x. Then $f_G(x)$ equals the number of double cosets $G(x)_{A(\infty)} g G(x)_K \subset G(x)_A$ which are contained in the principal class $G_{A(\infty)} G_K$. In particular, $f_G(x)$ is always finite. If absolute strong approximation holds for G, then $f_G(x) = \operatorname{cl}(G(x))$.*

PROOF: Let $\mathfrak{g}$ be the quotient set obtained from $\operatorname{gen}(x)$ by identifying the elements belonging to the same class. Since $f_G(x) = |\mathfrak{g}(x)|$, to prove the theorem it suffices to establish a one-to-one correspondence between $\mathfrak{g}(x)$ and the set M of double cosets $G(x)_{A(\infty)} g G(x)_K \subset G(x)_A$ which are contained in $G_{A(\infty)} G_K$.

Let $\bar{g} = G(x)_{A(\infty)} g G(x)_K \in M$, i.e.,

$$g = g_{A(\infty)} g_K, \tag{8.3}$$

where $g_{A(\infty)} \in G_{A(\infty)}$ and $g_K \in G_K$. Define

$$y = g_K x, \tag{8.4}$$

We claim $y \in \operatorname{gen}(x)$. First note that $y \in X_K$, by definition. Furthermore, (8.3) implies that for any v in V_f^K the v-component g_v is $g_{\mathcal{O}_v} g_K$, where $g_{\mathcal{O}_v} \in G_{\mathcal{O}_v}$. It follows that $g_K = g_{\mathcal{O}_v}^{-1} g_v$ and

$$y = g_{\mathcal{O}_v}^{-1} x, \tag{8.5}$$

since $g_v \in G(x)_{K_v}$; in particular, $y \in X_{\mathcal{O}_v}$. Therefore $y \in X_\mathcal{O}$, and (8.4) and (8.5) show that $y \in \operatorname{gen}(x)$.

Now we define $\theta \colon M \to \mathfrak{g}(x)$, mapping $\bar{g}$ into the class containing y. We claim first that θ is well defined. Suppose

$$\bar{g} = G(x)_{A(\infty)} g G(x)_K = G(x)_{A(\infty)} h G(x)_K,$$

i.e., $h = t_{A(\infty)} g t_K$, where $t_{A(\infty)} \in G(x)_{A(\infty)}$ and $t_K \in G(x)_K$. Consider an arbitrary factorization $h = h_{A(\infty)} h_K$ in $G_{A(\infty)} G_K$. Then

$$h = h_{A(\infty)} h_K = (t_{A(\infty)} g_{A(\infty)})(g_K t_K),$$

and consequently

$$s = h_{A(\infty)}^{-1} t_{A(\infty)} g_{A(\infty)} = h_K \, t_K^{-1} g_K^{-1} \in G_{A(\infty)} \cap G_K = G_\mathcal{O}.$$

Now $h_K = s g_K t_K$; letting $\tilde{y} = h_K x$, we have

$$\tilde{y} = h_K x = (s g_K t_K) x = s(g_K x) = sy,$$

from which it follows that $\tilde{y}$ lies in the same class as y, proving our claim.

Surjectivity of θ. Let $y \in \mathrm{gen}(x)$. Then

$$y = g_K x = g_v x \tag{8.6}$$

for suitable g_K in G_K and g_v in $G_{\mathcal{O}_v}$ $(v \in V_f^K)$. Let h denote the adele with components

$$h_v = \begin{cases} g_K & v \in V_\infty^K, \\ g_v, & v \in V_f^K. \end{cases} \tag{8.7}$$

Obviously, $h \in G_{A(\infty)}$. It follows from (8.6) and (8.7) that for any v in V^K we have $h_v^{-1} g_K \in G(x)_{K_v}$, so $g = h^{-1} g_K \in G(x)_A$. Thus, by assumption $\bar{g} = G(x)_{A(\infty)} g G(x)_K \in M$, and its image under θ is the equivalence class in $\mathfrak{g}(x)$ containing y, thereby proving θ to be surjective.

Injectivity of θ. Let g and h be elements in $G(x)_A$ for which the respective classes $\bar{g}$ and $\bar{h}$ lie in M and $\theta(\bar{g}) = \theta(\bar{h})$. Choose factorizations $g = g_{A(\infty)} g_K$ and $h = h_{A(\infty)} h_K$ in $G_{A(\infty)} G_K$. Then $\theta(\bar{g}) = \theta(\bar{h})$ means there exists s in $G_{\mathcal{O}}$ such that

$$h_K x = s g_K x.$$

Put $t_{A(\infty)} = h_{A(\infty)} s^{-1} g_{A(\infty)}^{-1}$ and $t_K = g_K^{-1} s^{-1} h_K$. It is easily verified that

$$t_{A(\infty)} \in G(x)_A \cap G_{A(\infty)} = G(x)_{A(\infty)},$$
$$t_K \in G(x)_A \cap G_K = G(x)_K.$$

Then $h = t_{A(\infty)} g t_K$, i.e $\bar{g} = \bar{h}$, establishing the injectivity of θ.

Thus we have proved the main part of Theorem 8.2. The finiteness of $f_G(x)$ now follows immediately from Theorem 8.1. If G has absolute strong approximation, then $\mathrm{cl}(G) = 1$ (cf. Proposition 5.4), i.e., $G_A = G_{A(\infty)} G_K$, and therefore $f_G(x) = \mathrm{cl}(G(x))$, completing the proof of Theorem 8.2.

Now we give some applications of Theorem 8.2.

EXAMPLE 1 (QUADRATIC FORMS): Let X be the variety of nonsingular symmetric $(n \times n)$-matrices, viewed as a subvariety of the n^2-dimensional affine space $\mathbb{A}^{n^2} \simeq M_n$. The points of X are in one-to-one correspondence with the nondegenerate n-dimensional quadratic forms, sending the points of X_K and $X_{\mathcal{O}}$ to K- and $\mathcal{O}$-defined forms, respectively. $G = \mathbf{GL}_n$ acts naturally on X, by

$$g(F) = {}^t g F g, \quad \text{for } g \in G,\ F \in X,$$

where ${}^t g$ is the matrix transpose to g; clearly this action is defined over $\mathcal{O}$. Therefore, using the above definition, we can introduce the concepts of the genus and the class of a symmetric matrix $F \in X_{\mathcal{O}}$, as well as the concept of the number of classes $f_G(F)$ in the genus. Since there is a one-to-one correspondence between the elements of X and quadratic forms, all the concepts mentioned carry over to quadratic forms and become the classical concepts in the theory of quadratic forms which goes back to Lagrange and Gauss. Thus, for example, the genus $\mathrm{gen}(f)$ of a quadratic form f with coefficients in $\mathcal{O}$ is the set of quadratic forms with coefficients in $\mathcal{O}$ which are equivalent to f over K and over all $\mathcal{O}_v$ for v in V_f^K; also, $\mathrm{cl}(f)$ is the set of forms which are $\mathcal{O}$-equivalent to f. Here the number of classes in the genus is traditionally designated by $c(f)$.

If f is a nondegenerate quadratic $\mathcal{O}$-defined form and F is the corresponding symmetric matrix in $X_{\mathcal{O}}$, then the stabilizer $G(F)$ is $\mathbf{O}_n(f)$. Let us show that always $\mathbf{O}_n(f)_A \subset GL_n(A(\infty)) GL_n(K)$. For each v in V_f^K, clearly $GL_n(\mathcal{O}_v)$ contains a matrix with determinant -1; therefore, any element of $\mathbf{O}_n(f)_A$ can be put into $SL_n(A)$ by multiplying by a suitable element of $GL_n(A(\infty))$. But, as we have noted, $\mathrm{cl}(\mathbf{SL}_n) = 1$, i.e.,

$$SL_n(A) = SL_n(A(\infty)) SL_n(K),$$

from which it follows that $\mathbf{O}_n(f)_A \subset GL_n(A(\infty)) GL_n(K)$. In view of this, Theorem 8.2 yields

PROPOSITION 8.4. *The number of classes $c(f)$ in the genus of a nondegenerate quadratic form f is finite and equals the class number $\mathrm{cl}(\mathbf{O}_n(f))$ of the corresponding orthogonal group.*

Here it is relevant to cite a straightforward example, due to Milnor, which shows that in general $c(f) \neq 1$. Take two symmetric integral matrices over $\mathbb{Q}$:

$$F_1 = \begin{pmatrix} 5 & 0 \\ 0 & 11 \end{pmatrix}, \qquad F_2 = \begin{pmatrix} 1 & 0 \\ 0 & 55 \end{pmatrix}.$$

Let us introduce the following nonsingular rational matrices:

$$g_1 = \begin{pmatrix} \frac{1}{4} & -\frac{11}{4} \\ \frac{1}{4} & \frac{5}{4} \end{pmatrix}, \qquad g_2 = \begin{pmatrix} \frac{1}{7} & -\frac{22}{7} \\ \frac{2}{7} & \frac{5}{7} \end{pmatrix}.$$

Direct computation shows that ${}^t g_i F_1 g_i = F_2$ $(i = 1, 2)$. Since the g_i are rational, and moreover $g_1 \in GL_2(\mathbb{Z}_p)$ for all $p \neq 2$ and $g_2 \in GL_2(\mathbb{Z}_2)$, it follows that F_1 and F_2 (and their respective quadratic forms f_1, f_2) lie in the same genus. At the same time, if we assume that F_1 and F_2 lie in the same class, then there must be an integral matrix $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ such that

${}^tgF_1g = F_2$. This relation, as one can easily verify, reduces to the following system of equations

$$\begin{cases} 5a^2 + 11c^2 = 1 \\ 5ab + 11cd = 0 \\ 5b^2 + 11d^2 = 55, \end{cases}$$

in which even the first equation has no integral solution. Thus, $f_{\mathbf{GL}_2}(F_1) = c(f_1) > 1$.

EXAMPLE 2 (INTEGRAL REPRESENTATIONS): Let Γ be a finitely generated group, and let $X = R_n(\Gamma)$ be the variety of n-dimensional representations of Γ viewed as a subvariety of $(\mathbf{GL}_n)^d$ (cf. §§2.4, 7.5). The group $G = \mathbf{GL}_n$ acts naturally on $R_n(\Gamma)$, since the orbits of this action are the classes of equivalent representations. The points of $X_{\mathbb{Z}}$ correspond to integral representations $\varrho\colon \Gamma \to GL_n(\mathbb{Z})$ of degree n, and the general concepts of the genus and the class of an element reduce in this situation to the concepts of the genus and the class of an integral representation, used in representation theory (cf. Curtis-Reiner [1]). Since $\mathrm{cl}(\mathbf{GL}_n) = 1$ over $\mathbb{Q}$ according to Proposition 8.1, Theorem 8.2 implies

PROPOSITION 8.5. *Let $\varrho\colon \Gamma \to GL_n(\mathbb{Z})$ be an integral representation of a finitely generated group Γ, and let C be the centralizer of ϱ (= the centralizer of $\varrho(\Gamma)$). Then the number of classes in the genus of ϱ is finite and equals* $\mathrm{cl}(C)$.

Following Platonov [2], we shall use this fact to obtain a precise estimate for the number of classes in the genus of an integral representation (cf. §8.5), improving the estimate obtained by Roĭiter [1] using a technique from the theory of modules.

EXAMPLE 3 (CONJUGACY OF INTEGRAL MATRICES): Let G be a connected algebraic subgroup of $\mathbf{GL}_n$ defined over $\mathbb{Q}$. Consider the adjoint action

$$x(y) = xyx^{-1}, \quad x, y \in G.$$

The genus of an element g in $G_{\mathbb{Z}}$, which in the case under consideration is usually denoted as $[g]_G$, is the set of the elements of $G_{\mathbb{Z}}$ which are conjugate to g over $G_{\mathbb{Q}}$ and $G_{\mathbb{Z}_p}$, for all primes p; the class of g is its conjugacy class in $G_{\mathbb{Z}}$. Applying Theorem 8.2, we obtain the following assertion concerning $f_G(g)$.

PROPOSITION 8.6 (CENTRALIZER THEOREM, PLATONOV [8]). *The number of classes $f_G(g)$ in the genus of an element g in $G_{\mathbb{Z}}$ is finite, and is the number of double cosets $C_{A(\infty)}xG_{\mathbb{Q}} \subset C_A$ of the centralizer $C = Z_G(g)$ contained in the principal class $G_{A(\infty)}G_{\mathbb{Q}}$. In particular, if* $\mathrm{cl}(G) = 1$, *then* $f_G(g) = \mathrm{cl}(C)$.

In §8.5 we shall use this proposition to solve the genus problem (cf. Rapinchuk [1]).

In conclusion, we wish to point out another interpretation of the class number of an algebraic group, which in a sense is dual to the one discussed above. To do so, let us consider an algebraic K-group G in $\mathbf{GL}_n$ and a lattice M in K^n.

DEFINITION: By the *genus* $\mathrm{gen}(M)$ of M relative to G we mean the set of lattices N in K^n which are locally isomorphic to M relative to G, i.e., those lattices for which there exists g_v in G_{K_v} satisfying $g_v(M_v) = N_v$ for each v in V_f^K. The *class* of M consists of lattices which are isomorphic to M relative to G, i.e., lattices of the form $g(M)$, $g \in G_K$.

PROPOSITION 8.7. *The number of classes in the genus of M relative to G is finite and equals* $\mathrm{cl}(G^M)$.

PROOF: As usual, the proof consists of establishing a one-to-one correspondence between the set Λ of double cosets $G_K g G^M_{A(\infty)}$ in G_A, the number of which equals $\mathrm{cl}(G^M)$, and the set $\mathfrak{g}(M)$ of classes in the genus of M. To do so, consider the action of G_A on the lattices in K^n, induced by embedding G_A in $GL_n(A)$ and the action of $GL_n(A)$ considered above.

We claim that $\mathrm{gen}(M)$ is precisely the orbit $G_A(M)$. Clearly $G_A(M) \subset \mathrm{gen}(M)$. Now let $N \in \mathrm{gen}(M)$. Then for each v in V_f^K there is a g_v in G_{K_v} satisfying $g_v(M_v) = N_v$. Since $M_v = N_v = \mathcal{O}_v^n$ for almost all v, it follows that the element $h = (h_v)$ with components

$$h_v = \begin{cases} 1, & v \in V_\infty^K \\ g_v, & v \in V_f^K \end{cases}$$

is an adele; moreover, by construction $h(M) = N$. Since the stabilizer of M under the given action is $G^M_{A(\infty)}$ and the orbits of G_K are the classes of lattices in the sense defined above, we obtain the desired one-to-one correspondence $\Lambda \simeq \mathfrak{g}(M)$. Proposition 8.7 is proved.

EXAMPLE 4: Let $G = \mathbf{O}_n(f)$, where f is a nondegenerate quadratic form on K^n. Then the genus of M in K^n consists of those lattices N in K^n which are locally isometric to M, i.e., those lattices for which the localizations M_v and N_v are isometric for all v in V_f^K. (In other words, for each v in V_f^K there exists an isometry $\sigma_v \in \mathbf{O}_n(f)_{K_v}$ satisfying $\sigma_v(M_v) = N_v$.) The class of M consists of all lattices isometric to M. Thus, in this case our concepts of the genus and the class of a lattice coincide with the concepts used by O'Meara [1] in the arithmetic theory of quadratic forms. Combining Propositions 8.4 and 8.7, we arrive at the following assertion:

Let f be a nondegenerate quadratic form on K^n with coefficients in $\mathcal{O}$; then the following three numbers are the same:

(1) $c(f)$;
(2) $\mathrm{cl}(\mathbf{O}_n(f))$;
(3) the number of classes in the genus of $L = \mathcal{O}^n$ under the action of $G = \mathbf{O}_n(f)$.

Henceforth, bearing in mind the interpretation of the class number given in Proposition 8.7, we shall call M for which $\mathrm{cl}(G^M) = 1, 2, \ldots$ one-class, two-class, etc., respectively.

8.2. Class numbers and class groups of semisimple groups of noncompact type; the realization theorem.

In this section we shall obtain a complete description of the values taken on by $\mathrm{cl}(\varphi(G))$ for a semisimple K-group G of noncompact type with respect to the various representations φ. (Recall (cf. §4.4) that a semisimple K-group G is said to have noncompact type if it does not have any K-simple components G^i with the compact Archimedean part G^i_∞ of the adele group. An equivalent definition can be given using Theorem 7.12: G has noncompact type if and only if strong approximation holds for its simply connected covering $\tilde{G}$.) For this case it turns out that the values which $\mathrm{cl}(\varphi(G))$ can assume are by no means arbitrary; first we shall obtain the relevant constraints on the class number, and then we shall show that all values that are possible *a priori* are actually realized as $\mathrm{cl}(\varphi(G))$.

Let G be a semisimple K-group of noncompact type. Consider the universal K-covering $\pi\colon \tilde{G} \to G$ and the corresponding exact sequence of K-groups

$$1 \to F \to \tilde{G} \to G \to 1, \tag{8.8}$$

where $F = \ker \pi$ is the fundamental group of G. For any extension M/K we take the segment of the exact cohomological sequence

$$\tilde{G}_M \xrightarrow{\pi_M} G_M \xrightarrow{\psi_M} H^1(M, F),$$

where ψ_M is the coboundary morphism (cf. §1.3). Putting $M = K_v$ (where $v \in V^K$) and then passing to the direct product, we obtain the exact sequence

$$\prod_v \tilde{G}_{K_v} \xrightarrow{\Pi} \prod_v G_{K_v} \xrightarrow{\Psi} \prod_v H^1(K_v, F), \tag{8.9}$$

where $\Pi = \prod_v \pi_{K_v}$ and $\Psi = \prod_v \psi_{K_v}$. Let π_A and ψ_A denote the restrictions of Π and Ψ to the adele groups $\tilde{G}_A$ and G_A, respectively.

PROPOSITION 8.8. *Let G be a semisimple K-group of noncompact type. Then the principal class $G_{A(\infty)}G_K$ is a normal subgroup of G_A containing the commutator group $[G_A, G_A]$, and $\mathrm{cl}(G)$ is the order of the finite abelian group $\mathcyr{Cl}(G) = G_A/G_{A(\infty)}G_K$. Also*

$$\mathcyr{Cl}(G) \simeq \psi_A(G_A)/\psi_A(G_{A(\infty)}G_K); \tag{8.10}$$

in particular,

$$\mathrm{cl}(G) = [\psi_A(G_A) : \psi_A(G_{A(\infty)}G_K)]. \tag{8.11}$$

PROOF: First we establish that the sequence

$$\tilde{G}_A \xrightarrow{\pi_A} G_A \xrightarrow{\psi_A} \prod_v H^1(K_v, F)$$

is exact. Since (8.9) is exact it suffices to show that

$$(\prod_v \pi_{K_v}(\tilde{G}_{K_v})) \cap G_A = \pi_A(\tilde{G}_A).$$

This is equivalent to having

$$\pi_{K_v}(\tilde{G}_{K_v}) \cap G_{\mathcal{O}_v} = \pi_{K_v}(\tilde{G}_{\mathcal{O}_v}) \tag{8.12}$$

for almost all v in V_f^K. In §6.2 we saw that for almost all v in V_f^K there is an exact sequence

$$1 \to F_{\mathcal{O}_{K_v^{ur}}} \to \tilde{G}_{\mathcal{O}_{K_v^{ur}}} \xrightarrow{\pi} G_{\mathcal{O}_{K_v^{ur}}} \to 1,$$

where $F_{\mathcal{O}_{K_v^{ur}}}$ is F for almost all v in V_f^K. Then for g in $G_{\mathcal{O}_{K_v^{ur}}}$ we have $\pi^{-1}(g) \subset \tilde{G}_{\mathcal{O}_{K_v^{ur}}}$. In particular, if $g = \pi(x) \in G_{\mathcal{O}_v}$, where $x \in \tilde{G}_{K_v}$, then $x \in \tilde{G}_{\mathcal{O}_{K_v^{ur}}} \cap \tilde{G}_{K_v} = \tilde{G}_{\mathcal{O}_v}$, from which one obtains (8.12).

Now we note that the strong approximation property for $\tilde{G}$ implies that $\pi_A(\tilde{G}_A) \subset G_{A(\infty)}G_K$; moreover, $\pi_A(\tilde{G}_A) \subset g^{-1}G_{A(\infty)}gG_K$ for any g in G_A. Indeed, $U = \pi_A^{-1}(g^{-1}G_{A(\infty)}g)$ is open in $\tilde{G}_A$ and contains $\tilde{G}_\infty$; therefore, since $\tilde{G}_\infty\tilde{G}_K$ is dense in $\tilde{G}_A$, it follows that $\tilde{G}_A = UG_K$. Consequently,

$$\pi_A(\tilde{G}_A) = \pi_A(U\tilde{G}_K) \subset g^{-1}G_{A(\infty)}gG_K.$$

Since ψ_A is a homomorphism of G_A to an abelian group, we see that

$$[G_A, G_A] \subset \ker \psi_A = \mathrm{Im}\, \pi_A \subset g^{-1}G_{A(\infty)}gG_K, \tag{8.13}$$

for any g in G_A. Now the proof of the proposition is easily completed. For any g_i in $G_{A(\infty)}$ and h_i in G_K $(i = 1, 2)$, and any g in G_A, we have

$$
\begin{aligned}
&(g_1h_1)(g_2h_2) = (g_1g_2)([g_2^{-1}, h_1])h_1h_2 \in G_{A(\infty)}G_K,\\
&(g_1h_1)^{-1} = h_1^{-1}g_1^{-1} = g_1^{-1}[g_1, h_1^{-1}]h_1^{-1} \in G_{A(\infty)}G_K,\\
&g^{-1}g_1h_1g = g_1[g_1^{-1}, g^{-1}][g^{-1}, h_1]h_1 \in G_{A(\infty)}G_K
\end{aligned}
\tag{8.14}
$$

by virtue of $[G_A, G_A] \subset G_{A(\infty)}G_K$ (where $[x, y] = xyx^{-1}y^{-1}$). From (8.14) we see that the class $G_{A(\infty)}G_K$ is a normal subgroup of G_A containing $[G_A, G_A]$. To prove the assertion that the order of the quotient group $\mathcal{G}\mathrm{cl}(G) = G_A/G_{A(\infty)}G_K$ equals the class number, it suffices to establish that the double coset $G_{A(\infty)}xG_K$ coincides with the right coset $xG_{A(\infty)}G_K$, for any x in G_A. By virtue of (8.13), for any g, h in G_A we have

$$
\begin{aligned}
(gh)^{-1}G_{A(\infty)}(gh)G_K &\subset g^{-1}G_{A(\infty)}g[g^{-1}G_{A(\infty)}g, h^{-1}]G_K\\
&\subset g^{-1}G_{A(\infty)}g[G_A, G_A]G_K = g^{-1}G_{A(\infty)}gG_K.
\end{aligned}
$$

Setting $g = 1$ and $h = x$, we obtain

$$x^{-1}G_{A(\infty)}xG_K \subset G_{A(\infty)}G_K;$$

and setting $g = x$ and $h = x^{-1}$ we obtain the reverse inclusion, as desired. The proof of the isomorphism (8.10) follows from the standard homomorphism theorem, since $\ker \psi_A \subset G_{A(\infty)}G_K$. This completes the proof of Proposition 8.8.

DEFINITION: $\mathcal{G}\mathrm{cl}(G) = G_A/G_{A(\infty)}G_K$ is called the *class group* of a semisimple algebraic K-group G of noncompact type.

Proposition 8.8 implies

COROLLARY. *Let G be a semisimple K-group of noncompact type, and let f be the exponent of its fundamental group F. Then f is an exponent of $\mathcal{G}\mathrm{cl}(G)$. In particular, $\mathrm{cl}(G)$ always has the form $p_1^{\alpha_1}; \dots p_r^{\alpha_r}$, where $p_1, \dots, p_r$ are the distinct prime divisors of the order of F.*

The aim of this section is to show that all the numbers of the form described can be obtained as $\mathrm{cl}(\varphi(G))$ for a suitable realization φ of G. This is done by

THEOREM 8.3 (REALIZATION THEOREM). *Let G be a semisimple K-group of noncompact type, and suppose the kernel F of the universal covering $\pi\colon \tilde{G} \to G$ has exponent f. Then for any finite abelian group B of exponent f there exists a K-representation φ_B of G such that $\mathcal{G}\mathrm{cl}(\varphi_B(G))$ is isomorphic to B. In particular, one can determine effectively an integer n such that G has a faithful representation of degree n, and such that for any integer of the form $p_1^{\alpha_1} \dots p_r^{\alpha_r}$, where the p_i's are as above, there exists a free lattice $M(\alpha_1, \dots, \alpha_r) \subset K^n$ such that $\mathrm{cl}(G^{M(\alpha_1, \dots, \alpha_r)}) = p_1^{\alpha_1} \dots p_r^{\alpha_r}$.*

PROOF: Theorem 8.3 is proved in several steps, the first of which is the theorem on the existence of a one-class free lattice.

THEOREM 8.4. *Let G be a semisimple K-group of noncompact type and of degree n. Then there exists a free lattice L_0 in K^n such that $\mathrm{cl}(G^{L_0}) = 1$.*

PROOF: We use the following straightforward assertion, which allows us to choose a special set of representatives of double cosets.

LEMMA 8.2. *Let H be an algebraic K-group having weak approximation with respect to a finite subset S of V_f^K, and let W be an open subgroup of $H_{A(\infty)}$ of the form $W = H_\infty \times \prod_{v \in V_f^K} W_v$, where W_v is an open subgroup of $H_{\mathcal{O}_v}$ and $W_v = H_{\mathcal{O}_v}$ for almost all v in V_f^K. Then there exists a finite subset $T \subset V_f^K$ disjoint from S, and a finite system of representatives $\{h^i\}_{i=1}^r$ of the double cosets $W \setminus H_A/H_K$ such that the v-component h_v^i is 1 for any $v \notin T$ and any $i = 1, \dots, r$. In particular, $H_A = H_{A(T)}H_K$ for a suitable finite set T containing V_∞^K and disjoint from S.*

PROOF: Clearly W has finite index in $H_{A(\infty)}$; therefore Theorem 8.1 implies that there is a finite system of representatives $\{x^i\}_{i=1}^r$ of $W \setminus H_A/H_K$. Using the weak approximation property, for each $i = 1, \dots, r$ we choose a^i in $H_K \cap \prod_{v \in S} (W_v x_v^i)$ and put $\bar{x}^i = x^i(a^i)^{-1}$ and $y^i = (y_v^i)$, where

$$y_v^i = \begin{cases} 1, & v \notin S,\\ \bar{x}_v^i, & v \in S. \end{cases}$$

Then by assumption $y^i \in W$ for any $i = 1, \dots, r$, so the adele $z^i = (y^i)^{-1}x^i(a^i)^{-1}$ defines the same double coset as x^i. Put

$$T = \{\, v \in V_f^K : z_v^i \notin W_v \text{ for some } i = 1, \dots, r \,\}.$$

Clearly T is a finite subset; and since $z_v^i = 1$ for v in S, we have $T \cap S = \emptyset$. Now clearly for our desired system of representatives $\{h^i\}_{i=1}^r$ we can take the adeles z^i "truncated" at T, i.e., we can put $h^i = (h_v^i)$, where

$$h_v^i = \begin{cases} 1, & v \notin T,\\ z_v^i, & v \in T. \end{cases} \tag{8.15}$$

It remains to note that the system $\{h^i\}_{i=1}^r$ we have just constructed contains representatives of all the double cosets $H_{A(\infty)} \setminus H_A/H_K$; so

$$H_A = \bigcup_{i=1}^r H_{A(\infty)}h^iH_K = H_{A(T \cup V_\infty^K)}H_K,$$

since $h^i \in H_{A(T \cup V_\infty^K)}$ by virtue of (8.15). The lemma is proved.

By Theorem 7.7 there is a finite subset S_0 of V_∞^K such that, for any finite S in V^K disjoint from S_0, G has the weak approximation property with respect to S.

Applying Lemma 8.2 to the one-dimensional torus $H = \mathbb{G}_m$, we establish the existence of a finite subset S of V^K containing V_∞^K and disjoint from S_0, such that $J_K = J_K^S K^*$, where J_K^S is the group of S-integral ideles. Now let us fix a lattice L in K^n and let W denote the subgroup of $G_{A(\infty)}^L$ of the form

$$W = G_\infty \times \prod_{v \in V_f^K \setminus S} G_{\mathcal{O}_v}^{L_v} \times \prod_{v \in S_f} (G_{\mathcal{O}_v}^{L_v} \cap \pi_{K_v}(\tilde{G}_{K_v})),$$

where $S_f = S \setminus V_\infty^K$. Applying Lemma 8.2 again, this time to $H = G$ and to the set S_f (noting that by assumption G has weak approximation with respect to S), we obtain a system of representatives $\{g^i\}_{i=1}^l$ of $W \backslash G_A / G_K$, such that, for some finite $T \subset V_f^K$ disjoint from S, the v-component g_v^i is 1 for each $v \notin T$ and all $i = 1, \ldots, l$.

The desired L_0 is constructed by modifying the v-component of the original L, for v in $S \cup T$. For v in T, the necessary local components are obtained from the following assertion.

LEMMA 8.3. *There exists a lattice N_v in K_v^n such that*

$$G_{K_v} = G_{\mathcal{O}_v}^{N_v} \pi_{K_v}(\tilde{G}_{K_v}).$$

Indeed, by Proposition 3.18 there exists a maximal compact subgroup B of G_{K_v} such that $G_{K_v} = B \cdot \pi_{K_v}(\tilde{G}_{K_v})$. On the other hand, by Proposition 1.12, there is a lattice N_v in K_v^n satisfying $G_{\mathcal{O}_v}^{N_v} = B$.

The condition $J_K = J_K^S K^*$ and Proposition 8.2 imply the existence of lattices M_v in K_v^n, for v in S_f, such that the lattice L_0 having local components

$$(L_0)_v = \begin{cases} L_v, & v \notin S \cup T, \\ N_v, & v \in T, \\ M_v, & v \in S \end{cases}$$

is free; and it remains to show that $\mathrm{cl}(G^{L_0}) = 1$.

Let $g \in G_A$. Then there exist h in W, t in G_K, and i, $1 \le i \le l$, such that $g = hg^i t$. For v in T take the factorization

$$h_v g_v^i = b_v s_v,$$

where $b_v \in G_{\mathcal{O}_v}^{N_v}$ and $s_v \in \pi_{K_v}(\tilde{G}_{K_v})$, and introduce adeles x and y with components

$$x_v = \begin{cases} h_v, & v \notin S \cup T, \\ b_v, & v \in T, \\ 1, & v \in S, \end{cases} \qquad y_v = \begin{cases} 1, & v \notin S \cup T, \\ s_v, & v \in T, \\ h_v, & v \in S. \end{cases}$$

Then, since $g_v^i = 1$ for $v \notin T$, we have $hg^i = xy$; moreover, by assumption $x \in G_{A(\infty)}^{L_0}$ and $y \in \pi_A(\tilde{G}_A)$. Since G has noncompact type, $\pi_A(\tilde{G}_A) \subset G_{A(\infty)}^{L_0} G_K$; consequently $g = hg^i t = xyt \in G_{A(\infty)}^{L_0} G_K$, as desired. Q.E.D.

If we do not require that the one-class lattice constructed be free, then the proof of its existence becomes quite short and its main argument—the application of Proposition 3.18—stands out clearly. The proof of the latter proposition is based on the conjugacy of the Sylow pro-p-subgroups of $\pi_{K_v}(\tilde{G}_{K_v})$; thus it is an excellent example of applying abstract group-theoretic arguments to the study of subtle arithmetic questions. In this regard, it should be noted that much more preliminary work is required to prove Theorem 8.4 for the orthogonal group of an indefinite quadratic form in the context of lattice theory (cf. O'Meara [1]). We also wish to call the reader's attention to the fact that Theorem 8.4 evidently treats what is probably the most general case, in which the existence of one-class lattices is the rule, not the exception. Platonov-Bondarenko-Rapinchuk [1, §4] presented the examples of tori and semisimple groups of compact type which do not have a one-class realization in any space.

In this connection, we note the following curious fact, which shows that the existence of a one-class realization is determined by the intrinsic properties of the group itself and is independent of the choice of a faithful representation.

PROPOSITION 8.9. *Let $G \subset \mathbf{GL}_n$ be an arbitrary algebraic K-group of degree n. Assume there exists a lattice L in K^n such that $\mathrm{cl}(G^L) = 1$. Then, for any faithful K-representation $\varphi: G \to \mathbf{GL}_r$, there also exists a lattice $L(\varphi)$ in K^r such that $\mathrm{cl}(G^{L(\varphi)}) = 1$.*

PROOF: Let S denote a finite subset of V_f^K, such that the morphism φ is defined over $\mathcal{O}_v$ and $L_v = \mathcal{O}_v^n$ for all v in $V_f^K \setminus S$. The group $\varphi(G_{\mathcal{O}_v}^{L_v})$ is compact, for each v in S; therefore there exists a lattice M_v in K_v^r such that $\varphi(G_{\mathcal{O}_v}^{L_v}) \subset \varphi(G)_{\mathcal{O}_v}^{M_v}$. Let us define the localizations of the desired lattice $L(\varphi)$ as follows:

$$L(\varphi)_v = \begin{cases} \mathcal{O}_v^r, & v \notin S, \\ M_v, & v \in S. \end{cases}$$

Then it follows from our assumptions that $\varphi(G^L_{A(\infty)}) \subset \varphi(G)^{L(\varphi)}_{A(\infty)}$, and therefore $\varphi(G)_A = \varphi(G_A) = \varphi(G^L_{A(\infty)}G_K) \subset \varphi(G)^{L(\varphi)}_{A(\infty)}\varphi(G)_K$, in other words, $\mathrm{cl}(\varphi(G)^{L(\varphi)}) = 1$. The proposition is proved.

Now we return to the proof of Theorem 8.3. The desired lattices are constructed by starting with a special one-class lattice L, and modifying its v-components for v from a finite subset S of V_f^K in such a manner that the corresponding integral adele group becomes smaller. In this situation one can refine the isomorphism in (8.10).

PROPOSITION 8.10. *Let G be a semisimple K-group of noncompact type and of degree n, and let L be a lattice in K^n satisfying $\mathrm{cl}(G^L) = 1$. Assume that N is another lattice in K^n satisfying the following conditions:*

(1) $\psi_A(G^N_{A(\infty)}) \subset \psi_A(G^L_{A(\infty)})$;

(2) $N_v = L_v$ *for all v in $V_f^K \setminus S$, where S is a (fixed) finite subset of V_f^K.*

For any subset T of V_f^K, let $\delta_T\colon H^1(K,F) \to \prod\limits_{v\in T} H^1(K_v,F)$ be induced by the restriction maps, and let $\delta = \delta_{V^K}$. Then

$$\mathcal{G}\mathrm{cl}(G^N) \simeq \prod_{v\in S} \psi_{K_v}(G^{L_v}_{\mathcal{O}_v})/\delta_S(\psi_K(G^L_{\mathcal{O}})) \prod_{v\in S} \psi_{K_v}(G^{N_v}_{\mathcal{O}_v}). \tag{8.16}$$

Moreover, $\delta_S(\psi_K(G^L_{\mathcal{O}}))$ is the image of $\delta(\psi_K(G^L_{\mathcal{O}}))$ under the projection map $p_S\colon \prod\limits_v H^1(K_v,F) \to \prod\limits_{v\in S} H^1(K_v,F)$; and the latter group is finite and is given by the equality

$$\delta(\psi_K(G^L_{\mathcal{O}})) = \psi_A(G^L_{A(\infty)}) \cap \delta(\psi_K(G_K)).$$

PROOF: $\psi_A(G_A) = \psi_A(G^L_{A(\infty)}G_K)$, since $\mathrm{cl}(G^L) = 1$. Therefore, by (8.10) we have

$$\mathcal{G}\mathrm{cl}(G^N) \simeq \psi_A(G^L_{A(\infty)}G_K)/\psi_A(G^N_{A(\infty)}G_K). \tag{8.17}$$

In this case, applying the standard isomorphism $AB/CB \simeq A/(A\cap B)C$, which holds for any subgroups A, B, and C of a certain abelian group such that $C \subset A$, we obtain

$$\mathcal{G}\mathrm{cl}(G^N) \simeq \psi_A(G^L_{A(\infty)})/(\psi_A(G^L_{A(\infty)}) \cap \psi_A(G_K))\psi_A(G^N_{A(\infty)}).$$

Now, applying p_S and the fundamental theorem of homomorphisms, and bearing in mind that the kernel of the restriction of p_S to $\psi_A(G^L_{A(\infty)})$ lies in $\psi_A(G^N_{A(\infty)})$, we obtain the isomorphism

$$\mathcal{G}\mathrm{cl}(G^N) \simeq \prod_{v\in S} \psi_{K_v}(G^{L_v}_{\mathcal{O}_v})/\Gamma \prod_{v\in S} \psi_{K_v}(G^{N_v}_{\mathcal{O}_v}),$$

where Γ denotes the image under p_S of $\psi_A(G^L_{A(\infty)}) \cap \psi_A(G_K)$. Bearing in mind that $\psi_A(G_K) = \delta(\psi_K(G_K))$ and $\delta_S(\psi_K(G^L_{\mathcal{O}})) = p_S(\delta(\psi_K(G^L_{\mathcal{O}})))$, we see that it suffices to establish

$$\psi_A(G^L_{A(\infty)}) \cap \psi_A(G_K) = \psi_A(G^L_{\mathcal{O}}).$$

Let $x = \psi_A(g) = \psi_A(h)$, where $g \in G^L_{A(\infty)}$ and $h \in G_K$. Then $\psi_A(gh^{-1}) = 1$, and hence $y = gh^{-1} \in \ker\psi_A = \mathrm{Im}\,\pi_A$ (cf. proof of Proposition 8.8). The strong approximation property for $\tilde{G}$ implies

$$\pi_A(\tilde{G}_A) = (\pi_A(\tilde{G}_A) \cap G^L_{A(\infty)})\pi_A(\tilde{G}_K),$$

so $y = gh^{-1} = st$ for some s in $\pi_A(\tilde{G}_A) \cap G^L_{A(\infty)}$ and t in $\pi_A(\tilde{G}_K)$. We have

$$s^{-1}g = th \in G^L_{A(\infty)} \cap G_K = G^L_{\mathcal{O}};$$

hence $x = \psi_A(h) = \psi_A(th) \in \psi_A(G^L_{\mathcal{O}})$, as desired.

It remains to observe that $G^L_{\mathcal{O}}$ is finitely generated, by Theorem 4.17; therefore $\psi_K(G^L_{\mathcal{O}})$ is a finitely generated abelian group of finite exponent, and hence is itself finite. Proposition 8.10 is proved.

Now we have all the results necessary to prove Theorem 8.3. However, we shall provide a full proof only for the important case where the fundamental group F is cyclic. In this situation one can give an explicit description of the realizations obtained, and this is significant for arithmetic applications (cf. Theorem 8.6 and Proposition 8.13). Moreover, this case involves basic technical difficulties, and the general case can actually be reduced to this case (cf. Platonov-Bondarenko-Rapinchuk [3]).

THEOREM 8.5. *Let G be a semisimple K-group of noncompact type with a cyclic fundamental group F of order $f = p_1^{\alpha_1}\dots p_s^{\alpha_s}$. Assume that there exists a faithful K-representation $\varrho\colon G \to \mathbf{GL}_r$ and a finite extension P/K such that, for almost all v in V_f^K for which $P \subset K_v$, there is a lattice R_v in K_v^r satisfying $\psi_{K_v}(G^{R_v}_{\mathcal{O}_v}) = 1$. Then for any finite abelian group B of exponent f there is a free lattice $L(B)$ in K^r such that $\mathcal{G}\mathrm{cl}(G^{L(B)}) \simeq B$. In particular, for any integer of the form $p_1^{\beta_1}\dots p_s^{\beta_s}$ there is a free lattice $L(\beta_1,\dots,\beta_s)$ in K^r with $\mathrm{cl}(G^{L(\beta_1,\dots,\beta_s)}) = p_1^{\beta_1}\dots p_s^{\beta_s}$. If G has degree n as a linear group, then for ϱ one can always take the representation of degree $2n$, given by $\varrho(g) = \begin{pmatrix} g & 0 \\ 0 & E_n \end{pmatrix}$.*

PROOF: Enlarging P, we may, and shall, assume henceforth that P is a Galois extension of K, containing the Hilbert class field $\tilde{K}$, and such

that $F = F_P$. Let us fix a one-class lattice L in K^r and take a factorization $B = \prod_{i=1}^{l} B_i$ of B into the product of cyclic factors. Let S_1 denote the set of those v in V_f^K for which $\psi_{K_v}(G_{\mathcal{O}_v}^{L_v}) \neq H^1(K_v^{ur}/K_v, F)$. Note that Proposition 6.4 implies that S_1 is finite. Also, let S_2 be a finite subset of V_f^K such that, for any finite S disjoint from S_2, the map $\delta_S: H^1(K, F) \to \prod_{v \in S} H^1(K_v, F)$ is surjective (cf. Proposition 7.8, Corollary 2). By the Chebotarev density theorem one can choose l valuations $\bar{v}_1, \ldots, \bar{v}_l$ in $V_f^K \setminus (S_1 \cup S_2)$ with the property that $P \subset K_{\bar{v}_i}$ for $i = 1, \ldots, l$. Put $\bar{S} = \{\bar{v}_1, \ldots, \bar{v}_l\}$. Then we have

LEMMA 8.4. *There exists a free one-class lattice M in K^r such that*

$$\delta_{\bar{S}}(\psi_K(G_{\mathcal{O}}^M)) = \prod_{i=1}^{l} H^1(K_{\bar{v}_i}^{ur}/K_{\bar{v}_i}, F). \tag{8.18}$$

PROOF: Using Lemma 8.2, we choose a finite subset S of V^K containing V_∞^K and disjoint from $S_2 \cup \bar{S}$, such that $J_K = J_K^S K^*$. By our assumptions and Proposition 7.10, it follows that G has weak approximation with respect to $T = S \cup \bar{S}$. Consider two open subgroups of G_T:

$$W_1 = G_\infty \times \prod_{v \in T \setminus V_\infty^K} G_{\mathcal{O}_v},$$

$$W_2 = \prod_{v \in T} \pi_{K_v}(\tilde{G}_{K_v}).$$

The weak approximation property implies that $W_1 = (G_K \cap W_1)(W_1 \cap W_2)$ in the sense of the diagonal embedding of G_K in G_T; hence

$$\delta_T(\psi_K(G_K \cap W_1)) = \psi_T(W_1),$$

where $\psi_T = \prod_{v \in T} \psi_{K_v}$. Since all the cohomology groups $H^1(K_v, F)$ are finite (Theorem 6.14), $\psi_T(W_1)$ is also finite; and therefore there exists a finitely generated subgroup $\Gamma \subset G_K \cap W_1$ such that

$$\delta_T(\psi_K(\Gamma)) = \psi_T(W_1). \tag{8.19}$$

Clearly $\Gamma \subset G^L_{\mathcal{O}(V \cup V_\infty^K)}$ for some finite subset V of V_f^K disjoint from T. Now we define the desired M in K^r by means of its localizations, as follows:

$$M_v = \begin{cases} L_v, & v \notin V \cup S, \\ N_v, & v \in V, \\ J_v, & v \in S, \end{cases} \tag{8.20}$$

where N_v is the lattice from Lemma 8.3, and the components J_v are selected in such a way as to ensure that M be free (cf. Proposition 8.3).

We shall show that $\mathrm{cl}(G^M) = 1$. Since L is a one-class lattice, we obtain $\psi_A(G_A) = \psi_A(G^L_{A(\infty)} G_K)$; and therefore, by Proposition 8.8, it suffices to establish that $\psi_A(G^L_{A(\infty)}) \subset \psi_A(G^M_{A(\infty)} G_K)$. Since

$$M_v = L_v \quad \text{for } v \notin V \cup S \quad \text{and}$$
$$\psi_{K_v}(G_{\mathcal{O}_v}^{L_v}) \subset \psi_{K_v}(G_{\mathcal{O}_v}^{M_v}) = \psi_{K_v}(G_{K_v}) \quad \text{for each } v \text{ in } V,$$

we need only prove that

$$\Phi \subset \psi_A(G^M_{A(\infty)} G_K),$$

where Φ is $\prod_{v \in S} \psi_{K_v}(G_{\mathcal{O}_v}^{L_v})$ naturally embedded in $\psi_A(G_A)$. It follows from (8.19) that for any x in Φ there exists γ in Γ satisfying $\delta_S(\psi_K(\gamma)) = x$. Then, analysis of the local components and (8.20) easily yield that $x\psi_A(\gamma^{-1}) \in \psi_A(G^M_{A(\infty)})$, and hence

$$x = x(\psi_A(\gamma^{-1}))\psi_A(\gamma) \in \psi_A(G^M_{A(\infty)} G_K),$$

as desired.

According to Proposition 8.10, in order to compute $\delta_{\bar{S}}(\psi_K(G_{\mathcal{O}}^M))$ one has to take the image under the projection $p_{\bar{S}}$ of $\psi_A(G_{\mathcal{O}}^M) = \psi_A(G_K) \cap \psi_A(G^M_{A(\infty)})$. Denote the kernel of the restriction of δ_S to $\psi_K(\Gamma)$ by Δ; it follows from (8.19) that

$$\delta_{\bar{S}}(\Delta) = \prod_{v \in \bar{S}} \psi_{K_v}(G_{\mathcal{O}_v}^{L_v}) = \prod_{v \in \bar{S}} H^1(K_v^{ur}/K_v, F).$$

However, using (8.20), we obtain that $\delta(\Delta) \subset \psi_A(G_K) \cap \psi_A(G^M_{A(\infty)})$; hence $\delta_{\bar{S}}(\psi_K(G_{\mathcal{O}}^M)) \supset \prod_{v \in \bar{S}} H^1(K_v^{ur}/K_v, F)$. The reverse inclusion is obvious, since $G_{\mathcal{O}}^M \subset G_{\mathcal{O}_v}^{M_v} = G_{\mathcal{O}_v}^{L_v}$ for all v in $\bar{S}$. Lemma 8.4 is proved.

Note that thus far we have not used the fact that F is cyclic; therefore all our constructions and results also hold in general.

Now we continue with the proof of Theorem 8.5. Since $F = F_P$, we have $H^1(P, F) = \mathrm{Hom}(\mathrm{Gal}(\bar{P}/P), F)$; and we can consider the map

$$\theta: H^1(K, F) \to H^1(P, F) = \mathrm{Hom}(\mathrm{Gal}(\bar{P}/P), F).$$

Let H denote the intersection of the kernels of all homomorphisms $\chi \in \theta(\psi_K(G_{\mathcal{O}}^M))$. Since $E = \psi_K(G_{\mathcal{O}}^M)$ is finite (Proposition 8.10), H is a closed normal subgroup of $\mathrm{Gal}(\bar{P}/P)$ of finite index. We claim that H is actually a normal subgroup of $\mathrm{Gal}(\bar{K}/K)$. Indeed, if $\chi \in \theta(\psi_K(G_{\mathcal{O}}^M))$, $h \in \ker\chi$ and $g \in \mathrm{Gal}(\bar{K}/K)$, then

$$\chi(g^{-1}hg) = \chi(g^{-1})g^{-1}(\chi(hg)) = \chi(g^{-1})g^{-1}(\chi(h)h\chi(g))$$
$$= \chi(g^{-1})g^{-1}(\chi(g)) = \chi(gg^{-1}) = 1,$$

since χ is a cocycle on all $\mathrm{Gal}(\bar{K}/K)$ and h, as an element of $\mathrm{Gal}(\bar{P}/P)$, acts trivially on F. Let C denote the finite Galois extension of K corresponding to H. (It can be characterized as the smallest Galois extension of K containing P and satisfying $E \subset H^1(C/K, F)$. Then the homomorphism

$$\delta_{\bar{S}}: E \to \prod_{i=1}^{l} H^1(K_{\bar{v}_i}, F)$$

factors through $H^1(C/K, F)$. Now it follows from (8.18) that all the extensions $C_{\bar{v}_i}/K_{\bar{v}_i}$ $(i = 1, \dots, l)$ are unramified. Moreover, by assumption $F = F_P$ and $P \subset K_{\bar{v}_i}$; hence

$$H^1(K_{\bar{v}_i}^{ur}/K_{\bar{v}_i}, F) = \mathrm{Hom}(\hat{\mathbb{Z}}, F) \simeq F,$$

and the composition

$$\alpha: H^1(C/K, F) \to \prod_{i=1}^{l} H^1(C_{\bar{v}_i}K_{\bar{v}_i}, F) \to \prod_{i=1}^{l} H^1(K_{\bar{v}_i}^{ur}/K_{\bar{v}_i}, F) \simeq F^l$$

is given by

$$\chi \xrightarrow{\alpha} (\chi(\sigma_1), \dots, \chi(\sigma_l)),$$

where σ_i is the Frobenius automorphism of $C_{\bar{v}_i}/K_{\bar{v}_i}$, viewed as an element of $\mathrm{Gal}(C/K)$ (cf. §1.1). By the Chebotarev density theorem, outside any given finite set of valuations one can find $v_1, \dots, v_l$ in V_f^K such that C_{v_i}/K_{v_i} is unramified and the Frobenius automorphism $\mathrm{Fr}(C_{v_i}/K_{v_i})$ is $\tau_i = \sigma_i^{f/|B_i|}$ for $i = 1, \dots, l$ (note that $|B_i|$ divides f, since by assumption the exponent of B is f). In particular, we may assume that $\psi_{K_{v_i}}(G_{\mathcal{O}_{v_i}}^{M_{v_i}}) = H^1(K_{v_i}^{ur}/K_{v_i}, F)$ for each i, and there is a lattice R_{v_i} in $K_{v_i}^r$ with the property indicated in Theorem 8.5. (Note that by assumption $P \subset K_{\bar{v}_i}$, and therefore the restriction of σ_i to P is trivial; consequently, the restriction of τ_i to P is also trivial, and hence $P \subset K_{v_i}$.) Let us define the lattice $L(B)$ as follows:

$$L(B)_v = \begin{cases} M_v, & v \notin \{v_1, \dots, v_l\}, \\ R_v, & v \in \{v_1, \dots, v_l\}. \end{cases}$$

Since, for any i, the completion of K_{v_i} contains the Hilbert class field $\tilde{K}$, and since M is free, it follows that $L(B)$ is also free (Proposition 8.3).

LEMMA 8.5. $\mathcal{G}\mathrm{cl}(G^{L(B)}) \simeq B$.

PROOF: We use Proposition 8.10. In our case, the isomorphism (8.16) established in the proposition assumes the form

$$\mathcal{G}\mathrm{cl}(G^{L(B)}) \simeq \prod_{i=1}^{l} \psi_{K_{v_i}}(G_{\mathcal{O}_{v_i}}^{M_{v_i}})/\delta_S(E),$$

where $S = \{v_1, \dots, v_l\}$. (Recall that by assumption $\psi_{K_{v_i}}(G_{\mathcal{O}_{v_i}}^{R_{v_i}}) = 1$.) By definition $\psi_{K_{v_i}}(G_{\mathcal{O}_{v_i}}^{M_{v_i}}) = H^1(K_{v_i}^{ur}/K_{v_i}, F)$, the homomorphism $\delta_S: E \to \prod_{i=1}^{l} H^1(K_{v_i}, F)$ factors through $H^1(C/K, F)$, and the composition

$$\beta: H^1(C/K, F) \to \prod_{i=1}^{l} H^1(K_{v_i}^{ur}/K_{v_i}, F) \simeq F^l$$

is given by

$$\chi \xmapsto{\beta} (\chi(\tau_1), \dots, \chi(\tau_l)).$$

Since $\alpha(E) = F^l$ and $\tau_i = \sigma_i^{f/|B_i|}$, we have

$$\delta_S(E) = \beta(E) = \langle h^{f/|B_1|} \rangle \times \cdots \times \langle h^{f/|B_l|} \rangle,$$

where h is a generator of F (observe that σ_i acts trivially on F and hence the restriction of χ to $\langle \sigma_i \rangle$ is a homomorphism). It follows that $\mathcal{G}\mathrm{cl}(G^{L(B)}) \simeq \prod_{i=1}^{l} B_i = B$, as desired.

The assertion that on lattices L in K^r all numbers of the form $m = p_1^{\beta_1} \dots p_s^{\beta_s}$ are realized as class numbers follows from the fact that any finite abelian group with exponent f is realizable as a class group and from the remark that one can always find a group of order m and exponent f. Thus, it remains to show that if G is a linear group of degree n, then for dimension $r = 2n$ there exists a lattice R_v in K_v^r satisfying $\psi_{K_v}(G_{\mathcal{O}_v}^{R_v}) = 1$, for almost all v in V_f^K. To do so, we need

PROPOSITION 8.11. *Let $H = \mathbf{GL}_n$ and let $\varphi: H \to \mathbf{GL}_{2n}$ be the representation given by*

$$\varphi: g \mapsto \begin{bmatrix} g & 0 \\ 0 & E_n \end{bmatrix}.$$

Then, for any non-Archimedean v in V_f^K and any integer $t > 0$, there exists a lattice $L_v(t)$ in K_v^{2n} such that $H_{\mathcal{O}_v}^{L_v(t)} = \varphi(GL_n(\mathcal{O}_v, \mathfrak{p}_v^t))$.

The proof is analogous to that of Proposition 4.3.

Thus, if G is a linear group of degree n, then for any v in V_f^K there is always a lattice L_v in K_v^{2n} for which $G_{\mathcal{O}_v}^{L_v} = G_{\mathcal{O}_v}(\mathfrak{p}_v)$. Therefore, the proof of Theorem 8.5 is completed by the following

LEMMA 8.6. *If $v(|F|) = 0$, then $\psi_{K_v}(G_{\mathcal{O}_v}(\mathfrak{p}_v)) = 1$.*

PROOF: The kernel of the homomorphism $\psi_{K_v}: G_{K_v} \to H^1(K_v, F)$ is an open subgroup $\pi_{K_v}(\tilde{G}_{K_v})$. Therefore ψ_{K_v} is continuous if $H^1(K_v, F)$ is endowed with the discrete topology. It follows that $\Gamma = \psi_{K_v}(G_{\mathcal{O}_v}(\mathfrak{p}_v))$ is a discrete pro-p-group, i.e., a finite p-group. However, $\Gamma \subset H^1(K_v, F)$, and the latter group has exponent $f = |F|$. Thus $(p, f) = 1$, since $v(f) = 0$; hence $\Gamma = \{1\}$, as desired. Q.E.D.

Theorem 8.5 guarantees that all the class numbers that are possible *a priori*, for a semisimple K-group G of noncompact type and of degree n with cyclic fundamental group F, are realized for suitable lattices in K^{2n}. However, in some cases the desired lattices can be constructed in dimension n; this leads to interesting arithmetic applications of the realization theorem, one of which follows now. Recall that to say a quadratic form f is indefinite over K means that there exists a valuation v in V_∞^K such that f represents zero in K_v^n.

THEOREM 8.6 (KNESER [1]). *Let f be an indefinite quadratic form in $n \geq 3$ variables over the ring of integers $\mathcal{O}$ of an algebraic number field K. Then $c(f)$, the number of classes in the genus of f, has the form 2^d, where d is an integer ≥ 0. Conversely, for any integer $d \geq 0$, there is a quadratic form f_d which is K-equivalent to f, such that $c(f_d) = 2^d$.*

Note that f being indefinite over K is equivalent to $H = \mathbf{SO}_n(f)$ being K_v-isotropic (Proposition 2.14), and hence to $\mathbf{SO}_n(f)_{K_v}$ being noncompact. From this one easily obtains that, for $n \geq 3$, f is indefinite if and only if H has noncompact type. Furthermore, in view of Proposition 8.4, one can restate Theorem 8.6 as follows: under the assumptions of the theorem, with $G = \mathbf{O}_n(f)$, for any lattice L in K^n the class number $\mathrm{cl}(G^L)$ has the form 2^d; and for any integer $d \geq 0$ there is a free lattice $L(d)$ for which $\mathrm{cl}(G^{L(d)}) = 2^d$. Unfortunately, G is not connected, so Theorem 8.5 cannot be applied directly. Therefore, we shall prove the analogous assertion for $H = \mathbf{SO}_n(f)$. The case of $G = \mathbf{O}_n(f)$ is handled in a similar way, using the fact that the universal covering $\pi: \tilde{H} \to H$ of H extends to a covering of G, i.e., that there exists a group $\tilde{G}$ and a morphism $\varphi: \tilde{G} \to G$ for which

the following diagram is commutative and has exact rows:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & F & \longrightarrow & \tilde{H} & \xrightarrow{\pi} & H & \longrightarrow & 1 \\ & & \| & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & F & \longrightarrow & \tilde{G} & \xrightarrow{\varphi} & G & \longrightarrow & 1 \end{array} \tag{8.21}$$

We leave it to the reader to work out the details of the argument (cf. below).

Let us examine the class numbers of H. Since the universal covering of H in the given case has the form $\pi: \tilde{H} = \mathbf{Spin}_n(f) \to \mathbf{SO}_n(f) = H$, which means that $F = \{\pm 1\}$, it follows that $\mathrm{cl}(H)$ always has the form 2^d (corollary to Proposition 8.8). To obtain all powers of two as class numbers, we use the following construction of lattices in a quadratic space.

PROPOSITION 8.12. *Let $f = f_1 x_1^2 + \cdots + f_n x_n^2$, with respect to a base $e = (e_1, \ldots, e_n)$ of K^n. For v in V_f^K, let M_v denote the $\mathcal{O}_v$-lattice with the base $e_1, \pi_v e_2, \ldots, \pi_v^{n-1} e_n$, where π_v is a uniformizing parameter. If $v(f_i) = 0$ for all $i = 1, \ldots, n$, then*

$$G_{\mathcal{O}_v}^{M_v} = \Gamma B,$$

where

$$\Gamma = \Gamma(e) = \{\, x \in G : x(e_i) = \pm e_i,\ i = 1, \ldots, n \,\},$$
$$B = \{\, x = (x_{ij}) \in G_{\mathcal{O}_v}(\mathfrak{p}_v) : x_{ij} \in \mathfrak{p}_v^{|i-j|},\ i, j = 1, \ldots, n \,\}.$$

(The matrix notation refers to the basis e.) If in addition $v(2) = 0$, then $H_{\mathcal{O}_v}^{M_v} = (\Gamma \cap H)(B \cap H)$.

PROOF: Let $x \in G_{\mathcal{O}_v}^{M_v}$ and $x = (x_{ij})$ with respect to the basis $e_1, \ldots, e_n$. Then

$$x(\pi_v^{j-1} e_j) = \sum_{i=1}^{n} \pi_v^{j-i} x_{ij} (\pi_v^{i-1} e_i) \tag{8.22}$$

for all $j = 1, \ldots, n$. Therefore $x_{ij} \in \mathfrak{p}_v^{i-j}$ for $i \geq j$. But $x \in G$, i.e., ${}^t x F x = F$, where $F = \mathrm{diag}(f_1, \ldots, f_n)$ is the matrix of f. This gives us the matrix relation

$${}^t x = F x^{-1} F^{-1},$$

which means that $x_{ij} = f_i f_j^{-1} y_{ij}$, where $y = (y_{ij}) = x^{-1}$. Since $y \in G_{\mathcal{O}_v}^{M_v}$ and hence $y_{ij} \in \mathfrak{p}_v^{i-j}$ for $i \geq j$, the condition $v(f_i) = 0$ $(i = 1, \ldots, n)$

implies that $x_{ij} \in \mathfrak{p}_v^{|i-j|}$ for all i, j. Furthermore, again using ${}^t x F x = F$, we obtain that $\sum_{i=1}^n f_i x_{ij}^2 = f_j$ for any $j = 1, \ldots, n$; hence $x_{jj}^2 \equiv 1 \pmod{\mathfrak{p}_v}$, so $x_{jj} \equiv \pm 1 \pmod{\mathfrak{p}_v}$. We have proved $G_{\mathcal{O}_v}^{M_v} \subset \Gamma B$. The inverse inclusion follows from (8.22), which gives the action of x on the base $\{\pi_v^{j-1} e_j\}$.

Now let $x \in H_{\mathcal{O}_v}^{M_v}$ and $x = yz$, where $y \in \Gamma$ and $z \in B$. Then

$$1 = \det x = \det y \det z,$$

where $\det y = \pm 1$ and $\det z \equiv 1 \pmod{\mathfrak{p}_v}$. If $v(2) = 0$, then $-1 \not\equiv 1 \pmod{\mathfrak{p}_v}$, and hence $\det y = 1$, i.e., $y \in \Gamma \cap H$ and $z \in B \cap H$. The proposition is proved.

Now let ψ denote the coboundary map corresponding to the universal covering $\pi\colon \tilde{H} \to H$ of H. Let P be a finite Galois extension of K such that $\psi_K(\Gamma \cap H)$ lies in $H^1(P/K, F)$. If $P \subset K_v$ and $v(2) = v(f_1) = \cdots = v(f_n) = 0$, then for the lattice constructed in Proposition 8.12 we have $\psi_{K_v}(H_{\mathcal{O}_v}^{M_v}) = \psi_{K_v}(\Gamma \cap H)\psi_{K_v}(B \cap H) = 1$ by Lemma 8.6, since $B \cap H \subset H_{\mathcal{O}_v}(\mathfrak{p}_v)$. Thus, the assumptions of Theorem 8.5 are satisfied and therefore, for any integer $d \geq 0$ there is free lattice $L(d)$ in K^n for which $\mathrm{cl}(H^{L(d)}) = 2^d$.

EXERCISE: Let f be a nondegenerate, indefinite quadratic form over K in $n \geq 3$ variables, and let $G = \mathbf{O}_n(f)$ and $H = \mathbf{SO}_n(f)$.

(1) Using the strong approximation theorem for $\tilde{H}$ and the fact that, for any extension L/K, the commutator groups of H_L and G_L are the same (cf. Dieudonné [2]), show that the principal class $G_{A(\infty)}G_K$ is a subgroup of G_A and that $\mathrm{cl}(G)$ is $[G_A : G_{A(\infty)}G_K]$. Also, show that if θ is the coboundary map corresponding to the covering φ in (8.21) (which is none other than the spinor norm), and θ_A is the restriction of $\prod_v \theta_{K_v}$ to G_A, then

$$\mathrm{cl}(G) = [\theta_A(G_A) : \theta_A(G_{A(\infty)}G_K)].$$

(Hint: follow the proof of Proposition 8.8.) It follows that $\mathrm{cl}(G)$ always has the form 2^d.

(2) Prove there exists a form g over K, equivalent to f, with $c(g) = 1$; in other words, that there is L in K^n for which $\mathrm{cl}(G^L) = 1$. To do so, establish that

$$G_A^L = G_{A(\infty)}^L H_A^L$$

for any L in K^n, from which it follows immediately that $\mathrm{cl}(G^L) \leq \mathrm{cl}(H^L)$; then use Theorem 8.4.

(3) Prove Theorem 8.6 by imitating the proof of Theorem 8.5. Note that in this case (and in general, when $|F| = p$) one can omit the step of the proof given by Lemma 8.4, pertaining to the construction of a special one-class lattice, and can begin the subsequent constructions with an arbitrary one-class lattice.

(4) Establish the following relationship between $\mathrm{cl}(G^L)$ and $\mathrm{cl}(H^L)$:

$$\mathrm{cl}(G^L) = \frac{1}{2}\mathrm{cl}(H^L)[G_{\mathcal{O}}^L : H_{\mathcal{O}}^L].$$

It follows that $\mathrm{cl}(G^L)$ is $\mathrm{cl}(H^L)$ or $\frac{1}{2}\mathrm{cl}(H^L)$; moreover, if one has $[G_{\mathcal{O}}^L : H_{\mathcal{O}}^L] = 2$ (in particular, if n is odd), then $\mathrm{cl}(G^L) = \mathrm{cl}(H^L)$. For any $d \geq 0$, construct $L(d)$ in K^n such that $\mathrm{cl}(H^{L(d)}) = 2^d$ and $[G_{\mathcal{O}}^{L(d)} : H_{\mathcal{O}}^{L(d)}] = 2$. In this way, give another proof of Kneser's theorem.

We shall present one more classical example, in which Theorem 8.5 allows one to obtain a complete description of the class numbers that occur: the problem of computing the number of classes in the genus of lattices in the full matrix algebra under conjugation. Two lattices L_1 and L_2 in $M_n(K)$ are said to belong to the same genus if their localizations L_{1v} and L_{2v} are conjugate by a matrix in $GL_n(K_v)$ for all non-Archimedean valuations v of K, and to the same class if they are conjugate by a matrix in $GL_n(K)$. What are the possible values of $c(L)$, the number of classes in the genus of an arbitrary lattice L in $M_n(K)$? An exhaustive answer to this question is given by

PROPOSITION 8.13. *Let $n = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$ be the canonical factorization of n. Then $c(L)$ has the form $p_1^{\beta_1} \ldots p_r^{\beta_r}$, for any L in $M_n(K)$; and conversely, for any $p_1^{\beta_1} \ldots p_r^{\beta_r}$, there is a lattice $L(\beta_1, \ldots, \beta_r)$ in $M_n(K)$ for which $c(L(\beta_1, \ldots, \beta_r)) = p_1^{\beta_1} \ldots p_r^{\beta_r}$.*

PROOF: The action of $\mathbf{GL}_n$ on $W = M_n$ by conjugation induces a faithful representation of $G = \mathbf{PSL}_n$ in $\mathbf{GL}(W) = \mathbf{GL}_{n^2}$. Let $\varphi\colon \mathbf{GL}_n \to G$ denote the morphism of algebraic groups that arises thereby. Since $\ker\varphi \simeq \mathbb{G}_m$, for any extension P/K the exact sequence

$$GL_n(P) \xrightarrow{\varphi} G_P \to H^1(P, \ker\varphi) = 1$$

yields $\varphi(GL_n(P)) = G_P$; in other words, the transformations of G_P are realized by conjugation using matrices from $GL_n(P)$. Applying Proposition 8.7, we now obtain that in the given case $c(L) = \mathrm{cl}(G^L)$ for any L in $M_n(K)$. Thus, the problem of computing $c(L)$ leads to the computation of the class number of the projective group. The universal covering π of G is obtained by restricting φ to $\mathbf{SL}_n$; therefore $\ker\pi$ is a cyclic group of order

n, and one can invoke Theorem 8.5. To apply this theorem one needs a construction of lattices R_v in $M_n(K_v)$ satisfying $\psi_{K_v}(G_{\mathcal{O}_v}^{R_v}) = 1$, where ψ is the coboundary morphism corresponding to π. In view of Lemma 8.6, the desired construction is given by

LEMMA 8.7. *There exists a finite subset S of V_f^K such that, for v in $V_f^K \setminus S$, there is a lattice R_v in W_{K_v} satisfying $G_{\mathcal{O}_v}^{R_v} \subset G_{\mathcal{O}_v}^{L_v}(\mathfrak{p}_v)$, where L is the lattice spanned by the standard base e_{ij} of the matrix algebra.*

PROOF: Consider the quadratic form f on W given by $f(x) = \mathrm{tr}(x^2)$, where tr denotes the trace of a matrix. It is easy to see that the corresponding bilinear form can be written as $b(x, y) = \mathrm{tr}(xy)$, where for $x = (x_{ij})$ we have $b(x, e_{ij}) = x_{ij}$. The latter equation shows that f is nondegenerate.

Let W_0 denote the subspace of W consisting of matrices with trace 0, and let W_1 denote the subspace of scalar matrices. Then clearly W is the orthogonal direct sum of W_0 and W_1. It follows that the restriction f_0 of f to W_0 is also nondegenerate. Let $w_1, w_2, \ldots, w_m$ $(m = n^2 - 1)$ be a base of W_{0K} in which f_0 has the canonical form $f_0 = a_1 x_1^2 + \cdots + a_m x_m^2$, and let w_{m+1} be a nonzero vector of W_{1K}. Let M denote a lattice with base $w_1, w_2, \ldots, w_{m+1}$, and take the exceptional subset S to be $S_1 \cup S_2$, where $S_1 = \{ v \in V_f^K : L_v \neq M_v \}$ and $S_2 = \{ v \in V_f^K : v(a_i) \neq 0 \text{ for some } i = 1, \ldots, m \}$.

Now suppose $v \in V_f^K \setminus S$. Then $L_v = M_v$, so $G_{\mathcal{O}_v}^{L_v} = G_{\mathcal{O}_v}^{M_v}$ and $G_{\mathcal{O}_v}^{L_v}(\mathfrak{p}_v) = G_{\mathcal{O}_v}^{M_v}(\mathfrak{p}_v)$. We show that for the desired R_v we can take the $\mathcal{O}_v$-lattice with the base

$$w_1 + \pi_v^{-m} w_{m+1}, \ldots, \pi_v^{(j-1)} w_j + \pi_v^{(j-m-1)} w_{m+1}, \ldots, \pi_v^{(m-1)} w_m + \pi_v^{-1} w_{m+1}, w_{m+1},$$

where π_v is a uniformizing parameter. Let $x \in G_{\mathcal{O}_v}^{R_v}$ and $x = (x_{ij})$ in the base $w_1, w_2, \ldots, w_{m+1}$. Since the trace is invariant under conjugation, W_0 and f_0 are invariant under G; moreover, G acts trivially on W_1. It follows that x has the form $x = \begin{pmatrix} y & 0 \\ 0 & 1 \end{pmatrix}$, where $y = (y_{ij})$ is a matrix of degree m which is orthogonal with respect to f_0; thus it suffices to show that $y \in GL_m(\mathcal{O}_v, \mathfrak{p}_v)$ with respect to the base $w_1, \ldots, w_m$. We have

$$x(\pi_v^{(j-1)} w_j + \pi_v^{(j-m-1)} w_{m+1}) = \pi_v^{(j-1)} \sum_{i=1}^{m} y_{ij} w_i + \pi_v^{(j-m-1)} w_{m+1}$$

$$= \sum_{i=1}^{m} \alpha_{ij} (\pi_v^{(i-1)} w_i + \pi_v^{(i-m-1)} w_{m+1}) + \alpha_{m+1,j} w_{m+1},$$

hence

(8.23)
$$y_{ij} = \pi_v^{(i-j)} \alpha_{ij}, \quad i \neq j$$

(8.24)
$$y_{jj} = 1 - \pi_v^{(m+1-j)} \alpha_{m+1,j} - \sum_{i \neq j} y_{ij} \quad (i, j = 1, \ldots, m).$$

Since $\alpha_{ij} \in \mathcal{O}_v$, we obtain, as in the proof of Proposition 8.12, that

$$y_{ij} \in \mathfrak{p}_v^{|i-j|} \quad \text{for all } i, j$$

as a consequence of (8.23), since y is orthogonal with respect to f_0 and $v \notin S_2$. Then, turning to (8.24), we find that $y_{ij} \equiv 1 \pmod{\mathfrak{p}_v}$. This completes the proof of Lemma 8.7 and Proposition 8.13.

The problem of the number of classes in the genus of a lattice in the full matrix algebra under conjugation admits the following natural generalization. Let G be a simple adjoint algebraic K-group. Then the adjoint action of G on its Lie algebra $\mathfrak{g}$ induces a faithful K-representation $G \to \mathbf{GL}(\mathfrak{g})$, and one may ask what values $\mathrm{cl}(G^L)$ can assume on all the lattices L in $\mathfrak{g}_K$. (The above analysis is a special case of this problem for $G = \mathbf{PSL}_n$, since W_0 introduced in the proof of Lemma 8.7 is actually the Lie algebra $L(G)$.) The methods which we have developed enable us to answer this question.

PROPOSITION 8.14. *Let G be a simple adjoint algebraic K-group of noncompact type other than D_{2n}. Assume G is realized as a group of inner automorphisms of its Lie algebra $\mathfrak{g}$, and let $f = p_1^{\alpha_1} \ldots p_s^{\alpha_s}$ be the exponent of the corresponding fundamental group F. Then for any finite abelian group B of exponent dividing f there is a lattice $L(B)$ in $\mathfrak{g}_K$ for which $\mathcal{G}\mathrm{cl}(G^{L(B)}) \simeq B$. In particular, for any number of the form $p_1^{\beta_a} \ldots p_s^{\beta_s}$, there is a lattice $L(\beta_1, \ldots, \beta_s)$ in $\mathfrak{g}_K$ with $\mathrm{cl}(G^{L(\beta_1, \ldots, \beta_s)}) = p_1^{\beta_1} \ldots p_s^{\beta_s}$.*

PROOF: The fundamental group F of any simple algebraic group of type other than D_{2n} is cyclic; therefore by Theorem 8.5 it suffices to construct lattices R_v in $\mathfrak{g}_{K_v}$ for which $\psi_{K_v}(G_{\mathcal{O}_v}^{R_v}) = 1$. To this end, let us consider the Killing form h on $\mathfrak{g}$, which is a nondegenerate K-defined quadratic form on $\mathfrak{g}$, invariant under the action of G. Then one can use the following

LEMMA 8.8. *Let $G \subset \mathbf{GL}_n$ be an algebraic K-group such that $G \subset \mathbf{O}_n(h)$ for a suitable nondegenerate K-defined quadratic form h. Assume that h has the canonical form $h = h_1 x_1^2 + \cdots + h_n x_n^2$ with respect to the base $e = (e_1, \ldots, e_n)$ of K^n; and for any v in V_f^K let R_v denote the $\mathcal{O}_v$-lattice*

with the base $e_1, \pi_v e_2, \dots \pi_v^{n-1} e_n$, *where* π_v *is a uniformizing parameter. Then for almost all* v *in* V_f^K *we have*

$$G_{\mathcal{O}_v}^{R_v} = \Phi C, \tag{8.25}$$

where

$$\Phi = \{ x \in G : x(e_i) = \pm e_i,\ i = 1, \dots, n \},$$
$$C = \{ x = (x_{ij}) \in G_{\mathcal{O}_v}(\mathfrak{p}_v) : x_{ij} \in \mathfrak{p}_v^{|i-j|},\ i, j = 1, \dots, n \}.$$

PROOF: We have $G_{\mathcal{O}_v}^{R_v} = G \cap \mathbf{O}_n(h)_{\mathcal{O}_v}^{R_v}$, where $\mathbf{O}_n(h)_{\mathcal{O}_v}^{R_v} = \Gamma B$ for almost all v, notation as in Proposition 8.12. It is easy to see that $\Phi = G \cap \Gamma$ and $C = G \cap B$; therefore to prove (8.25) we must show that

$$G \cap \Gamma B = (G \cap \Gamma)(G \cap B) \tag{8.26}$$

for almost all v in V_f^K. Put $\Delta = \Gamma \setminus \Phi$. Then the Zariski-closed sets G and Δ are disjoint; hence, for almost all v, their reductions modulo v are disjoint (Lemma 3.12), i.e.

$$G_{\mathcal{O}_v} GL_n(\mathcal{O}_v, \mathfrak{p}_v) \cap \Delta GL_n(\mathcal{O}_v, \mathfrak{p}_v) = \emptyset.$$

In particular, G cannot intersect ΔB, thereby yielding (8.26). Lemma 8.8 is proved.

The rest of the proof of Proposition 8.14 is standard. Consider a finite Galois extension P/K such that $\psi_K(\Phi) \subset H^1(P/K, F)$. Then, for almost all v satisfying $P \subset K_v$, by Lemmas 8.6 and 8.8 we have

$$\psi_{K_v}(G_{\mathcal{O}_v}^{R_v}) = \psi_{K_v}(\Phi)\psi_{K_v}(C) = 1,$$

as desired.

Proposition 8.14 also holds for groups of type D_{2n}, as can be seen easily from the proof of the general case of Theorem 8.3 (the Realization Theorem; cf. Platonov-Bondarenko-Rapinchuk [3]).

A characteristic peculiarity in the proof of Theorem 8.3 is that the computations of class number involved there are of a general nature, in the sense that they are not attached to any particular representation $\varphi: G \to \mathbf{GL}_d$ and are applicable every time one has the corresponding lattices in the representation space. On the other hand, whether such lattices can be constructed for an arbitrary faithful representation is still an open question. Thus, one has the

PROBLEM: Let $\varphi: G \to \mathbf{GL}_d$ be an arbitrary faithful K-defined representation of a semisimple K-group G of noncompact type, and let f be the exponent of the fundamental group F of G. Is it true that any finite abelian group B of exponent f can be obtained as the class group $\mathcal{G}\mathrm{cl}(G^{L(B)})$, for a suitable lattice $L(B)$ in K^d?

We showed above that an affirmative answer can be given for adjoint realizations of adjoint groups. If G is a simple adjoint group of type B_l, then the answer is affirmative for any realization of G. (The proof is analogous to the proof of Proposition 8.13, taking into consideration the fact that, for any representation $\varrho: G \to \mathbf{GL}_d$, there exists a nondegenerate G-invariant quadratic form; cf. Bourbaki [4].) This is virtually all that is known about the problem, and its solution apparently requires the development of essentially new methods of constructing lattices, using the representation theory of algebraic groups. We are somewhat optimistic in this regard, due to the following assertion, which shows that there always exist lattices with "small" stabilizers.

PROPOSITION 8.15 (RAPINCHUK). *Let* $G \subset \mathbf{GL}_n$ *be a reductive algebraic* K*-group which is not a normal subgroup of* $\mathbf{GL}_n$. *Then for any* v *in* V_f^K *there exists a sequence of lattices* $L(i)$ *in* K_v^n *such that* $\mu_v(G_{\mathcal{O}_v}^{L(i)}) \underset{i \to \infty}{\longrightarrow} 0$, *where* μ_v *is the Haar measure on* G_{K_v}.

PROOF: Suppose, to the contrary, that there is a constant $c > 0$ such that $\mu_v(G_{\mathcal{O}_v}^L) \geq c$ for any L in K_v^n. Let us fix a base $e_1, \dots, e_n$ of K^n. Taking $L = x(\mathcal{O}_v e_1 + \dots + \mathcal{O}_v e_n)$, with an arbitrary x in $GL_n(K_v)$, we have

$$G_{\mathcal{O}_v}^L = x(x^{-1}Gx)_{\mathcal{O}_v} x^{-1}$$

(where the integral points are taken with respect to the base $e_1, \dots, e_n$).

We claim that these subgroups $H(x) = x(x^{-1}Gx)_{\mathcal{O}_v} x^{-1}$ $(x \in GL_n(K_v))$ split into a finite number of conjugacy classes with respect to G_{K_v}. Indeed, by Proposition 3.16, any compact subgroup of G_{K_v} is contained in some maximal compact subgroup. On the other hand, by the results in §3.4 the maximal compact subgroups of G_{K_v} split into a finite number of conjugacy classes; let $H_1, H_2, \dots H_d$ be a full set of representatives of the conjugacy classes of the maximal compact subgroups of G_{K_v}. Thus, for any x in $GL_n(K_v)$, there is a g in G_{K_v} and $j = 1, \dots, d$ satisfying $gH(x)g^{-1} \subset H_j$. Moreover, we have clearly

$$[H_j : gH(x)g^{-1}] = \frac{\mu_v(H_j)}{\mu_v(H(x))} \leq \frac{\mu_v(H_j)}{c},$$

so $[H_j : gH(x)g^{-1}]$ is bounded from above. Thus it suffices to show that H_j has only a finite number of subgroups of a given index t. If $[H_j : D] = t$,

then $D \supset \varphi_s(H_j)$, where $s = t!$ and $\varphi_s(x) = x^s$. But from Proposition 3.3 it follows easily that the map φ_s is open at the identity; in particular, the (obviously normal) subgroup N of H_j, generated by $\varphi_s(H_j)$, is open. It follows that the number of subgroups of index t in H_j equals the number of those in H_j/N. It remains to note that the latter quotient group is finite, since H_j is compact.

Let us fix a finite set of elements $x_1, \dots, x_r$ in $GL_n(K_v)$, such that any subgroup $H(x)$ is conjugate in G_{K_v} to one of the $H(x_i)$, $i = 1, \dots, r$. Furthermore, let Z denote the centralizer of G in $\mathbf{GL}_n$ and let P denote the reductive subgroup ZG of $\mathbf{GL}_n$. Let us show that the quotient space $GL_n(K_v)/P_{K_v}$ is compact. To do so, it suffices to find a compact subset D of $GL_n(K_v)$ such that $GL_n(K_v) = Z_{K_v} G_{K_v} D$. Put

$$B_i = \{\, x \in GL_n(K_v) : H(x) = H(x_i) \,\}.$$

Then $GL_n(K_v) = \bigcup_{i=1}^{r} G_{K_v} B_i$, since we have $H(gx) = gH(x)g^{-1}$ for g in G_{K_v}; and it suffices to find compact subsets C_i such that $B_i \subset Z_{K_v} C_i$. If $x \in B_i$, then, putting $y = x^{-1}x_i$, we will have

$$y(x_i^{-1} G x_i)_{\mathcal{O}_v} y^{-1} = (x^{-1} G x)_{\mathcal{O}_v};$$

i.e., $B_i \subset x_i Y_i^{-1}$, where

$$Y_i = \{\, y \in GL_n(K_v) : y(x_i^{-1} G x_i) y^{-1} \subset GL_n(\mathcal{O}_v) \,\}.$$

We shall show that the Y_i have the form $Y_i = D_i Z_{\mathbf{GL}_n}(x_i^{-1} G x_i)_{K_v}$ with D_i compact. Then

$$B_i \subset x_i Y_i^{-1} = x_i x_i^{-1} Z_{K_v} x_i D_i^{-1} = Z_{K_v}(x_i D_i^{-1}),$$

as desired.

Let $a_1, \dots, a_d$ be a finite system of topological generators of $(x_i^{-1} G x_i)_{\mathcal{O}_v}$. Consider the map

$$\varphi\colon \mathbf{GL}_n \to W = \underbrace{\mathbf{GL}_n \times \cdots \times \mathbf{GL}_n}_{d},$$

given by $\varphi(g) = (ga_1 g^{-1}, \dots, ga_d g^{-1})$. Clearly $Y_i = \varphi^{-1}(W_{\mathcal{O}_v}) \cap GL_n(K_v)$. Now note that the Zariski closure of the subgroup generated by $a_1, \dots, a_d$ is $x_i G x_i^{-1}$, since $(x_i^{-1} G x_i)_{\mathcal{O}_v}$ is Zariski-dense in $x_i^{-1} G x_i$ (Lemma 3.2). In particular, the fibers of φ are the cosets modulo the centralizer $Z_i = Z_{\mathbf{GL}_n}(x_i^{-1} G x_i)$. But clearly Z_i is the algebraic group defined by the multiplicative group of the centralizer in $M_n(K_v)$ of the K_v-hull $K_v[(x_i^{-1} G x_i)_{K_v}]$,

which is a semisimple K_v-algebra, since G is reductive. It follows that $H^1(K_v, Z_i) = 1$, and consequently $\varphi^{-1}(x)_{K_v} \neq \emptyset$ for each x in $\operatorname{Im}\varphi \cap W_{K_v}$. Therefore $\varphi(Y_i) = \operatorname{Im}\varphi \cap W_{\mathcal{O}_v}$. By Theorem 2.16, the image of $\operatorname{Im}\varphi$ is Zariski-closed, so $\varphi(Y_i)$ is compact. Then $\varphi(Y_i) = \varphi(D_i)$ for a suitable compact D_i in $GL_n(K_v)$ and $Y_i = D_i(Z_i)_{K_v}$, as desired.

Now we can easily complete the proof of the proposition. Since the space $GL_n(K_v)/P_{K_v}$ is compact, it follows that P contains a Borel subgroup B of $\mathbf{GL}_n$ (Theorem 3.1), which certainly will also be a Borel subgroup of P. Since P is reductive, it contains a Borel subgroup B^- opposite to B. Clearly B^- is the opposite of B also with respect to $\mathbf{GL}_n$. But by the Bruhat decomposition, $B^- B$ contains a Zariski-open subset of $\mathbf{GL}_n$, and hence B and B^- generate $\mathbf{GL}_n$. Hence $P = \mathbf{GL}_n$. Recalling that $P = ZG$, where Z is the centralizer of G, we see that G is a normal subgroup of $\mathbf{GL}_n$ (i.e., is either contained in the center or contains $\mathbf{SL}_n$). This contradiction proves the proposition.

8.3. Class numbers of algebraic groups of compact type.

Theorem 8.3 in §8.2 gives a complete description of the possible values of $\operatorname{cl}(G)$, for a semisimple K-group G of noncompact type. In this section we shall examine the opposite case. The most definitive results are obtained for the case where G has compact type (cf. Theorem 8.8), i.e., when the Archimedean part G_∞ of the adele group is compact. This is the most important case in terms of applications, since the orthogonal groups of positive definite quadratic forms are of this type, and consequently we obtain results on the corresponding number of classes in the genus. However, if we do not insist on taking the desired lattices in the former dimension, then we can obtain analogous results for a broader class of semisimple K-groups G of mixed type, which means that there exists a K-simple component G^i in G with G^i_∞ compact.

THEOREM 8.7. *Let G be a semisimple algebraic K-group of mixed type and of degree n. Then, for any positive integer r, there is a free lattice $M(r)$ in K^{2n} such that $\operatorname{cl}(G^{M(r)})$ is divisible by r.*

PROOF: Let us fix a free lattice L in K^n and henceforth designate the group $G^L_{A(\infty)}$ simply by $G_{A(\infty)}$. For any v_0 in V_f^K and any open subgroup U of $G_{\mathcal{O}_{v_0}}$, we put

$$G_{A(\infty)}(v_0, U) = \prod_{v \in V_\infty^K} G_{K_v} \times \prod_{\substack{v \in V_f^K \\ v \neq v_0}} G_{\mathcal{O}_v} \times U,$$

and

$$G_{A(\infty)}(v_0) = G_{A(\infty)}(v_0, G_{\mathcal{O}_{v_0}}(\mathfrak{p}_{v_0})),$$

where, as usual, $G_{\mathcal{O}_{v_0}}(\mathfrak{p}_{v_0})$ is the congruence subgroup of level $\mathfrak{p}_{v_0}$. Let us write $c(G, v_0, U)$ (resp., $c(G, v_0)$) to denote the number of double cosets $G_{A(\infty)}(v_0, U) \setminus G_A/G_K$ (resp., $G_{A(\infty)}(v_0) \setminus G_A/G_K$). Instead of Theorem 8.7, we shall prove the following somewhat more technical result: For any positive integer r, there is a v_0 in V_f^K such that $\tilde{K} \subset K_{v_0}$ and $c(G, v_0)$ is divisible by r. Theorem 8.7 follows in the obvious way from this statement. Indeed, Proposition 8.11 implies the existence of a lattice N in K^{2n} such that $N_v = L_v$ for $v \neq v_0$ and $G_{\mathcal{O}_{v_0}}^{N_{v_0}} = G_{\mathcal{O}_{v_0}}(\mathfrak{p}_{v_0})$. Then, obviously, $G_{A(\infty)}^N = G_{A(\infty)}(v_0)$; in particular, $\mathrm{cl}(G^N) = c(G, v_0)$ is divisible by r. However, N is free by Proposition 8.2, in view of the condition that $\tilde{K} \subset K_{v_0}$.

Let $G_A = \bigcup_{i=1}^m G_{A(\infty)} z_i G_K$ be a partition of G_A into double cosets. Without loss of generality, we may assume that there exists a finite subset S_0 of V_f^K such that the v-component $(z_i)_v = 1$ for all $v \notin S_0$ and all $i = 1, \ldots, m$. Let $G_{\mathcal{O}}^{(i)}$ denote $z_i^{-1} G_{A(\infty)} z_i \cap G_K$. Also let $c_i(G, v_0, U)$ (resp., $c_i(G, v_0)$) be the number of double cosets in $G_{A(\infty)} z_i G_K$ modulo the subgroups $G_{A(\infty)}(v_0, U)$ (resp., $G_{A(\infty)}(v_0)$) and G_K.

LEMMA 8.9. *We have*

$$c(G, v_0, U) = \sum_{i=1}^m c_i(G, v_0, U). \tag{8.27}$$

Moreover, $c_i(G, v_0, U)$ equals the number of double cosets $U \setminus G_{\mathcal{O}_{v_0}}/G_{\mathcal{O}}^i$ for v_0 in $V_f^K \setminus S_0$. In particular, $c_i(G, v_0)$ is given by

$$c_i(G, v_0) = [G_{\mathcal{O}_{v_0}} : G_{\mathcal{O}}^{(i)} G_{\mathcal{O}_{v_0}}(\mathfrak{p}_{v_0})]. \tag{8.28}$$

PROOF: Formula (8.27) is obvious, therefore we shall establish the remaining assertions. For α in $G_{\mathcal{O}_{v_0}}$, let $x^{v_0}(\alpha)$ denote the adele with components

$$x_v = \begin{cases} 1, & v \neq v_0, \\ \alpha, & v = v_0. \end{cases} \tag{8.29}$$

Then

$$G_{A(\infty)} z_i G_K = \bigcup_{\alpha} G_{A(\infty)}(v_0, U) x^{v_0}(\alpha) z_i G_K,$$

where the union is taken over all α in $G_{\mathcal{O}_{v_0}}$. Now we show that the conditions

$$G_{A(\infty)}(v_0, U) x^{v_0}(\alpha) z_i G_K = G_{A(\infty)}(v_0, U) x^{v_0}(\beta) z_i G_K \tag{8.30}$$

and

$$U\alpha G_{\mathcal{O}}^{(i)} = U\beta G_{\mathcal{O}}^{(i)} \tag{8.31}$$

are equivalent. If (8.30) holds, then

$$x^{v_0}(\alpha) z_i = a x^{v_0}(\beta) z_i b \tag{8.32}$$

for some a in $G(v_0, U)$ and b in G_K. Then, clearly,

$$b = z_i^{-1} x^{v_0}(\beta^{-1}) a^{-1} x^{v_0}(\alpha) z_i \in z_i^{-1} G_{A(\infty)} z_i;$$

hence $b \in G_{\mathcal{O}}^{(i)}$. Projecting (8.32) on the v_0-component, and bearing in mind that by assumption $(z_i)_{v_0} = 1$, we obtain $\alpha = a_{v_0} \beta b$, where $a_{v_0} \in U$, i.e., (8.31). Conversely, if (8.31) holds, then $\alpha = c\beta d$, where $c \in U$ and $d \in G_{\mathcal{O}}^{(i)}$. Putting $a = x^{v_0}(\alpha) z_i d^{-1} z_i^{-1} x^{v_0}(\beta^{-1})$ and $b = d$, we ensure that (8.32) holds, and it suffices to establish that $a \in G(v_0, U)$. Since $d \in G_{\mathcal{O}}^{(i)}$, by our set-up $z_i d^{-1} z_i^{-1} \in G_{A(\infty)}$, and hence $a \in G_{A(\infty)}$. It remains to compute the v_0 component a_{v_0}. Since $(z_i)_{v_0} = 1$, we have

$$a_{v_0} = \alpha d^{-1} \beta^{-1} = c \in U,$$

as we wished to show.

Since, as we have seen, (8.30) and (8.31) are equivalent, we obviously obtain $c_i(G, U, v_0) = |U \setminus G_{\mathcal{O}_{v_0}}/G_{\mathcal{O}}^{(i)}|$. To prove (8.28) it remains to note that, since $U = G_{\mathcal{O}_{v_0}}(\mathfrak{p}_{v_0})$ is normal in $G_{\mathcal{O}_{v_0}}$, the double coset $UxG_{\mathcal{O}}^{(i)}$ (for x in $G_{\mathcal{O}_{v_0}}$) is the right coset xW modulo the subgroup $W = G_{\mathcal{O}}^{(i)} G_{\mathcal{O}_{v_0}}(\mathfrak{p}_{v_0})$; so $c_i(G, v_0) = [G_{\mathcal{O}_{v_0}} : W]$. Lemma 8.9 is proved.

PROPOSITION 8.16. *Suppose G is a semisimple algebraic K-group of mixed type (cf. 4.4). Then, for any positive integer r, there is v_0 in V_f^K such that $\tilde{K} \subset K_{v_0}$ and all the $c_i(G, v_0)$ $(i = 1, \ldots, m)$ are divisible by r. In particular, $c(G, v_0)$ is divisible by r.*

PROOF: The definition of a group of mixed type implies that G is an almost direct product of semisimple groups F and H, where H has compact type. Put $D = G/F$, and let $\pi: G \to D$ be the corresponding quotient map. By Proposition 6.5, there is a finite subset S_1 of V_f^K such that, for each v in $V_f^K \setminus S_1$, π is defined over $\mathcal{O}_v$ and $\pi(G_{\mathcal{O}_v}) = D_{\mathcal{O}_v}$; then $\pi(G_{\mathcal{O}_v}(\mathfrak{p}_v)) \subset D_{\mathcal{O}_v}(\mathfrak{p}_v)$. Now for each $v \notin S_0 \cup S_1$, $c_i(G, v_0)$ is divisible by $[\pi(G_{\mathcal{O}_v}) : \pi(G_{\mathcal{O}}^{(i)}) \pi(G_{\mathcal{O}_v}(\mathfrak{p}_v))]$, and thus also is divisible by $[D_{\mathcal{O}_v} : \pi(G_{\mathcal{O}}^{((i)}) D_{\mathcal{O}_v}(\mathfrak{p}_v)]$.

Now we prove that all the $\pi(G_{\mathcal{O}}^{(i)})$ are finite. It follows from the definitions that

$$\pi(G_{\mathcal{O}}^{(i)}) \subset \pi(z_i)^{-1}\pi(G_{A(\infty)})\pi(z_i) \cap D_K. \tag{8.33}$$

But, since D is isogenous to H, it has compact type; it follows easily that the subgroup $\pi(G_{A(\infty)})$ of D_A is compact. On the other hand, the subgroup D_K of D_A is discrete. The intersection in (8.33), being simultaneously compact and discrete, is thus finite. Let l denote the least common multiple of the orders of all the $\pi(G_{\mathcal{O}}^{(i)})$. From what we have proven it follows, for each $i = 1, \dots, m$, that $c_i(G, v_0)$ has the form $\frac{d_i}{l}[D_{\mathcal{O}_{v_0}} : D_{\mathcal{O}_{v_0}}(\mathfrak{p}_{v_0})]$ for suitable d_i.

Therefore, the proof of Proposition 8.16, as well as Theorem 8.7, is completed by

LEMMA 8.10. *Let D be a nontrivial reductive K-group, and let F/K be a finite extension. Then, for any positive integer r, there exists an infinite set of v in V_f^K for which $F \subset K_v$ and $[D_{\mathcal{O}_v} : D_{\mathcal{O}_v}(\mathfrak{p}_v)]$ is divisible by r.*

PROOF: It is easy to see that the group of points $D_{\bar{K}}$ over the algebraic closure of K contains a finite subgroup C of order r. (One can find such a subgroup, for example, by considering an arbitrary (nontrivial) torus T of D and using the isomorphism $T_{\bar{K}} \simeq (\bar{K}^*)^{\dim T}$). Let P denote a finite Galois extension of K containing F and for which $C \subset G_P$. It follows from the Chebotarev density theorem that $S = \{ v \in V_f^K : P \subset K_v \}$ is infinite, and therefore there is an infinite number of v_0 in S such that $C \subset D_{\mathcal{O}_{v_0}}$, and the restriction of the reduction map modulo $\mathfrak{p}_{v_0}$ to C is injective. In this case $D_{\mathcal{O}_{v_0}}/D_{\mathcal{O}_{v_0}}(\mathfrak{p}_{v_0})$ contains an isomorphic image of C, so $[D_{\mathcal{O}_{v_0}} : D_{\mathcal{O}_{v_0}}(\mathfrak{p}_{v_0})]$ is divisible by r. Lemma 8.10 is proved.

Theorem 8.7 shows intuitively that, unlike the case of semisimple groups of noncompact type, the class number of the groups of mixed type can take on rather diverse values. Since it is impracticable to obtain a precise description of these values, rather than going into an elaboration of the theorem itself, below we shall focus our attention on obtaining arithmetic applications of Theorem 8.7. That is, we shall study class numbers in the original representation, since this enables one to characterize, for example, the possible number of classes in the genus of positive definite quadratic forms. Thus far, it has been shown that the analogous assertion to Theorem 8.7 holds for the groups of compact type in the original dimension n.

THEOREM 8.8. *Let G be a connected linear algebraic K-group of compact type and of degree n. Then, for any positive integer r, there exists a free lattice $L(r)$ in K^n such that $\mathrm{cl}(G^{L(r)})$ is divisible by r.*

For a nondegenerate n-dimensional quadratic form f, the group $G = \mathbf{SO}_n(f)$ has compact type if and only if f is K_v-anisotropic for each v in V_∞^K (in particular, the field must be totally real). Thus, if f is positive definite over all K_v, where $v \in V_\infty^K$ (in which case f simply is said to be positive definite), then Theorem 8.8 applies to $G = \mathbf{SO}_n(f)$. The same proof of Theorem 8.8 works without any modification also for $G = \mathbf{O}_n(f)$; so, in view of Proposition 8.4, we obtain the following result (compare with Theorem 8.6).

THEOREM 8.9. *Let f be a positive definite quadratic form of degree $n \geq 2$, with coefficients from the ring of integers $\mathcal{O}$ of a totally real algebraic number field K. Then, for any positive integer r, there exists a form f_r with coefficients from $\mathcal{O}$ which is K-equivalent to f and for which $c(f_r)$, the number of classes in the genus, is divisible by r.*

The local components of the desired $L(r)$ in Theorem 8.8 are constructed with the help of Lemma 8.8, which can be applied by virtue of the following

PROPOSITION 8.17. *Let G be a connected algebraic K-group of compact type and of degree n. Then there exists a positive definite quadratic form f with coefficients from K in n variables, such that $G \subset \mathbf{SO}_n(f)$.*

PROOF: Let W be the space of all quadratic forms in n variables; it can be identified with the space of symmetric $(n \times n)$-matrices in M_n. Let $\tilde{W}$ denote the K-subspace of W consisting of matrices invariant under G_K, i.e., $\tilde{W} = \{ A \in W : {}^t gAg = A \text{ for all } g \in G_K \}$. By assumption G_{K_v} is compact for any v in V_∞^K; therefore each $\tilde{W}_{K_v}$ must contain a positive definite matrix (cf. §3.2). It follows that the subset of positive definite matrices in $\tilde{W}_{K_v}$ is nonempty and open. Therefore, using the weak approximation property for $\tilde{W}$, we can find a matrix F in $\tilde{W}_K$ which is positive definite relative to any v in V_∞^K. Let f be the associated quadratic form. Then $G_K \subset \mathbf{O}_n(f)$. However, G_K is Zariski-dense in G (Theorem 2.2), since G is connected; so $G \subset \mathbf{O}_n(f)$, and the desired assertion follows. Proposition 8.17 is proved.

Now we outline the proof of Theorem 8.8. Using Proposition 8.17, we choose an n-dimensional positive definite G-invariant quadratic form f. Put f in the canonical form $f = f_1x_1^2 + \cdots + f_nx_n^2$ with respect to a suitable base $e = (e_1, \dots, e_n)$ of K^n. If $\tilde{K} \subset K_{v_0}$ for v_0 in V_f^K, then there is a uniformizing parameter π_{v_0} in $\mathcal{O}$ such that $\pi_{v_0} \in U_v$ for $v \neq v_0$, and we consider the lattice $L(v_0)$ with base $e_1, \pi_{v_0}e_2, \dots, \pi_{v_0}^{(n-1)}e_n$. Then $L(v_0)_v = L_v$, for $v \neq v_0$, where L is the lattice with base $e_1, \dots, e_n$; and for almost all v_0 the stabilizer $B(v_0) = G_{\mathcal{O}_{v_0}}^{L(v_0)_{v_0}}$ is described (Lemma 8.8) by:

$$B(v_0) = \Phi C, \tag{8.34}$$

where

$$\Phi = \{\, x \in G : x(e_i) = \pm e_i,\ i = 1, \dots, n \,\}$$

and

$$C = \{\, x = (x_{ij}) \in G_{\mathcal{O}_{v_0}}(\mathfrak{p}_{v_0}) x_{ij} \in \mathfrak{p}_{v_0}^{|i-j|},\ i, j = 1, \dots, n \,\}$$

(where the matrix notation is taken with respect to e). Fix a partition

$$G_A = \bigcup_{i=1}^{m} G^L_{A(\infty)} z_i G_K, \tag{8.35}$$

with the property that $(z_i)_v = 1$ for $i = 1, \dots, m$ for all v lying outside some finite subset S_0 of V_f^K. Then, by Lemma 8.9, for $v_0 \notin S_0$ we obtain the formula

$$\mathrm{cl}(G^{L(v_0)}) = \sum_{i=1}^{m} d_i(v_0),$$

where

$$d_i(v_0) = |B(v_0) \setminus G^{L_{v_0}}_{\mathcal{O}_{v_0}} / G^{(i)}_{\mathcal{O}}|, \qquad G^{(i)}_{\mathcal{O}} = z_i^{-1} G_{A(\infty)} z_i \cap G_K.$$

Thus far the argument has been completely analogous to the proof of Theorem 8.7; however, from here on additional complications arise. To wit, in computing $c_i(G, v_0) = |G_{\mathcal{O}_{v_0}}(\mathfrak{p}_{v_0}) \setminus G_{\mathcal{O}_{v_0}} / G^{(i)}_{\mathcal{O}}|$ in the proof of Theorem 8.7, we used the fact that the congruence-subgroup is normal, and reduced the computation of the number of double cosets to the computation of the index of a certain subgroup. In our case, $B(v_0)$ in general is not a normal subgroup of $G_{\mathcal{O}_{v_0}}$ and therefore another approach is called for. One trick is to choose the base e and the decomposition (8.35) in a special way, so that the corresponding $G^{(i)}_{\mathcal{O}}$ is contained in $\{\pm E_n\}$; then again $d_i(v_0) = |G^{L_{v_0}}_{\mathcal{O}_{v_0}} : G^{(i)}_{\mathcal{O}} B(v_0)|$, and the argument from the proof of Theorem 8.7 carries over without any modification. It turns out that this trick can be applied every time G is a proper subgroup of $\mathbf{SO}_n(f)$.

PROPOSITION 8.18. *Let G be a proper connected K-subgroup of $H = \mathbf{SO}_n(f)$. Then there exists an orthogonal base $e = (e_1, \dots, e_n)$ of K^n with respect to f, such that $G \cap \Gamma(e) \subset \{\pm E_n\}$, where*

$$\Gamma(e) = \{\, x \in \mathbf{GL}_n : x(e_i) = \pm e_i,\ i = 1, \dots, n \,\}.$$

PROOF: For $n = 2$, H is a one-dimensional torus; so G is trivial and there is nothing to prove. Therefore, we may assume $n > 2$. Let us fix an orthogonal base $e^0 = (e_1^0, \dots, e_n^0)$ of K^n with respect to f, and put

$\Gamma_0 = \Gamma(e^0)$. If $h \in H_K$, then, putting $h(e^0) = (h(e_1^0), \dots, h(e_n^0))$, we have $\Gamma(h(e^0)) = h\Gamma_0 h^{-1}$; therefore it suffices to show that there is h in H_K such that $G \cap (h\Gamma_0 h^{-1}) \subset \{\pm E_n\}$. Assume that this is not possible; then

$$H_K \subset \bigcup_{\gamma \in \Delta} C(\gamma), \tag{8.36}$$

where $C(\gamma) = \{\, h \in H : h^{-1}\gamma h \in G \,\}$ and $\Delta = \Gamma_0 \setminus \{\pm E_n\}$. Clearly $C(\gamma)$ is a Zariski-closed subset of H; so $H = \bigcup_{\gamma \in \Delta} C(\gamma)$ follows from (8.36) and the fact that H_K is dense in H (Theorem 2.2). Therefore, since H is connected, we have $H = C(\gamma)$ for some γ in Δ; i.e., G contains the conjugacy class $\{\, h^{-1}\gamma h : h \in H \,\}$. Therefore, the proposition follows from

LEMMA 8.11. *For $n > 2$, the normal subgroup of H generated by any element γ in $\Gamma_0 \setminus \{\pm E_n\}$ is H.*

Indeed, for $n \neq 4$, any proper normal subgroup of H lies in $\{\pm E_n\}$, therefore we need only consider the case $n = 4$. Here $H = H_1 H_2$ is an almost direct product of two groups isomorphic to $\mathbf{SL}_2$, identifying the centers. If we assume that the normal subgroup N of H generated by some γ in $\Gamma_0 \setminus \{\pm E_n\}$ is proper, then either $N = H_1$ or $N = H_2$. Under the isomorphism $H_i \simeq \mathbf{SL}_2$, the element γ goes over to $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ (this is the only element of order 2 in $\mathbf{SL}_2$). But then $\gamma = -E_4$, contradiction. This completes the proofs of Lemma 8.11 and Proposition 8.18.

PROPOSITION 8.19. *Let G be a proper K-subgroup of $\mathbf{SO}_n(f)$, where f is a positive definite quadratic form. Then there exists a base $e_1, \dots, e_n$ of K^n, orthogonal with respect to f, and a partition*

$$G_A = \bigcup_{i=1}^{n} G^L_{A(\infty)} z_i G_K$$

(where L is the lattice with base $e_1, \dots, e_n$) such that $(z_j)_v = 1$ for all v not in some finite subset S_0 of V_f^K, and all the $G^{(i)}_{\mathcal{O}} = z_i^{-1} G_{A(\infty)} z_i \cap G_K$ lie in $\{\pm E_n\}$.

PROOF: Let $u = (u_1, \dots, u_n)$ be the orthogonal base of K^n constructed in Proposition 8.18, and let M be the lattice with base u. Fix the partition

$$G_A = \bigcup_{j=1}^{r} G^M_{A(\infty)} t_j G_K,$$

in which $(t_j)_v = 1$ for $j = 1, \dots, r$, and for all v outside some finite subset S of V_f^K. The group G_∞ is compact since f is positive definite;

it follows that all the $\bar{G}_{\mathcal{O}}^{(j)} := t_j^{-1} G_{A(\infty)}^{M} t_j \cap G_K$ are finite. Let us put $R = (\bigcup_{j=1}^{r} \bar{G}_{\mathcal{O}}^{(j)}) \setminus \{\pm E_n\}$ and take a finite subset S_1 of V_f^K such that

$$R \cap (\pm G_{\mathcal{O}_v}(\mathfrak{p}_v)) = \emptyset,$$

for v in $V_f^K \setminus S_1$. Furthermore, choose v_0 in $V_f^K \setminus (S \cup S_1)$ such that $\tilde{K} \subset K_{v_0}$ and the stabilizer $B(v_0)$ of the lattice with base $u_1, \pi_{v_0} u_2, \ldots, \pi_{v_0}^{(n-1)} u_n$ is described by (8.34) (where π_{v_0} in $\mathcal{O}$ is a uniformizing parameter such that $\pi_{v_0} \in U_v$ for $v \neq v_0$). We wish to show that the desired base is

$$e_1 = u_1,\ e_2 = \pi_{v_0} u_2, \ldots,\ e_n = \pi_{v_0}^{(n-1)} u_n.$$

Let L be the lattice with base $e_1, \ldots, e_n$. Then by assumption $L_v = M_v$, for $v \neq v_0$ and $G_{\mathcal{O}_{v_0}}^{L_{v_0}} \subset G_{\mathcal{O}_{v_0}}^{M_{v_0}}$; so representatives of all the cosets $G_{A(\infty)}^{L} \setminus G_A / G_K$ can be chosen from adeles of the form $z(j,\alpha) = x^{v_0}(\alpha) t_j$, where $\alpha \in G_{\mathcal{O}_{v_0}}^{M_{v_0}}$ (see Lemma 8.9 for notation). Note that $(z(j,\alpha))_v = 1$ for $v \notin S_0 := S \cup \{v_0\}$. Therefore it suffices to show that

$$G_{\mathcal{O}}^{(j,\alpha)} := z(j,\alpha)^{-1} G_{A(\infty)}^{L} z(j,\alpha) \cap G_K \subset \{\pm E_n\}$$

for any j and α. We have

$$G_{\mathcal{O}}^{(j,\alpha)} = z(j,\alpha)^{-1} G_{A(\infty)}^{L} z(j,\alpha) \cap G_K \subset t_j^{-1} G_{A(\infty)}^{M} t_j \cap G_K = \bar{G}_{\mathcal{O}}^{(j)}.$$

However, taking the projection onto the v_0-component, we obtain

$$G_{\mathcal{O}}^{(j,\alpha)} \subset \alpha^{-1} G_{\mathcal{O}_{v_0}}^{L_{v_0}} \alpha;$$

i.e., finally

$$G_{\mathcal{O}}^{(j,\alpha)} \subset \bar{G}_{\mathcal{O}}^{(j)} \cap \alpha^{-1} B(v_0) \alpha,$$

where, as we required above, $B(v_0) = G_{\mathcal{O}_{v_0}}^{L_{v_0}}$ is described by (8.34), and $\Gamma(e) \cap G = \{\pm E_n\}$. It follows that for any α in $G_{\mathcal{O}_{v_0}}^{M_{v_0}}$ one has

$$\alpha^{-1} B(v_0) \alpha \subset \pm G_{\mathcal{O}_{v_0}}^{L_{v_0}}(\mathfrak{p}_{v_0}).$$

Thus

$$G_{\mathcal{O}}^{(j,\alpha)} \setminus \{\pm E_n\} \subset R \cap (\pm G_{\mathcal{O}_{v_0}}^{L_{v_0}}(\mathfrak{p}_{v_0})) = \emptyset,$$

since $R \cap (\pm G_{\mathcal{O}_{v_0}}(\mathfrak{p}_{v_0})) = \emptyset$. Proposition 8.19 is proved.

PROOF OF THEOREM 8.8 FOR $G \subsetneq \mathbf{SO}_n(f)$: Let $e = (e_1, \ldots, e_n)$ be the orthogonal base constructed in Proposition 8.19, and let L be the lattice generated by this base. Then, as we saw above, for almost all v_0 in V_f^K satisfying $\tilde{K} \subset K_{v_0}$ we have

$$\mathrm{cl}(G^{L(v_0)}) = \sum_{i=1}^{m} d_i(v_0),$$

with $d_i(v_0) = |B(v_0) \setminus G_{\mathcal{O}_{v_0}}^{L_{v_0}} / G_{\mathcal{O}}^{(i)}|$, where

$$B(v_0) = G_{\mathcal{O}_{v_0}}^{L(v_0)_{v_0}}, \qquad G_{\mathcal{O}}^{(i)} = z_i^{-1} G_{A(\infty)}^{L} z_i \cap G_K,$$

notation as above. Since by assumption $G_{\mathcal{O}}^{(i)} \subset \{\pm E_n\}$ for any $i = 1, \ldots, m$, we have $d_i(v_0) = |G_{\mathcal{O}_{v_0}}^{L_{v_0}} : G_{\mathcal{O}}^{(i)} B(v_0)|$. But $B(v_0) \subset \pm G_{\mathcal{O}_{v_0}}^{L_{v_0}}(\mathfrak{p}_{v_0})$, from which it follows that if $|G_{\mathcal{O}_{v_0}}^{L_{v_0}} : G_{\mathcal{O}_{v_0}}^{L_{v_0}}(\mathfrak{p}_{v_0})|$ is divisible by $2r$, then each $d_i(v_0)$ is divisible by r, and hence also $\mathrm{cl}(G^{L(v_0)})$ is divisible by r. Thus the proof is completed by applying Lemma 8.11.

It remains to prove Theorem 8.8 for $\mathbf{SO}_n(f)$, where f is a positive definite quadratic form. The argument here is technically more difficult than in the case of proper subgroups of $\mathbf{SO}_n(f)$; but, as we have mentioned, it applies as well to $\mathbf{SO}_n(f)$ and $\mathbf{O}_n(f)$. Since $\mathrm{cl}(\mathbf{O}_n(f))$ is $c(f)$, and hence is of special interest from the arithmetic viewpoint, we shall establish the analogous assertion to Theorem 8.8 for $G = \mathbf{O}_n(f)$; this gives us a proof of Theorem 8.9.

First, one proves the following analog of Proposition 8.19.

PROPOSITION 8.20. *There exists an orthogonal base $e_1, \ldots, e_n$ of K^n relative to f and a partition*

$$G_A = \bigcup_{i=1}^{m} G_{A(\infty)}^{L} z_i G_K \tag{8.37}$$

(where L is the lattice with base $e_1, \ldots, e_n$) such that $(z_i)_v = 1$ for all v not in some finite subset S_0 of V_f^K, and all the $G_{\mathcal{O}}^{(i)} = z_i^{-1} G_{A(\infty)}^{L} z_i \cap G_K$ are conjugate in G_K to a subgroup of $\Gamma = \{ x \in G : x(e_i) = \pm e_i,\ i = 1, \ldots, n \}$.

PROOF: Write f in diagonal form $f = a_1 x_1^2 + \cdots + a_n x_n^2$, with respect to a base $u_1, \ldots, u_n$ of K^n. Let M denote the lattice with base $u_1, \ldots, u_n$, and let us fix a partition

$$G_A = \bigcup_{j=1}^{n} G_{A(\infty)}^{M} t_j G_K,$$

in which $(t_j)_v = 1$ for $j = 1, \dots, r$, for all v not in some finite subset S_1 of V_f^K. As in the proof of Proposition 8.19, we conclude that all the $\bar{G}_{\mathcal{O}}^{(j)} = t_j^{-1} G_{A(\infty)}^M t_j \cap G_K$ are finite. Let us put $R = \bigcup_{j=1}^r \bar{G}_{\mathcal{O}}^{(j)}$ and find a finite subset S_2 of V_f^K such that for v in $V_f^K \setminus S_2$ we have

$$R \cap G_{\mathcal{O}_v}^{M_v}(\mathfrak{p}_v) = \{E_n\}.$$

Let us choose v_0 in $V_f^K \setminus (S_1 \cup S_2)$ such that $\tilde{K} \subset K_{v_0}$ and $v_0(a_i) = 0$ for all $i = 1, \dots, n$. Also, let us choose a uniformizing parameter π_{v_0} in $\mathcal{O}$ such that $\pi_{v_0} \in U_v$ for $v \neq v_0$, and show that the desired base is $e_1 = u_1$, $e_2 = \pi_{v_0} u_2, \dots, e_n = \pi_{v_0}^{(n-1)} u_n$.

Let L be the lattice with base $e_1, \dots, e_n$. Then $L_v = M_v$ for $v \neq v_0$, and the stabilizer $C = G_{\mathcal{O}_{v_0}}^{L_{v_0}}$ is as described in Proposition 8.12. Then, as above, we note that the representatives of all the cosets $G_{A(\infty)}^L \backslash G_A / G_K$ can be chosen among the adeles $z(j, \alpha)$ where $j = 1, \dots, r$ and $\alpha \in G_{\mathcal{O}_{v_0}}^{M_{v_0}}$ (cf. proof of Proposition 8.19). Moreover, $z(j, \alpha)_v = E_n$ for $v \notin S_0 := S_1 \cup \{v_0\}$ and

$$G_{\mathcal{O}}^{(j,\alpha)} = z(j, \alpha)^{-1} G_{A(\infty)}^L z(j, \alpha) \cap G_K \subset \bar{G}_{\mathcal{O}}^{(j)} \cap \alpha^{-1} C \alpha.$$

Since $C = \Gamma B$, where

$$B \subset G_{\mathcal{O}_{v_0}}^{M_{v_0}}(\mathfrak{p}_{v_0}), \qquad \Gamma = \{ x \in G : x(u_i) = \pm u_i,\ i = 1, \dots, n \},$$

we have $x^2 \in \bar{G}_{\mathcal{O}}^{(j)} \cap \alpha^{-1} B \alpha = \{E_n\}$, for any x in $G_{\mathcal{O}}^{(j,\alpha)}$; i.e., $x^2 = E_n$. Thus, the proof of Proposition 8.20 is completed by

LEMMA 8.12. *Let $\Theta \subset G_{\bar{K}}$ be a subgroup of exponent 2. Then Θ is conjugate in $G_{\bar{K}}$ to a subgroup of Γ.*

PROOF: Left to the reader as an exercise.

Take the base $e = (e_1, \dots, e_n)$ constructed in Proposition 8.20, a lattice L spanned by this base, and the corresponding partition (8.37). We shall assume that f has the form $f = f_1 x_1^2 + \cdots + f_n x_n^2$ with respect to e. Let us also consider g_i in $G_{\bar{K}}$ $(i = 1, \dots, m)$ for which

$$g_i^{-1} G_{\mathcal{O}}^{(i)} g_i \subset \Gamma.$$

Let P be a finite Galois extension of K containing $\tilde{K}$, the coefficients of the matrices g_j, and $\sqrt{-1}, \sqrt{f_1}, \dots, \sqrt{f_n}$. Let T denote a K-subtorus $\mathbf{SO}_2(h)$ of $\mathbf{SO}_n(f)$, where h is the restriction of f to the subspace spanned by e_1, e_2.

For given r it follows from Lemma 8.10 that there exists v_0 in $V_f^K \setminus S_0$ such that

(1) $P \subset K_{v_0}$,
(2) $|T_{\mathcal{O}_{v_0}}^{L_{v_0}} : T_{\mathcal{O}_{v_0}}(\mathfrak{p}_{v_0})|$ is divisible by $2^{2n} r$,
(3) $v(2) = v(f_1) = \cdots = v(f_n) = 0$,
(4) $g_j \in G_{\mathcal{O}_{v_0}}^{L_{v_0}}$.

LEMMA 8.13. *There exists an orthogonal base u_1, u_2 of $\mathcal{O}_{v_0} e_1 \oplus \mathcal{O}_{v_0} e_2$ such that $f(u_i) = a f_i$, $i = 1, 2$, where a in U_{v_0} is a unit element which is not a square.*

PROOF: It follows from our set-up that $h = f_1 x_2^2 + f_2 x_2^2$ is equivalent over $\mathcal{O}_{v_0}$ to the form $x_1 x_2$, for which the assertion is verified immediately.

For $i > 2$ put $u_i = e_i$, and let N_{v_0} denote the $\mathcal{O}_{v_0}$-lattice with base $u_1, \pi_{v_0} u_2, \dots, \pi_{v_0}^{(n-1)} u_n$, where π_{v_0} is a uniformizing parameter. Let us define $L(r)$ as follows:

$$L(r)_v = \begin{cases} L_v, & v \neq v_0, \\ N_{v_0}, & v = v_0. \end{cases}$$

It follows from Proposition 8.2 that $L(r)$ is free. Let us show that $\mathrm{cl}(G^{L(r)})$ is divisible by r. Note that $L(r)_v = L_v$ when $v \neq v_0$. On the other hand for $v = v_0$, by Proposition 8.12, $C = G_{\mathcal{O}_{v_0}}^{L(r)_{v_0}} = \Delta B$ where

$$\Delta = \{ x \in G : x(u_i) = \pm u_i,\ i = 1, \dots, n \}$$

and $B \subset G_{\mathcal{O}_{v_0}}^{L_{v_0}}(\mathfrak{p}_{v_0})$. Thus Lemma 8.9 yields

$$\mathrm{cl}(G^{L(r)}) = \sum_{i=1}^m c_i, \text{ where } c_i = |C \setminus G_{\mathcal{O}_{v_0}}^{L_{v_0}} / G_{\mathcal{O}}^{(i)}|.$$

From the choice of v_0 it follows that $G_{\mathcal{O}}^{(i)}$ is conjugate in $G_{\mathcal{O}_{v_0}}^{L_{v_0}}$ to a subgroup of Γ, for any $i = 1, \dots, m$. Therefore, the following proposition implies that all the c_i, and hence also $\mathrm{cl}(G^{L(r)})$, are divisible by r.

PROPOSITION 8.21. *Let H be a finite subgroup of $G_{\mathcal{O}_{v_0}}^{L_{v_0}}$ such that $g^{-1} H g \subset \Gamma$ for some g in $G_{\mathcal{O}_{v_0}}^{L_{v_0}}$. Then the number of double cosets $|C \setminus G_{\mathcal{O}_{v_0}}^{L_{v_0}} / H|$ is divisible by r.*

PROOF: Let $\mathcal{H}$ denote the set of all subgroups of H, and for H' in $\mathcal{H}$ put

$$D(H') = \{\, x \in G_{\mathcal{O}_{v_0}}^{L_{v_0}} : H \cap x^{-1}Cx = H' \,\},$$

and let $i(H')$ be such that $2^{i(H')} = [H : H']$.

LEMMA 8.14. *Notation as above,*

$$|C \setminus G_{\mathcal{O}_{v_0}}^{L_{v_0}}/H| = \sum_{H' \in \mathcal{H}} 2^{-(n+i(H'))} |B \setminus D(H')|.$$

PROOF: It is easy to see that $CD(H')H = D(H')$, i.e., $D(H')$ is the union of some family of double cosets CxH. So

$$|C \setminus G_{\mathcal{O}_{v_0}}^{L_{v_0}}/H| = \sum_{H' \in \mathcal{H}} |C \setminus D(H')/H|,$$

and it suffices to prove that

$$|C \setminus D(H')/H| = 2^{-(n+i(H'))} |B \setminus D(H')|.$$

To do so we establish that any double coset CxH, where $x \in D(H')$, consists of precisely $2^{(n+i(H'))}$ left cosets By, where $y \in D(H')$. We have

$$CxH = \bigcup_{h \in H} Cxh, \tag{8.38}$$

and moreover, $Cxh_1 = Cxh_2 \Leftrightarrow h_2 h_1^{-1} \in H \cap x^{-1}Cx = H'$. Thus, there are $2^{i(H')}$ disjoint cosets in (8.38). At the same time, for any y in $G_{\mathcal{O}_{v_0}}^{L_{v_0}}$,

$$Cy = \bigcup_{\delta \in \Delta} B\delta y, \tag{8.39}$$

and all the cosets in (8.39) are distinct, since $\Delta \cap B = \{1\}$. Lemma 8.14 is proved.

Since $i(H') \leq n$, to finish the proof of the proposition it suffices to show that $|B \setminus D(H')|$ is divisible by $2^{2n}r$ for any subgroup H' in $\mathcal{H}$. Put $\mathcal{H}(H') = \{\, H'' \in \mathcal{H} : H'' \supsetneqq H' \,\}$ and $\tilde{D}(H') = \{\, x \in G_{\mathcal{O}_{v_0}}^{L_{v_0}} : H' \subset x^{-1}Cx \,\}$. Then

$$D(H') = \tilde{D}(H') \setminus \bigcup_{H'' \in \mathcal{H}(H')} \tilde{D}(H''),$$

from which it follows that

$$|B \setminus D(H')| = |B \setminus \tilde{D}(H')| - |B \setminus \bigcup_{H'' \in \mathcal{H}(H')} \tilde{D}(H'')|.$$

To compute the number of elements in the union we use the following well-known formula: if $A_1, \ldots, A_m$ are finite sets, then

$$|A_1 \cup \cdots \cup A_m| = \sum_{l=1}^{m} (-1)^{l+1} \sum_{1 \leq i_1 \leq \ldots \leq i_l \leq m} |A_{i_1} \cap \cdots \cap A_{i_l}|.$$

Since $\tilde{D}(H_1'') \cap \tilde{D}(H_2'') = \tilde{D}(H_1''H_2'')$, it follows that there exist integers $b_{H''}$ $(H'' \in \mathcal{H})$ for which

$$|B \setminus \bigcup_{H'' \in \mathcal{H}(H')} \tilde{D}(H'')| = \sum_{H'' \in \mathcal{H}(H')} b_{H''} |B \setminus \tilde{D}(H'')|.$$

Therefore, the proof of Proposition 8.21 and Theorem 8.9 is completed by

LEMMA 8.15. *$|B \setminus \tilde{D}(H')|$ is divisible by $2^{2n}r$, for any subgroup H' of $\mathcal{H}$.*

PROOF: We show that if $\tilde{D}(H') \neq \emptyset$, then $Z = xT_{\mathcal{O}_{v_0}}^{L_{v_0}} x^{-1}$ centralizes H', for suitable x in $G_{\mathcal{O}_{v_0}}^{L_{v_0}}$. Then $\tilde{D}(H')Z = \tilde{D}(H')$, so $|B \setminus \tilde{D}(H')|$ can be expressed as $\sum_{ByZ} [\{\, Bz : Bz \subset ByZ \,\}|$, where the sum is taken over all double cosets ByZ and each term is the number of left cosets Bz contained in the double coset ByZ. It is easy to see that this number equals

$$[Z : Z \cap (y^{-1}By)] = [T_{\mathcal{O}_{v_0}}^{L_{v_0}} : T_{\mathcal{O}_{v_0}}^{L_{v_0}} \cap ((yx)^{-1}B(yx))].$$

Since $B \subset G_{\mathcal{O}_{v_0}}^{L_{v_0}}(\mathfrak{p}_{v_0})$, by assumption this index is a multiple of $2^{2n}r$, and hence the number of cosets $B \setminus \tilde{D}(H')$ is also a multiple of $2^{2n}r$.

Thus, let $d \in \tilde{D}(H')$, i.e., $H' \subset d^{-1}Cd$. By the theorem on the conjugacy of Sylow subgroups in profinite groups, $bdH'd^{-1}b^{-1} \subset \Delta$ for suitable b in B, since H is a 2-group and Δ is a Sylow 2-subgroup of $C = \Delta B$. We wish to show that $x = bd$ is as desired. To do so, it suffices to establish that $xH'x^{-1} \subset \Delta_0$, where

$$\Delta_0 = \{\, \delta \in \Delta : \delta(u_1) = u_1,\ \delta(u_2) = u_2, \text{ or } \delta(u_1) = -u_1,\ \delta(u_2) = -u_2 \,\}.$$

Let $\delta = xhx^{-1} \notin \Delta_0$, for suitable h in H'. Put

$$W(\delta) = \{\, w \in K_{v_0}^n : \delta(w) = w \,\}.$$

Then $W(\delta)$ contains exactly one of the elements u_1, u_2, let us say, u_1, and therefore has a base of the form $u_1, u_{i_1}, \dots, u_{i_l}$, where $i_j > 2$ $(j = 1, \dots, l)$. In particular, the discriminant $d(W(\delta))$ equals $af_1 f_{i_1} \dots f_{i_l}$, and hence $d(W(\delta)) \notin K_{v_0}^{*2}$. On the other hand, by assumption $g^{-1}Hg \subset \Gamma$, so the analogous space $W(\gamma) = \{ w \in K_{v_0}^n : \gamma(w) = w \}$ for an element $\gamma = g^{-1}hg$ has a base of the form $e_{j_1}, \dots, e_{j_m}$; hence $d(W(\gamma)) = f_{j_1} \dots f_{j_m} \in K_{v_0}^{*2}$. But $\gamma = (xg)^{-1}\delta(xg)$, implying $W(\delta) = (xg)W(\gamma)$; i.e., $W(\delta)$ and $W(\gamma)$ must be isometric and, in particular, have the same discriminants. Proof by contradiction. This completes the proof of all the theorems in this section.

Note: it would be interesting to obtain the analog of Theorem 8.8 for groups of mixed type.

8.4. Estimating the class number for reductive groups.

The results of §8.3 show that the possible values of the class number $\mathrm{cl}(\varphi(G))$ of a semisimple K-group G depend on the arithmetic properties of the group. Therefore, in order to characterize these numbers one needs to know more about G. But what can one say about $\mathrm{cl}(\varphi(G))$ in the most general case? Here, of course, one must exclude the case where G has absolute strong approximation, since in that case $\mathrm{cl}(\varphi(G)) = 1$ for any representation φ. It turns out that in the remaining cases the numbers $\mathrm{cl}(\varphi(G))$ are not bounded.

THEOREM 8.10. *Let G be a linear algebraic K-group of degree n, without the strong approximation property. Then, for any r, there is a lattice $M(r)$ in K^{2n} such that $\mathrm{cl}(G^{M(r)}) > r$.*

PROOF: Fix a lattice L in K^n, and for any open subgroup U of $G^L_{A_f(\infty)}$ let $c(U)$ denote the number of double cosets $(G_\infty \times U) \setminus G_A / G_K$.

LEMMA 8.16. *For any positive integer r, there is an open subgroup U such that $c(U) > r$.*

PROOF: Suppose the contrary. Then, $c(U_0)$ takes on a maximal value d, for some open subgroup U_0 of $G^L_{A_f(\infty)}$. Fix a partition

$$G_A = \bigcup_{i=1}^{d} (G_\infty \times U_0) z_i G_K \tag{8.40}$$

into double cosets. The assumption that $c(U_0)$ is maximal implies that, for any subgroup U of U_0, we have $c(U) = c(U_0)$; hence

$$(G_\infty \times U_0) z_i G_K = (G_\infty \times U) z_i G_K$$

for all $i = 1, 2, \dots, d$. Passing to the projections onto G_{A_f}, and denoting the projection of z_i by $\tilde{z}_i$, we obtain

$$U_0 \tilde{z}_i G_K = U \tilde{z}_i G_K,$$

and consequently

$$U_0 \tilde{z}_i G_K = \bigcap U \tilde{z}_i G_K, \tag{8.41}$$

where the intersection is taken over all the open subgroups U of U_0. Now we need the following elementary result from topological group theory: if a topological group H has a fundamental system $\mathfrak{U} = \{U\}$ of neighborhoods of the identity consisting of subgroups, then the closure of any subset Γ of H is given by $\bar{\Gamma} = \bigcap_{U \in \mathfrak{U}} U\Gamma$. It follows that the right side of (8.41) is the closure of $\tilde{z}_i G_K$ in G_{A_f}, i.e., is $\tilde{z}_i \bar{G}_K$, where $\bar{G}_K$ is the closure of G_K. From (8.40) we obtain

$$G_{A_f} = \bigcup_{i=1}^{d} U_0 \tilde{z}_i G_K = \bigcup_{i=1}^{d} \tilde{z}_i \bar{G}_K,$$

i.e., $\bar{G}_K$ has finite index in G_{A_f}. But this is impossible, since Theorem 7.12 and the absence of strong approximation for G imply that one of the conditions of Proposition 7.13 holds, according to which $\bar{G}_K$ has infinite index in G_{A_f}. The lemma is proved.

Now we continue the proof of Theorem 8.10. By Lemma 8.16, one can find an open subgroup U of $G^L_{A_f(\infty)}$ such that $c(U) > r$, and it suffices to find a lattice M in K^{2n} satisfying $G^M_{A_f(\infty)} \subset U$. But, since U is open, it contains a subgroup of the form $W = \prod_{v \in T} G^{L_v}_{\mathcal{O}_v}(\mathfrak{p}_v^{m_v}) \times \prod_{v \in V_f^K \setminus T} G^{L_v}_{\mathcal{O}_v}$, where T is a finite subset of V_f^K, and m_v $(v \in T)$ are suitable positive integers. By Proposition 8.11, for each v in T there exists a lattice $L_v(m_v)$ in K_v^{2n} such that $G^{L_v(m_v)}_{\mathcal{O}_v} = G^{L_v}_v(\mathfrak{p}_v^{m_v})$. We define the lattice M in K^{2n} by its localizations:

$$M_v = \begin{cases} L_v(m_v), & v \in T, \\ L_v \oplus \mathcal{O}_v^n, & v \notin T. \end{cases}$$

Then $G^M_{A_f(\infty)}$ is obviously W; so M is the desired lattice. Q.E.D.

Theorem 8.10 implies the following curious remark: if $\mathrm{cl}(\varphi(G))$ of an arbitrary algebraic K-group G takes on even one value $\neq 1$, then by changing φ we can obtain an infinite set of distinct values.

It would be interesting to obtain an analog of Theorem 8.10 for the original dimension n (assuming, naturally, that G is not a normal subgroup of $\mathbf{GL}_n$). Evidently this should be done by modifying suitably the proof of Proposition 8.15. For tori of $\mathbf{GL}_n$ other than the scalar torus this follows from Proposition 8.25, to be proved in §8.5 in connection with the genus problem in arithmetic groups.

Now we proceed to an exposition of results on the connection between the class number of an algebraic group and the class numbers of its parabolic subgroups and maximal tori. One of the primary motivations for studying this relationship is the hypothetical possibility of thereby obtaining estimates of class numbers of the maximal tori of a group; this may prove useful in using methods of algebraic group theory to study the class numbers of algebraic number fields. At present research in this topic is just beginning to develop, so the results which we have are only preliminary. Therefore we present the next theorems without proofs.

THEOREM 8.11 (BONDARENKO-RAPINCHUK [1]). *Let G be a reductive algebraic K-group, and let P be an arbitrary parabolic K-subgroup of G. Then $\mathrm{cl}(G) \leq \mathrm{cl}(P)$.*

COROLLARY 1. *Let G be a reductive K-split algebraic group, and let T be an arbitrary maximal K-split torus of G. Then $\mathrm{cl}(G) \leq \mathrm{cl}(T)$.*

Indeed, let $B = TU$ be a Borel subgroup of G containing T. Then, by Theorem 8.11, $\mathrm{cl}(G) \leq \mathrm{cl}(B)$. On the other hand, by Proposition 5.4, $\mathrm{cl}(B) \leq \mathrm{cl}(T)$, since U has the strong approximation property.

Corollary 1 gives an "efficient" version of Theorem 8.4 on one-class lattices for split groups over a one-class field.

COROLLARY 2. *Let G be a reductive split group over a one-class field K. Then $\mathrm{cl}(G) = 1$ in any K-realization of G for which G contains a maximal K-split torus in diagonal form. (More precisely, if $G \subset \mathbf{GL}_n$ and, for some base $e_1, \ldots, e_n$ of K^n, there is a maximal torus of G which is given by diagonal matrices, then $\mathrm{cl}(G^L) = 1$, where L is the lattice with base $e_1, \ldots, e_n$.)*

Let T be a maximal K-split torus of G, such that $T \subset D_n$. Since $\mathrm{cl}(G) \leq \mathrm{cl}(T)$ (Corollary 1), it suffices to show that $\mathrm{cl}(T) = 1$. Let $r = \dim T$ and let $\varphi: D_r \simeq T$ be a K-isomorphism. Since K is a one-class field, we have $\mathrm{cl}(D_r) = 1$ and therefore it suffices to verify that $\varphi(D_{r_{A(\infty)}}) \subset T_{A(\infty)}$. But in the coordinate notation for φ,

$$\varphi: (x_1, \ldots, x_r) \mapsto (\varphi_1(x_1, \ldots, x_r), \ldots, \varphi_n(x_1, \ldots, x_r)),$$

the rational functions φ_i must be multiplicative, and therefore have the form $\varphi_i(x_1, \ldots, x_r) = \prod_{j=1}^{r} x_j^{\alpha_{ij}}$ for suitable integers α_{ij}, yielding the desired result.

As we shall see in the examples below, the relationship between $\mathrm{cl}(G)$ and $\mathrm{cl}(T)$, where T is an arbitrary K-torus of an algebraic K-group G, can vary greatly. Therefore, the next result, which treats the case of semisimple groups of noncompact type, cannot be extended to a wider class of groups.

THEOREM 8.12 (PLATONOV-BONDARENKO-RAPINCHUK [2]). *Let G be a semisimple K-group of noncompact type, and let $\pi: \tilde{G} \to G$ be its universal K-covering. Then, for any maximal K-torus T of G,*

$$\mathrm{cl}(T) \geq \frac{\mathrm{cl}(G)}{|Ш(T)||H^1(\mathcal{G}, \mathbf{X}(\tilde{T}))|},$$

where $\mathbf{X}(\tilde{T})$ is the group of characters of $\tilde{T} = \pi^{-1}(T)$ and $\mathcal{G}$ is the Galois group over K of the splitting field L of T and $\tilde{T}$.

Note that if T is a maximal torus of G, split over K, then $Ш(T) = H^1(\mathcal{G}, \mathbf{X}(\tilde{T})) = 1$; thus we arrive at the estimate that $\mathrm{cl}(T) \geq \mathrm{cl}(G)$, obtained in a different way in Corollary 1 of Theorem 8.11.

COROLLARY 3. *Let G be a semisimple K-group of noncompact type. Then there exists a constant $M > 0$, depending only on G, such that, for any φ,*

$$\min_T \mathrm{cl}(\varphi(T)) \geq \frac{1}{M} \mathrm{cl}(\varphi(G)), \tag{8.42}$$

where the minimum is taken over all maximal K-tori of G.

Next we present two interesting examples, illustrating various types of relationships between $\min_T \mathrm{cl}(T)$ and $\mathrm{cl}(G)$.

EXAMPLE 1: Let $G = \mathbf{SL}_2$ over $\mathbb{Q}$. We shall show that for any $m > 0$ there is a lattice $L(m)$ in $\mathbb{Q}^4$ such that $\mathrm{cl}(T^{L(m)}) > m$ for any maximal $\mathbb{Q}$-torus T of G, whereas $\mathrm{cl}(G^{L(m)}) = 1$.

Fix a lattice L in $\mathbb{Q}^2$ and, for each prime number p, let M_p denote a lattice of $\mathbb{Q}_p^4$ such that $G_{\mathbb{Z}_p}^{M_p} = G_{\mathbb{Z}_p}^{M_p}(p)$ (cf. Proposition 8.12). Let $S(m) = \{p_1, \ldots, p_m\}$ be a set of m distinct odd prime numbers. Let us define $L(m)$ in $\mathbb{Q}^4$ by the conditions:

$$L(m)_p = \begin{cases} L_p \oplus \mathbb{Z}_p^2, & p \notin S(m), \\ M_p, & p \in S(m). \end{cases}$$

We shall show that $\mathrm{cl}(T^{L(m)}) \geq 2^{m-2}$ for any maximal $\mathbb{Q}$-torus T of G; this will yield the desired result at once. We have

$$\begin{aligned}\mathrm{cl}(T^{L(m)}) &= [T_A : T^{L(m)}_{A(\infty)} T_{\mathbb{Q}}] \\ &= [T_A : T^{L}_{A(\infty)} T_{\mathbb{Q}}][T^{L}_{A(\infty)} T_{\mathbb{Q}} : T^{L(m)}_{A(\infty)} T_{\mathbb{Q}}] \\ &= \mathrm{cl}(T^L)[T^L_{A(\infty)} : T^{L(m)}_{A(\infty)} T^L_{\mathbb{Z}}] \\ &= \mathrm{cl}(T^L)\left[\prod_{p\in S(m)} T^{L_p}_{\mathbb{Z}_p} : \tau_{S(m)}(T^L_{\mathbb{Z}}) \prod_{p\in S(m)} T^{L_p}_{\mathbb{Z}_p}(p)\right],\end{aligned}$$

where $\tau_{S(m)}: T_{\mathbb{Q}} \to \prod_{p\in S(m)} T_{\mathbb{Q}_p}$ is the diagonal embedding.

The matrix $\left[\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right]$ belongs to all the $T^{L_p}_{\mathbb{Z}_p}$ but not to any of the $T^{L_p}_{\mathbb{Z}_p}(p)$, since p is odd. Therefore, in the decomposition of the abelian group $\prod_{p\in S(m)} T^{L_p}_{\mathbb{Z}_p}/T^{L_p}_{\mathbb{Z}_p}(p)$ into cyclic groups, one encounters at least m cyclic factors of order divisible by 2. On the other hand, by Corollary 1 of Theorem 4.11, $T^L_{\mathbb{Z}}$ is the direct product of a finite group Φ and a free abelian group Γ of rank ≤ 1. One has $T \simeq \mathbb{G}_m$, since $\dim T = 1$; consequently Φ is cyclic. Thus, $T^L_{\mathbb{Z}}$ has at most two cyclic factors, which means that the quotient group

$$D = \prod_{p\in S(m)} T^{L_p}_{\mathbb{Z}_p} \Big/ \left(\tau_{S(m)}(T^L_{\mathbb{Z}}) \prod_{p\in S(m)} T^{L_p}_{\mathbb{Z}_p}(p)\right)$$

has at least $(m-2)$ cyclic factors of order divisible by 2. In particular, $|D| \geq 2^{m-2}$, and hence $\mathrm{cl}(T^{L(m)}) = \mathrm{cl}(T^L)|D| \geq 2^{m-2}$. On the other hand, by the strong approximation theorem $\mathrm{cl}(G^{L(m)}) = 1$.

Example 1 shows that the difference between the left and right sides in (8.42) can be arbitrarily large; i.e., there cannot exist any estimates of the type $M\,\mathrm{cl}(G) \geq \min_T \mathrm{cl}(T)$, where M is a constant depending solely on the birational properties of G but not on its concrete realization.

EXAMPLE 2: Let $f = x^2 + y^2 + z^2$ with respect to a base e_1, e_2, e_3 of $\mathbb{Q}^3$, and let $G = \mathbf{SO}_3(f)$. Then $T = \mathbf{SO}_2(g)$, for $g = x^2 + y^2$, is a maximal torus of G.

Take an odd prime p and an integer $n \geq 0$; let $L(n)$ denote the lattice with base $e_1, e_2, p^n e_3$. Our objective is to show that $\mathrm{cl}(G^{L(n)}) \underset{n\to\infty}{\longrightarrow} +\infty$ whereas $\mathrm{cl}(T^{L(n)}) = 1$.

Put $D_n = G^{L(n)}_{\mathbb{Z}_p}$. Then, repeating the steps in the proof of Proposition 8.12, we can show that

$$D(n) = \{\, x = (x_{ij}) \in G_{\mathbb{Z}_p} : x_{ij} \equiv \pm\delta_{ij} \pmod{p^n},\ \text{if } i \text{ or } j \text{ equals } 3 \,\}$$

(where the matrix notation is taken with respect to e_1, e_2, e_3 and δ_{ij} is the Kronecker delta). Therefore $D(1) \supset D(2) \supset D(3) \supset \ldots$; moreover,

$$\bigcap_{n>0} D(n) = \{\, 1, \gamma \,\} T_{\mathbb{Z}_p},$$

where $\gamma = \mathrm{diag}(1, 1, -1)$. Since $T_{\mathbb{Z}_p}$ has infinite index in $G_{\mathbb{Z}_p}$, it follows that $[G_{\mathbb{Z}_p} : D(n)] \underset{n\to\infty}{\longrightarrow} +\infty$; consequently also

$$i(n) = |D(n) \setminus G_{\mathbb{Z}_p}/G_{\mathbb{Z}}| \underset{n\to\infty}{\longrightarrow} +\infty,$$

since $G_{\mathbb{Z}}$ is finite, because the form f is positive definite. On the other hand, arguing as in the proof of Lemma 8.9, it is easy to show that $i(n)$ is the number of double cosets of the form $G^{L(n)}_{A(\infty)} x G_{\mathcal{O}}$ contained in the principal class $G_{A(\infty)} G_{\mathbb{Q}}$; in particular, $\mathrm{cl}(G^{L(n)}) \geq i(n)$ and $\mathrm{cl}(G^{L(n)}) \underset{n\to\infty}{\longrightarrow} +\infty$.

It remains to establish that $\mathrm{cl}(T^{L(n)}) = 1$ for any n. Since the action of T on e_3 is trivial, it follows that $\mathrm{cl}(T^{L(n)}) = \mathrm{cl}(\mathbf{SO}_2(g))$ for all n. But it is well known (cf., for example, Borevich-Shafarevich [1]) that g is a one-class form, and therefore, by Proposition 8.4, $\mathrm{cl}(\mathbf{O}_2(g)) = 1$. Since $\mathbf{O}_2(g)_{\mathbb{Z}}$ contains a matrix of determinant -1, one can easily see that $\mathrm{cl}(\mathbf{SO}_2(g)) = 1$, as desired.

EXERCISE: Give another proof of $\mathrm{cl}(T^L) = 1$ in Example 2, using the fact that $K = \mathbb{Q}(\sqrt{-1})$ is a one-class field. (This follows from the existence of a Euclidean algorithm for the ring of Gaussian integers $\mathbb{Q} = \mathbb{Z}[i]$.) More precisely, consider the natural realization of $S = \mathbf{R}_{K/\mathbb{Q}}(\mathbb{G}_m)$ defined by the regular representation of K with respect to a suitable base of $\mathcal{O}/\mathbb{Z}$. It follows from $h_K = 1$ that $\mathrm{cl}(S) = 1$. Using $T \simeq \mathbf{R}^{(1)}_{K/\mathbb{Q}}(\mathbb{G}_m)$, construct, using Hilbert's Theorem 90 a surjective morphism $\theta: S \to T$ having $\ker\theta = \mathbb{G}_m$. Show that $\theta_A(S_A) = T_A, \theta(S_{A(\infty)}) \subset T_{A(\infty)}$, and deduce from this that $\mathrm{cl}(T) = 1$.

Example 2 shows that Theorem 8.12 (and even its corollaries) cannot be extended to the groups of compact type.

The relationship between the class numbers of a group and of its maximal tori undoubtedly merits further investigation. The purely algebraic methods which have been used thus far apparently need to be supplemented by analytic arguments, which ultimately should help clarify the "averaged"

picture of variation of the class number of tori, and in particular should answer the question as to whether the set of tori of an algebraic group with a given class number is finite or infinite (a modern version of Gauss' problem).

To conclude this section, we shall discuss briefly one other sort of problem—the change of class number of an algebraic group under a change of the ground field. More precisely, let G be an algebraic K-group and let E/K be a finite extension. How is $\mathrm{cl}(G)$ related to $\mathrm{cl}_E(G)$, the class number of the same G viewed as a group over E? (Henceforth we have in mind a realization of G by a given lattice L in K^n; then $\mathrm{cl}_E(G)$ and the corresponding group of integral points are taken with respect to $L\otimes_{\mathcal{O}}\mathcal{O}_E \subset E^n$, where $\mathcal{O}_E$ is the ring of integers of E.) Various aspects of this problem were studied by Bartels [1],[2] and Earnest-Hsia [1],[2]. We shall confine ourselves to pointing out the connection with the local-global principle for the cohomology of arithmetic subgroups. To state the results more concisely, we fix the principal class $G_{A_E(\infty)}G_E$ to be the distinguished element of the set of double cosets $G_{A_E(\infty)} \backslash G_{A_E}/G_E$.

THEOREM 8.13 (ROHLFS [1]). *Suppose E/K is a Galois extension, and that the Hasse principle holds for G over E (i.e., that the kernel of the map $H^1(E/K, G_E) \to \prod_v H^1(E_w/K_v, G_{E_w})$ is trivial). Then one has the following exact sequence of sets with distinguished element:*

$$1 \to \ker(G_{A(\infty)} \backslash G_A/G_K \to G_{A_E(\infty)} \backslash G_{A_E}/G_E) \xrightarrow{\alpha} H^1(E/K, G_{\mathcal{O}_E}) \xrightarrow{\beta} \prod_v H^1(E_w/K_v, G_{\mathcal{O}_{E_w}})$$

(for each v in V^K we choose a single extension w in V^E and assume that $\mathcal{O}_{E_w} = E_w$ for w in V_∞^E).

PROOF: Consists of several steps.

CONSTRUCTING α: Let $x \in G_A$ and $x = yz$, where $y \in G_{A_E(\infty)}$ and $z \in G_E$. Then for any σ in $\mathcal{G} = \mathrm{Gal}(E/K)$ we have

(8.43)
$$a_\sigma = y^{-1}y^\sigma = (xz^{-1})^{-1}(zx^{-1})^\sigma = z(z^{-1})^\sigma \in G_{A_E(\infty)} \cap G_E = G_{\mathcal{O}_E};$$

so $a = \{a_\sigma\}$ defines a cocycle in $H^1(E/K, G_{\mathcal{O}_E})$. Any other decomposition $x = y'z'$ is associated with $x = yz$ as follows: $y' = yt$ and $z' = t^{-1}z$, where $t \in G_{\mathcal{O}_E}$; therefore the corresponding cocycle

$$a'_\sigma = (y')^{-1}(y')^\sigma = t^{-1}y^{-1}y^\sigma t^\sigma = t^{-1}a_\sigma t^\sigma$$

is equivalent to $\{a_\sigma\}$. Moreover, if $x_1 = gxh$, where $g \in G_{A(\infty)}$ and $h \in G_K$, then $x_1 = (gy)(hz)$ and $(gy)^{-1}(gy)^\sigma = y^{-1}y^\sigma$, which shows that a depends only on $G_{A(\infty)}xG_K$. Thus, we have constructed a well-defined map α.

SHOWING ($\ker\alpha = \{1\}$): Suppose the cocycle $a = \{a_\sigma\}$ corresponding to x is trivial in $H^1(E/K, G_{\mathcal{O}_E})$, i.e., $a_\sigma = t^{-1}t^\sigma$ for suitable t in $G_{\mathcal{O}_E}$. Then (8.43) yields

$$y^{-1}y^\sigma = z(z^{-1})^\sigma = t^{-1}t^\sigma \qquad \text{for all } \sigma \text{ in } \mathcal{G}.$$

Therefore $(yt^{-1})^\sigma = yt^{-1}$ and $(tz)^\sigma = tz$; i.e.,

$$y' = yt^{-1} \in G_{A_E(\infty)} \cap G_A = G_{A(\infty)}$$

and

$$z' = tz \in G_E \cap G_A = G_K.$$

Then $x = yz = y'z'$ belongs to the principal class $G_{A(\infty)}G_K$, as desired.

SHOWING EXACTNESS AT $H^1(E/K, G_{\mathcal{O}_E})$: By definition $a_\sigma = y^{-1}y^\sigma$, where $y \in G_{A(\infty)}$; i.e., a becomes trivial in

$$H^1(E/K, G_{A_E(\infty)}) = \prod_v H^1(E/K, \prod_{w|v} G_{\mathcal{O}_{E_w}}) = \prod_v H^1(E_w/K_v, G_{\mathcal{O}_{E_w}}).$$

Thus, $\mathrm{Im}\,\alpha \subset \ker\beta$. Conversely, if $a = \{a_\sigma\} \in H^1(E/K, G_{\mathcal{O}_E})$ lies in $\ker\beta$, then $a_\sigma = y^{-1}y^\sigma$ for suitable y in $G_{A_E(\infty)}$. Hence the image of a in $H^1(E/K, G_E)$ becomes trivial in $H^1(E_w/K_v, G_{E_w})$ for each v in V^K; since the Hasse principle holds for G, it follows that a is trivial in $H^1(E/K, G_E)$, i.e., there exists z in G_E such that $a_\sigma = z(z^{-1})^\sigma$. Put $x = yz$. Then, for any σ in $\mathcal{G}$, we have

$$x^\sigma = y^\sigma z^\sigma = (ya_\sigma)(a_\sigma^{-1}z) = zy = x;$$

so $x \in G_A$. Moreover, by assumption $x \in G_{A_E(\infty)}G_E$. Thus, the class $G_{A(\infty)}xG_K$ lies in $\ker(G_{A(\infty)} \backslash G_A/G_K \to G_{A_E(\infty)} \backslash G_{A_E}/G_K)$, and from the description of α it follows that $\alpha(G_{A(\infty)}xG_K) = a$. This completes the proof of Theorem 8.13.

COROLLARY 4 (THE HASSE PRINCIPLE FOR COHOMOLOGY OF ARITHMETIC SUBGROUPS OF SIMPLY CONNECTED GROUPS). *Let G be a simply connected semisimple K-group of noncompact type. Then for any Galois extension E/K, the kernel of the map*

$$H^1(E/K, G_{\mathcal{O}_E}) \to \prod_v H^1(E_w/K_v, G_{\mathcal{O}_{E_w}})$$

is trivial.

Indeed, the Hasse principle always holds for cohomology of groups of rational points of simply connected groups (Theorem 6.6). However, the strong approximation property for G (Theorem 7.12) yields $\mathrm{cl}(G) = 1$, and the assertion follows from the exact sequence of the theorem.

An interesting result for the groups of compact type is obtained by arguing conversely: first derive the Hasse principle for the cohomology, and as a corollary show that $\ker(G_{A(\infty)} \backslash G_A/G_K \to G_{A_E(\infty)} \backslash G_{A_E}/G_E)$ is trivial.

COROLLARY 5. *Let G be an algebraic $\mathbb{Q}$-group with compact group of $\mathbb{R}$-points, and let $K/\mathbb{Q}$ be a totally real Galois extension. Suppose that $G_{\mathcal{O}_K} = G_{\mathbb{Z}}$ (cf. §4.8) and that the Hasse principle holds for G over K. Then the kernel of the canonical map*

$$G_{A_{\mathbb{Q}}(\infty)} \setminus G_{A_{\mathbb{Q}}}/G_{\mathbb{Q}} \to G_{A_K(\infty)} \setminus G_{A_K}/G_K$$

is trivial.

Let $G = \mathbf{O}_n(f)$ for a quadratic form f. In view of the fact (Proposition 8.4) that the double cosets $G_{A(\infty)} \setminus G_A/G_K$ are in one-to-one correspondence with the classes in the genus of f (where the principal class $G_{A(\infty)}G_K$ corresponds to the class containing f) Corollary 5 yields

COROLLARY 6. *Let f be a positive definite quadratic form with integral coefficients, and let $K/\mathbb{Q}$ be a totally real Galois extension. Suppose $\mathbf{O}_n(f)_{\mathcal{O}_K} = \mathbf{O}_n(f)_{\mathbb{Z}}$ (which is always true if f is diagonal, cf. §4.8). If an integral form g lies in the genus of f and is equivalent to f over $\mathcal{O}_K$, then it is equivalent to f over $\mathbb{Z}$.*

The proof of Corollary 5 follows from the exact sequence of the theorem and the next result, interesting in its own right.

THEOREM 8.14 (BARTELS [2]). *Let G be an algebraic $\mathbb{Q}$-group, and let $K/\mathbb{Q}$ be a totally real Galois extension. Suppose $G_{\mathcal{O}_K} = G_{\mathbb{Z}}$. Then the kernel of the canonical map*

$$H^1(K/\mathbb{Q}, G_{\mathcal{O}_K}) \xrightarrow{\varrho} \prod_{v \in V} H^1(K_w/\mathbb{Q}_v, G_{\mathcal{O}_{K_w}}) \tag{8.44}$$

is trivial.

PROOF: Since the action of $\mathcal{G} = \mathrm{Gal}(K/\mathbb{Q})$ on $G_{\mathcal{O}_K} = G_{\mathbb{Z}}$ is trivial, the 1-cocycles on $\mathcal{G}$ with values in $G_{\mathcal{O}_K}$ are homomorphisms $\varphi\colon \mathcal{G} \to G_{\mathcal{O}_K}$, and the trivial class in $Z^1(K/\mathbb{Q}, G_{\mathcal{O}_K})$ corresponds to the trivial homomorphism. Now let $\varphi \in \ker \varrho$. Our objective is to show that $\varphi = 1$. For any w in V_f^K, let $\mathcal{G}_w^{(1)}$ denote the corresponding inertia group. The canonical maps

$$G_{\mathcal{O}_K} \to G_{\mathcal{O}_{K_w}} \to \Gamma = G_{\mathcal{O}_{K_w}}/G_{\mathcal{O}_{K_w}}(\mathfrak{P}_w)$$

and the inclusions

$$\mathcal{G}_w^{(1)} \subset \mathcal{G}_w = \mathrm{Gal}(K_w/\mathbb{Q}_v) \subset \mathcal{G}$$

induce the cohomology maps

$$H^1(K/\mathbb{Q}, G_{\mathcal{O}_K}) \xrightarrow{\varrho_w} H^1(K_w/\mathbb{Q}_v, G_{\mathcal{O}_{K_w}}) \xrightarrow{\theta_w} H^1(\mathcal{G}_w^{(1)}, \Gamma).$$

Since $\varphi \in \ker \varrho$, we have $\theta_w \circ \varrho_w(\varphi) = 1$. But $\mathcal{G}_w^{(1)}$ acts trivially on Γ, so this is equivalent to the triviality of the composition of the restriction of φ to $\mathcal{G}_w^{(1)}$ with the homomorphism sending $G_{\mathcal{O}_K}$ to Γ. In other words,

$$\varphi(\mathcal{G}_w^{(1)}) \subset G_{\mathcal{O}_K}(\mathfrak{P}_w) = G_{\mathbb{Z}}(p_w),$$

where p_w is the prime corresponding to w. Minkowski's lemma (cf. §4.8) implies that $G_{\mathbb{Z}}(p_w)$ is trivial for p_w odd. Reasoning analogously, we can easily show that $G_{\mathbb{Z}}(p_w)$ has exponent 2, for $p_w = 2$. Therefore, bearing in mind that $\mathcal{G}$ is generated by all the $\mathcal{G}_w^{(1)}$ (a corollary of Hermite's theorem, cf. §1.1), we obtain $\varphi(\mathcal{G}) \subset G_{\mathbb{Z}}(2)$; hence $\varphi(\mathcal{G}) \simeq (\mathbb{Z}/2\mathbb{Z})^l$ for suitable l.

Let L denote the subfield of K corresponding to $\ker \varphi$. Since $\mathcal{G}_w^{(1)} \subset \ker \varphi$ if p_w is odd, $L/\mathbb{Q}$ can be ramified only at diadic points. However, the fact that $\mathrm{Gal}(L/\mathbb{Q}) = \mathrm{Im}\,\varphi \simeq (\mathbb{Z}/2\mathbb{Z})^l$ implies that L is a compositum of quadratic extensions of $\mathbb{Q}$. Since the only real quadratic extension of $\mathbb{Q}$ that ramifies only at diadic points is of $\mathbb{Q}(\sqrt{2})$, it follows that either $l = 0$, which gives the desired result, or $L = \mathbb{Q}(\sqrt{2})$ and, in particular, $l = 1$.

We have the following commutative diagram with exact rows:

$$\begin{array}{ccccc} 1 & \longrightarrow & H^1(L/\mathbb{Q}, G_{\mathcal{O}_L}) & \xrightarrow{\alpha} & H^1(K/\mathbb{Q}, G_{\mathcal{O}_K}) \\ & & \downarrow \delta & & \downarrow \varrho \\ 1 & \longrightarrow & \prod_v H^1(L_w/\mathbb{Q}_v, G_{\mathcal{O}_{L_w}}) & \longrightarrow & \prod_v H^1(K_w/\mathbb{Q}_v, G_{\mathcal{O}_{K_w}}). \end{array} \tag{8.45}$$

Let $\mathrm{Gal}(L/\mathbb{Q}) = \{1, \sigma\}$ and $\varphi(\sigma) = a$. It follows from (8.45) that $\varphi \in \ker \delta$; therefore, arguing as above, we obtain $a \in G_{\mathbb{Z}}(2)$. We also need the following straightforward result.

LEMMA 8.17 (MINKOWSKI). *Let $a \in GL_n(\mathbb{Z}, 2)$ and let $a^2 = E_n$. Then there exists a matrix c in $GL_n(\mathbb{Z})$ such that $cac^{-1} = \mathrm{diag}(\varepsilon_1, \ldots, \varepsilon_n)$, where $\varepsilon_i = \pm 1$.*

Indeed, put $a_1 = \frac{1}{2}(E_n - a)$ and $a_2 = \frac{1}{2}(E_n + a)$. Then $a_i \in M_n(\mathbb{Z})$, $aa_1 = -a_1$, $aa_2 = a_2$, and $a_1 + a_2 = E_n$. It follows that any z in $\mathbb{Z}^n$ can be written as $z = z_1 + z_2$, where $z_i = a_i(z) \in \mathbb{Z}^n$. Thus, putting $M_i = a_i(\mathbb{Z}^n)$, we obtain $\mathbb{Z}^n = M_1 + M_2$. Moreover, if $z_i \in M_i$, then $a(z_i) = (-1)^i z_i$; therefore this sum is direct and a has the required form with respect to the base of $\mathbb{Z}^n$ which is the union of the bases of M_1 and M_2.

So, let c in $GL_n(\mathbb{Z})$ be chosen so that $d = cac^{-1}$ is $\operatorname{diag}(\varepsilon_1, \dots, \varepsilon_n)$, where $\varepsilon_i = \pm 1$. Moreover, since $\varphi \in \ker \delta$, one can choose a matrix b in $G_{\mathcal{O}_{L_2}}$ such that $a = b\sigma(b)^{-1}$. Then, for the matrix $t = (t_{ij}) = c\sigma(b)$ in $GL_n(\mathcal{O}_{L_2})$, we have

$$\sigma(t) = \sigma(c\sigma(b)) = cb = ca\sigma(b) = dt,$$

i.e., $\sigma(t_{ij}) = \varepsilon_i t_{ij}$ for entries t_{ij} of t. But if $\varepsilon_i = -1$ then $t_{ij} \in \sqrt{2}\mathcal{O}_{L_2}$ for all j, yielding $\det t \in \sqrt{2}\mathcal{O}_{L_2}$, which is impossible. Thus, all the $\varepsilon_i = 1$, i.e., $a = E_n$. We have shown that φ is trivial, and thus have completed the proof of Theorem 8.14.

With regard to Theorem 8.13, Corollary 1, and Theorem 8.14, it would be interesting to see whether (in the same sense as Corollary 1) the Hasse principle always holds for the cohomology of arithmetic subgroups of simply connected groups.

8.5. The genus problem.

In §8.1 we gave a general definition of the genus and the class of an integral element of an algebraic variety under the action of an algebraic group, and showed that computing the number of classes in the genus reduces to counting certain double cosets. In this section we use the methods developed for computing the class numbers of algebraic groups in order to illustrate specific instances of estimating and characterizing the number of classes in the genus.

We begin by examining the *genus problem in arithmetic groups*, first studied by Platonov [8]. Let G be a linear algebraic group defined over $\mathbb{Q}$. Recall (cf. §8.1) that two elements a and b in $G_{\mathbb{Z}}$ are said to belong to the same genus if they are conjugate in $G_{\mathbb{Q}}$ and $G_{\mathbb{Z}_p}$ for all primes p, and to the same class if they are conjugate in $G_{\mathbb{Z}}$. Let $[a]_G$ denote the genus of a in $G_{\mathbb{Z}}$, and let $f_G(a)$ be the number of classes contained in $[a]_G$. This number is always finite (cf. Proposition 8.6). The genus problem consists of studying the properties of the function $f_G(a)$ (where $a \in G_{\mathbb{Z}}$), and is closely related to the problem of conjugacy separability of finitely generated linear groups, to estimation of the class numbers of maximal tori of reductive groups, and to other arithmetic and group theoretic questions.

For commutative groups the genus problem is meaningless, therefore the greatest interest lies in studying $f_G(a)$ for G semisimple. In this case f_G

turns out to be unbounded on the arithmetic subgroups H of $G_{\mathbb{Z}}$, under the natural condition that $G_{\mathbb{Z}}$ be infinite or, equivalently (cf. §4.6), that the group of real points $G_{\mathbb{R}}$ be noncompact.

THEOREM 8.15. *Let G be a semisimple algebraic $\mathbb{Q}$-group such that $G_{\mathbb{R}}$ is noncompact. Then $\sup_{a \in H} f_G(a) = \infty$, for any arithmetic subgroup H of $G_{\mathbb{Z}}$.*

Theorem 8.15 was obtained for $\mathbb{Q}$-isotropic groups by Platonov [8]. There he conjectured that this theorem should hold in general. This conjecture was confirmed for orthogonal groups over $\mathbb{Q}$ by Matveev [1]. Theorem 8.15 was put in its final form by Rapinchuk [1].

First we reduce the proof of Theorem 8.15 to the case of simply connected $\mathbb{Q}$-simple groups.

PROPOSITION 8.22. *Let $\pi: \tilde{G} \to G$ be a $\mathbb{Q}$-isogeny of $\mathbb{Q}$-groups. If*

$$\sup_{a \in \tilde{H}} f_{\tilde{G}}(a) = \infty$$

for any arithmetic subgroup $\tilde{H}$ of $\tilde{G}_{\mathbb{Z}}$, then also $\sup_{a \in H} f_G(a) = \infty$ for any arithmetic subgroup H of $G_{\mathbb{Z}}$.

PROOF: Since $\pi_A: \tilde{G}_A \to G_A$ is continuous and $F = \ker \pi$ is finite it follows that there exists an open normal subgroup U of $\tilde{G}_{A(\infty)}$ containing G_∞, such that $\pi_A(U) \subset G_{A(\infty)}$ and $U \cap F_{\mathbb{Q}} = \{1\}$. Clearly $[G_{A(\infty)}: U]$ is some finite number l. Furthermore, $\Gamma = \tilde{G}_{\mathbb{Q}} \cap U$ has finite index in $\tilde{G}_{\mathbb{Z}} = \tilde{G}_{\mathbb{Q}} \cap \tilde{G}_{A(\infty)}$; therefore, by Theorem 4.1 we see that $[G_{\mathbb{Z}} : \pi(\Gamma)]$, which we denote by m, is finite. (Note that $\pi(\Gamma) \subset G_{\mathbb{Q}} \cap \pi_A(U) \subset G_{\mathbb{Q}} \cap G_{A(\infty)} = G_{\mathbb{Z}}$.) Theorem 4.1 also implies that the inverse image $\pi^{-1}(H)$ of any arithmetic subgroup H of $G_{\mathbb{Z}}$ is an arithmetic subgroup of $\tilde{G}$; therefore

$$\tilde{H} = \pi^{-1}(H) \cap \Gamma \subset \tilde{G}_{\mathbb{Z}}$$

is arithmetic. To prove the proposition we shall show that if $a \in \tilde{H}$ then there is b in $[a]_{\tilde{G}}$ such that $f_G(\pi(b)) \geq \frac{f_{\tilde{G}}(a)}{ml}$.

Put $t = f_{\tilde{G}}(a)$ and let $a_1 = a, a_2, \dots, a_t$ be representatives of the distinct classes contained in $[a]_{\tilde{G}}$. It follows from the definition of the genus that for each $i = 1, \dots, t$ one can find g_i in $\tilde{G}_{A(\infty)}$ satisfying $a_i = g_i^{-1} a g_i$. Consider the partition $\{1, \dots, t\} = \bigcup_{j=1}^{l} I_j$, assuming that i_1 and i_2 fall in the same class I_j if $g_{i_1} U = g_{i_2} U$. Then clearly one can find j_0 for which $I = I_{j_0}$ contains no fewer than t/l elements. Let us put $b = a_i$, where $i \in I$, and show that b is the desired element.

First note that $a_i = g_i^{-1} a g_i \in U \cap \tilde{G}_{\mathbb{Q}} = \Gamma$ for any $i = 1, \dots, t$; since $a \in \tilde{H} \subset U$ and U is a normal subgroup of $\tilde{G}_{A(\infty)}$, so $c_i = \pi(a_i) \in G_{\mathbb{Z}}$. Furthermore, by definition the a_i (i in I) are conjugate in U; therefore the corresponding c_i are conjugate in $\pi(U)$ and also in $G_{A(\infty)}$. Moreover, the a_i are conjugate in $\tilde{G}_{\mathbb{Q}}$, and therefore the c_i are conjugate in $G_{\mathbb{Q}}$. By this argument, the c_i ($i \in I$) lie in the same genus, i.e., $c_i \in [\pi(b)]_G$.

To prove that $f_G(\pi(b)) \geq \frac{|I|}{m} \geq \frac{t}{ml}$, it now suffices to find at least $\frac{|I|}{m}$ elements among the c_i ($i \in I$) which are not conjugate in $G_{\mathbb{Z}}$. To this end, now consider the partition $I = \bigcup_{k=1}^{s} J_k$, such that the indexes i_1 and i_2 in I belong to the same class if c_{i_1} and c_{i_2} are conjugate in $G_{\mathbb{Z}}$.

We shall show for any k that $|J_k| \leq m$. Then $s \geq \frac{|I|}{m}$, but also $f_G(\pi(b)) \geq s$, which gives the desired result. Suppose $|J_k| > m$. Fix an index i_0 in J_k, and for each i in J_k find an element z_i in $G_{\mathbb{Z}}$ satisfying $c_i = z_i^{-1} c_{i_0} z_i$. For any two distinct $i_1, i_2 \in J_k$, we have $z_{i_1} = z_{i_2} \pi(g)$ for suitable g in Γ, since $[G_{\mathbb{Z}} : \pi(\Gamma)] = m$. Then

$$c_{i_1} = z_{i_1}^{-1} c_{i_0} z_{i_1} = \pi(g)^{-1} z_{i_2}^{-1} c_{i_0} z_{i_2} \pi(g) = \pi(g)^{-1} c_{i_2} \pi(g).$$

Recalling that $c_i = \pi(a_i)$, we obtain $\pi(a_{i_1}) = \pi(g^{-1} a_{i_2} g)$, i.e.,

$$x = a_{i_1}^{-1} g^{-1} a_{i_2} g \in F_{\mathbb{Q}}.$$

On the other hand, it follows from our definitions and the fact that U is a normal subgroup of $\tilde{G}_{A(\infty)}$ that $x \in U$. Therefore $x \in U \cap F_{\mathbb{Q}} = \{1\}$, and hence $a_{i_1} = g^{-1} a_{i_2} g$; contradiction, since the a_i are not conjugate in $G_{\mathbb{Z}}$ or in Γ. Proposition 8.22 is proved.

Now let G be an arbitrary semisimple $\mathbb{Q}$-group with a noncompact group of $\mathbb{R}$-points. Let $\pi: \tilde{G} \to G$ be the universal $\mathbb{Q}$-covering. By Proposition 8.22 it suffices to prove Theorem 8.15 for $\tilde{G}$. But $\tilde{G}$ is a direct product of its $\mathbb{Q}$-simple components G^i, and $G^{i_0}_{\mathbb{R}}$ is noncompact for some i_0. We claim that if Theorem 8.15 holds for G^{i_0} then it also holds for $\tilde{G}$. Indeed, Proposition 8.22 implies that the validity of Theorem 8.15 for $\tilde{G}$ is independent of the realization of $\tilde{G}$; therefore we can fix a realization of $\tilde{G}$ which is the direct product of the realizations of its components. Then $\tilde{G}_{\mathbb{Z}} = \prod_i G^i_{\mathbb{Z}}$ and $\tilde{G}_{\mathbb{Z}_p} = \prod_i G^i_{\mathbb{Z}_p}$ for any p; it follows for any a in $\tilde{G}_{\mathbb{Z}}$ that $f_{\tilde{G}}(a) \geq f_{G^{i_0}}(\mathrm{pr}_{i_0}(a))$, where $\mathrm{pr}_{i_0}: \tilde{G} \to G^{i_0}$ is the projection on G^{i_0}. Since $H' = \mathrm{pr}_{i_0}(H) \subset G^{i_0}_{\mathbb{Z}}$ is arithmetic for any arithmetic subgroup H of $\tilde{G}_{\mathbb{Z}}$ (Theorem 4.1), we can prove that $\sup_{a \in H} f_{\tilde{G}}(a) = \infty$ by proving $\sup_{a \in H'} f_{G^{i_0}}(a) = \infty$.

Thus, it suffices to prove Theorem 8.15 for simply connected $\mathbb{Q}$-simple groups. Let us show that in this case the following, more precise, assertion holds.

PROPOSITION 8.23. *Let G be a simply connected almost $\mathbb{Q}$-simple algebraic group whose group of $\mathbb{R}$-points is noncompact. Then, for any arithmetic subgroup H of $G_{\mathbb{Z}}$ and any positive integer r, there is an element a in H such that $f_G(a)$ is divisible by r.*

The proof rests on the following two facts:

PROPOSITION 8.24. *Let T be a noncentral K-torus of a connected K-group G. Then for any positive integer r there is an element g in G_K for which $\mathrm{cl}(g^{-1} T g)$ is divisible by r.*

LEMMA 8.18. *Under the assumptions of Proposition 8.23, there exists a semisimple element ε in $G_{\mathbb{Z}}$ such that ε^m is regular for any positive integer m.*

PROOF: Let G be a linear group of degree n; i.e., $G \subset \mathbf{GL}_n$. It is well known that the Euler function has the property $\varphi(r) \underset{r \to \infty}{\longrightarrow} \infty$; therefore there exists t in $\mathbb{N}$ such that $\varphi(r) > n!$ whenever $r > t$. Put $d = t!$ and consider the map $\tau_d: G \to G$ given by $\tau_d(x) = x^d$. Now, let G_s denote the set of all semisimple elements of G and let U denote an open Zariski-dense subset of G consisting of regular semisimple elements (cf. §2.1.11). With this notation, obviously $\tau_d(G_s) = G_s \supset U$, and in particular $\tau_d(G)$ is dense in G. But $G_{\mathbb{Z}}$ is also dense in G (Theorem 4.10), so finally $\tau_d(G_{\mathbb{Z}})$ is a dense subset of G. Since U is open, $U \cap \tau_d(G_{\mathbb{Z}})$ contains some element θ. We shall show that if $\theta = \tau_d(\varepsilon)$, where $\varepsilon \in G_{\mathbb{Z}}$, then ε is the desired element.

Let T be a maximal torus of G containing ε. By the criterion of regularity (cf. §2.1.11), an element x in T is regular if and only if $\alpha(x) \neq 1$ for any root α in $R(T, G)$; therefore we need to show that $\varrho = \alpha(\varepsilon)$ is not a root of unity. First we establish that ϱ belongs to the extension $F = \mathbb{Q}(\varepsilon_1, \dots, \varepsilon_n)$ of $\mathbb{Q}$ generated by the eigenvalues $\varepsilon_1, \dots, \varepsilon_n$ of ε. Indeed, by definition $\mathfrak{g} = L(G)$ contains a nonzero element X such that $\varepsilon^{-1} X \varepsilon = \alpha(\varepsilon) X$. Let us put ε in diagonal form; i.e., take a matrix z in $\mathbf{GL}_n$ such that $\xi = z^{-1} \varepsilon z$ is the diagonal matrix $\mathrm{diag}(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n)$. Then for $Y = z^{-1} X z$ one has $\xi^{-1} Y \xi = \alpha(\varepsilon) Y$. Therefore, if $Y = (y_{ij})$ and $y_{i_0 j_0} \neq 0$, then $\alpha(\varepsilon) = \varepsilon_{i_0}^{-1} \varepsilon_{j_0} \in F$. Since F is a splitting field of a polynomial of degree n with rational coefficients (the characteristic polynomial of ε), one has $[F : \mathbb{Q}] \leq n!$. However, if $\varrho^r = 1$, where $r > 0$ is minimal with this property, then $[\mathbb{Q}(\varrho) : \mathbb{Q}] = \varphi(r)$, from which it follows that $\varphi(r) \leq n!$. By assumption this yields $r \leq t$, and consequently r divides $d = t!$. Therefore $\alpha(\theta) = \alpha(\varepsilon^d) = \varrho^d = 1$, contradicting the regularity of θ. Lemma 8.18 is proved.

We postpone the proof of Proposition 8.24 and now complete the proof of Proposition 8.23. Let ε be the element constructed in Lemma 8.16. Then the centralizer $T = Z_G(\varepsilon)$ is a maximal torus of G. Indeed, since ε is

regular, the connected component $Z_G(\varepsilon)^0$ is a maximal torus; but it is well known (cf. Steinberg [2]) that in the simply connected case the centralizers of semisimple elements are connected. Note also that $Z_G(\varepsilon^m) = T$, since ε^m is regular for any m.

Now let us fix an arbitrary positive integer r. By Proposition 8.24 one can find g in $G_{\mathbb{Q}}$ for which $\mathrm{cl}(g^{-1}Tg)$ is divisible by r. Proposition 4.1 implies that $D = g^{-1}G_{\mathbb{Z}}g$ is arithmetic in G, from which it follows that $[D : D \cap H]$ is finite. Choose a normal subgroup $N \subset D$ of finite index, which is contained in $D \cap H$, and let l denote the exponent of D/N. Then $\zeta = g^{-1}\varepsilon^l g \in H$, and $f_G(\zeta)$ is divisible by r. Indeed, under the assumptions of Proposition 8.23, the strong approximation property holds for G; therefore $\mathrm{cl}(G) = 1$, and consequently $f_G(\zeta) = \mathrm{cl}(Z_G(\zeta))$ (Proposition 8.6). But $Z_G(\zeta) = g^{-1}Z_G(\varepsilon^l)g = g^{-1}Tg$ and $\mathrm{cl}(g^{-1}Tg)$ is divisible by r. This completes the proof of Proposition 8.23 and Theorem 8.15, as well.

PROOF OF PROPOSITION 8.24: Let a realization of G in $\mathbf{GL}_n$ be given by a lattice L in K^n, and let P be the splitting field of T. Since T is noncentral in G, its adjoint action on the corresponding Lie algebra $\mathfrak{g} = L(G)$ is nontrivial. Consequently, there is a non-trivial character α in $\mathbf{X}(T)$ and a nonzero element X in $\mathfrak{g}$ such that $\mathrm{Ad}(t)(X) = \alpha(t)X$ for all t in T. Moreover, since α is defined over P, one can choose X in $\mathfrak{g}_P$. Let l be a positive integer such that $\mathbf{X}(T) \cap \mathbb{Q}\alpha$ is generated by $\beta = \frac{1}{l}\alpha$. Since $\alpha \neq 1$, it follows that X is nilpotent (say $X^n = 0$), and we can consider the "truncated" exponential map

$$\varphi(a) = \sum_{m=0}^{n-1} \frac{a^m X^m}{m!}, \tag{8.46}$$

which gives a P-morphism of algebraic groups $\varphi: \mathbb{G}_a \to \mathbf{GL}_n$ (cf. §2.1.8). Let $W = \varphi(\mathbb{G}_a)$ be the corresponding one-dimensional unipotent subgroup. Then the Lie algebra $L(W)$ is generated by X and consequently $L(W) \subset \mathfrak{g}$ and $W \subset G$. It is also clear that the morphism $\psi: W \to \mathbb{G}_a$, which is the inverse of φ, is given by the "truncated" logarithmic map

$$\psi(u) = \sum_{m=1}^{n-1} (-1)^{m+1} \frac{(u-1)^m}{m}. \tag{8.47}$$

Moreover, for any a in $\mathbb{G}_a$ and t in T, we have

$$t^{-1}\varphi(a)t = \varphi(\alpha(t)a). \tag{8.48}$$

Let $e_1, \ldots, e_n$ be a base of P^n in which the elements of T can be written as diagonal matrices, and let M denote the $\mathcal{O}_P$-lattice generated by this

base. Let S consist of all the v in V_f^K for which at least one of the following conditions fails to hold for some extension $w|v$:

(i) $\{ a \in P_w : aX \in M_n(\mathcal{O}_{P_w}) \} = \mathcal{O}_{P_w}$,
(ii) $M_w = \mathcal{O}_{P_w} L$,
(iii) $w((n-1)!l) = 0$.

It is easy to see that S is finite; therefore the Chebotarev density theorem implies that $V_0 = \{ v \in V_f^K \setminus S : P \subset K_v \}$ is infinite.

LEMMA 8.19.

(1) *$g(g^{-1}Tg)_{\mathcal{O}_v}g^{-1} \subset T_{\mathcal{O}_v}$, for each $v \notin S$ and any g in G_{K_v}.*
(2) *If $v \in V_0$, then $\alpha(T_{\mathcal{O}_v}) = U_v^l$, where U_v is the group of v-adic units.*
(3) *Put $g = \varphi(\pi_v^{-1})$ for v in V_0, where π_v is a uniformizing parameter. Then $\alpha(g(g^{-1}Tg)_{\mathcal{O}_v}g^{-1}) \subset U_v^{(1)}$, where*

$$U_v^{(1)} = \{ a \in U_v : a \equiv 1 \pmod{\mathfrak{p}_v} \}.$$

PROOF: (1) Consider any P-isomorphism from T to a group of diagonal matrices D_r. In the proof of Corollary 2 in §8.4 we saw that this isomorphism is defined over $\mathcal{O}_P$ if T is put in diagonal form. Consequently, $T^{M_w}_{\mathcal{O}_{P_w}} \xrightarrow{\sim} (D_r)_{\mathcal{O}_{P_w}}$ for any w in V^P. But $(D_r)_{\mathcal{O}_{P_w}}$ is obviously the unique maximal compact subgroup of $(D_r)_{P_w}$ (i.e., contains each compact subgroup); therefore the same is true of $T^{M_w}_{\mathcal{O}_{P_w}}$ in T_{P_w}. Thus

$$g(g^{-1}Tg)_{\mathcal{O}_v}g^{-1} \subset T^{M_w}_{\mathcal{O}_{P_w}} \cap T_{K_v} = T_{\mathcal{O}_v},$$

since $M_w = \mathcal{O}_{P_w} L_v$ by virtue of the fact that $v \notin S$.

(2) It follows from our definitions that there exists a base $\chi_1, \ldots, \chi_r$ of $\mathbf{X}(T)$ such that $\chi_1 = \beta$. Then, by Theorem 2.1, there is a P-isomorphism $T \xrightarrow{\sim} D_r$ under which χ_1 corresponds to the character ζ_1 in $\mathbf{X}(D_r)$, given by $\zeta_1(\mathrm{diag}(x_1, \ldots, x_r)) = x_1$. Since $v \in V_0$, i.e., $v \notin S$ and $P_w = K_v$, it follows from the proof of (1) that $T \xrightarrow{\sim} D_r$ induces an isomorphism $T_{\mathcal{O}_v} \xrightarrow{\sim} (D_r)_{\mathcal{O}_v}$; hence $\beta(T_{\mathcal{O}_v}) = U_v$ and $\alpha(T_{\mathcal{O}_v}) = U_v^l$.

(3) If $t \in g(g^{-1}Tg)_{\mathcal{O}_v}g^{-1}$, then $g^{-1}tg \in G_{\mathcal{O}_v}$; moreover, also $t \in G_{\mathcal{O}_v}$, by (1). Using (8.48) we obtain

$$t^{-1}g^{-1}tg = \varphi(1 - \alpha(t)\pi_v^{-1}) \in G_{\mathcal{O}_v}.$$

By condition (iii), the denominators of all the terms in (8.47) are v-integral; therefore

$$\psi(t^{-1}g^{-1}tg)X = (1 - \alpha(t))\pi_v^{-1}X \in M_n(\mathcal{O}_v).$$

But then condition (i) implies that $(1-\alpha(t))\pi_v^{-1} \in \mathcal{O}_v$, i.e., $\alpha(t) \equiv 1 \pmod{\mathfrak{p}}_v$. Lemma 8.19 is proved.

We construct the desired g's in G_K in Proposition 8.26 by suitably approximating the elements $\varphi(\pi_v^{-1})$. More precisely, for each v_0 in V we find $g(v_0)$ in G_K, such that $g(v_0) \in \varphi(\pi_{v_0}^{-1})G_{\mathcal{O}_{v_0}}$ and $g(v_0) \in G_{\mathcal{O}_v}$ for v in S. Such an element always exists, even if G does not have weak approximation. Indeed, let $G = HR_u(G)$ be the Levi decomposition of G, let $B = [H,H]$ be the semisimple part of H, and let $\theta\colon \tilde{B} \to B$ be the universal K-covering. Using θ, we define an action of $\tilde{B}$ on $R_u(G)$ and take an isogeny

$$\tau\colon \tilde{D} = \tilde{B}R_u(G) \to BR_u(G) = D$$

of the respective semidirect products. Since $G/D = H/B$ is a torus, the unipotent element $x_{v_0} = \varphi(\pi_{v_0}^{-1})$ lies in D. Furthermore, arguing as in §7.2, we can show easily that in fact $x_{v_0} \in \tau(\tilde{D}_{K_{v_0}})$.

Let $x_{v_0} = \tau(y_{v_0})$, where $y_{v_0} \in \tilde{D}_{K_{v_0}}$. Choose open subgroups E_v of $\tilde{D}_{K_v}$ for v in $\{v_0\} \cup S$, such that $\tau(E_v) \subset G_{\mathcal{O}_v}$. It follows from Proposition 7.9 that $\tilde{D}$ always has weak approximation, which means one can find h in $\tilde{D}_K$ satisfying $h \in y_{v_0}E_{v_0}$ and $h \in E_v$ for v in S. Then $g(v_0) = \tau(h)$ will be the desired element.

Let us show that for suitable v_0 in V_0, $\mathrm{cl}(g(v_0)^{-1}Tg(v_0))$ is divisible by any preassigned positive integer r.

LEMMA 8.20. *$c(v_0) = \mathrm{cl}(g(v_0)^{-1}Tg(v_0))$ is divisible by $[U_{v_0}^l : \Gamma U_{v_0}^{(1)}]$, where $\Gamma = \alpha(T_0)$.*

PROOF: Put $C_v = g(v_0)(g(v_0)^{-1}Tg(v_0))_{\mathcal{O}_v}g(v_0)^{-1}$, for v in V_f^K. Then $c(v_0)$ is clearly $[T_A : CT_K]$, where $C = T_\infty \times \prod_{v \in V_f^K} C_v$. It follows from Lemma 8.19 (1) that $C_v \subset T_{\mathcal{O}_v}$ when $v \notin S$. But by assumption $g(v_0) \in G_{\mathcal{O}_v}$ when $v \in S$; therefore this inclusion also holds when $v \in S$. Thus, $C \subset T_{A(\infty)}$, yielding:

$$\begin{aligned} c(v_0) = [T_A : CT_K] &= [T_A : T_{A(\infty)}T_K][T_{A(\infty)}T_K : CT_K] \\ &= \mathrm{cl}(T)[T_{A(\infty)} : T_{A(\infty)} \cap (CT_K)] = \mathrm{cl}(T)[T_{A(\infty)} : CT_{\mathcal{O}}]. \end{aligned}$$

Projecting onto the v_0-component, we obtain that $[T_{A(\infty)} : CT_{\mathcal{O}}]$ is divisible by $[T_{\mathcal{O}_{v_0}} : C_{v_0}T_{\mathcal{O}}]$. Finally, applying α and using assertions (2) and (3) of Lemma 8.19, we obtain the desired result. (Note that $U_{v_0}^{(1)} \subset U_{v_0}^l$ since $v(l) = 0$.) Lemma 8.20 is proved.

Now we can easily complete the proof of Proposition 8.24. By Theorem 4.20, $T_{\mathcal{O}}$ is finitely generated. Let $a_1, \ldots, a_s$ be a finite set of generators of $\Gamma = \alpha(T_{\mathcal{O}})$. Put $d = lr$ and with the Chebotarev density theorem

find v_0 in $V_f^K \setminus S$, relatively prime to r, such that

$$P(\varrho_d, \sqrt[d]{a_1}, \ldots, \sqrt[d]{a_s}) \subset K_{v_0},$$

where ϱ_d is a primitive d-th root of unity. Then obviously $v_0 \in V_0$. Let us show that $[U_{v_0}^l : \Gamma U_{v_0}^{(1)}]$ is divisible by r. The quotient group $U_{v_0}/U_{v_0}^{(1)}$ is isomorphic to the multiplicative group $k_{v_0}^*$ of the corresponding residue field, and therefore is cyclic. Let Σ denote the cyclic subgroup of K_{v_0} generated by ϱ_d, which has order d. Since $U_{v_0}^{(1)}$ is a pro-p-group with respect to the prime p corresponding to v_0, and since $v_0(d) = 0$, it follows that $\Sigma \cap U_{v_0}^{(1)} = (1)$; this implies that $U_{v_0}/U_{v_0}^{(1)}$ contains an isomorphic image of Σ and, consequently, has order divisible by d. But then $U_{v_0}^l/U_{v_0}^d$ has order r. On the other hand, by assumption $\Gamma U_{v_0}^{(1)} \subset U_{v_0}^d$, so $[U_{v_0}^l : \Gamma U_{v_0}^{(1)}]$ is divisible by r. Proposition 8.24 is proved.

Proposition 8.24 immediately yields, in particular, a characterization of the class numbers of algebraic tori.

PROPOSITION 8.25. *Let $T \subset \mathbf{GL}_n$ be an algebraic torus of positive dimension.*

(i) *If T coincides with the torus S consisting of scalar matrices, then, for any lattice L in K^n, $\mathrm{cl}(T^L)$ equals the class number h_K of K;*
(ii) *If $T \neq S$, then, for any positive integer r, there exists a lattice $L(r)$ in K^n such that $\mathrm{cl}(T^{L(r)})$ is divisible by r.*

Now we are in a position to answer the main question of this chapter: what values can the class number $\mathrm{cl}(\varphi(G))$ of an algebraic group G assume, for arbitrary φ?

THEOREM 8.16. *Let G be a reductive algebraic K-group of degree n.*

(i) *If G is a semisimple group of noncompact type, then, for any φ, $\mathrm{cl}(\varphi(G))$ has the form $p_1^{\alpha_1}, \ldots, p_r^{\alpha_r}$, where $p_1, \ldots, p_r$ are the distinct prime divisors of the order of the fundamental group of G; moreover, all such numbers are indeed realized for suitable φ.*
(ii) *Otherwise, for any positive integer r, there is a lattice $L(r)$ in K^{2n} such that $\mathrm{cl}(G^{L(r)})$ is divisible by r.*

PROOF: We determined the class numbers of semisimple groups of noncompact type in Theorem 8.5. Assertion (ii) for semisimple groups of mixed type is proved in Theorem 8.7. The case where G is an algebraic torus is treated in Proposition 8.25. We leave it to the reader to analyze the remaining case of an almost direct product of a torus by a semisimple group,

as an exercise summarizing this chapter. We remind the reader that in studying class numbers we were compelled to enlarge the original realization. Therefore, we would like to underscore the problem of calculating $\mathrm{cl}(\varphi(G))$ for the case where φ has the same degree as a linear group G.

Theorem 8.15 has an interesting application to abstract group theory (cf. Platonov-Matveyev [1]). Recall that an abstract group Γ is said to be *conjugacy separable* if any two of its elements are conjugate in Γ if and only if their images are conjugate in all finite quotients of Γ (in other words, if the conjugacy classes in Γ are closed in the profinite topology of Γ). This concept is useful in studying algorithmic problems; in particular, it is well known that the answer to the conjugacy problem is affirmative in any group which is finitely presented and conjugacy separable. This property holds for free groups, polycyclic groups, and several other classes of groups (cf. Remeslenikov [1]). At the same time, Theorem 8.15 also enables us to construct large classes of examples of arithmetic groups which are not conjugacy separable.

Let G be a simply connected $\mathbb{Q}$-simple algebraic group with a noncompact group of $\mathbb{R}$-points. To state the conditions under which $\Gamma = G_{\mathbb{Z}}$ is not conjugacy separable we shall need several elementary results related to the congruence subgroup problem, discussed briefly in §9.5. Below we use τ_a and τ_c, respectively, to denote the arithmetic and congruence topologies, and $C = C(\Gamma)$ for the corresponding congruence kernel (note that $C = C^{V_\infty^K}(G)$, notation as in §9.5).

PROPOSITION 8.26. *We keep the previous assumption and notation. Assume that $C(\Gamma)$ is central. Then $\Gamma = G_{\mathbb{Z}}$ is not conjugacy separable.*

PROOF: It is well known (cf. §9.5) that the centrality of $C(\Gamma)$ implies its finiteness. Let $\hat{\Gamma}$ denote the completion of Γ under τ_a. There is an open normal subgroup N of Γ such that $N \cap C(\Gamma) = \{1\}$. Put $d = [\hat{\Gamma} : N]$. We shall show that if $a \in \Gamma$ and $a_1, \dots, a_r$ belong to the genus $[a]_G$, then there is a subset I of $\{1, \dots, r\}$ of cardinality $|I| \geq \frac{r}{d^2}$ such that a_i and a_j are conjugate in $\hat{\Gamma}$, for any i, j in I. To begin with, note that the strong approximation theorem implies that the completion $\bar{\Gamma}$ of Γ under τ_c is $\prod_p G_{\mathbb{Z}_p}$; so the a_i, which belong to the same genus by assumption, are conjugate in $\bar{\Gamma}$. Therefore, for any $i = 1, \dots, r$, one can find z_i in $\hat{\Gamma}$ and c_i in $C(G)$ satisfying $z_i^{-1} a_1 z_i = c_i a_i$. We introduce a partition

$$\{1, \dots, r\} = \bigcup_{k=1}^{t} I_k,$$

taking i and j in the same class if $a_i \in a_j N$ and $z_i \in z_j N$. Clearly t, the number of such classes, does not exceed d^2, and therefore among the I_k one can find a set I of order $|I| \geq \frac{r}{d^2}$. We shall show that I is the desired set.

Indeed, our definitions yield that

$$c_i = z_i^{-1} a_1 z_i a_i^{-1} \in (z_j^{-1} a_1 z_j a_j^{-1}) N = c_j N,$$

for i, j in I; hence $c_j^{-1} c_i \in N \cap C(\Gamma) = \{1\}$, i.e., $c_j = c_i$. Then, since $C(\Gamma)$ is central, letting $s = z_i^{-1} z_j$ we have

$$\begin{aligned} s^{-1} a_i s = c_i^{-1} s^{-1} (c_i a_i) s = c_i^{-1} z_j^{-1} z_i z_i^{-1} a_1 z_i z_i^{-1} z_j \\ = c_i^{-1} z_j^{-1} a_1 z_j = c_i^{-1} c_j a_j = a_j, \end{aligned}$$

as desired.

By Theorem 8.15 one can find a in $G_{\mathbb{Z}}$ whose class number in the genus is $r = f_G(a) > d^2$. Let $a_1, \dots, a_r$ be representatives of disjoint classes of $[a]_G$, and let I be a subset of $\{1, \dots, r\}$ of cardinality $|I| \geq \frac{r}{d^2} > 1$, constructed as above. Then a_i and a_j are conjugate in $\hat{\Gamma}$, for all $i \neq j$ in I; i.e., their images are conjugate in all finite quotients of Γ. On the other hand, by definition a_i and a_j lie in different classes and consequently are not conjugate in Γ. Proposition 8.26 is proved.

It follows from Proposition 8.26 and well-known results on the congruence subgroup problem (cf. §9.5) that if, for example, $G = \mathbf{R}_{K/\mathbb{Q}}(\mathbf{SL}_n)$, where $n \geq 3$ and K is any algebraic number field, then $\Gamma = G_{\mathbb{Z}}$ is not conjugacy separable, since $C(\Gamma)$ here is either trivial or is a central cyclic subgroup. Moreover, it should be noted that since, in general, $C(\Gamma) \neq 1$, to prove Proposition 8.26 it is not enough to find a's in $G_{\mathbb{Z}}$ for which $f_G(a) > 1$, i.e., elements for which the local-global principle for conjugation is violated; rather, one needs Theorem 8.15 on the existence of a in $G_{\mathbb{Z}}$ with $f_G(a)$ arbitrarily large.

REMARK: As we shall see in §9.5, it is natural to study the congruence subgroup problem in the more general context of S-arithmetic subgroups, since then the conjectured conditions for the centrality of the corresponding congruence kernel can be described uniformly as follows:

$$\mathrm{rank}_S G = \sum_{v \in S} \mathrm{rank}_{K_v} G \geq 2 \quad \text{and} \quad \mathrm{rank}_{K_v} G \geq 1, \quad \text{for } v \text{ in } S \setminus V_\infty^K.$$

In this regard, we point out that all the results in this section can be extended to such a situation without any modification. Here, instead of the usual double cosets $G_{A(\infty)} \backslash G_A / G_K$ one has to work with $G_{A(S)} \backslash G_A / G_K$. The methods used to count these classes hardly differ from those developed

in §8.2–8.4 for computing usual class numbers, and therefore all the results in this chapter, including Theorem 8.16, have their S-arithmetic analogs.

Besides the genus problem in arithmetic groups, we shall consider the *genus problem for integral representations* of finite groups (for the relevant definitions, cf. §8.1). Although we do not intend to present a comprehensive exposition of the theory of integral representations (cf. Curtis-Reiner [1]), we discuss this subject for two reasons. Firstly, it provides an example of efficient use of adele groups and class numbers of algebraic groups in what might seem to be an area that is far removed from the arithmetic of algebraic groups. Secondly, the answer to the genus problem here is diametrically opposed to that in Theorem 8.15; namely, the basic result affirms the uniform boundedness of the class numbers in the genus of all the integral representations of a given finite group Γ (among which, in general, there are infinitely many nonequivalent representations; cf. Curtis-Reiner [1, §8.1A]). Needless to say, to keep our digression on the theory of integral representations brief, we sketch only the main points.

THEOREM 8.17. *Let G be a finite group. Then there is an effectively determinable constant t such that the number of classes in the genus of any integral representation of Γ is bounded by t.*

PROOF: (Platonov [1].) Let $\varrho\colon \Gamma \to GL_n(\mathbb{Z})$ be an arbitrary integral representation, and let $G = Z_{GL_n}(\varrho(\Gamma))$ be its centralizer. We already know (cf. Proposition 8.5) that the number of classes in the genus of ϱ is $\mathrm{cl}(G^L)$, where $L = \mathbb{Z}^n$; therefore our objective is to obtain an estimation of $\mathrm{cl}(G^L)$ which is independent of ϱ and is determined only by the properties of Γ. Even a superficial familiarity with representation theory of finite groups suggests that the answer should be related to the properties of the corresponding group algebra $D = \mathbb{Q}[\Gamma]$. By Maschke's theorem, D is semisimple; i.e., it has the form $D = \bigoplus_{i=1}^{d} M_{n_i}(T_i)$, where T_i is a division algebra over $\mathbb{Q}$. In fact, T_i are in one-to-one correspondence with the equivalence classes R_i of the $\mathbb{Q}$-irreducible representations of Γ; i.e., if $\varrho_i \in R_i$ and $\varrho_i\colon \Gamma \to GL_{l_i}(\mathbb{Q})$, then T_i is the centralizer of $\varrho_i(\Gamma)$ in $M_{l_i}(\mathbb{Q})$. (The reader can find these and several other results from representation theory, needed in the proof, in Curtis-Reiner [1].) If ϱ is viewed as a representation over $\mathbb{Q}$, then one has the following direct sum decomposition:

$$\varrho = \bigoplus_{i=1}^{d} \left(\bigoplus_{j=1}^{m_i} \varrho_j \right), \qquad m_i \geq 0.$$

Then G is an algebraic $\mathbb{Q}$-group of the form $G = \prod_{i=1}^{d} \mathbf{R}_{K_i/\mathbb{Q}}(\mathbf{GL}_{m_i}(T_i))$, where K_i is the center of T_i and $\mathbf{GL}_0$ is assumed to be trivial over any skew

field. We would like to obtain an estimate of $\mathrm{cl}(G^L)$ which is independent of m_i. To do so, in each $G_i = \mathbf{R}_{K_i/\mathbb{Q}}(\mathbf{GL}_{m_i}(T_i))$ consider the subgroup

$$H_i = \begin{pmatrix} \mathbf{R}_{K_i/\mathbb{Q}}(\mathbf{GL}_1(T_i)) & & 0 \\ & 1 & \\ & & \ddots \\ 0 & & & 1 \end{pmatrix}$$

and put $H = \prod_{i=1}^{d} H_i$.

LEMMA 8.21. *$\mathrm{cl}(G^M) \leq \mathrm{cl}(H^M)$, for any lattice M in $\mathbb{Q}^n$.*

PROOF: For each $i = 1, \ldots, d$, if $m_i > 1$ let F_i denote the subgroup $\mathbf{R}_{K_i/\mathbb{Q}}(\mathbf{SL}_{m_i}(T_i))$ of G_i; otherwise put $F_i = (1)$. Clearly $F = \prod_{i=1}^{d} F_i$ is a normal subgroup of G. We shall show that $G_A = F_A H_A$. It suffices to establish that $G_{iA} = F_{iA} H_{iA}$ for each i. If $m_i \leq 1$, then $G_i = H_i$ and we have nothing to prove; therefore we may assume that $m_i > 1$. Letting D_i denote the algebra $M_{m_i}(T_i)$, whose center is K_i, we clearly have $\mathrm{Nrd}_{D_i/K_i}(GL_{m_i}(T_i)) = \mathrm{Nrd}_{D_i/K_i}(GL_1(T_i))$, where $GL_1(T_i)$ is embedded in $GL_{m_i}(T_i))$ in the natural way and Nrd_{D_i/K_i} is the reduced norm. A similar equality holds over any extension $P/\mathbb{Q}$; hence $G_{iP} = F_{iP} H_{iP}$. In particular, for any p one has $G_{i\mathbb{Q}_p} = F_{i\mathbb{Q}_p} H_{i\mathbb{Q}_p}$. Moreover, for almost all p, one can identify $G_{i\mathbb{Q}_p}$ with $GL_s(K_i \otimes \mathbb{Q}_p)$, where $s = m_i b$ and b is the index of T_i, and $H_{i\mathbb{Q}_p}$ with the subgroup

$$\begin{pmatrix} GL_b(K_i \otimes \mathbb{Q}_p) & & 0 \\ & 1 & \\ & & \ddots \\ 0 & & & 1 \end{pmatrix}.$$

Hence $G_{i\mathbb{Z}_p} = F_{i\mathbb{Z}_p} H_{i\mathbb{Z}_p}$. Therefore $G_{iA} = F_{iA} H_{iA}$, as desired. It follows from our definitions that F_i has absolute strong approximation; therefore, applying the argument in the proof of Proposition 5.4 to $G_A = F_A H_A$, we obtain the desired inequality. Lemma 8.21 is proved.

The arguments below use results on orders in semisimple algebras (cf. §1.5.3). The integral group ring $\Delta = \mathbb{Z}[\Gamma]$ is an order in $D = \mathbb{Q}[\Gamma]$ and therefore is contained in some maximal order $\tilde{\Delta}$. Put $f = [\tilde{\Delta} : \Delta]$; then $f\tilde{\Delta} \subset \Delta$. Let us extend ϱ to a representation of D. Since ϱ is an integral representation of Γ, it follows that $\varrho(\Delta)L = L$, and therefore

$$M = \varrho(\tilde{\Delta})L \subset \frac{1}{f}\varrho(\Delta)L = \frac{1}{f}L. \tag{8.49}$$

In particular, M is a lattice; moreover, clearly $\varrho(\tilde{\Delta}) \subset \mathrm{End}(M)$. Let C denote the centralizer of $\varrho(D)$ in $M_n(\mathbb{Q})$. Then $C = \bigoplus_{i=1}^{d} M_{m_i}(T_i)$ as an algebra; also, it is clear that G_P is the group of invertible elements of $C \otimes_{\mathbb{Q}} P$, for any $P/\mathbb{Q}$. Let Θ be the centralizer of $\varrho(\tilde{\Delta})$ in $\mathrm{End}(M)$; one can show that Θ is a maximal order in C. To estimate the class number of G we need to pass from Θ to Φ in C, which has the form $\bigoplus_{i=1}^{d} M_{m_i}(\mathcal{O}_i)$, where $\mathcal{O}_i$ is a maximal order in T_i. The order Φ is maximal in C, so $\Theta_p = \Theta \otimes_{\mathbb{Z}} \mathbb{Z}_p$ and $\Phi_p = \Phi \otimes_{\mathbb{Z}} \mathbb{Z}_p$ are maximal orders in $C_p = C \otimes_{\mathbb{Q}} \mathbb{Q}_p$, for any p. Consequently, by the theorem on the conjugacy of maximal orders in semisimple algebras over a local field, one can find g_p in $C_p^* = G_{\mathbb{Q}_p}$ such that $g_p \Theta_p g_p^{-1} = \Phi_p$. Moreover, for almost all p we have $\Theta_p = \Phi_p$, and one can put $g_p = 1$.

Let g denote the element of G_A whose p-component is g_p and whose real component is 1. Put $L_1 = g(L)$ and $M_1 = g(M)$, in the sense of the action of $GL_n(A)$ on lattices in $\mathbb{Q}^n$, as defined in §8.1. Then, by Lemma 8.21, we obtain

$$\mathrm{cl}(G^L) = \mathrm{cl}(G^{L_1}) \leq \mathrm{cl}(H^{L_1}). \tag{8.50}$$

We claim that $H_{\mathbb{Z}_p}^{L_{1p}} \subset H_{\mathbb{Z}_p}^{M_{1p}}$ for all p, and consequently $H_{A(\infty)}^{L_1} \subset H_{A(\infty)}^{M_1}$. Indeed, it suffices to show that $G_{\mathbb{Z}_p}^{L_{1p}} \subset G_{\mathbb{Z}_p}^{M_{1p}}$. We have $G_{\mathbb{Z}_p}^{L_{1p}} = g_p G_{\mathbb{Z}_p}^{L_p} g_p^{-1}$ and $G_{\mathbb{Z}_p}^{M_{1p}} = g_p G_{\mathbb{Z}_p}^{M_p} g_p^{-1}$; therefore the problem reduces to proving

$$G_{\mathbb{Z}_p}^{L_p} \subset G_{\mathbb{Z}_p}^{M_p}.$$

But any element from $G_{\mathbb{Z}_p}^{L_p}$ commutes with $\varrho(\tilde{\Delta})$, and therefore also leaves $M_p = \varrho(\tilde{\Delta}) L_p$ fixed, as desired. Thus, using (8.50) we obtain:

$$\mathrm{cl}(G^L) \leq \mathrm{cl}(H^{L_1}) \leq \mathrm{cl}(H^{M_1})[H_{A(\infty)}^{M_1} : H_{A(\infty)}^{L_1}]. \tag{8.51}$$

We proceed by looking at each factor separately. By assumption, $G_{\mathbb{Z}_p}^{M_p}$ is Θ_p^*, for any p; therefore $G_{\mathbb{Z}_p}^{M_{1p}} = g_p G_{\mathbb{Z}_p}^{M_p} g_p^{-1}$ is Φ_p^*. It follows that $H_{\mathbb{Z}_p}^{M_{1p}}$ is naturally isomorphic to $\prod_{i, m_i \neq 0} \mathcal{O}_{ip}^*$. Thus, $\mathrm{cl}(H^{M_1})$ is bounded from above by $h = \prod_{i=1}^{d} h_i$, where h_i is the number of double cosets taken in

$$(\mathcal{O}_i \otimes_{\mathbb{Z}} A_{(\infty)})^* \setminus (T_i \otimes_{\mathbb{Q}} A)^* / T_i^*.$$

The noncommutative analog of Proposition 8.1 shows that h_i is the class number of T_i, which is independent of the choice of the maximal order $\mathcal{O}_i$ (for more detail, see Deuring [1]).

To estimate the second factor in (8.51), note that (8.49) implies

$$fM_1 \subset L_1 \subset M_1.$$

It follows that, for any p, the congruence subgroup

$$H_{\mathbb{Z}_p}^{M_{1p}}(f) = H_{\mathbb{Z}_p}^{M_{1p}} \cap (E_n + f\,\mathrm{End}(M_{1p}))$$

is contained in $H_{\mathbb{Z}_p}^{L_{1p}}$. Indeed, for any g in $H_{\mathbb{Z}_p}^{M_{1p}}(f)$ and any l in L_{1p} we have

$$g(l) = (g - E_n)(l) + l \in fM_{1p} + l \subset L_{1p},$$

as desired. Therefore, identifying $H_{\mathbb{Z}_p}^{M_{1p}}$ with $\prod_{i, m_i \neq 0} \mathcal{O}_{ip}^*$ as above, we see that $[H_{A(\infty)}^{M_1} : H_{A(\infty)}^{L_1}]$ is bounded by $k = \prod_{i=1}^{d} k_i$, where

$$k_i = \prod_p [\mathcal{O}_{ip}^* : \mathcal{O}_{ip}^* \cap (1 + f\mathcal{O}_{ip})].$$

(Note that k_i is also independent of the choice of the maximal order $\mathcal{O}_i \subset T_i$.) Thus, finally, we see that we can take hk for the t in Theorem 8.17. Q.E.D.

Note that this proof of Theorem 8.17 also holds for integral representations of an arbitrary semisimple $\mathbb{Z}$-algebra Δ, since the fact that $\Delta = \mathbb{Z}[\Gamma]$ is not actually used.

BIBLIOGRAPHIC NOTE: The number of classes in the genus of quadratic forms and the class numbers of number fields were first studied by Gauss [1]. Since then a vast number of papers have been written on the subject. They treat various aspects of the problem, ranging from determining the class number in specific situations to obtaining asymptotic estimates of the class number for certain sets of forms, fields, etc. This chapter has been devoted to results that generalize the concept of class number to arbitrary algebraic groups. The fact that the numbers of classes in the genus of arithmetic objects are related to the class numbers of the corresponding algebraic groups (Theorem 8.2) is well known, but apparently has never been noted in such generality. This connection was utilized by Kneser [1] to obtain a complete description of the number of classes in the genus of an indefinite quadratic form (Theorem 8.6). Further results describing class numbers and class groups of semisimple groups of noncompact type were obtained in a series of papers by Platonov, Bondarenko and Rapinchuk [1–3]. Besides a complete proof of the realization theorem, these papers contain the theorem

on unboundedness of the class numbers of groups without absolute strong approximation, estimates of the class numbers of maximal tori, and some examples and applications of these results to classical arithmetical problems (in particular, the problem of calculating the class number in the genus of lattices on the full matrix algebra under conjugation). Analysis of class numbers in the genus of semisimple groups of mixed type on lattices of double dimension was begun in [3]. This investigation was completed by Rapinchuk [2] for groups of compact type in the original dimension; this, in particular, made it possible to obtain a characterization of the number of classes in the genus of positive definite quadratic forms. Section 8.5 contains the solution of the genus problem in arithmetic groups obtained by Rapinchuk [1], and an effective estimation of the number of classes in the genus of integral representations of a given finite group, due to Platonov [2].

9. Normal subgroup structure of groups of rational points of algebraic groups

The main results of this chapter focus on the following problem: let G be a simply connected simple algebraic group defined over an algebraic number field K; what can be said about the structure of G_K, the group of K-rational points? Of the many questions which arise in this regard, the problem of analyzing the normal subgroup structure of G_K has been singled out. This can be viewed as a tribute to the algebraic tradition which goes back to the work of Artin and Dieudonné on the normal subgroups of $SL_n(D)$ and other classical groups, as well as to the needs of closely related areas, in particular the theory of automorphic functions, the theory of group representation, etc.

As we indicated in Chapter 7, one must distinguish between the cases when G is K-isotropic and when G is K-anisotropic. Whereas, in the first case, much energy was directed at proving the Kneser-Tits conjecture for G (cf. Theorem 9.1), the subject long remained obscure for the second one, even in the general picture. Thus, until 1979, the only result bearing on this problem was the paper by Kneser [2], dated 1956 and studying the spinor groups of quadratic forms. In the past decade, research in this area has gained considerable impetus, in no small measure due to the conjecture on the criterion for G_K being projective simple, first put forward by Platonov at the International Congress of Mathematicians in Vancouver in 1974.

We shall begin our exposition with a discussion of this conjecture and its generalizations, followed by the statement of recent results (§9.1). Sections 9.2–9.4 are devoted to proving the theorems stated in §9.1. It should be noted that we are dealing here with results that were obtained quite recently (through 1989) and inherently are rather intricate. Therefore, the exposition in this section is more concise, stylistically resembling a paper in a journal more than a book. Nevertheless, in order not to lose the main train of thought, the proofs of some secondary assertions are left to the reader. In a word, this chapter demands more of the reader than previous chapters. We believe, however, that it will provide the attentive reader with the necessary background material for continuing independent research in this area. Lastly, in §9.5 we present a survey of the latest results on the congruence subgroup problem.

9.1. Main conjectures and results.

Throughout this chapter unless otherwise stated G denotes a simple simply connected algebraic group, defined over an algebraic number field K. The basic problem which we address is as follows: when does G_K, the group of K-rational points, have no noncentral normal subgroups? A more

general problem would be to describe all the possible normal subgroups of G_K. Analogous problems can be posed for arbitrary K; however there is no hope of obtaining a solution to the problem in such generality. (Note, also, that it hardly makes sense to discuss them for a broader class of groups than that singled out above, since when the radical of G is nontrivial the problem becomes meaningless, whereas the case of semisimple groups essentially reduces to that of simple groups.) The situation looks brighter for the case of a number field, since here, hypothetically, one can pass from the local analysis of normal structure to the global. The relevant conjecture has been formulated by Platonov [11].

CONJECTURE 9.1. *G_K is projectively simple (i.e., $G_K/Z(G_K)$ is simple[1]) if and only if, for all v in V^K, the local groups G_{K_v} are projectively simple.*

Thus formulated, this conjecture is a qualitatively new version of the local-global principle, which pervades all of the arithmetic theory of algebraic groups. Earlier statements of this principle were related to local-global isomorphisms of objects, and therefore generally could be reduced to proving injectivity of the maps of cohomology groups (cf. Chapter 6). Here we suggest the possibility of moving from local to global with respect to simplicity of an abstract group—a property which can in no way be conveyed *a priori* by cohomological invariants.

Conjecture 9.1 can be stated equivalently as follows: For an absolutely simple simply connected K-group G, the group G_K is projectively simple if and only if G is K_v-isotropic, for all v in V_f^K. Indeed, G_{K_v} is always projectively simple, for all v in V_∞^K (Proposition 7.6); therefore it remains to show that, for v in V_f^K, G_{K_v} being projectively simple is equivalent to G being K_v-isotropic. In one direction, this follows from the proof of the Kneser-Tits conjecture over non-Archimedean local fields (Theorem 7.6). The converse follows from the fact that, when G is K_v-anisotropic, G_{K_v} is compact (Theorem 3.1) and hence also profinite (cf. §3.3). Therefore G_{K_v} has a base of neighborhoods of the identity consisting of normal subgroups, and one cannot even speak of G_{K_v} being simple. Moreover, if N is an open normal subgroup of G_{K_v} (as is any noncentral normal subgroup of G_{K_v}, cf. Theorem 3.3), then $N_1 = N \cap G_K$ is a normal subgroup of G_K. In addition, the fact that G has weak approximation (Proposition 7.9) implies that $G_{K_v} = NG_K$; hence $G_{K_v}/N \simeq G_K/N_1$. Thus, the intersection of G_K with any proper, noncentral normal subgroup of G_{K_v} is a proper normal subgroup of G_K. Note, by Proposition 3.17, that N has finite index in

[1] Note that in the theorems presented below, we consider projective simplicity in a stronger sense, namely as the absence of proper noncentral normal subgroups. However, this formulation of the concept seems to be more elegant.

G_{K_v} and therefore N_1 is always infinite; hence the conditions given in Conjecture 9.1 are necessary for G_K to be projectively simple.

Moreover, if the conditions of Conjecture 9.1 are not satisfied, then it follows from the above that G_K, as well as G_{K_v}, has a system of normal subgroups $\mathfrak{N} = \{N\}$ of finite index, such that $\bigcap_{N\in\mathfrak{N}} N = (1)$, i.e., G_K is residually finite. This above argument can be sharpened as follows. If G is K_v-anisotropic for v in V_f^K, then $G \simeq \mathbf{SL}_1(D)$ over K_v, where D is a finite-dimensional central division algebra over K_v (Theorem 6.5). But then $G_{K_v} \simeq SL_1(D)$ is prosolvable, by the results in §1.4.4. Therefore, when the conditions of Conjecture 9.1 are violated, G_K is approximated by normal subgroups of finite index with solvable quotients; in particular, $G_K \neq [G_K, G_K]$.

By the conjecture, if G is K_v-isotropic for all v in V_f^K (which is always the case if G belongs to a type other than A_n), then G_K is projectively simple. In general, consider $T = \{v \in V_f^K : G \text{ is } K_v\text{-anisotropic}\}$; it follows from Theorem 6.7 that T is always finite. If $T \neq \emptyset$, then, as we noted above, for any v in T, G_{K_v} has a base of neighborhoods of the identity consisting of normal subgroups, each of them intersecting G_K in a nontrivial normal subgroup of G_K. It is easy to see that the analogous assertion also holds if, instead of a single G_{K_v}, one considers the product $G_T = \prod_{v\in T} G_{K_v}$; namely, G_T has a base of the neighborhood of the identity consisting of normal subgroups, and each proper, open normal subgroup H of G_T yields a proper normal subgroup $N = G_K \cap H$ of G_K. Since G_{K_v} is isomorphic to a group of type $SL_1(D)$, for v in T, the results of §1.4.4 (in particular, Theorem 1.10) give a description of the normal subgroups in the local case. Therefore, one may say that the normal structure of G_K has been fully studied if one knows that all noncentral, normal subgroups of G_K can be obtained in the manner described above.

CONJECTURE 9.2 (MARGULIS [3]). *For any noncentral normal subgroup N of G_K one can find an open normal subgroup H of G_T such that $N = \delta^{-1}(H)$, where $\delta: G_K \to G_T$ is the diagonal embedding.*

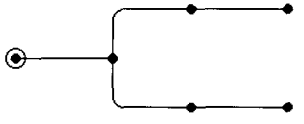
Conjecture 9.2 resembles the congruence subgroup problem for the groups of rational points, which we shall discuss in §9.5 for S-arithmetic groups. Note, also, that for $T = \emptyset$ (in particular, if G belongs to a type other than A_n) Conjectures 9.1 and 9.2 become equivalent.

The aim of this chapter is to set forth the current results on these conjectures. To begin with, we must distinguish two cases: when G is K-isotropic and when G is K-anisotropic. In the first one, analysis of the normal structure of G_K reduces to the question whether the Kneser-Tits conjecture (cf. §7.2) holds for G; for number fields we have the following,

almost definitive, result:

THEOREM 9.1. *Let G be a simple simply connected algebraic group defined over an algebraic number field K. Suppose G belongs to a type other than ${}^2E_6$. Then $G_K = G_K^+$, and consequently G_K has no proper noncentral normal subgroups.*

For the classical groups the main points in the proof of this theorem were set forth in §7.2. For the exceptional groups the argument requires verification case by case; and, by Theorem 7.4 it suffices to consider groups having K-rank equal to 1. Unfortunately, a complete exposition of this part of the proof has not yet been published (although Prasad-Raghunathan [3] promised one); nevertheless, it can be reconstructed with the help of Tits' lecture [4] at the Bourbaki seminar. The case of a K-form of type ${}^2E_6$ having K-rank equal to 1 with the Tits index



has not yet been studied.

Now let G be a simple simply connected K-anisotropic group. The most difficult groups to analyze are those of type A_n; at present (1989) for most outer forms of type A_n we have practically no results. Therefore, let us assume that G is an inner form of type A_n. Then $G = \mathbf{SL}_1(D)$, where D is a finite-dimensional central division algebra over K. In this case T, introduced before Conjecture 9.2, is the set of all v in V_f^K for which $D_v = D \otimes K_v$ remains a division algebra. Conjecture 9.2 has been fully solved only for quaternion skew fields.

THEOREM 9.2. *Let D be a quaternion skew field over K, and let $G = \mathbf{SL}_1(D)$. Then Conjecture 9.2 holds for G_K. In particular, if $T = \emptyset$, then G_K has no proper noncentral normal subgroups.*

(The conjecture on the projective simplicity of $SL_1(D)$, where D is a quaternion skew field, was set forth by Kneser [2] for $T = \emptyset$ and remained unproved for almost 25 years. The reader should also note that the groups mentioned in Theorem 9.2 comprise all the anisotropic groups of type A_1.)

At present, for division algebras of arbitrary index we have only the following partial result:

THEOREM 9.3. *Let N be a normal subgroup of G_K, satisfying Conjecture 9.2. Then Conjecture 9.2 also holds for the commutator group $[N, N]$.*

For the convenience of references, we state Theorem 9.3 separately for $N = G_K$.

THEOREM 9.4. *Conditions as above,*

$$[G_K, G_K] = G_K \cap \prod_{v \in T} [G_{K_v}, G_{K_v}].$$

In particular, if $T = \emptyset$, then $G_K = [G_K, G_K]$.

These theorems were actually proved in several stages. First, the authors [1] obtained a proof of Theorem 9.4 for the case where D is a quaternion skew field and $T = \emptyset$, developing the multiplicative arithmetic of quaternions. Using the latter, Margulis [4] then proved Theorem 9.2. Subsequently, the authors managed to generalize the methods and results of [1] to division algebras of arbitrary index. In other words, a multiplicative arithmetic of division algebras of arbitrary index was developed and applied to the proof of Theorem 9.4, with one small constraint: it was assumed that $v((n, 2)) = 0$ for v in T, where n is the index of D. Lastly, Raghunathan [7] proved that this condition is superfluous, and derived the more general Theorem 9.3 from Theorem 9.4.

We devote §9.2 to the proofs of Theorems 9.2–9.4, beginning with Theorem 9.4, whose proof is technically the most intricate. The arguments here follow the general scheme described in Platonov-Rapinchuk [4], with several modifications which, firstly, remove the previously imposed condition on D, and secondly, reduce the reliance on class field theory to a minimum. In particular, the version of the proof presented here does not use the Grünwald-Wang theorem, which in a somewhat generalized form plays a key role in the proof given by Raghunathan [7]. Then we derive Theorem 9.3 from Theorem 9.4. The argument we present is more direct than the original one used by Raghunathan [7] and is based on establishing a connection with the metaplectic problem, treated in §9.5. Lastly, following Margulis [4], we prove Theorem 9.2.

We devote §9.3 to the normal subgroup structure of groups of rational points of algebraic groups belonging to other classical types. The main result here can be stated as follows:

THEOREM 9.5. *Let G be a simple simply connected algebraic K-group belonging to one of the following types: B_l $(l \geq 2)$, C_l $(l \geq 2)$, D_l $(l \geq 4$, except for ${}^3D_4$ and ${}^6D_4)$; or the special unitary group $\mathbf{SU}_m(L, f)$ of a nondegenerate m-dimensional Hermitian form f over a quadratic extension L/K, having type ${}^2A_{m-1}$ $(m \geq 3)$. Then G_K has no proper noncentral normal subgroups; in particular, Conjecture 9.1 holds.*

This theorem has apparently not been published before in such complete form. Its proof evolved over more than three decades, from the work of Kneser [2] in 1956, to the present day. A key role in the argument is played

by the fact that the groups under consideration have a convenient geometric realization as groups of automorphisms of various vector spaces over a division algebra, endowed either with a Hermitian or a skew-Hermitian form. This approach was used by Kneser [2] to prove the projective simplicity of the groups of rational points of the spinor groups $G = \mathbf{Spin}(f)$ of nondegenerate quadratic forms in $n \geq 5$ variables, belonging to type $B_{\frac{n-1}{2}}$ for n odd and to type $D_{\frac{n}{2}}$ for n even. The case of groups of type C_l and of $\mathbf{SU}_m(L, f)$ of type ${}^2A_{m-1}$, related to a quadratic extension L/K and a nondegenerate Hermitian form f, was studied by Borovoi [1]. Later Chernousov [4] reduced the proof of Theorem 9.5 for groups of type D_l ($l \geq 4$) to groups of type $D_3 = A_3$. The definitive result for groups of type D_l was obtained independently by Tomanov [2] and Borovoi [3]. In this regard, Tomanov's arguments are direct analogs of those used by Kneser [2], whereas Borovoi's approach develops methods used in his earlier work [1]. A crucial observation is that the proof of Theorem 9.5 can be reduced not merely to groups of type $D_3 = A_3$, but actually to groups of this type which are isomorphic to $\mathbf{SU}_4(L, f)$; these groups were studied earlier. (Note that the argument in Chernousov [4] can also be carried through to the end with the help of this remark.)

We shall give a new proof of Theorem 9.5 which, although it uses several points from the works mentioned above (mostly Borovoi [1], [3]), differs from the previous proofs first and foremost in terms of its general nature and does not require treating each type separately. On the whole, the argument is inductive, with Theorem 9.2 providing the base of induction (recall that $B_1 = C_1 = A_1$ and $D_2 = A_1 + A_1$), the inductive step being justified by Theorem 9.13.

The method used in the proof of Theorem 9.5 can also be applied to non-classical groups. For instance, applying it to the 7-dimensional representation of a group of type G_2, we obtain the following result:

THEOREM 9.6. *Let G be a simple K-group of type G_2. Then G_K is projectively simple.*

We still have to consider groups of type E_6, E_7, E_8 and F_4. The analysis of these types is complicated by the fact that there are no convenient geometric realizations for groups of the E series. The proof of the projective simplicity of the groups of K-rational points of simple groups of the latter three types, obtained by Chernousov ([3], [5]), appeared rather unexpectedly. By applying several methods which he developed previously [2] in order to study the rationality of the varieties of real algebraic groups, Chernousov proved the following theorem.

THEOREM 9.7. *Let G be a simple simply connected algebraic groups of rank $l \geq 2$, defined and anisotropic over K, but split over a quadratic extension L/K. Then G_K has no proper, noncentral normal subgroups and, in particular, is projectively simple.*

Groups of all types except A_1 have K-forms to which one can apply Theorem 9.7. However, any K-group belonging to type B_l, C_l, E_7, E_8, F_4 or G_2 always splits over some quadratic extension of K (Proposition 6.17). Since it has already been shown that for K-isotropic groups of these types there are no noncentral normal subgroups of G_K (Theorem 9.1), Theorem 9.7 yields

COROLLARY. *The groups of K-rational points of simple simply connected groups of types B_l ($l \geq 2$), C_l ($l \geq 2$), E_7, E_8, F_4, and G_2 do not have proper noncentral normal subgroups.*

Thus, for groups of type B_l and C_l ($l \geq 2$) we obtain one more proof of the projective simplicity of G_K. In §9.4 we present a modified proof of Theorem 9.7. Like Chernousov's original proof (cf. [3],[5]), it is by induction on the rank l of the group under consideration, beginning with $l = 2$. Since there are only three types having rank 2 (namely, A_2, $B_2 = C_2$, and G_2), and since any K-anisotropic group of type A_2, split over a suitable quadratic extension L/K, is precisely $\mathbf{SU}_3(L, f)$, it follows that the starting point of the induction is given by Theorems 9.5 and 9.6.

In summary, aside from the case of groups of type A_l ($l \geq 2$), we see that at present Conjectures 9.1 and 9.2 are proved for all groups, except for the forms of type ${}^3D_4$, ${}^6D_4$ and E_6. Therefore, from this perspective, the main problem is to complete the analysis of groups of type A_l, both for inner forms, for which the known results are assembled in Theorems 9.2–9.4, as well as outer forms, for which analogous results have not yet been obtained.

Although the methods used in §§9.2–9.4 vary widely, approximation is used in all the proofs. Therefore, in this introductory section we present the following two results, which will be used repeatedly in the sequel.

Let G be a simple simply connected algebraic K-group, and let $T = \{ v \in V_f^K : G_{K_v} \text{ is } K_v\text{-anisotropic} \}$. For any noncentral normal subgroup N of G_K and any finite subset S of V^K, let N_S denote the closure of N in $G_S = \prod_{v \in S} G_{K_v}$.

LEMMA 9.1.

(1) *N_S is an open normal subgroup of G_S.*
(2) *$N_S = N_{T \cap S} \times G_{S \setminus (T \cap S)}$; in particular, if $T \cap S = \emptyset$, then $N_S = G_S$.*

PROOF: By Proposition 7.9, G_K is dense in G_S; therefore N_S is a normal subgroup of G_S. For v in S, there is a natural embedding of G_{K_v} in G_S, and one can consider $W_v = [N_S, G_{K_v}]$. Then clearly W_v is a normal subgroup

of G_{K_v}, and $W_v \not\subset Z(G_{K_v})$. Indeed, let x be a noncentral element in N, and let $\varphi: G \to G$ be the map given by $\varphi(g) = [x, g]$. Since $x \notin Z(G)$ and G is connected, the closure of the image of φ has positive dimension. But G_{K_v} is Zariski-dense in G (Theorem 2.2), so $\varphi(G_{K_v}) \subset W_v$ is infinite; in particular, $W_v \not\subset Z(G_{K_v})$.

Theorem 3.3 implies that W_v is open in G_{K_v}. On the other hand, since N_S is a normal subgroup, we have $W_v \subset N_S$ for any v in S; so $\prod_{v \in S} W_v \subset N_S$ and N_S is open. Now if $v \in S \setminus (T \cap S)$, then G_{K_v} has no noncentral normal subgroups; hence $W_v = G_{K_v} \subset N_S$, which means that $G_{S \setminus (T \cap S)} \subset N_S$. Now consider the projection of N_S on $G_{S \cap T}$. Its image is an open subgroup of $G_{S \cap T}$ and at the same time contains N as a dense subgroup; i.e., it coincides with $N_{S \cap T}$, and the lemma is proved.

LEMMA 9.2. *Notation as above, the following conditions are equivalent:*

(i) *N satisfies the congruence assertion in Conjecture 9.2;*
(ii) *N is open in G_K in the T-adic topology;*
(iii) *N is closed in G_K in the T-adic topology.*

PROOF: (i)⇒ (ii)⇒ (iii) are obvious, therefore we shall prove (iii) ⇒(i). As above, let N_T denote the closure of N in G_T. If follows from Lemma 9.1 that N_T is an open normal subgroup of G_T and therefore N is dense in $G_K \cap N_T$ in the T-adic topology of G_K. Then by (iii) we have $N = G_K \cap N_T$, which means that the congruence assertion of Conjecture 9.2 holds for N (with $H = N_T$). Lemma 9.2 is proved.

To conclude, we look at a qualitative aspect of the problem of the normal subgroup structure of groups of rational points. Theorem 3.1 implies that G_{K_v} is compact for each v in T; therefore G_T itself is compact. Now suppose the congruence assertion of Conjecture 9.2 holds for a normal subgroup N of G_K, i.e., that $N = G_K \cap H$ for some open normal subgroup H of G_T. Then, since G_T is compact, it follows immediately that $[G_T : H]$ is finite; hence also $[G_K : N]$ is finite. Since Conjecture 9.2 has not yet been proved, one naturally wonders whether *a priori* G_K could have noncentral normal subgroups of infinite index. The answer to this question is provided by the following

THEOREM 9.8 (PRASAD [1], MARGULIS [3]). *Let G be a simple simply connected algebraic K-group. Then any noncentral normal subgroup of G_K has finite index.*

With the help of the strong approximation theorem, the proof is easily obtained from the following general result.

THEOREM 9.9 (MARGULIS [3]). *Let Γ be an S-arithmetic subgroup of a simple algebraic K-group G, where S is a finite subset of V^K containing V_∞^K. If $\operatorname{rank}_S G = \sum_{v \in S} \operatorname{rank}_{K_v} G \geq 2$, then any normal subgroup of Γ either has finite index in Γ, or is contained in the center of G.*

Several special cases of Theorem 9.9 were known before Margulis [3] and had been proved by purely algebraic methods. For $\operatorname{rank}_K G \geq 2$, Theorem 9.9 was obtained by Raghunathan [4]. Apparently, by modifying Raghunathan's arguments, one can prove Theorem 9.9 for an arbitrary S-arithmetic subgroup of a K-isotropic group G for which $\operatorname{rank}_S G \geq 2$. However, such an approach cannot be applied in the K-anisotropic case. Margulis [3] uses arguments of an essentially different nature, based on the fact that Γ is a lattice of G_S (Theorem 5.7) and using deep results from measure theory and the theory of infinite-dimensional representations. Since these methods are not covered in our book, unfortunately we cannot present the proof of Theorem 9.9 here and must refer the reader to the original proof in Margulis [3].

Nevertheless, we shall show how Theorem 9.8 is derived from Theorem 9.9. We introduce a finite subset S of V^K, containing T and V_∞^K and satisfying the following conditions:

(i) $\operatorname{rank}_S G \geq 2$;
(ii) $N \cap G_{\mathcal{O}(S)}$ is not contained in $Z(G)$, the center of G.

Such an S can easily be constructed if we proceed from the following two facts:

(1) G is K_v isotropic, i.e., $\operatorname{rank}_{K_v}(G) \geq 1$, for almost all v in V_f^K;
(2) if $x \in N \setminus Z(G)$, then $x \in G_{\mathcal{O}(S)}$ for S sufficiently large.

Also, consider the diagonal embedding of G_K in the group G_{A_S} of S-adeles, and let $\bar{N}$ denote the closure of N in G_{A_S}. Then $\bar{N} = G_{A_S}$. Indeed, G_K is dense in G_{A_S} by the strong approximation theorem; hence $\bar{N}$ is a normal subgroup of G_{A_S}. For any $v \notin S$ there is a natural embedding of G_{K_v} in G_{A_S}, and the commutator subgroup $[G_{K_v}, \bar{N}]$ is contained in $\bar{N}$ and is a noncentral normal subgroup of G_{K_v}. But by assumption $v \notin T$, so G_{K_v} cannot have any proper noncentral normal subgroups (Theorem 7.6); hence $G_{K_v} \subset \bar{N}$. But it follows from the definition of the adele topology that the subgroup of G_{A_S} generated by all the G_{K_v} (where $v \notin S$) is dense; therefore, finally, $\bar{N} = G_{A_S}$. In particular,

$$G_{A_S} = N G_{A_S(S)} \tag{9.1}$$

where $G_{A_S(S)}$ is the group of S-integral adeles in G_{A_S}. From (9.1) we obtain that $G_K = N G_{\mathcal{O}(S)}$, from which it follows that $G_K / N \simeq G_{\mathcal{O}(S)} / N \cap G_{\mathcal{O}(S)}$.

It remains to note that by assumption $N \cap G_{\mathcal{O}(S)} \not\subset Z(G)$; thus the latter quotient group is finite, by (i) and Theorem 9.9. Therefore G_K/N is also finite and Theorem 9.8 is proved.

Note that Theorem 9.8 is essential in proving the theorems formulated above, in particular Theorems 9.2 and 9.5.

9.2. Groups of type A_n.

Throughout this section let G be a simple simply connected K-anisotropic group which is an inner form of type A_{n-1}. Thus, $G = \mathbf{SL}_1(D)$, where D is a finite-dimensional central division algebra over K of index n. Put $T = \{ v \in V_f^K : D_v = D \otimes_K K_v \text{ is a division algebra} \}$. As we noted in §9.1, what we know at present about the normal subgroups of G_K is summarized in Theorems 9.2–9.4; this section is devoted to the proofs of these theorems. Our arguments use approximation theorems for G and several norm properties of the maximal subfields of D; we shall begin our exposition with the latter.

The most technically intricate part of the proofs of Theorems 9.2–9.4 lies in the following assertion, for which we introduce the following notation. Fix an arbitrary noncentral normal subgroup N of $G_K = SL_1(D)$, and for x in D^* let $\Omega(x)$ denote the subgroup of D^* generated by the multiplicative groups of all the maximal subfields of D^* of the form $K(xz)$, where $z \in N$. Furthermore, let N_T be the closure of N in G_T, and let $\Omega_T(x)$ be the subgroup of $D_T^* = \prod_{v \in T} D_v^*$ generated by the products $\prod_{v \in T} K_v[xz_v]^*$ for which $\bar{z} = (z_v) \in N_T$ and $K_v[xz_v]$ is a maximal semisimple commutative subalgebra of D_v for all v in T.

THEOREM 9.10. $\mathrm{Nrd}_{D/K}(\Omega(x)) = \mathrm{Nrd}_{D/K}(D^*) \cap \mathrm{Nrd}_{D_T/K_T}(\Omega_T(x))$ *(here* Nrd_{D_T/K_T} *denotes the product of the maps* Nrd_{D_v/K_v} *for* v *in* T*).*

First we show how Theorem 9.10 is derived from the following

PROPOSITION 9.1. *Put* $T_0 = \{ v \in V_f^K : D_v \not\simeq M_n(K_v) \}$. *Then*

$$\mathrm{Nrd}_{D/K}(D^*) \cap \prod_{v \in T_0} K_v^{*m} \subset \mathrm{Nrd}_{D/K}(\Omega(x)),$$

for any x *in* D^*, *where* $m = n!$.

We shall need two lemmas.

LEMMA 9.3. *Let* $v \in V^K$, $x \in D_v^*$, *and let* H *be a maximal semisimple commutative subalgebra of* D_v. *If* $\mathrm{Nrd}_{D_v/K_v}(x) \in \mathrm{Nrd}_{D_v/K_v}(H^*)$, *then* $H = K_v[xz]$ *for suitable* z *in* G_{K_v}. *In particular,*

(1) *if* $D_v \simeq M_n(K_v)$, *then there exists* z *in* G_{K_v} *such that* $K_v[xz] \simeq K_v^n$;

(2) *if* $v \in V_f^K \setminus T$, *then there exists* z *in* G_{K_v} *such that*

$$\mathrm{Nrd}_{D_v/K_v}(K_v[xz]^*) = K_v^*.$$

PROOF: We use the following fact: if $y \in H^*$, then for any open subgroup R of G_{K_v} there is z in $R \cap H$ satisfying $H = K[yz]$. For the proof, let B denote the maximal K_v-torus of $\mathbf{GL}_1(D)$ corresponding to H, and let W be the set of regular elements in B; then W is Zariski-open in B (cf. §2.1.11). Since $B = B_1 B_2$, where $B_1 = \mathbb{G}_m$ and $B_2 = B \cap G$, it follows that $W(y) = \{ b \in B_2 : yb \in W \}$ is nonempty and open in B_2, for any y in B. On the other hand, $B_2 \cap R$ is an open subgroup of B_{2K_v} in the v-adic topology; hence it is Zariski-dense in B_2 (Lemma 3.2). Therefore, one can find z in $W(y) \cap R$, which will be the desired element.

The first assertion of the lemma and (1) are immediate; to prove (2) it remains to construct a maximal semisimple commutative subalgebra H of D_v satisfying $\mathrm{Nrd}_{D_v/K_v}(H^*) = K_v^*$. To do so, write $D_v = M_l(\Delta)$, where Δ is a division algebra over K_v. Since $v \in V_f^K \setminus T$, we have $l > 1$ and one can consider the algebra $H = E \oplus P^{l-1}$, where E (resp., P) is a maximal unramified (resp. totally ramified) subfield of Δ. Then $\mathrm{Nrd}_{D_v/K_v}(H^*)$ contains $\mathrm{Nrd}_{\Delta/K_v}(E^*)$ and $\mathrm{Nrd}_{\Delta/K_v}(P^*)$. But the first of these groups contains the group of v-adic units U_v, and the second contains a uniformizing parameter of K_v, so in the end $\mathrm{Nrd}_{D_v/K_v}(H^*) = K_v^*$. The lemma is proved.

LEMMA 9.4. *Let* $x \in D^*$, *let* S *be a finite subset of* V^K, *and for each* v *in* S *fix a maximal semisimple commutative* K_v*-subalgebra* H_v *of* D_v. *Suppose there is* $\bar{z} = (z_v) \in N_S$ *satisfying* $K_v[xz_v] \simeq H_v$ *for all* v *in* S. *Then there is* z *in* N *such that* $K_v[xz] \simeq H_v$ *for all* v *in* S.

PROOF: Without loss of generality we may assume that $H_v = K_v[xz_v]$. It follows from the proof of Proposition 6.13 that the set Y_v, consisting of those y in D_v^* for which $K_v[y]$ is conjugate in D_v to H_v, is open in D_v^*. Then $Y = N_S \cap (\prod_{v \in S} x^{-1} Y_v)$ contains $\bar{z}$ and therefore is a nonempty, open subset of N_S. Hence $Y \cap N$ is nonempty, and any z in $Y \cap N$ will be the desired element. The lemma is proved.

Now let $a \in \mathrm{Nrd}_{D/K}(D^*) \cap \mathrm{Nrd}_{D_T/K_T}(\Omega_T(x))$. This means there exist $\bar{z}_1, \ldots, \bar{z}_r$ in N_T (where $\bar{z}_i = (z_{iv})$) such that $a = \mathrm{Nrd}_{D_T/K_T}(\bar{x}_1, \ldots, \bar{x}_r)$, where $\bar{x}_i \in \prod_{v \in T} K_v[xz_{iv}]^*$ and $K_v[xz_{iv}]$ is a maximal semisimple commutative subalgebra of D_v for all v in T, $(i = 1, \ldots, r)$. Using Lemma 9.4, we can find $z_1, \ldots, z_r$ in N such that $K_v[xz_i] \simeq K_v[xz_{iv}]$ for all v in T and all $i = 1, \ldots, r$. Then $\mathrm{Nrd}_{D_T/K_T}(\bar{x}_i) = \mathrm{Nrd}_{D_T/K_T}(x_i)$ for suitable x_i in

$\prod_{v\in T} K_v[xz_i]^*$. Furthermore, by Lemmas 9.1, 9.3 and 9.4 there is z_{r+1} in N such that $\mathrm{Nrd}_{D_v/K_v}(K_v[xz_{r+1}]^*) = K_v^*$ for all v in $T_0 \setminus T$. It follows from our definitions that there exist t_i in $Z_i = \prod_{v\in T_0} K_v[xz_i]^*$ $(i = 1, \dots, r+1)$ such that $a = \mathrm{Nrd}_{D_{T_0}/K_{T_0}}(t_1 \dots t_{r+1})$. Applying the weak approximation theorem to $K(xz_i)$, we find s_i in $K(xz_i)^* \cap t_i Z_i^m$. We have

$$a\,\mathrm{Nrd}_{D/K}(s_1 \dots s_{r+1})^{-1} \in \mathrm{Nrd}_{D/K}(D^*) \cap \prod_{v\in T_0} K_v^{*m},$$

which means that $a\,\mathrm{Nrd}_{D/K}(s_1 \dots s_{r+1})^{-1} \in \mathrm{Nrd}_{D/K}(\Omega(x))$, by Proposition 9.1. But then also $a \in \mathrm{Nrd}_{D/K}(\Omega(x))$, as desired.

Now we sketch the proof of Proposition 9.1. Let

$$a \in \mathrm{Nrd}_{D/K}(D^*) \cap \prod_{v\in T_0} K_v^{*m}.$$

It suffices to find z_1, z_2 in N such that $M_i = K(xz_i)$ are maximal subfields of D and $a \in N_{M_1/K}(M_1^*)N_{M_2/K}(M_2^*)$. We prove the latter inclusion by applying the multinorm principle (cf. §6.3) to the normal closures P_i of M_i in a given algebraic closure (then $L_i = P_i$, notation as in Proposition 6.11). To construct the $M_i = K(xz_i)$ in such a way that the conditions of Proposition 6.11 hold for the P_i, we need the following stronger version of Lemma 9.4

PROPOSITION 9.2 *Given an element x in D^*, a finite extension F of K, a finite subset S of V^K, and an element $\bar{z} = (z_v) \in N_S$ such that $K_v[xz_v]$ is a maximal semisimple commutative subalgebra of D_v, for all v in S; then there exists z in N such that the following holds for the field $M = K(xz)$ and its normal closure P (in a given algebraic closure):*

(1) *$M \otimes_K K_v \simeq K[xz_v]$ for all v in S;*
(2) *$P \cap F = K$;*
(3) *P/K satisfies the Hasse norm principle.*

PROOF: Obtained by reducing to Lemma 9.4. Namely, we show that there exist a finite subset S_1 of $V_f^K \setminus ((V_f^K \cap S) \cup T_0)$ and, for each v in S_1, a maximal semisimple commutative subalgebra H_v of D_v such that $H_v = K_v[xz_v]$ for suitable z_v in G_{K_v}; and if $M \otimes_K K_v \simeq H_v$ for v in S_1, then conditions (2) and (3) hold. (Intuitively, we shall show that one can guarantee (2) and (3) by fixing a finite number of local conditions that are "independent" of the conditions stipulated in (1).) Then the existence of z in N with the requisite properties follows immediately from Lemma 9.4, for the application of which one must note that $\bar{z} = (z_v)_{v\in S\cup S_1}$ lies in $N_{S\cup S_1}$, by Lemma 9.1.

Condition (2) is the easiest to handle.

LEMMA 9.5. *For any finite subset S_0 of V^K and any finite extension F/K there exists a finite subset $S(F)$ of $V_f^K \setminus (V_f^K \cap S_0)$ such that, if $P \supset K$ and $P_w = K_v$ for all v in $S(F)$ and all $w|v$, then $P \cap F = K$.*

PROOF: We may assume without loss of generality that F/K is Galois. Consider a system of generators $\sigma_1, \dots, \sigma_r$ of $\mathrm{Gal}(F/K)$. By the Chebotarev density theorem, for each $i = 1, 2, \dots, r$ there is a v_i in $V_f^K \setminus (V_f^K \cap S_0)$ and its extension $\bar{v}_i$ to F such that the Frobenius automorphism $\mathrm{Fr}(F_{\bar{v}_i}/K_{v_i}) = \sigma$. Put $S(F) = \{v_1, \dots, v_r\}$. If $P \supset K$ and $E = P \cap F \neq K$, then there is an automorphism σ_i that acts nontrivially on E. Let w denote a valuation of P extending the restriction of $\bar{v}_i$ to E. Then $w|v_i$ and $P_w \neq K_v$, since σ_i in $\mathrm{Gal}(F_{\bar{v}_i}/K_{v_i})$ is not the identity on $E_{\bar{v}_i}$; consequently $E_{\bar{v}_i} \neq K_{v_i}$. The lemma is proved by contradiction.

Let us choose $S(F)$ as constructed in Lemma 9.5 so that it is not in $S_0 = T_0 \cup S$. Then, on the one hand, for any v in $S(F)$ there exists z_v in G_{K_v} satisfying $K_v[xz_v] \simeq K_v^n$ (Lemma 9.3 (1)); on the other hand, if $M \otimes_K K_v \simeq K_v^n$ for all v in $S(F)$, then the normal closure P of M satisfies $P_w = K_v$ whenever $v \in S(F)$ and $w|v$; hence $P \cap F = K$, i.e., condition (2) is satisfied.

It remains to dispose of condition (3). By Theorem 6.11, the Hasse principle holds for a Galois extension P/K with Galois group $\mathcal{G}$ if and only if the canonical map

$$H^3(\mathcal{G}, \mathbb{Z}) \to \prod_v H^3(\mathcal{G}_v, \mathbb{Z})$$

is injective (where $\mathcal{G}_v$ is the decomposition group of an extension of v). Since in our case P is a normal closure of an extension of degree n, we see that $\mathcal{G}$ is isomorphic to a subgroup of the symmetric group S_n, and consequently it follows from Lemma 1.2 that P/K always satisfies the Hasse principle whenever $n \leq 3$. Therefore, below we assume that $n \geq 4$.

Choose any two valuations v_1 and v_2 in $V_f^K \setminus (S \cup T_0 \cup S(F))$, and consider the following maximal semisimple commutative subalgebras $H_{v_i} \subset D_{v_i} \simeq M_n(K_{v_i})$:

$$\begin{aligned} H_{v_1} &= E \oplus K_{v_1} \\ H_{v_2} &= R_1 \oplus R_2 \oplus K_{v_2}^{(n-4)}, \end{aligned} \tag{9.2}$$

where E is an unramified extension of K_{v_1} of degree $n-1$, and R_1, R_2 are unramified and totally ramified quadratic extensions of K_{v_2}, respectively. Clearly $\mathrm{Nrd}_{D_{v_i}/K_{v_i}}(H_{v_i}^*) = K_{v_i}^*$ for $i = 1, 2$; therefore Lemma 9.3 implies that there exist z_i in $G_{K_{v_i}}$ such that $H_{v_i} = K_{v_i}[xz_i]$.

We shall show that if M is an extension of K of degree n such that $M \otimes_K K_{v_i} \simeq H_{v_i}$ for $i = 1, 2$, then the Hasse principle holds for P/K. First we compute $\mathcal{G} = \mathrm{Gal}(P/K)$. Let f be an irreducible polynomial of degree n determining M/K. The action of $\mathcal{G}$ on the roots of f gives an injective homomorphism $\theta: \mathcal{G} \to S_n$ to the symmetric group; moreover, in view of the irreducibility of f, the image of $\theta(\mathcal{G})$ is a transitive subgroup. It follows from (9.2) that we have $P_{w_1} = E$ for $w_1|v_1$; so the splitting group $\mathcal{G}(w_1)$ is a cyclic subgroup of order $n-1$, and under θ any of its generators passes to a cycle of length $n-1$. Similarly, for $w_2|v_2$ we have $P_{w_2} = R_1 R_2$; consequently $\mathcal{G}(w_2)$ is the direct product of two cyclic groups of order 2, whose generators pass under θ to two permutations.

Thus $\theta(\mathcal{G})$ is a transitive subgroup of S_n containing a cycle of length $n-1$ and a permutation, so $\theta(\mathcal{G}) = S_n$. (Cf. van der Waerden [1].) Then it follows from Lemma 1.2 and the description of $\mathcal{G}(w_2)$ that $H^3(\mathcal{G}, \mathbb{Z}) \to H^3(\mathcal{G}(w_2), \mathbb{Z})$ is injective, and consequently the Hasse principle holds for P/K. This completes the proof of Proposition 9.2.

Now we complete the proof of Proposition 9.1. Let

$$a \in \mathrm{Nrd}_{D/K}(D^*) \cap \prod_{v \in T_0} K_v^{*m};$$

we shall show that $a \in \mathrm{Nrd}_{D/K}(K(xz_1)^* K(xz_2)^*)$ for suitable z_i in N such that the $M_i = K(xz_i)$ are maximal subfields of D. Choose an element z_1 in N such that the following conditions hold:

- (1_1) $K_v[xz_1] \simeq K_v^n$ for v in $V(a) \setminus (V(a) \cap T_0)$ (recall that $V(a) = \{ v \in V_f^K : v(a) \neq 0 \}$);
- (2_1) the Hasse principle holds for the normal closure P_1 of $M_1 = K(xz_1)$
- (3_1) $a \in N_{P_{1w}/K_v}(P_{1w}^*)$ for $w|v$ in V_∞^K.

The existence of such a z_1 follows from Lemmas 9.1 and 9.3 and Proposition 9.2. More precisely, for $S = (V(a) \setminus (V(a) \cap T_0)) \cup (V_\infty^K \setminus T_\infty)$ where $T_\infty = \{ v \in V_\infty^K : D_v \not\simeq M_n(K_v) \}$, Lemmas 9.1 and 9.3 imply the existence of $z = (z_v)$ in N_S, such that $K_v[xz_v] \simeq K_v^n$ for all v in S. Then, applying Proposition 9.2, we can find z_1 in N satisfying conditions (1) and (2), and moreover $K_v[xz_1] \simeq K_v^n$ for v in $V_\infty^K \setminus T_\infty$. With the latter fact, we verify condition (3). For v in $V_\infty^K \setminus T_\infty$ we have $P_{1w} = K_v$, and obviously (3) holds. But if $v \in T_\infty$, then noting $K_v = \mathbb{R}$ and $P_{1w} = \mathbb{C}$, we have $a > 0$ in K_v, since $a \in \mathrm{Nrd}_{D_v/K_v}(D_v^*)$; therefore $a \in N_{P_{1w}/K_v}(P_{1w}^*)$.

Furthermore, one can choose z_2 in N satisfying the following conditions:

- (1_2) $K_v[xz_2] \simeq K_v^n$ for all v in $V_f^K \setminus T_0$ such that P_{1w}/K_v is ramified;
- (2_2) the normal closure P_2 of $M_2 = K(xz_2)$ satisfies $P_1 \cap P_2 = K$.

One can see as above that such a z_2 exists.

Let us show that $a \in N_{M_1/K}(M_1^*) N_{M_2/K}(M_2^*)$. In fact, in our case we shall prove the stronger assertion that $a \in N_{P_1/K}(P_1^*) N_{P_2/K}(P_2^*)$. By Proposition 6.11, in view of conditions (2_1) and (2_2), it suffices to show that

$$a \in N_{P_1/K}(J_{P_1}) N_{P_2/K}(J_{P_2}).$$

(Note that $L_i = P_i$ in the notation of Proposition 6.11.) If $v \in V_f^K \setminus V(a)$ and P_{1w}/K_v is unramified, then a is a norm of the w-adic unit of P_{1w}. Therefore, in view of (3_1), it remains to verify

$$a \in N_{P_{1w}/K_v}(P_{1w}) N_{P_{2w}/K_v}(P_{2w}) \tag{9.3}$$

for $w|v$ in V_f^K such that either $v \in V(a)$ or P_{1w}/K_v is ramified. If in addition $v \in T_0$, then by assumption $a \in K_v^{*m}$ and (2) obviously holds, since $[P_{1w} : K_v]$ divides $m = n!$. But if $v \notin T_0$, then by assumption either $P_{1w} = K_v$ or $P_{2w} = K_v$ respectively, and again (9.3) is satisfied. This completes the proof of Proposition 9.2.

A general remark is in order. If N is a noncentral normal subgroup of G_K, then $d = [G_K : N]$ is finite by Theorem 9.8. In this case the subgroup N_0 of G_K generated by $\{ x^d : x \in G_K \}$ is contained in N and is a normal subgroup of D^*. Moreover, as follows from Lemma 9.2 for example, if Conjecture 9.2 holds for N_0, then it also holds for N. Therefore, henceforth we shall only consider those normal subgroups of G_K that are normal subgroups of D^*.

Let $N \subset G_K$ be a noncentral normal subgroup of D^*. For x in D^*, put $Z(x) = \{ u \in D^* : uxu^{-1}x^{-1} \in N \}$.

LEMMA 9.6. $\Omega(x) \subset Z(x)$. *Consequently, for any x and y in D^* and any a in $\Omega(x)$ and b in $\Omega(y)$, we have*

$$[x, y] \equiv [x, ya] \equiv [xb, y],$$

where $[x, y] = xyx^{-1}y^{-1}$ and $\equiv$ denotes equivalence modulo N.

Indeed, it suffices to show that $K(xz)^* \subset Z(x)$ for any z in N. Let $u \in K(xz)^*$. Then, since N is a normal subgroup of D^*, we have $[u, x] \equiv [u, xz] = 1$, as desired. Furthermore, since $Z(x) = Z(x^{-1})$, it follows that

$$[x, ya] = xyax^{-1}a^{-1}y^{-1} \equiv xyx^{-1}y^{-1} = [x, y].$$

Similarly, $[xb, y] = xbyb^{-1}x^{-1}y^{-1} \equiv [x, y]$, and Lemma 9.6 is proved.

We must introduce some additional notation. Put $\tilde{N}_T = N_T \prod_{v \in T} K_v^*$. Applying Corollary 1 of Proposition 3.3 to $\psi : \mathbb{G}_m \times G \to \mathbf{GL}_1(D)$, the

product map, we see that the map $K_v^* \times G_{K_v} \to D_v^*$ is open for any v in V^K. Therefore, since $N_T \subset G_T$ is open (cf. proof of Lemma 9.1), we see that $\tilde{N}_T$ is an open normal subgroup of $D_T^* = \prod_{v \in T} D_v^*$. It follows that in the T-adic topology $\tilde{N} = D^* \cap \tilde{N}_T$ and $\bar{N} = G_K \cap N_T$ are open subgroups of D^* and G_K respectively, and that they are normalized by D^*.

PROPOSITION 9.3. *Let $N \subset G_K$ be a noncentral normal subgroup of D^*, and let $x \in \tilde{N}$. Then $Z(x)\bar{N} = D^*$.*

PROOF: First we show that $G_K \subset Z(x)\bar{N}$. Let P be an arbitrary maximal subfield of D such that the P_v/K_v are unramified for all v in T, and let $S = \mathbf{R}_{P/K}(\mathbb{G}_m)$ be the corresponding maximal torus of $H = \mathbf{GL}_1(D)$. Let W denote the set of regular elements in S. Using Proposition 3.3 one can easily verify that for any v in V^K the map $\varphi_v \colon D_v^* \times W_{K_v} \to D_v^*$ given by $\varphi_v(g, x) = gxg^{-1}$ is open; so also $\varphi_T = \prod \varphi_v \colon D_T^* \times W_T \to D_T^*$ is open.

Thus, if we take a descending chain $U_1 \supset U_2 \supset \dots$ of open subgroups of D_T^* converging to 1, then $B_r = \varphi_T(U_r, W_T)$ is open in D_T^*, for each $r \geq 1$. Since NK^* is obviously dense in $\tilde{N}_T$, the set $x^{-1}B_r$ should intersect NK^*, for any $r \geq 1$. It follows that there exist y_r in N and u_r in U_r such that $u_r(S_r)_T u_r^{-1} = S_T$, where $S_r = Z_H(xy_r)$ is the centralizer of the regular element xy_r. Let $P_r = K(xz_r)$. Clearly S_r has the form $\mathbf{R}_{P_r/K}(\mathbb{G}_m)$, and the P_{r_v}/K_v are unramified for all v in T. Therefore, Proposition 7.8 implies that the corresponding norm tori $S_r^{(1)} = S_r \cap G$ do have weak approximation relative to T. In particular, for any z in $S_K^{(1)}$ one can find z_r in $(u_r^{-1} z u_r) N_T \cap (S_r^{(1)})_K$. Then

$$z^{-1} z_r \in G_K \cap ((z^{-1} u_r^{-1} z u_r) N_T) = G_K \cap N_T = \bar{N}$$

for sufficiently large r, since $u_r \to 1$ and N_T is open in G_T. On the other hand, $z_r \in \Omega(x) \subset Z(x)$; hence $z \in Z(x)\bar{N}$, which means $S_K^{(1)} \subset Z(x)\bar{N}$. Note that for P one can take an arbitrary maximal subfield of D such that all the P_v/K_v $(v \in T)$ are unramified; therefore it remains to show that together all possible $S_K^{(1)}$'s generate G_K. To simplify the notation, put $P^{(1)} = S_K^{(1)}$ and let B denote the subgroup of G_K generated by the various $P^{(1)}$, for all P in D having the specified properties. Also, for v in T, let Δ_v denote the set of those z in G_{K_v} for which $K_v[z]$ is a maximal unramified subfield of D_v. Then Δ_v is open in G_{K_v}, and one can easily deduce from Theorem 1.8 that Δ_v generates G_{K_v}. It follows that $\Delta = \prod_{v \in T} \Delta_v$ is open in G_T and generates G_T.

LEMMA 9.7. *Let Γ be a dense subgroup of a topological group Φ, and let U be an open subset of Φ. Then the subgroup generated by $\Gamma \cap U$ is $\Gamma \cap W$, where W is the subgroup (algebraically) generated by U.*

PROOF: An easy exercise for the reader.

Since G_K is dense in G_T, it follows from Lemma 9.7 that the subgroup of G_K generated by $G_K \cap \Delta$ is G_K. However, by assumption, for any z in $G_K \cap \Delta$ the algebra $K_v[z]$ is an unramified extension of K_v of degree n for all v in T; i.e., $P = K[z]$ satisfies the required properties, and hence $P^{(1)} \subset B$. Thus, $G_K \cap \Delta \subset B$ and $G_K = B \subset Z(x)\bar{N}$.

Now all we need to complete the proof of Proposition 9.3 is to show that $\mathrm{Nrd}_{D/K}(Z(x)) = \mathrm{Nrd}_{D/K}(D^*)$. In view of $\Omega(x) \subset Z(x)$, it suffices to establish by Theorem 9.10 that $\Omega_T(x) = D_T^*$ for each x in $\tilde{N}$. But it follows from the definition of $\tilde{N}$ that in the given case, for any choice of maximal semisimple commutative subalgebras H_v of D_v $(v \in T)$, there is an element $\bar{z} = (z_v) \in N_T$ such that $K[xz_v] \simeq H_v$, yielding the desired result.

Proposition 9.3 is proved.

COROLLARY. *If $\bar{N}/N$ is abelian, then $\tilde{N}/N$ lies in the center of D^*/N.*

Indeed, let $x \in D^*$ and $y \in \tilde{N}$. Since $D^* = \bar{N}Z(y)$ by Proposition 9.3, we have $[x, y] \equiv [s, y]$ for suitable s in $\bar{N}$. Symmetrically, using the factorization $D^* = \bar{N}Z(s)$, we obtain that $[x, y] \equiv [s, t]$ for suitable s and t in $\bar{N}$. But since $\bar{N}/N$ is abelian, it follows that $[s, t] \equiv 1$ and hence $[x, y] \equiv 1$, i.e., x centralizes y modulo N.

Having completed these preliminaries, we proceed directly to the proof of Theorems 9.2–9.4.

PROOF OF THEOREM 9.4: A crucial role in the proof is played by

THEOREM 9.11 (CONGRUENCE THEOREM). *Let*

$$x \in U = \{\, x \in D^* : \mathrm{Nrd}_{D/K}(x) \in U_v,\ \forall v \in T \,\},$$

and let $y \in D^*$. Suppose $x \in U_v(1 + \mathfrak{P}_v)$ for all v in $T \cap V(\mathrm{Nrd}_{D/K}(y))$, where $\mathfrak{P}_v$ is the valuation ideal in D_v (cf. 1.4). Then $[x, y] = xyx^{-1}y^{-1} \in [G_K, G_K]$. In particular, $[U, U] = [G_K, G_K]$.

First we shall prove Theorem 9.4, assuming that Theorem 9.11 is known. The proof is based on the following natural idea: since $G_K = [D^*, D^*]$ (Theorem 2.14), using a presentation of z in $G_K \cap \prod_{v \in T} [G_{K_v}, G_{K_v}]$ as the product of group commutators, one can try to replace z by an element of zN, where $N = [G_K, G_K]$, which can be expressed in terms of group commutators of the form described in Theorem 9.11; then $z \in [G_K, G_K]$. Throughout the proof of Theorem 9.4, N denotes $[G_K, G_K]$, and the notation $z_1 \equiv z_2$ indicates the fact that $z_1^{-1} z_2 \in [G_K, G_K]$. Also note that for any finite subset S of V^K we have $N_S = \prod_{v \in S} N_v$, where $N_v = [G_{K_v}, G_{K_v}]$, and that $N_v = G_{K_v}$ for $v \notin T$.

LEMMA 9.8. *Any element of G_K is the product of group commutators of the form $[x, y]$, where $x \in U$ and $y \in D^*$.*

PROOF: Since $G_K = [D^*, D^*]$, it suffices to show that any commutator $[x, y]$ $(x, y \in D^*)$ can be written as the product of group commutators of the specified form. Let F be a maximal subfield of D such that F_v/K_v is totally ramified for each v in T. Then $v(\mathrm{Nrd}_{D_v/K_v}(F_v^*)) = \mathbb{Z}$, and therefore, applying the weak approximation theorem to F, one can find s and t in F satisfying

$$\begin{aligned} v(\mathrm{Nrd}_{D/K}(s)) &= v(\mathrm{Nrd}_{D/K}(x)) \\ v(\mathrm{Nrd}_{D/K}(t)) &= v(\mathrm{Nrd}_{D/K}(y)) \end{aligned} \tag{9.4}$$

for all v in T. In view of (9.4), one has $x_0 = xs^{-1}$, $y_0 = yt^{-1} \in U$. Then the lemma follows immediately from the relation:

$$[x, y] = [x_0, t][tx_0t^{-1}, sy_0s^{-1}][y_0^{-1}, y_0sy_0^{-1}].$$

As before, let F denote a maximal subfield of D such that F_v/K_v is totally ramified for all v in T. Furthermore, choose t in F^* satisfying $v(\mathrm{Nrd}_{D/K}(t)) = 1$ for all v in T. Then t is a uniformizing parameter of D_v, for any v in T.

PROPOSITION 9.4. *For any z in G_K one can find x in U such that $z \equiv [x, t]$.*

PROOF: For x and y in U and any s in D^* we have

$$[xy, s] = xysy^{-1}x^{-1}s^{-1} = x[y, s](sx^{-1}s^{-1}) \equiv [x, s][y, s], \tag{9.5}$$

since $[y, s]$ and $sx^{-1}s^{-1}$ lie in U and hence, by the congruence theorem, commute modulo N. Therefore, in view of Lemma 9.8, it suffices to show that any $[a, b]$ where $a \in U$ and $b \in D^*$ is equivalent to $[x, t]$ for suitable x in U.

Let $T = \{v_1, \ldots, v_d\}$. The weak approximation theorem for $K(a)$ implies that there exist $a_1, \ldots, a_d$ in U such that $a = a_1 \ldots a_d$ and

$$\begin{aligned} a_i &\equiv a \pmod{\mathfrak{P}_{v_i}} \\ a_i &\equiv 1 \pmod{\mathfrak{P}_{v_j}}, \quad j \neq i \end{aligned}$$

for all $i = 1, \ldots, d$. Then, by (9.5)

$$[a, b] \equiv [a_1, b] \ldots [a_d, b]. \tag{9.6}$$

Furthermore, putting $\alpha_i = v_i(\mathrm{Nrd}_{D/K}(b))$ we obtain

$$[a_i, b] = a_i t^{\alpha_i}(t^{-\alpha_i}b)a_i^{-1}b^{-1} \equiv [a_i, t^{\alpha_i}], \tag{9.7}$$

since by assumption $T \cap V(\mathrm{Nrd}_{D/K}(t^{-\alpha_i}b)) \subset T \setminus \{v_i\}$; so $a_i \equiv a \pmod{\mathfrak{P}_v}$ for v in $T \cap V(\mathrm{Nrd}_{D/K}(t^{-\alpha_i}b))$, and by the congruence theorem a_i and $t^{-\alpha_i}b$ commute modulo N. In view of (9.6) and (9.7), to complete the argument we have to show that any $[a, t^\alpha]$, where $a \in U$ and $\alpha \in \mathbb{Z}$, is equivalent to a commutator of the form $[d, t]$ for suitable d in U.

For $\alpha > 0$, put $d = \prod_{i=0}^{\alpha-1}(t^iat^{-i}) = a(ta)^{\alpha-1}t^{-(\alpha-1)} \in U$. Then, with (9.5) we obtain

$$[d, t] \equiv \prod_{i=0}^{\alpha-1}[t^iat^{-i}, t] = \prod_{i=0}^{\alpha-1}(t^iata^{-1}t^{-(i+1)}) = [a, t^\alpha].$$

Similarly, assuming that $\alpha < 0$ and putting

$$d = \prod_{i=\alpha}^{-1}(t^ia^{-1}t^{-i}) = t^\alpha(a^{-1}t)^{-\alpha} \in U,$$

we obtain

$$[d, t] = \prod_{i=\alpha}^{-1}[t^ia^{-1}t^{-i}, t] = \prod_{i=\alpha}^{-1}(t^ia^{-1}tat^{-(i+1)}) = t^\alpha a^{-1}t^{-\alpha}a \equiv [a, t^\alpha],$$

since a and $t^\alpha a^{-1}t^{-\alpha}$ lie in U and hence commute modulo N. Proposition 9.4 is proved.

Now we complete the proof of Theorem 9.4. Let $z \in G_K \cap \prod_{v \in T}[G_{K_v}, G_{K_v}]$. Using Proposition 9.4, choose x in U such that $z \equiv [x, t]$. Since

$$[G_{K_v}, G_{K_v}] = G_{K_v} \cap (1 + \mathfrak{P}_v) \quad \text{for } v \text{ in } T \text{ (Theorem 1.9)},$$

the inclusion $[x, t] \in [G_{K_v}, G_{K_v}]$ yields

$$txt^{-1} \equiv x \pmod{\mathfrak{P}_v} \quad \text{for any } v \text{ in } T. \tag{9.8}$$

But we know (cf. §1.4.1) that in our case the residue field $d_v = \mathcal{O}_{D_v}/\mathfrak{P}_v$ is commutative and is a Galois extension of the residue field k_v; moreover, the automorphism induced by $\mathrm{Int}\, t$ generates the entire Galois group $\mathrm{Gal}(d_v/k_v)$. Therefore (9.8) implies that the residue $\bar{x}$ of x falls in k_v, i.e.,

$$x \in U_v(1 + \mathfrak{P}_v).$$

Since the latter inclusion holds for all v in T, by the congruence theorem we have $[x, t] \in N$, and then also $z \in N$. Q.E.D.

PROOF OF THE CONGRUENCE THEOREM: We begin with the second assertion, namely, that $[U, U] = [G_K, G_K]$. Bearing in mind that $[x, y] \equiv [x, ya] \equiv [xb, y]$ for a in $\Omega(x)$ and b in $\Omega(y)$ (Lemma 9.6), we see easily that the above assertion follows from

LEMMA 9.9. *If $x \in U$, then* $\mathrm{Nrd}_{D/K}(\Omega(x)) \supset \mathrm{Nrd}_{D/K}(U)$.

PROOF: By Theorem 9.10, it suffices to show that

$$\prod_{v \in T} U_v \subset \mathrm{Nrd}_{D_T/K_T}(\Omega_T(x)).$$

Since $N_T = \prod_{v \in T} N_v$, clearly $\Omega_T(x) = \prod_{v \in T} \Omega_v(x)$, where $\Omega_v(x)$ is the subgroup of D_v^* generated by the multiplicative groups of the maximal subfields of the form $K_v(xz)$, $z \in N_v$. It suffices to establish that among these subfields there is a maximal unramified subfield $L \subset D_v$, since then by Proposition 1.2 $U_v \subset N_{L/K_v}(L^*) = \mathrm{Nrd}_{D_v/K_v}(L^*)$. By assumption $\mathrm{Nrd}_{D/K}(x) \in U_v$, so it follows that $x \in L^* G_{K_v}$. Furthermore, Theorem 1.8 implies that $G_{K_v} = L^{(1)} N_v$, where $L^{(1)} = \{x \in L^* : N_{L/K_v}(x) = 1\}$; hence $x \in L^* N_v$. But then $L = K[xz]$ for suitable z in N_v (cf. proof of Lemma 9.3). Lemma 9.9 is proved.

To establish the first assertion of the congruence theorem we prove that under our conditions, $b = \mathrm{Nrd}_{D/K}(y) \in \mathrm{Nrd}_{D/K}(\Omega(x))$. By Theorem 9.10 it suffices to show that $b \in \mathrm{Nrd}_{D_T/K_T}(\Omega_T(x))$, where, notation as in Lemma 9.9, $\Omega_T(x) = \prod_{v \in T} \Omega_v(x)$. We have already seen that $b \in \Omega_v(x)$ if $v(b) = 0$. Otherwise, one has $x = st$, where $s \in U_v$ and $t \in 1 + \mathfrak{P}_v$; so $a = \mathrm{Nrd}_{D/K}(x) = s^n r$, where $r = \mathrm{Nrd}_{D_v/K_v}(t) \in 1 + \mathfrak{p}_v$. Let us show that then $b \in \mathrm{Nrd}_{D_v/K_v}(K_v[xz]^*)$, for suitable z in N_v. To do so, first we construct an extension L of K_v of degree n, satisfying $a, b \in N_{L/K_v}(L^*)$. Let p_v be the prime corresponding to v, and let $n = p_v^\alpha m$, where m is relatively prime to p_v.

LEMMA 9.10. *Let $b \in K_v^*$ and let m be an arbitrary integer ≥ 1. Then there exists an extension F/K_v of degree m such that $b \in N_{F/K_v}(F^*)$.*

PROOF: Left to the reader as an exercise. (Hint: reduce the problem to the case m prime. Furthermore, analyze $m = 2$ and m odd separately; in the second case it is useful to rely on the fact that if $b \notin K_v^{*m}$, then the polynomial $X^m - b$ is irreducible over K_v, cf. Lang [3].)

Let F be an extension of K_v of degree m such that $b = N_{F/K_v}(c)$, for suitable $c \in F^*$. Since $a = s^n \cdot r$, where $r \in 1 + \mathfrak{p}_v$, the fact that m and p_v are relatively prime implies that $a = d^m$, for some $d \in K_v^*$. We shall show that there is an extension L of F of degree $l = p_v^\alpha$ satisfying $c, d \in N_{L/F}(L^*)$.

It is well known (cf. §1.1.2) that $F^* \simeq \mathbb{Z} \times E \times \mathbb{Z}_{p_v}^\delta$, where E is the group of roots of unity in F and $\delta = [F : \mathbb{Q}_{p_v}]$. It follows that $F^*/F^{*l} \simeq (\mathbb{Z}/l\mathbb{Z})^{\delta+1} \times E/E^l$. If $\delta > 1$, then the subgroup generated by the images of

c and d in F^*/F^{*l} has index divisible by l; so there exists an open subgroup W of F^* of index l containing both c and d, and for L one can take the abelian extension of F of degree l with norm subgroup W, constructed via local class field theory. If $\delta = 1$ (i.e., $F = \mathbb{Q}_{p_v}$) and $p_v \neq 2$, then one can put $L = F(\sqrt[l]{p_v})$. Indeed, as the exercise below shows, L does not contain any abelian extensions of F and therefore, by local class field theory, $N_{L/F}(L^*) = F^*$.

EXERCISE: If $p \neq 2$, then $\mathbb{Q}_p(\sqrt[l]{p})$ $(l = p^\alpha)$ does not contain any abelian (or even any normal) extensions of $\mathbb{Q}_p$. (Hint: use induction on α. The case $\alpha = 0$ is obvious. Let $\alpha \geq 1$ and let $L \subset \mathbb{Q}_p(\sqrt[l]{p})$ be a Galois extension of $\mathbb{Q}_p$. Then $L \subset \mathbb{Q}_p(\sqrt[l]{p}) \cap \mathbb{Q}_p(\xi\sqrt[l]{p}) = \mathbb{Q}_p(\sqrt[p^{\alpha-1}]{p})$, where ξ is a primitive p-th root of unity, and one applies induction.)

We have yet to consider the case $p_v = 2$, i.e., $F = \mathbb{Q}_2$. Here $F^*/F^{*2} \simeq (\mathbb{Z}/2\mathbb{Z})^3$; therefore, arguing as above, we find a quadratic extension P/F such that $c = N_{P/F}(c')$ and $d = N_{P/F}(d')$ for suitable c' and d' in P. But by what we have seen there exists an extension M/P of degree $p_v^{\alpha-1}$ for which $c', d' \in N_{M/P}(M^*)$, and one can take $L = M$.

Thus, we have proved that there exists an extension L/K_v of degree n such that $a, b \in N_{L/K_v}(L^*)$. One can embed L in D_v as a maximal subfield, and it suffices to find z in N_v such that $L = K_v(xz)$. To do so, again write $x = st$, where $s \in U_v$ and $t \in 1 + \mathfrak{P}_v$. Since $a = \mathrm{Nrd}_{D/K}(x) \in N_{L/K_v}(L^*)$, it follows that

$$\mathrm{Nrd}_{D_v/K_v}(t) = s^{-n} a \in N_{L/K_v}(L^*) \cap (1 + \mathfrak{p}_v).$$

Therefore, by Proposition 9.13, $\mathrm{Nrd}_{D_v/K_v}(t) = N_{L/K_v}(g)$ for some g in $1 + \mathfrak{P}_L$, where $\mathfrak{P}_L$ is the valuation ideal of L. Then

$$z = t^{-1} g \in G_{K_v} \cap (1 + \mathfrak{P}_v) = N_v$$

and $xz = sg \in L$. It remains to modify xz, multiplying it by an element of $L^* \cap N_v$ in such a way that it generates all of L (cf. proof of Lemma 9.3). This completes the proof of the congruence theorem, as well as the proof of Theorem 9.4.

REMARK: If $T = \emptyset$, then by Theorem 9.4, G_K is its own commutator group; so one can ask about computing the commutator length of G_K, i.e., finding a minimal $l = l(G_K)$ such that any element of G_K can be written as the product of at most l commutators. In the proof of Theorem 9.4 for the case where D is a quaternion algebra and $T = \emptyset$ (cf. Platonov-Rapinchuk [1]), it was shown that $l(G_K) \leq 3$. No other estimates of the commutator length of G_K (or even a proof of its finiteness in the general case) are known.

Now we proceed to the proof of Theorem 9.3. By Lemma 9.2, it suffices to prove the following: if a normal subgroup F of G_K is open in the T-adic topology, then its commutator group $[F,F]$ is also open. First we consider the case where D is a quaternion algebra. Let τ denote the canonical involution on D. The restriction of τ to any maximal subfield of D induces a nontrivial automorphism; therefore by the Skolem-Noether theorem, for any x in D^*, one can find y in D^* such that $\tau(x) = yxy^{-1}$. However, $\mathrm{Nrd}_{D/K}(x) = x\tau(x)$; in particular, the elements of $G_K = SL_1(D)$ are characterized by $\tau(x) = x^{-1}$. Thus, for any x in G_K one has y in D^* satisfying $x^{-1} = yxy^{-1}$.

Now let F be an arbitrary subgroup of G_K, open in the T-adic topology. Then, for suitable $\alpha_v > 0$ $(v \in T)$, we have $F_0 = G_K \cap \prod_{v\in T}(1+\mathfrak{P}_v^{\alpha_v}) \subset F$, where $\mathfrak{P}_v$ is the valuation ideal of D_v. Clearly F_0 is a normal subgroup of D^*; and since $[F_0,F_0]$ is open, it follows that $[F,F]$ is open. Thus we may assume that F is a normal subgroup of D^*.

Put $N = [F,F]$ and let $\bar{N}$ and $\tilde{N}$ be as before (cf. p. 523). Since $\bar{N} \subset F$, the quotient group $\bar{N}/N$ is abelian; therefore $\tilde{N}/N$ lies in the center of D^*/N, by the corollary to Proposition 9.3. Let Z denote the set of elements of the form $x\tau(x)^{-1}$ $(x \in \tilde{N})$. We have noted that $\tau(x) = yxy^{-1}$ for suitable y in D^*; hence $Z \subset N$, since $\tilde{N}/N$ is central in D/N. Let us show, on the other hand, that $\tilde{N} \subset ZN$. To do so, it suffices to establish that Z is open in G_K in the T-adic topology, as we shall now show. By assumption $\tilde{N}$ is open in D^* in the T-adic topology; so $D^* \cap \prod_{v\in T}(1+\mathfrak{P}_v^{\beta_v}) \subset \tilde{N}$ for suitable integers $\beta_v > 0$ $(v \in T)$. Then the identity $x = \left(\frac{1+x}{2}\right)\tau\left(\frac{1+x}{2}\right)^{-1}$, which is true for any x in G_K, immediately implies that $G_K \cap \prod_{v\in T}(1+2\mathfrak{P}_v^{\beta_v}) \subset Z$, as desired.

The above argument can be carried over verbatim to the general case, provided one knows that, for any normal subgroup U of D^* open in the T-adic topology, $[U,D^*]$ is also open (for then $\bar{N} \subset [\tilde{N},D^*]N = N$). One can get information on $[U,D^*]$ from the initial segment

$$H^1(D^*/U) \to H^1(D^*) \to H^1(U)^{D^*} \to H^2(D^*/U) \to H^2(D^*) \tag{9.9}$$

of the Hochschild-Serre spectral sequence, arising from the extension

$$1 \to U \to D^* \to D^*/U \to 1,$$

where $H^i(*)$ denotes the i-th cohomology group with coefficients in $J = \mathbb{Q}/\mathbb{Z}$ viewed as a G-module with trivial action of G. We have

$$H^1(U)^{D^*} = \mathrm{Hom}(U/[U,D^*],J). \tag{9.10}$$

But by assumption $U = D^* \cap W$, where W is an open normal subgroup of D_T^* (coinciding with the closure of U), and one can consider the Hochschild-Serre sequence of continuous cohomology groups with coefficients in J endowed with the discrete topology:

$$H^1(D_T^*/W) \to H^1(D_T^*) \to H^1(W)^{D_T^*} \to H^2(D_T^*/W) \xrightarrow{\psi} H^2(D_T^*), \tag{9.11}$$

corresponding to the topological extension $1 \to W \to D_T^* \to D_T^*/W \to 1$. Viewing the cohomology in (9.9) as the continuous cohomology of discrete groups, we combine sequences (9.9) and (9.11) into the commutative diagram

$$\begin{array}{ccccccccc}
H^1(D^*/U) & \longrightarrow & H^1(D^*) & \xrightarrow{\varphi} & H^1(U)^{D^*} & \longrightarrow & H^2(D^*/U) & \longrightarrow & H^2(D^*) \\
\uparrow{\scriptstyle\alpha} & & \uparrow & & \uparrow{\scriptstyle\beta} & & \uparrow{\scriptstyle\gamma} & & \uparrow{\scriptstyle\delta} \\
H^1(D_T^*/W) & \longrightarrow & H^1(D_T^*) & \longrightarrow & H^1(W)^{D_T^*} & \longrightarrow & H^2(D_T^*/W) & \xrightarrow{\psi} & H^2(D_T^*),
\end{array}$$

in which the vertical arrows are the restriction maps. The weak approximation theorem for D^* implies that $D^*/U \simeq D_T^*/W$, i.e., α and γ are isomorphisms. If it were known that δ (or even its restriction to $\mathrm{Im}\,\psi$) is injective, then one could easily obtain from (9.11) that

$$H^1(U)^{D^*} = \mathrm{Im}\,\beta + \mathrm{Im}\,\varphi. \tag{9.12}$$

In terms of (9.10), any element of $\mathrm{Im}\,\beta + \mathrm{Im}\,\varphi$ induces the trivial homomorphism on $[D^*,D^*] \cap [W,D_T^*] = G_K \cap [W,D_T^*]$; therefore (9.12) implies $[U,D^*] = G_K \cap [W,D_T^*]$; in particular, $[U,D^*]$ is open.

Thus, if we could establish the injectivity of $\delta\colon H^2(D_T^*) \to H^2(D^*)$ (or even the injectivity of the restriction of δ to the image in $H^2(D_T^*)$ of $\varinjlim H^2(D_T^*/W)$ taken over all open normal subgroups W of D_T^*), then we would have a proof of Theorem 9.3 which does not rely on Theorem 9.4, and, in particular, we would have another proof of Theorem 9.4 itself. Thus, we see a connection between Theorem 9.3 and the problem of computing $\ker\delta$, which is naturally called the *weak metaplectic problem* (the terminology is related to the analogous concepts used in studying the congruence subgroup problem, cf. §9.5). This connection was first noted by Rapinchuk [6] in his analysis of the (strong) metaplectic problem. Unfortunately, we do not yet have a direct computation of $\ker\delta$, or even of $\ker\delta\,|_{\varinjlim H^2(D_T^*/W)}$; however, Rapinchuk [6] proved the triviality of the kernel of the corresponding map for G, i.e., $\theta\colon H^2(G_T) \to H^2(G_K)$, where, as above, one considers continuous cohomology groups with coefficients in J viewed as a discrete G-module

with the trivial action, and G_K is assumed to be endowed with the discrete topology. Rapinchuk [6] derived the triviality of $\ker\theta$ from Theorem 9.3, a proof of which was obtained by Raghunathan [7] in another way. Here we shall argue in the opposite direction, showing that Theorem 9.3 can be obtained from the triviality of $\ker\theta$ and using the following result.

THEOREM 9.12 (WEAK METAPLECTIC CONJECTURE) *Suppose $n > 2$. Then $\theta: H^2(G_T) \to H^2(G_K)$ is injective.*

The proof of Theorem 9.12, presented in §9.5 in connection with the congruence problem, uses results from Prasad-Raghunathan [5]. Theorem 9.12 also holds for $n = 2$, but then, as in Rapinchuk [6], the triviality of $\ker\theta$ must be derived from Theorem 9.3, which has already been proved for quaternion algebras.

For $n > 2$, the derivation of Theorem 9.3 from Theorem 9.12 follows the scheme outlined above. Namely, let U be a normal subgroup of G_K, open in the T-adic topology, and let W be its closure in G_T; then $U = G_K \cap W$. Consider the commutative diagram analogous to (9.11)

(9.13)

$$\begin{array}{ccccccccc} H^1(G_K/U) & \longrightarrow & H^1(G_K) & \longrightarrow & H^1(U)^{G_K} & \longrightarrow & H^2(G_K/U) & \longrightarrow & H^2(G_K) \\ \uparrow{\scriptstyle\alpha} & & \uparrow{\scriptstyle\beta} & & \uparrow{\scriptstyle\gamma} & & \uparrow{\scriptstyle\delta} & & \uparrow{\scriptstyle\theta} \\ H^1(G_T/W) & \longrightarrow & H^1(G_T) & \longrightarrow & H^1(W)^{G_T} & \longrightarrow & H^2(G_T/W) & \longrightarrow & H^2(G_T), \end{array}$$

in which the vertical arrows are restriction maps and the rows are the initial segments of the Hochschild-Serre spectral sequences corresponding to the extensions $1 \to U \to G_K \to G_K/U \to 1$ and

$$1 \to W \to G_T \to G_T/W \to 1,$$

respectively. The weak approximation theorem for G shows that $G_K/U \simeq G_T/W$, so α and δ are isomorphisms. Furthermore, by Theorem 9.4 one can say that the natural map $G_K/[G_K, G_K] \to G_T/[G_T, G_T]$ is an isomorphism, and then β is also an isomorphism. With these facts and the injectivity of θ (Theorem 9.12), diagram (9.13) easily yields that γ is an isomorphism. But $H^1(U)^{G_K} = \mathrm{Hom}(U/[U, G_K], J)$ and $H^1(W)^{G_T} = \mathrm{Hom}(W/[W, G_T], J)$; therefore we see that $U \subset W$ induces an isomorphism $U/[U, G_K] \simeq W/[W, G_T]$; in particular, $[U, G_K] = U \cap [W, G_T]$ is open in the T-adic topology.

Thus, we have shown that if a normal subgroup U of G_K is open in the T-adic topology, then $[U, G_K]$ is also open. Now let F be an arbitrary T-adically open subgroup of G_K; let us show that $[F, F]$ is also open. Without loss of generality one may assume F to be a normal subgroup of D^*. Let

U denote the closure $[F, F]$ of G_K in the T-adic topology. Then it follows from the above assertion that $[U, G_K]$ is open; so

$$U = [U, G_K][F, F]. \tag{9.14}$$

On the other hand, $U/[F, F]$ is abelian, since $U \subset F$ by virtue of F being open; hence it lies in the center of $D^*/[F, F]$ (corollary to Proposition 9.3). In particular, $[U, G_K] \subset [F, F]$; so (9.14) yields $U = [F, F]$, as desired.

We conclude this section with the proof of Theorem 9.2. We shall need the following stronger version of Proposition 9.1.

PROPOSITION 9.5. *Let D be a quaternion algebra, let $x \in D^*$, and let Ψ be a finite set of maximal subfields of D. Then for any finite subset B of $\mathrm{Nrd}_{D/K}(D^*) \cap \prod_{v\in T} K_v^{*2}$ and any noncentral normal subgroup N of G_K there is an element n in N such that $B \subset \mathrm{Nrd}_{D/K}(L^*K(xn)^*)$ for any L in Ψ.*

PROOF: Put $V_0 = \{ v \in V^K : B \subset \mathrm{Nrd}_{D_v/K_v}(L_v^*)$ for each L in $\Psi \}$. Since L_v/K_v $(L \in \Psi)$ is unramified, and the elements of B are v-adic units, for almost all v in V_f^K, it follows that $S = V^K \setminus V_0$ is finite. Moreover, from $B \subset \mathrm{Nrd}_{D/K}(D^*) \cap \prod_{v\in T} K_v^{*2}$ it obviously follows that S does not intersect $T \cup T_\infty$. Since in the given case $T = T_0$, Lemmas 9.3 and 9.4 imply that there exists n in N such that $K(xn)_v \simeq K_v \oplus K_v$ for all v in S. Then

$$B \subset \mathrm{Nrd}_{D_v/K_v}((L \otimes K_v)^* K_v[xn]^*) \text{ for all } v \text{ in } V^K.$$

One can pass from local to global norms either by using Proposition 6.11 or by the following argument, specially designed for the case at hand. Let $\alpha \in B$ and $L \in \Psi$. Then the expression $N_{L/K}(a) - \alpha N_{K(xn)/K}(b)$ is a 4-dimensional quadratic form with respect to the coefficients of a in L and b in $K(xn)$; and the condition $\alpha \in \mathrm{Nrd}_{D/K}(L^*K(xn)^*)$ is equivalent to this form representing zero in K. By the Minkowski-Hasse theorem it suffices to verify the representability of zero over all completions K_v, where it is a consequence of $\alpha \in \mathrm{Nrd}_{D_v/K_v}((L \otimes K_v)^* K_v[xn]^*)$. The proposition is proved.

As usual, henceforth we shall assume that $N \subset G_K$ is a normal subgroup of D^*. For v in T, let Φ_v denote an open subgroup of K_v^* having finite index and not containing -1, and put $H = (N_T \prod_{v\in T} \Phi_v) \cap D^*$. It is easy to see that H is a T-adically open subgroup of D^* of finite index; moreover, $H \cap G_K = N_T \cap G_K = \bar{N}$, because $-1 \notin \Phi_v$. Consider the natural action of H on $\bar{N}/N$ by inner automorphisms, and let F denote the kernel of this action.

LEMMA 9.11. *For any x in D^* there is n in N satisfying:*

$$H = (K(xn)^* \cap H)\bar{N}F.$$

PROOF: By Theorem 9.8, $\bar{N}/N$ is finite; therefore $[D^* : F]$ is finite, since $[D^* : H]$ is finite. In particular, $\mathrm{Nrd}_{D/K}(D^*)/\mathrm{Nrd}_{D/K}(F)$ is finite; let q denote the number of subgroups of this quotient group. Also, choose a finite subset B of representatives of the cosets $\mathrm{Nrd}_{D/K}(H)/\mathrm{Nrd}_{D/K}(F)$, and note that by our definitions $B \subset \mathrm{Nrd}_{D/K}(D^*) \cap \prod_{v\in T} K_v^{*2}$. Thus, by induction, Proposition 9.5 yields $n_1 = 1, n_2, \ldots, n_{q+1}$ in N such that

$$B \subset \mathrm{Nrd}_{D/K}(K(xn_i)^* K(xn_j)^*) \quad \text{for } 1 \le i < j \le q+1.$$

It follows from the definition of q that, for some $i \neq j$, the images of $\mathrm{Nrd}_{D/K}(K(xn_i)^*)$ and $\mathrm{Nrd}_{D/K}(K(xn_j)^*)$ in $\mathrm{Nrd}_{D/K}(D^*)/\mathrm{Nrd}_{D/K}(F)$ are the same; then for $n = n_i$ we have

$$\mathrm{Nrd}_{D/K}(H) = B\,\mathrm{Nrd}_{D/K}(F) \subset \mathrm{Nrd}_{D/K}(K(xn)^*)\,\mathrm{Nrd}_{D/K}(F). \tag{9.15}$$

Let us show that $\mathrm{Nrd}_{D/K}(H) \cap \mathrm{Nrd}_{D/K}(K(xn)^*) = \mathrm{Nrd}_{D/K}(H \cap K(xn)^*)$. This follows from

LEMMA 9.12. *Let L/K be a quadratic extension, let T be a finite subset of V^K, and let W be an arbitrary open subgroup of $L_T = \prod_{v\in T} (L \otimes_K K_v)^*$. Then*

$$N_{L/K}(L^*) \cap N_{L_T/K_T}(W) = N_{L/K}(L^* \cap W).$$

PROOF: If $N_{L/K}(a) = N_{L_T/K_T}(b)$ for a in L^* and b in W, then $ab^{-1} \in S_T$, where $S = \mathbf{R}^{(1)}_{L/K}(\mathbb{G}_m)$ is the corresponding norm torus. Proposition 7.8 implies that S has weak approximation with respect to any finite subset of valuations; therefore $(ab^{-1}W) \cap S_K$ is nonempty, i.e., contains some element c. Then $ac^{-1} \in L^* \cap W$ and $N_{L/K}(ac^{-1}) = N_{L/K}(a)$, as desired.

Now (9.15) can be rewritten as

$$\mathrm{Nrd}_{D/K}(H) = \mathrm{Nrd}_{D/K}(K(xn)^* \cap H)\,\mathrm{Nrd}_{D/K}(F);$$

hence $H = (K(xn)^* \cap H)(G_K \cap H)F$, and it remains to use the fact that $G_K \cap H = \bar{N}$. The lemma is proved.

Now let us suppose $\Gamma = \bar{N}/N$ is nontrivial. It follows from Theorem 9.3 that Γ coincides with its own commutator group, and consequently cannot be solvable. Therefore, replacing N by the inverse image of the maximal solvable normal subgroup of Γ, under the natural homomorphism

$\bar{N} \to \bar{N}/N$, we reduce the problem to the case where Γ does not contain any solvable normal subgroups. Then, in particular, the center of Γ is trivial; so $F \cap \bar{N} = N$, and we have the embedding

$$\Gamma = \bar{N}/N \hookrightarrow H/F = \Delta.$$

As we saw in the proof of Theorem 9.3 for quaternion algebras, the openness of H in the T-adic topology implies the openness of

$$Z = \{\, z = x\tau(x)^{-1} : x \in H \,\};$$

so $\bar{N} \subset ZN$. However, for any x in H there is y in D^* satisfying $\tau(x) = yxy^{-1}$; hence

$$z = x\tau(x)^{-1} = [x, y] \in G_K \cap [N_T \prod_{v\in T} \Phi_v, y] \subset G_K \cap N_T = \bar{N}.$$

Therefore, $Z \subset \bar{N}$, yielding $\bar{N} = ZN$. Bearing in mind that $x\tau(x)^{-1} = x^2\,\mathrm{Nrd}_{D/K}(x)^{-1}$ and that $K^* \subset F$, we obtain $\Gamma = \Delta^2$. Thus, Lemma 9.11 puts us in a position to apply the following result from group theory.

LEMMA 9.13. *Suppose a finite group Γ is embeddable in a finite group Δ so that the following conditions hold:*

(1) $\Delta^2 = \Gamma$;
(2) *for any g in Δ there is an abelian group $B(g) \subset \Delta$ containing g such that $\Delta = B(g)\Gamma$.*

Then $\Gamma_2 = \{\, g \in \Gamma : g^2 = e \,\}$ is a normal subgroup of Γ.

(Note that, applying Lemma 9.11, for $g = xN$ we can take $B(g)$ to be the image in Δ of $K(xn)^* \cap H$ from Lemma 9.11.)

PROOF: Consider the map $\psi\colon \Delta \to \Gamma$ given by $\psi(g) = g^2$. Condition (1) yields

$$|\Delta| = \sum_{h\in\Gamma} |\psi^{-1}(h)|. \tag{9.16}$$

However, if $h \in \Gamma$ and $h = g^2$ where $g \in \Delta$, then $\psi^{-1}(h) \supset gB(g)_2$; therefore

$$|\psi^{-1}(h)| \ge |B(g)_2| \ge |(B(g)/(B(g) \cap \Gamma))_2| = |(\Delta/\Gamma)_2| = |\Delta/\Gamma|. \tag{9.17}$$

Here we use the fact that for any finite abelian group B and any subgroup C of B one has $|B_2| \ge |(B/C)_2|$. Comparing (9.16) and (9.17), we obtain that

$|\psi^{-1}(h)| = |\Delta/\Gamma|$ for any h in Γ; and, if $h = g^2$, then $\psi^{-1}(h) = gB(g)_2$. In particular, $\Delta_2 = \psi^{-1}(e) = B(e)_2$ is a subgroup of Δ. Therefore $\Gamma_2 = \Gamma \cap \Delta_2$ is clearly a normal subgroup of Γ. The lemma is proved.

Since we are supposing that Γ has no non-trivial solvable normal subgroups, it follows from Lemma 9.12 that $\Gamma_2 = (e)$; i.e., the order of Γ is odd. But then, by the Feit-Thompson theorem, Γ itself must be solvable; contradiction. The argument can also be made without using the Feit-Thompson theorem. Indeed, as we noted in the beginning of the proof of Theorem 9.2, x and $x^{-1} = \tau(x)$ are conjugate in D^*, for any x in G_K. If in addition $x \in \bar{N}$, then Proposition 9.3 implies that the images of x and x^{-1} in Γ are conjugate (in Γ). It follows that if $g \in \Gamma$ and $g^2 \neq e$, then $\{ h \in \Gamma : hgh^{-1} \in \{g, g^{-1}\} \}$ consists of two cosets modulo the centralizer of g. So, if Γ is nontrivial, then it must have even order, and hence $\Gamma_2 \neq (e)$.

Thus, we have completed the proof of Theorems 9.2–9.4. This required the development of a specific technique, which we call the *multiplicative arithmetic method* (cf. Platonov-Rapinchuk [4]). We deliberately set forth the basic results of multiplicative arithmetic in a somewhat more general form than necessary for the proof of these theorems. Naturally, this has not been done for the sake of generality *per se*, but because we are confident that by applying the method developed here one will be able to prove Conjecture 9.2 for all G that are inner forms of type A_n. At this time we have virtually no results for algebraic groups of the form $G = \mathbf{SU}_1(D)$, where D is a finite-dimensional skew field with involution τ of the second kind, which are outer forms of type A_n. In this area, apparently one should begin by obtaining the analogs of Theorems 9.3 and 9.4. The starting point must be to prove that the commutator group of the unitary group $U_1(D) = \{ x \in D^* : xx^\tau = 1 \}$ is $SU_1(D) = U_1(D) \cap SL_1(D)$, the analog of the frequently used equality, $SL_1(D) = [D^*, D^*]$. One possible way might be to use the triviality of the reduced unitary Whitehead group $SUK_1(D) = \Sigma'_\tau/\Sigma_\tau$ (cf. §7.2), where Σ'_τ is the subgroup of the elements of D^* with τ-symmetric reduced norm, and Σ_τ is generated by symmetric elements. Namely, let $a \in SU_1(D)$ be an element generating a maximal subfield P over the center L of D. Then $\tau(P) = P$ and $N_{P/M}(a) = aa^\tau = 1$, where M is the subfield of symmetric elements in P. Therefore, by Hilbert's Theorem 90, $a = b(b^\tau)^{-1}$ for some b in P. Moreover,

$$\mathrm{Nrd}_{D/K}(b)/\mathrm{Nrd}_{D/K}(b^\tau) = \mathrm{Nrd}_{D/K}(b(b^\tau)^{-1}) = \mathrm{Nrd}_{D/K}(a) = 1,$$

so $b \in \Sigma'_\tau$. Since $SUK_1(D)$ is trivial, it follows that there exist symmetric $t_1, \ldots, t_r$ in D^* such that $b = t_1 \ldots t_r$, and then

$$a = t_1 \ldots t_r t_1^{-1} \ldots t_r^{-1}. \tag{9.18}$$

Can (9.18) be transformed in such a way as to obtain an expression for a as a product of commutators in $U_1(D)$? We leave this unsolved problem for the reader to ponder.

9.3. The classical groups.

The object of this section is to prove Theorem 9.5. While the arguments in the previous section were based on the inner structure of G, here a key role is played by the fact that any group G belonging to one of the types under consideration has a nice geometric realization. Our starting point is the fact that all the classical series under considerations stem from groups of type A_1 (i.e., $B_1 = C_1 = A_1$, $D_2 = A_1 + A_1$), whose normal subgroups are described in Theorem 9.2; thus the task at hand reduces to setting up an induction on dimension in describing normal subgroups. The following terminology will be helpful. For a semisimple simply connected K-group G, we shall say that G_K has a *standard description of normal subgroups* if there exists a finite subset S of V^K such that any Zariski-dense normal subgroup N of G_K is open in G_K in the S-adic topology.

LEMMA 9.14.

(1) *If a normal subgroup N of G_K is open in the S-adic topology, then it is also open in the S_f-adic topology, where $S_f = S \cap V_f^K$.*

(2) *For a simple simply connected K-group G, the standard description of normal subgroups holds for G_K if and only if Conjecture 9.2 holds for G.*

(3) *If $G = \prod_{i=1}^{l} \mathbf{R}_{L_i/K}(G_i)$ is a semisimple simply connected K-group, where the G_i are simple L_i-groups, then the standard description of normal subgroups holds for G_K if and only if it holds for all the $(G_i)_{L_i}$. In particular, if all the simple components of G have type A_1, then G has the standard description of normal subgroups.*

PROOF: (1) If $N = G_K \cap W$, where W is an open subset of G_S, then the weak approximation property for G (Proposition 7.9) implies that the closure N_S of N in G_S contains W and therefore is an open normal subgroup. Since for v in V_∞^K there are no noncentral normal subgroups of G_{K_v} (Proposition 7.6), then arguing as in the proof of Lemma 9.3 we obtain that $N_S = G_{S \cap V_\infty^K} \times N_{S_f}$, where N_{S_f} is an open normal subgroup of G_{S_f}. In view of the fact that N is S-adically-closed in G_K, we obtain that $N = G_K \cap N_S = G_K \cap N_{S_f}$, i.e., N is open in the S_f-adic topology.

(2) If Conjecture 9.2 holds for G_K, then clearly G_K has the standard description of normal subgroups relative to $S = T$. Conversely, if the standard description of normal subgroups holds for G_K relative to S, then the formula $N_S = N_{S \cap T} \times G_{S \setminus (S \cap T)}$ for the closure N_S of a normal subgroup

N of G_K in the S-adic topology (cf. Lemma 9.1) implies that any non-central normal subgroup is closed in the $(S \cap T)$-adic topology and hence also in the T-adic topology; by Lemma 9.2, equivalently one may say that Conjecture 9.2 holds.

(3) $G_K \simeq \prod_{i=1}^{l} (G_i)_{L_i}$; moreover, for any finite subset S of V^K, the S-adic topology on G_K is the product of the $\bar{S}_i$-adic topologies on the $(G_i)_{L_i}$, where $\bar{S}_i$ consists of all extensions of the valuations from S to L_i. It follows in particular that if the standard description of normal subgroups holds for G_K relative to S, then it holds for each $(G_i)_{L_i}$ relative to $\bar{S}_i$. Conversely, the standard description of normal subgroups for $(G_i)_{L_i}$ relative to $S_i \subset V^{L_i}$ implies the standard description for G_K relative to $S = \bigcup_i V_i$, where V_i consists of the restrictions of the valuations of S_i to K. The latter assertion of (3) follows from Theorem 9.2. Lemma 9.14 is proved.

Now let G be a simple simply connected K-group of one of the types listed in Theorem 9.5. By the results in §2.3, there is a natural action of G on $\bar{W} = W \otimes_K \bar{K}$, where W is an m-dimensional space over a skew field D with involution τ, and this action preserves a Hermitian or skew-Hermitian form f on W. All the forms which arise in this manner appear in the list at the end of §2.3.4, to which we shall refer repeatedly. Note that in case (1) of this list (groups of type ${}^2A_n$), by assumption $D = L$ is a quadratic extension of K. On the other hand, in case (3), G is K-split and it is well known that G_K is projectively simple (cf. §7.2); thus we are fully justified in excluding this case from further consideration. In the remaining cases, W contains vectors which are anisotropic with respect to f, and one can use the following result, crucial to the proof of Theorem 9.5.

THEOREM 9.13. *Let $m \geq m_0 + 1$, let x be an arbitrary anisotropic vector in W, and let $G(x)$ be its stabilizer. If a standard description of normal subgroups holds for $G(x)_K$, then it also holds for G_K.*

(The value of m_0 for each type of form is given in the list in §2.3.4. Note that $G(x)$ is simply connected and semisimple for $m \geq m_0 + 1$ (Proposition 2.21), and therefore one can speak of a standard description of normal subgroups for $G(x)_K$.)

PROOF: Now let N be an arbitrary noncentral (=Zariski-dense) normal subgroup of G_K. By assumption there is a finite subset S of V^K such that any Zariski-dense normal subgroup of $G(x)_K$ is open in the S-adic topology. In addition, by Lemma 9.14 (1), we may assume without loss of generality that $S \subset V_f^K$. Since N has finite index in G_K (Theorem 9.8), it follows that $G(x)_K \cap N$ has finite index in $G(x)_K$ and, in particular, is Zariski-dense in $G(x)$. Since $S \subset V_f^K$, one can find an open subgroup U of G_S satisfying

$$G(x)_K \cap U \subset G(x)_K \cap N. \tag{9.19}$$

Let us put $X = \{ y \in \bar{W} : f(y) = f(x) \}$. Suppose we are able to prove

$$\text{the orbit } (U \cap N)x \text{ is open in } G_K x \text{ in the } S_0\text{-adic topology, where } S_0 = S \cup V_\infty^K. \tag{9.20}$$

Since the action of G_{S_0} on X_{S_0} is continuous, it follows that there exists an open subset B of G_{S_0} containing the identity, such that $(B \cap G_K)x \subset (U \cap N)x$. Let $\bar{N}$ be the closure of N in G_K in the S_0-adic topology. Then $U \cap N$ is dense in $U \cap \bar{N}$ under this topology, and, in particular, $U \cap \bar{N} \subset (U \cap N)(B \cap G_K)$. It follows that

$$(U \cap \bar{N})x \subset (U \cap N)(B \cap G_K)x \subset (U \cap N)x,$$

and therefore $U \cap \bar{N} \subset (U \cap N)(G(x)_K \cap U) \subset N$ by virtue of (9.19). But $\bar{N} = (U \cap \bar{N})N$, so $\bar{N} = N$, and the theorem is proved.

Thus, it remains to prove (9.20). To do so, we introduce a technical concept. We shall say that a vector z in $\bar{W}$ is *regular* if $f(z) \in \bar{D}^*$. More generally, a $\bar{D}$-submodule V of $\bar{W}$ is said to be regular if it is free and its discriminant with respect to some (or any) $\bar{D}$-base lies in $\bar{K}^*$.

LEMMA 9.15.

(1) *A vector z in W is regular if and only if it is anisotropic; and, for a D-subspace V of W, the $\bar{D}$-submodule $V \otimes_K \bar{K}$ is regular if and only if V is nondegenerate.*
(2) *If z is a regular vector in $\bar{W}$, then $Z = \{ z' \in \bar{W} : f(z') = f(z) \}$ is a homogeneous space of G.*

PROOF: (1) is obvious. To prove (2) let us consider an arbitrary anisotropic vector x in W. There exists an element d in $\bar{D}^*$ such that $f(z) = f(xd)$. Since, by Witt's theorem (Theorem 2.11), the variety $\{ y \in \bar{W} : f(y) = f(x) \}$ is a homogeneous space of G, then so is Z. The lemma is proved.

Put $Y = \{ (x, z, g) \in X \times X \times G : gx = y,\ gz = z \}$, and let Y_0 denote the subset of Y consisting of (y, z, g) such that

$$\begin{aligned} &\text{(a) } (x - y) \text{ is a regular vector;} \\ &\text{(b) the } \bar{D}\text{-submodule of } \bar{W} \text{ generated by } x \text{ and} \\ &\quad y \text{ is } \bar{D}\text{-free and regular.} \end{aligned} \tag{9.21}$$

Furthermore, consider the projections:

$$p: Y \to X \times X, \qquad p(x, z, g) = (y, z)$$
$$q: X \times X \to X, \qquad q(y, z) = y.$$

Clearly $p(Y) \subset F = \{ (y, z) \in X \times X : f(z, x) = f(z, y) \}$. Moreover, $p(Y_0) \subset F_0$, where F_0 consists of pairs (y, z) satisfying (9.21).

LEMMA 9.16. *Y_0 and F_0 are nonempty Zariski-open subsets of Y and F respectively, and the morphisms $p\colon Y_0 \to F_0$ and $q\colon F_0 \to X$ are dominant.*

PROOF: Clearly $\bar{D}^*$ is a Zariski-open subset of $\bar{D}$; therefore the set of vectors y in $\bar{W}$ satisfying condition (a) of (9.21) is also open, since it is the inverse image of $\bar{D}^*$ under the map sending y to $f(x-y)$. Similarly, one can show that the set of vectors z in $\bar{W}$ satisfying condition (b) is open. It follows that Y_0 is an open subset of Y and F_0 is an open subset of F.

Let X_0 denote the subset of X consisting of those y satisfying the following conditions:

(9.22)
(i) the vector $x-y$ is regular;
(ii) the $\bar{D}$-submodule generated by x and y is $\bar{D}$-free and regular;
(iii) $f(x-y,x) \in \bar{D}^*$ and $f(x-y,x)^{-1}f(x-y,y) - 1 \in \bar{D}^*$.

From what we have seen above, X_0 is clearly a Zariski-open subset of X. Moreover, if y in $\bar{W}$ is such that $y \perp x$ and $f(y) = f(x)$, then one can see immediately that $y \in X_0$ and thus $X_0 \neq \emptyset$. Since the Witt theorem implies that X is irreducible, it follows that X_0 is open and dense in X. We wish to show that $X_0 \subset q(F_0)$, from which it will follow that F_0 is nonempty and $q\colon F_0 \to X$ is dominant. Thus, let $y \in X_0$; put $\lambda = -f(x-y,x)^{-1}f(x-y,y)$ and $t = x\lambda + y$. Immediate verification shows that t and $x-y$ form an orthogonal $\bar{D}$-base of the $\bar{D}$-submodule generated by x and y. Therefore t is regular, and by choosing d in $\bar{D}^*$ so that $f(td) = f(x)$, for $z = td$ we obtain $(y,z) \in F_0$, and the proof is completed.

To prove the remaining assertions of the lemma, we shall show that $p(Y_0) = F_0$, i.e., if $(y,z) \in F_0$, then $y = g(x)$ for suitable g in G satisfying $gz = z$. By Theorem 2.11, one has h in G for which $hx = z$. Then, putting $x_1 = h^{-1}x$ and $y_1 = h^{-1}y$, it is easy to see that to construct g it suffices to find s in $G(x)$ such that $sx_1 = y_1$. Let W_0 denote the orthogonal complement of x in W, and put $x_2 = x_1 - xf(x)^{-1}f(x_1,x)$ and $y_2 = y_1 - xf(x)^{-1}f(y_1,x)$. Then $x_2, y_2 \in \bar{W}_0 = W_0 \otimes_K \bar{K}$, and $f(x_2) = f(y_2)$, with x_2, y_2 regular. Now, applying Lemma 9.15 (2) to $\bar{W}_0$, and bearing in mind that $G(x)$ is the universal covering of the special unitary group of W_0, we obtain the desired result. Lemma 9.16 is proved.

We proceed to the proof of (9.20). Take U as in (9.19). By making U smaller if necessary, we may assume that $U = \prod_{v \in S} U_v$, where U_v is an open subgroup of G_{K_v} for each v in S. Put $U_0 = U \times G_{S \setminus S_0} = \prod_{v \in S_0} U_v$, where

$U_v = G_{K_v}$ for v in $S_0 \setminus S = V_\infty^K$ and

$$C = (Y_0)_{S_0} \cap (X_{S_0} \times U_0 x \times U_0).$$

LEMMA 9.17.

(1) *Y and F_0 are irreducible varieties.*
(2) *$C = \prod_{v \in S_0} C_v$, where C_v is a nonempty subset of Y_{0K_v}, open in the v-adic topology and dense in the Zariski topology.*

PROOF: Consider the map $\varphi\colon P = G \times G(x) \to X \times X \times G$ given by $(g,h) \mapsto ((ghg^{-1}x), gx, ghg^{-1})$. From Witt's theorem one can easily deduce that $\varphi(P) = Y$. It follows that Y is irreducible; hence also F_0 is irreducible, since Y_0 is open in Y and $p\colon Y_0 \to F_0$ is dominant (Lemma 9.16).

It is easy to see that $C = \prod_{v \in S_0} C_v$, where

$$C_v = (Y_0)_{K_v} \cap (X_{K_v} \times U_v x \times U_v),$$

and therefore it follows from Proposition 3.3 that C_v is open in Y_{K_v}. However $C_v \supset \varphi((U_v \times (G(x) \cap U_v)) \cap P_0)$, where $P_0 = \varphi^{-1}(Y_0)$. Since P is smooth and irreducible, $U_v \times (G(x) \cap U_v)$ is Zariski-dense (Lemma 3.2) and P_0 is Zariski-open in P; it follows easily that C_v is dense. Lemma 9.17 is proved.

Since C_v is dense in Y, it follows that for each v in S_0 there exists a simple point c in C_v such that $b = p(c)$ is a simple point of F_0 and the differential $d_c p\colon T_c(Y) \to T_b(F)$ is surjective. Then, by Proposition 3.3, $p(C_v)$ contains a subset B_v of F_{0K_v} which is open in the v-adic topology and dense in the Zariski topology. Applying the same argument again, we obtain that $q(B_v)$ contains a subset E_v which is open in X_{K_v}. Put $B = \prod_{v \in S_0} B_v$ and $E = \prod_{v \in S_0} E_v$. Then, to prove (9.20), it suffices to establish

$$E \cap X_K \subset (U \cap N)x. \tag{9.23}$$

Let $y \in E \cap X_K$. By assumption one can find $\bar{z}$ in X_{S_0} such that $(y,\bar{z}) \in B$. If $\bar{z} = (z_v)_{v \in S_0}$, then for any v in S_0 we have

$$f(z_v,x) = f(z_v,y)$$
$$f(z_v) = f(x).$$

Let g denote the restriction of f to the orthogonal complement W_0 of $(x-y)$. Then taking $Z = \{\, t \in W_0 \otimes_K \bar{K} : g(t) = f(x) \,\}$ we have $Z_{K_v} \neq \emptyset$

for all v in S_0; in particular, $Z_{K_v} \neq \emptyset$ for v in V_∞^K. Since $m \geq m_0 + 1$, it follows that $\dim W_0 = m - 1 \geq m_0$. Thus, comparing the values of m_0 with the minimal dimensions in Claims 6.1′, 6.2 and 6.3 of §6.6, we obtain that $Z_K \neq \emptyset$. Furthermore, there exists a neighborhood $J \subset Z_{S_0}$ of $\bar{z}$ such that $(y, J) \subset B$. By Proposition 7.4, Corollary 2, Z satisfies weak approximation, and hence there is a point z in $Z_K \cap J$. Then $(y, z) \in p(C)$, i.e., $z \in U_0 x$, and the subspace spanning x and z is nonsingular.

Now we need the following

LEMMA 9.18. *Suppose there is a K-action of an algebraic K-group H on an algebraic K-variety M, and S is a finite subset of V^K containing V_∞^K. If x is a point in M_K such that the stabilizer $H(x)$ is semisimple and simply connected, then $M_K \cap Ux = (H_K \cap U)x$ for any open subgroup U of H_S.*

PROOF: Follows from the validity for $H(x)$ of the Hasse principle (Theorem 6.6) and of the weak approximation property (Proposition 7.9). Indeed, let $y \in M_K \cap Ux$ and $y = hx$, where $h \in H_{\bar{K}}$. Then $\alpha_\sigma = h^{-1}\sigma(h)$ lies in $H(x)$, for any σ in $\mathrm{Gal}(\bar{K}/K)$; moreover, the family $\{\alpha_\sigma\}$ determines a cocycle ξ in $H^1(K, H(x))$. Since by assumption $y \in H_{K_v} x$ for v in $S \supset V_\infty^K$, it follows that ξ lies in the kernel of $H^1(K, H(x)) \to \prod_{v \in V_\infty^K} H^1(K_v, H(x))$. Therefore, since the Hasse principle holds for $H(x)$, we see that ξ is trivial; i.e., $\alpha_\sigma = h^{-1}\sigma(h) = g^{-1}\sigma(g)$ for suitable g in $H(x)$ and all σ in $\mathrm{Gal}(\bar{K}/K)$. Then $h' = hg^{-1} \in H_K$ and $y = h'x \in H_K x$. Thus, $y = h_1 x = h_2 x$, where $h_1 \in H_K$ and $h_2 \in U$. Then $r = h_1^{-1} h_2 \in H(x)_S$, and by the weak approximation property there exists t in $H(x)_K \cap (r(H(x)_S \cap U))$. We have $h_1 t \in H_K \cap U$ and $y = (h_1 t)x \in (H_K \cap U)x$. The lemma is proved.

Applying Lemma 9.18 to the action of G on X, and bearing in mind that $G(x)$ is simply connected (Proposition 2.21), we obtain that $X_K \cap U_0 x = (G_K \cap U_0)x$; in particular,

$$z = gx, \qquad g \in G_K \cap U_0. \tag{9.24}$$

Furthermore, by definition $(y, z) \in p(C)$, i.e., $y \in (G(z)_{S_0} \cap U_0)x$. Therefore, applying Lemma 9.5 to the action of $G(z)$ on X (which is permissible, since $G(x, z)$ is simply connected, again by Proposition 2.21), we obtain

$$y = hx, \qquad h \in G(z)_K \cap U_0. \tag{9.25}$$

Since $G(z) = gG(x)g^{-1}$, it follows from (9.24) and (9.25) that

$$h \in G(z)_K \cap U_0 = g(G(x)_K \cap U_0)g^{-1} = g(G(x)_K \cap U)g^{-1} \subset N \cap U,$$

which means $y = hx \in (N \cap U)x$. This completes the proof of Theorem 9.13.

PROOF OF THEOREM 9.5: By Lemma 9.14 (2) it suffices to show that G_K has a standard description of normal subgroups. This will follow from Theorem 9.13 by induction on the degree m of the group under consideration. Since the types listed in Theorem 9.4 correspond precisely to the condition $m \geq m_0 + 1$, the induction step is obvious and it remains to justify the base of induction for each case. In other words, in an m-dimensional space W over D, for $m = m_0 + 1$, one needs to find a vector x, anisotropic with respect to f, such that $G(x)$ will have a standard description of normal subgroups. But in case (1) from the list of classical groups (cf. §2.4.4), where $D = L$ and $m = m_0 + 1 = 3$, and in case (4), where $m = m_0 + 1 = 2$, $G(x)$ has type A_1 for any anisotropic vector x in W; therefore the standard description of normal subgroups holds for $G(x)_K$ (Lemma 9.14 (3)). Similarly, in the case (2), where $m = m_0 + 1 = 5$, $G(x)$ has type $D_2 = A_1 + A_1$, and again we can apply Lemma 9.1.

Case (5), where $m = m_0 + 1 = 4$, is somewhat more difficult to handle. Here $H = G(x)$ has type $D_3 = A_3$. We show that x in W can be chosen in such a manner that H will either be K-isotropic (in which case Theorem 9.1 implies that H_K has no proper, noncentral normal subgroups), or else a group of the form $\mathbf{SU}_4(f)$, where f is a Hermitian form over a quadratic extension L/K, which we have already considered. To this end, we use the following test.

LEMMA 9.19. *Let H be a simple simply connected K-group of type A_3. If H is split by some quadratic extension L/K, then H is one of the following groups: $\mathbf{SL}_4$; $\mathbf{SL}_2(D)$, where D is a quaternion skew field over K; or $\mathbf{SU}_4(f)$, where f is a nondegenerate Hermitian form over L.*

PROOF: Follows easily from the description of groups of type A_n (cf. §2.3).

Thus it remains to construct an anisotropic vector x in W for which $H = G(x)$ satisfies the conditions of Lemma 9.19. First we show that there are vectors e_1 and e_2 in W satisfying

$$e_1 \perp e_2, \qquad f(e_1) = f(e_2) \neq 0. \tag{9.26}$$

To this end, for each v in V_∞^K, let us find regular vectors s^v and t^v in $W \otimes_K K_v$ such that $s^v \perp t^v$ and $f(s^v) = f(t^v)$. With the weak approximation property in W and the orthogonalization process, one can construct s and t in W such that $s \perp t$ and

$$\begin{aligned} f(s) &\in f(s^v D_v^*) \\ f(t) &\in f(t^v D_v^*) \end{aligned} \tag{9.27}$$

for all v in V_∞^K. We put $e_1 = s$ and show that the orthogonal complement W_0 of e_1 contains a vector e_2 for which $f(e_2) = f(e_1)$. By Claim 6.3

of §6.6, it suffices to find e^v in $W_0 \otimes_K K_v$ for each v in V_∞^K, such that $f(e^v) = f(e_1)$. But by (9.27) $f(s) = f(s^v d_1)$ and $f(t) = f(t^v d_2)$ for suitable d_1 and d_2 in D_v^*. Then $e^v = td_2^{-1}d_1 \in W_0 \otimes_K K_v$ is the desired vector, since $f(e^v) = f(t^v d_1) = f(s^v d_1) = f(s)$. Thus, we have established the existence of e_1 and e_2 satisfying (9.26).

Put $U = e_1 D + e_2 D$, and let h denote the restriction of f to U. Then $F = \mathbf{SU}_2(h)$ belongs to type $D_2 = A_1 \times A_1$. On the other hand, F becomes split over a quadratic extension $P = K(a)$ of K, where $a = f(e_1) = f(e_2)$. Indeed, let T_i denote the special unitary group of the space spanned by the e_i. Then $T_i \simeq \mathbf{R}^{(1)}_{P/K}(\mathbb{G}_m)$, and $T = T_1 \times T_2$ is a maximal torus of F, as desired. It follows that $F = F_1 \times F_2$ is the direct product of groups of type A_1 over K. We have $F_i = \mathbf{SL}_1(D_i)$, where D_i is a quaternion algebra over K.

Now we establish the existence of e_3 in $U^\perp$ such that $b = f(e_3) \neq 0$ and $L = K(b)$ splits D_1 and D_2. We claim that we may then choose x to be any vector orthogonal to e_1, e_2, e_3. Indeed, let us put $H = G(x)$ and show that H is L-split. Clearly H contains $F \times T_3$, where $T_3 \simeq \mathbf{R}^{(1)}_{L/K}(\mathbb{G}_m)$ is a one-dimensional torus which is the special unitary group of the space spanning e_3. But by construction L splits F and T_3; so there is nothing more to prove, since H and $F \times T_3$ have the same rank.

To construct e_3, let S denote the finite subset of V^K consisting of those v for which at least one of the algebras D_{1v}, D_{2v} is a skew field. Let $v \in S$; then there is a regular vector u^v in $U^\perp \otimes_K K_v$ such that $K_v[b^v]$ is a field for $b^v = f(u^v)$. Indeed, if D_v is a skew field, then for u^v one can take any anisotropic vector; if not, one uses the fact that a 4-dimensional quadratic form over K_v always contains an anisotropic, binary subform. (Note that since $v \in S$, certainly $K_v \neq \mathbb{C}$.) For e_3 choose a vector from $U^\perp$ which is sufficiently close to the u^v for v in S so that, for $b = f(e_3)$, the algebras $K_v[b]$ and $K_v[b^v]$ will be isomorphic for all v in S. (The existence of such approximations is easily established with the help of Krasner's lemma, for example, cf. §6.4.) Then it follows from §1.5.1 and our constructions that $L = K(b)$ is the desired field. This completes the proof of Theorem 9.5.

We have yet to prove Theorem 9.6. So, let G be a simple algebraic K-group of type G_2. It is well known (cf. Jacobson [1]) that G can be realized as the group of all automorphisms of $C \otimes_K \bar{K}$, where C is a Cayley algebra over K. There is a norm map $N: C \to K$ on C which is a nondegenerate quadratic form of degree 8 in the coefficients with respect to a base C/K. Let W denote the space of "pure" octonions, i.e., the orthogonal complement of the identity of C with respect to the bilinear form $(\ |\ )$ associated with N, and let f be the restriction of N to W. The space $\bar{W} = W \otimes_K \bar{K}$ and f are invariant under G; moreover, by restricting the action of G to W we obtain its well-known 7-dimensional K-representation.

The proof of Theorem 9.6 uses the following properties of this representation.

PROPOSITION 9.6 (WITT'S THEOREM). *Let a and b in $\bar{W}$ be anisotropic vectors such that $f(a) = f(b)$. Then there exists g in G satisfying $g(b) = a$. Furthermore, if a_1, a_2 and b_1, b_2 are pairs of vectors of $\bar{W}$ generating nonsingular subspaces with respect to f, such that $f(a_i) = f(b_i)$ $(i = 1, 2)$ and $(a_1|a_2) = (b_1|b_2)$, then there exists g in G satisfying $g(b_i) = a_i$ $(i = 1, 2)$.*

PROPOSITION 9.7. *For any vector x in $\bar{W}$, anisotropic with respect to f, the stabilizer $G(x)$ is isomorphic either to $\mathbf{SL}_3$ or to $\mathbf{SU}_3(\varphi)$, where φ is a nondegenerate Hermitian form over a quadratic extension L/K; and for any pair of vectors x, y in W generating a nonsingular subspace with respect to f, the stabilizer $G(x, y)$ is either $\mathbf{SL}_2$ or $\mathbf{SU}_2(\varphi)$. Thus, $G(x)$ and $G(x, y)$ are semisimple and simply connected.*

It follows from Proposition 9.7 and Theorem 9.5 that for anisotropic x in W we have a standard description of normal subgroups of $G(x)_K$; therefore, in this case, it suffices to establish the analog of Theorem 9.13. This analog indeed holds, and its proof is a replica of the proof of Theorem 9.13. The following result, a direct consequence of Claim 6.1′ in §6.6 and Proposition 7.4, Corollary 2, contains all the necessary arithmetic facts:

Let z be an anisotropic vector in W, let W_0 be the orthogonal complement of z, and let $Z = \{x \in W_0 \otimes_K \bar{K} : f(x) = c\}$, where $c \in K^*$. If $Z_{K_v} \neq \emptyset$ for each v in V_∞^K, then $Z_K \neq \emptyset$; moreover, in this case Z has weak approximation with respect to any finite subset S of V^K.

We leave it to the reader to work out the details of the argument as an exercise.

Chernousov (unpublished) has found another proof of the projective simplicity of G_K, for a K-anisotropic group G of type G_2.[2] It is based on the fact, already used in our proof of the Hasse principle for G, that any maximal K-torus T of G lies in a K-subgroup H of G of type A_2 (cf. §6.8). Let us take an arbitrary, noncentral normal subgroup N of G_K and show that $N = G_K$. Let $x \in G_K$. Since G is assumed K-anisotropic, it follows that x is semisimple and therefore is contained in a maximal K-torus T of G. Take a K-subgroup H of G of type A_2, containing T. By Theorem 9.8, $[G_K : N]$ is finite; hence, in particular, $H_K \cap N$ is a noncentral normal subgroup of H_K. Therefore, to show that $x \in N$ and thus complete the proof, it suffices to establish that H_K is projectively simple. But this will follow from Theorem 9.5 once it is shown that H has the form $\mathbf{SU}_3(f)$

[2] It can be shown that any K-group of type G_2 is either K-split or K-anisotropic; thus, one obtains another proof of Theorem 9.6.

for a suitable Hermitian form f over a quadratic extension L/K. To do so we use the fact (cf. Proposition 6.17) that G becomes split over some quadratic extension L/K. Let B be a Borel L-subgroup of G. We have $\dim G = 14$, $\dim H = 8$ and $\dim B = 8$; so $\dim(B \cap H) \geq 2$. It follows that H becomes isotropic over L. On the other hand, the list of all the possibilities for H is as follows:

$$ {}^1A_2 = \begin{cases} (i)\ \mathbf{SL}_3 \\ (ii)\ \mathbf{SL}_1(D), & D \text{ is a skew field of index 3} \end{cases} $$

$$ {}^2A_2 = \begin{cases} (iii)\ \mathbf{SU}_3(f) \\ (iv)\ \mathbf{SU}_1(D), & D \text{ is a skew field of index 3,} \end{cases} $$

and neither of the groups in cases (ii) and (iv) can be L-isotropic. Q.E.D.

9.4. Groups split over a quadratic extension.

This section is devoted to the proof of Theorem 9.7. We shall use induction on the rank l of G. For $l = 2$, G belongs either to type A_2, $B_2 = C_2$, or G_2. For groups of type B_2 or G_2 the absence of noncentral normal subgroups of G_K follows from Theorems 9.5 and 9.6. The normal structure of arbitrary groups of type A_2 has not yet been analyzed fully; however in our case one only encounters groups of this type that are split over a quadratic extension L/K. Such groups have the form $G = \mathbf{SU}_3(f)$, where f is a nondegenerate, 3-dimensional Hermitian form over L (cf. the discussion at the end of the previous section), and again the projective simplicity of G_K follows from Theorem 9.5.

Let us suppose the theorem holds for all the groups described in its statement, of rank less than l ($l \geq 3$), and show that it is true if the rank of G equals l. To the end, we establish the existence of an open subset U of G_∞ such that any g in $G_K \cap U$ can be written as

$$ g = g_1 \dots g_m, \tag{9.28} $$

where the g_i ($i = 1, \dots, m$) lie in G_{i_K}, for suitable simple simply connected K-subgroups G_i of G which are split over L and whose ranks are between 2 and $l-1$. If N is a noncentral normal subgroup of G_K, then $[G_K : N] < \infty$ (Theorem 9.8), and, in particular, $G_{i_K} \cap N$ is a noncentral normal subgroup of G_{i_K}. Therefore, by the induction hypothesis, $G_{i_K} \cap N = G_{i_K}$; hence $g \in N$, which means that $G_K \cap U \subset N$. But by Lemma 9.1 we have $N_\infty = G_\infty$, so $NU = G_\infty$ and $N(G_K \cap U) = G_K$. Therefore, finally we obtain $N = G_K$, and the theorem is proved.

To establish the existence of (9.28) we need to use some information on the structure of G. By Lemma 6.20 there exists a maximal K-torus T of

G which is split over an extension L/K. As we noted after the proof of Lemma 6.20 (§6.6), the nontrivial automorphism σ in $\mathrm{Gal}(L/K)$ acts on the group of characters $\mathbf{X}(T)$ by multiplication by -1; so, for any root α in $R = R(T, G)$, the root subgroup G_α of G generated by the one-dimensional unipotent subgroups U_α and $U_{-\alpha}$ is defined over K (note that $G_\alpha \simeq \mathbf{SL}_2$ over L). Furthermore, let us fix Π, a subsystem of simple roots of R, and for any subset Σ of Π let G_Σ denote the subgroup of G generated by the G_α, for α in Σ. Lastly, put $T_\Sigma = T \cap G_\Sigma$ (in particular, $T_\alpha = T \cap G_\alpha$). We shall need the following well-known properties (cf., for example, Steinberg [2]):

(9.29)
(1) for any subset Σ of Π, the group G_Σ is a simple simply connected K-group of rank equal to $|\Sigma|$;
(2) if $\Sigma_1 \cap \Sigma_2 = \emptyset$, then $G_{\Sigma_1} \cap G_{\Sigma_2} = (1)$;
(3) $T = \prod_{\alpha \in \Pi} T_\alpha$.

In each $(G_\alpha)_L$ ($\alpha \in \Pi$) we choose an element w_α which represents a nontrivial element $\bar{w}_\alpha$ of the Weyl group $W(T_\alpha, G_\alpha)$, and let X'_α denote the corresponding "large cell" in the Bruhat decomposition of G_α; i.e., we put $X'_\alpha = B_\alpha w_\alpha B_\alpha$, where $B_\alpha = T_\alpha U_\alpha$ is a Borel subgroup of G_α. Since $\sigma(B_\alpha) = B_{-\alpha} = T_\alpha U_{-\alpha}$ and $\sigma(w_\alpha) = w_\alpha t$ for suitable t in T_α, it follows that $\sigma(X'_\alpha) = B_{-\alpha} w_\alpha B_{-\alpha}$; consequently the variety

$$ X_\alpha = X'_\alpha \cap \sigma(X'_\alpha) = B_\alpha w_\alpha B_\alpha \cap B_{-\alpha} w_\alpha B_{-\alpha} \tag{9.30} $$

is defined over K and is an open, dense subset of G_α. In particular, $\dim X_\alpha = 3$. Also put $Y_\alpha = X_\alpha T = T X_\alpha$ and note that actually $Y_\alpha \simeq X_\alpha \times T_{\Pi \setminus \{\alpha\}}$ by property (2) of (9.29).

In §2.1.10 we noted that $S = \{ \bar{w}_\alpha : \alpha \in \Pi \}$ generates $W = W(T, G)$, where (W, S) is a Coxeter group. Let us take an element $\bar{w}$ in W which has maximal length with respect to the set of generators S. It is well known (cf. Bourbaki [4]) that such an element is unique and is characterized by the fact that it transforms positive roots to negative ones; moreover r, the length of its reduced decomposition $\bar{w} = \bar{w}_{\alpha_1} \dots \bar{w}_{\alpha_r}$ ($\alpha_i \in \Pi$), equals the number of positive roots. (Some of the α_i may well coincide.) Put $X = X_{\alpha_1} \times \dots \times X_{\alpha_r}$, $Y = Y_{\alpha_1} \times \dots \times Y_{\alpha_r}$, and let $\varphi: Y \to G$ be the product morphism. Moreover, let us define the action of T^{r-1} on Y as follows: if $t = (t_1, \dots, t_{r-1}) \in T^{r-1}$ and $y = (y_1, \dots, y_r) \in Y$, then

$$ yt = (y_1 t_1,\ t_1^{-1} y_2 t_2,\ \dots,\ t_{r-2}^{-1} y_{r-1} t_{r-1},\ t_{r-1}^{-1} y_r). \tag{9.31} $$

(In this section it will be more convenient for us to view the action on the right, and not, as is customary, on the left.) It follows from $Y_\alpha = X_\alpha T =$

TX_α that the right side of (9.31) lies in Y, and consequently the action is well-defined. In addition, it is immediately evident from (9.31) that the stabilizer in T^{r-1} of any y in Y is trivial.

LEMMA 9.20.

(1) *For any extension P/K we have $\varphi(X_P) = \varphi(Y_P)$.*
(2) *φ is dominant and its nonempty fibers are the orbits of T^{r-1}.*

(In current terminology, the second assertion means, in particular, that Y is a torsor with base $\varphi(Y)$ and structure group T^{r-1}.)

PROOF: (1) Since $Y_\alpha \simeq X_\alpha \times T_{\Pi\setminus\{\alpha\}}$, we have $(Y_\alpha)_P = (X_\alpha)_P(T_{\Pi\setminus\{\alpha\}})_P$. But, as we noted above, T normalizes X_α, and therefore T_P normalizes $(X_\alpha)_P$. On the other hand, $(X_\alpha)_P(T_\alpha)_P = (X_\alpha)_P$. With these facts it is easy to show that $\varphi((Y_{\alpha_1})_P \times \cdots \times (Y_{\alpha_r})_P) = \varphi((X_{\alpha_1})_P \times \cdots \times (X_{\alpha_r})_P)$.

(2) For $m \le r$ consider the product morphism

$$\varphi^{(m)}\colon Y^{(m)} = Y_{\alpha_1} \times \cdots \times Y_{\alpha_m} \to G,$$

and by induction on m we show that the fibers of $\varphi^{(m)}$ are the orbits of the action of T^{m-1} on $Y^{(m)}$, given by the analogous formula to (9.31):

$$(9.32)\quad (y_1, \dots, y_m)(t_1, \dots, t_{m-1}) = (y_1 t_1,\ t_1^{-1} y_2 t_2,\ \dots,\ t_{m-2}^{-1} y_{m-1} t_{m-1},\ t_{m-1}^{-1} y_m).$$

It follows from (9.32) that $\varphi^{(m)}(yT^{m-1}) = \varphi^{(m)}(y)$ for any y in $Y^{(m)}$. Therefore it remains to show that if $\varphi^{(m)}(y) = \varphi^{(m)}(z)$, then $z = yt$ for suitable t in T^{m-1}. This is obvious for $m = 1$. So, let $m > 1$, and let y_i and z_i in Y_{α_i} $(i = 1, \dots, m)$ be such that

$$(9.33)\qquad y_1 \dots y_m = z_1 \dots z_m.$$

Let us put $g = y_m z_m^{-1}$ and show that $g \in T$. It follows from (9.30) that $Y_\alpha \subset Bw_\alpha B \cap B^- w_\alpha B^-$, where B is the Borel subgroup of G associated with Π and B^- is the opposite Borel subgroup. We shall show that $g \in B$; similarly, one can show that $g \in B^-$, and then $g \in B \cap B^- = T$, as desired. Since G_{α_m} is normalized by T, it follows that $g \in G_{\alpha_m} T$. If we assume that $g \notin B$, then the Bruhat decomposition

$$G_{\alpha_m} = B_{\alpha_m} \cup B_{\alpha_m} w_{\alpha_m} B_{\alpha_m}$$

implies that $g \in (B_{\alpha_m} w_{\alpha_m} B_{\alpha_m})T \subset Bw_{\alpha_m} B$. Since $\bar{w}_{\alpha_1} \dots \bar{w}_{\alpha_m}$ is a segment of the reduced decomposition of $\bar{w}$ and hence is irreducible, it follows

that $(Bw_{\alpha_1} \dots w_{\alpha_i} B)(Bw_{\alpha_{i+1}} B) = Bw_{\alpha_1} \dots w_{\alpha_{i+1}} B$ for any $i < m$ (cf. Steinberg [2]). This yields

$$z' = z_1 \dots z_{m-1} \in Bw_{\alpha_1} \dots w_{\alpha_{m-1}} B,$$
$$y' = y_1 \dots y_{m-1} g \in Bw_{\alpha_1} \dots w_{\alpha_m} B.$$

But by (9.33) we have $y' = z'$, which contradicts the fact that the double cosets in the Bruhat decomposition of G are disjoint. Thus, $g \in T$. Then $y_{m-1} g \in Y_{\alpha_{m-1}}$ and by the induction hypothesis $y' = z'$ implies the existence of $t_1, \dots, t_{m-2}$ in T such that

$$z_1 = y_1 t_1,\ z_2 = t_1^{-1} y_2 t_2,\ \dots,\ z_{m-1} = t_{m-2}^{-1} y_{m-1} g.$$

Then, putting $t_{m-1} = g$ and $t = (t_1, \dots, t_{m-1})$, we obtain $(y_1, \dots, y_m)t = (z_1, \dots, z_m)$.

Thus, the fibers of φ are the orbits of T^{r-1} and therefore have dimension $l(r-1)$, where l is the rank of G. It then follows from the theorem on the dimension of fibers and the image of a morphism that

$$\dim \overline{\varphi(Y)} = r \dim Y_\alpha - (r-1)l = r(3 + (l-1)) - (r-1)l = 2r + l = \dim G,$$

since G has exactly $2r$ roots. Thus, φ is dominant and Lemma 9.20 is proved.

It follows from the fact that $\varphi\colon Y \to G$ is dominant and from Proposition 3.3 that $\varphi(Y_\infty)$ contains U, an open subset of G_∞. Let us show that for g in $G_K \cap U$ we do have (9.28). Let $y \in \varphi^{-1}(g)_{\bar{K}}$. Then $\varphi(y) = \varphi(\theta(y)) = g$ for any θ in $\mathrm{Gal}(\bar{K}/K)$; so by Lemma 9.20 there is a unique t_θ in $T_{\bar{K}}^{r-1}$ satisfying $\theta(y) = yt_\theta$. One can easily verify that $\xi = \{ t_\theta : \theta \in \mathrm{Gal}(\bar{K}/K) \}$ defines a cocycle with values in T^{r-1}; moreover, the conditions

$$g \in \varphi(Y_P) \quad \text{and} \quad \xi \in \ker(H^1(K, T^{r-1}) \to H^1(P, T^{r-1}))$$

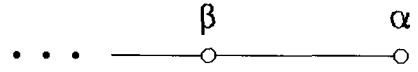
are equivalent for any extension P of K. By definition T is split over L, so $H^1(L, T^{r-1}) = 1$, and consequently $g \in \varphi(Y_L)$. But $\varphi(Y_L) = \varphi(X_L)$ (Lemma 9.20 (1)), therefore one can choose $x = (x_1, \dots, x_r)$ in X_L such that $\varphi(x) = g$. Let $\xi = \{t_\theta\}$ be a cocycle in $H^1(K, T^{r-1})$ such that $\theta(x) = xt_\theta$. A basic property of ξ which we shall need below is that

$$\xi \in \ker(H^1(K, T^{r-1}) \to \prod_{v \in V_\infty^K} H^1(K_v, T^{r-1})),$$

since by definition $g \in \varphi(Y_\infty)$. Moreover, $g \in \varphi(Y_L)$, and therefore ξ lies in $H^1(L/K, T^{r-1})$, i.e., is given by a single element $t = t_\sigma \in T_L^{r-1}$ such that $t\sigma(t) = 1$. With these facts, we show how to pass from

$$(9.34)\qquad g = x_1 \dots x_r$$

to a factorization as in (9.28). Let α in Π be an end root in the Dynkin diagram of R, and let β be a (unique) adjacent root



Put $\Sigma = \Pi \setminus \{\alpha\}$. It suffices to establish the existence of g_i's in G_{i_K} $(i = 1, \dots, d)$, where each G_i is a simple simply connected L-split K-subgroup of G of rank 2, such that $g' = g_d \dots g_1 g$ can be written as

$$g' = h_1 h_2, \tag{9.35}$$

where $h_1 \in (G_\Sigma)_L$ and $h_2 \in (G_\alpha)_L$. Indeed, since $g' \in G_K$ and $G_\Sigma \cap G_\alpha = (1)$, it follows from (9.35) that $h_1 \in (G_\Sigma)_K$ and $h_2 \in (G_\alpha)_K \subset (G_{\{\alpha,\beta\}})_K$; therefore the factorization $g = g_1^{-1} \dots g_d^{-1} h_1 h_2$, equivalent to (9.35), satisfies all the requirements of (9.28). To pass from (9.34) to (9.35) one must rearrange the factors in (9.34) in such a manner as to collect separately all the x_i for which $\alpha_i \in \Sigma$ and all the x_i for which $\alpha_i = \alpha$, compensating for the permutation of factors by multiplying by suitable g_i's. This is easily done using an obvious inductive argument, based on the following

PROPOSITION 9.8. *Suppose z in G_K has the form $z = z_1 z_2 x_i \dots x_r$, where $z_1 \in (G_\Sigma)_L$, $z_2 \in (G_\alpha)_L$ and the x_i are from (9.34). Then one can find a simple simply connected L-split K-subgroup H of G of rank 2 and elements g in H_K, z_3 in $(G_\Sigma)_L$, and z_4 in $(G_\alpha)_L$ such that $gz = z_3 z_4 x_{i+1} \dots x_r$.*

PROOF: If $\alpha_i = \alpha$ then put $z_3 = z_1$ and $z_4 = z_2 x_i$. If $\alpha_i \neq \alpha, \beta$, then there are no roots of the form $j\alpha_i + k\alpha$ (where $j, k \in \mathbb{Z} \setminus (0)$); therefore it follows from the commutator relations (cf. Steinberg [2]) that G_{α_i} and G_α commute. In particular, z_2 and x_i commute, so one can put $z_3 = z_1 x_i$ and $z_4 = z_2$. Therefore, it remains to consider the case $\alpha_i = \beta$. Let $t = (t_1, \dots, t_{r-1}) \in T_L^{r-1}$ be the element introduced above satisfying $t\sigma(t) = 1$ and $\sigma(x) = xt$. Then

$$\sigma(x_1) = x_1 t_1,\ \sigma(x_2) = t_1^{-1} x_2 t_2,\ \dots,\ \sigma(x_r) = t_{r-1}^{-1} x_r. \tag{9.36}$$

We shall work with the "parts" of t; namely, put $u = t_i$ and let s denote the projection of t_{i-1} to T_Σ in the sense of the direct product decomposition $T = T_\Sigma \times T_\alpha$. If follows from $t\sigma(t) = 1$ that $s\sigma(s) = u\sigma(u) = 1$, i.e., that s and u determine cocycles in $H^1(L/K, T_\Sigma)$ and $H^1(L/K, T)$ respectively. Note that these cocycles become trivial when one passes to real localizations, since by construction the cocycle ξ in $H^1(L/K, T^{r-1})$ determined by t lies in

$$\ker(H^1(K, T^{r-1}) \to \prod_{v \in V_\infty^K} H^1(K_v, T^{r-1})).$$

Put $a = z_1$, $b = z_1 z_2 x_i$.

LEMMA 9.21. $\sigma(a) = as$, $\sigma(b) = bu$.

PROOF: Since $z = b x_{i+1} \dots x_r \in G_K$, it follows that

$$b^{-1}\sigma(b) = (x_{i+1} \dots x_r)\sigma(x_{i+1} \dots x_r)^{-1} = t_i = u$$

by (9.36). Similarly, it can be shown that $\sigma(az_2) = az_2 t_{i-1}$. By construction, $t_{i-1} = ss'$ for some s' in T_α; hence

$$s^{-1}a^{-1}\sigma(a) = (s^{-1} z_2 s) s' \sigma(z_2)^{-1} \in G_\Sigma \cap G_\alpha = (1)$$

and $\sigma(a) = as$, as desired.

LEMMA 9.22. *Let f be an element of G_L such that $e = f^{-1}\sigma(f) \in T_L$, and let $\delta = \operatorname{Int} f$ be the corresponding inner automorphism. Then, for any subset Δ of Π, the group $\delta(G_\Delta)$ and the restriction $\delta\,|_T : T \to \delta(T)$ are defined over K.*

PROOF: $\delta(G_\Delta)$ and $\delta\,|_T$ are defined over L *a fortiori*; to prove they are defined over K it suffices to establish that they are invariant under σ. We have $\sigma(fG_\Delta f^{-1}) = \sigma(f) G_\Delta \sigma(f)^{-1} = feG_\Delta e^{-1} f^{-1} = fG_\Delta f^{-1}$, since T normalizes G_Δ. Similarly, for any t in T_L we obtain $\sigma(ftf^{-1}) = fe\sigma(t)e^{-1}f^{-1} = f\sigma(t)f^{-1}$, as desired.

Now we can complete the proof of Proposition 9.8. Put $\delta = \operatorname{Int} a$ and $H = \delta(G_{\{\alpha,\beta\}})$. It follows from Lemmas 9.21 and 9.22 that H is defined over K, and H obviously has rank 2. It suffices to find h in H_K, y_1 in $(H_\beta)_L$, and y_2 in $(H_\alpha)_L$, where $H_\alpha = \delta(G_\alpha)$ and $H_\beta = \delta(G_\beta)$, such that

$$h\delta(z_2 x_i) = y_1 y_2, \tag{9.37}$$

since then

$$\begin{aligned} hz = h\delta(z_2 x_i) a x_{i+1} \dots x_r &= y_1 y_2 a x_{i+1} \dots x_r \\ &= a\delta^{-1}(y_1)\delta^{-1}(y_2) x_{i+1} \dots x_r, \end{aligned}$$

and one can put $z_3 = a\delta^{-1}(y_1)$ and $z_4 = \delta^{-1}(y_2)$.

We have

$$\sigma(\delta(z_2 x_i)) = \sigma(ba^{-1}) = bus^{-1}a^{-1} = \delta(z_2 x_i)\delta(us^{-1}). \tag{9.38}$$

Therefore, the problem reduces to finding y_1 and y_2 for which

$$\sigma(y_1 y_2) = y_1 y_2 \delta(us^{-1}). \tag{9.39}$$

Indeed, in this case (9.38) and (9.39) yield that $h = \delta(z_2 x_i)(y_1 y_2)^{-1}$ lies in H_K and obviously satisfies (9.37).

LEMMA 9.23. *Let $\gamma \in \Pi$ and let d be an element in $(T_\gamma)_L$ such that $d\sigma(d) = 1$. Assume that the cocycle in $H^1(L/K, T_\gamma)$ determined by d lies in* $\ker(H^1(K, T_\gamma) \to \prod_{v \in V_\infty^K} H^1(K_v, T_\gamma))$. *Then, for any f in G_L such that $f^{-1}\sigma(f) \in T_L$, there is an element g in $f(G_\gamma)_L f^{-1}$ satisfying $g^{-1}\sigma(g) = fdf^{-1}$.*

PROOF: Put $\delta = \operatorname{Int} f$. By the previous lemma, $\delta(G_\gamma)$ and the restriction of δ to T are defined over K. It follows that $t = \delta(d)$ determines a cocycle ξ in $H^1(L/K, \delta(T_\gamma))$ which lies in

$$\ker(H^1(K, \delta(T_\gamma)) \to \prod_{v \in V_\infty^K} H^1(K_v, \delta(T_\gamma)).$$

But then, since the Hasse principle holds for $\delta(G_\gamma)$, we obtain

$$\xi \in \ker(H^1(K, \delta(T_\gamma)) \to H^1(K, \delta(G_\gamma))),$$

i.e., $t = g^{-1}\sigma(g)$ for suitable g in $\delta(G_\gamma)_L$, and the lemma is proved.

In our case $\delta(us^{-1}) \in H \cap \delta(T) = \delta(T_{\{\alpha,\beta\}})$; so $d = us^{-1} \in T_{\{\alpha,\beta\}}$, and one can write $d = d_1 d_2$, where $d_1 \in (T_\beta)_L$ and $d_2 \in (T_\alpha)_L$. It follows by definition that d_1 and d_2 determine cocycles in $H^1(L/K, T_\beta)$ and $H^1(L/K, T_\alpha)$, respectively, which become trivial when one passes to real localizations. Then Lemma 9.23 immediately implies that there exists y_1 in $(H_\beta)_L$ such that $y_1^{-1}\sigma(y_1) = ad_1a^{-1}$. Put $f = y_1 a$. Then

$$f^{-1}\sigma(f) = a^{-1}y_1^{-1}\sigma(y_1)a = d_1 \in T_L.$$

Applying Lemma 9.23 once more, we find p in $f(H_\alpha)_L f^{-1}$ satisfying $p^{-1}\sigma(p) = fd_2f^{-1}$. Putting $y_2 = y_1^{-1}py_1$, we obtain

$$\begin{aligned}\sigma(y_1y_2) &= \sigma(y_1)\sigma(y_1)^{-1}\sigma(p)\sigma(y_1) \\ &= pfd_2f^{-1}y_1ad_1a^{-1} = pfd_2d_1a^{-1} = y_1y_2\sigma(d_1d_2),\end{aligned}$$

and (9.39) is proved. This completes the proof of Proposition 9.8 and Theorem 9.7.

As we noted in §9.1, Proposition 6.17 implies that Theorem 9.7 can be applied to any simply connected K-anisotropic group of type B_n, C_n, E_7, E_8, F_4 or G_2; thus the groups of K-rational points of these groups are always projectively simple.

9.5. The congruence subgroup problem (a survey).

Let G be a simply connected simple K-group, and let N be a noncentral normal subgroup of G_K. If S is a finite subset of V^K containing $T \cup V_\infty^K$ such that G_S is noncompact (i.e., $\operatorname{rank}_S G = \sum_{v \in S} \operatorname{rank}_{K_v} G \geq 1$),[3] then $\Gamma = G_{\mathcal{O}(S)}$ is infinite and, as the proof of Theorem 9.8 shows,

$$G_K/N \simeq \Gamma/\Gamma \cap N. \tag{9.40}$$

We inferred the finiteness of the quotient group on the left from the finiteness of the quotient group on the right; and the latter is finite when $\operatorname{rank}_S G \geq 2$ and $\Gamma \cap N \not\subset Z(G)$. This connection between the normal subgroup structure of G_K, the group of K-rational points, and that of its S-arithmetic subgroups (for arbitrary $S \subset V^K$ containing V_∞^K) calls for further investigation. In particular, one naturally wonders what property of normal subgroups of Γ guarantees that Conjectures 9.1 and 9.2 will hold for G_K? Γ always contains an extensive family of normal subgroups of finite index, consisting of the congruence subgroups

$$\Gamma(\mathfrak{a}) = \{\, g \in \Gamma : g \equiv e \pmod{\mathfrak{a}} \,\}, \tag{9.41}$$

corresponding to the nonzero ideals $\mathfrak{a}$ of $\mathcal{O}(S)$. (As usual, when dealing with integral or S-integral points, we fix a matrix realization of G; in particular, the equality in (9.41) is viewed with respect to this realization.) Thus, *à propos* the normal structure of Γ, one naturally wonders whether the congruence subgroups thus defined exhaust *all* the normal subgroups of Γ of finite index? Further analysis shows that the best way of putting the question is as follows:

(9.42) *Does any normal subgroup of finite index in Γ contain a suitable congruence subgroup $\Gamma(\mathfrak{a})$?*

This question has become known as the *congruence subgroup problem.* Its connection with the normal structure of groups of rational points is treated by

PROPOSITION 9.9. *Let G be a simple simply connected K-group, and let S be a finite subset of V^K containing V_∞^K. Assume that* $\operatorname{rank}_S G \geq 1$ *and that for $\Gamma = G_{\mathcal{O}(S)}$ the answer to the congruence subgroup problem (9.42) is affirmative. Then Conjecture 9.2 (cf. §9.1) holds for G_K.*

[3] Recall that T denotes the set of those v in V_f^K for which G is K_v-anisotropic, cf. §9.1.

PROOF: Let $\bar{N}$ denote the closure of N in the group of S-adeles G_{A_S}. Then, arguing as in the proofs of Lemma 9.1 and Theorem 9.8, we can easily show that

$$\bar{N} = N_{T\setminus(T\cap S)} \times G_{A_{S\cup T}}. \tag{9.43}$$

We wish to prove that

$$N = G_K \cap N_{T\setminus(T\cap S)} = G_K \cap H,$$

where $H = N_{T\setminus(T\cap S)} \times G_{T\cap S}$ is an open normal subgroup of G_T. By assumption, for a suitable nonzero ideal $\mathfrak{a}$ of $\mathcal{O}(S)$ one has $\Gamma(\mathfrak{a}) \subset \Gamma \cap N$. The definition of the adele topology implies that there exists an open subgroup U of G_{A_S} such that $U \cap G_K = \Gamma(\mathfrak{a})$. Then $U_0 = U \cap \bar{N}$ is an open subgroup of G_{A_S} contained in $\bar{N}$, and therefore $\bar{N} = U_0 N$. Taking the intersection with G_K and applying (9.43) we obtain

$$G_K \cap N_{T\setminus(T\cap S)} = (U_0 \cap G_K)N.$$

But by assumption $U_0 \cap G_K \subset U \cap G_K = \Gamma(\mathfrak{a}) \subset N$, from which it follows that $G_K \cap N_{T\setminus(T\cap S)} = N$, as desired.

Observe that our argument indicates that necessarily $S \cap T = \emptyset$ in order for the congruence subgroup problem to be true for Γ. Indeed, suppose $v_0 \in S \cap T$ and let W be an arbitrary proper, open normal subgroup of $G_{K_{v_0}}$. Then the weak approximation theorem implies that the following properties hold for the normal subgroup $N = G_K \cap W$:

(1) $G_K/N \simeq G_{K_{v_0}}/W \neq 1$,
(2) $N_{T\setminus(T\cap S)} = G_{T\setminus(T\cap S)}$.

Now suppose that the congruence subgroup problem has an affirmative answer for $\Gamma = G_{\mathcal{O}(S)}$. Then it follows from the proof of Proposition 9.9 and property (2) that $N = G_K$; but this contradicts property (1).

Thus, if one solves the congruence subgroup problem affirmatively for $\Gamma = G_{\mathcal{O}(S)}$ then one can solve the problem of describing the normal subgroups of G_K. In this sense the congruence subgroup problem is, *a priori*, a more general and more complicated problem. Indeed, it has long been known that $SL_n(\mathbb{Q})$ $(n \geq 2)$ has no normal subgroups, although the congruence subgroup problem for $SL_n(\mathbb{Z})$ $(n \geq 3)$ was only fully solved in 1964 and for $SL_2(\mathbb{Z})$, surprisingly, the answer was negative. To give the reader an accurate impression of how these problems interrelate, we present a historical survey of research on the congruence subgroup problem, which we recommend comparing with the historical background given in §7.2 and §9.1.

The fact that the answer to the congruence subgroup problem is negative for $\Gamma = SL_2(\mathbb{Z})$ was first noted by F. Klein [1] in 1880, in connection with his study of modular functions. For $\Gamma = SL_3(\mathbb{Z})$, however, little progress was made for many years, until, in 1965–1965, Bass-Lazard-Serre [1] and Mennicke [1] found a positive solution of the problem for $SL_n(\mathbb{Z})$ $(n \geq 3)$. Subsequent investigation (cf. Bass-Milnor-Serre [1]) revealed that for $\Gamma = SL_n(\mathcal{O})$, where $\mathcal{O}$ is the ring of integers of an algebraic number field K, the answer to the congruence subgroup problem depends not only on the algebraic properties of SL_n itself, but also on the arithmetic of the ground field K. If K is not totally imaginary, then, as before, the congruence problem has a positive solution. On the other hand, if K is totally imaginary, then the answer to (9.42) is negative; however, there exists a subgroup Γ' of Γ of finite index, for which (9.42) is solved affirmatively. It can be shown that for $\Gamma = SL_2(\mathbb{Z})$ there is no such subgroup. Thus, when the answer to (9.42) is negative one needs to characterize the degree to which the congruence subgroup property described in (9.42) is violated. This leads to the important concept of the congruence kernel (cf. Serre [6], Humphreys [3]), which we now define.

Let G be an algebraic group defined over K, and let S be a finite subset of V^K containing V_∞^K. Straightforward verification by means of Proposition 1 in Bourbaki [2, Ch. 3, §1.2] shows that two Hausdorff topologies τ_a and τ_c can be defined on G_K under which G_K is a topological group. The first, called the arithmetic topology, has a fundamental system of neighborhoods of the identity consisting of all subgroups of Γ of finite index; the second, called the congruence topology, has as its fundamental system of neighborhoods of the identity the set of all congruence subgroups $\Gamma(\mathfrak{a})$. With the results in *loc. cit.* Ch. 3, §3.4, one can show that there exist completions $\hat{G}$ and $\bar{G}$ of G_K under these topologies. In addition, since τ_a is stronger than τ_c, this gives rise to the continuous homomorphism $\pi\colon \hat{G} \to \bar{G}$ whose kernel $C^S(G)$ is called the *congruence kernel.* One also has completions $\hat{\Gamma}$ and $\bar{\Gamma}$ of Γ under the induced topologies, which are the closures of Γ in $\hat{G}$ and $\bar{G}$, respectively. Then π induces a continuous homomorphism $\pi_0\colon \hat{\Gamma} \to \bar{\Gamma}$; and it is easy to see that $\ker\pi = \ker\pi_0 \subset \hat{\Gamma}$. Also $\hat{\Gamma}$ is precisely the *profinite completion* of Γ, i.e., $\varprojlim \Gamma/N$ taken over all the normal subgroups of finite index. This easily yields the following result (cf. Serre [2], Humphreys [3]).

PROPOSITION 9.10. *π is surjective, and its kernel $C^S(G)$ is a profinite group. Moreover, $C^S(G)$ is trivial if and only if the congruence subgroup problem as stated in (9.42) holds for $\Gamma = G_{\mathcal{O}(S)}$.*[4]

Thus, $C^S(G)$ measures the degree of deviation from the positive solu-

[4] Most of the results in this section will be presented without proofs.

tion of the congruence subgroup problem as stated in (9.42). Therefore, in contrast to the classical formulation given in (9.42), the contemporary formulation of the congruence subgroup problem is usually understood as the problem of computing $C^S(G)$. Using the concept of congruence kernel, we can state the result of Bass-Milnor-Serre [1] as follows:

THEOREM 9.14. *Let G be either $\mathbf{SL}_n$ $(n \geq 3)$ or $\mathbf{Sp}_{2n}$ $(n \geq 2)$ over an algebraic number field K. Then for $S = V_\infty^K$ we have*

$$C^S(G) = \begin{cases} 1 & \text{if } K \text{ is not totally imaginary,} \\ E(K) & \text{if } K \text{ is totally imaginary.} \end{cases} \tag{9.44}$$

where $E(K)$ is the group of roots of unity in K.

Thus, for the groups under consideration, the congruence kernel is finite. On the other hand, one can show that for $SL_2(\mathbb{Z})$ it is a free profinite group of countable rank (cf. Melnikov [1]).

Matsumoto [2], elaborating on the method used in Bass-Milnor-Serre [1], obtained a similar computation of the congruence kernel for all universal Chevalley groups of rank ≥ 2. In the remaining case, SL_2, first Mennicke [2] solved (9.42) positively for $SL_2\left(\mathbb{Z}[\frac{1}{p}]\right)$, and then Serre [6] studied the general case and showed that for $|S| > 1$ the congruence kernel is trivial if S does not consist entirely of imaginary places, and is isomorphic to $E(K)$ otherwise (cf. (9.49) below). On the basis of his analysis of the available results, Serre [6] formulated the following congruence subgroup conjecture:[5]

(9.45) Let G be a simple simply connected algebraic K-group. Then $C^S(G)$ should be finite if $\operatorname{rank}_S G = \sum_{v \in S} \operatorname{rank}_{K_v} G \geq 2$ and $\operatorname{rank}_{K_v} G \geq 1$ for v in $S \setminus V_\infty^K$, and should be infinite if $\operatorname{rank}_S G = 1$.

(It may seem strange to the reader that, having defined $C^S(G)$ for arbitrary algebraic groups, we speak of computing it only for simple simply connected groups. Actually, this does not restrict the generality, since one can show (cf. Platonov [6], Platonov-Sharomet [1]) that the computation of $C^S(G)$ reduces to the semisimple case, and $C^S(G)$ is always infinite for a non-simply connected semisimple K-group G whose simply connected covering $\tilde{G}$ has strong approximation relative to S (cf. Serre [2], Platonov [20]).

We are interested primarily in the first part of the congruence subgroup conjecture, which treats to the finiteness of $C^S(G)$. Now we set forth

[5] Actually Serre did not impose the condition that $\operatorname{rank}_{K_v} G \geq 1$ for $v \in S \setminus V_\infty^K$; but, as we have seen, this condition is necessary.

the main line of reasoning which has been applied in all the work on this question.

By definition $C = C^S(G)$ enters the exact sequence

$$1 \to C \to \hat{G} \to \bar{G} \to 1. \tag{9.46}$$

Consider the initial segment of the Hochschild-Serre spectral cohomological sequence, corresponding to (9.46):

$$H^1(\bar{G}) \xrightarrow{\varphi} H^1(\hat{G}) \to H^1(C)^{\bar{G}} \xrightarrow{\psi} H^2(\bar{G}), \tag{9.47}$$

where $H^i(*)$ denotes the i-th continuous cohomology group with coefficients in the one-dimensional torus $\mathbb{R}/\mathbb{Z}$. It is easy to see that

$$\operatorname{coker} \varphi = \overline{[G_K, G_K]}/[G_K, G_K],$$

where bar denotes closure in G_K under the S-arithmetic topology. Furthermore, one notes that the S-congruence topology on G_K is the topology induced by the topology in the group of S-adeles under the embedding $G_K \hookrightarrow G_{A_S}$. Therefore, if we suppose that the conditions of the congruence conjecture hold here, then the strong approximation theorem implies that $\bar{G}$ can be identified with G_{A_S}. However, by assumption G_K embeds in $\bar{G}$ as well as in $\hat{G}$; i.e., (9.46) splits over G_K and actually is a "universal" sequence with this property (cf. Prasad-Raghunathan [2]). It follows that

$$\operatorname{Im} \psi = M(G, S),$$

where $M(G,S) = \ker(H^2(G_{A_S}) \to H^2(G_K))$ is the *metaplectic kernel* (viewing G_K as endowed with the discrete topology). Thus (9.47) yields the following exact sequence:

$$1 \to \operatorname{coker} \varphi \to H^1(C)^{\bar{G}} \to M(G, S) \to 1. \tag{9.48}$$

Unfortunately, in general $H^1(C)^{\bar{G}}$ provides information only about part of C. This term lets us reconstruct C in full only when C is central, i.e., when it lies in the center of $\hat{G}$, since then $H^1(C)^{\bar{G}} = H^1(C)$ is C^*, the Pontryagin dual of C.

THEOREM 9.15. *If C is central, then it is finite. Moreover, if* $\operatorname{coker} \varphi = 1$, *then $C^* = M(G, S)$.*

Indeed, the metaplectic kernel $M(G,S)$ is always finite (cf. Raghunathan [4], Prasad-Raghunathan [2]). On the other hand, by Theorem 9.8 $[G_K, G_K]$ has finite index in G_K; in particular, $\operatorname{coker} \varphi$ is also finite. Therefore, the finiteness of C follows from (9.48) and the remarks following it. The second assertion of the theorem is evident.

It should be noted that the finiteness of C is in fact equivalent to its centrality. More precisely, if C is finite and G_K is projective simple, then C is central. Thus, the qualitative aspect of determining C (i.e., proving its finiteness) reduces to proving its centrality.

The next stage of the investigation naturally involves the precise computation of C. To do so, first of all one must establish whether or not $\operatorname{coker}\varphi$ is trivial. Clearly $\operatorname{coker}\varphi = 1$ if G_K has no proper noncentral normal subgroups. Therefore, by the results of §9.1, $\operatorname{coker}\varphi = 1$ if either G is K-isotropic and does not have type ${}^2E_6$, or if G has type B_l $(l \geq 2)$, C_l $(l \geq 2)$, D_l $(l \geq 4$, except for ${}^3D_4$, ${}^6D_4)$, E_7, E_8, F_4, or G_2, or if G is $\mathbf{SU}_m(L, f)$ $(m \geq 4)$ of a nondegenerate Hermitian form f over a quadratic extension L/K.

Now suppose G is a K-anisotropic inner form of type A_n and that $T = \{ v \in V_f^K : G \text{ is } K_v\text{-anisotropic} \}$. The conditions of the congruence subgroup conjecture imply $S \cap T = \emptyset$; so, by Theorem 9.4, $[G_K, G_K]$ is closed in the S-arithmetic topology, and again $\operatorname{coker}\varphi = 1$. Thus, there remain only forms of type ${}^2A_n$, ${}^3D_4$, ${}^6D_4$ and E_6, for which the triviality of $\operatorname{coker}\varphi$ has not been established; in other words, in most instances computation of C (when it is central) reduces to computation of $M(G, S)$.

$M(G, S)$ has been determined for Chevalley groups in the fundamental works of Moore [1] and Matsumoto [1]. Their results, resembling (9.44), are as follows:

THEOREM 9.16. *Let G be a simple simply connected K-split group, and let S be a finite subset of V^K containing V_∞^K. Then*

$$M(G,S) = \begin{cases} 1, & \text{if } \exists v \in S : K_v \neq \mathbb{C}, \\ E(K) & \text{if } \forall v \in S : K_v = \mathbb{C}. \end{cases} \tag{9.49}$$

The case of quasisplit groups has been studied by Deodhar [1].

Lively interest in this question during the late 60's was followed by more than a decade of neglect. Interest in the subject revived in the 80's when Prasad-Raghunathan [2, 3] computed $M(G, S)$ for all K-isotropic groups (for the classical groups, cf. also Bak-Rehman [1], [2], Bak [1]).

THEOREM 9.17. *Let G be a simple simply connected K-isotropic group. Then*

$$M(G,S) = \begin{cases} 1, & \text{if } S \neq V_\infty^K, \\ \subset E(K) & \text{if } S = V_\infty^K. \end{cases}$$

Prasad and Raghunathan's proof uses various K-subgroups of G of type $\mathbf{SL}_2$, whose construction depends on the fact that G is K-isotropic. Therefore their arguments could not be carried over to the K-anisotropic case,

which was investigated by Rapinchuk [3], [4], [6] using other methods. Unfortunately, the results are not yet as unified as those of Theorem 9.17, and will have to be stated separately for the various types of groups.

INNER FORMS OF TYPE A_{n-1}: Here $G = \mathbf{SL}_1(D)$, where D is a skew field of index n over K. Put $S_e = \{ v \in V^K \setminus S : D \otimes_K K_v \simeq M_2(F_v)$, where F_v is a division algebra over $K_v \}$ and $s = |S_e|$ (s is finite when $n > 2$ and infinite when $n = 2$).

THEOREM 9.18. *Suppose S contains a non-Archimedean valuation v_0 such that $D \otimes_K K_{v_0} \simeq M_n(K_{v_0})$. Then $M(G, S)$ is a finite subgroup of the group $B(D, S) = (\mathbb{Z}/2\mathbb{Z})^s$. In general $M(G, S)$ is isomorphic to a finite subgroup of an extension of $B(D, S)$ by $E(K)$, the group of all the roots of unity in K.*

COROLLARY. *If $S_e = \emptyset$, in particular if n is odd, then*

$$M(G,S) = \begin{cases} 1, & \text{if } \exists v_0 \in S : K_{v_0} \neq \mathbb{C} \text{ and } D_{v_0} \simeq M_n(K_{v_0}), \\ \subset E(K) & \text{otherwise.} \end{cases}$$

(This result is actually analogous to the classical result (9.49).)

The theorem is proved by reducing the problem to the study of the reciprocity laws for maximal K-tori of G. In general outline, the reductive part of the argument is analogous to the classical argument of Matsumoto [2], the only difference being that in working with anisotropic groups one naturally encounters anisotropic tori. The reciprocity laws which arise are studied using algebraic number theory. (Analogous results on reciprocity laws were obtained independently by Prasad [3]).

OUTER FORMS OF TYPE A_{n-1}: These are the special unitary groups $G = \mathbf{SU}_m(D, f)$, where D is a finite-dimensional skew field with involution σ of the second kind, where K is the fixed subfield under σ of the center of D, and f is a nondegenerate σ-Hermitian form of degree m over D (cf. §2.3).

THEOREM 9.19. *Let $G = \mathbf{SU}_m(D, f)$ and let $m \geq 3$. If S contains a non-Archimedean valuation, then $M(G, S)$ has exponent ≤ 2. In general $M(G, S)$ is finite and is an extension of a group of exponent ≤ 2 by a subgroup of $E(K)$.*

PROOF: Uses Theorem 9.18, the properties of Hermitian forms, and the local computations of Prasad-Raghunathan [2].

THE REMAINING CLASSICAL GROUPS: Using Theorem 9.18 and the geometric realization of the classical groups, one obtains the following result:

THEOREM 9.20. *Let G be a simple simply connected K-group of type B_n $(n \geq 2)$, C_n $(n \geq 2)$, or D_n $(n \geq 5)$. Suppose S contains a non-Archimedean valuation v_0 and that the following conditions hold:*

(1) *if G has type B_n, then either $n \geq 3$, or $n = 2$ and G is K_{v_0}-split;*
(2) *If G has type C_n, then G is K_{v_0}-split.*

Then $M(G,S)$ has exponent ≤ 2. In general $M(G,S)$ is finite and is an extension of a group of exponent ≤ 2 by a subgroup of $E(K)$.

THE EXCEPTIONAL GROUPS:

THEOREM 9.21. *Let G be a simple K-group of type E_8, F_4 or G_2. Then $M(G,S)$ is trivial if S contains a non-Archimedean valuation, and is isomorphic to a subgroup of $E(K)$ if S does not contain such a valuation.*

For groups of type E_7 one obtains a result similar to Theorem 9.20. Thus, it remains to study the metaplectic kernel for groups of types ${}^2A_n$, D_4 and E_6.

We shall not give a detailed analysis of the main points of the proofs of Theorems 9.18–9.21, of which Theorem 9.18 is the most fundamental; however, we must prove the *weak metaplectic conjecture* (cf. Theorem 9.12), which we used to derive Theorem 9.3 and which actually comprises part of the proof of Theorem 9.18.

PROOF OF THEOREM 9.12: Let $G = \mathbf{SL}_1(D)$, where D is a skew field over K of index $n > 2$, and let $T = \{ v \in V_f^K : D_v \text{ is a skew field} \}$. We need to show that the restriction map $\theta: H^2(G_T) \to H^2(G_K)$ is injective. (Here and below we consider continuous cohomology groups with coefficients in the trivial discrete module $J = \mathbb{Q}/\mathbb{Z}$. One can show, however, that that in our case the same results can be obtained if the module of coefficients J is replaced by the one-dimensional torus $\mathbb{R}/\mathbb{Z}$.) To do so, consider a maximal subfield L of D such that all the local extensions L_v/K_v are unramified for $v \in T$, and let $F = \mathbf{R}^{(1)}_{L/K}(\mathbb{G}_m)$ be the corresponding maximal K-torus of G. We shall show that $\mu: H^2(G_T) \to H^2(F_K)$ is already injective. Clearly μ is a composition of the two restriction maps

$$H^2(G_T) \xrightarrow{\zeta} H^2(F_T) \xrightarrow{\eta} H^2(F_K),$$

and it suffices to establish that each map is injective.

LEMMA 9.24. *η is injective.*

PROOF: By §1.3.1 each cocycle α in $H^2(H)$ corresponds to a central extension

$$1 \to J \to E \xrightarrow{\varrho} H \to 1, \tag{9.50}$$

which can be used to associate with any two commuting subgroups A and B of H a bimultiplicative map $\delta: A \times B \to J$ given by $\delta(a,b) = [\tilde{a},\tilde{b}] = \tilde{a}\tilde{b}\tilde{a}^{-1}\tilde{b}^{-1}$, where $\tilde{a} \in \varrho^{-1}(a)$ and $\tilde{b} \in \varrho^{-1}(b)$. Moreover, if H is a topological group and α is continuous, then (9.50) is a topological extension and δ is continuous. With these preliminary remarks, we proceed immediately to proving that η is injective.

Let $\alpha \in \ker \eta$ and let

$$1 \to J \to E \xrightarrow{\varrho} F_T \to 1 \tag{9.51}$$

be the central extension corresponding to α. Then α is trivial if and only if this extension is trivial (i.e., if it splits); and, since F_T is abelian and J is divisible, this condition is equivalent to E being abelian (Lemma 1.1). To show that E is abelian, let us consider the bimultiplicative map $\delta: F_T \times F_T \to J$ defined above and show that it is trivial. The condition that $\alpha \in \ker \eta$ reduces to the fact that (9.51) splits over F_K, i.e., there exists a section $\varphi: F_K \to E$ of ϱ. It follows easily that the restriction of δ to $F_K \times F_K$ is trivial. But Proposition 7.8 implies that F_K is dense in F_T, therefore by continuity we obtain that δ is also trivial. Lemma 9.24 is proved.

LEMMA 9.25. *ζ is injective.*

PROOF: Easily obtained from the following result of Prasad and Raghunathan [5].

THEOREM 9.22. *For each v in T, the map $H^2(G_{K_v}) \to H^2(F_{K_v})$ is injective.*

Let $\alpha \in \ker \zeta$ and let

$$1 \to J \to E \xrightarrow{\varrho} G_T \to 1 \tag{9.52}$$

be the corresponding central extension. It is easy to see that, for each v in T, the cocycle α_v corresponding to the induced extension

$$1 \to J \to \varrho^{-1}(G_{K_v}) \to G_{K_v} \to 1 \tag{9.53}$$

lies in the kernel of $H^2(G_{K_v}) \to H^2(F_{K_v})$ and therefore, by Theorem 9.22, is trivial; i.e., (9.53) splits. In other words, for each v in T there is a continuous homomorphism $\varphi_v: G_{K_v} \to E$ which is a section of ϱ over G_{K_v}. A necessary and sufficient condition for the product $\varphi = \prod_{v \in T} \varphi_v$ to provide a section of ϱ over all G_T, is that the subgroups $\varrho^{-1}(G_{K_v})$ $(v \in T)$ of E be elementwise commuting. Let $v_1, v_2 \in T$ and let $\delta: G_{K_{v_1}} \times G_{K_{v_2}} \to J$

be the bimultiplicative map defined by taking the commutator of arbitrary pre-images. We wish to show that δ is trivial. Since δ is bimultiplicative, it can be viewed as a map

$$G_{K_{v_1}}/[G_{K_{v_1}}, G_{K_{v_1}}] \times G_{K_{v_2}}/[G_{K_{v_2}}, G_{K_{v_2}}] \to J.$$

However, since $\alpha \in \ker \zeta$, the restriction of δ to $F_{K_{v_1}} \times F_{K_{v_2}}$ is trivial. Therefore the triviality of δ is a consequence of the equality

$$G_{K_{v_i}} = F_{K_{v_i}}[G_{K_{v_i}}, G_{K_{v_i}}],$$

which follows from Theorem 1.8. This completes the proof of Lemma 9.25, and hence also of Theorem 9.12.

We have yet to prove Theorem 9.22. To simplify the notation, we put $C = G_{K_v}$, $B = F_{K_v}$, and for $i = 1, 2, \ldots$ we let C_i denote the congruence subgroup $G_{K_v} \cap (1 + \mathfrak{P}_v^i)$, where $\mathfrak{P}_v$ is the valuation ideal of D_v; we shall also write C_0 for C. Thus, our notation is consistent with that of §1.4.4, whose results we use in the proof. We shall prove that $\xi: H^2(C) \to H^2(B)$ is injective as follows. It is easy to see that

$$H^2(C) = \varinjlim H^2(C/C_i),$$

where the direct limit is taken with respect to the natural inflation maps $H^2(C/C_i) \to H^2(C/C_j)$ for $i \geq j$. Let $H^2(C)_i$ denote the image of $H^2(C/C_i)$ in $H^2(C)$. Then

$$H^2(C) = \bigcup_i H^2(C)_i.$$

Since C/C_1 is cyclic (cf. Proposition 1.8), it follows that $H^2(C/C_1) = 1$. Therefore, for any nontrivial α in $H^2(C)$ one can find minimal $i \geq 2$ for which $\alpha \in H^2(C)_i$. Having taken α in $\ker \xi$ and chosen the minimal i, we show that actually $\alpha \in H^2(C)_{i-1}$, from which it follows that $\alpha = 1$. We shall outline the argument, and leave the reader to work out the details.

Let $r \geq 2$, let $\alpha \in H^2(C/C_r)$, and let

$$1 \to J \to E \to C/C_r \to 1$$

be the central extension corresponding to α. For $s \leq r$ we put $E(s) = \varrho^{-1}(C_s/C_r)$. Below we always assume that the condition $n > 2$ of Theorem 9.12 is satisfied.

LEMMA 9.26.

(1) *$E(2)$ centralizes $E(r-1)$.*
(2) *α lies in the image of the inflation map $H^2(C/C_{r-1}) \to H^2(C/C_r)$ if and only if $E(1)$ centralizes $E(r-1)$.*

PROOF: Follows easily from the commutation relations for congruence subgroups (cf. §1.4.4) and is left to the reader.

A slight restatement of the lemma is helpful. Since $E(2)$ acts trivially on $E(r-1)$, the commutator map $(x, y) \to [x, y]$ gives a well-defined map

$$\Lambda^\alpha: E(1)/E(2) \times E(r-1)/E(r) \to J.$$

But clearly $E(1)/E(2) = C_1/C_2 = F(1)$ and $E(r-1)/E(r) = C_{r-1}/C_r = F(r)$, notation as in §1.4.4 (p. 34). It is easy to see that Λ^α is biadditive, and invariant under the natural action of $\Delta = E/E(1) = C/C_1$ on $F(1)$ and $F(r)$. Since the exponent of $F(i)$ is equal to the prime p corresponding to v, it follows that

$$\operatorname{Im} \Lambda^\alpha \subset \frac{1}{p}\mathbb{Z}/\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z}.$$

Thus, Λ^α can be viewed as the biadditive Δ-invariant map

$$F(1) \times F(r) \to F_p = \mathbb{Z}/p\mathbb{Z}.$$

Moreover,

$$\alpha \in \operatorname{Im}(H^2(C/C_{r-1}) \to H^2(C/C_r)) \Leftrightarrow \Lambda^\alpha = 0. \tag{9.54}$$

As in §1.4, let $B(F(1), F(r-1))$ denote the set of biadditive Δ-invariant maps $F(1) \times F(r-1) \to F_p$. It follows that the correspondence

$$H^2(C/C_r) \to B(F(1), F(r-1))$$

given by $\alpha \mapsto \Lambda^\alpha$ is a homomorphism of abelian groups, whose kernel is $\operatorname{Im}(H^2(C/C_{r-1}) \to H^2(C/C_r))$. Actually, this homomorphism is connected with one of the maps in the Hochschild-Serre spectral sequence corresponding to the extension

$$1 \to C_{r-1}/C_r \to C/C_r \to C/C_{r-1} \to 1.$$

Besides the Λ^α, we shall need the "higher" biadditive Δ-invariant maps Λ_i^α $(i < r)$:

$$\Lambda_i^\alpha: F(i) \times F(r-i) \to \mathbb{Z}/p\mathbb{Z},$$

which are induced by the map $(x, y) \to [x, y]$, where $F(i) = E(i)/E(i+1)$. To establish that the Λ_i^α are well-defined one must show that $E(i+1)$ centralizes $E(r-i)$ for any $i = 1, \ldots, r-1$.

PROPOSITION 9.11.

(1) *$E(i+1)$ centralizes $E(r-i)$ for any $i = 1, \dots, r-1$; so, the Λ_i^α are well-defined. Moreover, the Λ_i^α are biadditive and Δ-invariant.*

(2) *Suppose r is a multiple of n. Then for any α in $H^2(C/C_r)$ the map Λ^α is given by $\Lambda^\alpha(x,y) = \mathrm{Tr}_{l/F_p}(\lambda^\alpha x\sigma(y))$, where λ^α is a suitable element of the residue field l of D_v, σ is the canonical generator of $\mathrm{Gal}(l/k_v)$, and the $F(i)$ are identified with the subgroups of the additive group of l (cf. §1.4.4). In this case $\Lambda_i^\alpha(x,y) = \mathrm{Tr}_{l/F_p}(\lambda_i^\alpha x\sigma^i(y))$, where $\lambda_i^\alpha = \sum_{j=0}^{i-1}\sigma^j(\lambda^\alpha)$.*

PROOF: Uses Hall's identity:

$$\big[[a,b],{}^b c\big]\,\big[[b,c],{}^c a\big]\,\big[[c,a],{}^a b\big] = 1,$$

true for any elements a, b and c of a group, where ${}^x y$ denotes the element xyx^{-1}. We prove (1) by induction on i. The case $i = 1$ is analyzed in Lemma 9.26. Assume it has been proved that $E(i)$ centralizes $E(r-i+1)$, and let $a \in E(1)$, $b \in E(i)$, and $c \in E(r-i)$. Then Hall's identity and the induction hypothesis imply that

$$\big[[a,b],{}^b c\big] = 1,$$

i.e., $[a,b]$ and ${}^b c$ commute. Since ${}^b c c^{-1} = [b,c] \in E(r-i+1)$, by induction it follows that $[a,b]$ and ${}^b c c^{-1}$ also commute; hence $[a,b]$ and c commute, as well. But the commutation relations for congruence subgroups (cf. §1.4.4) imply that $[E(1), E(i)]J = E(i+1)$; consequently $E(i+1)$ commutes with $E(r-i)$, as desired. The assertions that the Λ_i^α are biadditive and Δ-invariant are evident.

Now let r be a multiple of n. If $F(1)$ is a simple Δ-module, then with appropriate identifications Λ^α is given by

$$\Lambda^\alpha(x,y) = \mathrm{Tr}_{l/F_p}(\lambda^\alpha x\sigma(y)) \tag{9.55}$$

for suitable λ^α in l (Theorem 1.11). Somewhat later we shall show that Λ^α always has the form of (9.55); but now we use (9.55) to obtain a formula for $\Lambda_i^\alpha(x,y)$. Again we use induction on i.

Let us suppose that the formula for has already been established for Λ_{i-1}^α and prove it for Λ_i^α. Take any a in $E(1)$, b in $E(i-1)$, and c in $E(r-i)$. Then, fixing a uniformizing parameter Π in D_v, we have

$$\begin{aligned}\varrho(a) &= 1 + s\Pi,\\ \varrho(b) &= 1 + t\Pi^{i-1},\\ \varrho(c) &= 1 + u\Pi^{r-i}\end{aligned}$$

for suitable s, t and u from the ring of integers $\mathcal{O}_{D_v}$. Then Lemma 1.8 implies that

$$\begin{aligned}\varrho([a,b]) &= 1 + x\Pi^i, && \text{where } \bar{x} = \bar{s}\sigma(\bar{t}) - \sigma^{i-1}(\bar{s})\bar{t},\\ \varrho([b,c]) &= 1 + y\Pi^{r-1}, && \text{where } \bar{y} = \bar{t}\sigma^{i-1}(\bar{u}) - \sigma^{r-i}(\bar{t})\bar{u},\\ \varrho([c,a]) &= 1 + z\Pi^{r-i+1}, && \text{where } \bar{z} = \bar{u}\sigma^{r-i}(\bar{s}) - \sigma(\bar{u})\bar{s},\end{aligned} \tag{9.56}$$

where bar denotes the residue of the respective element in l. Since C_1 acts trivially on $F(i)$, Hall's identity yields

$$\Lambda_i^\alpha(\bar{x},\bar{u}) = \Lambda_{r-1}^\alpha(\bar{y},\bar{s}) + \Lambda_{r-i+1}^\alpha(\bar{z},\bar{t}) = 0.$$

Furthermore, the obvious identity $[a,b]^{-1} = [b,a]^{-1}$ implies that $\Lambda_i^\alpha(x,y) = -\Lambda_{r-i}^\alpha(y,x)$ for all x in $F(i)$ and y in $F(r-i)$; hence

$$\Lambda_i^\alpha(\bar{x},\bar{u}) = \Lambda_1^\alpha(\bar{s},\bar{y}) + \Lambda_{i-1}^\alpha(\bar{t},\bar{z}). \tag{9.57}$$

Now, using induction, we obtain

$$\begin{aligned}\Lambda_i^\alpha(\bar{x},\bar{u}) &= \mathrm{Tr}_{l/F_p}(\lambda^\alpha \bar{s}\sigma(\bar{t}\sigma^{i-1}(\bar{u}) - \sigma^{r-i}(\bar{t})\bar{u}))\\ &\quad + \mathrm{Tr}_{l/F_p}((\lambda^\alpha + \cdots + \sigma^{i-r}(\lambda^\alpha))\cdot\bar{t}\sigma^{i-1}(\bar{u}\sigma^{r-i}(\bar{s}) - \sigma(\bar{u})\bar{s}))\\ &= \mathrm{Tr}_{l/F_p}((\lambda^\alpha + \sigma(\lambda^\alpha) + \cdots + \sigma^{i-1}(\lambda^\alpha))\bar{s}\sigma(\bar{t})\sigma^i(\bar{u}))\\ &\quad - \mathrm{Tr}_{l/F_p}((\lambda^\alpha + \sigma(\lambda^\alpha) + \cdots + \sigma^{i-1}(\lambda^\alpha))\sigma^{i-1}(\bar{s})\sigma^r(\bar{t})\sigma^i(\bar{u}))\\ &= \mathrm{Tr}_{l/F_p}((\lambda^\alpha + \cdots + \sigma^{i-1}(\lambda^\alpha))(\bar{s}\sigma(\bar{t}) - \sigma^{i-1}(\bar{s})\bar{t})\sigma^i(\bar{u}))\\ &= \mathrm{Tr}_{l/F_p}(\lambda_i^\alpha \bar{x}\sigma^i(\bar{u})),\end{aligned}$$

since r is a multiple of n.

Thus we see that the biadditive maps $\Lambda_i^\alpha(x,y)$ and $\mathrm{Tr}_{l/F_p}(\lambda_i^\alpha x\sigma^i(y))$ coincide for x in $F(i)$ and y in $F(r-i)$ such that $x = s\sigma(t) - \sigma^{i-1}(s)t$ for s in $F(1)$ and t in $F(i-1)$. However, as we have seen in the proof of Theorem 1.9, elements of this form generate all of $F(i)$; therefore one has

$$\Lambda_i^\alpha(x,y) = \mathrm{Tr}_{l/F_p}(\lambda_i^\alpha x\sigma^i(y)).$$

It remains to show that the map Λ^α also has the form (9.55) in the case where $F(1)$ is not a simple Δ-module. Since $n > 2$, by Proposition 1.9 we need only consider the case where l/k_v is F_{64}/F_4. As we know (Theorem 1.11), in this case one can guarantee that

$$\Lambda^\alpha(x,y) = \mathrm{Tr}_{l/F_p}(\lambda x\sigma(y) + \mu x\sigma(y)^8)$$

for suitable $\lambda, \mu \in l$; we want to show that $\mu = 0$. From (9.56) and (9.57) we obtain, for any s, t, and u in l, that

$$(9.58)\quad \Lambda_2^\alpha(s\sigma(t) - \sigma(s)t, u) = \Lambda_1^\alpha(s, t\sigma(u) - \sigma^{r-2}(t)u) + \Lambda_1^\alpha(t, u\sigma^{r-2}(s) - \sigma(u)s)$$

(note that $r \geq n = 3$). Let $t = \zeta s$, $\zeta \in k_v$. Then (9.58) yields

$$(9.59)\quad \begin{aligned} 0 &= \Lambda^\alpha(s, \zeta(s\sigma(u) - \sigma^{r-2}(s)u)) + \Lambda^\alpha(\zeta s, u\sigma^{r-2}(s) - \sigma(u)s) \\ &= \mathrm{Tr}_{l/F_p}(\mu(\zeta + \zeta^8)s\sigma(s\sigma(u) - \sigma^{r-2}(s)u)^8). \end{aligned}$$

LEMMA 9.27. *In the case at hand, l is generated as an abelian group by elements of the form $s\sigma(s\sigma(u) - \sigma^{r-2}(s)u)^8$ $(s, u \in l)$.*

PROOF: Left to the reader.

The lemma and (9.59) imply that $\mu(\zeta + \zeta^8) = 0$, and since one can choose ζ in k_v such that $\zeta + \zeta^8 \neq 0$ ($k_v = F_4 \not\subset F_8$!), it follows that $\mu = 0$. Proposition 9.11 is proved.

Now we complete the proof of Theorem 9.22. Let $\beta \in \ker \xi$, where $\xi: H^2(C) \to H^2(B)$ is the restriction map and $\beta \neq 0$. Choose r minimal > 1 for which $\beta \in H^2(C)_r$, and let α in $H^2(C/C_r)$ be an element which goes over to β under $H^2(C/C_r) \to H^2(C)$. We claim that r is a multiple of n. Indeed, if r is not a multiple of n then Theorem 1.11 implies

$$B(F(1), F(r-1)) = 0,$$

and by (9.54) $H^2(C/C_{r-1}) \to H^2(C/C_r)$ is surjective. Thus, since r is minimal, it follows that r must be a multiple of n. Then, by Theorem 1.11, the corresponding map Λ^α is given by

$$\Lambda^\alpha(x, y) = \mathrm{Tr}_{l/F_p}(\lambda^\alpha x\sigma(y)), \qquad x \in F(1),\ y \in F(r-1),$$

for some λ^α in l. We wish to show that $\omega = \mathrm{Tr}_{l/k_v}(\lambda^\alpha) = 0$. Note that by Proposition 9.11

$$(9.60)\qquad \Lambda_n^\alpha(x, y) = \mathrm{Tr}_{l/F_p}(\omega xy), \qquad x \in F(n),\ y \in F(r-n).$$

Furthermore, β becomes trivial when restricted to B. It follows that $\varrho^{-1}(BC_r/C_r)$ (where ϱ is the extension corresponding to α) is commutative. However, by Proposition 1.8,

$$C_n = (C_n \cap B)C_{n+1} \quad \text{and} \quad C_{r-n} = (C_{r-n} \cap B)C_{r-n+1}.$$

Therefore the definition of Λ_n^α implies $\Lambda_n^\alpha = 0$. Since $F(n)$ and $F(r-n)$ are canonically identified with $l^{(0)} = \{ x \in l : \mathrm{Tr}_{l/k_v}(x) = 0 \}$, we obtain finally

$$(9.61)\qquad \mathrm{Tr}_{l/F_p}(\omega xy) = 0 \qquad \text{for all } x, y \text{ in } l^{(0)}.$$

But $(l^{(0)})^\perp = \{ z \in l : \mathrm{Tr}_{l/k_v}(zl^{(0)}) = 0 \}$ is precisely k_v, so (9.61) implies $\omega l^{(0)} \subset k_v$. This is impossible if $\omega \neq 0$, since $\dim_{k_v} l^{(0)} = n - 1 > 1$. Thus

$$\omega = \mathrm{Tr}_{l/k_v}(\lambda^\alpha) = 0.$$

We conclude as follows. Construct γ in $\ker(H^2(C/C_r) \to H^2(C/C_{r+1}))$ such that $\Lambda^\alpha = \Lambda^\gamma$. Then, by (9.54),

$$\alpha - \gamma \in \mathrm{Im}(H^2(C/C_{r-1}) \to H^2(C/C_r)),$$

and therefore the image of $\alpha - \gamma$ in $H^2(C)$ by construction lies in $H^2(C)_{r-1}$. However, the image of $\alpha - \gamma$ in $H^2(C)$ is precisely the image of α; hence $\beta \in H^2(C)_{r-1}$; contradiction.

To construct γ, we write $\lambda^\alpha = \delta - \sigma\delta$ $(\delta \in l)$ (which can be done since $\mathrm{Tr}_{l/k_v}(\lambda^\alpha) = 0$), and define φ in $\mathrm{Hom}(F(r), F_p)$ by $\varphi(x) = \mathrm{Tr}_{l/F_p}(\delta x)$. Using $\mathbb{Z}/p\mathbb{Z} \simeq \frac{1}{p}\mathbb{Z}/\mathbb{Z} \subset J$, we can view φ as an element of $\mathrm{Hom}(F(r), J)$. Consider the trivial extension

$$1 \to J \to E' = (C/C_{r+1}) \times J \to C/C_{r+1} \to 1,$$

and let Φ denote the subgroup of E' consisting of elements of the form $(g, -\varphi(g))$, where $g \in C_r/C_{r+1}$. Since r is a multiple of n, it follows that C_r/C_{r+1} lies in the center of C/C_{r+1}; hence we see that Φ is a normal subgroup of E'. Let γ be the cocycle in $H^2(C/C_r)$ corresponding to the extension

$$1 \to J \to E = E'/\Phi \xrightarrow{\varepsilon} C/C_r = C/C_{r+1} \Big/ C_r/C_{r+1} \to 1.$$

By definition $\gamma \in \ker(H^2(C/C_r) \to H^2(C/C_{r+1}))$ and it remains to show that

$$\Lambda^\gamma(x, y) = \mathrm{Tr}_{l/F_p}(\lambda^\alpha x\sigma(y)) = \mathrm{Tr}_{l/F_p}((\delta - \sigma\delta)x\sigma(y))$$

for all x in $F(1)$ and y in $F(r-1)$. To do so, note that the group commutator of a in $E(1)$ and b in $E(r-1)$ can be computed as follows: take arbitrary inverse images c and d of $\varepsilon(a)$ and $\varepsilon(b)$ in C/C_{r+1} and consider the group

commutator $[c,d]$ in $C_r/C_{r+1} = F(r)$; then $[a,b] = \varphi([c,d])$. Therefore, it follows from the commutator formulas (cf. Lemma 1.8) that

$$\begin{aligned}\Lambda^\gamma(x,y) &= \varphi(x\sigma(y) - \sigma^{r-1}(x)y)\\ &= \mathrm{Tr}_{l/F_p}(\delta(x\sigma(y) - y\sigma^{r-1}(x)))\\ &= \mathrm{Tr}_{l/F_p}((\delta - \sigma\delta)x\sigma(y))\\ &= \Lambda^\alpha(x,y).\end{aligned}$$

Q.E.D.

To complete our survey of the work done so far on the congruence problem we present the results currently available on the centrality of the congruence kernel. To be begin with, the centrality of the congruence kernel can be established by manipulating the unipotent elements in G_K (if they exist). This idea goes back to the basic works of Bass-Milnor-Serre [1], Mennicke [1], [2], Matsumoto [1] and Serre [6]. The definitive result is due to Raghunathan [4], [6], who showed that for a simple simply connected K-group G the existence of unipotent elements in G_K (i.e., the fact that G is K-isotropic), together with the condition that $\mathrm{rank}_S G \geq 2$, indeed guarantees the centrality of the congruence kernel $C^S(G)$. The presence of unipotent elements in G_K is essential to his argument, and therefore the latter results cannot be extended to anisotropic groups. Until recently the only result on the centrality of $C^S(G)$ also applicable to some anisotropic groups was Kneser's theorem [14] treating spinor groups of quadratic forms. Kneser's argument, however, turns out to be general and applicable to other groups that have a convenient geometric realization. First Raghunathan and Tomanov treated groups of type C_n, and later Rapinchuk [9] proved the following general result:

THEOREM 9.23. *Let G be a simple simply connected K-group of one of the following types: B_n $(n \geq 2)$, C_n $(n \geq 2)$, D_n $(n \geq 5)$, or G_2; or let it be $\mathbf{SU}_m(L,f)$ $(m \geq 4)$ of a nondegenerate Hermitian form f over a quadratic extension L of K, having type ${}^2A_{m-1}$. If $\mathrm{rank}_S G \geq 2$, then $C^S(G)$ is central.*

The proof is based on a development of Kneser's method [14] and uses the techniques introduced in §9.3. As in §9.3, the argument here is general and can be applied to other groups having a convenient geometric realization; the argument for groups of type G_2 is given in Rapinchuk [8].

The geometric method, by which Theorem 9.23 was obtained, apparently cannot be applied to the exceptional groups since these groups do not have suitable geometric realizations. Here a solution to the congruence subgroup problem was obtained by a new approach, using the intrinsic structure of the group.

THEOREM 9.24 (RAPINCHUK [9]). *Let G be a simple simply connected K-anisotropic group of type E_7, E_8, or F_4. If $\mathrm{rank}_S G \geq 2$, then $C^S(G)$ is central.*

PROOF: Uses the fact that the groups of the types under consideration are split over a quadratic extension of K (which is why E_6 is not included in the list).

It should be noted that the projective simplicity of the group of rational points is used in the proof of practically all the results on the congruence subgroup problem, in particular in Theorems 9.23 and 9.24.

Unfortunately we do not yet know anything about the congruence subgroup problem for anisotropic inner forms of type A_n. Many years of investigation notwithstanding, no progress has been made even for the minimal case of groups of type A_1, even though the normal subgroup structure of the groups of rational points is known here (Theorem 9.2). In the special case $G = \mathbf{SL}_1(D)$, where D is a quaternion skew field over $\mathbb{Q}$, $S = \{\infty, p\}$, and the prime p is chosen such that $\mathbb{Q}_p$ splits D, the problem is due to Ihara (cf. Kourovka Notebook, 1978, problem 5.33). Note that Serre's results [7] make it possible to determine the precise algebraic structure of $G_{\mathbb{Z}(S)}$. Apparently the main results here have yet to be discovered.

Appendix A.

This supplement sets forth several results that appeared while the book was being prepared for press. Although a series of important results in the arithmetic theory of algebraic groups was discovered in the interim, a full, systematic exposition of these results would considerably exceed the scope of an appendix; yet, a proper balance between the Appendix and the main body of the book requires that we do more than simply list these results. Therefore we have decided to give a brief, conceptual exposition of two of the results, closely related to the problems handled in the book. The first of these presents finiteness theorems of a new sort, and the second is related to Platonov's conjecture on arithmeticity.

§A.1. Finiteness theorems for discrete subgroups of semisimple groups having a quotient space of bounded volume

In §4.6 we established that, for a semisimple algebraic $\mathbb{Q}$-group G, any arithmetic subgroup Γ of $G_{\mathbb{R}}$ is a lattice, i.e., is a discrete subgroup for which $G_{\mathbb{R}}/\Gamma$ has finite volume. We calculated the precise volume of $G_{\mathbb{R}}/\Gamma$ only for $G = \mathbf{SL}_2$. Until recently, such calculations existed only for split groups (Langlands [1]) and quasisplit groups (Lai [2]). Also, many natural quantitative questions about the volume of $G_{\mathbb{R}}/\Gamma$ were pending; in particular, whether this volume can be arbitrarily small. Answers to many of these deep questions are found in Borel-Prasad [1] and Prasad [4], and will be discussed in this appendix.

For G a simple group defined over $\mathbb{R}$ with $\operatorname{rank}_{\mathbb{R}} G > 1$, it has long been known[1] that there are only finitely many conjugacy classes of lattices $\Gamma \subset G_{\mathbb{R}}$ for which the volume of $G_{\mathbb{R}}/G$ with respect to a given Haar measure on $G_{\mathbb{R}}$ is bounded by some constant. Later Tits asked whether the analogous result holds for lattices Γ in the groups of points G_K of a simple algebraic group G over a non-Archimedean local field K; but in his formulation of the question only the constant bounding the volume of G_K/Γ was fixed, and it was allowed to vary K and the K-group G (under a certain "universal" definition of the Haar measure on G_K). Put in this way, the question not only acquires a new meaning for lattices in real groups, but can also be generalized to lattices in products of real and p-adic groups (in particular, to S-arithmetic subgroups, cf. §5.4). This problem is studied for S-arithmetic subgroups in Borel-Prasad [1]. Before presenting the main results, we introduce some notation.

Let G be a simple simply connected algebraic group over a number field

[1] Cf. Wang H. C. *Topics on totally discontinuous groups: Symmetric spaces*. New York: Marcel Dekker, 1972, pp.460–472.

K, and let G' be a group isogeneous to G over K. For v in V^K, let μ'_v denote the Haar measure on G'_{K_v} (cf. §3.5), which is normalized as follows. For v in V_f^K we require $\mu'_v(I_v) = 1$, where I_v is an Iwahori subgroup of G'_{K_v} (cf. §3.4). For v in V_∞^K, consider the group $H = \mathbf{R}_{K_v/\mathbb{R}}(G')$. Then $G'_{K_v} \simeq H_\mathbb{R}$, and it suffices to determine the Haar measure μ'_v on $H_\mathbb{R}$. Let H_0 be a $\mathbb{C}/\mathbb{R}$-form of H such that $H_{0\mathbb{R}}$ is compact. (Such a group always exists.) Since the Lie algebras $L(H)$ and $L(H_0)$ are isomorphic over $\mathbb{C}$, any invariant differential form of degree $n = \dim H$ on H corresponds to some form on H_0, and therefore any Haar measure on $H_\mathbb{R}$ corresponds to a Haar measure on $H_{0\mathbb{R}}$ (cf. §3.5). Then μ'_v is normalized in such a way that the volume of $H_{0\mathbb{R}}$ under the corresponding measure is 1. For any finite subset S of V^K containing V_∞^K, let μ'_S denote the Haar measure on G'_S, which is the product of the μ'_v for all v in S. With this notation, we have

THEOREM A1. *Fix a constant $c > 0$. There are only finitely many possibilities for choosing a number field K, a finite subset S of V^K containing V_∞^K, and (up to K-isomorphism) a K-group G' of absolute rank ≥ 2, such that there is an S-arithmetic subgroup Γ' of G'_S for which $\mu'_S(G'_S/\Gamma') \leq c$. Moreover, there are also only finitely many conjugacy classes of such Γ' in G'_S.*

Theorem A.1 is a finiteness theorem of a basically new type. Indeed, all the versions of finiteness theorems studied in the book assert the finiteness of certain groups ($H^1(K,G)$, $\mathrm{Sh}(G)$, $G_{A(\infty)}\backslash G_A/G_K$, etc.), associated with an individual algebraic group G. Here the theorem deals with the finiteness of a certain class of objects (S-arithmetic subgroups having a quotient space with bounded volume) in arbitrary simple groups of rank ≥ 2. In other words, it proves not only that there are finitely many conjugacy classes of such subgroups in each particular group, but also that they occur only in a finite number of groups.

The methods developed to prove Theorem A.1 also yield an interesting result on the uniform growth of the class numbers of simply connected simple algebraic groups of compact type. To formulate this result we introduce the following notation. Let S be a finite subset of V^K containing V_∞^K, and let $P_v \subset G_{K_v}$ be a parahoric subgroup for each v in $V^K \setminus S$. We say the collection $P = (P_v)_{v \in V^K \setminus S}$ is *coherent* if $P_v = G_{\mathcal{O}_v}$ for almost all v in $V^K \setminus S$. In this case $U(S,P) = G_S \times \prod_{V \in V^K \setminus S} P_v$ is an open subgroup of G_A. Now suppose that $S = V_\infty^K$, and let us write $U(P)$ instead of $U(V_\infty^K, P)$ for a coherent collection P. Then Theorem 5.1 implies that the number $c(P)$ of double cosets $U(P) \setminus G_A/G_K$ is finite.

THEOREM A2. *Fix a constant $C > 0$. There are only finitely many options for a number field K, a simple simply connected K-group G of compact type, and a conjugacy class in G_{A_f} of coherent families $P = (P_v)_{v \in V_f^K}$ of parahoric subgroups, such that $c(P) \leq C$.*

Note that for an arbitrary lattice L defining a realization of G there is a coherent collection P of parahoric subgroups such that $G^L_{A(\infty)} \subset U(P)$. Then $\mathrm{cl}(G^L) \geq c(P)$, and therefore Theorem A.2 yields

COROLLARY. *For any $C > 0$ there are a finite number of pairs (G_i, L_i) $(i = 1, \ldots, d)$, consisting of a simple simply connected algebraic group $G_i \subset \mathbf{GL}_{n_i}$ defined over a number field K_i, and of a lattice $L_i \subset K_i^{n_i}$, such that the following holds: If $G \subset \mathbf{GL}_n$ is a simple simply connected algebraic group of compact type over a number field K, and $L \subset K^n$ is a lattice for which $\mathrm{cl}(G^L) \leq C$, then, for suitable $i \in \{1, \ldots, d\}$, we have $K = K_i$, $G \simeq G_i$ over K, and $G^L_{A(\infty)}$ is isomorphic to a subgroup which is conjugate to $G^{L_i}_{i_{A(\infty)}}$ in G_{i_A}.*

In other words, there are only finitely many simple simply connected groups of compact type that have a realization with bounded class number, and each such group has only finitely many essentially distinct such realizations. Theorem A.2 also establishes the existence of a system of intrinsic constraints, which "prohibit" almost all simple simply connected groups of compact type from having realizations with small class numbers (in particular, one-class realizations, cf. Theorem 8.4). It would be interesting to discover a purely arithmetic mechanism by which this works. Moreover, one would like to have a theorem analogous to Theorem A.2, for all semisimple groups, not only for simple simply connected ones. In this regard, we note that for orthogonal groups of positive definite quadratic forms the question of one-class realization is solved by the following theorem due to Pfeuffer:[2] One-class positive definite quadratic forms in three or more variables exist only over a finite number of algebraic number fields; over each K there are only finitely many equivalence classes of such forms f for which the ideal $\mathfrak{s}(f)$ has bounded norm. ($\mathfrak{s}(f)$ is the ideal in the ring of integers $\mathcal{O}_K$ of K, generated by the values of the corresponding bilinear form on the lattice $\mathcal{O}_K^n$; in particular, the condition $\mathfrak{s}(f) = \mathcal{O}_K$ picks out the primitive forms.)

We discuss briefly some of the main points in the proofs of Theorems A.1 and A.2. One of these is the formula given by Prasad [4] for computing the volume of $\mu_S(G_S/\Gamma)$, where Γ is a principal S-arithmetic subgroup, i.e., a subgroup of the form $G_K \cap (\prod_{v \in V^K \setminus S} P_v)$, where $(P_v)_{v \in V^K \setminus S}$ is a coherent collection of parahoric subgroups. We give a general statement

[2] Pfeuffer, H. "Einklassige Geschlechter totalpositiver quadratischer Formen in totalreellen algebraischen Zahlkörpern," *J. Number Theory* 3 (1971), 371–411.

of this formula, omitting the definition of some constants allowing explicit description. Let L be the smallest extension of K over which G becomes an inner form if G has type other than ${}^6D_4$. Also, let $m_1 \leq \ldots \leq m_r$ be the exponents of the root system of G (cf. Bourbaki [4, Ch. VI,§1.11]).

THEOREM A3.

$$\mu_S(G_S/\Gamma) = D_K^{\frac{1}{2}\dim G}(D_L/D_K^{[L:K]})^{\frac{1}{2}s}\left(\prod_{i=1}^{r}\frac{m_i!}{(2\pi)^{m_i+1}}\right)^{[K:\mathbb{Q}]}\tau(G)\varepsilon,$$

where D_K (respectively D_L) is the discriminant of K (respectively L), s is a constant that depends only on the inner type of G, $\tau(G)$ is the Tamagawa number of G, and ε is a constant that depends on the collection of parahoric subgroups $(P_v)_{v\in V^K\setminus S}$.

Another fact used in the proofs is that actually $\tau(G) = 1$ (cf. p. 263), and therefore this factor may be omitted. Analyzing the formula in Theorem A.3 by means of various number-theoretic estimates, especially estimates for the discriminants of number fields, Borel and Prasad obtained the finiteness of triples (K, S, G) such that, for suitable G' isogeneous to G over K, there exists an S-arithmetic subgroup $\Gamma' \subset G'_S$ for which $\mu'_S(G'_S/\Gamma') \leq c$. The final step in the proof of Theorem A.1 establishes the finiteness, for a given group, of the number of conjugacy classes of S-arithmetic subgroups having a quotient space of bounded volume. Here one uses the finiteness theorems for Galois cohomology and estimates of the indexes of S-arithmetic subgroups in their normalizers, obtained by appropriately generalizing results due to Rohlfs [3].

Note that, with some minor restrictions, most of the results in this section also hold for groups over global fields of positive characteristic.

§A.2. Representations of groups with bounded generation

Let Γ be a finitely generated abstract group. In this section we shall analyze representations of Γ exclusively over fields of characteristic 0, and in most cases the ground field will be $\mathbb{C}$. Let $R_n(\Gamma)$ and $\mathbf{X}_n(\Gamma)$ denote the variety of n-dimensional representations of Γ and the variety of their characters, respectively. In §7.5 we discussed groups of finite representation type, i.e., groups satisfying

$$\dim \mathbf{X}_n(\Gamma) = 0 \quad \text{for all } n \geq 1. \tag{1}$$

At present, the analysis of such groups is focused on proving Platonov's conjecture on arithmeticity (cf. p. 437); but, unfortunately, little progress has been made here so far. Nevertheless, all the known examples of groups

satisfying (1) indeed come from S-arithmetic groups. Even for such groups, it is by no means easy to verify (1), and the corresponding argument relies either on a positive solution of the congruence problem or on the superrigidity results due to Margulis [6]. Neither of these methods, however, enables one to trace a connection between (1) and the structural properties of Γ. Yet it is clear that without elucidating this connection it is impossible to progress very far in analyzing groups of finite representation type. One example of a structural approach towards verifying (1) is presented in §7.5; namely, for $\Gamma = SL_n(\mathbb{Z})$ $(n \geq 3)$ one can derive (1) from the fact that Γ is boundedly generated by the set of elementary matrices (cf. Proposition 7.14). Recently Rapinchuk[3] obtained an abstract version of this result; namely, he showed that (1) can be derived from the purely combinatorial property of bounded generation of Γ.

Recall that Γ is said to be a group with bounded generation of degree $\leq t$ if there exist $\gamma_1, \ldots, \gamma_t$ in Γ such that $\Gamma = \langle\gamma_1\rangle \ldots \langle\gamma_t\rangle$, where $\langle\gamma_i\rangle$ is the cyclic subgroup generated by γ_i. Let us also introduce the following condition:

(2) $\Gamma_1^{ab} = \Gamma_1/[\Gamma_1, \Gamma_1]$ is finite, for any subgroup Γ_1 of Γ of finite index.

THEOREM A4. *Let Γ be a group of bounded generation satisfying (2). Then $\dim \mathbf{X}_n(\Gamma) = 0$ for all $n \geq 1$.*

Note that (2) is necessary for (1) to be satisfied. Let us also point out several corollaries of Theorem A.4.

COROLLARY 1. *Let $\Gamma \subset GL_n(\mathbb{C})$ be a fully reducible subgroup with bounded generation, satisfying (2). Then there exists g in $GL_n(\mathbb{C})$ such that $g\Gamma g^{-1} \subset GL_n(K)$, for a suitable algebraic number field K.*

COROLLARY 2. *Suppose $G \subset GL_n(\mathbb{C})$ is a simple algebraic $\mathbb{R}$-group. If $\operatorname{rank}_{\mathbb{R}} G \geq 2$ and $\Gamma \subset G_{\mathbb{R}}$ is a lattice which as an abstract group has bounded generation, then there exists a matrix g in $GL_n(\mathbb{R})$ such that $g\Gamma g^{-1} \subset GL_n(K)$ for a suitable algebraic number field K.*

The following result is crucial for the proof of Theorem A.4.

PROPOSITION A1. *Let Γ be an abstract group having bounded generation of degree $\leq t$. Then, for any subgroup Γ_1 of Γ of finite index, the pro-p-completion $\hat{\Gamma}_1^{(p)}$ is an analytic pro-p-group (i.e., a compact Lie group over $\mathbb{Q}_p$) of dimension $\leq t$.*

[3] Rapinchuk, A. S., "Representations of groups with bounded generation," *Dokl. Akad. Nauk SSSR* 315 (1990), 536–540.

The proof is obtained by using one of the criteria for analyticity (cf. Lazard [1, p. 206]).

As Tavgen [3] has noted, Proposition A.1 implies that a group Γ with bounded generation is linear if and only if there exists a subgroup Γ_1 of Γ of finite index which is p-residually finite for some prime p. Thus, Platonov's conjecture on arithmeticity, if true, would yield the following abstract characterization of arithmetic groups: if Γ has bounded generation, satisfies (2), and has a subgroup Γ_1 of finite index which is p-residually finite for some prime p, then Γ is a group of arithmetic type.

Proposition A.1 implies that, for a suitable subgroup $\Gamma_1 \subset \Gamma$ of finite index, the pro-p-completion $\hat{\Gamma}_1^{(p)}$ is an analytic pro-p-group of the largest possible dimension. Then the corresponding Lie algebra $\mathfrak{g}_1$ over $\mathbb{Q}_p$ is independent up to isomorphism of the choice of a subgroup Γ_1 of Γ having the properties described above. We call $\mathfrak{g}_1$ the Lie p-algebra of Γ, and call $\dim_{\mathbb{Q}_p} \mathfrak{g}_1$ the analytic p-dimension of Γ, denoted by $\dim_p \Gamma$. One may ask the following interesting question: For Γ a linear group of finite width, is it true that $\dim_p \Gamma$ is independent of p, for almost all p?

Let us sketch the proof of Theorem A.4. As in the proof of Proposition 7.14, it suffices to show that for any representation

$$\varrho: \Gamma \to GL_n(\mathbb{C})$$

the set of traces $X = \{ \operatorname{tr} \varrho(\gamma) : \gamma \in \Gamma \}$ consists entirely of algebraic numbers. It turns out that one can replace Γ by any subgroup of finite index.

LEMMA A1. *Let $\Gamma_1 \subset \Gamma$ be a subgroup of finite index, and let $X_1 = \{ \operatorname{tr} \varrho(\gamma) : \gamma \in \Gamma_1 \}$. Then the field $\mathbb{Q}(X)$ is an algebraic (even finite) extension of $\mathbb{Q}(X_1)$.*

We have $\varrho(\Gamma) \subset GL_n(A)$, for a suitable finitely generated subring A of $\mathbb{C}$. Then one uses the following result, whose proof is based on embeddings in locally compact fields (cf. Platonov [10]).

LEMMA A2. *There exists a finite subset Π of prime numbers such that, for each p in Π, there are infinitely many embeddings $\sigma_1, \sigma_2 \ldots$ (not necessarily distinct) of A in $\mathbb{Z}_p$ such that $\sigma_i(A) \cap \sigma_j(A)$ consists of algebraic numbers for $i \neq j$.*

Let us define $\varrho_i: \Gamma \to GL_n(\mathbb{Z}_p)$ as the composite of ϱ with the embedding induced by σ_i. Let $\mathfrak{g}$ be the Lie p-algebra of Γ. Then $\mathfrak{g} = \mathfrak{s} \oplus \mathfrak{r}$, where $\mathfrak{r}$ is the radical of $\mathfrak{g}$ and $\mathfrak{s}$ is semisimple. There are only a finite number (say, d) of inequivalent representations $\tau: \mathfrak{s} \to \mathfrak{gl}_n(\mathbb{Q}_p)$. Let us consider the representations $\varrho_1, \ldots, \varrho_{d+1}$. Passing to a subgroup of finite index, we may assume without loss of generality that the images of $\varrho_i(\Gamma)$ $(i = 1, \ldots, d+1)$ lie in the congruence subgroup $GL_n(\mathbb{Z}_p, p)$; hence the ϱ_i extend to analytic representations $\hat{\varrho}_i: \hat{\Gamma}^{(p)} \to GL_n(\mathbb{Z}_p)$, and, moreover, $\hat{\Gamma}^{(p)}$ is a semidirect product $S \ltimes R$, where S and R are analytic pro-p-groups with Lie algebras $\mathfrak{s}$ and $\mathfrak{r}$ respectively. Our setup implies that there are two indexes i, j in $\{1, \ldots, d+1\}$ such that $\hat{\varrho}_i$ and $\hat{\varrho}_j$ induce equivalent representations of $\mathfrak{s}$; therefore, passing to a subgroup of finite index, we may assume that $\hat{\varrho}_i \mid_S$ and $\hat{\varrho}_j \mid_S$ are equivalent. In particular, $\operatorname{tr} \hat{\varrho}_i(x) = \operatorname{tr} \hat{\varrho}_j(x)$ for all x in S. On the other hand, (2) implies that for any $\lambda: \Gamma \to GL_n(\mathbb{C})$ the radical of the connected component G^0 of the algebraic group G, obtained as the closure of $\lambda(\Gamma)$, is unipotent; therefore, again passing to a subgroup of finite index, we may assume that $\operatorname{tr} \hat{\varrho}_k(xy) = \operatorname{tr} \hat{\varrho}_k(s)$ for all x in S, y in R $(k = i, j)$. But then $\operatorname{tr} \hat{\varrho}_i(x) = \operatorname{tr} \hat{\varrho}_j(x)$ for all x in $\hat{\Gamma}^{(p)}$. In particular, $\sigma_i(\operatorname{tr} \varrho(\gamma)) = \sigma_j(\operatorname{tr} \varrho(\gamma))$ for each γ in Γ. Therefore, Lemma A.2 implies that $\operatorname{tr} \varrho(\gamma)$ is an algebraic number, as desired.

Theorem A.4 gives a qualitative description of the set of all possible representations of Γ. It turns out that for S-arithmetic subgroups with bounded generation one can give a complete description of these representations.

THEOREM A5. *Let G be a simple simply connected algebraic group over an algebraic number field K, let S be a finite subset of V^K containing V_∞^K, and let Γ be a Zariski-dense S-arithmetic subgroup of G_K. Suppose Conjecture 9.2 (cf. §9.1) holds for G over K. If Γ has bounded generation, then for any representation $\varrho: \Gamma \to GL_n(\mathbb{C})$ there exists a rational homomorphism $\varrho': \mathbf{R}_{K/\mathbb{Q}}(G) \to GL_n(\mathbb{C})$ such that ϱ and ϱ' coincide on some subgroup Γ' of Γ of finite index.*

COROLLARY 3. *Under the assumptions of Theorem A.5, Γ does not have any noncentral normal subgroups N of finite index such that Γ/N is linear. In particular, (2) holds.*

There is an interesting connection between bounded generation of S-arithmetic subgroups and the congruence subgroup problem. Namely, several years ago the second author conjectured that for an S-arithmetic subgroup of a simple simply connected group, bounded generation should imply the finiteness of the congruence kernel. This has been proved in part by Rapinchuk[4] and in full by Platonov and Rapinchuk.[5] In this regard,

[4] Cf. Rapinchuk, A. S., "The congruence subgroup problem for arithmetic groups with bounded generation," *Dokl. Akad. Nauk SSSR* 314 (1990), 1327–1331.

[5] Cf. Platonov, V. P., and Rapinchuk, A. S., "Abstract characterizations of arithmetic groups with the congruence subgroup property," *Dokl. Akad. Nauk SSSR* 319 (1991), 1322–1327.

one naturally raises the following conjecture, now an important question of the theory of arithmetic groups: suppose Γ is an S-arithmetic subgroup of a simple algebraic group G; if $\operatorname{rank}_S G = \sum_{v \in S} \operatorname{rank}_{K_v} G \geq 2$, then Γ has bounded generation (or, in a weaker version, the profinite completion $\hat{\Gamma}$ has bounded generation as a profinite group).

Appendix B. Basic Notation

K^* (resp. K^+) — the multiplicative (resp. additive) group of a field K.
V^K — the set of all inequivalent valuations of the number field K.
V_f^K (resp. V_∞^K) — the subset of non-Archimedean (resp. Archimedean) valuations of V^K.
K_v — the completion of K with respect to the valuation v in V^K.
$\mathcal{O}_v$ — the ring of v-adic integers (for v in V_f^K).
$\mathfrak{p}_v$ — the valuation ideal of $\mathcal{O}_v$.
U_v — the group of v-adic units.
$\mathcal{O}$ — the ring of integers of K.
$\mathcal{O}(S)$ — the ring of S-integers of K (for finite $S \subset V^K$ containing V_∞^K).
$w|v$ — an extension of a valuation.
A — the ring of adeles.
$A(S)$ — the ring of S-integral adeles.
$A(\infty)$ — the ring of integral adeles.
A_S — the ring of S-adeles.
A_f — the ring of finite adeles.
$A_S(T)$ — the ring of T-integral S-adeles (for $T \supset S$).
J_K — the group of ideles.
J_K^∞ — the group of integral ideles.
h_K — the class number of K.
$\operatorname{Br}(K)$ — the Brauer group of K.
$N_{L/K}$ (respectively, $\operatorname{Tr}_{L/K}$) — the norm (respectively, trace) in a finite extension L/K.
$\operatorname{Nrd}_{D/K}$ (respectively, $\operatorname{Trd}_{D/K}$) — the reduced norm (respectively, reduced trace).
F_p — the field of p elements.
$\mathbb{Z}$ (respectively, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}_p$) — the ring of integers (respectively, field of rational, real, complex, and p-adic numbers).
$\mathbb{A}^n$ (respectively, $\mathbb{P}^n$) — the n-dimensional affine (respectively, projective) space.
$\mathbb{G}_m$ — the one-dimensional K-split torus.
$\mathbb{G}_a$ — the one-dimensional connected unipotent group.
$SL_n(D)$, $SU_m(D, f)$ — classical groups over skew fields.
$\mathbf{SL}_n(D)$, $\mathbf{SU}_m(D, f)$ — their corresponding algebraic groups.
$\mathbf{R}_{L/K}$ — the restriction of scalars.
$\mathbf{X}(G)$ — the group of characters of an algebraic group G.
$\mathbf{X}_*(G)$ — the group of cocharacters (one-parameter subgroups).
$R(T, G)$ — the root system of an algebraic group G with respect to a torus T.

$W(T,G)$ — the Weil group of an algebraic group G with respect to a torus T.
$\mathfrak{g} = L(G)$ — the Lie algebra of an algebraic group G.
U_α — the one-dimensional unipotent subgroup corresponding to a root α in $R(T,G)$.
G_α — the corresponding root subgroup.
$\mathcal{T}$ — the variety of maximal tori.
$\mathcal{B}$ — the variety of Borel subgroups.
$R(\Gamma,G)$ — the variety of representations of a finitely generated group Γ in an algebraic group G.
$R_n(\Gamma)$ — the variety of n-dimensional representations.
$X_n(\Gamma)$ — the variety of n-dimensional characters.
$T_x(X)$ — the tangent space to a variety X at the point x.
$d_x f$ — the differential of a morphism f at x.
$\operatorname{rank}_K G$ — the rank of G over K (K-rank).
$\operatorname{rank}_S G = \sum_{v\in S} \operatorname{rank}_{K_v} G$ — the S-rank of G (for finite $S \subset V^K$).
G_K — the group of K-points of an algebraic K-group G.
$G_{\mathcal{O}}$ — the group of integral points.
$G_{\mathcal{O}(S)}$ — the group of S-integral points.
$G_{\mathcal{O}_v}^{L_v}$ — the group of v-adic integral points relative to a local lattice $L_v \subset K_v^n$.
G_A — the group of adeles.
$G_{A(\infty)}$ — the group of integral adeles.
$G_{A(\infty)}^L$ — the group of integral adeles relative to a lattice $L \subset K^n$.
$G_{A(S)}$ — the group of S-integral adeles.
$G_{A_S(T)}$ — the group of T-integral S-adeles.
$G_S = \prod_{v\in S} G_{K_v}$, $G_\infty = G_{V_\infty^K}$.
$\operatorname{cl}(G)$ — the class number of G.
$\operatorname{cl}(G^L)$ — the class number with respect to the realization given by $L \subset K^n$.
$\mathcal{G}\operatorname{cl}(G)$ — the class group of a semisimple algebraic group G of noncompact type.
$\operatorname{cl}(a)$ — the class of an element a.
$\operatorname{gen}(a)$ — the genus of an element a.
$f_G(a)$ — the number of classes in the genus of a.
$H^i(G,A)$ — the i-th cohomology group (in the noncommutative case, the i-th cohomology set).
$H^i(L/K,G) = H^i(\operatorname{Gal}(L/K), G_L)$ — the i-th Galois cohomology group (set) of an algebraic K-group G with respect to a Galois extension L/K.

$H^i(K,G) = H^i(\operatorname{Gal}(\bar{K}/K), G_{\bar{K}})$ (where $\bar{K}$ is the algebraic closure of K).
$\hat{H}^i(G,A)$ — the i-th Tate cohomology group.
Res — the restriction homomorphism.
Cor — the corestriction homomorphism.
$\varprojlim$ — the projective limit.
$\varinjlim$ — the inductive limit.
A^G — the set of G-invariant elements of a G-module A.
$G(a)$ — the stabilizer of an element a under the action of G.
Ga — the orbit of a.
$[X]$ — the cardinality of a set X.

Bibliography

Abels H.

[1] "Finite presentability of S-arithmetic groups," in *Proceedings of Groups—St. Andrews 1985*, London Math. Soc. Lect. Notes Series, No. 121, Cambridge University Press Cambridge, 1986, pp. 128–134.

[2] *Finite Presentability of S-Arithmetic Groups, Compact Presentability of Solvable Groups*, Lecture Notes in Math., No. 1261, Springer, Berlin-Heidelberg-New York, 1987, pp. 1–176.

Albert A. A.

[1] *Structure of Algebras*, Amer. Math. Soc. Colloq. Publ. 24, revised edition, Amer. Math. Soc., Providence, R.I., 1961.

Allan N. D.

[1] "The problem of the maximality of arithmetic groups," in *Algebraic Groups and Discontinuous Subgroups*, Proc. Symp. Pure Math., No. 9, Amer. Math. Soc., Providence, 1966, pp. 104–109.

[2] "Maximality of some arithmetic groups," *An. Acad. Brasil. Siens.* **38** 2 (1966), 223–227.

[3] "Arithmetic subgroups of some classical groups," *An. Acad. Brasil. Siens.* **39** 1 (1967), 15–18.

[4] "On the commensurability class of the Siegel modular group," *Bull. Amer. Math. Soc.* **74** 1 (1968), 115–118.

[5] "Some non-maximal arithmetic groups," *Rev. Colomb. Math.* **2** 1 (1970), 21–28.

[6] "On the maximality of $Sp(L)$ in $Sp_n(K)$," *Rev. Colomb. Math.* **4** 1 (1970), 7–15.

[7] "Maximal open compact subgroups of the projective symplectic group over a locally compact discrete valuation field," *Rev. Colomb. Math.* **5** 3 (1971), 31–58.

[8] "A note on the arithmetic of the orthogonal groups," *Rev. Colomb. Math.* **7** 2 (1973), 53–66.

[9] "A note on the arithmetic of the orthogonal groups II," *Port. Math.* **33** 3–4 (1974), 193–197.

ANT

Algebraic Number Theory, Proceedings of an instructional conference organized by the London Mathematical Society, edited by J. W. S. Cassels and A. Frohlich, Academic Press, London and New York, 1967.

Appelgate H., Oniahi H.

[1] "Similarity problem over $SL(n, \mathbb{Z}_p)$," *Proc. Amer. Math. Soc.* **87** 2 (1983), 233–238.

Arason J. Kr.

[1] "Cohomologische Invarianten quadratischer Formen," *J. Algebra* **36** (1975), 448–491.

Artin E.

[1] *Geometric Algebra*, Interscience, New York-London, 1957.

Artin E., Tate J.

[1] *Class-field Theory*, Benjamin, New York, 1968.

Artin M.

[1] "Brauer-Severi varieties," in *Brauer Groups in Ring Theory and Algebraic Geometry*, Lecture Notes in Math., No. 917, Springer, Berlin-Heidelberg-New York, 1982, pp. 194–210.

Ash A.

[1] "Cohomology of congruence subgroups of $SL(n, \mathbb{Z})$," *Math. Ann.* **249** 1 (1980), 55–73.

[2] "On the top Betti number of subgroups of $SL(n,\mathbb{Z})$," *Math. Ann.* **264** 3 (1983), 277–281.
[3] "Small-dimensional classifying spaces for arithmetic subgroups of general linear groups," *Duke Math. J.* **51** 2 (1984), 459–468.

Ash A., Grayson D., Green P.
[1] "Computations of cuspidal cohomology of congruence subgroups of $SL(3,\mathbb{Z})$," *J. Number Theory* **19** 3 (1984), 412–436.

Ash A., Stevans G.
[1] "Cohomology of arithmetic groups and congruences between systems of Hecke eigenvalues," *J. reine und angew.* **365** (1986), 192–220.

Bak A.
[1] "Le problème des sous-groupes de congruence et le problème métaplectique pour les groupes classiques de rang > 1," *C.R. Acad. Sci. Ser. 1* **292** 5 (1981), 307–310.

Bak A., Rehmann U.
[1] "The congruence subgroup problem for skew fields," *C.R. Acad. Sci.* **289** 3 (1979), p. A151.
[2] "The congruence subgroup and metaplectic problems for $SL_{n\geq 2}$ of division algebras," *J. Algebra* **78** 2 (1982), 475–547.
[3] "K_2-analogs of Hasse's norm theorem," *Comment. Math. Helv.* **59** 1 (1984), 1–11.

Bartels H.-J.
[1] "Invarianten hermitescher Formen über Schiefkörpern," *Math. Ann.* **215** 3 (1975), 269–288.
[2] "Zur Klassifikation schifhermitescher Formen über Zahlkörpern," *Math. Ann.* **219** 1 (1976), 13–19.
[3] "Definite arithmetische Gruppen," *J. reine und angew.* **301** (1978), 27–29.
[4] "Zur Galoiskohomologie definiter arithmetischer Gruppen," *J. reine und angew.* **278** (1978), 89–97.
[5] "Zur Arithmetik von Konjugationsklassen in algebraischen Gruppen," *J. Algebra* **70** 1 (1981), 179–199.
[6] "Zur Arithmetik von Diedergruppenerweiterungen," *Math. Ann.* **256** (1981), 465–473.

Bartels H.-J., Kitaoka Y.
[1] "Endliche arithmetische Untergruppen der GL_n," *J. reine und angew.* **313** (1980), 151–156.

Bass H.
[1] "The congruence subgroup problem," in *Proc. Conf. Local Fields. Driebergen, 1966*, Springer, Berlin-Heidelberg-New York, 1967, pp. 16–22.
[2] *Algebraic K-Theory*, W. A. Benjamin, New York-Amsterdam, 1968.

Bass H., Lazard M., Serre J.-P.
[1] "Sous groupes d'indice fini dans $SL(n,\mathbb{Z})$," *Bull. Amer. Math. Soc.* **70** (1964), 385–392.

Bass H., Milnor J., Serre J.-P.
[1] "Solution of the congruence subgroup problem for SL_n ($n \geq 3$) and Sp_{2n} ($n \geq 2$)," *Publ. Math. I.H.E.S.* **33** (1967), 59–137.

Bayer-Fluckiger E.
[1] "Intersections de groupes orthogonaux et principe de Hasse faible pour les systèmes de formes quadratiques sur un corps global," *C.R. Acad. Sci. Ser. 1* **301** 20 (1985), 911–914.
[2] "Principe de Hasse faible pour les systèmes de formes quadratiques," *J. reine und angew.* **378** (1987), 53–59.

Behr H.
[1] "Über die endliche Definierbarkeit von Gruppen," *J. reine und angew.* **211** (1962), 116–122.
[2] "Über die endliche Definierbarkeit verallgemeinerter Einheitengruppen II," *Invent. Math.* **4** 4 (1967), 265–274.
[3] "Zur starken Approximation in algebraischen Gruppen über globalen Korpern," *J. reine und angew.* **229** (1968), 107–116.
[4] "Endliche Erzeugbarkeit arithmetischer Gruppen uber Funktionenkörpern," *Invent. Math.* **7** 1 (1969), 1–32.
[5] "Explizite Präsentation von Chevalleygruppen über $\mathbb{Z}$," *Math. Z.* **141** (1975), 235–241.
[6] "$SL_3(F_q[t])$ is not finitely presentable," in *Homological Group Theory*, London Math. Soc. Lect. Notes Series, No. 36, Cambridge University Press Cambridge, 1979, pp. 213–224.
[7] "Finite presentability of arithmetic groups over global function fields," *Proc. Edinburgh Math. Soc.* **30** 1 (1987), 23–39.

Bertrand D.
[1] "Endomorphismes de groupes algébriques: applicationes arithmétiques," in *Approxim. diophant. et nombres transcendents*, Colloq. Luminy 13–19 Juin, 1982, Boston, 1983, pp. 1–45.

Beyl F.
[1] "The Schur multiplicator of $SL(2,\mathbb{Z}/m\mathbb{Z})$ and the congruence subgroup property," *Math. Z.* **191** 1 (1986), 23–42.

Beyl F. R., Tappe J.
[1] *Group Extensions, Representations and the Schur Multiplicator*, Lecture Notes in Math., No. 958, Springer, Berlin-Heidelberg-New York, 1982.

Böge S.
[1] "Eine Bemerkung zur Reduktiontheorie in orthogonalen Gruppen," *Math. Ann.* **193** 1 (1971), 38–48.

Bondarenko A. A.
[1] "On the problem of maximality of arithmetic sugbroups of orthogonal groups of type B_n," *Mat. Zametki* **16** 1 (1974), 151–161.
[2] "Towards a classification of maximal arithmetic subgroups of orthogonal groups of type (D_l)," *Dokl. Akad. Nauk BSSR* **18** 9 (1974), 773–776.
[3] "Classification of maximal arithmetic subgroups of orthogonal groups of type (D_l)," *Dokl. Akad. Nauk BSSR* **19** 11 (1975), 969–972.
[4] "Classification of maximal arithmetic subgroups of decomposable groups," *Mat. Sb.* **102** 2 (1977), 155–172.
[5] "Classification of maximal arithmetic subgroups of indeterminate orthogonal groups of type (B_l)," *Mat. Sb.* **127** 1 (1985), 72–91.

Bondarenko A. A., Rapinchuk A. S.
[1] "On estimating the number of dual cosets of adele groups of algebraic groups," *Dokl. Akad. Nauk BSSR* **22** 5 (1978), 397–400.

Borel A.
[1] "Some finiteness properties of adele groups over number fields," *Publ. Math. I.H.E.S.* **16** (1963), 101–126.
[2] "Arithmetic properties of linear algebraic groups," in *Proceedings of the International Congress of Mathematicians (Stockholm)*, 1962, pp. 10–22.
[3] "Some properties of adele groups attached to algebraic groups," *Bull. Amer. Math. Soc.* **67** (1961), 583–585.

[4] "Ensembles fondamentaux pour les groupes arithmétiques," in *Colloque sur la theorie des groupes algébriques, Bruxelles*, Louvain-Paris, 1962.
[5] "Density and maximality of arithmetic subgroups," *J. reine und angew.* **224** (1966), 78–89.
[6] *Ensembles fondamentaux pour les groupes arithmetiques et formes automorphes*, Faculte des sciences de Paris, mimeographed lecture notes, 1967.
[7] *Introduction aux groupes arithmétiques*, Hermann, Paris, 1969.
[8] *Linear Algebraic Groups*, Benjamin, New York-Amsterdam, 1969.
[9] "Cohomologie réelle stable des groupes S-arithmétiques classiques," *C.R. Acad. Sci.* **274** (1972), A1700–A1702.
[10] "Stable real cohomology of arithmetic groups," *Ann. Sci. Ecole Norm. Sup.* **7** (1974), 235–272.
[11] "Cohomology of arithmetic groups," in *Proceedings of the International Congress of Mathematicians (Vancouver, 1974)*, Canadian Mathematical Congress, Vancouver, 1975, Vol. **1**, pp. 435–442.
[12] "Admissible representations of a semi-simple group over a local field with vectors, fixed under Iwahori subgroup," *Invent. Math.* **35** (1976), 233–259.
[13] "Cohomologie de sous-groupes discrets et représentations des groupes semisimples," *Asterisque* **32–33** (1976), 73–112.
[14] "Stable and L^2-cohomology of arithmetic groups," *Bull. Amer. Math. Soc.* **3** 3 (1980), 1025–1027.
[15] "On free subgroups of semi-simple groups," *Enseign. Math.* **29** 1–2 (1983), 151–164.
[16] *Oeuvres–Collected papers, Vol. 1, 1948–1958*, Springer, Berlin, 1983.
[17] *Oeuvres–Collected papers, Vol. 2, 1959–1968*, Springer, Berlin, 1983.
[18] *Oeuvres–Collected papers, Vol. 3, 1969–1982*, Springer, Berlin, 1983.

Borel A., Casselman W.
[1] "Cohomologie d'intersection et L^2-cohomologie de variétés arithmétiques de rang rationnel 2," *C.R. Acad. Sci. Ser. 1* **301** 7 (1985), 369–373.

Borel A., Harder G.
[1] "Existence of discrete compact subgroups of reductive groups over local fields," *J. reine und angew.* **298** (1978), 53–64.

Borel A., Harish-Chandra
[1] "Arithmetic subgroups of algebraic groups," *Bull. Amer. Math. Soc.* **67** 6 (1961), 579–583.
[2] "Arithmetic subgroups of algebraic groups," *Math. Ann.* **75** (1962), 485–535.

Borel A., Mostow G. D., eds.
[1] *Algebraic Groups and Discontinuous Subgroups*, Proc. Symp. Pure Math., No. 9, Amer. Math. Soc., Providence, 1966.

Borel A., Prasad G.
[1] "Finiteness theorems for discrete subgroups of bounded covolume in semi-simple groups," *Publ. Math. I.H.E.S.* **69** (1989), 119–171.

Borel A., Serre J.-P.
[1] "Théorèmes de finitude en cohomologie galoisienne," *Comment. Math. Helv.* **39** 2 (1964), 111–164.
[2] "Adjonction de coins aux espaces symétriques; applications à la cohomologie des groupes arithmétiques," *C.R. Acad. Sci.* **271** 23 (1970), p. A1156.
[3] "Cohomologie à supports compacts des immeubles de Bruhat-Tits; applications à la cohomologie des groupes S-arithmétiques," *C.R. Acad. Sci.* **272** 2 (1971), A110–A113.
[4] "Corners and arithmetic groups," *Comment. Math. Helv.* **48** (1973), 436–491.

[5] "Cohomologie d'immeubles et de groupes S-arithmétiques," *Topology* **15** 3 (1976), 211–232.

Borel A., Springer T. A.
[1] "Rationality properties of linear algebraic groups," *Tohoku Math. J.* **20** (1968), 443–497.

Borel A., Tits J.
[1] "Groupes reductifs," *Publ. Math. I.H.E.S.* **27** (1965), 55–150.
[2] "Complements à l'article 'Groupes reductifs'," *Publ. Math. I.H.E.S.* **41** (1972), 253–276.
[3] "Éléments unipotents et sous-groupes paraboliques de groupes reductifs, I," *Invent. Math.* **12** 2 (1971), 95–104.

Borel A., Wallach N.
[1] *Continuous cohomology, discrete subgroups and representations of reductive groups*, Annals of Mathematics Studies, No. 94, Princeton Univ. Press, Princeton, 1980.

Borevich Z. I., Shafarevich I. P.
[1] *Number Theory*, Moscow, 1985.

Borovoi M. V.
[1] "Abstract simplicity of several simple anisotropic algebraic groups over number fields," *Dokl. Akad. Nauk SSSR* **283** 4 (1985), 794–797.
[2] "Galois cohomology of real reductive groups and real forms of simple Lie algebras," *Funct. Anal. i evo Prilozhenia* **22** 2 (1988), 63–64.
[3] "Abstract simplicity of groups of type D_n over number fields," *Uspekhi Mat. Nauk.* **43** 5 (1988), 179–180.
[4] "Weak approximation and homogeneous spaces," *Dokl. Akad. Nauk SSSR* **314** 1 (1990), 21–24.

Bourbaki N.
[1] *Algèbre Commutative*, Hermann, Paris, 1964–1969.
[2] *Groupes el algèbres de Lie, Chap. 4–6*, Hermann, Paris, 1968.
[3] *Groupes el algèbres de Lie, Chap. 1*, 2nd ed., Hermann, Paris, 1972.
[4] *Groupes et algèbres de Lie, Chap. 2–3.*, Hermann, Paris, 1972.
[5] *Groupes et algèbres de Lie, Chap. 7–8*, Hermann, Paris, 1975.
[6] *Elements de mathematique*, Vol. 6. (Integration), Hermann, Paris.
[7] *Algèbre*, Vol. 2, Hermann, Paris.
[8] *Topologie generale*, Vol. 3, Hermann, Paris.

Britto J.
[1] "On defining a subgroup of the special linear group by a congruence," *J. Indian Math. Soc.* **40** 1–4 (1976), 235–243.
[2] "On the construction of non-congruence subgroups," *Acta Arith.* **33** 3 (1977), 261–267.

Brown K. S.
[1] *Cohomology of Groups*, Springer, 1982.

Bruhat F.
[1] "Sur les représentations des groupes classiques p-adiques I," *Amer. J. Math.* **83** 2 (1961), 321–338.
[2] "Sur les représentations des groupes classiques p-adiques II," *Amer. J. Math.* **83** 2 (1961), 343–368.
[3] "Sur une classe de sous-groupes compacts maximaux de groupes de Chevalley sur un corps p-adique," *Publ. Math. I.H.E.S.* **23** (1964), 621–650.
[4] "Groupes algébriques semisimples sur un corps local," in *Actes Congr. Intern. Math. (Paris, 1970)*, Gauthier-Villars, Paris, 1971, Vol. **2**, pp. 285–290.

Bruhat F., Tits J.
[1] "Groupes algébriques simples sur un corps local," in *Proc. Conf. Local Fields, Driebergen, 1966*, Springer Verlag, Berlin-Heidelberg-New York, 1967, pp. 23–26.
[2] "BN-paires de type affine et données radicielles," *C.R. Acad. Sci.* **263** 18A (1966), 598–601; "Groupes simple residuellement deployés sur un corps local," *C.R. Acad. Sci.* **263** 21A (1966), 766–768; "Groupes algébriques simples sur un corps local," *C.R. Acad. Sci.* **263** 23A (1966), 822–825; "Groupes algébriques simples sur un corps local: cohomologie galoisienne, decompositions d'Iwasawa et de Cartan," *C.R. Acad. Sci.* **263** 23A (1966), 867–869.
[3] "Groupes reductifs sur un corps local," *Publ. Math. I.H.E.S.* **41** (1972), 5–252.
[4] "Groupes reductifs sur un corps local, Ch. II. Schemas en groupes. Existence d'une donnée radicielle valuée," *Publ. Math. I.H.E.S.* **60** (1984).
[5] "Schemas en groupes et immeubles des groupes classiques sur un corps local," *Bull. Soc. Math. Fr.* **112** 2 (1984), 259–301.
[6] "Groupes algébriques sur un corps local, Ch. III. Complements et applications à la cohomologie galoisienne," *J. Fac. Sci. Univ. Tokyo Sec 1A* **34** 3 (1987), 671–688.
Bürgisser B.
[1] "On the projective class group of arithmetic groups," *Math. Z.* **184** 3 (1983), 339–357.
Cartan E.
[1] "Sur certaines formes riemanniennes remarquables des géométries de groupe fondamental simple," *Ann. Sci. Ecole Norm. Sup.* **44** (1927), 345–467.
Cartan H., Eilenberg S.
[1] *Homological Algebra*, Princeton Math Series, No. 19, Princeton University Press, Princeton, 1956.
Carter D., Keller G.
[1] "Bounded elementary generation of $SL_n(O)$," *Amer. J. Math.* **105** 3 (1983), 673–687.
Cassels J. W. S.
[1] *Rational Quadratic Forms*, London Math. Soc. Monographs, No. 13, Academic Press, London, 1978.
Chahal J. S.
[1] "Solution of the congruence subgroup problem for solvable algebraic groups," *Nagoya Math. J.* **79** (1980), 141–144.
[2] "Arithmetic subgroups of algebraic groups," *Indiana Univ. Math. J.* **33** 6 (1984), 799–804.
Chernousov V. I.
[1] "On the rationality of spinor varieties over the field of rational numbers," *Dokl. Akad. Nauk BSSR* **25** 4 (1981), 293–296.
[2] "On the rationality of compact group varieties of classical type," *Dokl. Akad. Nauk BSSR* **27** 12 (1983), 1061–1064.
[3] "On projective simplicity of algebraic groups which split over a quadratic extension of a number field," *Dokl. Akad. Nauk SSSR* **296** 6 (1987), 1301–1305.
[4] "On the structure of groups of rational points of algebraic groups of type D_l," *Dokl. Akad. Nauk BSSR* **31** 7 (1987), 593–596.
[5] "On the projective simplicity of several groups of rational points over algebraic number fields," *Izv. Akad. Nauk SSSR, Ser. Mat.* **53** 2 (1989), 398–410.
[6] "On the Hasse principle for groups of type E_8," *Dokl. Akad. Nauk SSSR* **306** 25 (1989), 1059–1063.

Chevalley C.
[1] *Theory of Lie Groups*, Vol. 1, Princeton University Press, Princeton, 1946; Vols. 2 and 3, Hermann, Paris, 1951 and 1955.
[2] "Deux théorèmes d'arithmétiques," *J. Math. Soc. Japan* **3** 1 (1951), 36–44.
[3] "On algebraic group varieties," *J. Math. Soc. Japan* **6** 3–4 (1954), 303–324.
[4] "Sur certain groupes simples," *Tohôku Math. J.* **7** (1955), 14–66.
Coray D. F.
[1] "The Hasse principle for pairs of quadratic forms," in *Journées Arithmétiques*, London Math. Soc. Lect. Notes Series, No. 56, Cambridge University Press, Cambridge, 1982, pp. 237–246.
Cox D., Parry W.
[1] "Genera of congruence subgroups in Q-quaternion algebras," *J. reine und angew.* **351** (1984), 66–112.
Coxeter H. S. M., Moser W. O. J.
[1] *Generators and relations for discrete groups*, Springer, 1972.
Cram G.-M.
[1] "Locally isomorphic algebras and a Hasse principle for split metacyclic groups," *Arch. Math.* **47** 4 (1986), 330–338.
Curtis C. W., Reiner I.
[1] *Representation Theory of Finite Groups and Associative Algebras*, John Wiley and Sons, 1962.
Danset R.
[1] "Methode du cercle adelique et principe de Hasse fin pour certain systèmes de formes," *Enseign. Math.* **31** 1–2 (1985), 1–66.
Deligne P.
[1] "Extensions centrales non-residuellement finies de groupes arithmétiques," *C.R. Acad. Sci.* **287** (1978), 203–208.
Delone B. H., Galiulin P. V., Stogrin H. I.
[1] "On types of Bravais lattices," *Itogi Nauki i Tekhniki [Progress in Science and Technology], Contemporary problems in Mathematics: Basic Directions* **2** (1973), 119–254.
Demazure M.
[1] "Sous-groupes arithmétiques des groupes algébriques linéaires," in *Séminaire Bourbaki (1961–1962)*, Paris, 1962, Vol. **3**, pp. 235/1–235/12.
Deodhar V. V.
[1] "On central extensions of rational points of algebraic groups," *Amer. J. Math.* **100** 2 (1978), 303–386.
[2] "On central extensions of rational points of algebraic groups," *Contemporary Math.* **9** (1982), 319–322.
Deuring M.
[1] *Algebren*, Springer, Berlin, 1935.
Dieudonné J.
[1] "On the structure of unitary groups," *Trans. Amer. Math. Soc.* **72** (1952), 367–385.
[2] *La géométrie des groupes classiques*, Springer, 1971.
Doyle C., James D.
[1] "Discreteness criteria and high order generators for subgroups of $SL(2,\mathbb{R})$," *Illinois J. Math.* **15** 2 (1981), 191–200.
Drakokhrust Yu. A.
[1] "On a total obstruction to the Hasse principle," *Dokl. Akad. Nauk BSSR* **30** 1 (1986), 5–8.

Drakokhrust Yu. A., Platonov V. P.
[1] "The Hasse norm principle for algebraic number fields," *Izv. Akad. Nauk SSSR, Ser. Mat.* **50** 5 (1986), 946–968.
Draxl P., Kneser M.
[1] *SK_1 von Schiefkörpern*, Lecture Notes in Math., No. 778, Springer, Berlin-Heidelberg-New York, 1980.
Dwyer W.G.
[1] "Homology of integral upper-triangular matrices," *Proc. Amer. Math. Soc.* **94** 3 (1985), 523–528.
Earnest A. G.
[1] "Partitionings of a genus of quadratic forms," *J. Number Theory* **14** 1 (1982), 1–8.
Earnest A. G., Hsia J. G.
[1] "Springer-type theorems for spinor genera of quadratic forms," *Bull. Amer. Math. Soc.* **81** 5 (1975), 942–943.
[2] "Spinor genera under field extensions," *Acta Arith.* **32** 2 (1977), 115–128.
Eichler M.
[1] "Allgemeine Kongruenzklassenteilungen der Ideal einfacher Algebren über algebraischen Zahlkörpern und ihre L-Reihen," *J. reine und angew.* **179** (1938), 227–251.
[2] *Quadratische Formen und orthogonale Gruppen*, Springer, Berlin, 1952.
[3] "Zur Zahlentheorie der quaternionen Algebren," *J. reine und angew.* **195** 3–4 (1955), 127–151.
Eiichi A.
[1] "Generation of some discrete subgroups of simple algebraic groups," *Tohoku Math. J.* **17** 2 (1965), 178–184.
Elstrodt J., Grunewald F., Mennicke J.
[1] "$PSL(2)$ over imaginary quadratic integers," *Asterisque* **94** (1982), 43–60.
[2] "On the group $PSL(2, \mathbb{Z}[i])$," in *Journées Arithmétiques*, London Math. Soc. Lect. Notes Series, No. 56, Cambridge University Press, Cambridge, 1982, pp. 255–283.
Flöge D.
[1] "Zur Struktur der PSL_2 über einigen imaginär-quadrischen Zahlringen," *Math. Z.* **183** 2 (1983), 255–279.
Fuliwara M.
[1] "On the strong approximation theorem for the group F_4 and E_6," *Sci. Pap. Coll. Gen. Educ. Univ. Tokyo* **21** 2 (1971), 123–126.
Garland H.
[1] "The spectrum of non-compact G/T and the cohomology of arithmetic groups," *Bull. Amer. Math. Soc.* **75** 4 (1969), 807–811.
[2] "A finiteness theorem for K_2 of a number field," *Ann. Math.* **94** (1971), 534–548.
[3] "On the cohomology of discrete subgroups of p-adic groups," in *Proceedings of the International Congress of Mathematicians (Vancouver, 1974)*, Canadian Mathematical Congress, Vancouver, 1975, Vol. **1**, pp. 449–453.
Garland H., Raghunathan M. S.
[1] "Fundamental domains for lattices in (R)-rank 1 semisimple Lie groups," *Ann. Math.* **92** 2 (1970), 279–326.
Garland H., Hsiang W. C.
[1] "A square integrability criterion for the cohomology of arithmetic groups," in *Proc. Nat. Acad. Sci., USA*, 1968, Vol. **59**, pp. 354–360.
Gauss C. F.
[1] *Disquisitiones arithmeticae*, Werke, 1801, Vol. **1**.

Gentile E. R.
[1] "Metodos locales-globales (aspectos historicos)," *Trab. Mat. Inst. Argent. Math.* **96** (1986), 1–29.
Gerstein L. J.
[1] "On the proper spinor genus of a quadratic form," *Lin. and Mult. Algebra* **11** 2 (1982), 203–208.
Giraud T.
[1] *Cohomology non-abelienne*, Springer, Berlin-Heidelberg-New York, 1971.
Godement R.
[1] "Domaines fondamentaux des groupes arithmétiques," in *Seminaire Bourbaki (1962–1963)*, Paris, 1964, Vol. **15**, pp. 257/01–257/25.
[2] "Formes automorphes et produite eulériens (d'apres R. P. Langlands)," in *Séminaire Bourbaki, Vol. 1968/69*, Lecture Notes in Math., No. 179, Springer, Berlin-Heidelberg-New York, 1971, pp. 37–53.
Goto M., Grosshans F. D.
[1] *Semisimple Lie Algebras*, Lecture Notes in Pure and Applied Mathematics, No. 38, Marcel Dekker, 1978.
Gromov M.
[1] "Hyperbolic groups," in *Essays in Group Theory*, New York, 1987, pp. 75–263.
Gromov M., Piatetski-Shapiro I.
[1] "Non-arithmetic groups in Lobachevsky spaces," *Publ. Math. I.H.E.S.* **66** (1988), 93–103.
Grothendieck A.
[1] "Représentations linéaires et compactification profinie des groupes discrets," *Manusc. Math.* **2** (1970), 375–396.
Grunewald F. J., O'Hallorau J.
[1] "Niplotent groups and unipotent algebraic groups," *J. Pure Appl. Algebra* **37** 3 (1985), 299–313.
Grunewald F. J., Segal D.
[1] "A note on arithmetic groups," *Bull. London Math. Soc.* **10** (1978), 297–302.
[2] "The solubility of certain decision problems in arithmetic and algebra," *Bull. Amer. Math. Soc.* **1** 6 (1979), 915–918.
[3] "Some general algorithms I: Nilpotent groups," *Ann. Math.* **112** 3 (1980), 531–583.
[4] "Some general algorithms II: Nilpotent groups," *Ann. Math.* **112** 3 (1980), 585–617.
[5] "Decision problems concerning S-arithmetic groups," *J. Symbolic Logic* **50** 3 (1985), 743–772.
Grunewald F. J., Schwermer J.
[1] "Free non-abelian quotients of SL_2 over orders of imaginary quadratic number fields," *J. Algebra* **69** 2 (1981), 298–304.
Gurak S.
[1] "On the rational equivalence of full decomposable forms," *J. Number Theory* **14** 2 (1982), 251–259.
[2] "On the Hasse norm principle," *J. reine und angew.* **299/300** (1978), 16–27.
Harder G.
[1] "Über die Galoiskohomologie halbeinfacher Matrizengruppen I," *Math. Z.* **90** 5 (1965), 404–428.
[2] "Über die Galoiskohomologie halbeinfacher Matrizengruppen II," *Math. Z.* **92** 5 (1966), 396–415.
[3] "Halbeinfacher Gruppenschemata über Dedekindringen," *Invent. Math.* **4** (1967), 165–191.

[4] "Bericht über neure Resultate der Galoiskohomologie halbeinfacher Gruppen," *Jahresber. Deutsch. Math. Verein.* **70** 4 (1968), 182–216.
[5] "Minkowskische Reduktiontheorie über Funktionkörpern," *Invent. Math.* **7** 1 (1969), 33–54.
[6] "Semi-simple group schemes over curves and automorphic functions," in *Actes Congr. Intern. Math. (Paris, 1970)*, Gauthier-Villars, Paris, 1971, Vol. **2**, pp. 307–312.
[7] "A Gauss-Bonnet formula for discrete arithmetically defined groups," *Ann. Sci. Ecole Norm. Sup.* **4** (1971), 409–455.
[8] "Chevalley groups over function fields and automorphic forms," *Ann. Math.* **100** 2 (1974), 249–306.
[9] "A Gauss-Bonnet formula for discrete arithmetically defined groups," *Ann. Sci. Ecole Norm. Sup.* **4** (1971), 409–455.
[10] "On the cohomology of discret arithmetically defined groups," in *Discrete subgroups Lie Groups and Appl Moduli*, Pap. Bombay Coll. 1973, Oxford, 1975, pp. 129–160.
[11] "Über die Galoiskohomologie halbeinfacher algebraischer Gruppen," *J. reine und angew.* **274–275** (1975), 125–138.
[12] "Die Kohomologie S-arithmetischer Gruppen über Funtionenkörpern," *Invent. Math.* **42** (1977), 135–175.

Harish-Chandra, Dijk D.
[1] *Harmonic Analysis on Reductive p-adic Groups*, Lecture Notes in Math., No. 162, Springer, Berlin-Heidelberg-New York, 1970.

Hartshorne R.
[1] *Algebraic Geometry*, Springer, 1977.

Hashimoto K.
[1] "A formula for the number of semi-simple conjugacy classes in the arithmetic subgroups," *Proc. Jap. Acad.* **A61** 2 (1985), 48–50.
[2] "On certain elliptic conjugacy classes of the Siegel modular group," *Proc. Jap. Acad.* **A61** 3 (1985), 74–77.
[3] "Elliptic conjugacy classes of the Siegel modular group and unimodular hermitian forms over the ring of cyclotomic integers," *J. Fac. Sci. Univ. Tokyo Sec. IA* **33** 1 (1986), 57–82.

Hasse H.
[1] "Über p-adische Schiefkörper und ihre Bedeutung für die Arithmetik hypercomplexer Zahlsystem," *Math. Ann.* **104** (1931), 495–534.
[2] "Neue Begründung und Verallgemeinerung der Theorie des Normenrestsymbols," *J. reine und angew.* **162** (1930), 134–144.

Helgason S.
[1] *Differential Geometry and Symmetric Spaces*, Academic Press, 1962.

Helm P.
[1] "A note on non-congruence subgroups," *Comm. in Algebra* **12** 5–6 (1984), 691–701.

Hermite C.
[1] *Oeuvres Completes*, Gauthier-Villars, Paris, 1905, Vol. **1**.

Herstein I. N.
[1] *Noncommutative Rings*, Mathematical Association of America, 1968.

Hijikata H.
[1] "Hasse's principle on quaternionic anti-hermitian forms," *J. Math. Soc. Japan* **75** 2 (1963), 165–175.

[2] "On the structure of semisimple algebraic groups over valuation fields I," *Jap. J. Math, new series* **1** 2 (1975), 225–300.

Hochschild G.
[1] *Basic Theory of Algebraic Groups and Lie Algebras*, Springer, New York, 1981.

Humphreys J. E.
[1] *Linear algebraic groups*, Springer, 1975.
[2] *Arithmetic Groups*, Springer, 1980.

Huppert B.
[1] *Endliche Gruppen I*, Springer, Berlin, 1967.

Hürlimann W.
[1] "On algebraic tori of norm type," *Comment. Math. Helv.* **59** 4 (1984), 539–549.

Hurrelbriuk J.
[1] "On presentations of $SL_n(\mathbb{Z}_n)$. $\mathbb{Z}_s = \mathbb{Z}\left[\frac{1}{p_1}, \ldots, \frac{1}{p_s}\right]$.," *Comm. in Algebra* **11** 9 (1983), 937–947.

Igusa J.-I.
[1] "Some observations on metaplectic groups," *Amer. J. Math.* **103** 6 (1981), 1343–1365.

Ihara Y.
[1] "Discrete subgroups of $PL(2, k_{\mathfrak{p}})$," in *Algebraic Groups and Discontinuous Subgroups*, Proc. Symp. Pure Math., No. 9, Amer. Math. Soc., Providence, 1966, pp. 272–278.
[2] "Congruence relations and fundamental groups," *J. Algebra* **75** 2 (1982), 445–451.

Iwahori N., Matsumoto H.
[1] "On some Bruhat decompositions and the structure of the Hecke rings of p-adic Chevalley groups," *Publ. Math. I.H.E.S.* **25** (1965), 5–48.

Iwasawa K.
[1] *Local Class Field Theory*, Oxford University Press, New York, 1986.

Iyanaga K.
[1] "Arithmetic of special unitary groups and their simplectic representations," *J. Fac. Sci. Univ. Tokyo* **15** 1 (1968), 35–36.
[2] "On certain double coset spaces of algebraic groups," *J. Math. Soc. Japan* **23** (1971), 103–122.

Jacobson N.
[1] "Cayley numbers and simple Lie algebras of type G," *Duke Math. J.* **5** (1939), 775–783.
[2] "Composition algebras and their automorphisms," *Rend Circolo Math. Palermo* **7** 1 (1958), 55–80.

James D.
[1] "On the normal subgroups of integral orthogonal groups," *Pacific J. Math.* **52** 1 (1974), 107–114.
[2] "Orthogonal groups of three-dimensional anisotropic quadratic forms," *J. Algebra* **37** 1 (1975), 121–136.

Jehne W.
[1] "Der Hassesche Normensatz und seine Entwicklung," *Mitt. math. Ges. Hamburg* **11** 1 (1982), 143–153.

Jhuk I. K.
[1] "On the rationality of several homogeneous spaces of $SO(q)$," *Dokl. Akad. Nauk BSSR* **26** 9 (1982), 773–775.

Johnson F. E. A.
[1] "On the existence of irreducible lattices," *Arch. Math.* **43** 5 391–396 (1984).

Johnson R. P.
[1] "Orthogonal groups of local anisotropic spaces," *Amer. J. Math.* **91** 4 (1969), 1077–1105.
Kaneda M.
[1] "Generators and relations for special linear algebras and groups," *J. Algebra* **94** 1 (1985), 1–18.
Kariyama K.
[1] "On the conjugacy classes of the anisotropic maximal tori of a Chevalley group over a local field," *J. Algebra* **99** 1 (1986), 2–49.
Katayama S.
[1] "Class number relations of algebraic tori I," *Proc. Jap. Acad.* **A62** 6 (1986), 216–218.
[2] "Class number relations of algebraic tori II," *Proc. Jap. Acad.* **A62** 8 (1986), 321–322.
Kazhdan D. A.
[1] "On the relationship between the dual space of a group and the structure of its closed subgroups," *Funct. Anal. i evo Prilozhenia* **1** 1 (1967), 71–79.
Kitaoka Y.
[1] "Scalar extension of quadratic lattices," *Nagoya Math. J.* **66** (1977), 139–149.
[2] "Scalar extension of quadratic lattices II," *Nagoya Math. J.* **67** (1977), 159–164.
Klein F.
[1] "Zur Theorie der elliptischen Modulfunktionen," *Math. Ann.* **17** (1880), 72–76.
Klose J.
[1] "Metaplektische Erweiterungen von Quaternionen-schiefkörpern," *Math. Z.* **193** 4 (1986), 625–649.
Kneser M.
[1] "Klassenzahlen indefiniter quadratischer Formen in drei oder mehr Veränderlichen," *Arch. Math.* **7** 5 (1956), 323–332.
[2] "Orthogonale Gruppen über algebraischen Zahlkörpern," *J. reine und angew.* **196** 3–4, 213–220.
[3] "Klassenzahlen definiter quadratischer Formen," *Arch. Math.* **8** 4 (1957), 241–250.
[4] "Einfach zusammenhängende algebraische Gruppen in der Arithmetik," in *Proc. Intern. Congr. Math. Djursholm*, Uppsala, 1962, pp. 260–263.
[5] "Schwache approximation in algebraische Gruppen," in *Colloque sur la theorie des groupes algébriques, Bruxelles*, Louvain-Paris, 1962, pp. 41–52.
[6] "Approximationssätze für algebraische Gruppen," *J. reine und angew.* **209** 1 (1962), 96–97.
[7] "Erzeugende und Relationen verallgemeinerter Einheitengruppen," *J. reine und angew.* **214–215** (1964), 345–349.
[8] "Galois-Kohomologie halbenfacher algebraischer Gruppen über p-adischen Körpern I," *Math. Z.* **88** 1 (1965), 40–47.
[9] "Galois-Kohomologie halbenfacher algebraischer Gruppen über p-adischen Körpern II," *Math. Z.* **89** (1965), 250–272.
[10] "Starke approximation in algebraischer Gruppen I," *J. reine und angew.* **218** (1965), 190–203.
[11] "Strong approximation," in *Algebraic Groups and Discontinuous Subgroups*, Proc. Symp. Pure Math., No. 9, Amer. Math. Soc., Providence, 1966, pp. 187–197.
[12] *Lectures on Galois Cohomology of Classical Groups*, Tata Inst. of Fund. Research, Bombay, 1969.

[13] "Normal subgroups of integral orthogonal groups," in *Algebraic K-Theory and its Geometric Applications*, Lecture Notes in Math., No. 108, Springer, Berlin-Heidelberg-New York, 1969, pp. 67–71.
[14] "Normalteiler gannzähliger Spingruppen," *J. reine und angew.* **311–312** (1979), 191–214.
[15] "Erzeugung ganzzahlige orthogonaler Gruppen durch Spiegelungen," *Ann. Math.* **255** 4 (1981), 453–462.
Kneser M., Tamagawa T.
[1] "Another formulation and proof of Siegel's theorems on quadratic forms," in *Abstr. Short Communs. Intern. Congr. Math.*, Edinburgh, 1958, p. 32.
Knopp M. J., Newman M.
[1] "Congruence subgroups of positive genus of the modular group," *Illinois J. Math.* **9** 4 (1965), 577–583.
Koch H.
[1] *Galoissche Theorie der p-Erweiterungen*, Berlin, 1970.
Kolivagin V. A.
[1] "Finiteness of $E(\mathbb{Q})$ and $Ш(E,\mathbb{Q})$ for a subset of Weil curves," *Izv. Akad. Nauk SSSR, Ser. Mat.* **52** 3 (1988), 522–540.
[2] "On Mordel-Weil and Shafarevich-Tate groups for eliptical Weil curves," *Izv. Akad. Nauk SSSR, Ser. Mat.* **52** 6 (1988), 1154–1180.
Kostant B.
[1] "Groups over $\mathbb{Z}$," in *Algebraic Groups and Discontinuous Subgroups*, Proc. Symp. Pure Math., No. 9, Amer. Math. Soc., Providence, 1966, pp. 90-98.
Kottwitz R.
[1] "Stable trace formula: cuspidal tempered terms," *Duke Math. J.* **51** 3 (1984), 611–650.
[2] "Stable trace formula: elliptical singular terms," *Math. Ann.* **275** (1986), 365–399.
[3] "Tamagawa numbers," *Ann. Math.* **127** 3 (1988), 629–646.
Kunyavski B. E.
[1] "Arithmetic properties of three-dimensional algebraic tori," *Zap. Nauch. Sem. LOMI Akad. Nauk SSSR* **16** (1982), 102–107.
Kursov V. V.
[1] "On the commutator length of Chevalley groups over a field," *Dokl. Akad. Nauk BSSR* **29** 1 (1985), 27–30.
Kursov V. V., Yanchevskiĭ V. I.
[1] "Crossed products of simple algebras and their group automorphisms," *Dokl. Akad. Nauk BSSR* **32** 9 (1988), 777-780.
Labesse J.-P., Schwermer J.
[1] "On liftings and cusp cohomology of arithmetic groups," *Invent. Math.* **83** 2 (1986), 383–401.
Lai K. F.
[1] "On the Tamagawa number of quasi-split groups," *Bull. Amer. Math. Soc.* **82** 2 (1976), 300–302.
[2] "Tamagawa number of reductive algebraic groups," *Compos. Math.* **41** 2 (1980), 153–188.
[3] "On the cohomology of congruence subgroups of symplectic groups," *Nagoya Math. J.* **85** (1982), 155–174.
Lamont P.
[1] "Approximation theorems for the group G_2," *Indag. Math* **26** 2 (1964), 187–192.

Landherr W.
[1] "Liesche Ringe vom Typus A über einen algebraischen Zahlkörper und hermitesche Formen über einem Schiefkörper," *Abh. Math. Sem. Univ. Hamburg* **12** (1938), 200–241.
Lang S.
[1] "Algebraic groups over finite fields," *Amer. J. Math.* **78** 3 (1958), 553–563.
[2] *Algebraic Numbers*, Addison-Wesley, London, 1964.
[3] *Algebra*, Addison-Wesley, London, 1965.
Langlands R. P.
[1] "The volume of the fundamental domain for some arithmetical subgroups of Chevalley groups," in *Algebraic Groups and Discontinuous Subgroups*, Proc. Symp. Pure Math., No. 9, Amer. Math. Soc., Providence, 1966, pp. 143–148.
Lazard
[1] "Groupes analytiques p-adiques," *Publ. Math. I.H.E.S.* **26** (1965), 5–219.
Lee G.
[1] "A geometric method for presenting subgroups of discrete groups," *Topol. and Appl.* **18** 2–3 (1984), 179–195.
Lewis D. W.
[1] "Quaternionic skew-hermitian forms over a number field," *J. Algebra* **74** 1 (1982), 232–240.
Liehl B.
[1] "On the group SL_2 over orders of arithmetic type," *J. reine und angew.* **323** (1981), 753–771.
[2] "Beschränkte Wortlänge in SL_2," *Math. Z.* **186** 4 (1984), 509–524.
Lubotzky A.
[1] "Free quotients and the ocngruence kernel of SL_2," *J. Algebra* **77** 2 (1982), 411–418.
Lyndon R., Schupp P.
[1] *Combinatorial Group Theory*, Springer, 1977.
Macdonald I. G.
[1] "Spherical functions on a group of p-adic type," in *Publications of the Ramanujan Institute*, No. 2, Ramanujan Institute, University of Madras, 1971, pp. vii and 79.
Maclachlan C.
[1] "On the structure of certain arithmetic subgroups of $SL_2(\mathbb{R})$," *Math. Proc. Cambridge Phil. Soc.* **97** 2 (1985), 211–217.
Malcev A. I.
[1] "On semisimple subgroups of Lie groups," *Izv. Akad. Nauk SSSR, Ser. Mat.* **8** 4 (1944), 143–174.
[2] "On the theory of the Lie groups in the large," *Mat. Sb.* **16** 2 (1945), 163–189.
Margulis G. A.
[1] "Discrete isometry groups of varieties with negative curvature," in *Proceedings of the International Congress of Mathematicians (Vancouver, 1974)*, Canadian Mathematical Congress, Vancouver, 1975, Vol. **2**, pp. 21–33.
[2] "Corestricted subgroups of algebraic groups over local fields," *Funct. Anal. i evo Prilozhenia* **11** 2 (1977), 45–57.
[3] "Quotient groups of discrete subgroups and measure theory," *Funct. Anal. i evo Prilozhenia* **12** 4 (1978), 64–80.
[4] "Finiteness of quotient groups of discrete subgroups," *Funct. Anal. i evo Prilozhenia* **13** 3 (1979), 28–39.
[5] "On the multiplicative group of a quaternion algebra over a global field," *Dokl. Akad. Nauk SSSR* **252** 3 (1980), 542–546.

[6] "Arithmeticity of irreducible lattices of semisimple groups of rank greater than 1," *Invent. Math.* **76** 1 (1984), 93–120.
Margulis G. A., Soifer G. A.
[1] "Maximal subgroups of infinite index in finitely generated linear groups," *J. Algebra* **69** 1 (1981), 1–23.
Mars J. G.
[1] "Les nombres de Tamagawa de certains groupes exceptionnels," *Bull. Soc. Math. Fr.* **94** 2 (1966), 97–140.
[2] "Solution d'un problème posé par A. Weil," *C.R. Acad. Sci.* **266** 9 (1968), A484–A486.
[3] "The Tamagawa number of ${}^2A_n$," *Ann. Math.* **89** 3 (1969), 557–574.
[4] "Le nombres de Tamagawa de groupes semisimples," in *Séminaire Bourbaki, Vol. 1968/69*, Lecture Notes in Math., No. 179, Springer, Berlin-Heidelberg-New York, 1971, pp. 79–94.
Mathieu P.
[1] "Le principe de Hasse et les groupes semi-simples I," *Bull. Soc. Math. Belg.* **35** 2 (1983), 119–125.
Matsumoto M.
[1] "Une théorème de Sylow les groupes semisimple p-adiques," *C.R. Acad. Sci.* **262** 8 (1966), A425–A427.
[2] "Sur les sous-groupes arithmétiques des groupes semisimples deployée," *Ann. Sci. Ecole Norm. Sup.* **2** 1 (1969), 1–62.
Matthews C. R.
[1] "Counting points modulo p for some finitely generated subgroups of algebraic groups," *Bull. London Math. Soc.* **14** 2 (1982), 149–154.
Matthews C. R., Vaserstein L. N., Weisfeiller B.
[1] "Congruence properties of Zariski-dense subgroups I," *Proc. London Math. Soc.* **48** 3 (1984), 514–532.
Matveev G. V.
[1] "The genus of the elements of an orthogonal group," *Mat. Zametki* **13** 5 (1973), 695–702.
[2] "The genus of the elements of unitary groups," *Dokl. Akad. Nauk BSSR* **18** 5 (1974), 391–393.
[3] "The Hasse principle for lattices in a complete matrix algebra," *Mat. Zametki* **30** 6 (1981), 801–805.
Melnikov O. V.
[1] "The congruence-kernel of the group $SL_2(\mathbb{Z})$," *Dokl. Akad. Nauk SSSR* **228** 5 (1976), 1034–1036.
Mendoza E. R.
[1] "Cohomology of $PGL(2)$ over imaginary quadratic integers," *Bonn. Math. Schr.* **128** (1980).
Mennicke J.
[1] "Finite factor groups of the unimodular group," *Ann. Math.* **81** 1 (1965), 31–37.
[2] "On Ihara's modular group," *Invent. Math.* **4** 3 (1967), 202–228.
[3] "Discontinuous Groups," in *Groups—Korea 1983, Proceedings*, Lecture Notes in Math., No. 1098, Springer, Berlin-Heidelberg-New York-Tokyo, 1984, pp. 75–80.
Milne J. S.
[1] *Etale Cohomology*, Princeton University Press, Princeton, 1980.
[2] "The action of an automorphism of $\mathbb{C}$ on a Shimura variety and its special points," in *Arithmetic and Geometry*, Birkhäuser, Boston, 1983, Vol. **1**, pp. 239–264.

[3] *Arithmetic duality theorems*, Academic Press, Boston, 1986.

Milson J. J., Raghunathan M. S.

[1] "Geometric construction of cohomology for arithmetic groups," *Proc. Indian Acad. Sci. Math. Sci.* **90** 2 (1981), 103–123.

Minkowski H.

[1] "Über den arithmetischen Begriff der äquivalenz und über die endlichen Gruppen linearer ganzzahliger Substitutionenn," *J. reine und angew.* **109** (1887), 449–458.

[2] "Zur Theorie der positiven quadratischen Formen," *J. reine und angew.* **101** (1887), 196–202.

[3] *Geometrie der Zahlen*, Leipzig, 1910.

Mincev Kh. P.

[1] "Strong approximation for varieties over an algebraic number field," *Dokl. Akad. Nauk BSSR* **33** 1 (1989), 5–8.

Monastirni A. P., Yanchevskiĭ V. I.

[1] "On Whitehead groups and the Kneser-Tits conjecture for spinor groups," *Dokl. Akad. Nauk SSSR* **307** 1 (1989), 31–35.

Moore C.

[1] "Group extensions of p-adic and adelic linear groups," *Publ. Math. I.H.E.S.* **35** (1968), 5–70.

Moss K.

[1] "Homology of $SL\left(n, \mathbb{Z}\left[\frac{1}{p}\right]\right)$," *Duke Math. J.* **47** 4 (1980), 803–818.

Mostow G. D.

[1] "Self-adjoint groups," *Ann. Math.* **62** 1 (1955), 44–55.

[2] "Fully reducible subgroups of algebraic groups," *Amer. J. Math.* **78** (1956), 200–221.

[3] "Discrete subgroups of Lie groups," *Asterisque num. hous. ser.* (1985), 289–309.

Mostow G. D., Tamagawa T.

[1] "On the compactness of arithmetically defined homogeneous spaces," *Ann. Math.* **76** 3 (1962), 446–464.

Nagata M.

[1] "Invariants of a group in an affine ring," *J. Math. Kyoto Univ.* **3** (1964), 369–377.

Nakayama T., Matsushima Y.

[1] "Über die multiplikative Gruppe einer p-adischen Divisionsalgebra," *Proc. Imperial Academy (Tokyo)* **19** (1943), 622–628.

Newman M.

[1] "Normal congruence subgroups of the modular group," *Amer. J. Math.* **85** 3 (1963), 419–427.

[2] "Classification of normal subgroups of the modular group," *Trans. Amer. Math. Soc.* **126** (1967), 267–277.

[3] "The classical modular groups as a subgroup of $GL(2, \mathbb{Z})$," *Glasgow Math. J.* **27** (1985), 161–164.

Nisnevich Y.

[1] "Non-abelian cohomology and finiteness theorems for integral orbits of affine group schemes," *Izv. Akad. Nauk SSSR, Ser. Mat.* **39** 4 (1975), 773–795.

[2] "Espaces homogenes principaux rationellement triviaux et arithmétique des schemas en groupes reductifs sur les anneaux de Dedekind," *C.R. Acad. Sci.* **299** 1 (1984), 5–8.

Nori M.

[1] "Groupe de monodromie non arithmétique," *C.R. Acad. Sci.* **302** 2 (1986), 71–72.

[2] "On subgroups of $GL_n(F_p)$," *Invent. Math.* **88** 2 (1987), 257–275.

O'Meara O. T.

[1] *Introduction to Quadratic Forms*, Springer, Berlin-Heidelberg-New York, 1963.

[2] "On the finite generation of linear groups over Hasse domains," *J. reine und angew.* **217** (1965), 79–108.

Ono T.

[1] "On the compacity of the orthogonal groups," *Nagoya Math. J.* **7** (1954), 111-114.

[2] "Arithmetic of orthogonal groups," *Nagoya Math. J.* **9** (1955), 129–146.

[3] "The Hasse principle in orthogonal groups," *Sugaku* **7** 1 (1956), 15–22.

[4] "Sur une propriété arithmétique des groupes algébriques commutatifs," *Bull. Soc. Math. Fr.* **85** 3 (1957), 307–323.

[5] "Arithmetic of algebraic tori," *Ann. Math.* **74** 1 (1961), 101–139.

[6] "On the Tamagawa number of algebraic tori," *Ann. Math.* **78** 1 (1963), 47–73.

[7] "On the Tamagawa number," *Sugaku* **15** 2 (1963), 72–81.

[8] "On the relative theory of Tamagawa numbers," *Bull. Amer. Math. Soc.* **70** 2 (1964), 325–326.

[9] "The Gauss-Bonnet theorem and the Tamagawa number," *Bull. Amer. Math. Soc.* **71** 2 (1965), 345–348.

[10] "On the relative theory of Tamagawa numbers," *Ann. Math.* **82** 1 (1965), 88–111.

[11] "On algebraic groups and discontinuous groups," *Nagoya Math. J.* **27** 1 (1966), 279–322.

[12] "A generalization of Gauss' theorem on the genera of quadratic forms," *Proc. Jap. Acad.* **A61** 4 (1985), 109–111.

Opolka H.

[1] "Zur Auflosung zahlentheoŕetischer Knoten," *Math. Z.* **173** 1 (1980), 95–103.

[2] "Geschlechter von zentralen Erweiterungen," *Arch. Math.* **37** 5 (1981), 418–424.

Parimala R., Sridharan R.

[1] "A local-global principle for quadratic forms over polynomial rings," *J. Algebra* **74** 1 (1982), 264–269.

Piatetski-Shapiro I. I.

[1] "Arithmetic groups in complex domains," *Uspekhi Mat. Nauk.* **19** 6 (1964), 93–121.

[2] "Automorphic functions and arithmetic groups," in *Proceedings of the International Congress of Mathematicians (Moscow, 1966)*, Mir, Moscow, 1968, pp. 232–247.

Pierce R. S.

[1] *Associative Algebras*, Springer, 1982.

Pizer A.

[1] "On the arithmetic of quaternion algebras," *Acta Arith.* **31** 1 (1976), 61–89.

[2] "On the arithmetic of quaternion algebras II," *J. Math. Soc. Japan* **28** 4 (1976), 676–688.

Platonov V. P.

[1] "Adele groups and the genus problem for integral representations," *Dokl. Akad. Nauk BSSR* **12** 10 (1968), 866–868.

[2] "Adele groups and integral representations," *Izv. Akad. Nauk SSSR, Ser. Mat.* **33** 1 (1969), 155–162.

[3] "Strong approximation in algebraic groups and the Kneser-Tits conjecture," *Dokl. Akad. Nauk BSSR* **13** 7 (1969), 585–587.

[4] "The strong approximation problem and the Kneser-Tits conjecture for algebraic groups," *Izv. Akad. Nauk SSSR, Ser. Mat.* **33** 6 (1969), 1211–1219.

[5] "Additions to 'The strong approximation problem and the Kneser-Tits conjecture for algebraic groups'," *Izv. Akad. Nauk SSSR, Ser. Mat.* **34** 4 (1970), 775–777.

[6] "On the congruence problem for solvable integral groups," *Dokl. Akad. Nauk BSSR* **15** 10 (1971), 869–872.
[7] "On the maximality problem for arithmetic groups," *Dokl. Akad. Nauk SSSR* **200** 3 (1971), 530–533.
[8] "On the genus problem in arithmetic groups," *Dokl. Akad. Nauk SSSR* **200** 4 (1971), 793–796.
[9] "The arithmetic theory of linear algebraic groups and number theory," *Trudi Mat. Inst. Steklov. Akad. Nauk SSSR* 132 (1973), 162–168.
[10] "The Dieudonné conjecture and the non-surjectivity of coverings of algebraic groups on k-points," *Dokl. Akad. Nauk SSSR* **216** 5 (1974), 986–989.
[11] "Arithmetical and structural problems in linear algebraic groups," in *Proceedings of the International Congress of Mathematicians (Vancouver, 1974)*, Canadian Mathematical Congress, Vancouver, 1975, Vol. **1**, pp. 1471–476.
[12] "Algebraic groups," *Itogi Nauki i Tekhniki [Progress in Science and Technology]—Algebra, Topologoy, Geometry* **11** (1974), 5–36.
[13] "On the Tannaka-Artin problem," *Dokl. Akad. Nauk SSSR* **221** 5 (1975), 1038–1041.
[14] "Approximation in algebraic groups over arbitrary fields," *Dokl. Akad. Nauk SSSR* **229** 4 (1976), 804–807.
[15] "The Tannaka-Artin problem and reduced K-theory," *Izv. Akad. Nauk SSSR, Ser. Mat.* **40** 2 (1976), 227–261.
[16] "Reduced K-theory and approximation in algebraic groups," *Trudi Mat. Inst. Steklov. Akad. Nauk SSSR* **142** (1976), 198–207.
[17] "Birational properties of reduced Whitehead groups," *Dokl. Akad. Nauk BSSR* **21** 3 (1977), 227–261.
[18] "On the problem of the rationality of spinor varieties," *Dokl. Akad. Nauk SSSR* **248** 3 (1979), 524–527.
[19] "Algebraic groups and reduced K-theory," in *Proceedings of the International Congress of Mathematicians (Helsinki, 1978)*, 1980, pp. 311–317.
[20] "Birational properties of spinor varieties," *Trudi Mat. Inst. Steklov. Akad. Nauk SSSR* **157** (1981), 161–169.
[21] "The arithmetic theory of algebraic groups," *Uspekhi Mat. Nauk.* **37** 3 (1982), 3–54.
[22] "Adele groups and class numbers," *Trudi Mat. Inst. Steklov. Akad. Nauk SSSR* **163** (1984), 205–214.
[23] "Rings and varieties of representations of finitely generated groups," in *Problems in Algebra, 4th edition*, Minsk University Press, Minsk, 1988, pp. 36–40.
[24] "Representations of finitely generated groups and Grothendieck's problem," *Russian Math. Surveys* **45** (1990) N6, 191–192.

Platonov V. P., Benyash-Krivetz V. V.
[1] "Rings of characters of n-dimensional representations of finitely generated groups," *Dokl. Akad. Nauk SSSR* **289** 2 (1986), 293–297.

Platonov V. P., Bondarenko A. A., Rapinchuk A. S.
[1] "Class numbers of algebraic groups," *Dokl. Akad. Nauk SSSR* **245** 1 (1979), 26–31.
[2] "Class numbers and class groups of algebraic groups I," *Izv. Akad. Nauk SSSR, Ser. Mat.* **43** 3 (1979), 603–627.
[3] "Class numbers and class groups of algebraic groups II," *Izv. Akad. Nauk SSSR, Ser. Mat.* **44** 2 (1980), 395–414.

Platonov V. P., Chernousov V. I.
[1] "On the rationality of canonical spinor varieties," *Dokl. Akad. Nauk SSSR* **252** 5 (1980), 796–800.

Platonov V. P., Drakokhrust Yu. A.
[1] "The Hasse principle for algebraic number fields," *Dokl. Akad. Nauk SSSR* **281** 4 (1985), 793–797.
[2] "The Hasse norm principle for prime extensions of algebraic number fields," *Dokl. Akad. Nauk SSSR* **285** 4 (1985), 812–815.

Platonov V. P., Matveev G. V.
[1] "Adele groups and the finite approximability of linear groups under conjugation," *Dokl. Akad. Nauk BSSR* **14** 9 (1970), 777–779.

Platonov V. P., Milovanov M. V.
[1] "Determinability of algebraic groups by arithmetic subgroups," *Dokl. Akad. Nauk SSSR* **209** 1 (1973), 43–46.

Platonov V. P., Rapinchuk A. S.
[1] "Groups of rational points of three-dimensional groups," *Dokl. Akad. Nauk SSSR* **247** 2 (1979), 279–282.
[2] "The multiplicative structure of division algebras over number fields and the Hasse principle," *Dokl. Akad. Nauk SSSR* **266** 3 (1982), 560–564.
[3] "Algebraic Groups," *Itogi Nauki i Tekhniki [Progress in Science and Technology]—Algebra, Topologoy, Geometry* **21** (1983), 80–134.
[4] "The multiplicative structure of division algebras over number fields and the Hasse norm principle," *Trudi Mat. Inst. Steklov. Akad. Nauk SSSR* **165** (1984), 171–187.

Platonov V. P., Sharomet A. A.
[1] "On the congruence problem for linear groups over arithmetic rings," *Dokl. Akad. Nauk BSSR* **16** 5 (1972), 393–396.

Platonov V. P., Tavgen O. I.
[1] "On Grothendieck's problem on profinite completions of groups," *Dokl. Akad. Nauk SSSR* **288** 5 (1986), 1054–1058.
[2] "Grothendieck's Problem on Profinite Completions and Representations of Groups," *K-Theory* **4** 1 (1990).

Platonov V. P., Yanchevskiĭ V. I.
[1] "The structure of unitary groups and the commutator of a simple algebra over global fields," *Dokl. Akad. Nauk SSSR* **208** 3 (1973), 541–544.
[2] "On Harder's conjecture," *Dokl. Akad. Nauk SSSR* **221** 4 (1973), 784–787.
[3] "On the Kneser-Tits conjecture for unitary groups," *Dokl. Akad. Nauk SSSR* **225** 1 (1975), 48–51.
[4] "Towards a theory of Henselian division algebras," *Dokl. Akad. Nauk SSSR* **297** 2 (1987), 294–298.
[5] "Finite-dimensional Henselian division algebras," *Dokl. Akad. Nauk SSSR* **297** 3 (1987), 542–546.

Plesken W.
[1] "Finite unimodular groups of prime degree and circulants," *J. Algebra* **97** 1 (1985), 286–312.

Prasad G.
[1] "Strong approximation for semi-simple groups over function fields," *Ann. Math.* **105** 3 (1977), 553–572.
[2] "Non-vanishing of the first cohomology," *Bull. Soc. Math. Fr.* **105** 4 (1977), 415–418.
[3] "A variant of a theorem of Calvin Moore," *C.R. Acad. Sci. Ser. 1* **302** 11 (1986), 405–408.
[4] "Volumes of S-arithmetic quotients of semi-simple groups," *Publ. Math. I.H.E.S.* **69** (1989), 91–117.

Prasad G., Ragunathan M. S.
[1] "Tame subgroup of a semisimple group over a local field," *Amer. J. Math.* **105** 4 (1983), 1023–1048.
[2] "On the congruence subgroup problem: Determination of the metaplectic kernel," *Invent. Math.* **71** 1 (1983), 21–42.
[3] "Topological central extensions of semisimple groups over local fields," *Ann. Math.* **119** 1–2 (1984), 143–268.
[4] "On the Kneser-Tits problem," *Comment. Math. Helv.* **60** 1 (1985), 107–121.
[5] "Topological central extensions of $SL_1(D)$," *Invent. Math.* **92** 4 (1988), 645–689.
Quillen D. L.
[1] "Classification of normal congruence subgroups of the modular group," *Amer. J. Math.* **87** 2 (1965), 285–296.
Radtke W.
[1] "Diskontinuierliche arithmetische Gruppen im Funktionenkörperfall," *J. reine und angew.* **363** (1985), 191–200.
Raghunathan M. S.
[1] "Cohomology of arithmetic subgroups of algebraic groups I," *Ann. Math.* **86** 3 (1967), 409–424.
[2] "Cohomology of arithemtic subgroups of algebraic groups II," *Ann. Math.* **87** 2 (1968), 279–304.
[3] "A note on quotients of real algebraic groups by arithmetic subgroups," *Invent. Math.* **4** (1968), 318–335.
[4] "On the congruence subgroup problem," *Publ. Math. I.H.E.S.* **46** (1976), 107–161.
[5] *Discrete Subgroups of Lie Groups*, Springer, Berlin-Heidelberg-New York, 1972.
[6] "On the congruence subgroup problem II," *Invent. Math.* **85** 1 (1986), 73–117.
[7] "On the group of norm 1 elements in division algebra," *Math. Ann.* **279** (1988), 457–484.
Rapinchuk A. S.
[1] "On Platonov's conjecture concerning genus in arithmetic groups," *Dokl. Akad. Nauk BSSR* **25** 2 (1981), 101–104.
[2] "Class numbers in the genus of quadratic forms and algebraic groups," *Izv. Akad. Nauk SSSR, Ser. Mat.* **43** 4 (1981), 775–792.
[3] "On the metaplectic kernel for anisotropic groups," *Dokl. Akad. Nauk BSSR* **29** 12 (1985), 1068–1071.
[4] "The metaplectic kernel for $SL(1, D)$," *Dokl. Akad. Nauk BSSR* **30** 3 (1986), 197–200.
[5] "The Hasse principle for symmetric spaces," *Dokl. Akad. Nauk BSSR* **31** 9 (1987), 773–776.
[6] "The multiplicative arithmetic of division algebras over number fields and the metaplectic problem," *Izv. Akad. Nauk SSSR, Ser. Mat.* **51** 5 (1987), 1033–1064.
[7] "On the finite definability of the reduced norm in simple algebras," *Dokl. Akad. Nauk BSSR* **32** 1 (1988), 5–8.
[8] "The congruence problem for algebraic groups and strong approximation in affine varieties," *Dokl. Akad. Nauk BSSR* 7 (1988 32), 581–584.
[9] "On the congruence problem for algebraic groups," *Dokl. Akad. Nauk SSSR* **306** 6 (1989), 1304–1307.
Remeslennikov V. N.
[1] "The finite approximability of groups under conjugation," *Sibirsk. Mat. Z.* **12** 5 (1971), 1085–1099.

Richardson R.
[1] "Conjugacy classes in Lie algebras and algebraic groups," *Ann. Math.* **86** 1 (1967), 1–15.
Riehm C.
[1] "The norm 1 group of p-adic division algebras," *Amer. J. Math.* **92** 2 (1970), 499-523.
[2] "The congruence subgroup problem over local fields," *Amer. J. Math.* **92** 3 (1970), 771–778.
Rohlfs J.
[1] "Arithmetische definierte Gruppen mit Galois-operation," *Invent. Math.* **4** 2 (1978), 185–205.
[2] "Über maximale arithmetische definierte Gruppen," *Math. Ann.* **234** 3 (1978), 239–252.
[3] "Die maximalen arithmetische definierten Untergruppen zerfallender einfacher Gruppen," *Math. Ann.* **244** (1979), 219–231.
[4] "On the cuspidal cohomology of the Bianchi modular groups," *Math. Z.* **188** 2 (1985), 253–269.
Roĭter A. V.
[1] "On integral representations pertaining to like genus," *Izv. Akad. Nauk SSSR, Ser. Mat.* **30** 6 (1966), 1315–1324.
Rubin K.
[1] "Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication," *Invent. Math.* **89** 3 (1987), 527–560.
Sansuc J.-J.
[1] "Groupe de Brauer et arithmétique des groupes algébriques linéaires sur un corps de nombres," *J. reine und angew.* **327** (1981), 12–80.
[2] "Principle de Hasse, surfaces cubiques et intersections de deux quadriques," *Asterisque* **147–148** (1987), 183–207.
Sarkisyan R. A.
[1] "On an equality problem for Galois cohomology," *Algebra i Logika* **19** 6 (1980), 707–725.
[2] "Algorithmic questions regarding linear algebraic groups I," *Mat. Sb.* **113** 2 (1980), 179–216.
[3] "Algorithmic questions regarding linear algebraic groups II," *Mat. Sb.* **113** 3 (1980), 400–436.
Sataka I.
[1] "On compactifications of the quotient spaces for arithmetically defined discontinous groups," *Ann. Math.* **72** (1960), 555–580.
[2] "Theory of spherical functions on reductive algebraic groups over p-adic fields," *Publ. Math. I.H.E.S.* **18** (1963), 1–69.
Schacher M.
[1] "Subfields of division rings I," *J. Algebra* **9** 4 (1968), 451–477.
Scharlau W.
[1] *Quadratic and Hermitian Forms*, Springer, Berlin-Heidelberg-New York, 1985.
Schinzel A.
[1] "Hasse's principle for systems of ternary quadratic forms and for one biquadratic form," *Stud. Math.* **77** 2 (1983), 103–109.
Schur I.
[1] "Über die Darstellung der symmetrischen und der alterniernden Gruppen durch gebrochene lineare Substitutionen," *J. reine und angew.* **139** (1911), 155–250.

Schwermer J.
[1] *Kohomologie arithmetische definierter Gruppen und Eisensteinreihen*, Lecture Notes in Math., No. 988, Springer, Berlin-Heidelberg-New York-Tokyo, 1983.
[2] "On arithmetic quotients on the Siegel upper half space of degree two," *Compos. Math.* **58** 2 (1986), 233–258.
Schwermer J., Vogtmann K.
[1] "The integral homology of SL_2 and PSL_2 of euclidean imaginary quadratic integers," *Comment. Math. Helv.* **58** 4 (1983), 573–598.
Seip-Hornix E. A. M.
[1] "Clifford algebras of quadratic quaternion forms I, II," *Indag. Math.* **27** 2 (1965), 326–363.
Seminar on Algebraic Groups, Mir, Moscow, 1973.
Serre J.-P.
[1] *Cohomologie Galoisienne*, Springer, 1964.
[2] "Groupes de congruence," in *Séminaire Bourbaki (1966–1967)*, Benjamin, New York, 1968.
[3] *Groupes algébriques et corps de classes*, Hermann, Paris, 1959.
[4] *Lie Algebras and Lie Groups*, Benjamin, New York-Amsterdan, 1965.
[5] "Cohomologie des groupes discrets," in *Séminaire Bourbaki, Vol. 1970/71*, Lecture Notes in Math., No. 244, Springer, Berlin-Heidelberg-New York, 1971, pp. 337–350.
[6] "Cohomologie des groupes discrets," in *Prospects in Mathematics*, Annals of Mathematics Studies, No. 70, Princeton Univ. Press, Princeton, 1971, pp. 77–169.
[7] "Le problème des groupes de congruence pour SL_2," *Ann. Math.* **92** 3 (1970), 489–527.
[8] *Cours d'Arithmétique*, Paris, 1970.
[9] *Abelian l-adic representations and elliptic curves*, Benjamin, New York-Amsterdam, 1968.
[10] *Trees*, Springer, 1980.
[11] "Cohomologie des groupes discrets," in *Prospects in Mathematics*, Annals of Mathematics Studies, No. 70, Princeton Univ. Press, Princeton, 1971.
[12] "Arithmetic groups," in *Homological Group Theory*, London Math. Soc. Lect. Notes Series, No. 36, Cambridge University Press Cambridge, 1979, pp. 105–135.
Shafarevich I. R.
[1] *Fundamentals of Algebraic Geometry*, 2 volumes, Nauka, Moscow, 1988.
Sharomet A. A.
[1] "The congruence problem for solvable algebraic groups over global fields with char > 0," *Dokl. Akad. Nauk BSSR* **31** 3 (1987), 201–204.
Shimizu A.
[1] "On complex tori with many endomorphisms," *Tsukuba J. Math.* **8** 2 (1984), 297–318.
Shimura G.
[1] "Arithmetic of unitary groups," *Ann. Math.* **79** (1964), 369–409.
[2] *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton University Press, 1971.
Shyr J.-M.
[1] "On some class number relations of algebraic tori," *Mich. Math. J.* **24** 3 (1977), 365–377.
[2] "A generalization of Dirichlet's unit theorem," *J. Number Theory* **9** 2 (1977), 213–217.

Siegel C. L.
[1] "Über die analytische Theorie der quadratischen Formen," *Ann. Math.* **36** (1935), 527–606.
Sliman M.
[1] "Theorie de Mackey pour les groupes adeliques," *Asterisque* **115** (1984), p. 151.
[2] "Theorie de Mackey pour les groupes adeliques. Decomposition de $L^2(G_A/G_{\mathbb{Q}})$ et $L^2(G_{\mathbb{R}}/G_{\mathbb{Z}})$," *C.R. Acad. Sci. Ser. 1* **298** 12 (1984), 261–264.
Smythe N.
[1] "A presentation for group of integer matrices," *Canad. Math. Bull.* **25** 2 (1982), 215–221.
Soule C.
[1] "The cohomology of $SL_3(\mathbb{Z})$," *Topology* **17** (1978), 1–22.
Soule C., Tezuka M., Yagita N.
[1] "Cohomological behaviour of the reduction modulo a prime of $GL_3(\mathbb{Z})$," *J. Pure Appl. Algebra* **32** 2 (1984), 219–229.
Speh B.
[1] "Unitary representations of $SL(n, \mathbb{R})$ and the cohomology of congruence subgroups," in *Non-Commutative Harmonic Analysis and Lie Groups. Proceedings, 1980*, Lecture Notes in Math., No. 880, Springer, Berlin-Heidelberg-New York, 1981, pp. 483–505.
Springer T. A.
[1] "On the equivalence of quadratic forms," *Indag. Math.* **21** (1959), 241–253.
[2] *Linear Algebraic Groups*, Birkhäuser, Boston, 1981.
[3] "Conjugacy classes in algebraic groups," in *Group Theory, Beijing 1984*, Lecture Notes in Math., No. 1185, Springer, Berlin-Heidelberg-New York-Tokyo, 1986, pp. 175–209.
Steinberg R.
[1] "Regular elements of semisimple algebraic groups," *Publ. Math. I.H.E.S.* **25** (1965), 281–312.
[2] "Endomorphisms of linear algebraic groups," *Mem. Amer. Math. Soc.* **80** (1968), 1–108.
[3] *Lectures on Chevalley Groups*, Yale University Press, 1967.
Stothers W. W.
[1] "Level and index in the modular group," *Proc. Roy. Soc. Edinburgh* **A99** 1–2 (1984), 115–126.
Stuhler U.
[1] "Zur Frage der endlichen Präsentierbarkeit gewisser arithmetischer Gruppen in Funktionenkörperfall," *Math. Ann.* **224** (1976), 217–232.
[2] "Homological properties of certain arithmetic groups in the function field case," *Invent. Math.* **57** 3 (1980), 263–281.
[3] "On the cohomology of SL_n over rings of algebraic functions," in *Algebraic K-Theory. Proceedings, 1980*, Lecture Notes in Math., No. 967, Springer, Berlin-Heidelberg-New York, 1982, pp. 316–359.
[4] "Über die Faktorkommutatorgruppe der Gruppen $SL_2(\mathbb{Q})$ im Funktionenkörperfall," *Arch. Math.* **42** 4 (1984), 314–324.
[5] "Über die Kohomologie einiger arithmetischer Varietäten," *Math. Ann.* **273** 4 (1986), 685–699.
Suzuki K.
[1] "On normal subgroups of twisted Chevalley groups over local rings," *Sci. Rep. Tokyo Kyoiku Daigaku, Sect. A* **13** 366–382 (1977), 238–249.

Swift J., Reiner D.
[1] "Congruence subgroups of matrix groups," *Pacific J. Math.* **6** 3 (1956), 529–540.
Tamagawa T.
[1] "On indefinite quadratic forms," *J. Math. Soc. Japan* **29** 2 (1977), 355–361.
Tate J.
[1] "The cohomology groups of tori in finite Galois extensions of number fields," *Nagoya Math. J.* **27** (1966), 709–719.
Tavgen O. I.
[1] "The Grothendieck problem in a set of solvable groups," *Dokl. Akad. Nauk BSSR* **31** 10 (1987), 873–876.
[2] "On the Grothendieck and Platonov conjectures," *Dokl. Akad. Nauk BSSR* **32** 6 (1988), 489–492.
[3] "The finite width of arithmetic Chevalley subgroups of rank ≥ 2," *Dokl. Akad. Nauk SSSR* **310** 4 (1990), 802–806.
Tezuka M., Yagita N.
[1] "The cohomology of subgroups of $GL_n(F_q)$," *Contemporary Math.* **19** (1983), 379–396.
Séminaire Sophus Lie, 1954–1955
[1] *Theorie des algebres de Lie. Topologie des groupes de Lie*, Paris, 1955.
Thomas S.
[1] "An identification theorem for the locally finite nontwisted Chevalley groups," *Arch. Math.* **40** 1 (1983), 21–31.
Tits J.
[1] "Algebraic and abstract simple groups," *Ann. Math.* **80** 2 (1964), 313–329.
[2] "Classification of algebraic semisimple groups," in *Algebraic Groups and Discontinuous Subgroups*, Proc. Symp. Pure Math., No. 9, Amer. Math. Soc., Providence, 1966.
[3] "Systèmes generateurs de groupes de congruence," *C.R. Acad. Sci.* **283** 9 (1976), A693–A695.
[4] "Groupes de Whitehead de groupes algébriques simples sur un corps (d'apres V. P. Platonov et al.)," in *Séminaire Bourbaki, Vol. 1976/77, Exp. 505*, Lecture Notes in Math., No. 677, Springer, Berlin-Heidelberg-New York, 1978, pp. 218–236.
[5] "Reductive groups over local fields," in *Automorphic Forms, Representations and L-Functions*, Proc. Symp. Pure Math., No. 33, Amer. Math. Soc., Providence, 1979, pp. 29–69.
[6] *Liescher Gruppen und Algebren*, Springer, Berlin, 1983.
Tomanov G. M.
[1] "About the multiplicative structure of division algebras over number fields," *Dokl. Bulg. Akad. Nauk* **38** 1 (1985), 11–14.
[2] "Sur la structure des groupes algébriques simples de type D_n definis sur des corps de nombres," *C.R. Acad. Sci. Ser. 1* **306** 15 (1988), 647–650.
[3] "On Grunwald-Wang's theorem," *J. reine und angew.* **389** (1988), 209–220.
Van-der-Waerden B. L.
[1] *Algebra*, Ungar, New York, 1970.
[2] *Algebra*, Ungar, New York, 1970.
Vasserstein L. N.
[1] "On SL_2 over an arithmetic Dedekind ring," *Mat. Sb.* **89** 2 (1972), 313–322.
[2] "On full subgroups of Chevalley groups," *Tohôku Math. J.* **37** 4 (1985), 423–454.
[3] "On arithmetic subgroups of simple algebraic groups," *Linear Algebra and Appl.* **72** (1985), 93–96.

Venkataramana T. N.
[1] "Sur la super-rigiditée et la'arithméticité des reseaux dans les groupes sur des corps locaux de characteristique quelconque," *C.R. Acad. Sci.* **302** 10 (1986), 371–373.
[2] "Zariski-dense subgroups of arithmetic groups," *J. Algebra* **108** 2 (1987), 325–339.
Vinberg E. B.
[1] "On the groups of units of certain quadratic forms," *Mat. Sb.* **87** 1 (1972), 18–36.
Vinberg E. B., Gorbatsevich V. V., Schwarzman O. V.
[1] "Discrete subgroups of Lie groups," *Itogi Nauki i Tekhniki [Progress in Science and Technology], Contemporary problems in Mathematics: Basic Directions* **21** (1988), 5–120.
Vinberg E. B., Onishchik A. L.
[1] *Seminar on Lie groups and algebraic groups*, Nauka, Moscow, 1988.
Vinberg E. B., Schwarzman O. V.
[1] "Discrete isometry groups of spaces with constant curvature," *Itogi Nauki i Tekhniki [Progress in Science and Technology], Contemporary problems in Mathematics: Basic Directions* **29** (1988), 147–259, VINITI.
Voronovich I. I.
[1] "The local-global principle for algebras over fields of rational functions," *Dokl. Akad. Nauk BSSR* **31** 10 (1987), 877–880.
[2] "A linear local-global principle for algebras over fields of rational functions," Preprint No. 25/295, Minsk Inst. Math. AN BSSR.
Voskresenskiĭ V. Ye.
[1] "Birational properties of linear algebraic groups," *Izv. Akad. Nauk SSSR, Ser. Mat.* **34** 1 (1970), 3–19.
[2] "On weak approximation in algebraic groups," *Studies in Number Theory, Saratov Institute [Russian]* **4**, 3–7.
[3] *Algebraic Tori*, Nauka, Moscow, 1977.
[4] "Integral structures in algebraic tori and class groups of number fields," in *Seminar on the Arithmetic of Algebraic Varieties, Saratov*, 1979, pp. 8–15.
[5] "Projective invariant Demazure models," *Izv. Akad. Nauk SSSR, Ser. Mat.* **46** 2, 195–210.
[6] "Arithmetic of algebraic groups and homogeneous spaces," *Studies in Number Theory, Saratov Institute [Russian]* **9**, 7–38.
Vogtmann K.
[1] "Rational homology of Bianchi groups," *Math. Ann.* **272** 3 (1985), 399–419.
Wallace D. I.
[1] "Conjugacy class of hyperbolic matrices in $SL(n, \mathbb{Z})$ and ideal classes in an order," *Trans. Amer. Math. Soc.* **283** 1 (1984), 177–184.
Wang S.
[1] "On the commutator group of a simple algebra," *Amer. J. Math.* **72** 2 (1950), 323–334.
[2] "A note on free subgroups in linear groups," *J. Algebra* **71** 1 (1981), 232–234.
[3] "On anisotropic solvable linear algebraic groups," *Proc. Amer. Math. Soc.* **84** 1 (1982), 11–15.
Wehrfritz B. A. E.
[1] "The conjugacy of tori," *Bull. London Math. Soc.* **18** 1 (1986), 11–16.
Weil A.
[1] "Sur la theorie des formes quadratiques," in *Colloque sur la theorie des groupes algébriques, Bruxelles*, Louvain-Paris, 1962, pp. 9–22.

[2] "On the arithmetic theory of the classical groups," in *Proc. Conf. Arithm. Algebr. Geom.*, New York, 1963, pp. 1–3.
[3] "Algebras with involutions and the classical groups," *J. Indian Math. Soc.* **24** (1961), 589–623.
[4] *Adeles and Algebraic Groups*, Lecture notes, the Institute for Advanced Study, Princeton, 1961, Vol. **7**.
[5] "Sur certains groupes d'operateurs unitaries," *Acta Math.* **111** 1–4 (1964), 143–211.
[6] "Sur la formule de Siegel dans la theorie des groupes classiques," *Acta Math.* **113** 1–2 (1965), 1–87.
[7] *Basic Number Theory*, Springer, 1967.
[8] *Adeles and algebraic groups*, Birkhaüser, Boston, 1982.

Weisfeiler B.
[1] "The Hasse principle for algebraic groups decomposable over quadratic extensions," *Funct. Anal. i evo Prilozhenia* **6** 2 (1972), 21–23.
[2] "Strong approximation for Zariski-dense subgroups of semi-simple algebraic groups," *Ann. Math.* **120** 2 (1984), 271–315.

Weisman C. S.
[1] "On the connected identity component of adele class group of an algebraic torus," *Proc. Amer. Math. Soc.* **21** 1 (1969), 155–160.

Whitney H.
[1] "Elementary structure of real algebraic varieties," *Ann. Math.* **66** 3 (1957), 545–556.

Witt E.
[1] "Schiefkörper über diskret Bewertung Körpern," *J. reine und angew.* **176** (1936), 153–156.

Yanchevskiĭ V. I.
[1] "Commutator groups of simple algebras with surjective reduced norm," *Dokl. Akad. Nauk SSSR* **221** 5 (1975), 1056–1058.
[2] "Reduced unitary K-theory and division algebras over Henselian discretely valued fields," *Izv. Akad. Nauk SSSR, Ser. Mat.* **42** 4 (1978), 879–918.
[3] "Reduced unitary K-theory. Applications to algebraic groups," *Mat. Sb.* **110** 4 (1979), 579–596.

Zakiryanov K. Kh.
[1] "Finite width of simplectic groups over rings of algebraic numbers with respect to elementary matrices," *Algebra i Logika* **24** 6 (1985), 667–673.

Zimmert R.
[1] "Zur SL_2 der ganzen Zahlen eines imaginarquadratischen Zahlkörpers," *Invent. Math.* **19** (1973), 73–82.

Zucker St.
[1] "Hodge theory and arithmetic groups," *Asterisque* **101–102** (1983), 365–381.

Index

D

E

F

G

H