Proceedings of Symposia in

PURE MATHEMATICS

Volume 9

Algebraic Groups and Discontinuous Subgroups

Symposium on Algebraic Groups
July 5-August 6, 1965
Boulder, Colorado

Armand Borel
George D. Mostow
Editors

American Mathematical Society
Providence, Rhode Island

PROCEEDINGS OF THE SYMPOSIUM IN PURE MATHEMATICS
OF THE AMERICAN MATHEMATICAL SOCIETY
HELD AT THE UNIVERSITY OF COLORADO
BOULDER, COLORADO JULY 5 - AUGUST 6, 1965

Prepared by the American Mathematical Society
under National Science Foundation Grant GP-3983
and Office of Naval Research Grant Nonr(G)00055-65

2000 *Mathematics Subject Classification.* Primary 14-XX.

International Standard Serial Number 0082-0717
International Standard Book Number 0-8218-1409-5
Library of Congress Catalog Number 66-18581

10 9 8 7 6 5 04 03 02 01 00

Foreword

This book is an outgrowth of the twelfth Summer Mathematical Institute of the American Mathematical Society, which was devoted to Algebraic Groups and Discontinuous Subgroups. The Institute was held at the University of Colorado in Boulder from July 5 to August 6, 1965, and was financed by the National Science Foundation and the Office of Naval Research. The present volume consists of the Institute lecture notes, in part slightly revised, and of a few papers written somewhat later.

From the beginning, it was understood that a comprehensive exposition of the arithmetic aspects of algebraic groups should be a central aim of the Institute. In order to survey effectively the topics chosen for discussion, some important parts of the theory of Lie groups and algebraic groups had to be omitted, and the program was concentrated around five major themes: linear algebraic groups and arithmetic groups, adèles and arithmetic properties of algebraic groups, automorphic functions and spectral decomposition of L^2-spaces of coset spaces, holomorphic automorphic functions on bounded symmetric domains and moduli problems, vector valued cohomology and deformation of discrete subgroups. The lectures fulfilled diverse needs, and accordingly the papers in this book are intended to serve various purposes: to supply background material, to present the current status of a topic, to describe some basic methods, to give an exposition of more or less known material for which there is no convenient reference, and to present new results. It is hoped that this collection of papers will facilitate access to the subject and foster further progress.

A. Borel
G. D. Mostow

Contents

I. Algebraic Groups, Arithmetic Groups

II. Arithmetic Properties of Algebraic Groups. Adèle Groups

III. Automorphic Functions and Decomposition of $L^2(G/\Gamma)$

IV. Bounded Symmetric Domains, Holomorphic Automorphic Forms, Moduli

V. Quotients of Symmetric Spaces. Deformations

I. Algebraic Groups, Arithmetic Groups

Linear Algebraic Groups

BY

ARMAND BOREL

This is a review of some of the notions and facts pertaining to linear algebraic groups. From §2 on, the word linear will usually be dropped, since more general algebraic groups will not be considered here.

1. **The notion of linear algebraic group.** According to one's taste about naturality and algebraic geometry, it is possible to give several definitions of linear algebraic groups. The first one is not intrinsic at all but suffices for what follows.

1.1. *Algebraic matrix group.* Let Ω be an algebraically closed field. We shall denote by $M(n, \Omega)$ the group of all $n \times n$ matrices with entries in Ω and by $GL(n, \Omega)$ the group of all $n \times n$ invertible matrices. $GL(n, \Omega)$ is an affine subvariety of Ω^{n^2+1} through the identification

$$g = (g_{ij}) \mapsto (g_{11}, g_{12}, \cdots, g_{nn}, (\det g)^{-1}).$$

The set $M(n, \Omega)$ carries a topology—the Zariski topology—the closed sets being the algebraic subsets of $M(n, \Omega) = \Omega^{n^2}$. The ring $GL(n, \Omega)$ is an open subset of $M(n, \Omega)$ and carries the induced topology.

A subgroup of G of $GL(n, \Omega)$ is called an algebraic matrix group if G is a closed subset of $GL(n, \Omega)$, i.e., if there exist polynomials $p_\alpha \in \Omega[X_{11}, X_{12}, \cdots, X_{nn}]$ $(\alpha \in J)$ such that

$$G = \{g = (g_{ij}) \in GL(n, \Omega) | p_\alpha(g_{ij}) = 0, \ (\alpha \in J)\}.$$

The coordinate ring $\Omega[G]$ of G, i.e., the ring of all regular functions on G, is the Ω-algebra generated by the coefficients g_{ij} and $(\det g)^{-1}$. It is the quotient ring $\Omega[X_{ij}, Z]/I$, where I is the ideal of polynomials in the $n^2 + 1$ letters X_{ij}, Z vanishing on G, considered as a subset of Ω^{n^2+1}, via the above imbedding of $GL(n, \Omega)$ in Ω^{n^2+1}.

When B is a subring of Ω, we shall denote by $GL(n, B)$ the set of $n \times n$ matrices g with entries in B, such that $\det g$ is a unit in B, and by G_B the intersection $G \cap GL(n, B)$.

Let k be a subfield of Ω. The algebraic matrix group G is *defined over* k or is a k-group if the ideal I of polynomials annihilated by G has a set of generators in $k[X_{ij}, Z]$. If I_k denotes the ideal of all polynomials with coefficients in k vanishing on G, the quotient ring $k[X_{ij}, Z]/I_k = k[G]$ is the coordinate ring of G over k.

REMARK. If the field k is not perfect, it is not enough to assume that G is k-closed (i.e., that G is defined by a set of equations with coefficients in k) to conclude that G is defined over k; one can only infer that G is defined over a purely inseparable extension k' of k.

The following variant of the definition eliminates the choice of a basis.

1.2. *Algebraic groups of automorphisms of a vector space.* Let V be an n-dimensional vector space over Ω, and $GL(V)$ the group of all automorphisms of V. Every base of V defines an isomorphism of $GL(V)$ with $GL(n, \Omega)$. A subgroup G of $GL(V)$ is called an algebraic group of automorphisms of V if any such isomorphism maps G onto an algebraic matrix group.

Let k be a subfield of Ω. Assume that V has a k-structure, i.e., that we are given a vector subspace V_k over k of V such that $V = V_k \otimes_k \Omega$. The subgroup of G of $GL(V)$ is then defined over k if there exists a basis of V_k such that the corresponding isomorphism $\beta: GL(V) \to GL(n, \Omega)$ maps G onto a k-group in the previous sense.

1.3. *Affine algebraic group.* Let G be an affine algebraic set. It is an affine algebraic group if there are given morphisms

$$\mu: G \times G \to G, \qquad \mu(a, b) = ab,$$
$$\rho: G \to G, \qquad \rho(a) = a^{-1},$$

of affine sets, with the usual properties. G is an affine algebraic group defined over k if G, μ and ρ are defined over k. One can prove that every affine algebraic group defined over k is isomorphic to an algebraic matrix group defined over k.

1.4. *Functorial definition of affine algebraic groups.* Sometimes one would like not to emphasize a particular algebraically closed extension of the field k. For instance in the case of adèle groups, an algebraically closed field containing every p-adic completion of a number field k is a cumbersome object. Let G be a k-group in the sense of §1.1. Then for any k-algebra A, we may consider the set G_A of elements of $GL(n, A)$ whose coefficients annihilate the polynomials in I_k. It is a group, which may be identified to the group $\mathrm{Hom}_k(k[G], A)$ of k-homomorphisms of $k[G]$ into A. Furthermore, to any homomorphism $\rho: A \to B$ of k-algebras corresponds canonically a homomorphism $G_A \to G_B$. Thus we may say that a k-group is a functor from k-algebras to groups, which is representable by a k-algebra $k[G]$ of finite type, such that $\bar{k} \otimes k[G]$ has no nilpotent element, $\bar{k}$ being an algebraic closure of k. (The last requirement stands for the condition that $I_k \otimes \Omega$ is the ideal of all polynomials vanishing on G, it would be left out in a more general context.) This definition was introduced by Cartier as a short cut to the notion of (absolutely reduced) "affine scheme of groups over k." The functors corresponding to the general linear group and the special linear group, will be denoted GL_n and SL_n, and $(GL_n)_A$ by $GL_n(A)$ or $GL(n, A)$.

Usually the more down to earth point of view of algebraic matrix groups will be sufficient.

1.5. *Connected component of the identity.* An algebraic set is reducible if it is the union of two proper closed subsets; it is nonconnected if it is the union of two proper disjoint closed subsets. An algebraic group is irreducible if and only if it is connected. To avoid confusion with the irreducibility of a linear group, we shall usually speak of connected algebraic groups. The connected component of the identity of G will be denoted by G^0. The index of G^0 in G is finite.

If $\Omega = \boldsymbol{C}$, every affine algebraic group G can be viewed as a complex Lie group; then G is connected as an algebraic group, if and only if G is connected as a Lie group. When G is defined over $\boldsymbol{R}$, $G_{\boldsymbol{R}}$ is a closed subgroup of $GL(n, \boldsymbol{R})$ and hence a real Lie group. It is not true that for a connected algebraic $\boldsymbol{R}$-group, the Lie group $G_{\boldsymbol{R}}$ is also connected, but in any case it has only finitely many connected components. The connected component of the identity for the usual topology will be denoted $G_{\boldsymbol{R}}^0$.

Let G be connected. Then $\Omega[G]$ is an integral domain. Its field of fractions $\Omega(G)$ is the field of rational functions on G. The quotient field of $k[G]$ is a subfield of $\Omega(G)$, consisting of those rational functions which are defined over k.

1.6. *The Lie algebra of an algebraic group.* A group variety is nonsingular, so that the tangent space at every point is well defined. The tangent space $\mathfrak{g}$ at e can be identified with the set of Ω-derivations of $\Omega[G]$ which commute with right translations. $\mathfrak{g}$, endowed with the Lie algebra structure defined by the usual vector space structure and bracket operations on derivations, is the *Lie algebra of* $\mathfrak{g}$. Of course, G and G^0 have the same Lie algebra. If G is connected, $\mathfrak{g}$ could alternatively be defined as the Lie algebra of Ω-derivations of the field $\Omega(G)$, which commute with right translations (and the definition would then be valid for any algebraic group linear or not). If G is defined over k, we have $\mathfrak{g} = \mathfrak{g}_k \otimes_k \Omega$, where $\mathfrak{g}_k$·is the set of derivations which leave $k[G]$ stable. If the characteristic p of k is $\neq 0$, then $\mathfrak{g}$ and $\mathfrak{g}_k$ are restricted Lie algebras, in the sense of Jacobson. However the connection between an algebraic group and its Lie algebra in characteristic $p \neq 0$ is weaker than for a Lie group; for instance, there does not correspond a subgroup to every restricted Lie subalgebra of $\mathfrak{g}$, and it may happen that several algebraic subgroups have the same Lie algebra.

The group G operates on itself by inner automorphisms. The differential of $\operatorname{Int} g : x \mapsto g \cdot x \cdot g^{-1}$ $(x, g \in G)$ at e is denoted $\operatorname{Ad}_{\mathfrak{g}} g$. The map $g \mapsto \operatorname{Ad}_{\mathfrak{g}} g$ is a k-morphism (in the sense of 2.1) of G into $GL(\mathfrak{g})$, called the *adjoint representation of G.*

1.7. *Algebraic transformation group.* If G is an algebraic group and V is an algebraic set, G operates morphically on V (or G is an algebraic transformation group) when there is given a morphism $\tau \colon G \times V \to V$ with the usual properties of transformation groups. It operates k-morphically if G, V and τ are defined over k.

An elementary, but basic, property of algebraic transformation groups is the existence of at least one closed orbit (e.g. an orbit of smallest possible dimension [1, §16]).

2. Homomorphism, characters, subgroups and quotient groups of algebraic groups.

2.1. *Homomorphisms of algebraic groups.* Let ρ, G, G' be algebraic groups and $\rho \colon G_\Omega \to G'_\Omega$ be a map. It is a morphism of algebraic groups if:

(1) ρ is a group homomorphism from G_Ω to G'_Ω;

(2) the transposed map ρ^0 of ρ is a homomorphism of $\Omega[G']$ into $\Omega[G]$ (if $f \in \Omega[G'], f$ is a map from G'_Ω to Ω and $\rho^0(f) = f \circ \rho$). In case G and G' are defined over k, the map ρ is a k-morphism if moreover ρ^0 maps $k[G']$ into $k[G]$. The differential $d\rho$ at the identity element of the morphism $\rho: G \to G'$ defines a homomorphism $d\rho: \mathfrak{g} \to \mathfrak{g}'$ of the corresponding Lie algebras.

A rational representation of G is a morphism $\rho: G \to \boldsymbol{GL}_m$. Let G be considered as a matrix group so that $\Omega[G] = \Omega[g_{11}, \cdots, g_{nn}, (\det g)^{-1}]$. Each coefficient of the matrix $\rho(g), g \in G$, is then a polynomial in $g_{11}, g_{12}, \cdots, g_{nn}, (\det g)^{-1}$.

2.2. *Characters.* A *character* of G is a rational representation of degree 1; $\chi: G \to \boldsymbol{GL}_1$. The set of characters of G is a commutative group, denoted by $X(G)$ or $\hat{G}$. The group $\hat{G}$ is finitely generated; it is free if G is connected [**8**]. If one wants to write the composition-law in $\hat{G}$ multiplicatively, the value at $g \in G$ of $\chi \in G$ should be noted $\chi(g)$. But since one is accustomed to add roots of Lie algebras, it is also natural to write the composition in $\hat{G}$ additively. The value of χ at g will then be denoted by g^χ. To see the similarity between roots and characters take $\Omega = \boldsymbol{C}$; if $X \in \mathfrak{g}$, the Lie algebra of G, $(e^X)^\chi = e^{d\chi(X)}$, where $d\chi$ is the differential of $d\chi$ at e; $d\chi$ is a linear form over $\mathfrak{g}$. In the sequel, we shall often not make any notational distinction between a character and its differential at e.

2.3. *Subgroups, quotients* [**4**, **7**]. Let G be an algebraic group defined over k, H a closed subgroup of G; it is a k-subgroup of G if it is defined over k as an algebraic group. H is in particular k-closed. The converse need not be true. The homogeneous space G/H can be given in a natural way a structure of quasi-projective algebraic set defined over k. (A quasi-projective algebraic set is an algebraic set isomorphic to an open subset of a projective set.) The projection $\pi: G \to G/H$ is a k-morphism of algebraic sets which is "separable" ($d\pi$ is surjective everywhere) such that every morphism $\phi: G \to V$, constant along the cosets of H, can be factored through π. Moreover, G acts on G/H as an algebraic group of transformation; if H is a normal k-subgroup of G, then G/H is an algebraic group defined over k.

Assume that in G there exist a subgroup H and a normal subgroup N such that

(1) G is the semidirect product of H and N as abstract group,

(2) the map $\mu: H \times N \to G$, with $\mu(h, n) = hn$, is an isomorphism of algebraic varieties.

Then G is called the semidirect product of the algebraic groups H and N. In characteristic zero the condition (2) follows from (1). In characteristic $p > 0$, it is equivalent with the transversality of the Lie algebras of H and N or with the regularity of $d\mu$ at the origin, but does not follow from (1).

2.4. *Jordan decomposition of an element of an algebraic group* [**1**, **4**]. Let

$$g \in \boldsymbol{GL}(n, \Omega),$$

g can be written uniquely as the product $g = g_s \cdot g_n$, where g_s is a semisimple matrix (i.e., g_s can be made diagonal) and g_n is a unipotent matrix (i.e., the only eigenvalue of g_n is 1, or equivalently $g_n - I$ is nilpotent) and $g_s \cdot g_n = g_n \cdot g_s$. If G is an algebraic matrix group and $g \in G$, one proves that g_n and g_s belong also to G and that the decomposition of g in a semisimple and an unipotent part does not depend on the representation of G as a matrix group. More generally, if $\phi : G \to G'$ is a morphism of algebraic groups and $g \in G$, then $\phi(g_s) = [\phi(g)]_s$ and $\phi(g_n) = [\phi(g)]_n$. If $g \in G_k$, g_s and g_n are rational over a purely inseparable extension of k.

3. **Algebraic tori [1, 3, 4]**. An algebraic group G is an *algebraic torus* if G is isomorphic to a product of d copies of $\boldsymbol{GL}_1$ (where $d = \dim G$).

If $\Omega = \boldsymbol{C}$, an algebraic torus is isomorphic to $(\boldsymbol{C}^*)^d$, and so is not an ordinary torus. However, the algebraic tori have many properties analogous to those of usual tori in compact real Lie groups. Since in what follows the tori in the topological sense will occur rarely, the adjective "algebraic" will be dropped.

3.1. THEOREM. *For a connected algebraic group G the following conditions are equivalent*:

(1) *G is a torus*;

(2) *G consists only of semisimple elements*;

(3) *G, considered as matrix group, can be made diagonal.*

Property (3) means that there always exists a basis of Ω^n such that G is represented by diagonal matrices with respect to that basis. Each diagonal element of the matrix, considered as a function on G, is then a character.

Let T be a torus of dimension d. Every element $x \in T$ can be represented by $(x_1, \cdots, x_d)$, with $x_i \in \Omega^*$. A character χ of T can then be written

$$\chi(x) = x_1^{n_1} x_2^{n_2} \cdots x_d^{n_d}$$

with $n_i \in \boldsymbol{Z}$ hence $\hat{T} \cong \boldsymbol{Z}^d$.

3.2. THEOREM. *Let T be a torus defined over k. The following conditions are equivalent*:

(1) *All characters of T are defined over k: $\hat{T} = \hat{T}_k$.*

(2) *T has a diagonal realization over k.*

(3) *For every representation $\rho : T \to \boldsymbol{GL}_m$, defined over k, the group $\rho(T)$ is diagonalizable over k.*

DEFINITION. If T satisfies these three equivalent conditions, T is called a *split k-torus*, and is said to *split over k*.

If T splits over k, so does every subtorus and quotient of T. There always exists a finite separable Galois-extension k'/k such that T splits over k'. The Galois-group operates on $\hat{T}$. This action determines completely the k-structure of T. The subgroup $\hat{T}_k$ is the set of characters left fixed by the Galois group.

DEFINITION. A torus T is called *anisotropic over k* if $\hat{T}_k = \{1\}$. The anisotropic tori are very close to the usual compact tori. Let $k = \boldsymbol{R}$. If $\dim T = 1$, there are two possibilities; either T splits over k, and then $T_{\boldsymbol{R}} \cong \boldsymbol{R}^*$, or T is anisotropic over k; then T is isomorphic over k with $\boldsymbol{SO}_2$, and $T_{\boldsymbol{R}} = \boldsymbol{SO}(2, \boldsymbol{R})$ is the circle group. In the general case $T_{\boldsymbol{R}}$ is compact if and only if T is anisotropic over $\boldsymbol{R}$

(this is also true if $\boldsymbol{R}$ is replaced by a p-adic field). In this case, $T_{\boldsymbol{R}}$ is a topological torus (product of circle groups).

3.3. THEOREM. *Let T be a k-torus. There exist two uniquely defined k-subtori T_d and T_a, such that*

(1) T_d splits over k,

(2) T_a is anisotropic over k,

(3) $T_d \cap T_a$ is finite and $T = T_d \cdot T_a$.

This decomposition is compatible with morphisms of algebraic groups. (Property 3 will be abbreviated by saying that T is the *almost direct product of* T_d and T_a.)

If S is a k-subtorus of T, then there exists a k-subtorus S' such that T is almost direct product of S and S'.

EXAMPLE. If $k = \boldsymbol{R}$, $T = T_1 \cdot T_2 \cdot \cdots \cdot T_d$ where every T_i is one dimensional. The product is an almost direct product.

4. Solvable, nilpotent and unipotent groups.

4.1. DEFINITION. The algebraic group G is *unipotent* if every element of G is unipotent.

EXAMPLE. If $\dim G = 1$ and G is connected unipotent then G is isomorphic to the additive group of the field;

$$G \cong \boldsymbol{G}_a = \left\{ g \in \boldsymbol{GL}_2 | g = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \right\}.$$

A connected and unipotent matrix group is conjugate to a group of upper-triangular matrices with ones in the diagonal. Hence it is nilpotent; more precisely there exists a central series

$$G = G_0 \supset G_1 \supset \cdots \supset G_i \supset G_{i+1} \supset \cdots \supset G_n = \{e\}$$

such that $G_i/G_{i+1} \cong \boldsymbol{G}_a$. Conversely, if there exists a normal series ending with $\{e\}$ such that $G_i/G_{i+1} \cong \boldsymbol{G}_a$, where G_i is an algebraic subgroup of G, then G is unipotent.

In characteristic 0, a unipotent algebraic group is connected, and the exponential is a bijective polynomial mapping from the Lie algebra $\mathfrak{g}$ to G; the inverse map is the logarithm. In characteristic $p > 0$, this is no more true; in that case, G is a p-group.

DEFINITION. G is a *solvable* (resp. *nilpotent*) algebraic group, if it is solvable (resp. nilpotent) as an abstract group.

4.2. We now state some basic properties of a connected solvable group G.

(1) (Theorem of Lie–Kolchin): If G is represented as a matrix group, it is conjugate (over Ω) to a group of triangular matrices **[1]**.

(2) If G operates on a complete algebraic variety (in particular on a projective variety) then G has a fixed point **[1]**.

(3) The set of unipotent elements in G is a normal connected subgroup U. If G is defined over k, it has a maximal torus defined over k; G is the semidirect

product, as algebraic group, of T and U; any two maximal tori defined over k are conjugate by an element of G_k (Rosenlicht, Annali di Mat. (iv), **61** (1963), 97–120; see also [**3**, §11]).

(4) G has a compositicn series

$$G = G_0 \supset G_1 \supset \cdots \supset G_i \supset G_{i+1} \supset \cdots \supset G_n = \{e\}$$

where the G_i are algebraic subgroups of G such that G_i/G_{i+1} is isomorphic with $\mathbf{G}_a$ or $\mathbf{G}\,\mathbf{L}_1$.

(5) The group G is nilpotent if and only if it is the direct product of a maximal torus T and of a unipotent subgroup U. In this case T (resp. U) consists of all semisimple (resp. unipotent) elements of G.

Properties (1) and (2) are closely connected. In fact (2) implies (1): take the manifold of full flags (see §5.3) of the ambient vector space V, on which G acts in a natural way. Let F be a flag fixed by G; if one chooses a basis of V adapted to F, then G is triangular. On the other hand, for projective varieties, (2) follows immediately from (1). Property (4) is an immediate consequence of (1). In (3), one has to take care that, in contradistinction to the existence of a maximal torus defined over k, the normal subgroup U need not be defined over k, although it is k-closed [**8**].

4.3. Definition. Let G be a connected solvable group defined over k. G *splits over* k if there exists a composition series

$$G = G_0 \supset G_1 \supset \cdots \supset G_i \supset G_{i+1} \supset \cdots \supset G_m = \{e\}$$

consisting of connected k-subgroups of G such that G_i/G_{i+1} is isomorphic over k with $\mathbf{G}_a$ or $\mathbf{GL}_1$.

In particular, every torus T of G splits then over k. Conversely, when k is perfect, if the maximal tori of G which are defined over k split over k, then so does G.

Let G be a connected solvable k-group which splits over k, and V a k-variety on which G operates k-morphically. Then: (a) if V is complete and V_k is not empty, G has a fixed point in V_k [**8**]; (b) if G is transitive on V, the set V_k is not empty [**7**].

5. Radical. Parabolic subgroups. Reductive groups.

5.1. Definitions. Let G be an algebraic group. The *radical* $R(G)$ of G is the greatest connected normal subgroup of G; the *unipotent radical* $R_u(G)$ is the greatest connected unipotent normal subgroup of G. The group G is *semisimple* (resp. *reductive*) if $R(G) = \{e\}$ (resp. $R_u(G) = \{e\}$).

The definitions of $R(G)$ and $R_u(G)$ make sense, because if H, H' are connected normal and solvable (resp. unipotent) subgroups, then so is $H \cdot H'$. Both radicals are k-closed if G is a k-group. Clearly, $R(G) = R(G^0)$ and $R_u(G) = R_u(G^0)$.

The quotient $G/R(G)$ is semisimple, and $G/R_u(G)$ is reductive. In characteristic zero, the unipotent radical has a complement; more precisely: Let G be defined over k. There exists a maximal reductive k-subgroup H of G such that

$$G = H \cdot R_u(G),$$

the product being a semidirect product of algebraic groups. If H' is a reductive subgroup of G defined over k, then H' is conjugate over k to a subgroup of H. In characteristic $p > 0$, this theorem is false (not just for questions of inseparability): according to Chevalley, there does not always exist a complement to the unipotent radical, moreover there are easy counter-examples to the conjugacy property [3].

5.2. THEOREM. *Let G be an algebraic group. The following conditions are equivalent*:

(1) *G^0 is reductive,*

(2) *$G^0 = S \cdot G'$, where S is a central torus and G' is semisimple,*

(3) *G^0 has a locally faithful fully reducible rational representation,*

(4) *If moreover the characteristic of Ω is 0, all rational representations of G are fully reducible.*

If G is a k-group, and $k = \boldsymbol{R}$, these conditions are also equivalent to the existence of a matrix realization of G such that $G_{\boldsymbol{R}}$ is "self-adjoint"

$$(g \in G_{\boldsymbol{R}} \Rightarrow {}^t g \in G_{\boldsymbol{R}}).$$

In property (2) G' is the commutator subgroup $\mathscr{D}(G)$ of G; it contains every semisimple subgroup of G. The group G is separably isogenous to $S \times G'$ and every torus T of G is separably isogenous to $(T \cap S) \times (T \cap G')$.

5.3. THEOREM [1]. *Let G be a connected algebraic group.*

(1) *All maximal tori of G are conjugate. Every semisimple element is contained in a torus. The centralizer of any subtorus is connected.*

(2) *All maximal connected solvable subgroups are conjugate. Every element of G belongs to one such group.*

(3) *If P is a closed subgroup of G, then G/P is a projective variety if and only if P contains a maximal connected solvable subgroup.*

The *rank* of G is the common dimension of the maximal tori, (notation $rk(G)$).

A closed subgroup P of G is called parabolic, if G/P is a projective variety. Following a rather usual practice, the speaker will sometimes allow himself to abbreviate "maximal connected closed solvable subgroup" by "Borel subgroup."

EXAMPLE. $G = GL_n$. A *flag* in a vector space V is a properly increasing sequence of subspaces $0 \neq V_1 \subset \cdots \subset V_t \subset V_{t+1} = V$. The sequence (d_i)

$$(d_i = \dim V_i, i = 1, \cdots t))$$

describes the type of the flag. If $d_i = i$ and $t = \dim V - 1$, we speak of a *full flag*.

A parabolic subgroup of GL_n is the stability group of a flag F in Ω^n. G/P is the manifold of flags of the same type as F, and is well known to be a projective variety. A Borel subgroup is the stability group of a full flag. In a suitable basis, it is the group of all upper triangular matrices.

5.4. With respect to rationality questio̊n one can state that if G is a connected algebraic group defined over k, then

(1) G has a maximal torus defined over k (Grothendieck [**5**], see also [**2**]). The centralizer of any k-subtorus is defined over k ([**5**], [**3**, §10]).

(2) If k is infinite and G is reductive, G_k is Zariski dense in G (Grothendieck [**5**], see also [**2**]).

(3) If k is infinite and perfect, G_k is Zariski dense in G (Rosenlicht [**8**]).

Rosenlicht has constructed an example of a one dimensional unipotent group defined over a field k of characteristic 2 such that G is not isomorphic to G_a over k and G_k is not dense in G [**8**]. An analogous example exists for every positive characteristic (Cartier).

6. **Structure theorems for reductive groups.** The results stated below are proved in [**3**]. Over perfect fields, some of them are established in [**6**], [**9**].

6.1. *Root systems.* Let V be a finite dimensional real vector space endowed with a positive nondegenerate scalar product. A subset Φ of V is a root system when

(1) Φ consists of a finite number of nonzero vectors that generate V, and is symmetric ($\Phi = -\Phi$).

(2) for every $\alpha \in \Phi$, $s_\alpha(\Phi) = \Phi$, where s_α denotes reflection with respect to the hyperplane perpendicular to α.

(3) if α, $\beta \in \Phi$, then $2(\alpha, \beta)/(\alpha, \alpha) \in Z$. The group generated by the symmetrics $s_\alpha\,(\alpha \in \Phi)$ is called the Weyl group of Φ (notation $W(\Phi)$). It is finite. The integers $2(\alpha, \beta)/(\alpha, \alpha)$ are called the Cartan integers of Φ. Condition (3) means that for every α and β of Φ, $(s_\alpha(\beta) - \beta)$ is an integral multiple of α, since

$$s_\alpha(\beta) = \beta - 2\alpha(\alpha, \beta)/(\alpha, \alpha).$$

For the theory of reductive groups we shall have to enlarge slightly the notion of root system: if M is a subspace of V, we say that Φ is a root system in (N, M) if it generates a subspace P supplementary to M, and is a root system in P. The Weyl group $W(\Phi)$ is then understood to act trivially on M.

A root system Φ in V is the direct sum of $\Phi' \subset V'$ and $\Phi'' \subset V''$, if $V = V' \oplus V''$ and $\Phi = \Phi' \cup \Phi''$. The root system is called *irreducible* if it is not the direct sum of two subsystems.

6.2. *Properties of root systems.*

(1) Every root system is direct sum of irreducible root systems.

(2) If α and $\lambda\alpha \in \Phi$, then $\lambda = \pm 1, \pm\frac{1}{2}$, or ± 2.

The root system Φ is called *reduced* when for every $\alpha \in \Phi$, the only multiples of α belonging to Φ are $\pm\alpha$. To every root system Φ, there belongs two natural reduced systems by removing for every $\alpha \in \Phi$ the longer (or the shorter) multiple of α:

$$\Phi_s = \{\alpha \in \Phi | \tfrac{1}{2}\alpha \notin \Phi\},$$
$$\Phi_e = \{\alpha \in \Phi | 2\alpha \notin \Phi\}.$$

(3) The only reduced irreducible root systems are the usual ones:

$$\boldsymbol{A}_n \quad (n \geqq 1), \quad \boldsymbol{B}_n \quad (n \geqq 2), \quad \boldsymbol{C}_n \quad (n \geqq 3), \quad \boldsymbol{D}_n \quad (n \geqq 4),$$
$$\boldsymbol{G}_2, \quad \boldsymbol{F}_4, \quad \boldsymbol{E}_6, \quad \boldsymbol{E}_7, \quad \boldsymbol{E}_8.$$

(4) For each dimension n, there exists one irreducible nonreduced system, denoted by $\boldsymbol{BC}_n$ (see below).

EXAMPLES. $\boldsymbol{B}_n$: Take $\boldsymbol{R}^n$ with the standard metric and basis $\{x_1, \cdots, x_n\}$.

$$\boldsymbol{B}_n = \{\pm(x_i \pm x_j) \quad (i < j) \text{ and } \pm x_i \quad (1 \leqq i \leqq n)\}.$$

$W(\boldsymbol{B}_n) = \{s \in \boldsymbol{GL}(n, \boldsymbol{R}) | s$ a product of a permutation matrix with a symmetry with respect to a coordinate subspace$\}$

$$\boldsymbol{C}_n = \{\pm(x_i \pm x_j) \quad (i < j) \text{ and } \pm 2x_i \quad (1 \leqq i \leqq n)\},$$
$$W(\boldsymbol{C}_n) = W(\boldsymbol{B}_n),$$
$$\boldsymbol{BC}_n = \{\pm(x_i \pm x_j) \quad (i < j), \pm x_i \text{ and } \pm 2x_i \quad (1 \leqq i \leqq n)\},$$
$$W(\boldsymbol{BC}_n) = W(\boldsymbol{B}_n).$$

DEFINITION. A hyperplane of V is called *singular* if it is orthogonal to a root $\alpha \in \Phi$. A Weyl-chamber C^0 is a connected component of the complement of the union of the singular hyperplanes.

To a Weyl-chamber, is associated an ordering of the roots defined by:

$$\alpha > 0, \text{ if } (\alpha, v) > 0 \text{ for every } v \text{ in } C^0.$$

The root α is *simple* (relative to the given ordering) if it is not the sum of two positive roots. The set of simple roots is denoted by Δ. Δ is connected if it cannot be written as the union of $\Delta' \cup \Delta''$ where Δ' is orthogonal to Δ''.

(5) The Weyl group acts simply transitively on the Weyl-chambers (i.e., there is exactly one element of the Weyl group mapping a given Weyl-chamber on to another one).

(6) Every root of Φ is the sum of simple roots with integral coefficients of the same sign.

(7) The root system Φ is irreducible if and only if Δ is connected.

6.3. *Roots of a reductive group, with reference to a torus.* Let G be a reductive group, and S a torus of G. It operates on the Lie-algebra $\mathfrak{g}$ of G by the adjoint representation. Since S consists of semisimple elements, $\mathrm{Ad}_{\mathfrak{g}} S$ is diagonalizable

$$\mathfrak{g} = \mathfrak{g}_0^{(S)} \oplus \amalg_\alpha \mathfrak{g}_\alpha^{(S)}$$

where

$$\mathfrak{g}_\alpha^{(S)} = \{X \in \mathfrak{g} | \operatorname{Ad} s(x) = s^\alpha \cdot X\} \qquad (\alpha \in \hat{S};\ \alpha \neq 0).$$

The set $\Phi(G, S)$ of roots of G relative to the torus S is the set of nontrivial characters of S appearing in the above decomposition of the adjoint representation. If $T \supset S$, every root of G relative to T that is not trivial on S defines a root relative to S. If T is maximal $\Phi(G, T) = \Phi(G)$ is the set of roots of G in the usual sense.

6.4. *Anisotropic reductive groups.* A connected reductive group G defined over k is called *anisotropic* over k, if it has no k-split torus $S \neq \{e\}$.

EXAMPLES. (1) Let F be a nondegenerate quadratic form on a k-vector space V with coefficients in k. Let $G = O(F)$ be the orthogonal group of F. The group G is anisotropic over k if and only if F does not represent 0 over k, i.e., if V_k has no nonzero isotropic vector.

PROOF. Assume v is an isotropic vector. Then there exists a hyperbolic plane through v and in a suitable basis the quadratic form becomes

$$F(x_1, \cdots, x_n) = x_1 x_2 + F'(x_3, \cdots, x_n).$$

If $\lambda \in \Omega^*$, the set of transformations

$$x_1' = \lambda x_1, \qquad x_2' = \lambda^{-1} \cdot x_2, \qquad x_i' = x_i \qquad (i \geqq 3)$$

is a torus of G split over k. Conversely if there exists a torus S of G which splits over k, diagonalize S. There is a vector $v \in V_k - \{0\}$ and a nontrivial character $\chi \in \hat{S}$, such that $s(v) \equiv s^\chi v$. Since $s^\chi \neq \pm 1$ for some s, and $F(v) = F(s(v))$, one has $F(v) = 0$ and v is isotropic.

(2) If $k = \boldsymbol{R}$ or is a $\mathfrak{p}$-adic field, G is anisotropic over k if and only if G_k is compact. If k is an arbitrary field of characteristic 0, G is anisotropic over k if and only if G_k has no unipotent element $\neq e$ and $\hat{G}_k = \{1\}$.

6.5. *Properties of reductive k-groups.* Let G be a connected reductive group defined over k.

(1) The maximal k-split tori of G are conjugate over k (i.e., by elements of G_k). If S is such a maximal k-split torus, the dimension of S is called the k-rank of G (notation: $rk_k(G)$). $Z(S)$ is the connected component of $N(S)$. The finite group $N(S)/Z(S)$ is called the Weyl group of G relative to k (notation: ${}_kW(G)$). Every coset of $N(S)/Z(S)$ is represented by an element rational over k: $N(S) = N(S)_k Z(S)$.

(2) The elements of $\Phi(G, S)$, where S is a maximal k-split torus are called the k-roots, or roots relative to k. We write ${}_k\Phi$ or ${}_k\Phi(G)$ for $\Phi(G, S)$. This is a root system in $(\hat{S} \otimes \boldsymbol{R}, M)$ where M is the vector space over $\boldsymbol{R}$ generated by the characters which are trivial on $S \cap \mathscr{D}(G)$. The Weyl group of G relative to k and the Weyl group of ${}_k\Phi$ are isomorphic:

$$W({}_k\Phi) \cong {}_kW(G).$$

If G is simple over k, ${}_k\Phi$ is irreducible.

(3) The minimal parabolic k-subgroups P of G are conjugate over k. Furthermore there exists a k-split torus S such that

$$P = Z(S) \cdot R_u(P)$$

where the semidirect product is algebraic and everything is defined over k. If P and P' are minimal parabolic k-subgroups containing a maximal k-split torus S, then $P \cap P'$ contains the centralizer of S. The minimal parabolic k-subgroups containing $Z(S)$ are in $(1, 1)$ correspondence with the Weyl chambers: P corresponds to the Weyl chamber C if the Lie algebra of $R_u(P)$ is $\sum_{\alpha > 0} \mathfrak{g}_\alpha^{(S)}$, where the ordering of the roots is associated to the Weyl-chamber C. The Weyl group ${}_kW(G)$ permutes in a simply transitive way the minimal parabolic k-subgroups containing $Z(S)$. The unipotent radical of a minimal parabolic k-subgroup is a maximal unipotent k-subgroup, at least for a field of characteristic 0.

(4) Bruhat decomposition of G_k. Put $V = R_u(P)$, where P is a minimal parabolic k-subgroup. Then

$$G_k = U_k \cdot N(S)_k \cdot U_k,$$

and different elements of $N(S)_k$ define different double cosets; more generally if $n, n' \in N(S)$: $UnU = Un'U \Leftrightarrow n = n'$. Choose for every $w \in {}_kW$ a representative $n_w \in N(S)_k$; then the above equality can be written as

$$G_k = \bigcup_{w \in {}_kW} U_k \cdot n_w \cdot P_k,$$

the union being disjoint.

One can phrase this decomposition in a more precise way. If we fix $w \in {}_kW$, then there exist two k-subgroups U'_w and U''_w of U, such that $U = U'_w \times U''_w$ as an algebraic variety and such that the map of $U'_w \times P$ onto Un_wP sending (x, y) onto xn_wy is a biregular map defined over k. This decomposition gives rise to a cellular decomposition of G_k/P_k. Let π be the projection of G onto G/P. Then

$$(G/P)_k = G_k/P_k = \bigcup_{w \in {}_kW} \pi(U'_{w,k}).$$

If k is algebraically closed, $U'_{w''}$ as a unipotent group is isomorphic to an affine space. So one gets a cellular decomposition of G/P.

(5) *Standard parabolic k-subgroups* (with respect to a choice of S and P). Let ${}_k\Phi$ be the root system of G relative to k defined by the torus S. The choice of the minimal parabolic k-subgroup P determines a Weyl chamber of ${}_k\Phi$ and so a set of positive roots. Let ${}_k\Delta$ be the set of simple k-roots for this ordering. If Θ is a subset of ${}_k\Delta$, denote by S_Θ the identity component of $\bigcap_{\alpha \in \Theta} \ker \alpha$. S_Θ is a k-split torus, the dimension of which is $\dim S_\Theta = rk_k(G) - \operatorname{card} \Theta$. The standard parabolic k-subgroup defined by Θ is then the subgroup ${}_kP_\Theta$ generated by $Z(S_\Theta)$ and U. That subgroup can be written as the semidirect product $Z(S_\Theta)$. U_Θ, where $U_\Theta = R_u(P_\Theta)$. The Lie algebra of U_Θ is $\sum \mathfrak{g}_\alpha$, the sum going over all positive roots that are not linear combination of elements in Θ.

(6) Every parabolic k-subgroup is conjugate over k to one and only one standard parabolic k-subgroup. In particular, if two parabolic k-subgroups are conjugate over Ω, they are already conjugate over k.

(7) Let W_Θ be the subgroup of the Weyl group ${}_kW$ generated by the reflections s_α for $\alpha \in \Theta$. Then if Θ and Θ' are two subsets of ${}_k\Delta$,

$${}_kP_{\Theta,k}\backslash G_k/{}_kP_{\Theta',k} \cong W_\Theta\backslash{}_kW/W_{\Theta'}.$$

6.6. EXAMPLES. (1) $G = GL(n)$,

$$S = \text{group of diagonal matrices} = \left\{\begin{pmatrix} s^{\lambda_1} & & 0 \\ & s^{\lambda_2} \ddots & \\ 0 & & s^{\lambda_n} \end{pmatrix}\right\}$$

where $\lambda_i \in \hat{S}$ is such that $s^{\lambda_i} = s_{ii}$. S is obviously a split torus and is maximal. A minimal parabolic k-subgroup P is given by the upper triangular matrices, which is in this case a Borel subgroup. The unipotent radical U of P is given by the group of upper triangular matrices with ones in the diagonal. If e_{ij} is the matrix having all components zero except that with index (i, j) equal to 1, $\mathrm{Ad}_G\, s(e_{ij}) = (s^{\lambda_i}/s^{\lambda_j})e_{ij}$. So the positive roots are $\lambda_i - \lambda_j$ $(i < j)$ since the Lie algebra of U is generated by e_{ij} $(i < j)$. The simple roots are $(\lambda_1 - \lambda_2, \lambda_2 - \lambda_3, \cdots, \lambda_{n-1} - \lambda_n)$. The Weyl group is generated by s_α, where α is a positive root; since for $\alpha = \lambda_i - \lambda_j$, s_α permutes the i and j axis, ${}_kW \cong \mathfrak{S}_n$, the group of permutations of the basis elements. The parabolic subgroups are the stability groups of flags.

(2) G "splits over k" (i.e., G has a maximal torus which splits over k). Example (1) enters in this category. The k-roots are just the usual roots. A minimal parabolic k-subgroup is a maximal connected solvable subgroup. If k is algebraically closed G always splits over k and this gives just the usual properties of semisimple or reductive linear groups.

(3) G is the orthogonal group $SO(F)$ of a nondegenerate quadratic form F on a vector space V_k (where, to be safe, one takes char $k \neq 2$). In a suitable basis

$$F(x_1, \cdots, x_n) = x_1x_n + x_2x_{n-1} + \cdots + x_qx_{n-q+1} + F_0(x_{q+1}, \cdots, x_{n-q})$$

where F_0 does not represent zero rationally. The index of F, the dimension of the maximal isotropic subspaces in V_k, is equal to q. A maximal k-split torus S is given by the set of following diagonal matrices:

$$\begin{pmatrix} s^{\lambda_1} & & & & & & & & \\ & s^{\lambda_2} & & & & & & & \\ & & \ddots & & & & & & \\ & & & s^{\lambda_q} & & & & & \\ & & & & 1 \cdot & & & & \\ & & & & & \cdot 1 & & & \\ & & & & & & s^{-\lambda_q} & & \\ & 0 & & & & & & s^{-\lambda_{q-1}} & \\ & & & & & & & & \ddots \; s^{-\lambda_1} \end{pmatrix}$$

Let $SO(F_0)$ denote the proper orthogonal group of the quadratic form F_0, imbedded in $SO(F)$ by acting trivially on $x_1, \cdots, x_q$, $x_{n-q+1}, \ldots, x_n$. Then $Z(S) = S \times SO(F_0)$. The minimal parabolic k-subgroups are the stability groups of the full isotropic flags. For the above choice of S, and ordering of the coordinates, the standard full isotropic flag is

$$[e_1] \subset [e_1, e_2] \subset \cdots \subset [e_1, \cdots, e_q].$$

The corresponding minimal parabolic k-subgroup takes then the form

$$P = \left\{\begin{pmatrix} A_0 & A_1 & A_2 \\ 0 & B & A_3 \\ 0 & 0 & A_4 \end{pmatrix}\right\}$$

where A_0 and A_4 are upper triangular $q \times q$ matrices, $B \in SO(F_0)$, with additional relations that insure that $P \subset SO(F)$. The unipotent radical U of P is the set of matrices in P, where $B = I$, A_0, A_4 are unipotent, and

$$A_4 = {}^{\sigma}A_0^{-1}; \qquad Q \cdot A_3 + {}^{t}A_1 \cdot J \cdot A_4 = 0,$$
$${}^{t}A_4 \cdot J \cdot A_2 + {}^{t}A_3 \cdot Q \cdot A_3 + {}^{t}A_2 \cdot J \cdot A_4 = 0,$$

where Q is the matrix of the quadratic form F_0, J is the $q \times q$ matrix with one's in the nonprincipal diagonal and zeros elsewhere, and σ is the transposition with respect to the same diagonal, (${}^{\sigma}M = J{}^{t}MJ$). To determine the positive roots, one has to let S operate on U. To compute the root spaces it is easier to diagonalize Q: $q_{ij} = d_i \cdot \delta_{ij}$. Three cases are to be considered.

$i < j \leqq q$; $\lambda_i - \lambda_j$ is a root; the corresponding root space is generated by $e_{ij} - e_{n-j+1,n-i+1}$; the multiplicity of the root is 1.

$i \leqq q < j \leqq n - q$; λ_i is a root with multiplicity $n - 2q$; the corresponding root space is generated by

$$e_{ij} - d_j^{-1} e_{j,n-i+1} \qquad (q + 1 \leqq j < n - q).$$

$i < j \leqq q$; $\lambda_i + \lambda_j$ is a root with multiplicity one; the corresponding root space is generated by $e_{i,n-j+1} - e_{j,n-i+1}$. The simple roots are

$$\lambda_1 - \lambda_2, \lambda_2 - \lambda_3, \cdots, \lambda_{q-1} - \lambda_q,$$

and λ_q if $n \neq 2q$, $\lambda_{q-1} + \lambda_q$ if $n = 2q$. The Weyl group consists of all products of permutation matrices with symmetries with respect to a coordinate subspace (of any dimension if $n \neq 2q$ of even dimension if $n = 2q$). The group $SO(F)$ splits if and only if $q = [n/2]$. If it does not split, there exist roots with multiplicity >1. The parabolic k-subgroups are the stability subgroups of rational isotropic flags. The parabolic k-subgroups are conjugate over k if and only if there exists an element of G_k mapping one flag onto the other; by Witt's theorem this is possible if and only if the two flags have the same type.

(4) When one starts with a hermitian form, the same considerations apply, except that one gets a root system of type BC_q.

(5) For real Lie groups, this theory is closely connected with the Iwasawa and Cartan decompositions. If $\mathfrak{g}$ is the real Lie algebra of $G_{\boldsymbol{R}}$, G being a connected algebraic reductive group, then $\mathfrak{g} = \mathfrak{k} + \mathfrak{p}$, where $\mathfrak{g}$ is the Lie algebra of a maximal compact subgroup of $G_{\boldsymbol{R}}$. Then $G = K \cdot (\exp \mathfrak{y})$. Let $\mathfrak{a}$ be a maximal commutative subalgebra of $\mathfrak{y}$. Then $A = \exp \mathfrak{a}$ is the topological connected component of the groups of real points in a torus S which is maximal among $\boldsymbol{R}$-split tori. (On the Riemannian symmetric space $G_{\boldsymbol{R}}/K$, it represents a maximal totally geodesic flat subspace.)

$$N(A)_{\boldsymbol{R}} = N(S)_{\boldsymbol{R}} = [K \cap N(A)] \cdot A,$$

and

$$Z(S)_{\boldsymbol{R}} = (K \cap Z(A)) \cdot A;$$

the group $K \cap Z(A)$ is usually denoted by M. The Weyl group ${}_{\boldsymbol{R}}W(G, S)$ is isomorphic to $(K \cap N(A))/M$, i.e., to the Weyl group of the symmetric space G/K as introduced by E. Cartan. Similarly ${}_{\boldsymbol{R}}\Phi$ may be identified to the set of roots of the symmetric pair (G, K). Let $\mathfrak{n}$ be the Lie subalgebra generated by the root spaces corresponding to positive roots $\mathfrak{n} = \sum_{\alpha > 0} \mathfrak{y}_\alpha^{(S)}$, $\alpha \in {}_{\boldsymbol{R}}\Phi(G, S)$, for some ordering. Let $N = \exp \mathfrak{n}$. Then $G = K \cdot A \cdot N$ is an Iwasawa decomposition and $M \cdot A \cdot N$ is the group of real points of a minimal parabolic $\boldsymbol{R}$-group. Assume $G_{\boldsymbol{R}}$ simple and G/K to be a bounded symmetric domain. Then there are two possibilities for the root system ${}_{\boldsymbol{R}}\Phi$:

$$G_{\boldsymbol{R}}/K \text{ is a tube domain} \Leftrightarrow {}_{\boldsymbol{R}}\Phi \text{ is of type } C_t,$$

$$G_{\boldsymbol{R}}/K \text{ is not a tube domain} \Leftrightarrow {}_{\boldsymbol{R}}\Phi \text{ is of type} BC_t.$$

7. **Representations in characteristic zero** [3]. We assume here the ground field to be of characteristic zero, and G to be semisimple, connected. Let $P = Z(S) \cdot U$ be a minimal parabolic k-group, where $U = R_u(P)$, and S is a maximal k-split torus. We put on $X(S)$ an ordering such that u is the sum of the positive k-root spaces.

Assume first k to be algebraically closed. Let $\rho: G \to \mathrm{GL}(V)$ be an irreducible representation. It is well known that there is one and only one line $D_\rho \subset V$ which is stable under P. The character defined by the 1-dimensional representation of P in V is the highest weight λ_ρ of ρ. The orbit $G(D_\rho) = \mathscr{C}_\rho$ is a closed homogeneous cone (minus the origin). The stability group of D_ρ is a standard parabolic group $P_\rho \supset P$. The stability groups of the lines in $\mathscr{C}_\rho$ are conjugate to P_ρ, and these lines are the only ones to be stable under some parabolic subgroup of G. Every highest weight λ_ρ is a sum $\lambda_\rho = \sum_{\alpha \in \Delta} c_\alpha \cdot \Lambda_\alpha (c_\alpha \geqq 0, c_\alpha \in Z)$ of the fundamental highest weights Λ_α (and conversely if G is simply connected), where Λ_α is defined by $2(\Lambda_\alpha, \beta) \cdot (\beta, \beta)^{-1} = \delta_{\alpha\beta} (\alpha, \beta \in \Delta)$.

We want to indicate here a "relativization" of these facts for a nonnecessarily algebraically closed k.

Let T be a maximal torus of G, defined over k, containing S. We choose an ordering on $X(T)$ compatible with the given one on $X(S)$ (i.e., if $\alpha > 0$, and $r(\alpha) \neq 0$, then $r(\alpha) > 0$ where $r: X(T) \to X(S)$ is the restriction homomorphism. The k-weights of ρ are the restrictions to S of the weights of ρ with respect to T; the highest k-weight μ_ρ is the restriction of λ_ρ. It follows from standard facts that every k-weight μ is of the form

$$\mu = \mu_\rho - \sum m_\alpha(\mu)_\alpha, \qquad (\alpha \in \Delta),$$

with

$$m_\alpha(\mu) \in \boldsymbol{Z}, \qquad m_\alpha(\mu) \geqq 0.$$

Let

$$\Theta(\mu) = \{\alpha \in {}_k\Delta | m_\alpha(\mu) \neq 0\}.$$

Then $\Theta \subset {}_k\Delta$ is a $\Theta(\mu)$, for some k-weight μ, if and only if $\Theta(\mu) \cup \mu_\rho$ is connected.

Let us say that ρ is *strongly rational* over k if it is defined over k and if the cone $G(D_\rho)$ has a rational point over k. This is the case if and only if the above coefficients $\subset_\alpha$ satisfy the following conditions:

$$\subset_\alpha = 0 \text{ if } r(\alpha) = 0, \qquad \subset_\alpha = \subset_\beta \text{ if } r(\alpha) = r(\beta) \qquad (\alpha, \beta \in \Delta).$$

The highest weight of a strongly rational representation is a sum, with positive integral coefficients, of fundamental highest weights $M_\beta(\beta \in {}_k\Delta)$ where

$$M_\beta = \sum_{\alpha \in \Delta, r(\alpha) = \beta} r(\Lambda_\alpha)$$

(and conversely if G is simply connected). The $M_\beta(\beta \in {}_k\Delta)$ satisfy relations of the form $(M_\beta, \gamma) = d_\beta \cdot \delta_{\beta,\gamma}$, with $d_\beta > 0$. They will be called the *fundamental highest k-weights.*

Assume $k \subset \boldsymbol{C}$. Let ρ be strongly rational over k. Put on the representation space a Hilbert structure. Let $v \in D_\rho - 0$. Then the function $\phi: G \to \boldsymbol{R}^+$ defined by

$$\phi(g) = \|\rho(g) \cdot v\|,$$

satisfies

$$\phi(g \cdot p) = \phi(g)|p^{\mu_\rho}| \qquad (g \in G, \quad p \in P_\rho).$$

If in particular $k = \boldsymbol{Q}$, such functions appear in the discussion of fundamental sets and of Eisenstein series for arithmetic groups.

References

1. A. Borel, *Groupes linéaires algébriques*, Ann. of Math. (2) **64** (1956), 20–80.
2. A. Borel and T. A. Springer, *Rationality properties of linear algebraic groups*, Proc. Sympos. Pure Math., vol. 9, Amer. Math. Soc., Providence, R.I., 1966, pp. 26–32.
3. A. Borel and J. Tits, *Groupes réductifs*, Publ. I.H.E.S. **27** (1965), 55–150..

4. C. Chevalley, *Séminaire sur la classification des groupes de Lie algébriques*, 2 vols., Inst. H. Poincaré, Paris, 1958. (Mimeographed notes)

5. M. Demazure and A. Grothendieck, *Schémas en groupes*, I.H.E.S. Bures-sur-Yvette, France, 1964. (Mimeographed notes)

6. R. Godement, *Groupes linéaires algébriques sur un corps parfait*, Sém. Bourbaki, Exposé 206, Paris, 1960.

7. M. Rosenlicht, *Some basic theorems on algebraic groups*, Amer. J. Math. **78** (1956), 401–443.

8. ———, *Some rationality questions on algebraic groups*, Annali di Mat. (IV) **43** (1957), 25–50.

9. I. Satake, *On the theory of reductive groups over a perfect field*, J. Math. Soc. Japan **15** (1963), 210–235.

(From Notes by F. Bingen)

Reduction Theory for Arithmetic Groups

BY

ARMAND BOREL

This lecture is devoted to the statement of results concerning fundamental sets for arithmetic groups. The notation of [3] is used.

1.1. **Arithmetic groups.** We recall that two subgroups A, B of a group C are commensurable if $A \cap B$ has finite index in A and in B.

DEFINITION. Let G be an algebraic $\boldsymbol{Q}$-group. A subgroup Γ of $G_{\boldsymbol{Q}}$ is called an *arithmetic group* (or an arithmetic subgroup of G) if there exists a faithful rational representation $\rho: G \to \boldsymbol{GL}_n$ defined over $\boldsymbol{Q}$ such that $\rho(\Gamma)$ is commensurable with $\rho(G) \cap \boldsymbol{GL}(n, \boldsymbol{Z})$. (The same condition is then automatically fulfilled for every faithful $\boldsymbol{Q}$-representation of G.)

The arithmetic group Γ is a discrete subgroup of $G_{\boldsymbol{R}}$. It will act on $G_{\boldsymbol{R}}$ by right translations. If $X = K\backslash G_{\boldsymbol{R}}$, where K is a maximal compact subgroup of $G_{\boldsymbol{R}}$, then Γ operates also on X as a properly discontinuous group of translations.

One could apparently generalize the definition of arithmetic groups by starting from a number field k, an algebraic group G defined over k, a faithful k-representation $\rho: G \to \boldsymbol{GL}_n$ and taking as arithmetic group a subgroup of G_k commensurable with $G_{\mathfrak{o}_k} = \boldsymbol{GL}_n(n, \mathfrak{o}_k) \cap \rho(G)$, where $\mathfrak{o}_k$ is the ring of integers of k. But this class of arithmetic groups is the same as the one which was first defined. Indeed if $G' = R_{k/\boldsymbol{Q}}G$ is obtained from G by restriction of the ground field from k to $\boldsymbol{Q}$ (see [8]), using a basis of $\mathfrak{o}_k$ over $\boldsymbol{Z}$, it is easy to see that $G'_{\boldsymbol{Z}} \cong G_{\mathfrak{o}_k}$. On the other hand Γ will usually not be discrete in $G_{\boldsymbol{C}}$.

1.2. THEOREM. *Let $\rho: G \to G'$ be a surjective $\boldsymbol{Q}$-morphism of algebraic groups. If Γ is an arithmetic subgroup of G, then $\rho(\Gamma)$ is an arithmetic subgroup of G'.*

This is proved for isogenies in [4, §6], for general $\boldsymbol{Q}$-morphisms in [2]. Two simple consequences are:

(1) Let $G = H \cdot N$ be a semidirect product defined over $\boldsymbol{Q}$. Then $\Gamma_1 \cdot \Gamma_2$ is an arithmetic subgroup of G if Γ_1 is arithmetic in H and Γ_2 in N.

(2) Let G be the almost direct product of two normal $\boldsymbol{Q}$-subgroups G_1 and G_2 (i.e., G is $\boldsymbol{Q}$-isogeneous to $G_1 \times G_2$). If Γ is an arithmetic subgroup of G, then $\Gamma_i = \Gamma \cap G_i$ is arithmetic in G_i and $\Gamma_1 \cdot \Gamma_2$ is commensurable with Γ.

DEFINITION. Let Γ be an arithmetic group in G. The subgroup

$$C(\Gamma) = \{g \in G_{\boldsymbol{R}} | g \cdot \Gamma \cdot g^{-1} \text{ commensurable with } \Gamma\},$$

is called the *commensurability subgroup* of Γ. One has always that $G_{\boldsymbol{Q}} \subset C(\Gamma)$.

If $G_{\mathbf{R}}$ is compact, Γ is finite, every conjugate of Γ is commensurable to Γ, and so $C(\Gamma) = G_{\mathbf{R}}$.

1.3. THEOREM [2]. *Let N be the greatest normal $\mathbf{Q}$-subgroup of a semisimple algebraic $\mathbf{Q}$-group G, such that $N_{\mathbf{R}}$ is compact. If π is the projection of G onto $G' = G/N$, then $C(\Gamma) = \pi^{-1}(G'_{\mathbf{Q}}) \cap G_{\mathbf{R}}$.*

For instance, if G is $\mathbf{Q}$-simple, with center reduced to $\{e\}$, then $C(\Gamma) = G_{\mathbf{Q}}$. However, if $G_{\mathbf{C}}$ has a nontrivial center, this need not be so, as is already seen in the case where

$$G = SL_n, \qquad \Gamma = SL_{n,\mathbf{Z}}.$$

1.4. **Fundamental sets for arithmetic groups.** Let G be an algebraic $\mathbf{Q}$-group and Γ an arithmetic subgroup of G.

DEFINITION. A subset Ω of $G_{\mathbf{R}}$ is called a *fundamental set* for Γ if:

(F0) $K\Omega = \Omega$, where K is some maximal compact subgroup of $G_{\mathbf{R}}$;

(F1) $\Omega \cdot \Gamma = G_{\mathbf{R}}$;

(F2) for any g in $C(\Gamma)$, the set of translates $\Omega\gamma$, $\gamma \in \Gamma$, that meet $\Omega \cdot g$ is finite.

One could replace (F2) by the weaker condition:

(F2′) $\{\gamma \in \Gamma | \Omega \cap \Omega \cdot \gamma \neq \emptyset\}$ is finite.

But the stronger condition ensures that when one has a fundamental set Ω for Γ one can construct a fundamental set Ω' for a commensurable subgroup Γ' by taking $\Omega' = \bigcup_{\xi \in \Gamma'/\Gamma \cap \Gamma'} \Omega\xi$. The condition (F2) then goes over to Γ'. This would apparently not be the case with the weaker condition (F2′).

Due to condition (F0), the projection $\Omega' = \pi(\Omega)$ of a fundamental set Ω in $G_{\mathbf{R}}$ into $X = K\backslash G_{\mathbf{R}}$ satisfies the conditions

$$(\mathrm{F1})_X \qquad \Omega' \cdot \Gamma = X,$$

and (F2). A subset of X verifying $(\mathrm{F1})_X$ and (F2) will be called a fundamental set for Γ in X. Thus Ω is a fundamental set for Γ in $G_{\mathbf{R}}$ if and only $\Omega' = \pi(\Omega)$ is one in X, and then $\Omega = \pi^{-1}(\Omega')$.

If G is unipotent, then $G_{\mathbf{R}}/\Gamma$ is compact. Since G is the semidirect product $G = H \cdot R_u(G)$ of a reductive $\mathbf{Q}$-group and of its unipotent radical, it follows from (1.2) that the discussion of fundamental sets is easily reduced to the case of reductive groups, or of semisimple groups and tori.

When $G_{\mathbf{R}}/\Gamma$ is compact, there is often no need to have more information about the shape of a fundamental set. The purpose of the reduction theory outlined here is (a) to give a criterion for compactness, (b) in the noncompact case, to describe fundamental sets in which the complement of big compact subsets is a union of subsets which have properties similar to those of the cusps of fundamental domains for fuchsian groups.

1.5. THEOREM [4, 7]. *Let G be a $\mathbf{Q}$-group. $G_{\mathbf{R}}/\Gamma$ is compact if and only if $\hat{G}^0_{\mathbf{Q}} = 0$ and every unipotent element of $G_{\mathbf{Q}}$ belongs to $R_u(G)$.*

Let in particular G be reductive. Then $G_{\boldsymbol{R}}/\Gamma$ is compact if and only if G is anisotropic over $\boldsymbol{Q}$.

EXAMPLES. (1) SO(F) where F is an anisotropic quadratic form with rational coefficients.

(2) Let G' be the multiplicative group of a finite extension field k of $\boldsymbol{Q}$. $G = R_{k/\boldsymbol{Q}}G'$ is an algebraic group defined over $\boldsymbol{Q}$. It contains a $\boldsymbol{Q}$-subgroup N consisting of all elements of k of norm 1. The group N is anisotropic and so N/Γ, where Γ is an arithmetic subgroup of N, is compact. This is equivalent with the main part of Dirichlet's unit theorem.

1.6. **Siegel domains.** Siegel domains are defined in the cases where $G_{\boldsymbol{R}}/\Gamma$ is not compact. The reductive group G contains then a nontrivial maximal $\boldsymbol{Q}$-split torus S. Let P be a minimal parabolic subgroup containing S. The group P is different from G and $P = Z(S)\cdot U = M\cdot S\cdot U$, where U is the unipotent radical of P, $M \cap S$ is finite, M is reductive and anisotropic over $\boldsymbol{Q}$ (in particular every $\boldsymbol{Q}$-character of P or $Z(S)$ is trivial on M). Denote by ${}_{\boldsymbol{Q}}\Phi$ the sets of roots of G with respect to S. The choice of P orders this set; let ${}_{\boldsymbol{Q}}\Delta$ be the set of simple roots of ${}_{\boldsymbol{Q}}\Phi$ with respect to this ordering. For every $t \in \boldsymbol{R}^+$, define in $A = S_{\boldsymbol{R}}^0$ the subset

$$A_t = \{a \in A \mid a^\alpha \leqq t \text{ for every } \alpha \in {}_{\boldsymbol{Q}}\Delta\}.$$

Since every positive root is a positive linear combination of simple roots, there exists a $C > 0$ such that also $a^\alpha \leqq C$ for every positive root α in ${}_{\boldsymbol{Q}}\Phi$. A fundamental property of A_t is expressed by the following:

1.7. LEMMA. *If w is a compact set in $(M\cdot U)_{\boldsymbol{R}}$, then the set*

$$\{awa^{-1} \mid a \in A_t\}$$

is relatively compact.

PROOF. w is contained in a product $w_1 \cdot w_2$ where w_1 is compact in M and w_2 is compact in U. Since M centralizes S, $awa^{-1} \subset w_1 a w_2 a^{-1}$ and it is enough to prove the lemma for w compact in U. Since U is unipotent over a field of characteristic zero, the logarithm is a bijection of U onto its Lie algebra $\mathfrak{u}$. If $u \in U$, $\log u = \sum_{\alpha>0} c_\alpha \cdot X_\alpha$ and $\log(a\cdot u\cdot a^{-1}) = \sum_{\alpha>0} a^\alpha \cdot c_\alpha \cdot X_\alpha$. But a^α for $\alpha > 0$ stays bounded in A_t. So $\log(a\cdot u\cdot a^{-1})$ stays bounded as $a \in A_t$ and $u \in w$. The exponential being continuous, this proves the lemma.

1.8. **Siegel domains.** We keep the same notation as above. Let K be a maximal compact subgroup of $G_{\boldsymbol{R}}$ such that the Lie algebra of K is orthogonal to that of $S_{\boldsymbol{R}}$. Let w be a compact neighborhood of e in $(M\cdot U)_{\boldsymbol{R}} = M_{\boldsymbol{R}}\cdot U_{\boldsymbol{R}}$. The subset $\mathfrak{S} = K\cdot A_t\cdot w$ is called a Siegel domain for G. If $\pi: G \to X = K\backslash G_{\boldsymbol{R}}$, then $\pi(\mathfrak{S}) = \mathfrak{S}' = \sigma\cdot\mathfrak{S}$ (where o is the coset K) is called a Siegel domain in X. The set $(K\cap P)\cdot A_t\cdot w$ is a Siegel domain in $P_{\boldsymbol{R}}$. Since $G_{\boldsymbol{R}}$ is generated by K and $P_{\boldsymbol{R}}$, one has then $\mathfrak{S}' = o\cdot\mathfrak{S} = o\cdot A_t\cdot w$.

EXAMPLES. (1) $G = \boldsymbol{SL}(2, \boldsymbol{R})$, $\Gamma = \boldsymbol{SL}(2, \boldsymbol{Z})$, and $X = \boldsymbol{SO}(2, \boldsymbol{R})\backslash \boldsymbol{SL}(2, \boldsymbol{R})$ is the upper half plane. To be in agreement with the rest of this lecture, we let G act on X on the right by putting

$$z\cdot g = (a\cdot z + c)\cdot(b\cdot z + d)^{-1}, \qquad \left(g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \boldsymbol{SL}(2, \boldsymbol{R})\right).$$

Let

$$P = \left\{\begin{pmatrix} a & 0 \\ c & a^{-1} \end{pmatrix}\right\}, \qquad S = \left\{\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}\right\}, \qquad U = \left\{\begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}\right\}.$$

The positive root corresponding to this choice of U is $\alpha(a) = a^{-2}$. The fixed point of K is i. Let w be the set of elements in U for which $|c| \leqq C$. Then $\mathfrak{S}'$ is the rectangular domain:

$$\mathfrak{S}' = i\cdot A_t\cdot w = \{z \in X, |\operatorname{Re} z| \leqq C, \operatorname{Im} z \geqq t^{-1}\}.$$

It contains the classical fundamental domain $|z| \geqq 1$, $\operatorname{Re} z \leqq \frac{1}{2}$ if $C \geqq \frac{1}{2}$ and $t^2 \geqq \frac{4}{3}$.

(2) $G = \boldsymbol{GL}(n, \boldsymbol{R})$, $K = \boldsymbol{O}(n, \boldsymbol{R})$, S (resp. U, resp. P) group of diagonal (resp. unipotent upper triangular, resp. upper triangular) matrices. Then X is the space of positive nondegenerate quadratic forms in n variables. A_t is the set of diagonal matrices with positive entries a_i verifying $a_i/a_{i+1} \leqq t$. The natural projection of G onto $X = K\backslash G$ is the map $g \mapsto {}^t g\cdot g$. The image of the Siegel domain $K\cdot A_t\cdot w$ in X is then the set of matrices

$${}^t u\cdot a\cdot u \qquad (u \in w; a \in A_{t^2}).$$

It is well known to be a fundamental set if $t^2 \geqq \frac{4}{3}$, and if w contains all matrices $u = (u_{ij}) \in U$ such that $|u_{ij}| \leqq \frac{1}{2}$ $(i \neq j)$.

1.9. LEMMA. *A Siegel domain has finite Haar measure.*

PROOF. We have

$$G_{\boldsymbol{R}} = K\cdot P_{\boldsymbol{R}} = K\cdot A\cdot(M\cdot U)_{\boldsymbol{R}}.$$

The second decomposition is not unique but determined up to an element of the compact group $K \cap M$. By standard facts on Haar measures, we have:

$$\int_{\mathfrak{S}} dg = \int_{K\cdot A\cdot(M\cdot U)_{\boldsymbol{R}}} \phi\, dg$$

$$= c\cdot \int_K dk \cdot \int_{A_t\cdot w} a^{\chi}\, da\, dv$$

where ϕ is the characteristic function of $\mathfrak{S}$, dv is the Haar measure of $M\cdot U$ and $\chi = \det Ad_u a$. We have $\chi = \sum_{\alpha\in\Delta} c_\alpha \alpha$ and $c_\alpha > 0$. The only integral one has to evaluate to prove the finiteness is that extended over A_t; up to a constant factor, it is a product over $\alpha \in {}_{\boldsymbol{Q}}\Delta$ of integrals of the form

$$\int_{-\infty}^{t} \exp(c_\alpha x)\, dx,$$

which are finite since $c_\alpha > 0$.

1.10. THEOREM. *Let G be a connected semisimple algebraic group defined over $\boldsymbol{Q}$, and Γ an arithmetic subgroup of G.*

(1) *There exists a finite subset C of $G_{\boldsymbol{Q}}$ and a Siegel domain $\mathfrak{S}$ such that $\Omega = \mathfrak{S}C$ is a fundamental set in $G_{\boldsymbol{Q}}$ for Γ. The set C contains then at least one representative for every double coset $\Gamma\backslash G_{\boldsymbol{Q}}/P_{\boldsymbol{Q}}$. (In particular the number of such double cosets is finite.)*

(2) *Conversely if C is a finite subset of $G_{\boldsymbol{Q}}$ containing a representative for every double coset of $\Gamma\backslash G_{\boldsymbol{Q}}/P_{\boldsymbol{Q}}$, then there exists a Siegel domain $\mathfrak{S}$ such that $\Omega = \mathfrak{S}\cdot C$ is a fundamental set in $G_{\boldsymbol{R}}$ for Γ.*

It follows immediately from the lemma and the theorem that $G_{\boldsymbol{R}}/\Gamma$ has finite invariant volume.

1.11. THEOREM. *Let G be an algebraic group defined over $\boldsymbol{Q}$, Γ an arithmetic subgroup of $G_{\boldsymbol{Q}}$. Then $G_{\boldsymbol{R}}/\Gamma$ has finite volume if and only if $G^0_{\boldsymbol{Q}}$ has no characters defined over Q. ($\hat{G}^0_Q = \{0\}$.)*

Writing $G^0 = H\cdot Z\cdot U$, where U is the unipotent radical and Z the central torus of a maximal reductive subgroup, the condition states that Z is anisotropic over $\boldsymbol{Q}$.

Theorem 1.11 is proved in **[4]** and Theorem 1.10 is announced in **[1]**. For proofs which are different from those of **[1, 4]**, see **[6]**.

In Ω, the complement of a compact set is the union of sets of the form $KA_r\cdot w\cdot c$ ($c\in G_{\boldsymbol{Q}}$, $r > 0$, r sufficiently small). These are to be viewed as the analogues of the "cusps" for fuchsian groups. The minimum number of cusps is then the number of elements in $\Gamma\backslash G_{\boldsymbol{Q}}/P_{\boldsymbol{Q}}$ or, equivalently, the number of conjugacy classes of minimal parabolic $\boldsymbol{Q}$-subgroups under Γ.

EXAMPLES. If F is a quadratic form defined over $\boldsymbol{Q}$ and $G = \mathrm{SO}(F)$, $P_{\boldsymbol{Q}}$ is the stability group of a full isotropic flag. Then the minimal number of cusps for a fundamental set Ω is the number of transitivity classes of full isotropic flags under Γ. The same is true for $\boldsymbol{Sp}(n)$. Since $\boldsymbol{Sp}(n, \boldsymbol{Z})$ is transitive on the full isotropic flags, the minimum number of cusps for the modular group is 1, as is well known by Siegel's construction of a fundamental domain in this case. More generally, **[2**, Lemma 1**]**, we have $G_{\boldsymbol{Q}} = G_{\boldsymbol{Z}}\cdot P_{\boldsymbol{Q}}$ if G splits over $\boldsymbol{Q}$, and $G_{\boldsymbol{Z}}$ is the group of integral points for the canonical $\boldsymbol{Z}$-structure on G introduced by Chevalley, and described in **[5]**. In this case, there is only one cusp.

1.12. Minimum principles connected with fundamental domains.

EXAMPLE. 1. Let $X = \{Z\in \boldsymbol{M}(n, \boldsymbol{C})|{}^tZ = Z, \mathrm{Im}\, Z > 0\}$ be the Siegel upper half plane, $\mathfrak{S}$ a Siegel domain which is a fundamental domain for the modular group Γ. Consider for fixed $Z\in X$ the function $f(Z\gamma) = \det(\mathrm{Im}\, Z\cdot\gamma)^{-1}$ defined on Γ. It is well known that this function has a minimum on $Z\cdot\Gamma$ and that this minimum is taken in a point of $Z\cdot\Gamma\cap\mathfrak{S}$.

2. Let $G = GL(n)$, and $\mathfrak{S}$ a suitable big Siegel domain in $G_{\mathbf{R}}$. It is known from the Hermite or the Minkowski reduction theory that, if $\|x\|$ denotes the length of the vector $x \in \mathbf{R}^n$, then for every $g \in \mathbf{R}$, the function $f_g(\gamma) = \|g\gamma(e_1)\|$ from $GL(n, \mathbf{Z})$ to R^+ attains a minimum in $\mathfrak{S}$.

Such minimum principles hold for every semisimple algebraic group defined over $\mathbf{Q}$. Let P be a minimal parabolic $\mathbf{Q}$-subgroup of G; ${}_{\mathbf{Q}}\Delta$ the set of simple roots of G relative to this choice of a minimal parabolic subgroup. Take in $\hat{P}$ a set of fundamental weights Λ_α such that $(\Lambda_\alpha, \beta) = d_\alpha \delta_{\alpha\beta}$, $(\alpha, \beta \in {}_{\mathbf{Q}}\Delta)$, and $d_\alpha > 0$.

1.13. THEOREM. *Let $\chi \in \hat{P}$ with $\chi = \sum c_\alpha \Lambda_\alpha$ $(c_\alpha \geqq 0)$ and f a function from $G_{\mathbf{R}}$ to R^+ satisfying $f(x, p) = f(x)|p^\chi|$ $(p \in P_{\mathbf{R}})$. Take for C a set of representatives of the double cosets of $\Gamma \backslash G_{\mathbf{Q}}/P_{\mathbf{Q}}$. Then there exists a Siegel domain $\mathfrak{S}$ in $G_{\mathbf{R}}$ such that for any $x \in G_{\mathbf{R}}$ the function $f_x(c, \gamma) = f(x \cdot c \cdot \gamma)$ attains a minimum in $C \cdot \Gamma \cap x^{-1} \cdot \mathfrak{S}$; in other words, there exist $c_0 \in C$, $\gamma_0 \in \Gamma$ such that $xc_0\gamma_0 \in \mathfrak{S}$ and $f(xc_0\gamma_0) \leqq f(xc\gamma)$ $(c \in G', \gamma \in \Gamma)$.*

The Minkowski reduction theory in GL_n makes use of $n - 1$ successive minima. This approach was generalized to adèle groups of arbitrary semisimple groups in [6]. The number of successive minima is equal to $rk_{\mathbf{Q}}(G)$, and the functions which are minimized are associated to fundamental strongly $\mathbf{Q}$-rational representations, in the sense of [3, §7]. There is an analogue of this for $G_{\mathbf{R}}$ and Γ, which also generalizes §1.13, where, given an integer r in $(1 \leqq r \leqq rk_{\mathbf{Q}}G)$, one takes successive minima of r functions. The two cases just mentioned then correspond to $r = 1$, $r = rk_{\mathbf{Q}}G$. The formulation of this result is however more complicated than in the adèle case, because fundamental sets for Γ in $G_{\mathbf{R}}$ have in general more than one cusp. Details will be given in a future publication of the speaker.

REFERENCES

1. A. Borel, *Ensembles fondamentaux pour les groupes arithmétiques*, Coll. Théorie des groupes algébriques (Bruxelles 1962), pp. 23–40. Librairie Universitaire, Louvaine; Gauthier-Villars, Paris.

2. ———, *Density and maximality of arithmetic subgroups*, (to appear).

3. ———, *Linear algebraic groups*, Proc. Sympos. Pure Math., vol. 9, Amer. Math. Soc., Providence, R.I., 1966, pp. 3–19.

4. A. Borel and Harish-Chandra, *Arithmetic subgroups of algebraic groups*, Ann. of Math. (2) **75** (1962), 485–535.

5. P. Cartier, *Groups over Z*. Proc. Sympos. Pure Math., vol. 9, Amer. Math. Soc., Providence, R.I., 1966, pp. 90–98.

6. R. Godement, *Domaines fondamentaux des groupes arithmétiques*, Séminaire Bourbaki, vol. 15, (1962–1963), Exposé 257, Paris.

7. G. D. Mostow and T. Tamagawa, *On the compactness or arithmetically defined homogeneous spaces*, Ann. of Math. (2) **76** (1962), 446–463.

8. T. Tamagawa, *Adèles*, Proc. Sympos. Pure Math., vol. 9, Amer. Math. Soc., Providence, R.I., 1966, pp. 113–121.

(From Notes by F. Bingen)

Rationality Properties of Linear Algebraic Groups

BY

ARMAND BOREL AND T. A. SPRINGER

In this lecture, G is a connected linear algebraic group, $\mathfrak{g}$ its Lie algebra, k a field of definition for G and p the characteristic of k. Our purpose is to sketch, for infinite k, a proof of

THEOREM A. (i) *G contains a maximal torus and a Cartan subgroup defined over k.*

(ii) *Let G be reductive. Then G is unirational over k. In particular, if k is infinite, G_k is Zariski dense in G.*

(G unirational over k means that there exists a k-morphism of a k-open subset of an affine space into G, whose image contains a nonempty open subset of G.)

This theorem is due to Rosenlicht **[6]** over perfect fields, to Grothendieck **[5]** in the general case. In contrast with **[5]**, we shall give a proof which does not use schemes; however, it is in part based on similar ideas. We presuppose the theory of algebraic groups over an algebraically closed field **[1]**, **[4]**.

Notation. The Lie algebra of an algebraic group $H, M, \cdots$ is denoted by the corresponding German letter. Ad refers to the adjoint representation of G in $\mathfrak{g}$, and ad to the representation of $\mathfrak{g}$ into itself defined by ad $X(Y) = [X, Y]$. As is well known, ad is the differential of Ad. ${}^gA$ stands for $g \cdot A \cdot g^{-1}$ $(g \in G, A \subset G)$. For $X \in \mathfrak{g}$, we let $Z_G(X) = \{g \in G, \operatorname{Ad} g(X) = X\}$ and $z_G(X) = \{Y \in \mathfrak{g}, [Y, X] = 0\}$. Clearly, $Z_G(X)$ is a closed subgroup, whose Lie algebra is contained in $z_G(X)$. If no confusion can arise, we drop the subscript G.

Let $p \neq 0$. We denote by $[p]: X \to X^{[p]}$ the pth power operation in $\mathfrak{g}$. It is defined over k: if $\mathfrak{g} \subset \mathfrak{gg}_n$, then $X^{[p]} = X^p$. In particular, if $[X, Y] = 0$, then

$$(X + Y)^{[p]} = X^{[p]} + Y^{[p]}.$$

If $q = p^s$ is a power of p, we write $[q]$ for $[p]^s$. The pth power operation commutes with differentials of morphisms.

1. Jordan decomposition in $\mathfrak{g}$. The centralizer of a semisimple element.

1.1. DEFINITION. An element $X \in \mathfrak{g}$ is semisimple (resp. nilpotent) if it belongs to the Lie algebra of a sub-torus (resp. unipotent subgroup) of G.

1.2. LEMMA. *Let $G = T \cdot U$ be solvable, with one-dimensional unipotent radical U, where T is a maximal torus of G. Let $X \in \mathfrak{t}$. Then there are two possibilities:*

(1) $[X, \mathfrak{u}] = 0$, $Z(X) = G$.

(2) $[X, \mathfrak{u}] \neq 0$, $Z(X) = T$; *the map* $u \mapsto \operatorname{Ad} u(X) - X$ *is an isomorphism of U onto the additive algebraic group* Add($\mathfrak{u}$) *of* $\mathfrak{u}$. *Every element $X + Z$ ($Z \in \mathfrak{u}$) is semisimple.*

Let $\pi : G \to G' = G/U$ be the canonical projection. Then $d\pi$ maps $\mathfrak{t}$ isomorphically onto $\mathfrak{g}'$, and G' is commutative. Therefore, $\operatorname{Ad} g(X) - X \in \mathfrak{u}$ $(g \in G)$.

Assume $[X, \mathfrak{u}] = 0$, and identify G to a matrix group. If $Z(X) \neq G$, there exists $u \in U$ such that $\operatorname{Ad} u(X) = X + U$ $(U \in \mathfrak{u} - 0)$. But then $\operatorname{Ad} u(X)$ is on the one hand a semisimple matrix (being tangent to a torus), and on the other hand is the sum of a semisimple and a nonzero nilpotent matrix, commuting with each other, a contradiction.

Let now $[X, \mathfrak{u}] \neq 0$. Since ad is the differential of Ad, this implies that $Z(X) \neq G$. Since $Z(X) \supset T$, it follows, for dimensional reasons, that $Z(X)^0 = T$. However, in a connected solvable group, the centralizer and the normalizer of a torus are connected, and coincide [1]. Since $[\mathfrak{t}, \mathfrak{u}] \neq 0$, T is not central, hence $\operatorname{Norm}(T) = T$ and $Z(X) = T$. Let $Y \in \mathfrak{u} - 0$. Then $\operatorname{Ad} u(X) - X = c(u) \cdot Y$. Obviously c is a morphism of U into the additive group of $\mathfrak{u}$, injective since $Z(X) = T$, hence bijective. Thus every element $X + Z$ $(Z \in \mathfrak{u})$ is conjugate to X, hence is semisimple. The relation $[X, \mathfrak{u}] \neq 0$ implies that the differential of c is an isomorphism, therefore c is birational, biregular.

1.3. Proposition. *Every $X \in \mathfrak{g}$ can be written uniquely as $X = X_s + X_n$ with X_s semisimple, X_n nilpotent, $[X_s, X_n] = 0$. For any morphism $\pi : G \to \mathbf{GL}_n$, $d\pi(X) = d\pi(X_s) + d\pi(X_n)$ is the Jordan decomposition of $d\pi(X)$.*

Let $X = X_s + X_n$ be one decomposition of X with X_s semisimple, X_n nilpotent and $[X_s, X_n] = 0$. Then $d\pi(X_s)$ (resp. $d\pi(X_n)$) is tangent to a torus (resp. a unipotent group), hence is a semisimple (resp. nilpotent) matrix, whence the second assertion. Using a matrix realization of G, this implies the uniqueness of this decomposition. There remains to show its existence. We assume first G to be solvable, and proceed by induction on $\dim G$. Let $U = R_u(G)$ be the unipotent radical of G. There exists a connected one-dimensional subgroup N of the center of U which is normal in G. Let $\pi : G \to G' = G/N$ be the canonical projection. Let $X \in \mathfrak{g}$. By induction assumption,

$$d\pi(X) = A' + B' \qquad (A', B' \in \mathfrak{g}';\ A' \text{ semisimple, } B' \text{ nilpotent, } [A', B'] = 0).$$

Since $R_u(G') = \pi(R_u(G))$, and every torus of G' is the image of a torus of G, this yields

$$X = A + B \qquad (A \text{ semisimple, } B \text{ nilpotent, } d\pi(A) = A', d\pi(B) = B').$$

Let T be a maximal torus whose Lie algebra contains A. Since every rational representation of T is fully reducible, we may write $\mathfrak{u} = \mathfrak{r} \oplus \mathfrak{n}$, with $\mathfrak{r}$ stable under Ad T. Writing

$$B = B_1 + B_2 \qquad (B_1 \in \mathfrak{r}, B_2 \in \mathfrak{n}),$$

we have then

$$[A, B_1] = 0, \qquad [A, B_2] = C \in \mathfrak{n}, \qquad [B_1, B_2] = 0.$$

If $C = 0$, we are done, so assume $C \neq 0$. By Lemma 1.2, applied to $T \cdot N$, the sum $A + B_2$ is semisimple, hence the decomposition $X = X_s + X_n$ with $X_s = A + B_2, X_n = B_1$ has the required properties.

This proves Proposition 1.3 for solvable groups. The general case follows by using the following Lemma [5, XIV, Théorème 4.11]:

1.4. LEMMA. *Let B be a Borel subgroup of G. Then* $\mathfrak{g} = \bigcup_{g \in G} \operatorname{Ad} g(\mathfrak{b})$.

The proof is similar to that given in [3, VI] for the corresponding statement in G; it uses the two following facts, which follow from properties of reductive groups: B is the normalizer of $\mathfrak{b}$ in G, and there exists an element $X \in \mathfrak{b}$ which is not contained in any conjugate of $\mathfrak{b}$ distinct from $\mathfrak{b}$.

1.5. PROPOSITION. *Let $X \in \mathfrak{g}$ be semisimple. Then $z(X)$ is the Lie algebra of $Z(X)$.*

Since $z(X)$ contains the Lie algebra of $Z(X)$, it is enough to show that $\dim z(X) \leqq \dim Z(X)$.

(a) *G solvable.* We let $U, N, \pi: G \to G' = G/N$ be as in the previous proof, and let T be a maximal torus whose Lie algebra contains X. Let $X' = d\pi(X)$. The Lie algebra $\mathfrak{g}$ is the direct sum of $\mathfrak{n}$ and of a subspace $\mathfrak{r}$ stable under Ad T, whence immediately,

$$\dim z(X) = z(X) \cap \mathfrak{n} + \dim z(X').$$

By Lemma 1.2, $\dim z(X) \cap \mathfrak{n} = \dim Z(X) \cap N$; by induction $\dim Z_{G'}(X') = \dim z(X')$. It suffices therefore to show that $\pi(Z(X)) = Z_{G'}(X')$.

Let $g' \in Z_{G'}(X')$. There exists $g \in G$ such that $\pi(g) = g'$, hence such that $\operatorname{Ad} g(X) = X + Y\,(Y \in \mathfrak{n})$. There is something to prove only if $Y \neq 0$. Since $\operatorname{Ad} g(X)$ is semisimple, and Y is nilpotent, we must have $[X, Y] \neq 0$ by the uniqueness of the Jordan decomposition. By Lemma 1.2, there exists then $n \in N$ such that $\operatorname{Ad} n(X) = X - Y$. We have then $\operatorname{Ad} n \cdot g(X) = X$, and $\pi(n \cdot g) = g'$.

(b) *G not solvable.* Let T be a maximal torus whose Lie algebra contains X. It follows from known facts about reductive groups that G has two Borel subgroups B, B', normalized by T, which generate G, such that $\mathfrak{g} = \mathfrak{b} + \mathfrak{b}', \mathfrak{b} \cap \mathfrak{b}' = \mathfrak{t} + \mathfrak{u}$ ($\mathfrak{u}$ Lie algebra of $U = R_u(G)$) (see [3, §2]). Let $\mathfrak{c}, \mathfrak{c}'$ be supplementary subspaces of $\mathfrak{t} + \mathfrak{u}$ in $\mathfrak{b}$ and $\mathfrak{b}'$ respectively, stable under Ad T. The Lie algebra $z(X)$ is the direct sum of its intersections with $\mathfrak{c}, \mathfrak{c}'$ and $\mathfrak{t} + \mathfrak{u}$, say $\mathfrak{p}, \mathfrak{q}, \mathfrak{r}$. By (*a*) $\mathfrak{p} + \mathfrak{r}$ and $\mathfrak{q} + \mathfrak{r}$ belong to the Lie algebra of $Z(X)$, hence $\dim Z(X) \geqq \dim z(X)$.

REMARK. Using induction and the relation $\pi(Z(X)) = Z'_{G'}(X')$ proved above, one sees easily that $Z(X)$ is connected if G is solvable. Examples show that this need not be the case when G is semisimple.

1.6. PROPOSITION. *Let $X \in \mathfrak{g}$ be semisimple. Then* Ad $G(X)$ *is closed.*

Identify G with a matrix group. Let L be the set of $Y \in \mathfrak{g}$ which annihilate the minimal polynomial of X, and such that ad Y has the same characteristic polynomial as ad X. This is an algebraic subset of $\mathfrak{g}$, stable under Ad G. Let $Y \in L$. Its minimal polynomial divides that of X, hence has only simple factors, and Y is a semisimple matrix. By Proposition 1.3, it is a semisimple element of $\mathfrak{g}$, in the sense of Definition 1.1, consequently, (Proposition 1.5), $\dim Z(Y)$ is equal to the multiplicity of the eigenvalue zero of ad Y. By the definition of L, and Proposition 1.5, this implies $\dim Z(Y) = \dim Z(X)$. As a consequence, the orbits of G in L are all of the same dimension, hence are closed [**1**, §16].

1.7. COROLLARY. *Assume that every semisimple element of* $\mathfrak{g}$ *is central in* $\mathfrak{g}$. *Then the set of all semisimple elements of* $\mathfrak{g}$ *is a subspace* $\mathfrak{s}$ *defined over* k, *which is the Lie algebra of every maximal torus of* G.

Let T be a maximal torus of G. Then $\mathfrak{t} \subset \mathfrak{s}$. Let $X \in \mathfrak{g}$ be semisimple. By the conjugacy of maximal tori in G, there exists $g \in G$ such that $\mathrm{Ad}\, g(X) \subset \mathfrak{t}$. By assumption $[X, \mathfrak{g}] = 0$, hence (Proposition 1.5), $Z(X) = G$ and $\mathrm{Ad}\, g(X) = X$. Thus $\mathfrak{s} \subset \mathfrak{t}$. There remains to see that $\mathfrak{s}$ is defined over k, in other words, that it is generated over $\bar{k}$ by elements of $\mathfrak{g}_k$. This is obvious in char. 0 (or in fact over a perfect field, since in this case the Jordan decomposition is over the groundfield), so we assume $p \neq 0$. There exists a power q of p such that $X^{[q]} = 0$, whenever X is nilpotent. For arbitrary X we have $X^{[q]} = (X_s + X_n)^{[q]} = X_s^{[q]} + X_n^{[q]} = X_s^{[q]} \subset \mathfrak{t}$ (notation of §1.3). Thus $[q]: X \mapsto X^{[q]}$ maps $\mathfrak{g}$ into $\mathfrak{t}$. On the other hand, $\mathfrak{t}$ can be diagonalized, hence the restriction of $[q]$ to $\mathfrak{t}$ is bijective. Thus, $\mathrm{Im}[q] = \mathfrak{t}$. But $[q]$ is a morphism of $\mathfrak{g}$, viewed as an algebraic set, into itself, obviously defined over k. Therefore, $\mathrm{Im}[q]$ is also defined over k.

2. **Inseparable isogenies.**

The main tools which will allow us to get hold of fields of definition in char. $p \neq 0$ are the criterion of multiplicity one of intersection theory, and the following result of Barsotti and Serre ([**7**, Théorème 1], [**3**, §7]).

2.1. PROPOSITION. *Let* $\mathfrak{m}$ *be an ideal of* $\mathfrak{g}$ *which is stable under the* pth *power operation and under* Ad G. *Then there exists one and, up to k-isomorphism, only one k-group* G' *with the following properties*: (i) *there exists a purely inseparable k-isogeny* $\pi: G \to G'$ *such that* $\ker d\pi = \mathfrak{m}$; (ii) *every purely inseparable k-isogeny* $\theta: G \to G''$ *such that* $\ker d\theta \supset \mathfrak{m}$ *can be k-factored through* π.

We also write $G/\mathfrak{m}$ for G'. Note that, since π is purely inseparable, π is a bijective morphism of G onto G'.

2.2. PROPOSITION. *Let* G *be not nilpotent, and assume that every semisimple element of* $\mathfrak{g}$ *is central. Let* T *be a maximal torus of* G. *Then there exists a k-group* G', *such that not all semisimple elements of* $\mathfrak{g}'$ *are central, and a purely inseparable k-isogeny* $\pi: G \to G'$, *whose differential* $d\pi$ *had* $\mathfrak{t}$ *as kernel. The Lie algebra* $\mathfrak{g}'$ *is the direct sum of* $d\pi(\mathfrak{g})$ *and of the Lie algebra of any maximal torus.*

Let $\Phi = \Phi(G, T)$ be the set of roots of G with respect to T(nontrivial characters of T in $\mathfrak{g}$, under the adjoint representation). Since G is not nilpotent, T is not central, and Φ is not empty. (To see this, use the fact that G is generated by two solvable subgroups containing T, and the "lemme de dévissage" of [**4**], Exp. 9, Lemme 2.)

$\mathfrak{g}$ is the direct sum of the Lie algebra of $Z(T)$ and of the root spaces

$$\mathfrak{g}_a = \{X \in \mathfrak{g} | \operatorname{Ad} t(X) = t^a \cdot X, (t \in T)\} \qquad (a \in \Phi).$$

Let da be the differential of $a \colon T \to GL_1$. It is a linear form on $\mathfrak{t}$, and we have

$$[Y, X] = da(Y) \cdot X \qquad (Y \in \mathfrak{t}, X \in \mathfrak{g}_a).$$

It is easily seen that the differential of a character x of $T$is zero if and only if x is divisible by p, in the character group $X(T)$ of T. Let c be the smallest positive integer such that $\Phi \not\subset p^{c+1} \cdot X(T)$. The elements of $\mathfrak{t}$ are central in $\mathfrak{g}$ if and only if $c \geqq 1$. We prove Proposition 2.2 by induction on c.

By Corollary 1.7, $\mathfrak{t}$ is the set of all semisimple elements of $\mathfrak{g}$ and is defined over k. By Proposition 1.5, every $X \in \mathfrak{t}$ is centralized by G. Since $\mathfrak{t}$ is the Lie algebra of an algebraic group, it is stable under pth power operation therefore (Proposition 2.1), there exists a purely inseparable isogeny $\pi_1 \colon G \to G_1 = G/\mathfrak{t}$.

It follows from Proposition 1.3 that $d\pi_1(\mathfrak{g})$ consists of nilpotent elements; therefore if T' is a maximal torus of G, then $\mathfrak{t}' \cap d\pi_1(\mathfrak{g}) = 0$, hence, for dimensional reasons, $\mathfrak{g}' = \mathfrak{t}' \oplus d\pi_1(\mathfrak{g})$ (direct sum of vector spaces). This applies in particular to the Lie algebra $\mathfrak{t}_1$ of $T_1 = \pi(T)$, which implies readily that ${}^t\pi_1$ maps $\Phi(G_1, T_1)$ onto $\Phi(G, T)$. On the other hand, it follows from $d\pi(\mathfrak{t}) = 0$ that ${}^t\pi_1$ maps $X(T')$ into $p \cdot X(T)$. Thus, if d is the smallest positive integer such that

$$\Phi(G_1, T_1) \not\subset p^{d+1} \cdot X(T_1),$$

we have $d < c$. If $d = 0$, then $\mathfrak{t}'$ is not central, and we take $G' = G_1$. If $d \geqq 1$, we apply the induction assumption and get $\pi' \colon G_1 \to G'$, with $\ker d\pi' = \mathfrak{t}_1$, satisfying our conditions for G_1. Then $\pi = \pi' \circ \pi_1 \colon G \to G'$ has all the required properties.

3. **Proof of Theorem** A.

3.1. *Regular elements.* Let nil X be the multiplicity of the eigenvalue zero of ad X ($X \in \mathfrak{g}$), and let $n(\mathfrak{g}) = \min_{X \in \mathfrak{g}} \operatorname{nil}(X)$. An element X is *regular* if $\operatorname{nil}(X) = n(\mathfrak{g})$, *singular* otherwise. Clearly nil X = nil X_s (notation of §1.3), hence X is regular if and only if X_s is so. If $p \neq 0$, then X and $X^{[p]}$ are simultaneously regular or singular.

Let k be *infinite.* Then there exists a semisimple regular element $Y \in \mathfrak{g}_k$. In fact, the set S of singular elements is a proper algebraic subset (the set of zeros of the last nonidentically vanishing coefficient of the Killing equation), hence we may find $X \in \mathfrak{g}_k$ which is regular. Let $X = X_s + X_n$ be its Jordan decomposition. If $p = 0$, take $Y = Y_s$; if not, there exists a power q of p such that $X_n^{[q]} = 0$. Then put $Y = X^{[q]}$.

In the sequel, k is infinite.

3.2. *Proof of Theorem* A (i). A Cartan subgroup is the centralizer of a maximal torus [**1**], and the centralizer of a k-torus is defined over k [**2**, §10]. It suffices therefore to prove the existence of a maximal torus defined over k. We use induction on $\dim G$.

Let first G be nilpotent, then $G = T \times U$ (T unique maximal torus, U unipotent radical). If k is perfect, T is defined over k. If not, we let q be a power of p such that $U^q = \{e\}$. Then $G^q = T^q = T$, hence $g \mapsto g^q$ is a morphism of G onto T, clearly defined over k, and T is defined over k. (This argument, phrased slightly differently, is due to Rosenlicht [**6**].) Let now G be not nilpotent. We let $\pi : G \mapsto G'$ be the identity if not all of the semisimple elements of $\mathfrak{g}$ are central, and be as in Proposition 2.2 otherwise.

By §3.1, there exists a semisimple regular element $Y \in \mathfrak{g}'_k$. By construction of G', we have $n(\mathfrak{g}') \neq \dim G$, hence $z(Y) \neq \mathfrak{g}'$.

We let G operate on $\mathfrak{g}'$ by $\mathrm{Ad} \circ \pi$. Clearly, $G(Y) = \mathrm{Ad}\, G'(Y)$, hence $G(Y)$ is closed (Proposition 1.6). Let $\tilde{Z}_G(Y)$ be the isotropy group of Y. Then $\pi(\tilde{Z}_G(Y)) = Z_{G'}(Y)$, hence (Proposition 1.5), $\dim \tilde{Z}_G(Y) = \dim \mathfrak{g} - n(\mathfrak{g}')$ and $\tilde{Z}_G(Y)^0$ is a *proper* closed subgroup of G. We want to prove that it is defined over k. This is clear in char. 0 (or if k is perfect) so let $p \neq 0$. Let f be the map $g \mapsto \mathrm{Ad}\, \pi(g)(Y)$ of G onto $G(Y)$. It is defined over k. We claim that it is separable. To show this, it suffices to prove that $df_e : X \mapsto Y + [d\pi(X), Y]$ maps $\mathfrak{g}$ onto the tangent space to $G(Y)$ at Y. By 1.5, this tangent space is equal to $Y + [\mathfrak{g}', Y]$, so that our assertion is clear if π is the identity. If $\pi \neq \mathrm{Id}$, we are in the situation of Proposition 2.2. Then $d\pi(\mathfrak{g})$ is an ideal of $\mathfrak{g}'$, obviously stable under $\mathrm{Ad}\, G'$, which is a supplementary subspace of the Lie algebra of any maximal torus of G'. Since Y is contained in such an algebra, we see that $[Y, \mathfrak{g}'] = [Y, d\pi(\mathfrak{g})]$, whence our assertion. It follows that the graph Γ of f in $G \times G(Y)$, and $G \times \{Y\}$, cut each other transversally. By the criterion of multiplicity one [**8**, VI, §2, Theorem 6] the cycle, sum of the irreducible components of $\Gamma \cap (G \times \{Y\}) = Z_G(Y)$, each with coefficient one, is rational over k, hence $(\tilde{Z}_G(Y))^0$ is defined over k [**8**, Proposition 1, p. 208]. By induction assumption $\tilde{Z}_G(Y)^0$ has a maximal torus T defined over k. But $\tilde{Z}_G(Y)$ contains at least one maximal torus of G, hence T is a maximal torus of G.

3.3. *Proof of Theorem* A (ii). Let now G be reductive. The result is known if G is a torus [**6**], so we again use induction on $\dim G$. The group $\tilde{Z}_G(Y)^0$ considered above is reductive; in fact, it contains a maximal torus T, and it is clear that $\Phi(\tilde{Z}_G(Y)^0, T)$ is a symmetric subset of $\Phi(G, T)$ (see [**2**, §2.3, Remark]). We want to prove that the groups $\tilde{Z}_G(Y)^0$, where Y varies over the regular semisimple elements $Y \in \mathfrak{g}'_k$ generate G. Let H be the group they generate and $H' = \pi(H)$; assume $H' \neq G$. There exists then a regular element $X \in \mathfrak{g}'_k$ not in $\mathfrak{h}'$. We have then $z(X_s) \not\subset \mathfrak{h}'$, hence $z(X_s^{[q]}) = z(X_s) \not\subset \mathfrak{h}'$ for every power q of p. We can therefore find a regular semisimple element $Y \in \mathfrak{g}'_k$ such that $\mathrm{nil}\, z(Y) \not\subset \mathfrak{h}'$. Since $z(Y)$ is the Lie algebra of $Z(Y) = \pi(\tilde{Z}_G(Y))$ by Proposition 1.5, it follows that $\tilde{Z}_G(Y)^0 \not\subset H$, contradicting the definition of H. Thus $H = G$. There exist consequently finitely many connected reductive proper k-subgroups H_i ($i = 1, \cdots, t$), such that the product mapping $(h_1, \cdots, h_t) \mapsto h_1 \cdot \cdots \cdot h_t$ of $H_1 \times \cdots \times H_t$ into G is a surjective

k-morphism of the underlying algebraic varieties. By induction assumption, each H_i is unirational over k, hence so is G.

REMARKS. (1) Let X be a regular element in $\mathfrak{g}$. Its nilspace $\mathfrak{n}(X)$, i.e. the set of Y in $\mathfrak{g}$ which are annihilated by some power of ad Y, is by definition in [5] a Cartan subalgebra of $\mathfrak{g}$. We have $\mathfrak{n}(X) = \mathfrak{n}(X_s) = \mathfrak{z}(X_s)$, and, by Proposition 1.5, $\mathfrak{z}(X_s)$ is the Lie algebra of $Z(X_s)$. It follows that the subgroups of type (C) of [5] are the centralizers in G of the regular semisimple elements of $\mathfrak{g}$.

(2) In the same context, one can also prove that a reductive k-group splits over a finite separable extension of the groundfield, that the variety of Cartan subgroups of G is rational over k [5], give alternate proofs of some structure theorems of Rosenlicht's about unipotent groups acted upon by tori, and of the conjugacy over k of maximal k-tori in a solvable k-group. Details will be given elsewhere.

REFERENCES

1. A. Borel, *Groupes linéaires algébriques*, Ann. of Math. (2) **64** (1956), 20–80.

2. A. Borel and J. Tits, *Groupes réductifs*, Publ. Math. I.H.E.S. n° **27** (1965), 55–150.

3. P. Cartier, *Isogénies de variétés de groupes*, Bull. S.M.F. **87** (1959), 191–220.

4. C. Chevalley, *Séminaire sur la classification des groupes de Lie algébriques*, 2 vols. Paris, 1958. (Mimeographed)

5. M. Demazure and A. Grothendieck, *Schémas en groupes*, I.H.E.S. 1964. (Mimeographed)

6. M. Rosenlicht, *Some rationality questions on algebraic groups*, Annali di Mat. (IV) **43** (1957), 25–50.

7. J-P. Serre, *Quelques propriétés des variétés abéliennes en caractéristique p*, Amer. J. Math. **80** 1958, 715–739.

8. A. Weil, *Foundations of algebraic geometry*, Amer. Math. Soc. Colloq. Publ. vol. **29**, 2nd ed., Amer. Math. Soc., Providence, R.I. 1962.

Classification of Algebraic Semisimple Groups

BY

J. TITS

This is mostly an exposition of known results. However, part of the final classification, given at the end in the form of tables, a few propositions in §§2 and 3, and various improvements in the statements of other results may be new. The bibliographical references following each title serve a double purpose, historical and technical: they refer either to papers where, to the best knowledge of the author, the stated results have been announced first, or to places where proofs (or further information) are supplied. In general, proofs are given or sketched here, only when they are not available in the literature. A detailed justification of the classification tables would require much space and will not be found in this paper (the author hopes to write it down at some other occasion); however, using the indications given here or in the cited literature, the reader should not have much difficulty in reconstructing the arguments, except perhaps for some rather tricky existence proofs. At this point it should be mentioned that discussions with M. Kneser have been of considerable help in the final setting up of these tables; without him, several ugly question marks would still spoil them.

1. Algebraically closed fields, Dynkin diagrams.

1.1. *Dynkin diagrams* ([3], [5], [7], [11], [13], [29], [47]).

1.1.1. *Notations.* All semisimple groups considered in this paper are assumed to be connected. The following notations are used throughout the §1: K is an algebraically closed field, G a semisimple algebraic group defined over K, T a maximal torus of G, N its normalizer, $X = X^*(T)$ the character group of T, $\Sigma \subset X$ the set of all roots (of G relative to T). In $X \otimes \boldsymbol{R}$ we choose a scalar product (,) invariant under the Weyl group $W = N/T$ (which operates on X in the obvious way) and an ordering, Δ is the set of all simple roots (with respect to that ordering), $-\mu$ is the dominant (i.e. maximal) root and we set $\Delta' = \Delta \cup \{\mu\}$. If G is *almost simple* (i.e. has no proper infinite normal subgroup), μ depends only on Δ, that is, is the minimal root for any ordering for which Δ is the set of simple roots. (When G is not almost simple, there is little interest in considering μ and Δ'.) For every root $\alpha \in \Sigma$, we denote by $\alpha^* : X \otimes \boldsymbol{R} \to \boldsymbol{R}$ the linear form defined by

$$\alpha^*(x) = 2(\alpha, x)/(\alpha, \alpha).$$

One has $\alpha^*(\Sigma) \subset \boldsymbol{Z}$.

1.1.2. *Ordinary Dynkin diagram.* For every pair α, β of distinct elements of Δ', we have one of the following sets of relations, possibly after interchanging α and β:

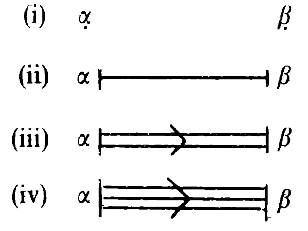
(i) $\alpha^*(\beta) = \beta^*(\alpha) = 0$,

(ii) $\alpha^*(\beta) = \beta^*(\alpha) = -1$,

(iii) $\alpha^*(\beta) = -1, \beta^*(\alpha) = -2$,

(iv) $\alpha^*(\beta) = -1, \beta^*(\alpha) = -3$.

To build the *Dynkin diagram* of G, one represents the elements of Δ by points (the *vertices* of the diagram) and one joins the points representing α and β as follows, according as to which one of the above sets of conditions is fulfilled:



(In the last case, it is often suitable to use a quadruple segment instead of a triple one, for reasons which will appear in §1.3.2; here we shall however use the above notation, which is the most common.)

1.1.3. *Affine* (= *extended*) *Dynkin diagram.* Assume first that G is almost simple. The construction described above for the Dynkin diagram, when applied to the set Δ' instead of the set Δ, gives rise to a new diagram, called the *affine* (or *extended*) *Dynkin diagram* of G. If G is not almost simple, we define its affine Dynkin diagram as the disjoint union of those of its almost simple normal subgroups. Since the affine Dynkin diagram is a function of the root system Σ, which is determined up to isometry by the (ordinary) Dynkin diagram, it will be meaningful to talk about *the affine diagram associated with* (*or extension of*) *a given Dynkin diagram.*

The main purpose of §1 is to indicate how important data relative to a group G can be read on its Dynkin diagrams.

1.2. *Classification up to isogeny* ([7], [11]).

1.2.1. *Isogenies.* An isogeny is a surjective homomorphism with finite kernel. If G and H are groups defined over K, an isogeny $\phi: H \to G$ is said to be *central* if for every K-algebra A, the kernel of the homomorphism $\phi_A: H_A \to G_A$ is central in H_A. (We denote by G_A and H_A the groups of points of G and H with coefficients in A; for the meaning of these notions, see [6].) Every separable isogeny of a connected group G is central. We shall say that two groups G, G' are (*strictly*) *isogenous* if there is a group H and two (central) isogenies $H \to G$ and $H \to G'$. This relation is transitive.

1.2.2. *The main theorem.*

THEOREM 1. *The field K being given, a semisimple group G is characterized up to strict isogeny by its Dynkin diagram. It is almost simple if and only if the diagram is connected. Any semisimple group G is strictly isogenous to a direct product of simple groups whose Dynkin diagrams are the connected components of the diagram* *of G. The complete list of Dynkin diagrams of almost simple groups is given in Table* I; *each diagram of that table determines a strict isogeny class of almost simple groups over any given field K.*

Table I gives simultaneously the ordinary and the affine Dynkin diagrams of each group: the strokes which join the vertex μ to the other vertices (and which therefore complement the ordinary diagram to give the affine one) are drawn in broken lines.

We mention further that the only almost simple groups which are isogenous without being strictly isogenous are the groups of types B_n and C_n, for the same $n \geqq 3$, over a field of characteristic 2.

Notice that Theorem 1 gives us the right to talk about "the Dynkin diagram of a strict isogeny class."

1.3. *Weyl groups* ([**5**], [**7**], [**29**], [**34**], [**47**]).

1.3.1. Let $V = X_*(T) \otimes \boldsymbol{R}$ be the dual of $X \otimes \boldsymbol{R}$. There is an obvious action of the Weyl group $W = N/T$ on V; we shall occasionally identify W with its canonical image in $\mathrm{GL}(V)$. For every root α (which we view as a linear form on V) and every integer $i \in \boldsymbol{Z}$, we denote by $r_{\alpha,i}$ the reflection with respect to the hyperplane $\alpha^{-1}(i)$, defined by means of some euclidean metric invariant under W (which metric one chooses is irrelevant). Finally, we set $r_\alpha = r_{\alpha,0}$.

1.3.2. *Generators and relations.* The Weyl group contains all the $r_\alpha(\alpha \in \Sigma)$, and is generated by the r_α $(\alpha \in \Delta)$. As an "abstract" group, it is defined by the relations

$$(r_\alpha r_\beta)^{m_{\alpha\beta}} = 1,$$

where α, β run through Δ, $m_{\alpha\alpha} = 1$ and $m_{\alpha\beta} = 2$ (resp. 3, 4, 6) when $\alpha \neq \beta$ and the pair α, β satisfies the set of relations (i) (resp. (ii), (iii), (iv)) in §1.1.2.

1.3.3. *Affine Weyl group.* Let G be almost simple. The group generated by all $r_{\alpha,i}$ is called the *affine Weyl group* of G. Set $r'_\alpha = r_\alpha$ if $\alpha \in \Delta$, and $r'_\mu = r_{\mu,1}$. Then, the affine Weyl group is generated by the r'_α $(\alpha \in \Delta')$ and is defined, as an abstract group, by the relations

$$(r'_\alpha r'_\beta)^{m_{\alpha\beta}} = 1,$$

where the $m_{\alpha\beta}$ are defined as above.

1.4. *Coefficients of the dominant root*; *dimension* ([**3**], [**5**], [**14**], [**24**], [**33**]).

1.4.1. The group G is again assumed to be almost simple. Set $-\mu = \sum c_\alpha \alpha$ and $c_\mu = 1$ so that

$$\sum_{\alpha \in \Delta'} c_\alpha \alpha = 0,$$

and, for every $\beta \in \Delta'$,

$$(1) \qquad \sum_{\alpha \in \Delta'} c_\alpha \beta^*(\alpha) = 0.$$

In this formula, it suffices of course to extend the summation to the set C_β of all elements α of Δ' which are connected to β in the affine Dynkin diagram. When all roots of G have equal length, (1) becomes

$$2c_\beta = \sum_{\alpha \in C_\beta} c_\alpha. \tag{2}$$

The formulae (1) and (2) give an effective way to compute rapidly the c_α. For instance, in the case of E_6, one finds successively, when numbering the simple roots as in Table I, $c_6 = 2c_\mu = 2, c_3 = 2c_6 - c_\mu = 3, c_2 = 2c_1, c_3 = 2c_2 - c_1 = 3c_1$, thus $c_1 = 1$, $c_2 = 2$, and similarly, $c_5 = 1$ and $c_4 = 2$.

1.4.2. If $r = \#\Delta$ is the rank of G and $c = \sum_{\alpha \in \Delta} c_\alpha$, the dimension of G is given by the formula

$$\dim G = r \cdot (c + 2).$$

For instance, $\dim E_6 = 6 \cdot (1 + 2 + 3 + 2 + 1 + 2 + 2) = 78$.

1.5. *Classification up to isomorphism; automorphism group and center* ([**3**], [**5**], [**7**], [**12**], [**14**], [**29**]).

1.5.1. *Opposition involution.* There exists a unique involutory permutation i of the simple roots such that the mapping $\alpha \to -i(\alpha)$ extends to an operation of the Weyl group. This permutation i, called the *opposition involution*, induces an automorphism of the Dynkin diagram $\mathscr{D}$. It can be determined by the following rule: i leaves invariant each connected component of $\mathscr{D}$ and induces a nontrivial automorphism on a given component $\mathscr{D}_0$ if and only if $\mathscr{D}_0$ is of type A_n, D_{2n+1} or E_6. (Notice that the diagrams of these types have a single nontrivial automorphism.) Whenever $\mathscr{D}$ is connected and possesses a nontrivial automorphism, i is that automorphism, except in the case of D_{2n}. Once one knows that, for the type D_m, the parity of m plays an essential role, there are two easy ways to remember "which is which": since $A_3 = D_3$, the type D_{2n+1} must behave like the types A, that is, i cannot be the identity; on the other hand, since i is "characteristic," that is, invariant by the automorphism group of $\mathscr{D}$, it follows from the symmetry of order 3 of the diagram D_4 that i must be the identity for this type, and therefore also for all types D_{2n}.

1.5.2. *The cocenter C^*.* To each strict isogeny class $\mathscr{G}$ of semisimple groups, we shall associate a certain finite commutative group $C^* = C^*(\mathscr{G})$, which will turn out to be the dual of the center of the simply connected group in $\mathscr{G}$ (see §§1.5.4 and 1.5.5), and whose knowledge permits an immediate classification up to isomorphism of the groups in $\mathscr{G}$ (§1.5.4). Here, we give a "natural" definition of C^* in terms of roots and weights. In §1.5.3, it will be seen how C^* can be deduced from the Dynkin diagrams of $\mathscr{G}$.

In the space $V^* = X \otimes \boldsymbol{R}$ (1.1.1), let $\bar{X}$ be the group generated by Σ and let $\tilde{X}$ be the group of all $v^* \in V^*$ such that $\alpha^*(v^*) \in \boldsymbol{Z}$ for all $\alpha \in \Sigma$ (§1.1.1). ($\tilde{X}$ is called the *weight group* of the root system.) The group C^* is then defined as the quotient $\tilde{X}/\bar{X}$. Its Pontrjagin dual, which we shall denote by $C = C(\mathscr{G})$ is canonically isomorphic (and will be identified) with the quotient $\bar{X}_*/\tilde{X}_*$, where

$$\tilde{X}_*(\subset V = X_*(T) \otimes \boldsymbol{R})$$

is generated by the α^*, with $\alpha \in \Sigma$, and $\bar{X}_*$ consists of all $v \in V$ such that $\alpha(v) \in \mathbf{Z}$ for all $\alpha \in \Sigma$.

1.5.3. *Automorphism groups of Dynkin diagrams.* As before, $\mathscr{D}$ denotes the Dynkin diagram of G and $\mathscr{D}'$ its associate affine diagram. Every automorphism of $\mathscr{D}$ extends uniquely to an automorphism $\mathscr{D}'$; therefore, we can identify the group $\mathrm{Aut}(\mathscr{D})$ of automorphisms of $\mathscr{D}$ with a subgroup of $\mathrm{Aut}(\mathscr{D}')$. There is a natural, effective action, which we want to describe, of the group C defined in §1.5.2 on $\mathscr{D}'$. For every $x \in \bar{X}_*$, the affine Weyl group W' contains a unique element whose product with the translation $v \mapsto v + x$ leaves invariant the "fundamental chamber" $\{v \in V | \alpha(v) > 0$ for all $\alpha \in \Sigma$ and $\mu(v) < 1\}$, that is, permutes the fixed hyperplanes of the reflexions r'_α with $\alpha \in \Delta'$ (§1.3.3). Through the permutation of Δ' thus defined, we obtain an action of x on $\mathscr{D}'$. It can be shown that the translations belonging to W' are exactly the translations by elements of $\tilde{X}_*$, and that W' operates trivially on the quotient $\bar{X}_*/\tilde{X}_*$. From this, it follows immediately that the mapping $\bar{X}_* \to \mathrm{Aut}\,\mathscr{D}'$ which has just been defined is a homomorphism whose kernel is $\tilde{X}_*$, and induces therefore a monomorphism $C \to \mathrm{Aut}(\mathscr{D}')$.

We now indicate a few properties of the group C, *considered as a subgroup of* $\mathrm{Aut}(\mathscr{D}')$. Notice that, since $\mathscr{D}'$ characterises Σ (up to isometry) which, in turn, determines C, we are allowed to talk about "the group C of an affine Dynkin diagram $\mathscr{D}'$", a group which we denote by $C(\mathscr{D}')$.

(1) If the diagram $\mathscr{D}'$ is the disjoint union of a set of subdiagrams $\mathscr{D}'_i$, the group $C(\mathscr{D}')$ is the direct product of the groups $C(\mathscr{D}'_i)$, where $C(\mathscr{D}'_i)$ is made to operate trivially on $\mathscr{D}'_j$ whenever $j \neq i$.

(2) The group C is a normal subgroup of $\mathrm{Aut}(\mathscr{D}')$, one has $\mathrm{Aut}(\mathscr{D}) \cap C = \{1\}$ and $\mathrm{Aut}(\mathscr{D}') = \mathrm{Aut}(\mathscr{D}) \cdot C$. In other words, $\mathrm{Aut}(\mathscr{D}')$ *is the semidirect product of* $\mathrm{Aut}(\mathscr{D})$ *and* C. In particular, there is a natural action of $\mathrm{Aut}(\mathscr{D})$ on C.

(3) Every element $c \in C$ is transformed in its inverse by the opposition involution i (that is, $ici^{-1} = c^{-1}$).

(4) *If $\mathscr{D}'$ is connected, the set of all vertices α such that $c_\alpha = 1$, with the notation of* §1.4.1, *is invariant under* $\mathrm{Aut}(\mathscr{D}')$, *and the group C is simply transitive on it.*

The subgroup C of $\mathrm{Aut}(\mathscr{D}')$ is completely characterized by (1), (3), and either one of the properties (2) and (4). More interesting perhaps, from a mnemonic point of view, is the fact (1) and (2) alone, together with the fact that C is commutative, characterize C except when $\mathscr{D}$ has a component of type D; in this case, it must be remembered that

$$C(D_{2n}) \cong (\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/2\mathbf{Z}), \qquad C(D_{2n+1}) \cong \mathbf{Z}/4\mathbf{Z}.$$

1.5.4. *Classification up to isomorphism; simply connected and adjoint groups.* To each group G of the strict isogeny class $\mathscr{G}$, we can associate the subgroup $C'(G) = X_*(T)/X_*$ of C, or equivalently the subgroup $C^*(G) = X^*/\bar{X}^*$ of C^*; we set $C(G) = \bar{X}_*/X_*(T) = C/C'(G)$. The classification up to isomorphism of the groups in $\mathscr{G}$ is now given by the

PROPOSITION 1. *Two groups G, $G' \in \mathscr{G}$ are isomorphic iff the groups $C'(G)$ and*

$C'(G')$ are conjugate in $\mathrm{Aut}(\mathscr{D}')$. *There exists a central isogeny $G \to G'$ iff $C'(G)$ is conjugate in* $\mathrm{Aut}(\mathscr{D}')$ *to a subgroup of $C'(G')$. Every subgroup of $C = C(\mathscr{G})$ is the group $C'(G)$ of some group $G \in \mathscr{G}$.*

Notice that the characteristic of the ground field plays no role here.

It follows from the proposition above that $\mathscr{G}$ contains a "biggest group" $\tilde{G}$ (such that $C(\tilde{G}) = C$) and a "smallest group" $\bar{G}$ (such that $C(\bar{G}) = \{1\}$). For any G in $\mathscr{G}$, the groups $\tilde{G}$ and $\bar{G}$ (together with central isogenies $\tilde{G} \to G$ and $G \to \bar{G}$) are respectively called the *simply connected* or *universal covering* of G, and the *adjoint group* of G.

The second statement of the proposition can be made more precise. Any central isogeny $G \to G'$ induces in a natural way an injection $C'(G) \to C'(G')$. For a given G, the central isogenies $\phi : G \to G'$ are thus exactly classified, up to equivalence, by the subgroups of $C(G)$ (two isogenies $\phi' : G \to G'$ and $\phi'' : G \to G''$ are called equivalent if there exists an isomorphism $f : G' \to G''$ such that $\phi'' = f \circ \phi'$). The isogeny ϕ is separable (resp. purely inseparable) iff the index $[C(G) : C(G')]$ is prime to the characteristic p of the ground field (resp. is a power of p).

1.5.5. *Center*. The center $\mathscr{Z}(G)$ of G is canonically isomorphic with the group $\mathrm{Hom}(C^*(G), K^*)$, where K^* is the multiplicative group of K. If one adopts a "classical", nonschematical point of view (that is, if one overlooks the nilpotent elements in the structural sheave of G), $\mathscr{Z}(G)$ is therefore isomorphic with the quotient of $C(G)$ by its p-primary component, where p is the characteristic of K.

1.5.6. *Automorphism group*. The group $\mathrm{Aut}(G)$ of all K-automorphisms of G is the semidirect product of the group $\mathrm{Int}(G)$ of all inner automorphisms and a finite group A, canonically isomorphic with the normalizer of $C(G)$ in $\mathrm{Aut}(\mathscr{D})$. In particular, if G is simply connected or adjoint, $A = \mathrm{Aut}(\mathscr{D})$.

1.6. *Parabolic subgroups* ([**4**], [**7**], [**37**], [**39**]). There is a natural one-to-one correspondence between the conjugacy classes of parabolic subgroups of G, and the subsets of the set Δ of all simple roots. To a subset $\Theta \subset \Delta$ is associated the conjugacy class containing the parabolic subgroup generated by T and by the groups $U_\alpha (\alpha \in \Delta)$ and $U_{-\alpha} (\alpha \in \Theta)$, where U_α denotes the "one-parameter root group" corresponding to the root α. In particular, the conjugacy class associated to the empty set is the class of all Borel subgroups, and the conjugacy class associated with Δ is $\{G\}$.

2. Non algebraically closed field. Index and anisotropic kernels.

2.1. *Introduction*; *notations* ([**2**], [**4**]). We now go over to the case where the ground field k is arbitrary. Our main aim is the proof of a theorem which is a sort of analogue for the algebraic semisimple groups (and to a certain extent a generalization) of Witt's theorem characterizing a quadratic form by means of its index and anisotropic kernel.

The following notations will be used all through §§2 and 3; k is a field, K the separable closure of k, $\Gamma = \mathrm{Gal}(K/k)$ the Galois group, G a semisimple group defined over k (which splits over K by Grothendieck's theorem), S a maximal k-split torus of G, T a maximal torus containing S and defined over k. Compatible orders are chosen in the character groups $X^*(S)$ and $X^*(T)$. Finally, we denote by Δ the system of simple roots of G with respect to T, Δ_0 the subsystem of those roots which vanish on S and ${}_k\Delta$ the system of simple relative (k-)roots (i.e. the set of restrictions to S of the elements of Δ).

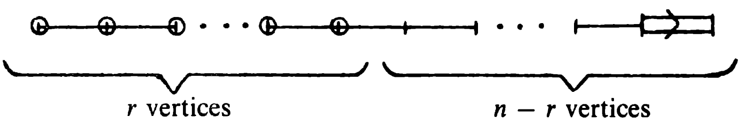
2.2. *Anisotropic kernels* ([**4**], [**27**], [**38**], [**40**], [**43**]). Let $\mathscr{Z}(S)$ be the centralizer of S, let $\mathscr{D}\mathscr{Z}(S)$ be its derived group and let Z_a be the maximal anisotropic subtorus of the center of $\mathscr{Z}(S)$. Then, the groups $\mathscr{D}\mathscr{Z}(S)$ and $\mathscr{D}\mathscr{Z}(S)\cdot Z_a$, which are, up to k-isomorphisms, independent of the choice of S, are respectively called the *semisimple anisotropic kernel* and the (*reductive*) *anisotropic kernel* of G. Notice that Δ_0 is the set of simple roots of $\mathscr{D}\mathscr{Z}(S)$ (with respect to the maximal torus $T \cap \mathscr{D}\mathscr{Z}(S)$ and to a suitable ordering of its character group), and that the product $\mathscr{D}\mathscr{Z}(S)\cdot Z_a$ is almost direct (i.e. is a direct product up to isogeny). If $\mathscr{D}\mathscr{Z}(S) = \{1\}$, which means that $\mathscr{Z}(S) = T$, the group G is said to be *quasi-split*.

2.3. *Index* ([**4**], [**26**], [**27**], [**38**], [**40**], [**42**]). We first define an action, called the *-*action*, of Γ on Δ. The elements of Δ are in canonical 1–1 correspondence with the conjugacy classes of maximal parabolic subgroups of G (§1.6); since G is split over K, these conjugacy classes are "defined over K" and therefore permuted by Γ. Through the above correspondence, Γ acts on Δ; the permutation of Δ corresponding to $\sigma \in \Gamma$ will be denoted by σ^*. It can also be defined as follows: since K is separably closed, T is split over K, therefore all its characters are defined over K and Γ operates naturally on $X^*(T)$; then, $\sigma(\Delta)$ is the system of simple root for a certain ordering of $X^*(T)$, there exists a well-defined element w of the Weyl group for which $w(\sigma(\Delta)) = \Delta$, and we set $\sigma^* = w \circ \sigma$. When the *-action of Γ on Δ is trivial (resp. not trivial), the group G is said of *inner* (resp. *outer*) *type*, and called an *inner* (resp. *outer*) *form* of ${}_KG$ (the same group, considered as defined over K).

We call (k-) *index* of the group G the data consisting of Δ (together with the Dynkin diagram of G), Δ_0 and the *-action of Γ on Δ. The following diagrammatic representation of the index will be used: the Dynkin diagram of G is drawn in such a way that vertices belonging to the same orbit of Γ are close to each other and the orbits—called *distinguished orbits*—whose elements do not belong to Δ_0 are circled (for an example, see §2.5.5, or Table II). Strictly speaking, this representation gives only the orbits of Γ in Δ and not its full action; however, in most "practical cases", this amounts to the same, once the group $\{\sigma | \sigma^* = \mathrm{id}\}$ (or, equivalently, the fixed field of this group) is known.

Notice that the index of the semisimple anisotropic kernel of G can be deduced from the index of G by simply removing the vertices of the Dynkin diagram of G which do not belong to Δ_0 (together with the strokes ending in such vertices). When G is quasi-split, all orbits of Γ in Δ are distinguished (i.e. $\Delta_0 = \varnothing$).

2.4. *An example; orthogonal groups*. The following example shows the relation between the above notions of anisotropic kernel and index, and the corresponding notions for quadratic forms. Let $G = {}_k\mathrm{SO}(f)$ be the special orthogonal group of a nondegenerate quadratic form f in $2n+1$ variables and let r be the index of f and f_0 be its anisotropic kernel (a form in $n-2r$ variables). Then, the index of G is



and its anisotropic kernel is ${}_k\mathrm{SO}(f_0)$. (For the case of an even number of variables, and other examples, see Table II.)

2.5. *How to deduce the relative root system from the index* ([4], [40]).

2.5.1. *Two elements of* Δ *which do not belong to* Δ_0 *have the same restriction to* S *if and only if they belong to the same orbit of* Γ. More precisely, S is the connected component of the subgroup of T defined by the following system of equations (where $t \in T$):

$$\begin{aligned} &\alpha(t) = 1 \qquad \text{for all } \alpha \in \Delta_0, \\ (1) \qquad &\beta(t) = (\sigma^*(\beta))(t) \qquad \text{for all } \beta \in \Delta \text{ and all } \sigma \in \Gamma. \end{aligned}$$

It follows that the elements of ${}_k\Delta$ are in canonical 1–1 correspondence with the orbits of Γ in Δ–Δ_0; the orbit corresponding to $\gamma \in {}_k\Delta$ will be denoted by $\mathcal{O}_\gamma$.

The above equations show that the torus S is known once the index of G is given; so therefore the relative root system and the relative Weyl group. To determine them explicitly is an easy exercise of which we state the results right away.

2.5.2. *Relative root system.* We introduce in $X^*(T) \otimes \boldsymbol{R}$ a scalar product $(\ ,\ )$, invariant under the Weyl group, and identify $X^*(S) \otimes \boldsymbol{R}$ with the subspace of $X^*(T) \otimes \boldsymbol{R}$ orthogonal to all characters vanishing on S. Let $c_{\alpha\beta}$, with $\alpha, \beta \in \Delta$ (resp. ${}_k\Delta$), be the coefficients of the inverse of the matrix whose coefficients are the scalar products of pairs of elements of Δ (resp. ${}_k\Delta$). Then, for all $\gamma, \delta \in {}_k\Delta$, one has

$$c_{\gamma\delta} = \sum_{\alpha \in \mathcal{O}_\gamma} \sum_{\beta \in \mathcal{O}_\delta} c_{\alpha\beta}.$$

To describe the relative root system completely, there remains to determine, for each simple root $\gamma \in {}_k\Delta$, the largest integer $n (= 1 \text{ or } 2)$ such that $n\gamma$ is a relative root. This is done as follows. Let $\mathscr{D}$ be the subdiagram of the Dynkin diagram of G whose vertices are the elements of $\Delta_0 \cup \mathcal{O}_\gamma$, and let $\mathscr{D}'$ be any connected component of $\mathscr{D}$ whose vertices do not all belong to Δ_0. Then, n is the sum of the coefficients of the roots belonging to $\mathcal{O}_\gamma$, in the expression as linear combination of simple roots of the dominant root of the root system corresponding to the Dynkin diagram $\mathscr{D}'$ (cf. §1.4.1; for an example, see §2.5.5).

2.5.3. *Relative Weyl group.* Let $\gamma, \delta \in {}_k\Delta$ be two relative simple roots, and let $m_{\gamma\delta}$ be the order of the product $r_\gamma r_\delta$ of the reflexions with respect to γ and δ (so that the relative Weyl group is defined, as an abstract group, by the relations

$$r_\gamma^2 = (r_\gamma r_\delta)^{m_{\gamma\delta}} = 1).$$

The orders $m_{\gamma\delta}$ are given by the formulae

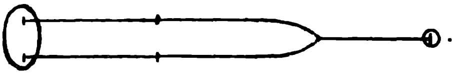
$$\cos(\pi/m_{\gamma\delta}) = (\gamma, \delta)^2/(\gamma, \gamma)(\delta, \delta).$$

However, one can also determine $m_{\gamma\delta}$ without computing first the (γ, δ)'s, which, by the method of §2.5.2, may be rather long. Let f_0 (resp. $f_\gamma ; f_\delta ; f_{\gamma\delta}$) be the number of roots of the root system whose Dynkin diagram is the subdiagram of the diagram of G having as vertices the elements of Δ_0 (resp. $\Delta_0 \cup \mathcal{O}_\gamma ; \Delta_0 \cup \mathcal{O}_\delta$; $\Delta_0 \cup \mathcal{O}_\gamma \cup \mathcal{O}_\delta$). Then,

$$m_{\gamma\delta} = \frac{2(f_{\gamma\delta} - f_0)}{f_\gamma + f_\delta - 2f_0}.$$

2.5.4. *Parabolic subgroups.* Let $\mathcal{P}$ be a conjugacy class of parabolic subgroups of G and let $\Delta' \subset \Delta$ be the associated set of simple roots (§1.6). Then, $\mathcal{P}$ contains a parabolic subgroup defined over k if and only if Δ' contains Δ_0 and is invariant under the $*$-action of Γ (§2.3). The class $\mathcal{P}$ is said to be *defined over k* whenever Δ' is invariant under Γ; in that case, $\mathcal{P}$ has a natural structure of projective algebraic variety defined over k, whose (possibly nonexistent) rational points are the parabolic subgroups in $\mathcal{P}$ which are defined over k.

2.5.5. *An example.* Let the index of G be



The simple roots of E_6 being numbered as in Table I, the orbits of Γ in $\Delta - \Delta_0$ are $\{1, 5\}$ and $\{6\}$. Let us denote by γ and δ the corresponding relative roots. We have

$$\begin{pmatrix} 2 & -1 & 0 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & 0 & -1 \\ 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & -1 & 2 & 0 \\ 0 & 0 & -1 & 0 & 0 & 2 \end{pmatrix}^{-1} = \frac{1}{3}\begin{pmatrix} 4 & 5 & 6 & 4 & 2 & 3 \\ 5 & 10 & 12 & 8 & 4 & 6 \\ 6 & 12 & 18 & 12 & 6 & 9 \\ 4 & 8 & 12 & 10 & 5 & 6 \\ 2 & 4 & 6 & 5 & 4 & 3 \\ 3 & 6 & 9 & 6 & 3 & 6 \end{pmatrix}.$$

Therefore

$$\begin{pmatrix} (\gamma, \gamma) & (\gamma, \delta) \\ (\delta, \gamma) & (\delta, \delta) \end{pmatrix} = 3 \cdot \begin{pmatrix} 4+2+4+2 & 3+3 \\ 3+3 & 6 \end{pmatrix}^{-1} = \tfrac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix}.$$

The diagram whose set of vertices is $\Delta_0 \cup \mathcal{O}_\gamma$ (resp. $\Delta_0 \cup \mathcal{O}_\delta$) is of type A_5 (resp. D_4); the sum of the coefficients of the roots 1, 5 (resp. the coefficient of the root 6) in the dominant root of the corresponding root system is 2 (resp. 1), therefore 2γ is a root (resp. 2δ is not a root) and the relative root system is of type BC_2.

The diagrams whose sets of vertices are Δ_0, $\Delta_0 \cup \mathcal{O}_\gamma$, $\Delta_0 \cup \mathcal{O}_\delta$, $\Delta_0 \cup \mathcal{O}_\gamma \cup \mathcal{O}_\delta$ are respectively of type A_3, A_5, D_4 and E_6. We have therefore, with the notations of §2.5.3,

$$f_0 = 12, \quad f_\gamma = 30, \quad f_\delta = 24, \quad f_{\gamma\delta} = 72,$$

and

$$m_{\gamma\delta} = \frac{2 \cdot (72 - 12)}{(54 - 24)} = 4,$$

which is coherent with the preceding conclusions.

Among the 2^6 conjugacy classes of parabolic subgroups of G, 2^4 are defined over k and 2^2 contain a parabolic subgroup defined over k.

2.6. *Isogeny.*

2.6.1. *Simply connected covering and adjoint group.*

PROPOSITION 2. *We recall that G is a semisimple group defined over k. There exists a sequence*

$$\tilde{G} \xrightarrow{\tilde{\pi}} G \xrightarrow{\bar{\pi}} \bar{G},$$

where $\tilde{G}$ is simply connected and defined over k, $\bar{G}$ is adjoint and defined over k and $\tilde{\pi}$, $\bar{\pi}$ are two central k-isogenies. The groups $\tilde{G}$, $\bar{G}$ and the isogenies $\tilde{\pi}$ and $\bar{\pi}$ are unique up to k-isomorphism.

PROOF. The theory of split groups ([**4**, §2], [**9**]) shows that there exists a sequence

$$\tilde{G}' \xrightarrow{\tilde{\pi}'} G' \xrightarrow{\bar{\pi}'} \bar{G}',$$

unique up to k-isomorphism, where the three groups are split over k, $\tilde{G}'$ (resp. $\bar{G}'$) is simply connected (resp. adjoint), G' is K-isomorphic with G, and $\tilde{\pi}', \bar{\pi}'$ are central k-isogenies. Furthermore, the isogenies $\tilde{\pi}'$ and $\bar{\pi}'$ induce monomorphisms $\tilde{\phi}\colon \mathrm{Aut}_K(G') \to \mathrm{Aut}_K(\tilde{G}')$ and $\bar{\phi}\colon \mathrm{Aut}_K(G') \to \mathrm{Aut}_K(\bar{G}')$ (where Aut_K means "the group of K-automorphisms"). The group G can be identified with G' twisted by a cocycle α of Γ with values in $\mathrm{Aut}_K(G')$. Twisting $\tilde{G}'$ and $\bar{G}'$ respectively by $\tilde{\phi}^*(\alpha)$ and $\bar{\phi}^*(\alpha)$ we obtain the desired groups $\tilde{G}$ and $\bar{G}$. The unicity—that is, the fact that $\tilde{G}$ and $\bar{G}$ are necessarily obtained in that way—follows immediately from the unicity of the sequence $\tilde{G}' \to G' \to \bar{G}'$ and the injectivity of $\tilde{\phi}$ and $\bar{\phi}$, since $\tilde{G}$ and $\bar{G}$ are split over K by Grothendieck's theorem ([**4**, §2.14], [**9**]) (*a posteriori*, the proposition shows that $\tilde{G}$ and $\bar{G}$ split over every splitting field of G).

2.6.2. *Definitions.* The groups $\tilde{G}$ and $\bar{G}$ of the preceding proposition will be called respectively the *simply connected covering* and the *adjoint group* of G.

Two groups will be said (*strictly*) *isogenous over k or k-isogenous* if all the groups and (central) isogenies which occur in the definition of §1.2.1 are defined over k.

2.6.3. PROPOSITION 3. *If two semisimple groups defined over k are strictly k-isogenous, their indices are isomorphic and their anisotropic kernels and anisotropic semisimple kernels are strictly k-isogenous.*

PROOF. It follows from the definition of the strict isogeny and from Proposition 2 that the simply connected coverings of the two groups are k-isomorphic. Therefore we may assume, without loss of generality, that the two groups in question are G and its simply connected covering $\tilde{G}$. Besides the general conventions of §2.1, we keep the notations of the proof of Proposition 2, and we denote by $\tilde{T}'$ a maximal k-split torus of $\tilde{G}'$, and by T' its image in G'. Since all maximal K-tori of G are conjugate over K, we can assume, without loss of generality, that the cocycle α has value in the normalizer of T' in $\mathrm{Aut}_K(G')$, and that T' twisted by α coincides with T. But then, $\tilde{\phi}^*(\alpha)$ has values in the normalizer of $\tilde{T}'$ in $\mathrm{Aut}_K(\tilde{G}')$, and the torus $\tilde{T}'$ twisted by $\tilde{\phi}^*(\alpha)$ is a maximal k-torus $\tilde{T}$ of $\tilde{G}$, whose projection in G is T. Let $\tilde{S}$ be the maximal k-split subtorus of $\tilde{T}$. Since $\tilde{\pi}$ is an isogeny, $\tilde{\pi}(\tilde{S}) = S$. The torus $\tilde{S}$ is a maximal split torus of $\tilde{G}$, otherwise, it would be contained in a bigger split torus $\tilde{S}_1$ and $\tilde{\pi}(\tilde{S}_1)$ would be a split torus containing properly S. The proposition is now an immediate consequence of the fact that the roots of $\tilde{G}$ with respect to $\tilde{S}$ are the image by $\tilde{\pi}^*$ of the roots of G with respect to S, and that $\tilde{\pi}(\mathscr{Z}(\tilde{S})) = \mathscr{Z}(S)$.

2.6.4. REMARK. There may exist k-isogenous groups with different k-ranks, and *a fortiori* different indices. Example: if k is a field of characteristic 2 and if Q is a nondegenerate quadratic form in three variables, with defect 1, which does not represent 0 (the existence of such a form implies that k is not perfect) the groups SL_2 and $\mathrm{O}_3(Q)$ are k-isogenous and their relative ranks are respectively 1 and 0. (The proofs of these statements are essentially found in [**4**, §4.26], although the explicit example given there is incorrect, since the quadratic form Q which is written down obviously represents 0.)

2.7. *A Witt-type theorem for the semisimple groups* ([**27**], [**38**], [**40**]).

2.7.1. THEOREM 2. *A semisimple group G defined over k is determined up to k-isomorphism by its K-isomorphism class, its index and its semisimple anisotropic kernel. More precisely, let G' be another group defined over k, let G_0 and G'_0 be the semisimple anisotropic kernels of G and G', and assume that there exists an isomorphism ι of the index of G on the index of G' which is induced by a K-isomorphism of G on G', and whose restriction to the index of G_0 (cf. last paragraph of* §2.3) *is induced by a k-isomorphism of G_0 on G'_0. Then, ι is also induced by a k-isomorphism of G on G'.*

PROOF. Let S' be a maximal k-split torus of G'. We identify G_0 (resp. G'_0) with $\mathscr{D}\mathscr{Z}(S)$ (resp. $\mathscr{D}\mathscr{Z}(S')$) and we set $T_0 = T \cap G_0$ (for the meaning of S, T, see §2.1). The hypothesis of the theorem means that there exists a K-isomorphism $\phi : G \to G'$ and a k-isomorphism $\psi : G_0 \to G'_0$ such that $\phi(S) = S'$, that ϕ is compatible with the $*$-actions of Γ on the sets of simple roots (§2.3), and that $\phi|_{G_0}$ and ψ differ only by an inner automorphism of G'_0. Since the tori $\phi(T_0)$ and $\psi(T_0)$ are both split over K, there is no loss of generality in assuming, after combining ϕ with an inner automorphism by an element of $G'_{0,K}$, that ϕ and ψ coincide on T_0 [**4**, §4.21 and §5.3]. We set $T'_0 = \phi(T_0)$ and $T' = \phi(T)$, and denote by χ the isomorphism $X^*(T) \to X^*(T')$ induced by ϕ^{-1}.

Since S' and T'_0 are defined over k, so is $T' = \mathscr{Z}(S' \cdot T'_0)$. From the assumption made, that ϕ is compatible with the *-actions of Γ, it follows that, for every $\sigma \in \Gamma$, the homomorphism $\phi^{-1}\sigma^{-1}\phi\sigma \colon X^*(T) \to X^*(T)$ is induced by an element w of the Weyl group. Since the restrictions of ϕ to T_0 and S are defined over k, w induces the identity on T_0 and S, and therefore is the identity (because $\mathscr{Z}(T_0 \cdot S) = T$). Thus, $\phi\sigma = \sigma\phi$, which means that the restriction of ϕ to T is defined over k.

The one-parameter group corresponding to a root α (of G relative to T) will be denoted by U_α. For every simple relative root $\gamma \in {}_k\Delta$, let Σ_γ (resp. $\Sigma_{2\gamma}$) be the set of all absolute roots whose restrictions to S is γ (resp. 2γ), and let $U_{(\gamma)}$ (resp. $U_{2\gamma}$) be the subgroup of G generated by the U_α with $\alpha \in \Sigma_\gamma \cup \Sigma_{2\gamma}$ (resp. $\alpha \in \Sigma_{2\gamma}$). The group $V_\gamma = U_{(\gamma)}/U_{2\gamma}$ is defined over k and has a natural structure of vector space defined over k [4, §3.17]. The torus T acts on V_γ (through its action on $U_{(\gamma)}$ by inner automorphisms), this representation of T in V_γ is defined over k and its weights are the elements of Σ_γ. Similarly, $V'_\gamma = \phi(U_{(\gamma)})/\phi(U_{2\gamma})$ is a vector space defined over k on which T' acts, the weights of this action being the elements of $\chi(\Sigma_\gamma)$. It is now easy to show—we leave it to the reader—that there exists a vector space isomorphism $\tau_\gamma \colon V_\gamma \to V'_\gamma$, defined over k which is compatible with the actions of T and T' and the isomorphism $\phi|_T \colon T \to T'$. For each $\gamma \in {}_k\Delta$ we choose such a τ_γ.

For every simple root $\alpha \in \Delta$, let $\bar{\phi}_\alpha \colon U_\alpha \to U_{\chi(\alpha)}$ be the K-isomorphism defined as follows. If $\alpha \in \Delta_0$, $\bar{\phi}_\alpha$ is the restriction of ψ to U_α, and if the restriction of α to S is γ, $\bar{\phi}_\alpha$ is the unique homomorphism which makes the diagram

$$\begin{tikzcd}
U_\alpha \arrow[r, "\bar{\phi}_\alpha"] \arrow[d] & U_{\chi(\alpha)} \arrow[d] \\
V_\gamma \arrow[r, "\tau_\gamma"] & V'_\gamma
\end{tikzcd}$$

commutative (the vertical arrows are the natural projections; they are injective). It follows from the proof of Theorem 2.13 in [4], that there exists a unique K-isomorphism $\bar{\phi} \colon G \to G'$ whose restrictions to the U_α's and T coincide respectively with $\bar{\phi}_\alpha$ and $\phi|_T$. We claim that $\bar{\phi}$ is in fact a k-isomorphism. To prove this, it suffices to show that $\bar{\phi}_K \colon G_K \to G'_K$ is compatible with the action of Γ. But it follows immediately from the way $\bar{\phi}_\alpha$ has been obtained and from the fact that $\phi|_T$ is defined over k, that the restriction of $\bar{\phi}_K$ to the $U_{\alpha,K}$'s and to T_K are compatible with the action of Γ. In other words, if $\sigma \in \Gamma$, the homomorphisms $\bar{\phi}_K$ and $\sigma^{-1}\bar{\phi}_K\sigma$ coincide on $U_{\alpha,K}$ and T_K. Since $\sigma^{-1}\bar{\phi}_K\sigma$ is the restriction to G_K of a K-isomorphism $G \to G'$, it follows from the unicity of $\bar{\phi}$ that $\sigma^{-1}\bar{\phi}_K\sigma = \bar{\phi}_K$, which finishes the proof.

2.7.2. Remarks. (a) The group G is already determined, up to k-isomorphism, by its K-isomorphism class, its index and its semisimple anisotropic kernel, *given up to k-isogeny*. More precisely, it would suffice, in the statement of the theorem, to assume that the restriction of ι to the index of the semisimple anisotropic kernel of G is induced by a k-isogeny. Indeed, this isogeny is then automatically an isomorphism, as a result of the fact that ι is induced by an *isomorphism* of G.

(b) The group G is determined up to *strict k-isogeny* by its strict K-isogeny class, its index and the k-isogeny class of its semisimple anisotropic kernel. This is an immediate consequence of the preceding theorem and the Propositions 2 and 3.

(c) The reader will have no difficulty to state for the reductive groups a theorem analogous to Theorem 2.

(d) There is a trivial but sometimes useful generalization of the Theorem 2, which we want to mention. Let S' be any k-split torus in G, let Δ' be the set of simple roots of G with respect to some maximal torus T' containing S' and some ordering of $X^*(T')$ compatible with an ordering of $X^*(S')$, and let Δ'_0 be the set of simple roots vanishing on S'. Exactly as in §2.3, we can define the $*$-action of Γ on Δ'. Let us call partial index (relative to S') the data consisting of Δ' (together with the Dynkin diagram), Δ'_0 and the $*$-action of Γ on Δ'. Then, in the statement of §2.7.1, one can replace the index and the semisimple anisotropic kernel respectively by the partial index relative to some k-split torus S' and the "corresponding semisimple kernel" $\mathscr{D}\mathscr{Z}(S')$ (which is still defined over k, but is no longer anisotropic in general).

3. **Classification.** According to the Theorem 2, the problem of classifying the semisimple algebraic groups over a given field k can be decomposed into two steps which can roughly be formulated as follows:

(1) Find all admissible indices of semisimple groups over k;

(2) For a given index, find all possible semisimple anisotropic kernels.

These two questions will be discussed here. However, we shall not consider the problem of classifying all anisotropic groups over k, which theoretically falls under (2) and is usually by far the most difficult part of the classification problem.

3.1. *Preliminary reductions.*

3.1.1. *Reduction to the simply connected (or to the adjoint) case.* Let there be given a simply connected group $\tilde{G}$ defined over k, a group G' defined over K and a central K-isogeny $\pi' : \tilde{G} \to G'$. Under which condition does G' admit a k-structure such that π' becomes a k-isogeny? More correctly, under which condition does there exist a group G, defined over k, and an isomorphism $f: G' \to G$ such that $f \circ \pi'$ is a k-isogeny? The answer is easy to formulate in terms of the index of G: Following §1.5, we can associate to $\tilde{G}$ a finite group $C(\tilde{G}) = C$ and the isogeny π' is then characterized up to equivalence by a subgroup C' of C (the kernel of the homomorphism $C \to C(G')$ induced by π'). Through its $*$-action on the Dynkin diagram of G, the Galois group operates on C, by §1.5.3 (2). Then:

The group G exists if and only if C' is invariant by Γ. In that case, G is unique up to isomorphism (more precisely, given two solutions $f: G' \to G$ and $f_1 : G' \to G_1$ of the above problem, there exists a k-isomorphism $\phi : G \to G_1$ such that $f_1 = \phi \circ f$).

The proof of this assertion, which goes along the line of §2.6.1, is quite easy and will not be developed here.

Notice that the condition imposed on C' is automatically satisfied when G' is an adjoint group ($C' = C$). The classification of adjoint groups over k is therefore completely equivalent with the classification of simply connected groups.

3.1.2. *Reduction to the absolutely simple case.* Let k' be a field such that $k \subset k' \subset K$, let $\Lambda = \mathrm{Gal}(K/k')$, let H be a semisimple group defined over k' which splits over K, and let $G = R_{k'/k}(H)$ be the group obtained from H by *restriction of the scalar field* from k' to k. (We shall not give here the definition of the functor $R_{k'/k}$, which can be found in [**4**]; let us just indicate that it is the algebro-geometrical analogue of the process of going over from a complex manifold to the underlying real manifold, and that the dimension of G is that of H multiplied by $[k' : k]$).

The k-index of G can be deduced as follows from the k'-index of H:$\mathscr{E}$ denoting the Dynkin diagram of H, let $\mathscr{D}$ be the disjoint union of $[k' : k]$ copies of $\mathscr{E}$ indexed by the elements of Γ/Λ; identify the copy indexed by Λ/Λ with $\mathscr{E}$ itself; let Γ operate on $\mathscr{D}$ in such a way that Γ permutes the copies of $\mathscr{E}$ in agreement with the natural action of Γ on Γ/Λ, and so that the restriction of the action of Γ on $\mathscr{D}$ to Λ and $\mathscr{E}$ coincides with the *-action of Λ on $\mathscr{E}$; finally, distinguish in $\mathscr{D}$ the vertices of $\mathscr{E}$ which are distinguished in the k'-index of H and all their transformed elements of Γ.

If H_0 denotes the semisimple anisotropic kernel of H (over k'), the semisimple anisotropic kernel of G is $R_{k'/k}(H_0)$.

The reduction announced in the title of this section is now achieved by the following proposition.

Every semisimple simply connected group defined over k is in a unique way a direct product of almost k-simple simply connected groups (*a group is almost k-simple if it has no infinite normal subgroup defined over k*). *If G is almost k-simple and simply connected, there exists a field k′ and an* (*absolutely*) *almost simple simply connected group H defined over k′, such that* $G \cong_k R_{k'/k}(H)$.

In that proposition, "simply connected" may be everywhere replaced by "adjoint," in which case, the "almost" can be dropped.

3.2. *Some necessary conditions* (*independent of the ground field*) *for the admissibility of indices* ([**4**], [**38**], [**40**]).

3.2.1. *Self-opposition. The index of a group G is invariant under the opposition involution i* (that is, i commutes with the *-action of Γ, and leaves invariant Δ_0).

3.2.2. *An induction process. If, from the index of a group G, one removes a distinguished orbit* $\mathscr{O}$ (*together with all strokes which have at least one endpoint in* $\mathscr{O}$), *the result is again an admissible index.* (It is the index of the group $\mathscr{D}\mathscr{Z}(S')$ where S' is the connected component of the intersection of the kernels of all relative simple roots which do not correspond to $\mathscr{O}$.) This, together with §3.2.1, provides an inductive process to exclude many indices from admissibility.

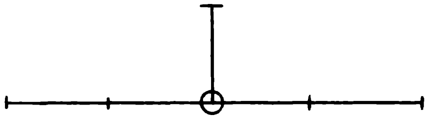
EXAMPLE. Consider an index whose underlying Dynkin diagram $\mathscr{D}$ is of type A_n and such that the *-action of Γ on this diagram is trivial. The vertices of $\mathscr{D}$

being given the natural ordering from 1 to n (see Table I), let $a_1 < a_2 < \cdots < a_r$ be the distinguished vertices. Then, one has $a_i = i \cdot (n + 1)/(r + 1)$. The proof goes by induction on r. When $r = 1$, the statement follows from §3.2.1. Assume now that $r > 1$. The assertion above for $\mathcal{O} = \{a_r\}$ implies, by virtue of the induction hypothesis, that $a_i = i \cdot a_r/r$. Similarly, for $\mathcal{O} = \{a_{r-1}\}$, we have

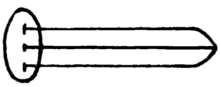
$$a_r - a_{r-1} = n + 1 - a_r.$$

These two relations imply the statement.

3.2.3. Other admissibility conditions for indices may be deduced from the formulae in §§2.5.2 and 2.5.3, which must lead to actual root systems and Weyl groups. For instance, the numbers $m_{\gamma\delta}$ of §2.5.3 must be integers, equal to 2, 3, 4 or 6, and the integer n of §2.5.2 must be $\leqq 2$. This last condition excludes such indices as



or



3.3. *Further admissibility conditions, for various special ground fields.*

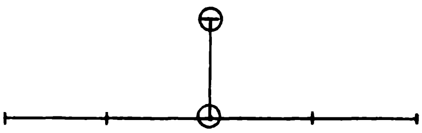
3.3.1. *Finite fields* ([**20**], [**31**], [**33**], [**43**]). If the ground field k is finite $\Delta_0 = \emptyset$; in other words every orbit of Γ in Δ is distinguished. This holds, more generally, whenever the cohomological dimension of k is 1.

3.3.2. *Real numbers* ([**17**], [**18**], [**26**], [**40**]). Let $k = \boldsymbol{R}$ and $K = \boldsymbol{C}$. Then, if G is anisotropic, the unique nonneutral element of Γ operates on the Dynkin diagram by the opposition involution.

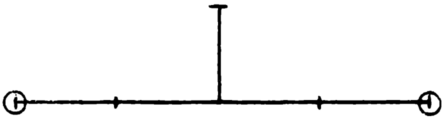
3.3.3. $\mathfrak{p}$-*adics* ([**23**], [**45**]). Let k be the field of $\mathfrak{p}$-adic numbers (for some $\mathfrak{p}$). Then, a group G which is anisotropic and absolutely almost simple is of inner type A_n (§2.3).

Notice that the two preceding statements give admissibility criterions (over the reals and the $\mathfrak{p}$-adics) for arbitrary diagrams, since the removal of all distinguished vertices from an admissible diagram must give rise to an admissible "anisotropic diagram" (in the $\mathfrak{p}$-adic case, one must occasionally also make use of the reduction of §3.1.2).

EXAMPLE. The index



cannot occur over the reals (whereas it does over the $\mathfrak{p}$-adics) and the index



cannot occur over the p-adics (whereas it does over the reals).

3.3.4. *Number fields* ([**1**], [**19**]). By means of the "Hasse principle," one can also use §§3.3.2 and 3.3.3 to exclude certain indices in the case of number fields.

All admissibility conditions stated in §3.3 are *necessary* conditions. Only in the first case (finite fields) are they also sufficient ([**20**], [**31**], [**33**], [**43**]). A complete list of all effectively admissible indices over the various types of fields considered here is given in Table II.

3.4. *Necessary and sufficient conditions on the anisotropic kernel* ([**30**], [**31**], [**38**]).

3.4.1. *Statement of the problem*; *notations*. The problem we want to study is the following:

Given an index $\mathscr{I}$, consisting of a Dynkin diagram $\mathscr{D}$, an action of $\Gamma = \mathrm{Gal}(K/k)$ *on $\mathscr{D}$ and a set Δ_0, invariant by Γ, of vertices of $\mathscr{D}$ (the nondistinguished vertices), and given a group A, defined and anisotropic over k, whose index $\mathscr{I}_0$ is (modulo a preassigned identification) the subindex of $\mathscr{I}$ having Δ_0 as set of vertices, then under which condition does there exist a group G, defined over k, with index $\mathscr{I}$, whose semisimple anisotropic kernel is strictly isogenous to A, the isogeny being compatible with the given injection $\mathscr{I}_0 \to \mathscr{I}$?*

(Concerning the fact that we want A to be the kernel only up to strict isogeny, see §§2.7.2(b) and 3.1.1.) There is no loss of generality in assuming—which we shall do—that the group A is simply connected.

We call $\mathscr{D}_0$ the underlying Dynkin diagram of $\mathscr{I}_0$ (that is, the subdiagram of $\mathscr{D}$ whose set of vertices is Δ_0), G^d a semisimple adjoint k-split group whose Dynkin diagram is $\mathscr{D}$ (after preassigned identification), G^q a semisimple adjoint k-quasi-split group whose diagram is $\mathscr{D}$ and such that the *-action of Γ on $\mathscr{D}$ is the one given by $\mathscr{I}$, T^d a maximal k-split torus of G^d, and T^q a maximal k-torus of G^q containing a maximal k-split torus T^{qd}. We choose orderings in the character groups $X^*(T^d)$ and $X^*(T^q)$, the ordering in $X^*(T^q)$ being compatible with an ordering in $X^*(T^{qd})$. The simple roots with respect to these orderings are in canonical 1–1 correspondence with the vertices of $\mathscr{D}$, and will usually be represented by the same letters. We denote by S^d (resp. S^q) the connected component of the subgroup of T^d (resp. T^q) defined by the equations (1) of §2.5.1.

In view of the various identifications which have been made, both the groups $G_0^d = \mathscr{D}\mathscr{Z}(S^d)$ and $G_0^q = \mathscr{D}\mathscr{Z}(S^q)$ have $\mathscr{D}_0$ as Dynkin diagrams. In particular, they are strictly isogenous to A. Furthermore, the *-operation of Γ on $\mathscr{D}_0$ is the same for the two groups G_0^q and A. From all this, it follows that the group A can be viewed, either as the simply connected covering $\tilde{G}_0^d$ of G_0^d twisted by a 1-cocycle τ^d of Γ with values in $\mathrm{Aut}_K(\tilde{G}_0^d)$, or as $\tilde{G}_0^q$ twisted by a 1-cocycle τ^q of Γ with values in $\mathrm{Int}_K(\tilde{G}_0^q) = \bar{G}^q_{0,K}$; here, Aut_K (resp. Int_K) denotes the group of K-automorphisms (resp. the group of inner K-automorphisms), and $\bar{G}_0^q$ is the adjoint group of G_0^q.

3.4.2. *Cohomological formulation of the condition.* An operation of Γ on the Dynkin diagram $\mathscr{D}$ being given, to each element of Γ is associated a coset of $\mathrm{Aut}(G^d)$ modulo $\mathrm{Int}(G^d)$ (§1.5.6); we shall say that a 1-cocycle of Γ in a subgroup of $\mathrm{Aut}_K(G^d)$ is *compatible* with the action of Γ on $\mathscr{D}$ if it sends each element of Γ in the corresponding coset. If H denotes an algebraic group defined over k, two 1-cocycle τ, τ' of Γ with values in $\mathrm{Aut}_K(H)$ will be called *innerly cohomologous*, if there is an element c of $\mathrm{Int}_K(H)$ such that $\tau'(\gamma) = c^{-1} \cdot \tau(\gamma) \cdot \gamma(c)$ for every $\gamma \in \Gamma$.

PROPOSITION 4. *Let B_K be the centralizer of S^d in $\mathrm{Aut}_K(G^d)$. Then, each one of the following two conditions is necessary and sufficient for the existence of the group* G (§3.4.1).

(i) *The cocycle τ^d is innerly cohomologous with a cocycle of the form $\phi^*(\tau)$, where $\tau \in Z^1(\Gamma, B_K)$ is a cocycle of Γ, with values in B_K, compatible with the given action of Γ on $\mathscr{D}$, and where $\phi^* : Z^1(\Gamma, B_K) \to Z^1(\Gamma, \mathrm{Aut}_K(\tilde{G}_0^d))$ denotes the mapping of* 1-*cocycle sets induced by the homomorphism $B_K \to \mathrm{Aut}_K(\tilde{G}_0^d)$, composed of the restriction homomorphism $B_K \to \mathrm{Aut}_K(G_0^d)$ and the natural injection $\mathrm{Aut}_K(G_0^d) \to \mathrm{Aut}_K(\tilde{G}_0^d)$.*

(ii) *The cohomology class of the cocycle τ^q belongs to the image of the homomorphism $H^1(\Gamma, \mathscr{Z}(S^q)_K) \to H^1(\Gamma, \bar{G}^q_{0,K})$ induced by the natural projection*

$$\mathscr{Z}(S^q)_K \to \bar{G}^q_{0,K}$$

(here, $\mathscr{Z}$ stands for "centralizer in G^q"; notice that $\bar{G}_0^q$ is the quotient of $\mathscr{Z}(S^q)$ by its center).

PROOF. If the condition (i) is satisfied, the group G^d twisted by the cocycle τ has all the properties required from G. Conversely, suppose that G exists. By §2.6.1 we can assume, without loss of generality, that G is an adjoint group. Let S be a maximal k-split torus of G. From the assumptions made on G and the definition of S^d, it follows that there exists a K-isomorphism $\phi: G \to G^d$, compatible with the given identification of the Dynkin diagrams of G^d and G, and such that $\phi(S) = S^d$. Then, the cocycle τ defined by $\tau(\gamma) = \gamma(\phi) \circ \phi^{-1}$ has the properties required in the condition (i).

The proof for condition (ii) is similar.

3.4.3. *Linear representations: terminology, notations.* In the next proposition, we want to interpret the condition (i) of §3.4.2 as an existence condition for certain linear representations of A defined over k.

Let $\{\rho_i : A \to \mathrm{GL}(V_i) | i \in I\}$ be a finite set of linear representations of A defined over K, and let there be given a permutation action of Γ on this set, or, what amounts to the same, on the set of indices I. Then, we shall say that the representation $\oplus\rho_i$, together with the given action of Γ, is Γ-*equivalent* to a representation $\rho: A \to \mathrm{GL}(V)$ defined over k, if there exists a K-isomorphism $\psi: \oplus V_i \to V$ such that ρ is the composed homomorphism $A \to \mathrm{GL}(\oplus V_i) \to \mathrm{GL}(V)$ (where the first arrow is $\oplus\rho_i$ and the second one is induced by ψ), and such that, for all $\gamma \in \Gamma$ and all $i \in I$, $\gamma(\psi(V_i)) = \psi(V_{\gamma(i)})$. If the action of Γ on I is trivial, this simply means that each ρ_i is equivalent to a representation defined over k.

We choose once and for all a K-isomorphism $\phi: A \to \tilde{G}_0^d$. Given a linear representation $\rho: G_0^d \to \mathrm{GL}(V)$ of G_0^d, we shall denote by the same symbol ρ this representation lifted to $\tilde{G}_0^d$ (that is, composed with the canonical isogeny $\tilde{G}_0^d \to G_0^d$), and also the representation $\rho \circ \phi$ of A. A representation of A obtained in that fashion will be said to *factorize through* G_0^d; if $\rho: G_0^d \to \mathrm{GL}(V)$ is an isomorphism of G_0^d on a subgroup of $\mathrm{GL}(V)$, we shall say that $\rho: A \to \mathrm{GL}(V)$ *factorizes through a faithful representation* of G_0^d (at this point, it should perhaps be recalled that G_0^d is *the* isogenous image of A which is imbedded in the *adjoint* group G^d).

Let Δ stand here for the set of all simple roots of G^d, and let Ω be the set of all integral linear combinations ω of elements of Δ such that $\beta^*(\omega) \geqq 0$ for all $\beta \in \Delta_0$. For every $\omega \in \Omega$, the restriction of ω to $T_0^d = T^d \cap G_0^d$, is the dominant weight of a certain irreducible representation of G_0^d defined over k.[1] This representation, and the corresponding representations of $\tilde{G}_0^d$ and A, will be denoted by ρ_ω. It is customary to characterize an equivalence class of irreducible representations of a split group by a set of nonnegative integers attached to the simple roots, namely the "normal coordinates" of the dominant weight (see for instance [**4**, §12.2]). For the representation ρ_ω, these numbers are $\beta^*(\omega)$. Particularly important is the case where $\omega \in \Delta' = (\Delta - \Delta_0) \cup \{-\mu\}$ (where $-\mu$ is the dominant root of G^d); these integers are then immediately read on the affine Dynkin diagram $\mathscr{D}'$.

The action of Γ on Δ given by $\mathscr{I}$ induces an action of Γ on Ω; it is this action which the following proposition refers to

3.4.4. *Representation-theoretical formulation of the condition.*

Proposition 5. *Let Ω' be a finite subset of Ω invariant by Γ. Then, a necessary condition for the existence of the group G is that the sum of the representations $\rho_\omega(\omega \in \Omega')$, together with the given action of Γ on Ω', be Γ-equivalent with a representation of A defined over k. If $\Omega' = \Delta - \Delta_0$, this condition is also sufficient.*

Corollary 1. *A necessary condition for the existence of G is that the representation $\rho_{-\mu}$ (where $-\mu$ denotes the dominant root of G^d) be equivalent with a representation defined over k.*

We shall only briefly sketch the

Proof of Proposition 5. The following notations will be used: V_ω is the vector space over k in which the representation $\rho_\omega: G_0^d$ (or $\tilde{G}_0^d$, or A) $\to \mathrm{GL}(V_\omega)$ is given,

$$V = \oplus_{\Omega'} V_\omega, \rho = \oplus_{\Omega'} \rho_\omega : G_0^d \to \mathrm{GL}(V),$$

$\hat{\Gamma}$ is the image of Γ by the homomorphism $\Gamma \to \mathrm{Aut}(\mathscr{D})$ given by $\mathscr{I}$, B is the centralizer of S^d in the algebraic group $\mathrm{Aut}(G^d)$, and $\hat{B}$ is the inverse image of $\hat{\Gamma}$ by the natural homomorphism $B \to \mathrm{Aut}(\mathscr{D})$ (§1.5.6). The group $\hat{B}$ is (over K) the semidirect product of $\hat{B}^0 = \mathscr{Z}(S^d)$ (centralizer in G^d) and a finite group canonically

[1] The author has been told—but has not verified—that the theory of linear representations developed in [7] in the algebraically closed case works equally well for split groups over arbitrary fields. If the reader is not willing to accept this fact, he may feel safer in assuming, from now on, that char $k = 0$; however, this restriction is undoubtedly much too strong since all results obtained here may already be established—by somewhat more complicated arguments—in the framework of the classical representation theory, provided the characteristic of k is "not too small" ($\neq 2, 3$ and possibly 5).

isomorphic with $\hat{\Gamma}$; we choose, once and for all, such a semidirect decomposition of $\hat{B}$ and identify the finite group in question with $\hat{\Gamma}$ itself.

We now extend ρ to a representation $\hat{\rho}: \hat{B} \to \mathrm{GL}(V)$ such that $\hat{\rho}(\gamma)(V_\omega) = V_{\gamma(\omega)}$ for every $\gamma \in \hat{\Gamma}$ (notice that, as a subgroup of $\mathrm{Aut}(\mathscr{D})$, $\hat{\Gamma}$ operates on Δ, and therefore also on Ω'). This is done as follows: First extend ρ to a representation

$$\hat{\rho}^0 : \hat{B}^0 \to \mathrm{GL}(V)$$

by imposing that, for every element t of the center of $\hat{B}^0$, $\hat{\rho}^0(t)$ leaves invariant each V_ω and induces on V_ω the scalar multiplication by $\omega(t)$ (this expression has a meaning since $t \in T^d$); then, choose in each V_ω an eigenvector v_ω belonging to the dominant weight; finally, notice that, in view of the unicity of the representation with a given dominant weight and because of Schur's lemma, $\hat{\rho}^0$ extends uniquely to a representation $\hat{\rho}$ of $\hat{B}$ such that $\hat{\rho}(\gamma)(v_\omega) = v_{\gamma(\omega)}$ for all $\gamma \in \hat{\Gamma}$ and all $\omega \in \Omega'$.

Now, assume that the group G exists. Then, there exists a 1-cocycle $\tau \in Z^1(\Gamma, B_K)$ satisfying the condition (i) of §3.4.2. The compatibility of τ with the action of Γ on $\mathscr{D}$ implies that $\tau \in Z^1(\Gamma, \hat{B}_K)$. But we have defined an action of $\hat{B}_K$ on the object $(\tilde{G}_0^d, V, \rho)$ ($\hat{B}_K$ operates on $\tilde{G}^d$ by the lifting of restrictions of inner automorphisms, and on V through $\hat{\rho}$). We can therefore twist that object by τ, and we obtain that way the representation of A (more precisely, of a group k-isomorphic with A) whose existence we had to establish.

Conversely, suppose that $\Omega' = \Delta - \Delta_0$, and that the condition stated is satisfied. This condition means that there exists a representation $\rho' : A \to \mathrm{GL}(V')$ of A defined over k, having certain properties which we do not repeat here. The two objects (A, V', ρ') and $(\tilde{G}_0^d, V, \rho)$ are K-isomorphic; therefore, the first one is isomorphic with the second one twisted by a cocycle τ' of Γ with values in $\mathrm{Aut}_K(\tilde{G}_0^d, V, \rho)$. But it is easy to see that, in the special case considered here (that is, the case where $\Omega' = \Delta - \Delta_0$), the group $\hat{B}^0$ is canonically isomorphic (through the natural action of $\hat{B}^0$ on $\tilde{G}_0^d$ and the representation $\hat{\rho}^0$) with the group of all automorphisms of the object $(\tilde{G}_0^d, V_\omega, \rho_\omega(\omega \in \Omega'))$. As a consequence, the action considered above of $\hat{B}_K$ on $(\tilde{G}_0^d, V, \rho)$ defines an injection of $\hat{B}_K$ in $\mathrm{Aut}_K(\tilde{G}_0^d, V, \rho)$. Furthermore, the conditions imposed on the representation ρ' imply that the cocycle τ' has values in the image of $\hat{B}_K$ by this injection; lifting it to $\hat{B}_K$, we obtain a cocycle $\tau \in Z^1(\Gamma, \hat{B}_K)$ satisfying the condition (i) of §3.4.2, and the group G exists by Proposition 4.

3.4.5. *The case of inner forms.* When the action of Γ on $\mathscr{D}$ given by $\mathscr{I}$ is trivial, the Propositions 4 and 5 can be given a much simpler and (for the second one) more general form. Notice that in that case, there is no difference between G^d and G^q, and that we can set $\tau^d = \tau^q$, which is now a 1-cocycle with values in $\bar{G}_{0,K}^d$ (where the bar means, as before, "adjoint group").

PROPOSITION 6. *Assume that Γ operates trivially on $\mathscr{D}$. Then, the group G exists if and only if the cohomology class of τ^d in $H^1(\Gamma, \bar{G}_{0,K}^d)$ belongs to the image of the homomorphism $H^1(\Gamma, G_{0,K}^d) \to H^1(\Gamma, \bar{G}_{0,K}^d)$ induced by the canonical projection.*

PROOF. Setting $S_1 = S^d/(S^d \cap G_0^d)$ (where the intersection must be understood in the set theoretical sense), we have a short exact sequence

$$\{1\} \to G^d_{0,K} \to \mathscr{Z}(S^d)_K \to S_{1,K} \to \{1\}.$$

(Notice that there is a purely inseparable extension $S_1 \to \mathscr{Z}(S^d)/G^d_0$, which is not always an isomorphism.) Since S_1 is a k-split torus, we have, by Hilbert Theorem 90, $H^1(\Gamma, S_{1,K}) = \{0\}$. Now, it follows from the cohomology sequence associated with the above exact sequence that the homomorphism

$$H^1(\Gamma, G^d_{0,K}) \to H^1(\Gamma, \mathscr{Z}(S^d)_K)$$

induced by the inclusion is surjective. Our proposition is then an immediate consequence of the second part of Proposition 4.

PROPOSITION 7. *Assume that* Γ *operates trivially on* $\mathscr{D}$. *Let* ρ *be any irreducible linear representation of* A *defined over* K *which factorizes through* G^d_0; *then, a necessary condition for the existence of the group* G *is that* ρ *be equivalent with a representation of* A *defined over* k. *Let* $\{\rho_i\}$ *be a set of irreducible linear representations of* A *defined over* K *whose direct sum factorizes through a faithful representation of* G^d_0 (§3.4.3); *then, a necessary and sufficient condition for the existence of* G *is that each* ρ_i *be equivalent with a representation of* A *defined over* k.

PROOF. We may assume that ρ *considered as a representation of* G^d_0, is defined over k. Let V be the vector space over k in which this representation is made. If the group G exists, the Proposition 6 shows that we can find a 1-cocycle $\tau \in Z^1(\Gamma, G^d_{0,K})$ whose image in $Z^1(\Gamma, \bar{G}^d_{0,K})$ is cohomologous with τ^d. Twisting the object $(\tilde{G}^d_0, V, \rho)$ (on which $\bar{G}^d_{0,K}$ operates in the obvious way) by this cocycle τ, we obtain the representation of A searched for.

We now pass to the proof of the second part of the proposition, and first make an assumption similar to the one above, namely that the $\rho_i : G^d_0 \to \mathrm{GL}(V_i)$ are representations defined over k. Let H be the connected component of the (algebraic) group of automorphisms of the object $(\tilde{G}^d_0, \{V_i\}, \{\rho_i\})$. Assume that each ρ_i, considered as a representation of A, is equivalent with a representation $\rho'_i : A \to \mathrm{GL}(V'_i)$ defined over k. Then, the object $(A, \{V'_i\}, \{\rho'_i\})$ is isomorphic with the object $(\tilde{G}^d_0, \{V_i\}, \{\rho_i\})$ twisted by a certain 1-cocycle in $Z^1(\Gamma, H_K)$ whose image in $\bar{G}^d_{0,K}$ (by the obvious homomorphism $H \to \bar{G}^d_0$) is cohomologous to τ^d; in particular, the cohomology class of τ^d belongs to the image of the homomorphism $H^1(\Gamma, H_K) \to H^1(\Gamma, \bar{G}^d_{0,K})$. On the other hand, if $\oplus\rho_i$ is a faithful representation of G^d_0, there is a natural injection $G^d_0 \to H$ (the group G^d_0 operates on $\tilde{G}^d_0$ by lifting of inner automorphisms, and on V_i through ρ_i) and H is an almost direct product (i.e. a direct product up to central isogeny) of G^d_0 and a k-split torus. Then, exactly by the same argument as in the proof of Proposition 6, one shows that the homomorphism $H^1(\Gamma, G^d_{0,K}) \to H^1(\Gamma, H_K)$ is surjective. Therefore, the cohomology class of τ^d belongs to the image of the homomorphism $H^1(\Gamma, G^d_{0,K}) \to H^1(\Gamma, \bar{G}^d_{0,K})$, and it follows from the preceding proposition that G exists.

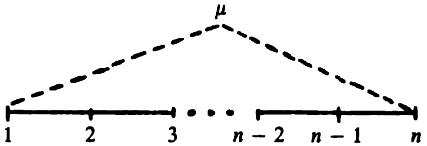
3.4.6. REMARK. In §3.4, we have always assumed that the group A was anisotropic; however, everything which has been said generalizes immediately to the (slightly) more general situation described in §2.7.2 (*d*).

Table I: Dynkin Diagrams

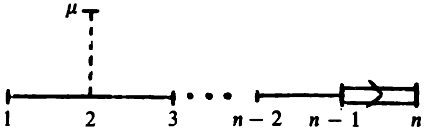
Explanations

See §§1.1 and 1.2.2. The vertex representing the minimal root is called μ; the vertices of the ordinary diagram are numbered in order to enable references.

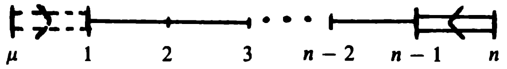
(A_n)



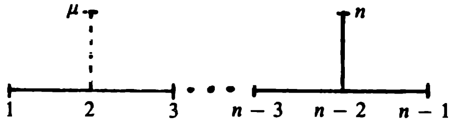
(B_n)



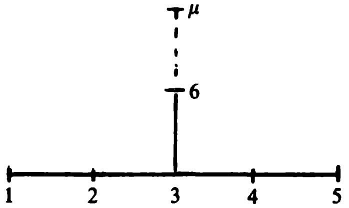
(C_n)



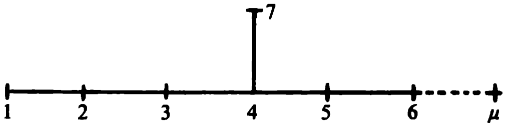
(D_n)



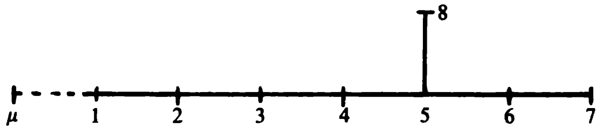
(E_6)



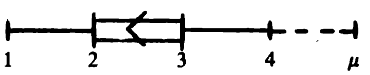
(E_7)



(E_8)



(F_4)



(G_2)

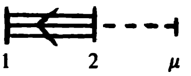


TABLE II: Indices

EXPLANATIONS

In this table, we enumerate all possible indices of absolutely simple groups (for the definition of the index and the diagrammatical representation, see §2.3; for the nonabsolutely simple case, see §3.1.2); all the indices which are listed can effectively occur over suitably chosen fields.

The letters n, r, d, a, m all denote nonnegative integers; n and r are respectively the absolute rank and the relative rank of the considered group, in other words, they are respectively equal to the total number of vertices and to the number of distinguished orbits of the diagram; in particular, they verify the relation $0 \leqq r \leqq n$; all other conditions imposed on n, r, d are stated explicitly in each case.

The numbers attached to braces always indicate the total number of *vertices* in the part of the diagram spanned by the braces in question.

In the case of the classical types, the indices cannot be drawn completely, because of the indeterminacy of the rank n; as they are represented, the pictures should be self-explanatory; however, to exclude any possibility of misinterpretation, we give separately, in those cases, the list of distinguished orbits, where we use the numbering of vertices fixed by Table I.

In order to make easier, later references to this table, we propose a notation for the various indices. In the symbol ${}^gX^t_{n,r}$, n and r are respectively the absolute and the relative rank, g denotes (as already in [43]) the order of the quotient of the Galois group Γ which operates effectively on the Dynkin diagram (in case the diagram has no nontrivial automorphism, g is necessarily $= 1$, and we omit it in the symbol) and t is a further invariant: in the case of classical types, t is the degree of a certain division algebra which occurs in the definition of the considered form, and in the case of exceptional types we have chosen as characteristic number t the dimension of the anisotropic kernel; in order to emphasize the difference between these two cases, we put t between parentheses when it stands for the degree of a division algebra. (N.B. Here, by *degree* of a central division algebra, we mean the square root of its dimension.) In the case of real forms of exceptional groups, the correspondence between our present notation ${}^g_{\boldsymbol{R}}X^t_{n,r}$ and the notation $X_{n(i)}$ introduced in [37] (where i was the Cartan "index") is given by the relation $i = r - t$.

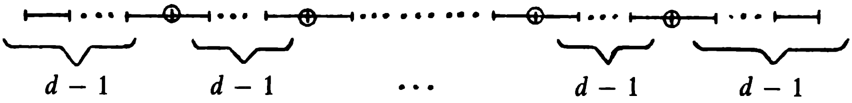
$\boldsymbol{F}$ means "finite fields," $\boldsymbol{R}$ "the field of real numbers," $\mathfrak{p}$ "p-adic fields" and $\boldsymbol{n}$ "number fields"; in the part of the table which deals with the exceptional types, "+" means "exists," and "−," "does not exist." When we say that a form exists over—say—number fields, it means that there exist number fields where the form occurs. Everything which we say about finite fields except the nonexistence of ${}^6D^2_{4,2}$, extends to an arbitrary field of cohomological dimension 1.

In the classical case, we give an "explicit" description of the groups having the various indices. Actually, we describe only one representative of each strict isogeny class; furthermore, the groups we describe are in fact abstract groups, but they are all, in a natural and rather obvious way, the groups of rational points of the algebraic groups we have in mind. The notations SL, Sp $\cdots$ are those of Dieudonné [10], except that we write SU and SO instead of U^+ and O^+. For further information concerning the classification in the classical case, see [46] (which has been extensively used to set up that part of the present table) and [25].

$[x]$ means "the largest integer $\leqq x$."

TYPE ^1A_n

$({}^1A_{n,r}^{(d)})$



Conditions: $d \cdot (r + 1) = n + 1, d \geqq 1$.

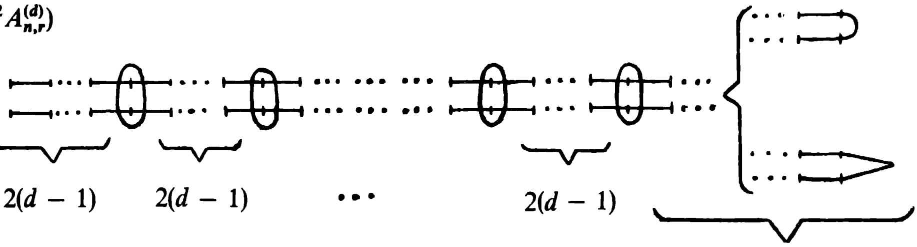
Distinguished vertices: $d, 2d, \cdots, rd$

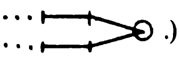
Description: Special linear group $SL_{r+1}(D)$, where D is a central division algebra of degree d over k.

Special fields: Over F, $d = 1$; over R, $d = 1$ or 2; over $\mathfrak{p}$ and $\mathfrak{n}$, d may be arbitrary.

TYPE ^2A_n

$({}^2A_{n,r}^{(d)})$



(When $n + 1 = 2rd$, the right end becomes  .)

Conditions: $d | n + 1$, $d \geqq 1$, $2rd \leqq n + 1$.

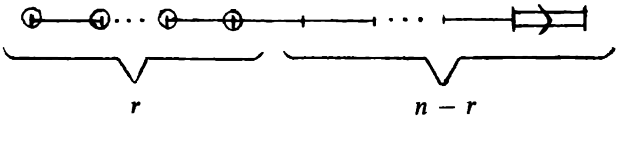
Distinguished orbits: $(d, n + 1 - d), (2d, n + 1 - 2d), \cdots, (rd, n + 1 - rd)$.

Description: Special unitary group $SU_{(n+1)/d}(D, h)$, where D is a central division algebra of degree d over a quadratic extension k' of k with an involution of the second kind σ such that $k = \{x \in k' | x^\sigma = x\}$, and h is a nondegenerate hermitian form of index r relative to σ.

Special fields: Over F, $d = 1$ and $r = [(n + 1)/2]$; over R, $d = 1$; over $\mathfrak{p}$, $d = 1$ and $n = 2r - 1$, $2r$ or $2r + 1$; over $\mathfrak{n}$, there is no special restriction on d and r.

TYPE B_n

$(B_{n,r})$



Conditions:

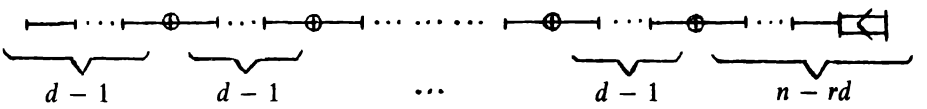
Distinguished vertices: $1, 2, \cdots, r$.

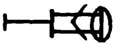
Description: Special orthogonal group $\mathrm{SO}_{2n+1}(k, q)$, where q is a quadratic form of index r, and defect 1 in case char $k = 2$.

Special fields: Over $\boldsymbol{F}$, $r = n$; over $\mathfrak{p}$, $r = n$ or $n - 1$; over $\boldsymbol{R}$ and $\boldsymbol{n}$, there is no special restriction on r.

TYPE C_n

$(C^{(d)}_{n,r})$



(When $n = rd$, the right end becomes ).

Conditions: $d = 2^a | 2n$, $d \geqq 1$; if $d = 1, n = r$.

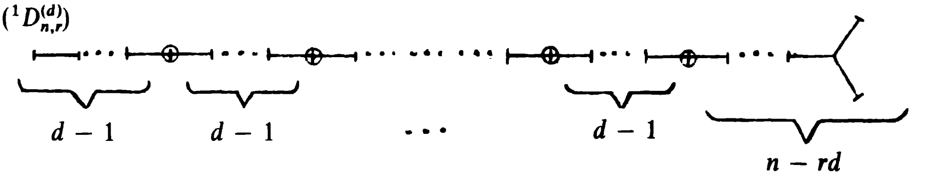
Distinguished vertices: $d, 2d, \cdots, rd$.

Description: Special unitary group $\mathrm{SU}_{2n/d}(D, h)$, where D is a division algebra of degree d over k, and h is a nondegenerate antihermitian sesquilinear form of index r relative to an involution σ of the first kind such that D^σ (the space of symmetric elements) has dimension $\frac{1}{2}d(d + 1)$. When $d = 1$, the group becomes simply $\mathrm{Sp}_{2n}(k)$. An equivalent description, when $d > 1$ and char $k \neq 2$, is: $\mathrm{SU}_{2n/d}(D, h)$, where D is as above, and h is a nondegenerate hermitian form of index r relative to an involution σ of the first kind such that $\dim D^\sigma = \frac{1}{2}d(d - 1)$.

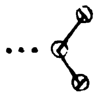
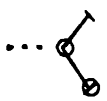
Special fields: Over $\boldsymbol{F}$, $d = 1$; over $\boldsymbol{R}$ and $\boldsymbol{n}$, $d = 1$ (and $r = n$) or $d = 2$; over $\mathfrak{p}$, $d = 1$ (and $r = n$) or $d = 2$ and $n = 2r$ or $2r - 1$.

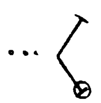
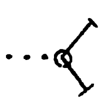
TYPE ${}^1D_n$

$({}^1D^{(d)}_{n,r})$



(When $n - rd \leqq 2$, the right end has one of the following forms:

 if $n = r, d = 1$;  if $n = 2r, d = 2$;

 if $n = rd, d \geqq 3$;  if $n = rd + 2$;

the case $n = rd + 1$ cannot occur.)

Conditions: $d = 2^a | 2n, d \geqq 1, rd \leqq n, n \neq rd + 1$.

Distinguished vertices: $d, 2d, \cdots, rd$.

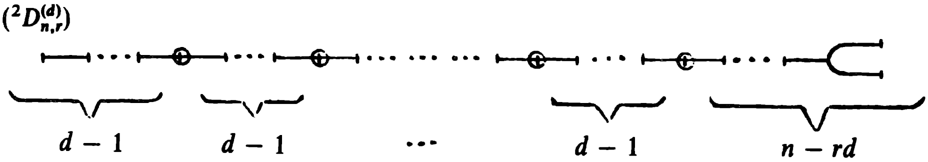
Description: If char $k \neq 2$, special unitary group $SU_{2n/d}(D, h)$, where D is a central division algebra of degree 2 over k, and h is a nondegenerate hermitian form of discriminant 1 and index r, relative to an involution σ of the first kind such that D^σ (the space of symmetric elements) has dimension $\frac{1}{2}d(d + 1)$. An equivalent description is, when $d > 1$: $SU_{2n/d}(D, h)$ where D is as above, and h is a nondegenerate antihermitian form of discriminant 1 and index r, relative to an involution σ of the first kind such that $\dim D^\sigma = \frac{1}{2}d(d - 1)$.

If char $k = 2$, "special orthogonal group" $SO_{2n/d}(D, h)$, where D is as above, and h is a nondegenerate and nondefective "quadratic form" of discriminant 1 and index r, relative to an involution of the first kind of D (with a suitable extension of the notion of quadratic form, introduced in the quaternion case by E. A. M. Seip-Hornix [**28**]).

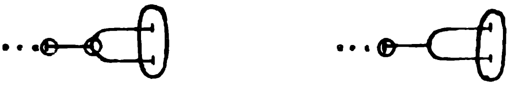
Special fields: Over F, $d = 1$ and $n = r$; over $\mathbf{R}$, $d = 1$ and $n - r = 2m$, or $d = 2$ and $n = 2r$; over p, $d = 1$ and $r = n$ or $n - 2$, or $d = 2$ and $n = 2r$ or $2r + 3$; over n, $d = 1$ and $n - r = 2m$, or $d = 2$ and $n - 2r = 2m$ or 3.

TYPE ^2D_n

$({}^2D^{(d)}_{n,r})$



(When $n = rd + 1$, which implies $d = 1$ or 2, the right end becomes respectively



.)

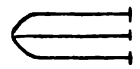
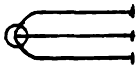
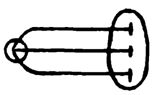
Conditions: $d = 2^a | 2n, d \geqq 1, rd \leqq n - 1$.

Distinguished orbits: $d, 2d, \cdots, rd$; the last one is replaced by $(n - 1, n)$ when $n = rd + 1$.

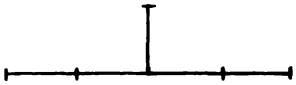
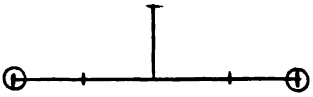
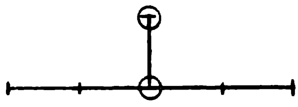
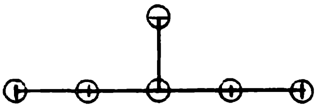
Description: The same as for $^1D^{(d)}_{n,r}$, except that all forms in question have now discriminant $\neq 1$.

Special fields: Over F, $d = 1$ and $n = r + 1$; over $\mathbf{R}$, $d = 1$ and $n - r = 2m + 1$, or $d = 2$ and $n = 2r + 1$; over p, $d = 1$ and $n = r + 1$, or $d = 2$ and $n = 2r + 1$ or $2r + 2$; over n, $d = 1$ or 2, and there is no special condition on r.

TYPES ${}^3D_4$ AND ${}^6D_4$

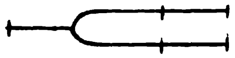
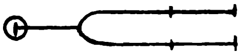
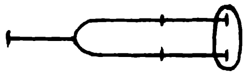
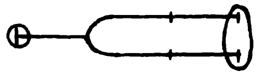
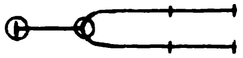
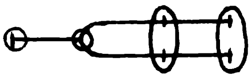
Symbol	Index	Special fields			
		F	R	$\mathfrak{p}$	$\mathfrak{n}$
${}^3D_{4,0}^{28}$		−	−	−	+
${}^6D_{4,0}^{28}$		−	−	−	+
${}^3D_{4,1}^{9}$		−	−	−	+
${}^6D_{4,1}^{9}$		−	−	−	+
${}^3D_{4,2}^{2}$		+	−	+	+
${}^6D_{4,2}^{2}$		−	−	+	+

TYPE ${}^1E_6$

Symbol	Index	Special fields			
		F	R	$\mathfrak{p}$	$\mathfrak{n}$
${}^1E_{6,0}^{78}$		−	−	−	+
${}^1E_{6,2}^{28}$		−	+	−	+
${}^1E_{6,2}^{16}$		−	−	+	+
${}^1E_{6,6}^{0}$		+	+	+	+

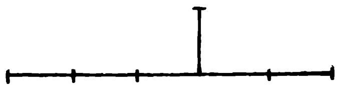
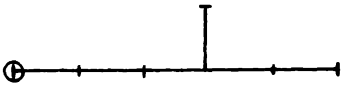
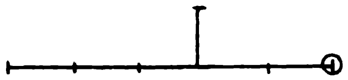
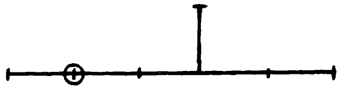
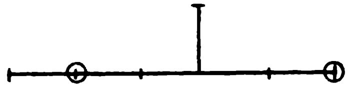
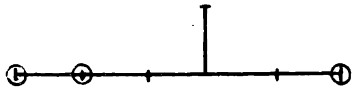
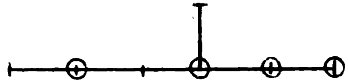
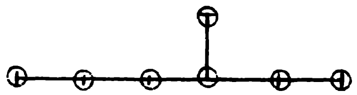
REMARK. ${}^1E_{6,2}^{28}$ is the form which can be realized as collineation group of a Cayley plane ([**15**], [**32**], [**35**]); ${}^1E_{6,2}^{16}$ is the form which is constructed by means of an associative division algebra of degree 3 ([**38**], [**44**]).

TYPE ${}^2E_6$

Symbol	Index	Special fields *F*	*R*	p	*n*
${}^2E_{6,0}^{78}$		−	+	−	+
${}^2E_{6,1}^{35}$		−	−	−	+
${}^2E_{6,1}^{29}$		−	−	−	+
${}^2E_{6,2}^{16'}$		−	+	−	+
${}^2E_{6,2}^{16''}$		−	−	−	+
${}^2E_{6,4}^{2}$		+	+	+	+

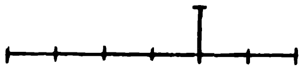
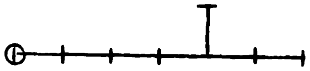
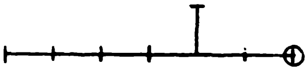
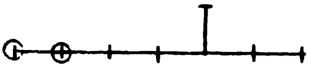
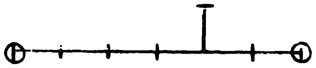
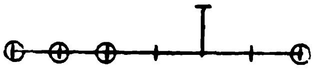
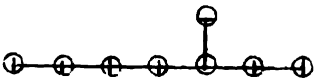
REMARKS. ${}^2_{\mathbf{R}}E_{6,2}^{16'}$ is the real form of E_6 which gives rise to a bounded symmetric domain. In the list given at the end of [42], the index ${}^2E_{6,1}^{35}$ has been erroneously omitted.

TYPE E_7

Symbol	Index	Special fields *F*	*R*	p	*n*
$E_{7,0}^{133}$		−	+	−	+
$E_{7,1}^{78}$		−	−	−	−
$E_{7,1}^{66}$		−	−	−	−
$E_{7,1}^{48}$		−	−	−	−
$E_{7,2}^{31}$		−	−	−	+
$E_{7,3}^{28}$		−	+	−	+
$E_{7,4}^{9}$		−	+	+	+
$E_{7,7}^{0}$		+	+	+	+

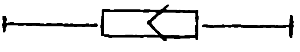
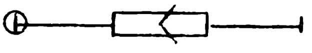
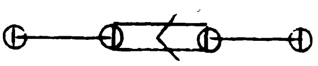
REMARK. $E_{7,3}^{28}$ is the form which is constructed by means of a division Cayley algebra ([**16**], [**36**], [**41**]); over the reals, it is also the form which gives rise to a bounded symmetric domain.

TYPE E_8

Symbol	Index	Special fields			
		F	*R*	$\mathfrak{p}$	*n*
$E_{8,0}^{248}$		−	+	−	+
(?) $E_{8,1}^{133}$		−	−	−	−
$E_{8,1}^{91}$		−	−	−	−
$E_{8,2}^{78}$		−	−	−	−
$E_{8,2}^{66}$		−	−	−	−
$E_{8,4}^{28}$		−	+	−	+
$E_{8,8}^{0}$		+	+	+	+

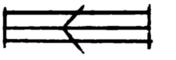
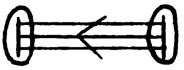
REMARK. $E_{8,4}^{28}$ is the form which is constructed by means of a Cayley division algebra ([**16**], [**44**]).

TYPE F_4

Symbol	Index	Special fields			
		F	*R*	$\mathfrak{p}$	*n*
$F_{4,0}^{52}$		−	+	−	+
$F_{4,1}^{21}$		−	+	−	+
$F_{4,4}^{0}$		+	+	+	+

Remark. A group of type F_4 is always the automorphism group of an exceptional simple Jordan algebra J ([**8**], [**15**], [**22**]); the three diagrams above correspond respectively to the cases where J does not have nonzero nilpotent elements, has such elements but does not have two nonproportional orthogonal ones, and finally has nonproportional orthogonal nilpotent elements.

TYPE G_2

Symbol	Index	Special fields			
		F	R	$\mathfrak{p}$	n
$G^{14}_{2,0}$		−	+	−	+
$G^{0}_{2,2}$		+	+	+	+

Remark. A group of type G_2 is always the automorphism group of a Cayley algebra ([**21**], [**31**]); the two diagrams above correspond respectively to the cases where this algebra is a division algebra, and is split.

Bibliography

1. A. A. Albert, *Structure of algebras*, Amer. Math. Soc. Colloq. Publ., vol. 24, Amer. Math. Soc., Providence, R.I., 1961.

2. A. Borel, *Linear algebraic groups*, Proc. Sympos. Pure Math., vol. 9, Amer. Math. Soc., Providence, R.I., 1966, pp. 3–19.

3. A. Borel, and J. de Siebenthal, *Les sous-groupes fermés connexes de rang maximum des groupes de Lie clos*, Comment. Math. Helv. **23** (1949–1950), 200–221.

4. A. Borel, and J. Tits, *Groupes réductifs*, Publ. Math. I.H.E.S. **27** (1965), 55–151.

5. N. Bourbaki, *Groupes et algèbres de Lie*, Chap. 5: "Systèmes de racines" (to appear).

6. P. Cartier, *Groupes algébriques et groups formels*, Coll. Théorie des groupes (Groupes algébriques), Bruxelles, 1962, pp. 87–111. Libraire Universitaire, Louvain; Gauthier–Villars, Paris, 1962.

7. C. Chevalley, *Classification des groupes de Lie algébriques*, Séminaire C. Chevalley (1956–1958), Sécrétariat mathématique, Paris.

8. C. Chevalley, and R. D. Schafer, *The exceptional simple Lie algebras F_4 and E_6*, Proc. Nat. Acad. U.S.A. **36** (1950), 137–141.

9. M. Demazure, and A. Grothendieck, *Schémas en groupes*, I.H.E.S., 1964 (notes polycopiées).

10. J. Dieudonné, *La géométrie des groupes classiques*, Ergebnisse d. Math., N.F. 5, Springer, Berlin–Göttingen–Heidelberg, 2nd ed., 1963.

11. E. B. Dynkin, *Struktura poluprostyh algebr Li*, Uspehi Mat. Nauk **4** (1947), 59–127.

12. ———, *Avtomorfizmy poluprostyh algebr Li*, Dokl. Akad. Nauk S.S.S.R. **76** (1951), 629–632.

13. ———, *Poluprostye podalgebry poluprostyh algebr Li*, Mat. Sbornik (72) **30** (1952), 349–362.

14. E. B. Dynkin, and A. L. Oniščik, *Kompaktnye gruppy Li v celom*, Uspehi Mat. Nauk **10** (1955), 3–74.

15. H. Freudenthal, *Oktaven, Ausnahmegruppen und Oktavengeometrie*. Mathematisch Instituut der Rijksuniversiteit, Utrecht, 1951 (2nd ed., 1960).

16. H. Freudenthal, *Beziehungen der E_7 und E_8 zur Oktavenebene*, I–XI, Proc. Kon. Ned. Akad. Wet. A **57** (1954), 218–230; 363–368; A **58** (1955), 151–157, 277–285; A **62** (1959), 165–201, 447–474; A **66** (1963), 457–487.

17. ———, *Lie groups*, Mimeographed lectures, Yale University, New Haven, Conn., 1961.

18. F. Gantmacher, *On the classification of real simple Lie groups*, Mat. Sbornik (47) **5** (1939), 217–249.

19. G. Harder, *Über die Galoiskohomolgie halbeinfacher Matrizengruppen.* I, Math. Z. **90** (1965), 404–428.

20. D. Hertzig, *Forms oj algebraic groups*, Proc. Amer. Math. Soc. **12** (1961), 657–660.

21. N. Jacobson, *Cayley numbers and simple Lie algebras of type G*, Duke Math. J. **5** (1939), 775–783.

22. ———, *Some groups of transformations defined by Jordan algebras*, I–III, Jour, Reine U. Angew. Math. **201** (1959), 187–195; **204** (1960), 74–98; **207** (1961), 61–85.

23. M. Kneser, *Galois–Kohomolgie halbeinfacher algebraischer Gruppen über p-adischen Körpern.* I, II, Math. Z. **88** (1965), 40–47, **89** (1965), 250–272.

24. B. Kostant, *The principal three-dimensional subgroup and the Betti numbers of a complex simple Lie group*, Amer. J. Math. **81** (1959), 973–1032.

25. W. Landherr, *Über einfache Liesche Ringe*, Abh. Math. Sem. Univ. Hamburg **11** (1936), 41–64.

26. I. Satake, *On representations and compactifications of symmetric Riemannian spaces*, Ann. of Math. (2) **71** (1960), 77–110.

27. ———, *On the theory of reductive algebraic groups over a perfect field*, Jour. Math. Soc. Japan **15** (1963), 210–235.

28. E. A. M. Seip-Hornix, *Clifford algebras of quadratic quaternion forms*, Proc. Kon. Ned. Akad. Wet. A **68** (1965), 326–363.

29. Séminaire Sophus Lie, Sém. Ec. Norm. Sup., Secrétariat mathématique, Paris, 1954–1955. (Mimeographed notes.)

30. J.-P. Serre, *Cohomologie galoisenne des groups algébriques linéaires*, Coll. Théorie des groupes (Groupes algébriques), Centre Belge Rech. Math. Bruxelles, June 1962, pp. 53–67.

31. ———, *Cohomologie galoisienne*, Lecture Notes in Math. No. 5, Springer, Berlin, 1964.

32. T. A. Springer, *The projective octave plane.* I, II, Proc. Kon. Ned. Akad. Wet. A **63** (1960), 74–101.

33. R. Steinberg, *Variations on a theme of Chevalley*, Pacific J. Math. **9** (1959), 875–891.

34. ———, *Finite reflection groups*, Trans. Amer. Math. Soc. **91** (1959), 493–504.

35. J. Tits, *Le plan projectif des octaves et les groupes de Lie exceptionnels*, Acad. Roy. Belg. Bull. Cl. Sci. 39 (1953), 309–329.

36. ———, *Le plan projectif des octaves et les groupes exceptionnels E_6 et E_7*, Acad. Roy. Belg., Bull. Cl. Sci. **40** (1954), 29–40.

37. ———, *Sur certaines classes d'espaces homogènes de groups de Lie*, Mém. Acad. Roy. Belg. (3) **29** (1955).

38. ———, *Sur la classification des groupes algébriques semi-simples*, C. R. Acad. Sci. Paris **249** (1959), 1438–1440.

39. ———, *Sur les groupes algébriques: théorèmes fondamentaux de structure; classification des groupes semi-simples et géométries associées*, Centro Internazionale Matematico estivo (C.I.M.E.), Saltino di Vallombrosa, Sept. 1959; Rome, 1960.

40. ———, *Groupes algébriques semi-simples et géométries associées*, Proc. Coll. Algebraical and Topological Foundations of Geometry, Utrecht, Aug. 1959; Pergamon Press, Oxford, 1962, pp. 175–192.

41. ———, *Une classe d'algèbres de Lie en relation avec les algèbres de Jordan*, Proc. Ned. Akad. Wet. A **65** (1962), 530–535.

42. ———, *Groupes semi-simples isotropes*, Colloque sur la Théorie des groupes algébriques, C.B.R.M., Bruxelles, June 1962, pp. 137–147.

43. ———, *Groupes simples et géométries associées*, Proc. Intern. Congress Math., Stockholm, 1962, pp. 197–221. Inst. Mittag-Leffer, Djursholm, 1963.

44. ———, *Algèbres alternatives, algèbres de Jordan et algèbres de Lie exceptionnelles*, II, Proc. Kon. Ned. Akad. Wet. (to appear) (Cf. also: Same title, mimeographed notes, Princeton, 1963).

45. B. Ju. Veisfeiler, *Classification of semi-simple Lie algebras over a p-adic field*, Doklady Akad. Nauk. SSSR **158** (1964), 258–260 = Soviet Math. **5** (1964), 1206–1208.

46. A. Weil, *Algebras with involution and the classical groups*, J. Indian Math. Soc. **24** (1960), 589–623.

47. E. Witt, *Spiegelungsgruppen und Aufzählung halbeinfacher Liescher Ringe*, Abh. Math. Sem. Hamburg **14** (1941), 289–322.

p-adic Groups

BY

FRANÇOIS BRUHAT

1. **Bounded subgroups.** If G is a real connected Lie group, then the following two statements are well known:

(1) Any compact subgroup of G is contained in a maximal compact subgroup of G.

(2) Two maximal compact subgroups are conjugate by an inner automorphism.

Now let P be the quotient field of a complete discrete valuation ring $\mathcal{O}$. Let $\mathfrak{p}$ be the maximal ideal of $\mathcal{O}$, and let π be a generator of $\mathfrak{p}$, and K be the residue field of $\mathcal{O}$ by $\mathfrak{p}$, i.e., $\mathfrak{p} = \mathcal{O}\pi$, $\mathrm{K} = \mathcal{O}/\mathfrak{p}$. P is locally compact for the topology induced by the valuation if and only if K is a finite field.

Let G be a linear algebraic group defined over P, realized in $\mathrm{GL}(V)$ where V is a vector space defined over P. Let G_P be the group of P-rational points of G. G_P can be considered as a subset of $\mathrm{GL}(n, P)$, and also a subset of the ambient space P^{n^2} of $\mathrm{GL}(n, P)$. With the topology induced by P^{n^2}, G_P is a topological group. If P is locally compact, then G_P is locally compact.

Let K be a subgroup of G_P, then the following three statements are equivalent:

(i) There exists a locally faithful matricial rational representation ρ of G defined over P s.t. the coordinates of the elements of $\rho(K)$ are bounded,

(ii) For any matricial rational representation, the coordinates of the elements of $\rho(K)$ are bounded.

(iii) For any rational linear representation ρ of G in a vector space V over P, there exists a lattice L in V s.t. $\rho(k)L = L$ for any k in K.

If K satisfies one of the above conditions, K is called a bounded subgroup of G_P.

The condition (iii) implies that any bounded subgroup is contained in an *open* and bounded subgroup. On the other hand, the open and bounded subgroups of G are related with the structure of G as *group scheme over the ring* $\mathcal{O}$: let $P[G]$ the affine algebra of G. The product in G gives a structure of coalgebra on $P[G]$, i.e., a linear map $d: P[G] \to P[G] \otimes_P P[G]$ which is defined by the condition:

$$d(f) = \sum f'_i \otimes f''_i \Leftrightarrow f(xy) = \sum f'_i(x) f''_i(y).$$

Now, an $\mathcal{O}$-structure for G is an $\mathcal{O}$-subalgebra of finite type $\mathscr{A}[G]$ such that $P[G] = P\mathscr{A}[G]$ and $d(\mathscr{A}[G]) \subset \mathscr{A}[G] \otimes_{\mathcal{O}} \mathscr{A}[G]$.

EXAMPLE. Let $G = \mathrm{GL}(V)$, let L a lattice in V_P, (g_{ij}) the matrix of $g \in G$ with respect to some basis of L. Then the algebra $\mathscr{A}[\mathrm{GL}] = \mathcal{O}[g_{ij}, (\det(g_{ij}))^{-1}]$ is an

$\mathcal{O}$-structure for GL(V). More generally, if G is a subgroup defined over P of GL(V), the image of $\mathscr{A}[\mathrm{GL}(V)]$ in $P[G]$ is an $\mathcal{O}$-structure for G. It can be shown that any $\mathcal{O}$-structure may be obtained in this way.

If $\mathscr{A}$ is an $\mathcal{O}$-structure on G, then for any $\mathcal{O}$-algebra B (commutative, with unit) the set $G_B = \mathrm{Hom}_{\mathcal{O}}(\mathscr{A}, B)$ is a group. In particular, $G_{\mathcal{O}}$ can be considered as a subset of $G_P = \mathrm{Hom}_{\mathcal{O}}(\mathscr{A}, P) = \mathrm{Hom}_P(P[G], P)$, and is a *bounded and open* subgroup of G_P.

We can also "reduce mod $\mathfrak{p}$": the algebra $\mathscr{A}/\mathfrak{p}\mathscr{A}$ over the residual field K is the affine algebra of a group scheme over K (which is not necessarily connected, nor reduced). If $\mathscr{A}/\mathfrak{p}\mathscr{A}$ is the affine algebra of a connected *algebraic group* defined over K, we shall say that the reduction mod $\mathfrak{p}$ of $\mathscr{A}$ is "good." In this case, the canonical map : $G_{\mathcal{O}} \to G_{\mathrm{K}}$ is *surjective*.

2. **Existence and classification of maximal bounded subgroups.** If G is an additive group of affine line G_a, then G has no maximal bounded subgroup, because $(G_a)_P = \bigcup \mathcal{O}\pi^{-n}$. More generally it can be proved that if G is not reductive and if the characteristic of P is zero, then G_P has no maximal compact subgroups. (If the characteristic of P is positive, there may exist a unipotent group defined over P without P-rational point, except e, so the above statement is no longer true.) In any way the interesting cases are that of reductive or semisimple groups. Then we have an existence theorem:

THEOREM (LANGLANDS).[1] *If P is a locally compact field, and G is a reductive group, then any compact subgroup of G_P is contained in a maximal compact subgroup of G_P.*

PROOF. We may assume $G \subset \mathrm{GL}(V)$, and irreducible. It suffices to show there is no infinite sequence of open compact subgroups K_n s.t. $K_n \subsetneqq K_{n+1} \subsetneqq \cdots$. Take a lattice L in V_P, and let $X_n = \{x \in L | kx \in L \text{ for any } k \in K_n\}$. It is obvious that X_n is K_n-invariant and $X_n \not\subset \pi L$. Let $Y_n = X_n \cap (L - \pi L)$. Since X_n is a closed subset of L, Y_n is compact nonempty. Let Y be the intersection of all Y_n, then Y is nonempty. Let X be the intersection of all X_n, then X has a nonzero vector of V_P, and is invariant under any K_n. Let W be the P-vector space generated by X. The Zariski closure $\mathrm{Cl}(\bigcup K_n)$ of $\bigcup K_n$ is open for the P-topology, and closed under Zariski topology, so $\mathrm{Cl}(\bigcup K_n) = G_P$, W is a nontrivial invariant subspace and X is a lattice in V_P. Now $\bigcup K_n$ fixes X invariant, and consequently compact. Therefore, there is no infinite sequence

$$K_n ; K_n \subsetneqq K_{n+1} \subsetneqq \cdots \text{in } G_P.$$

For classical groups (at least in the strict sense and if the characteristic of the residual field K is not 2), one knows the complete classification of conjugacy classes of maximal bounded subgroups.

[1] During this Institute, Tamagawa has indicated to me another method of proof, which is valid also for the nonlocally compact case and gives the existence of maximal bounded subgroups.

EXAMPLE 1. $G_P = \mathrm{SL}(n, D)$, D = a division algebra of center P. A maximal bounded subgroup is the stabilizer of a lattice in D^n and any two maximal bounded subgroup of G_P are conjugate under $\mathrm{GL}(n, D)$, but the number of conjugacy classes of bounded subgroups under inner automorphisms is equal to $n = rk_P(G) + 1$.

EXAMPLE 2. $G_P = \mathrm{PGL}(n, P)$. Let K be a maximal bounded subgroup of G_P, and $\tilde{K}$ the inverse image of K in $\mathrm{GL}(n, P)$. It can be shown that there exists a *divisor* d of n and a sequence of d lattices $L_0 \supset L_1 \supset \cdots \supset L_d = \pi L_0$ in P^n, with $\dim_K(L_i/L_{i+1}) = n/d$, such that $\tilde{K}$ is exactly the set of those elements of $\mathrm{GL}(n, P)$ which keep globally invariant the infinite sequence formed by the lattices $\pi^k L_i$ ($0 \leqq i < d, k \in Z$). (The proof is given in [4] with the assumption that the characteristic p of K does not divide n. But it is possible to give a more direct proof, which is valid in any case.) One sees that the number of classes of maximal bounded subgroups in PGL_n is equal to the number of divisors of n. The n classes of maximal bounded subgroups of SL_n give exactly one class for the isogenous group PGL_n, but other classes appear.

EXAMPLE 3. $G = \mathrm{SO}(Q)$, Q is a quadratic form over a vector space V over P (char $P \neq 2$). Let K be a bounded subgroup of G_P, then K fixes a lattice L in V_P; $K \subset \mathrm{End}(L)$. Q induces an involution $*$ in $\mathrm{End}(V)$. Since $g^* = g^{-1}$ for $g \in G_P, K \subset \mathrm{End}\, L \cap (\mathrm{End}\, L)^* \cap G_P$. If K is maximal bounded, then

$$K = \mathrm{End}\, L \cap (\mathrm{End}\, L)^* \cap G_P.$$

Now consider the set S of all the orders of $\mathrm{End}(V_P)$ which can be written as $\Omega \cap \Omega^*$ by some maximal order Ω of $\mathrm{End}(V_P)$. Let Φ be the symmetric bilinear form attached to Q, $e_i (i = 1 \cdots n)$ be a basis of a lattice L; then $(\mathrm{End}\, L) \cap (\mathrm{End}\, L)^*$ is maximal in S if and only if any elementary divisor of the matrix $(\Phi(e_i, e_j))$ is either 1 or π (up to a constant factor). The number of conjugacy classes of such lattices is finite. Since any maximal bounded subgroup K is contained in a maximal element of S, the number of conjugacy classes of maximal bounded subgroups of G_P is finite.

Let L_0 be a lattice in V_P, generated by a "Witt basis", i.e. a basis $e_1, \cdots, e_n$ of V_P satisfying the following conditions:

(a) $e_1, \cdots, e_r$ (resp. $e_{n-r+1}, \cdots, e_n$) generate over P a maximal isotropic subspace V_1 (resp. V_3) of V_P;

(b) $\Phi(e_i, e_{n+1-j}) = \delta_{ij}$ for $1 \leqq i, j \leqq r$;

(c) $e_{r+1}, \cdots, e_{n-r}$ generate over P the orthogonal V_2 of $V_1 + V_3$ (which is a maximal anisotropic subspace of V_P) and generate over the unique maximal $\mathcal{O}$-integral lattice of V_2.

Now let L_s be the lattice generated by $\pi e_1, \cdots, \pi e_s, e_{s+1}, \cdots, e_n$ with $0 \leqq s \leqq r$. Then the orders $\Omega_s = \mathrm{End}\, L_s \cap (\mathrm{End}\, L_s)^*$ are maximal elements of S and if char K $\neq 2$, any maximal element of S is conjugate to some Ω_s by an element of G_P.

Then (at least if char K $\neq 2$), there is exactly $r + 1$ classes of maximal bounded subgroups, represented by the subgroups $K_s = \Omega_s \cap G_P$ for $0 \leqq s \leqq r$.

Similar results hold for the other types of classical groups (symplectic, unitary, etc.) [**6**].

3. **Iwasawa and Cartan decompositions.**

G = connected semisimple group over P,
A = maximal P-split torus,
N = normalizer of A in G,
Z = centralizer of A in G,
U = unipotent radical of a minimal parabolic subgroup Γ of G over P, associated to A,
$\Gamma = ZU$, $W = N_P/Z_P$,
Y = the group of P-rational characters of Z,
$Z_{\mathcal{O}} = \{z \in Z_p \,\big|\, |\chi(z)|_P = 1 \text{ for any } \chi \in Y\}$, $D = Z_P/Z_{\mathcal{O}}$.

Let δ be the canonical map $Z_P \to D$. Then D is isomorphic to $\mathbf{Z}^r$ where r is the P-rank of G, and $D/\delta(A_P)$ is of finite index. W acts on D, A_P. Let

$$A_P^+ = \{a \in A_P \,\big|\, |\alpha(a)|_P \geqq 1 \text{ for any positive } \alpha \in X(A)\},$$

$$D^+ = \{d \in D \,\big|\, \text{there exists a positive integer } n \text{ with } nd \in \delta(A_P^+)\}.$$

CONJECTURE I. There exists a maximal bounded subgroup K of G_P satisfying the following conditions:

(i) $K \supset Z_{\mathcal{O}}, N_P \subset KZ_{\mathcal{O}}$,

(ii) $G_P = KZ_PU_P$ (Iwasawa Decomposition),

(iii) $G_P = KZ_PK$ (Cartan Decomposition), more precisely there is a one to one correspondence between $K\backslash G_P/K$ and D^+.

(iv) (a) If $\delta(z) \in D^+$ then $KzK \cap KzU_P = Kz$;

(b) there exists an order on D s.t. if $z, z^+ \in Z_P$, $\delta(z^+) \in D^+$ and

$$Kz^+K \cap KzU_P \neq \emptyset,$$

then $\delta(z) \geqq \delta(z^+)$.

This Conjecture I is true for *classical groups* (at least in the strict sense: unimodular group of a division algebra or groups of matrices of determinant 1 keeping invariant on ε-hermitian form), for *split groups* (of any isogeny type), and for *quasi-split* groups (at least with an unramified splitting field).

REMARK. The condition (iv) is often a consequence of the others, as soon as K is given as the stabilizer of a lattice L in the space V of a representation ρ of G, defined over P, with some properties like:

(a) L is a direct sum of sublattices $L_i (1 \leqq i \leqq m)$; each vector subspace $V_i = \mathrm{P}L_i$ is stable by $Z(A)_P$. Let $z, z' \in Z(A)_P$ and z_i, z_i' be their restrictions to V_i. If for all i z_i and z_i' have the same *invariant factors* (with respect to L_i), then $z' \in zZ(A)_{\mathcal{O}}$. Moreover, if $\delta(z) \in D^+$, then the invariant factors of z_i are less than those of z_{i+1}.

(b) If $u \in G_P$, then $\rho(u)$ is unipotent, upper triangular for the block decomposition, i.e., $(\rho(u) - \mathrm{Id})(V_i) \subset V_1 + - + V_{i-1}$ for $1 \leqq i \leqq m$.

On the other hand, it is possible that (iv) is too strong and has to be replaced by a weaker condition (cf. [**8**]).

EXAMPLE 1.

D = division quaternion over P,

$\tilde{\mathcal{O}}$ = the ring of integers of D,

$\tilde{\mathfrak{p}} = \tilde{\pi}\tilde{\mathcal{O}}$ = the maximal ideal of $\tilde{\mathcal{O}}$,

V_P = n-dimensional vector space over D,

Φ = hermitian form on V_P,

$G = \mathrm{SU}(V, \Phi)$ = special unitary group of (V, Φ).

For a $\tilde{\mathcal{O}}$-lattice L in V_P, the norm $n(L)$ of L is the smallest ideal $\mathfrak{g}$ of D s.t. $\Phi(x, y) \in \mathfrak{g}$ and there exists an element ξ in $\mathfrak{g}$ satisfying $\Phi(x, x) = \xi + \bar{\xi}$ for any x, y in L.

Now let L be a maximal lattice of norm $\tilde{\mathcal{O}}$. Then L has a canonical Witt basis $e_1 \cdots e_n$ satisfying the similar conditions as in §2, Example 3. With respect to this base one can take:

$$A_P = \begin{pmatrix} a_1 & & & & & & & & 0 \\ & \ddots & & & & & & & \\ & & a_{r_1} & & & & & & \\ & & & \ddots & & & & & \\ & & & & 1 & & & & \\ & & & & & \ddots & & & \\ & & & & & & a_r^{-1} & & \\ & & & & & & & \ddots & \\ 0 & & & & & & & & a_1^{-1} \end{pmatrix} \qquad a_i \in P^*,$$

$$Z_P = \begin{pmatrix} A_1 & & & & & & 0 \\ & \ddots & & & & & \\ & & A_r & & & & \\ & & & \boxed{G'} & & & \\ & & & & \bar{A}_r^{-1} & & \\ & & & & & \ddots & \\ 0 & & & & & & \bar{A}_1^{-1} \end{pmatrix} \qquad A_i \in D^*$$

G' = the special unitary group corresponding to the anisotropic part of (V, Φ).

K = stabilizer of L.

$U = G \cap$ (upper triangular matrices with diagonal 1).

If $g \in G_P$, $g(L)$ is a maximal lattice of some norm. We can prove the existence of a basis e_i' of L s.t. $L = \sum e_i'\tilde{\mathcal{O}}$, $g(L) = \sum e_i'\tilde{\pi}^{\nu_i}$ and get the decomposition (iii). Condition (iv) can be proved in the same way as in [2].

$D = Z_P/Z_{\mathcal{O}} = \mathbf{Z}^r$ is realized as

$$\mathrm{diag}(\tilde{\pi}^{\nu_1} \cdots \tilde{\pi}^{\nu_r}, 1, \cdots 1, \bar{\tilde{\pi}}^{-\nu_r} \cdots \bar{\tilde{\pi}}^{-\nu_1}),$$

$\delta(A_P) = \mathrm{diag}(\tilde{\pi}^{2\nu_1} \cdots \tilde{\pi}^{2\nu_r}, 1 \cdots)$, D^+ is the subset of D satisfying $\nu_1 \leqq \nu_2 \leqq \cdots \leqq \nu_r$. Let $g = k_1 d^+ k_2 = du$, $k_1, k_2 \in K$, $d^+ \in D^+$, $u \in U_P$, $d = \mathrm{diag}(\tilde{\pi}^{\mu_1} \cdots) \in D$.

$$du = \begin{pmatrix} \tilde{\pi}^{\mu_1} & & 0 \\ & \ddots & \\ 0 & & \ddots \end{pmatrix}\begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix} = \begin{pmatrix} \tilde{\pi}^{\mu_1} & & \\ 0 & & * \\ \vdots & & \\ 0 & & \end{pmatrix}.$$

But the elementary divisors of g are the same as those of d_+, so $\nu_1 \leqq \mu_1$. By induction we can show the condition (iv), where the order is the lexico-graphic order.

Example 2.

G = semisimple with split torus over P (Chevalley type).

$\mathfrak{g}$ = Lie algebra of G.

X_α, H_α = Chevalley base of $\mathfrak{g}$.

L = $\mathcal{O}$-module generated by X_α, H_α.

K = stabilizer of L.

Then (i) ~ (iv) are satisfied [3], [7].

Remark 1. There exist maximal bounded subgroups for which (ii), (iii) and (iv) are not true (even if P is locally compact).

Remark 2. There may exist several classes of maximal bounded subgroups satisfying (I), even not isomorphic.

4. **Tits system in a simply connected group.** Let us assume K is finite and let $\mathscr{A}$ an $\mathcal{O}$-structure on G, which has a good reduction with $\bar{G}$ semisimple over K, of same type as G. Then G is split or quasi-split with unramified splitting field, the $\mathcal{O}$-structure $\mathscr{A}$ is given as §3. Example 2, and the Conjecture I is true for $K = G_{\mathcal{O}}$. But in other cases, we may have an $\mathcal{O}$-structure $\mathscr{A}$, which does not have a good reduction, and, nevertheless, the Conjecture I is still true for $K = G_{\mathcal{O}}$. Moreover, this $\mathscr{A}$ has the following properties, which we state as a conjecture, because we are not able to prove them in the general case:

Conjecture II. If G is a connected semisimple *simply connected* group defined over P, there exists an $\mathcal{O}$-structure $\mathscr{A}$ on G such that:

(i) $G_{\mathcal{O}}$ satisfies the conditions of the Conjecture I.

(ii) The $\mathcal{O}$-structure determined by $\mathscr{A}$ on the maximal split torus A is the canonical one (i.e., given by the algebra generated by the characters) and so has a good reduction on a *torus* $\bar{A}$, split over K.

(iii) There exists a connected reductive algebraic group $G^=$ defined over K, containing $\bar{A}$ as a maximal K-split torus, and a morphism of group scheme from the reduced group scheme $\bar{G}$ to $G^=$, inducing the identity on $\bar{A}$, such that, if ρ is the associated map from $G_{\mathcal{O}}$ to $G^=_{\mathrm{K}}$, the inverse image $B = \rho^{-1}(\bar{B}_{\mathrm{K}})$ of the set of rational points of a minimal parabolic subgroup $\bar{B}$ of $G^=$ containing $\bar{A}$, constitutes with the subgroup $N = N(A)_P$ a *Tits system* (or a (B.N. pair)) in G_P. The Weyl group $\tilde{W} = N/B \cap N$ of this Tits system is an affine Weyl group, extension of the P-Weyl group of G by Z^r.

This conjecture has been firstly proved by N. Iwahori and H. Matsumoto in the split case [7] (for the $\mathcal{O}$-structure of §3 Example 2) then by H. Hijikata for quasi-split case [5] and classical cases [6].

REMARK. A triple of groups (G, B, N) is called a "Tits system" if it satisfies the following:

(0) G is generated by B and N, $B \cap N$ is a normal subgroup of N, $W = N/B \cap N$ is called the Weyl group of the Tits system.

(1) W is generated by involutive elements $r \in I$, $r^2 = 1$,

(2) $rBr^{-1} \neq B$ for any $r \in I$,

(3) $rBw \subset BrwB \cup BwB$ for any $r \in I$ and any $w \in W$.

If (G, B, N) is a Tits system, then:

(1) $w \to BwB$ gives a bijective map from W to $B\backslash G/B$.

(2) For any subset J of I, let W_J be the group generated by r $(r \in J)$, then $G_J = BW_JB$ is a group. $G_J = N_G(G_J)$. G_J is conjugate to G_K if and only if $K = J$. Any subgroup of G containing B has the form of G_J.

As a consequence if the Conjecture II is true, G_P has at least $r + 1$ classes of maximal bounded subgroups where $r = rk_P(G)$. Actually $\tilde{W}$ has $r + 1$ generators $I = \{w_1, \cdots w_r, w_0\}$, and a maximal bounded subgroup K_i $(i = 0, 1, \cdots r)$ is given by $K_i = BW_{I-\{w_i\}}B$.

CONJECTURE (II) (iv). Any maximal bounded subgroup of G_P contains a conjugate of B.

REMARK. (iv) is known for classical groups modulo some exception in the case of characteristic of K = 2. [6].

Added in November 1965. During the conference, considerable progress was made towards an affirmative solution of the conjectures above. It also appeared that the properties thus established have interesting applications; for instance, they provide a simplified approach to Kneser's theorem on H^1 of simply connected groups over the p-adics. A joint paper on this subject is in preparation, by F. Bruhat and J. Tits.

These results were exposed orally by J. Tits at the conference. The precise form on which they are given in the mimeographed notes of his talk must however be somewhat modified; in particular, it is not true that minimal k-parahoric subgroups of a group G—as defined in these notes—are conjugate by elements of G_k. In fact, the notion of k-parahoric subgroup given there does not appear to be "the good one" when G does not split over an unramified extension of k.

On the other hand, the methods sketched there turn out to give further results. For instance, it can be shown that the Conjecture (II) (iv) above is essentially a consequence of the other parts of that conjecture and, in particular, is true in the split case.

BIBLIOGRAPHY

1. F. Bruhat, *Distributions sur un groupe localement compact et applications à l'étude des representations des groupes* p*-adiques*, Bull. Soc. Math. France **89** (1961), 43–75.

2. ———, *Sur les representations des groupes classiques* p*-adiques*, Amer. J. Math. **83** (1961), 321–338, 343–368.

3. ———, *Sur une classe de sous-groupes compacts maximaux des groupes de Chevalley sur un corps* p*-adique*, Inst. Hautes Études Sci. Publ. Math. **23** (1964), 46–74.

4. H. Hijikata, *Maximal compact subgroups of* p*-adic classical groups* (in Japanese), Sugaku no Ayumi, 10–2, pp. 12–23, 1963.

5. ———, *On the arithmetic of* p*-adic Steinberg groups*, Yale University, 1964. (Mimeographed)

6. ———, *Maximal compact subgroups of some* p*-adic classical groups*, Yale University, 1964. (Mimeographed)

7. N. Iwahori and H. Matsumoto, *On some Bruhat decomposition and the structure of the Hecke rings of* p*-adic Chevalley group*, Inst. Hautes Études Sci. Publ. Math. **25** (1965), 5–48.

8. I. Satake, *Theory of spherical functions on reductive algebraic groups over* p*-adic field*, Inst. Hautes Études Sci. Publ. Math. **18** (1963), 5–69.

9. G. Shimura, *Arithmetic of alternating forms and quaternion hermitian forms*, J. Math. Soc. Japan **15** (1963), 33–65.

10. T. Tsukamoto, *On the local theory of quaternionic anti-hermitian forms*, J. Math. Soc. Japan **13** (1961), 387–600.

Generalized Tits System (Bruhat Decomposition) on $\mathfrak{p}$-Adic Semisimple Groups

BY

NAGAYOSHI IWAHORI

1. **Generalized Tits system.** In order to describe the situation where the algebraic group G is not simply connected (cf. Bruhat's talk; also see [3], [8]), we have to generalize the notion of *Tits system* (or BN-pair, see Tits [13]) as follows.

Let G be a group and B, N subgroups of G. The triple (G, B, N) is called a *generalized Tits system* if the following conditions (i) ~ (vi) are all satisfied.

(i) $H = B \cap N$ is a normal subgroup of N.

(ii) The factor group N/H is a semidirect product of a subgroup Ω and a normal subgroup $W: N/H = \Omega \cdot W$.

(iii) There exists a system of generators of W consisting of involutive elements $w_i\,(i \in I)$ with the following properties (iii; α) and (iii; β). [We assume that $w_i \neq 1$ and that $w_i \neq w_j$ (for $i \neq j$). We also identify the index set I with the generator system $\{w_i; i \in I\}$].

(iii; α) For any σ in ΩW and for any w_i in I,

$$\sigma B w_i \subset B\sigma w_i B \cup B\sigma B.$$

(For any element σ and τ in ΩW, $\sigma B \tau$ is defined as the set $\tilde{\sigma} B \tilde{\tau}$ where $\tilde{\sigma}$ and $\tilde{\tau}$ are elements of N projecting to σ, τ respectively. Obviously $\sigma B \tau$ is thus well defined. Similarly $B\sigma B$ is defined.)

(iii; β) $w_i B w_i^{-1} \neq B$ for all w_i in I.

(iv) Any element ρ in Ω normalizes $I: \rho I \rho^{-1} = I$.

(v) $\rho B \rho^{-1} = B$ for all ρ in Ω; $B\rho \neq B$ for any $\rho \in \Omega - \{1\}$.

(vi) G is generated by B and N.

W is called the Weyl group of (G, B, N); $\Omega W = N/H$ is called the generalized Weyl group of (G, B, N).

Let now (G, B, N) be a generalized Tits system. Then, Tits [13] (cf. also Iwahori and Matsumoto [8, §2]), one can prove the following main properties of the generalized Tits system (G, B, N).

(a) $G = \bigcup_{\sigma \in \Omega W} B\sigma B$ (disjoint union)

(b) The normalizer $N(B)$ of B in G is given by

$$N(B) = \bigcup_{\rho \in \Omega} B\rho B = B\Omega B = B\Omega = \Omega B.$$

Furthermore, $N(B)/B$ is isomorphic with Ω.

(c) For any subgroup H of G containing B, there exist a unique subgroup Ω_H of Ω and a unique subset J_H of I such that $H = B(\Omega_H W(J_H))B$; where $W(J_H)$ means the subgroup of W generated by J_H. Moreover, J_H is normalized by every element ρ in $\Omega_H: \rho J_H \rho^{-1} = J_H$. The pair (Ω_H, J_H) is called *associated* with the subgroup H.

(d) Conversely, let (Ω', J) be a pair of a subgroup Ω' of Ω and a subset J of I such that J is normalized by every element of Ω'. (Such a pair will be called an *admissible pair.*) Then there exists a unique subgroup H such that $G \supset H \supset B$ and that $\Omega' = \Omega_H$, $J = J_H$. Thus the mapping $H \rightarrow (\Omega_H, J_H)$ is a bijection from the set of all subgroups between G and B onto the set of all admissible pairs.

(e) Let L be the normalizer in G of a subgroup H containing B. Let (Ω_H, J_H), (Ω_L, J_L) be the admissible pairs associated to H, L respectively. Then,

$$J_L = J_H, \Omega_L = \{\rho \in \Omega; \rho\Omega_H\rho^{-1} = \Omega_H, \rho J_H \rho^{-1} = J_H\}.$$

(f) Let H_i $(i = 1, 2)$ be subgroups of G containing B and (Ω_i, J_i) $(i = 1, 2)$ the admissible pairs associated to H_1, H_2 respectively. Then the following conditions (α)–(γ) are equivalent:

(α) H_1 and H_2 are conjugate in G,

(β) H_1 and H_2 are conjugate by an element in $N(B)$,

(γ) $\rho\Omega_1\rho^{-1} = \Omega_2$ and $\rho J_1 \rho^{-1} = J_2$ for some ρ in Ω.

(g) $G_0 = BWB$ is a normal subgroup of G and (G_0, B, N_0) is a Tits system with W as its Weyl group, where $N_0 = N \cap G_0$. Moreover $G/G_0 \cong \Omega$.

(h) For any element g in G, the automorphism of G_0 defined by $x \rightarrow gxg^{-1}$ preserves the Tits system (G_0, B, N_0) up to the conjugacy in G_0, i.e., there exists an element g_0 in G_0 such that $gBg^{-1} = g_0Bg_0^{-1}$, $gN_0g^{-1} = g_0N_0g_0^{-1}$.

According to a remark of Tits, (g) and (h), provide the following alternative description of generalized Tits systems, which make them appear as sort of nonconnected analogues of the usual ones.

To begin with, let us recall the notion of saturation for a Tits system. In general, a generalized Tits system (G,B, N) is called *saturated* if

$$B \cap N = \bigcap_{n \in N} nBn^{-1}.$$

Note that any generalized Tits system (G, B, N) can be modified into a saturated one (G, B, N^*) without changing the factor group $N/B \cap N$. In fact, N^* is given as $N^* = N \cdot H^*$ where $H^* = \bigcap_{n \in N} nBn^{-1}$. Conversely, starting from a saturated system (G, B, N^*) one gets other systems by replacing N^* by any subgroup N such that $N \cdot H^* = N^*$.

Suppose now that G_0 is a normal subgroup of a group G and let (G_0, B_0, N_0) be a saturated Tits system on G_0. We assume that, for any element g in G, the automorphism $x \rightarrow gxg^{-1}$ of G_0 preserves the Tits system (G_0, B_0, N_0) up to the conjugacy in G_0 (cf. (h) above). Then we get a saturated, generalized Tits system (G, B, N) on G, where $N = \Gamma N_0$, $\Gamma = N_G(B) \cap N_G(N_0)$, $B = B_0$. $(N_G(X)$

means the normalizer of X in G.) Furthermore, $N/B \cap N$ is isomorphic to the semidirect product $\Omega \cdot W$, where W is the Weyl group of (G_0, B_0, N_0) and $\Omega = N_G(B)/B$. This procedure exhausts all saturated generalized Tits systems.

2. **Existence of a generalized Tits system on $\mathfrak{p}$-adic semisimple algebraic groups.** (Supplements to Bruhat's talk.) Let k be a *local field*, i.e., a field with nontrivial, nonarchimedean, discrete valuation. We denote by $\mathfrak{O}$ (resp. $\mathfrak{p}$, resp. π) the ring of integers (resp. the unique maximal ideal in $\mathfrak{O}$, resp. a generator of the ideal $\mathfrak{p}$). We also denote by κ the residue class field $\mathfrak{O}/\mathfrak{p}$.

Now let G be a connected, semisimple algebraic group of Chevalley type over the local field k. Let A be a maximal k-split torus of G and Φ the root system of (G, A). We denote by P_r (resp. by P) the $\boldsymbol{Z}$-module generated by all roots (resp. by all weights). Note that P_r and P are lattices of the vector space $\langle\Phi\rangle_{\boldsymbol{R}}$ spanned by Φ over $\boldsymbol{R}$. We recall also that an element λ in $\langle\Phi\rangle_{\boldsymbol{R}}$ is in P if and only if $2(\lambda, \alpha)/(\alpha, \alpha)$ is in $\boldsymbol{Z}$ for all α in Φ, where (,) is a suitable inner product in $\langle\Phi\rangle_{\boldsymbol{R}}$ (cf. Borel's talk p. 13). In particular, one has $P \supset P_r$ and P/P_r is a finite abelian group.

Now it is known that there is associated canonically a sublattice Γ such that $P \supset \Gamma \supset P_r$ and that $A_k \cong \operatorname{Hom}(\Gamma, k^*)$ (cf. [3]). We denote by h (χ) the element in A_k which corresponds to χ in $\operatorname{Hom}(\Gamma, k^*)$. Also for each root α, there is associated a rational homomorphism $x_\alpha\colon G_a \to G$ defined over k, where G_a is the additive group of the universal domain. (Note that G is simply connected (resp. the adjoint group, i.e., centerless) if and only if the associated lattice Γ coincides with P (resp. with P_r).)

Now let N be the normalizer of A in G. We shall now construct a generalized Tits system (G_k, B, N_k) on G_k by taking a certain subgroup B. Let $\mathfrak{G}_{\mathfrak{O}}$ be the Chevalley lattice in the Lie algebra $\mathfrak{G}_k$ of G over k (cf. Bruhat's talk and also Cartier's talk). We denote by $G_{\mathfrak{O}}$ the stabilizer of the Chevalley lattice $\mathfrak{G}_{\mathfrak{O}}$ in G_k:

$$G_{\mathfrak{O}} = \{g \in G_k; \operatorname{Ad}(g)\mathfrak{G}_{\mathfrak{O}} = \mathfrak{G}_{\mathfrak{O}}\}.$$

Then one can show [8] that $G_{\mathfrak{O}}$ is generated by the following elements in G_k:

$$\begin{aligned} &x_\alpha(t) && (t \in \mathfrak{O}; \alpha \in \Phi) \quad \text{and} \\ &h(\chi) && (\chi \in \operatorname{Hom}(\Gamma, \mathfrak{O}^*)), \end{aligned}$$

where $\mathfrak{O}^*$ means the group of invertible elements in $\mathfrak{O}$. Thus it is seen that the homomorphism ϕ of $G_{\mathfrak{O}}$ defined by the reduction mod $\mathfrak{p}$ maps $G_{\mathfrak{O}}$ onto the Chevalley group G_κ over κ associated to the lattice Γ. Thus one gets a "good reduction" (cf. Bruhat's talk).

Now let us fix a linear ordering in Φ. Then this determines a Borel subgroup B_κ of G_κ. Put

$$B = \phi^{-1}(B_\kappa).$$

As in the case where G is simply connected, the subgroup B thus defined is unique up to the conjugacy by elements in G_k (see Bruhat's talk). Now one can show [8] that our subgroup B is generated by the following elements in G_k:

$$\begin{aligned} &x_\alpha(t) && (t \in \mathfrak{p}, \alpha \in \Phi_+) \\ &x_\beta(t) && (t \in \mathfrak{O}, \beta \in \Phi_-) \\ &h(\chi) && (\chi \in \mathrm{Hom}(\Gamma, \mathfrak{O}^*)). \end{aligned}$$

Note that one gets $A_{\mathfrak{O}} = N_k \cap B$, and $A_{\mathfrak{O}}$ is generated by the elements $h(\chi)$, $\chi \in \mathrm{Hom}(\Gamma, \mathfrak{O}^*)$.

Our main purpose here is the following:

THEOREM. *(G_k, B, N_k) is a generalized Tits system on G_k.*

For the proof of this theorem together with other properties of B, see **[8]**. Let us describe here the structure of the factor group $N_k/B \cap N_k = N_k/A_{\mathfrak{O}}$. To begin with, we recall the notion of *the affine Weyl group* $\tilde{W}(\Phi)$ associated to the root system Φ. We denote by $w_{\alpha,\nu}$ $(\alpha \in \Phi, \nu \in \boldsymbol{Z})$ the reflection mapping of the Euclidean space $\langle \Phi \rangle_{\boldsymbol{R}}$ with respect to the hyperplane $\{x \in \langle \Phi \rangle_{\boldsymbol{R}};\ (\alpha, x) = \nu\}$, i.e.,

$$w_{\alpha,\nu}(x) = x - (x, \alpha) \cdot \alpha^* + \nu\alpha^*,$$

where $\alpha^* = 2\alpha/(\alpha, \alpha)$. We denote by $\tilde{W}(\Phi)$ the group generated by the reflections $w_{\alpha,\nu}$ $(\alpha \in \Phi, \nu \in \boldsymbol{Z})$, and call it the affine Weyl group associated to Φ. Note that the Weyl group $W(\Phi)$ is the subgroup of $\tilde{W}(\Phi)$ generated by the reflections $w_{\alpha,0}$ $(\alpha \in \Phi)$, and that $\tilde{W}(\Phi)$ is the semidirect product of $W(\Phi)$ and the normal subgroup D consisting of the translations of the following form: $x \rightarrow x + d$, where d is in the lattice $\Gamma^\perp = \{d \in \langle \Phi \rangle_{\boldsymbol{R}};\ (d, \gamma) \in \boldsymbol{Z} \text{ for all } \gamma \in \Gamma\}$. Thus $\tilde{W}(\Phi) = W(\Phi) \cdot D$, $D \cong \Gamma^\perp \cong \mathrm{Hom}(\Gamma, \boldsymbol{Z})$.

Now one gets **[8]** $N_k/A_{\mathfrak{O}} \cong \Omega \cdot \tilde{W}(\Phi)$ (semidirect product) where Ω is a finite abelian group isomorphic with P/Γ. The set I of generating involutive elements of $\tilde{W}(\Phi)$ appearing in the structure of the generalized Tits system (G_k, B, N_k) is given as follows **[8]**: let $\Phi = \Phi_1 \cup \cdots \cup \Phi_r$ be the decomposition of the root system Φ into irreducible components Φ_i. Let $\Delta_i = \{\alpha_1^{(i)}, \cdots, \alpha_{l_i}^{(i)}\}$ be the set of all simple roots in Φ_i (relative to the given ordering) and $\alpha_0^{(i)}$ the highest root in Φ_i. Then I is given by

$$I = \{w_{\alpha_j^{(i)},0}\ (1 \leqq i \leqq r, 1 \leqq j \leqq l_i),\quad w_{\alpha_0^{(i)},1}\ (1 \leqq i \leqq r)\}.$$

We refer to **[8**, §1**]** as for the more detailed description of the groups $\Omega \cdot \tilde{W}(\Phi)$, $\tilde{W}(\Phi)$.

We note that the analogue of the above theorem is also true for a reductive algebraic group G defined over a local field k which has a k-split maximal torus.

EXAMPLE. Let $G = \mathrm{GL}_n$. Then $G_k = \mathrm{GL}(n, k)$ and $G_{\mathfrak{O}} = \mathrm{GL}(n, \mathfrak{O})$. With respect to the usual ordering of roots, we get

$$B = \begin{pmatrix} \mathfrak{O}^* & & & \mathfrak{p} \\ & \ddots & & \\ & & \ddots & \\ \mathfrak{O} & & & \mathfrak{O}^* \end{pmatrix}, \quad A_k = \begin{pmatrix} k^* & & & 0 \\ & \ddots & & \\ & & \ddots & \\ 0 & & & k^* \end{pmatrix}.$$

Moreover we have $N_k = A_k \cdot S_n$, where S_n is the subgroup of G_k consisting of all permutation matrices. (Hence S_n may be regarded as the symmetric group of degree n.) Put

$$D=\left\{\begin{pmatrix}\pi^{\nu_1} & & 0\\ & \ddots & \\ 0 & & \pi^{\nu_n}\end{pmatrix};\nu_1,\cdots,\nu_n\in \boldsymbol{Z}\right\}.$$

Then $A_k = A_{\mathfrak{D}} \cdot D$ (direct product) with $A_{\mathfrak{D}} = A_k \cap B$, and one gets $N_k = A_{\mathfrak{D}}(DS_n)$ (semidirect product). Thus one gets **[4]** a generalized Tits system (G_k, B, N_k) with the following factor group:

$$N_k/B \cap N_k \cong \Omega \cdot \tilde{W},$$

where $\Omega \cong N(B)/B \cong \boldsymbol{Z}$ and $\tilde{W}$ is generated by involutive elements $w_1, \cdots, w_n$ in DS_n given by

$$w_i=\left(\begin{array}{c|cc|c} I_{i-1} & & & 0\\ \hline & 0 & 1 & \\ & 1 & 0 & \\ \hline 0 & & & I_{n-i-1}\end{array}\right)\quad(1\leqq i\leqq n-1),\quad w_n=\left(\begin{array}{c|ccc|c} 0 & & 0 & & \pi \\ \hline & 1 & & & \\ 0 & & \ddots & & 0\\ & & & 1 & \\ \hline \pi^{-1} & & 0 & & 0\end{array}\right).$$

Note that $N(B) = \{\omega\}B$ is a semidirect product where ω is an element in DS_n given by

$$\omega=\begin{pmatrix}0 & & & & \pi\\ 1 & 0 & & & \\ & 1 & 0 & & \\ & & \ddots & \ddots & \\ & & & 1 & 0\end{pmatrix}.$$

Furthermore we have $\omega w_i \omega^{-1} = w_{i+1}$ $(1 \leqq i \leqq n;\ w_{n+1} = w_1)$.

3. **A characterization of the subgroup** B **(cf. §2) for locally compact ground fields.** In this section we assume that k is a locally compact field with the (finite) residue class field κ of characteristic p.

Let G be a semisimple algebraic group defined over k. One sees then that for any open compact subgroup K of G_k, the normalizer $N(K)$ of K in G_k is also open and compact. Using this fact, one can prove the following theorem:

THEOREM (SYLOW). *Let G be a semisimple algebraic group defined over k. Then G_k has a maximal pro-p-subgroup S. Furthermore, any pro-p-subgroup of G_k is contained in a conjugate of S.*

We recall the terminologies used above: pro-finite group means the projective limit of finite groups; pro-p-group means the projective limit of finite p-groups.

Thus any two maximal pro-p-subgroup of G_k are conjugate. A maximal pro-p-subgroup of G_k is called a *Sylow subgroup* of G_k.

COROLLARY. *Let B be the normalizer in G_k of a Sylow subgroup S of G_k. Then, distinct subgroups of G_k containing B are never mutually conjugate in G_k, and each of them equals its own normalizer in G_k.*

Now for simply connected, semisimple groups of Chevalley type, we have the following

PROPOSITION (MATSUMOTO). *Let G be a connected, simply connected, semisimple group of Chevalley type over k. Then our subgroup B of G_k introduced in §2 is the normalizer of a Sylow subgroup of G_k.*

This proposition gives in a certain sense a "p-analytic" characterization of our BN-pair structure in G_k.

4. **Applications.**

4.1. *Maximal compact subgroups.* Let G be a connected, semisimple algebraic group of Chevalley type over a local field k. Then, since we have a generalized Tits system (G_k, B, N_k) on G_k (cf. §2), we can determine the conjugacy classes of subgroups of G_k containing a conjugate of B. Thus, in particular, when k is locally compact, we can determine the conjugacy classes of maximal compact subgroups of G_k. As an example, we shall give a table of the number s of conjugacy classes of the maximal compact subgroups of G_k containing B, when G is the adjoint group of simple groups [**8**].

Type of G	s
A_l	the number of (positive) divisors of $l + 1$
B_l and C_l	$l + 1$
D_l $(l = 2m + 1)$	l
D_l $(l = 2m)$	$l + 2$
E_6	5
E_7	8
E_8	9
F_4	5
G_2	3

Also, if G is simply connected and simple, then $s = l + 1$, when l is the rank of G [**8**].

We note that these values of s are shown to be the number of conjugacy classes of maximal compact subgroups of G_k by Hijikata [**5**], when G is of classical type. Thus it is an interesting question to prove (or disprove) this fact in general. Or one may formulate in the following way:

CONJECTURE 1. *Let G be a connected, semisimple algebraic group of Chevalley type over a locally compact field k. Then, every maximal compact subgroup K of G_k contains a conjugate of B (the subgroup introduced in* §2).

In other words, B has a fixed point on the homogeneous space G_k/K. In this respect, the following conjecture concerning the structure of the homogeneous space G_k/B seems to be interesting.

Let G_C be a connected, simply connected, complex semisimple Lie group (which is an algebraic linear group as is well known). Let k be the formal power series field $C((t))$ of one variable over C and $\mathfrak{O}$ be the ring of integral power series in k:

$$\mathfrak{O} = \left\{ \sum_{i=0}^{\infty} a_i t^i ; a_0, a_1, \cdots, \in C \right\}.$$

Then $\mathfrak{p} = t \cdot \mathfrak{O}$. Thus we can consider our subgroup B (in §2) in G_k. One has $G_k = \bigcup_{\sigma \in \tilde{W}} B\sigma B$. Hence G_k/B is a disjoint union of the sets $B\sigma B/B$. Now it is easy to show that $B\sigma B/B$ has the structure of a complex affine cell of dimension $\lambda(\sigma)$, where $\lambda(\sigma)$ is the word-length of σ relative to the generators given in §2 of the affine Weyl group $\tilde{W}$ (cf. [**8**]). The subset $G_{\mathfrak{O}}/B$ of G_k/B is easily identified with the generalized flag manifold G_C/B_C, where B_C is a Borel subgroup of G_C, because $G_C \subset G_k$ and $G_C \cap B = B_C$. Under this setting, let us state the following

CONJECTURE 2. *There exists a structure of a topological space of G_k/B with the following properties*:

(i) *G_k/B is an infinite dimensional* CW-*complex.*

(ii) *$G_k/B = \bigcup_{\sigma \in W} (B\sigma B/B)$ is a cellular decomposition of G_k/B. Each cell $B\sigma B/B$ is homeomorphic to $R^{2\lambda(\sigma)}$.*

(iii) *The Poincaré series $P(G_k/B, t)$ of G_k/B is equal to the product of the Poincaré polynomial $P(G_C/B_C, t)$ of G_C/B_C with Poincaré series $P(\Omega(G_C), t)$ of the loop space on G_C. Note that these Poincaré series are given by Bott as follows, using the exponents $m_1, \cdots, m_l$ of G_C*:

$$P(G_C/B_C, t) = \prod_{i=1}^{l} (1 + t^2 + t^4 + \cdots + t^{2m_i}) = \sum_{\sigma \in W} t^{2\lambda(\sigma)},$$

$$P(\Omega(G_C), t) = \prod_{i=1}^{l} (1 - t^{m_i})^{-1}.$$

Or, more strongly,

(iii)′ *G_k/B is homeomorphic to the product space $G_C/B_C \times \Omega(G_C)$. (Or G_k/B has the same homotopy type as the above product space.)*

(iv) (*Tits*) *G_k/B is the inductive limit of projective varieties of finite dimension.* (*A more precise statement of this conjecture has been given by Tits in his talk.*)

4.2. *Elementary divisor theorem.* Let $\mathfrak{O}$ be a Dedekind domain with the quotient field k. Then each prime ideal $\mathfrak{p}$ of $\mathfrak{O}$ defines a nontrivial, discrete, nonarchimedian valuation $x \to |x|_{\mathfrak{p}}$ of the quotient field k of $\mathfrak{O}$. The localization of $\mathfrak{O}$ relative to $\mathfrak{p}$ is denoted by $\mathfrak{O}_\mathfrak{p}$, i.e., $\mathfrak{O}_\mathfrak{p}$ is the ring of integers of k relative to the valuation $x \to |x|_\mathfrak{p}$. Then $\mathfrak{O}$ is the intersection of all localizations $\mathfrak{O}_\mathfrak{p}$ of $\mathfrak{O}$.

Now let G be a connected, semisimple algebraic group of Chevalley type over k. Then, fixing a Chevalley lattice in the Lie algebra $\mathfrak{G}_k$, one has the subgroups $G_\mathfrak{O}, G_{\mathfrak{O}_\mathfrak{p}}$ of G_k. Let A be the associated maximal k-split torus. Then by the structure of generalized Tits system on G_k with respect to the valuation $x \to |x|_\mathfrak{p}$, one sees that [8] $G_k = G_{\mathfrak{O}_\mathfrak{p}} A_k G_{\mathfrak{O}_\mathfrak{p}}$ for all prime ideal $\mathfrak{p}$ in $\mathfrak{O}$. Thus a natural question arises: can one replace $G_{\mathfrak{O}_\mathfrak{p}}$ by $G_\mathfrak{O} = \bigcap_\mathfrak{p} G_{\mathfrak{O}_\mathfrak{p}}$, i.e., does one get

$$G_k = G_\mathfrak{O} A_k G_\mathfrak{O}?$$

Now, this is not true in general. A counter example is obtained by Y. Ihara for the case $G = \mathrm{SL}_2$, $k = Q(\sqrt{(-5)})$, $\mathfrak{O}$ = "the principal order in k." On the other hand, this fact is known to be valid together with some uniqueness property when $\mathfrak{O}$ is a principal ideal domain and G is of classical type. (It is called the elementary divisor theorem.) In this respect, it is seen that a similar theorem is true for any semisimple groups of Chevalley type.

Thus, let k be the quotient field of a principal ideal domain $\mathfrak{O}$. Let G be a connected, semisimple algebraic group of Chevalley type over k. Let Γ be the lattice between the weight-lattice P and the root lattice P_r associated to G (cf. §2). We denote $\chi \to h(\chi)$ the isomorphism from $\mathrm{Hom}(\Gamma, k^*)$ onto A_k, where A is a k-split maximal torus of A. Fixing a Chevalley lattice associated to A, the subgroup $G_\mathfrak{O}$ is defined. Now, fixing an ordering in the root system Φ of (G, A), one gets the notion of a *dominant element* in A_k; i.e., an element $h(\chi) \in A_k$ with $\chi \in \mathrm{Hom}(\Gamma, k^*)$ is called dominant if $\chi(\Phi_+) \subset \mathfrak{O}$. We denote by A_k^+ the set of all dominant elements in A_k. Then, A_k^+ is a semigroup in A_k. A_k^+ contains a subgroup $A_\mathfrak{O} = \{h(\chi); \chi(\Gamma) \subset \mathfrak{O}^*\}$. Under these settings, we get the following elementary divisor theorem.

THEOREM (MATSUMOTO). $G_k = G_\mathfrak{O} A_k^+ G_\mathfrak{O}$. *Moreover, the space* $G_\mathfrak{O}\backslash G_k/G_\mathfrak{O}$ *of double cosets of* $G_k \bmod G_\mathfrak{O}$ *is bijective with* $A_k^+/A_\mathfrak{O}$ *by the natural mapping* $a \cdot A_\mathfrak{O} \to G_\mathfrak{O} \cdot a \cdot G_\mathfrak{O}$.

5. **Hecke rings associated to a generalized Tits system.** (Cf. Shimura's talk.) Let us recall the notion of the Hecke ring $\mathscr{H}(G, B)$ associated to a pair of a group G and a subgroup B of G such that B is commensurable with any of its conjugates, i.e., $[B : B \cap \sigma B \sigma^{-1}] < \infty$ for all σ in G. Let $\mathscr{H} = \mathscr{H}(G, B)$ be the free Z-module spanned by the double cosets $S_\sigma = B\sigma B$ $(\sigma \in G)$. Then a multiplication is defined in $\mathscr{H}$ as follows:

$$S_\sigma S_\tau = \sum_\rho m_{\sigma,\tau}^\rho S_\rho,$$

where $m_{\sigma,\tau}^\rho$ is the number of cosets of the form Bx contained in $(B\sigma^{-1}B\rho) \cap (B\tau B)$. It is seen that $m_{\sigma,\tau}^\rho$ is independent of the choice of the representatives σ, τ, ρ in the double coset; moreover, given σ, τ, the number of the double cosets $B\rho B$ satisfying $m_{\sigma,\tau}^\rho \neq 0$ is finite. Furthermore, it is shown that $\mathscr{H}(G, B)$ becomes an associative algebra with the unit element over $\mathbf{Z}$ (see e.g. [7]). K being any field (or commutative ring), $\mathscr{H}(G, B) \otimes_{\mathbf{Z}} K$ is denoted by $\mathscr{H}_K(G, B)$ and is called the Hecke algebra of the pair (G, B) over K.

Now let us assume that (G, B, N) be a generalized Tits system on G with the factor group $\Omega W = N/B \cap N$ and standard involutive generators $I = \{w_i\}$ of W. For any $\sigma \in W$, we denote by $\lambda(\sigma)$ the length of a reduced expression of σ in terms of I. Consider the normal subgroup $G_0 = BWB$ of G and the induced Tits system (G_0, B_0, N_0) on G_0 where $B_0 = B$, $N_0 = N \cap G_0$. Then, as is seen easily, B is commensurable with any conjugate in G if and only if B_0 is commensurable with any conjugate in G_0. Moreover, when this is the case, $\mathscr{H}(G, B)$ is obtained from $\mathscr{H}(G_0, B_0)$ as follows: we note that Ω acts on the ring $\mathscr{H}(G_0, B_0)$ as a group of automorphisms as follows: for $\rho \in \Omega$ and for $\sigma \in W$, $B_0\sigma B_0 \to B_0(\rho\sigma\rho^{-1})B_0$, or putting $S_\sigma = B_0\sigma B_0$, we express this automorphism by $S_\sigma \to \rho(S_\sigma) = S_{\rho\sigma\rho^{-1}}$. Now introduce a new multiplication in the tensor product $\mathbf{Z}[\Omega] \otimes_{\mathbf{Z}} \mathscr{H}(G_0, B_0)$ as follows ($\mathbf{Z}[\Omega]$ means the group ring of Ω over $\mathbf{Z}$):

$$(\rho \otimes S_\sigma)(\rho' \otimes S_{\sigma'}) = \rho\rho' \otimes (\rho')^{-1}(S_\sigma)S_{\sigma'}$$

for any ρ, $\rho' \in \Omega$ and σ, $\sigma' \in W$. Then one obtains a new ring structure on

$$\mathbf{Z}[\Omega] \otimes_{\mathbf{Z}} \mathscr{H}(G_0, B_0).$$

The ring thus obtained is denoted by $\mathbf{Z}[\Omega] \tilde{\otimes}_{\mathbf{Z}} \mathscr{H}(G_0, B_0)$, and is called the *twisted tensor product* of $\mathbf{Z}[\Omega]$, $\mathscr{H}(G_0, B_0)$. Now we get

PROPOSITION. $\mathscr{H}(G, B) \cong \mathbf{Z}[\Omega] \tilde{\otimes}_{\mathbf{Z}} \mathscr{H}(G_0, B_0)$.

Thus the question about the structure of the Hecke ring $\mathscr{H}(G, B)$ for a generalized Tits system (G, B, N) is reduced to the case where (G, B, N) is a usual Tits system; and in this case, the question was settled by [10] as follows.

Let (G, B, N) be a Tits system with the Weyl group W, and let $I = \{w_i\}$ the standard involutive generators of W. Suppose that B is commensurable with $w_iBw_i^{-1}$ for any $w_i \in I$. Then B is commensurable with any of its conjugates in G. Furthermore, for a reduced expression $\sigma = w_{i_1} \cdots w_{i_r}$ ($r = \lambda(\sigma)$) of $\sigma \in W$, one has

$$S_\sigma = S_{i_1} \cdots S_{i_r} \qquad (\text{where } S_j = S_{w_j}).$$

Thus the first half of the following theorem is obtained.

THEOREM [10]. *The set $\{S_i; i \in I\}$ generates the ring $\mathscr{H}(G, B)$. A system of defining relations for this generator $\{S_i\}$ is given as follows:*

$$S_i^2 = q_i \cdot 1 + (q_i - 1) \cdot S_i \quad (\textit{for all } i \in I),$$

$$(S_iS_j)^{m_{ij}} = (S_jS_i)^{m_{ij}}, \textit{ if the order of } w_iw_j \textit{ is } 2m_{ij} < \infty,$$

$$(S_iS_j)^{m_{ij}}S_i = (S_jS_i)^{m_{ij}}S_j, \textit{ if the order of } w_iw_j \textit{ is } 2m_{ij} + 1 < \infty.$$

where q_i is the number of cosets of the form Bx contained in Bw_iB.

Example 1. Let k be a local field such that $\kappa = \mathfrak{O}/\mathfrak{p}$ is finite. Let G be a simply connected, semisimple algebraic group of Chevalley type over k. Then the Tits system (G_k, B, N_k) in §2 satisfies the assumption made above relative to the commensurability of B with its conjugates. More precisely, for $\sigma \in W$, $B\sigma B$ contains $q^{\lambda(\sigma)}$ cosets of the form Bx, where q is the cardinality of the residue class field κ. In particular, all q_i's in the above theorem are equal to q in this case. Furthermore, the order of any $w_i w_j$ is always finite. [Especially, if G is SL_2, then it is seen (this is due to Oscar Goldman) that $\mathscr{H}_{\boldsymbol{Q}}(G_k, B) \cong \boldsymbol{Q}[\tilde{W}]$, where $\tilde{W}$ is the affine Weyl group of SL_2. (Note that $\tilde{W}$ is isomorphic with the free product of two copies of $\boldsymbol{Z}_2$ (= cyclic group of order 2).)

In this case, $G_{\mathfrak{O}}$ is also commensurable with any of its conjugate in G_k. Moreover, one can show that the Hecke ring $\mathscr{H}(G_k, G_{\mathfrak{O}})$ is commutative and is isomorphic with the polynomial ring in l variables over $\boldsymbol{Z}$ (l being the rank of G) (see [**1**], [**11**], [**12**]). We note the following formula for the number of cosets of the form $G_{\mathfrak{O}} \cdot x$ in $G_{\mathfrak{O}} \cdot h(\chi) \cdot G_{\mathfrak{O}}$ (with $h(\chi) \in A_k^+$). We may assume that $\chi(\lambda) = \pi^{(d,\lambda)}$ for some $d \in D = P^\perp = \{x \in \langle\Phi\rangle_{\boldsymbol{R}}; (x, P) \subset \boldsymbol{Z}\}$. Then the number # desired is given by

$$\# = q^{\varepsilon(d)} \sum_{\sigma \in W_d^1} q^{\lambda(\sigma)},$$

where (regarding $D \subset \tilde{W}$ as in §2),

$$\begin{aligned}\varepsilon(d) &= \operatorname*{Min}_{w \in W} \lambda(dw)\\ &= \sum_{\alpha \in \Phi_+ ; (\alpha, d) > 0} |(d, \alpha) - 1| + \sum_{\alpha \in \Phi_+ ; (\alpha, d) \leqq 0} |(d, \alpha)|,\end{aligned}$$

and W_d^1 is the following subset of W. Let W_d be the subgroup of W defined by $W_d = \{\sigma \in W ; \sigma(d) = d\}$. Then W_d is generated by the $w_{\alpha_i, 0}$ with $(\alpha_i, d) = 0$ ($\alpha_1, \cdots, \alpha_l$ being the simple roots). Now W_d^1 is defined by

$$W_d^1 = \{\sigma \in W ; \lambda(w\sigma) \geqq \lambda(\sigma) \text{ for any } w \in W_d\}.$$

(See Kostant [**9**].)

We note also that, if k is the quotient field of a principal ideal domain $\mathfrak{O}$, the Hecke ring $\mathscr{H}(G_k, G_{\mathfrak{O}})$ of a simply connected, semisimple algebraic group G of Chevalley type over k is isomorphic with the tensor product of the Hecke rings $\mathscr{H}(G_k, G_{\mathfrak{O}_{\mathfrak{p}}})$:

$$\mathscr{H}(G_k, G_{\mathfrak{O}}) \cong \otimes_{\mathfrak{p}} \mathscr{H}(G_k, G_{\mathfrak{O}_{\mathfrak{p}}}).$$

Example 2. Let G be a *finite* group and (G, B, N) be a Tits system on G with the Weyl group W. Then one has

Theorem (Tits). *Let k be an algebraically closed field whose characteristic does not divide the orders of G, W. Then $\mathscr{H}_k(G, B) \cong k[W]$.*

See the appendix for the proof.

Appendix: Proof After Tits of $\mathscr{H}_k(G, B) \cong k[W]$ for a Finite Tits System

1. **Rings obtained by a specialization.** Let A be an associative algebra over a commutative ring $\mathfrak{O}$. Let ϕ be a homomorphism of $\mathfrak{O}$ into a commutative ring $\mathfrak{O}'$. Then one has an $\mathfrak{O}$-module structure on $\mathfrak{O}'$ by $\alpha \cdot \beta = \phi(\alpha)\beta$ ($\alpha \in \mathfrak{O}, \beta \in \mathfrak{O}'$). Thus one may consider the tensor product

$$A_\phi = A \otimes_{\mathfrak{O}} \mathfrak{O}',$$

which has an obvious algebra-structure over $\mathfrak{O}'$. Note that if ϕ is surjective, then the homomorphism $\phi^* : A \to A_\phi$ defined by $\phi^*(a) = a \otimes 1$ is also surjective and $\mathrm{Ker}(\phi^*) = \mathrm{Ker}(\phi)$. Thus

$$A_\phi \cong A/A \cdot \mathrm{Ker}(\phi).$$

In particular, if A is a free $\mathfrak{O}$-module of finite rank with a basis $\{u_\lambda\}$, then A_ϕ is also a free $\mathfrak{O}'$-module with a basis $\{\phi^*(u_\lambda)\}$. The structure constants $\{C^\nu_{\lambda\mu}\}$ of A relative to $\{u_\lambda\}$ are mapped by ϕ into the structure constants $\{\phi(C^\nu_{\lambda\mu})\}$ of A_ϕ relative to $\{\phi^*(u_\lambda)\}$. Hence, Δ, Δ' being the discriminants of A, A_ϕ respectively, one has $\phi(\Delta) = \Delta'$.

For the special case where $\mathfrak{O}$ is a polynomial ring $k[t_1, t_2, \cdots t_r]$ over a field k and ϕ is the specialization $\mathfrak{O} \to k$ over k defined by $\phi(t_i) = \alpha_i$, we denote A_ϕ also by $A(\alpha_i)$ for brevity.

PROPOSITION 1. *Let $\mathfrak{O} = k[t_1, \cdots, t_r]$ be the polynomial ring ovɛr an algebraically closed field k. Suppose that A is an associative algebra over $\mathfrak{O}$ such that*

(i) *A is a free $\mathfrak{O}$-module of finite rank, and*

(ii) *the discriminant $\Delta(t_1, \cdots, t_r)$ of A (relative to a basis of A) is not zero. Then for any $(\alpha_i) \in k^r$, $(\beta_i) \in k^r$ such that $\Delta(\alpha_i) \neq 0$, $\Delta(\beta_i) \neq 0$, one has $A(\alpha_i) \cong A(\beta_i)$ as k-algebra.*

For the proof, we note that $A(\alpha_i)$ is separable, semisimple and refer to Gerstenhaber [14]. Also we note that an elementary proof is possible for this particular case. In fact, Ω being the algebraic closure of the quotient field of $\mathfrak{O}$, one gets the following isomorphism as Ω-algebra

$$A \otimes_{\mathfrak{O}} \Omega \cong A(\alpha_i) \otimes_k \Omega.$$

2. **An algebra associated with a Coxeter group.** By Proposition 1 above, in order to prove $\mathscr{H}_k(G, B) \cong k[W]$, it is enough to show the existence of an algebra A over some polynomial ring $\mathfrak{O} = k[t_1, \cdots, t_r]$ with above conditions and the existence of two points $(\alpha_i) \in k^r$, $(\beta_i) \in k^r$ such that

$$\Delta(\alpha_i) \neq 0,\ \Delta(\beta_i) \neq 0,\ A(\alpha_i) \cong \mathscr{H}_k(G, B),\ A(\beta_i) \cong k[W].$$

Now such an algebra was constructed by Tits as follows.
Let W be an Coxeter group with a fundamental generating involution $R = \{r\}$, i.e., the defining relations for R are obtained by $(rs)^{n_{rs}} = 1$ (n_{rs} being the order of

rs for all r and s in R; $n_{rr} = 1$). Denote by $l(w)$ the length of $w \in W$ relative to R. Then

LEMMA 1. *If $r, s \in R$ and $w \in W$ satisfy $l(rws) = l(w)$, $l(rw) = l(ws)$, then $s = w^{-1}rw$.*

Now let k be any commutative ring. Let C be the set of conjugacy classes represented by elements in R, and let $\{u_c, v_c; c \in C\}$ be indeterminates over k. We write also u_r, v_r for u_c, v_c for r in c. Denote by $\mathfrak{O}$ the polynomial ring

$$k[u_c, v_c; c \in C].$$

PROPOSITION 1. *Let V be the free $\mathfrak{O}$-module spanned by W. Then there exists a K-bilinear, associative multiplication $*$ in V such that*

$$\begin{aligned} r*w &= rw \qquad \text{if } l(rw) > l(w), \\ &= u_r rw + v_r w, \qquad \text{if } l(rw) < l(w). \end{aligned}$$

Moreover, such a multiplication is unique.

PROOF. Uniqueness is obvious. Let us prove the existence. Define

$$P_r, \lambda_r \in \operatorname{End}_{\mathfrak{O}}(V) \qquad (r \in R)$$

as follows:

$$\begin{aligned} P_r(w) &= rw & &\text{if } l(rw) > l(w), \\ &= u_r rw + v_r w, & &\text{if } l(rw) < l(w), \\ \lambda_r(w) &= wr & &\text{if } l(rw) > l(w), \\ &= u_r wr + v_r w, & &\text{if } l(rw) < l(w). \end{aligned}$$

Then, using Lemma 1, one can check $P_r\lambda_s = \lambda_s P_r$ for any $r, s \in R$. Let $\mathfrak{R}$ (resp. $\mathfrak{L}$) be the $\mathfrak{O}$-subalgebras of $\operatorname{End}_{\mathfrak{O}}(V)$ generated by $\{P_r; r \in R\}$ (resp. by $\{\lambda_r; r \in R\}$). It is seen that the mappings $\rho^*: \mathfrak{R} \to V$, $\lambda^*: \mathfrak{L} \to V$ defined by $\rho^*(\phi) = \phi(1)$ $(\phi \in \mathfrak{R})$, $\lambda^*(\psi) = \psi(1)$ $(\psi \in \mathfrak{L})$ are both bijective.

In fact, for any reduced expression $w = r_1 \cdots r_n$, one has

$$\rho^*(\rho_{r_1} \cdots \rho_{r_n}) = w.$$

Thus ρ^* is surjective. Same is true for λ^*. Injectivity of ρ^* is seen as follows from the commutativity of P_r, λ_s above: let $\rho^*(\phi) = 0$. Then $\phi(1) = 0$. Hence

$$0 = \psi(\phi(1)) = \phi(\psi(1))$$

for all $\psi \in \mathfrak{L}$. Hence $\phi = 0$ by the surjectivity of λ^*.

Now define the product $v*v'(v, v' \in V)$ by

$$\begin{aligned} v*v' &= \rho^*\{\rho^{*-1}(v) \cdot \rho^{*-1}(v')\} \\ &= \{\rho^{*-1}(v)\}(v'). \end{aligned}$$

Then one sees that * defines an algebra structure on V such that $r*w = P_r(w)$, which completes the proof.

Now let us return to the given Tits structure (G, B, W). We assume that k is an algebraically closed field whose characteristic does not divide the orders of G, W. Using above notations, one sees that the $\mathfrak{O}$-algebra $A = (V, *)$ associated to the Coxeter group W (cf. [10]) has the following properties:

(1) The discriminant $\Delta(u_c, v_c; c \in C)$ of A (note that this is a polynomial in the u_c, v_c) is not zero.

(2) By the specialization $u_c \to \alpha_c, v_c \to \beta_c$ $(c \in C; \alpha_c, \beta_c \in k)$, A gives rise to an algebra $A(\alpha_c, \beta_c)$ over k. In particular, by the theorem above one obtains

$A(q_c, q_c - 1) \cong \mathscr{H}_k(G, B)$ where q_c is the number of B-cosets in BrB, where $r \in c$,

$$A(1, 0) \cong k[W].$$

Note that $\mathscr{H}_k(G, B)$ and $k[W]$ are both semisimple algebras over k (cf. [7]). Thus, by our assumption on the characteristic of k, we get $\Delta(\alpha_i) \neq 0$, $\Delta(\beta_i) \neq 0$ for $(\alpha_i) = (q_c, q_c - 1)$, $(\beta_i) = (1, 0)$. This completes the proof.

References

1. F. Bruhat, *Sur une classe de sous-groupes compacts maximaux des groupes de Chevalley sur un corps* $\mathfrak{p}$*-adique*, Publ. Math., I.H.E.S., No. 23 (1964), 46–74.

2. C. Chevalley, *Sur certains groupes simples*, Tôhoku Math. J. **7** (1955), 14–66.

3. C. Chevalley, *Classification des groupes de Lie algébriques*, Séminaire E.N.S., Paris, 1956–1958.

4. O. Goldman and N. Iwahori, *On the structure of Hecke rings associated to general linear groups over* $\mathfrak{p}$*-adic fields* (unpublished).

5. H. Hijikata, *Maximal compact subgroups of some* $\mathfrak{p}$*-adic classical groups*, Mimeographed Notes from Yale University, (1964).

6. ———, *On arithmetic of* $\mathfrak{p}$*-adic Steinberg groups*, Mimeographed Notes from Yale University, 1964.

7. N. Iwahori, *On the structure of a Hecke ring of a Chevalley group over a finite field*, J. Fac. of Sci. Univ. Tokyo **10** (1964), 215–236.

8. N. Iwahori and H. Matsumoto, *On some Bruhat decomposition and the structure of the Hecke rings of the* $\mathfrak{p}$*-adic Chevalley groups*, Publ. Math., I.H.E.S., No. 25 (1965), 5–48.

9. B. Kostant, *Lie algebra cohomology and the generalized Borel–Weil theorem*, Ann. of Math. **74** (1961), 328–380.

10. H. Matsumoto, *Générateurs et relations des groupes de Weyl généralisés*, C. R. Paris **258** (1964), 3419–3422.

11. I. Satake, *Theory of spherical functions on reductive algebraic groups over* $\mathfrak{p}$*-adic fields*, Publ. Math., I.H.E.S., No. 18 (1964), 5–69.

12. T. Tamagawa, *On the* ζ*-functions of a division algebra*, Ann. of Math. **77** (1963), 387–405.

13. J. Tits, *Théorème de Bruhat et sous-groupes paraboliques*, C. R. Paris **254** (1962), 2910–2912.

14. M. Gerstenhaber, *On the deformation of rings and algebras*, Ann. of Math. **79** (1964), 59–103.

On Rational Points on Projective Varieties Defined Over a Complete Valuation Field[1]

BY

TSUNEO TAMAGAWA

1. Let k be a field with a nonarchimedian valuation $|\ |$, k^{n+1} denote the vector space over k of all $(n+1)$-tuples of elements of k and $\boldsymbol{P}_k^n$ denote the projective space of all one-dimensional subspaces of k^{n+1}. The one-dimensional subspace spanned by $x \in k^{n+1}$ will be denoted by $\langle x \rangle$. The norm of $x = (x_0, \cdots, x_n)$ is defined by $\|x\| = \mathrm{Max}(|x_0|, \cdots, |x_n|)$. Let $f(X_0, \cdots, X_n)$ be a homogeneous polynomial of degree d in k. Then the value $\|x\|^{-d}|f(x)|$ is uniquely determined by the point $P = \langle x \rangle \in \boldsymbol{P}_k^n$, so we denote it by $|f(P)|$. If $f(x) = 0$, we simply write $f(P) = 0$. The norm $\|f\|$ of a polynomial $f(X_0, \cdots, X_n) = \sum c_{i0} \cdots {}_{in} X_0^{i_1} \cdots X_n^{i_n}$ is defined by $\|f\| = \mathrm{Max}(|c_{i0} \cdots {}_{in}|)$. Obviously we have $|f(P)| \leqq \|f\|$ for all $P \in \boldsymbol{P}_k^n$. A set of homogeneous polynomials $f_1, \cdots, f_N$ in k will be called a zero set if we have

$$M(f_1, \cdots, f_N) = \mathrm{Inf}_{P \in \boldsymbol{P}_k^n} \mathrm{Max}(|f_1(P)|, \cdots, |f_N(P)|) = 0.$$

Let Ω be a universal domain containing k. Namely Ω is an algebraically closed field containing k such that there exist infinitely many elements in Ω which are algebraically independent over k. We denote the projective space $\boldsymbol{P}_\Omega^n$ by $\boldsymbol{P}^n$.

We will prove the following theorems:

THEOREM 1. *Assume that k is complete and perfect. If a set $\{f_1, \cdots, f_N\}$ of homogeneous polynomials $f_1, \cdots, f_N$ in k is a zero set, then there exists a point $P_0 \in \boldsymbol{P}_k^n$ such that $f_1(P_0) = 0, \cdots, f_N(P_0) = 0$.*

THEOREM 2. *Assume that k is complete and perfect. Let $V \subset \boldsymbol{P}^n$ be a variety defined over k, and V_k denote the set of all k-rational points on V. Let ϕ be a rational function on V defined over k. If ϕ is defined at all points of V_k, then $|\phi(P)|$ is bounded on V_k.*

An immediate consequence of Theorem 2 is the following:

THEOREM 3. *Assume that k is complete and perfect. Let G be a reductive algebraic group defined over k such that there is no subtorus of G which splits over k. Then the group G_k of all k-rational elements of G is bounded.*

[1] This work is partly supported by NSF Contract No. 4428.

If k is locally compact, then the space P_k^n is compact with respect to its natural topology. Hence we have quick proofs of Theorem 1 and Theorem 2 by using the compactness of P_k^n and continuity of $|f(P)|$ or $|\phi(P)|$. In this case, the field k is not necessarily perfect.

2. Let $\{f_1, \cdots, f_N\}$ be a set of homogeneous polynomials in k. Then the set $A(f_1, \cdots, f_N)$ of all $P \in P^n$ with $f_1(P) = 0, \cdots, f_N(P) = 0$ is a k-closed subset of P^n. Conversely if A is a k-closed set in P^n, the ideal $\mathfrak{A}(A)$ of $k[X_0, X_1, \cdots, X_n]$ generated by all homogeneous polynomials f with $f(P) = 0$ for all $P \in A$ is homogeneous and has a finite base $\{f_1, \cdots, f_N\}$ consisting of homogeneous polynomials. If $A = B_1 \cup \cdots \cup B_s$ is the decomposition of a k-closed set A into the k-irreducible components $B_1, \cdots, B_s$ of A, then the dimension of A is defined to be the maximum of $\dim B_1, \cdots, \dim B_s$.

LEMMA 1. *Let $\{f_1, \cdots, f_M\}$ and $\{g_1, \cdots, g_N\}$ be sets of homogeneous polynomials in k. If we have $A(f_1, \cdots, f_M) \subset A(g_1, \cdots, g_N)$ and $\{f_1, \cdots, f_M\}$ is a zero set, then $\{g_1, \cdots, g_N\}$ is a zero set.*

PROOF. From Nullstellensatz of Hilbert, we have

$$g_i(X)^\rho = \sum H_{ij}(X) f_j(X), \qquad i = 1, \cdots, N,$$

where ρ is a positive integer and H_{ij} are homogeneous polynomials in k such that $\deg H_{ij} + \deg f_j = \rho \deg g_i$. Then for $P \in P_k^n$ we have

$$|g_i(P)|^\rho \leqq \operatorname*{Max}_j (\|H_{ij}\| |f_j(P)|).$$

Our assertion is easily proved from this inequality.

A k-closed set $A \subset P^n$ will be called a Z-set if a homogeneous base $\{f_1, \cdots, f_N\}$ of $\mathfrak{A}(A)$ is a zero set. We have the following lemma.

LEMMA 2. *If $\{f_1, \cdots, f_N\}$ is a zero set, then $A(f_1, \cdots, f_N)$ is a Z-set. If A is a Z-set, then all k-closed sets containing A are Z-sets. If A and B are k-closed sets such that $A \cup B$ is a Z-set, then either A or B is a Z-set.*

PROOF. The first two assertions are immediate consequences of Lemma 1. Put $A = A(f_1, \cdots, f_M)$ and $B = B(g_1, \cdots, g_N)$. If $\{f_1, \cdots, f_M\}$ and $\{g_1, \cdots, g_N\}$ are not zero sets, then for every point $P \in P_k^n$, we have

$$\operatorname{Max}(|f_i(P)| |g_j(P)|; 1 \leqq i \leqq M, 1 \leqq j \leqq N) \geqq M(f_1, \cdots, f_M) M(g_1, \cdots, g_N) > 0.$$

Hence the set $\{f_i g_j; 1 \leqq i \leqq M, 1 \leqq j \leqq N\}$ is not a zero set. This set defines the k-closed set $A \cup B$, so $A \cup B$ is not a Z-set.

COROLLARY. *If a k-closed set A is a Z-set, then one of k-irreducible components of A is a Z-set.*

Now the following theorem is obviously equivalent with Theorem 1. The theorem is also true without the perfectness assumption.

THEOREM 4. *Assume that k is complete and perfect. If $A \subset \boldsymbol{P}^n$ is a Z-set, then $A_k = A \cap \boldsymbol{P}^n_k$ is not empty.*

We have to note something about the empty set $\varnothing$. Since $\mathfrak{A}(\varnothing) = k[X_0 \cdots X_n]$, $\mathfrak{A}(\varnothing)$ is obviously not a Z-set. If $\{f_1, \cdots, f_N\}$ is a set of homogeneous polynomials in k such that there is no point $P \in \boldsymbol{P}^n$ with $f_1(P) = 0, \cdots, f_N(P) = 0$, then $\{f_1, \cdots, f_N\}$ is not a zero set. For if $f_i \in k$ for some i, then our assertion is obvious. If $f_i \notin k$, $1 \leqq i \leqq N$, then $0 = (0, \cdots, 0)$ is the only common zero of $f_1, \cdots, f_N$ in Ω^{n+1}, so we have

$$X_i^\rho = \sum_j H_{ij} f_j, \qquad 0 \leqq i \leqq n,$$

with homogeneous polynomials H_{ij}. Then $\{X_0^\rho, \cdots, X_n^\rho\}$ is not a zero set, so $\{f_1, \cdots, f_N\}$ is not a zero set.

3. Now we assume that k is perfect. Let A be a k-irreducible closed set in $\boldsymbol{P}^n$. The set of all $x \in \Omega^{n+1}$ with $\langle x \rangle \in A$ together with 0 is denoted by $\hat{A}$. $\hat{A}$ is a k-irreducible closed set in Ω^{n+1}. A generic point $(x_0, x_1, \cdots, x_n)$ of $\hat{A}$ will be called a homogeneous generic point of A. Let r denote the dimension of A. Then the dimension of $(x_0, x_1, \cdots, x_n)$ over k is $r + 1$. Since k is perfect, $k(x_0, \cdots, x_n)$ is a separably generated extension of k. The set A will be called a k-irreducible set in a general position if the following conditions are satisfied:

(1) $k(x_0, \cdots, x_{r+1}) = k(x_0, \cdots, x_n)$,

(2) $x_{r+1}, \cdots, x_n$ are integral over $k[x_0, \cdots, x_r]$,

(3) X_{r+1} is separably algebraic over $k(x_0, \cdots, x_r)$.

LEMMA 3. *There exist $(n + 1) \times (n + 1)$ matrix $U = (u_{ij})$ in k, $0 \leqq i, j \leqq n$, such that* $\det(u_{ij}) \neq 0$ *and the projective transformation T defined by*

$$\langle x \rangle T = \langle x \cdot U \rangle$$

transforms A in a general position.

PROOF. From normalization lemma, we can find $(n + 1)(r + 1)$ elements u_{ij}, $0 \leqq i \leqq n$, $0 \leqq j \leqq r$ such that $y_j = \sum u_{ij} x_i$, $0 \leqq j \leqq r$, are algebraically independent over k and $x_0, \cdots, x_n$ are integral and separable over $k[y_0, \cdots, y_r]$. Now we can find $u_{0r+1}, \cdots, u_{nr+1}$ so that $y_{r+1} = \sum u_{ir+1} x_i$ generates the field $k(x_0, \cdots, x_n)$ over $k(y_0, \cdots, y_r)$, and the matrix (u_{ij}), $0 \leqq j \leqq r + 1$, is of rank $r + 1$. Now we can add $n - r - 1$ columns to (u_{ij}) so that the matrix (u_{ij}), $0 \leqq i, j \leqq n$ is non-singular. Such construction is possible because k is perfect and infinite (O. Zariski and P. Samuel [2, Chapter V, Theorem 8, p. 266]).

The set A is a Z-set if and only if AT is a Z-set. Now we assume that A is in a general position. Let $G_j(X_0, X_1, \cdots, X_r, X_j)$, $r + 1 \leqq j \leqq n$, be an irreducible polynomial in k such that $\|G_j\| = 1$ and $G_j(x_0, x_1, \cdots, x_r, x_j) = 0$. We have a polynomial G_j for each $r + 1 \leqq j \leqq n$. Put $G(X) = G_{r+1}(X)$, and

$$H(X) = \partial G(X)/\partial X_{r+1}.$$

Since x_{r+1} is separably algebraic over $k(x_0, \cdots, x_r)$, the polynomial $H(X)$ is not equal to 0. If d_j is the degree of $G_j(X)$, then $G_j(X)$ contains a term $cX_j^{d_j}$. Hence the ideal generated by $X_0, \cdots, X_r$ and $\mathfrak{A}(A)$ contains $X_{r+1}^{d_{r+1}}, \cdots, X_n^{d_n}$. Hence if $\{f_1, \cdots, f_N\}$ is a base of $\mathfrak{A}(A)$, then $\{X_0, \cdots, X_r, f_1, \cdots, f_N\}$ is not a zero set. Also we see that the specialization $(x_0, \cdots, x_r) \to (0, \cdots, 0)$ over k is uniquely extended to the specialization $(x_0, \cdots, x_n) \to (0, \cdots, 0)$. Hence the rational mapping π_r of $\boldsymbol{P}^n$ onto $\boldsymbol{P}^{r+1}$ defined by $\langle(a_0, \cdots, a_n)\rangle \to \langle(a_0, \cdots, a_{r+1})\rangle$ is defined at every point of A. Assume that A is a Z-set. Since $\{X_0, \cdots, X_r, f_1, \cdots, f_N\}$ is not a zero set, we have $M(X_0, \cdots, X_r, f_1, \cdots, f_N) = c > 0$. Hence if $0 < \varepsilon < c$, for every $P \in \boldsymbol{P}_k^n, P = \langle(a_0, \cdots, a_n)\rangle$, with $|f_1(P)| < \varepsilon, \cdots, |f_N(P)| < \varepsilon$, we have $\mathrm{Max}(|a_0|, \cdots, |a_n|)\|a\|^{-1} \leqq c$. Hence π_r is defined at P with

$$|f_1(P)| < \varepsilon, \cdots, |f_N(P)| < \varepsilon.$$

Now π_r is a birational morphism of A onto a k-irreducible set $A' = \pi_r(A)$ of $\boldsymbol{P}^r$. The set A' is defined by the polynomial $G(X_0, \cdots, X_{r+1})$. Let P' be a point on A' such that $H(P') \neq 0$. Such P' is a simple point of an absolutely irreducible component V' of A', and does not lie on any other component of A'. Since $x_{r+2}, \cdots, x_n$ are integral over $k[x_0, \cdots, x_r]$, there exist only a finite number of points in $\pi_r^{-1}(P') \cap A$, and they lie on an absolutely irreducible component V of A. Obviously π_r induces a birational morphism of V onto V'. Since P' is a simple point on V' and $\pi_r^{-1}(P') \cap V$ is a finite, nonempty set, $\pi_r^{-1}(P')$ consists of only one point P, and the restriction of π_r^{-1} to V' is defined at P' ("Zariski's Main Theorem," cf. A. Weil [**1**, Chapter VI, Theorem 13, p. 164]). Hence P is a simple point of V, and $k(P') = k(P)$. So if P' is rational over k, then P is also rational over k.

4. Now we assume that k is complete, and $\{f_1, \cdots, f_N, H\}$ is not a zero set. Put $\mu = M(f_1, \cdots, f_N, H)$. Since $\|G\| = 1$, we have $\|H\| \leqq 1$ and $0 < \mu \leqq 1$. We choose ε so that $0 < \varepsilon < \mathrm{Min}(\frac{1}{2}\mu^2, c\mu)$. We have $a = (a_0, \cdots, a_n)$ such that $\|a\| = 1$, $|f_1(a)| < \varepsilon, \cdots, |f_N(a)| < \varepsilon$ and $|G(a)| < \varepsilon$. Then we have $H(a) \geqq \mu$ and $\mathrm{Max}(|a_0|, \cdots, |a_{r+1}|) \geqq c$. Put $F(T) = G(a_0, \cdots, a_r, T)$. Then $F(a_{r+1}) = G(a_0, \cdots, a_{r+1})$ and $(dF/dT)(a_{r+1}) = H(a)$.
We have the following series:

$$b_0 = a_{r+1}, b_1 = b_0 - F(b_0)F'(b_0)^{-1}, b_2 = b_1 - F(b_1)F'(b_1)^{-1}, \cdots.$$

Then we have

$$|F(b_1)| = |(\tfrac{1}{2}F'')(b_0)(F(b_0)F'(b_0)^{-1})^e| \leqq \varepsilon^2\mu^{-2} < \tfrac{1}{2}\varepsilon,$$

$$|F'(b_1)| = |F'(b_0)| \geqq \mu,$$

$$\cdots$$

$$|F(b_\nu)| < \frac{1}{2^\nu}\varepsilon,$$

$$|F'(b_\nu)| \geqq \mu.$$

Hence there exists a limit $\lim_{r\to\infty} bv = a'_{r+1}$, and $F(a'_{r+1}) = G(a_0, \cdots, a_r, a'_{r+1}) = 0$,

$H(a_0, \cdots, a_r, a'_{r+1}) \neq 0$. Now we see that at least one of $a_0, \cdots, a_r$ is not equal to 0. If $a_0 = \cdots = a_r = 0$, then $|a_{r+1}| \geqq c$ and $|a'_{r+1}| \geqq C$, a contradiction. Hence $P' = \langle(a_0, \cdots, a_r, a'_{r+1})\rangle$ satisfies all our conditions.

LEMMA 4. *Assume that k is perfect and complete. Let A be a k-irreducible closed set in a general position $(x_0, x_1, \cdots, x_n)$ a homogeneous generic point of A over k, $G(X_0, \cdots, X_{r+1})$ an irreducible polynomial in k with $G(x_0, \cdots, x_{r+1}) = 0$ and $H(X_0, \cdots, X_{r+1})$ denote the polynomial $\partial G/\partial X_{r+1}$. Let S denote the k-closed set of all P with $H(P) = 0$. If A is a Z-set but $A \cap S$ is not a Z-set, then $A \cap P^n_k = A_k$ is not empty. In this case, A is absolutely irreducible.*

PROOF. Let $\{f_1, \cdots, f_N\}$ be a homogeneous base of $\mathfrak{A}(A)$. By assumption, we see that $\{f_1, \cdots, f_N\}$ is a zero set but $\{f_1, \cdots, f_N, H\}$ is not a zero set. Hence we have a simple point $P' \in \pi_r(A) \cap P^{r+1}_k$ and a simple point $\pi_r^{-1}(P') \cap A$ which is rational over k. Now A is k-irreducible, so if P lies on a component of A, then P lies on every component of A. Hence A contains only one component, so A is absolutely irreducible (and defined over k since k is perfect).

5. PROOF OF THEOREM 4. We use the induction with respect to the dimension of A.[2] Assume that $\dim A = 0$. We may assume that A is k-irreducible and in a general position. Then Lemma 4 shows that $A = A_k = \{P\}$. Now we assume our assertion is true for all Z-set of dimension less than r. Let A be a Z-set of dimension r. We may assume that A is k-irreducible and in a general position. Using the same notations in Lemma 4, we see that if $A \cap S$ is not a Z-set, then A_k is not empty. If $A \cap S$ is a Z-set, then S is a hypersurface and $\dim(A \cap S) = r - 1$. Hence we have $(A \cap S)_k \neq \emptyset$.

PROOF OF THEOREM 2. Let Q be a generic point of V over k. For every $P \in V_k$, there exist a pair of homogeneous polynomials $F(X), G(X) \in k[X_0, \cdots, X_n]$ such that $G(P) \neq 0$ and $\phi(Q) = F(Q)/G(Q)$. The set of all $P' \in V$ with $G(P') \neq 0$ is a k-open subset of V, and V_k is covered by a finite number of such open sets. Hence we have a finite number of pairs $(F_1, G_1), \cdots, (F_s, G_s)$ of homogeneous polynomials in k such that $\deg F_i = \deg G_i$, $\phi(Q) = F_i(Q)/G_i(Q)$ and for every $P \in V_k$ there exists i, $1 \leqq i \leqq S$, such that $\phi(P) = F_i(P)/G_i(P)$. Let $\{f_1, \cdots, f_N\}$ be a homogeneous base of the ideal $\mathfrak{A}(V)$. Then there is no $P \in P^n_k$ with

$$f_1(P) = 0, \cdots, f_N(P) = 0,$$

$G_1(P) = 0, \cdots, G_s(P) = 0$. Hence from Theorem 1, we see that $\{f_1, \cdots, f_N, G_1, \cdots, G_s\}$ is not a zero set. Put $\mu = M(f_1, \cdots, f_N, G_1, \cdots, G_s) > 0$. For every $P \in V_k$, we have $|G_i(P)| \geqq \mu$ for some i, hence

$$|\phi(P)| = |F_i(P)||G_i(P)|^{-1} \leqq \|F_i\|\mu^{-1} \leqq \operatorname{Max}(\|F_1\|, \cdots, \|F_s\|)\mu^{-1}.$$

PROOF OF THEOREM 3. Since G has no k-split subtorus and is reductive, there exists a morphism f of G into a projective variety V defined over k such that f

[2] The idea of using the induction over dim A was suggested by M. Kneser in a conversation with the author.

is defined over k, f is birational and biregular at every point $P \in G$, $f(G)$ is a k-open subset of V and $f(G_k) = V_k$. If u is a rational function on G which is holomorphic at every point of G, then $\phi = u \circ f^{-1}$ is a rational function on V which is defined at every point $P \in V_k$. From Theorem 2, $|\phi|$ is bounded on V_k, so $|u(g)|$ is bounded on G_k. Since matrix coefficients of G are holomorphic functions on G, G_k is bounded.

References

1. A. Weil, *Foundation of algebraic geometry*, 2nd ed. Amer. Math. Soc. Colloq. Publ. Vol. 29, Amer. Math. Soc., Providence, R.I., 1962.

2. O. Zariski and P. Samuel, *Commutative algebra*, Vol. I, Van Nostrand, New York, 1958.

Groups Over Z

BY

BERTRAM KOSTANT

1. Preliminaries.

1.1. Let C be a commutative ring with 1. Let A be a coalgebra over C with diagonal map $d : A \to A \otimes_C A$ (it is assumed A has a counit $\varepsilon : A \to C$) and let R be an algebra over C with multiplication $m : R \otimes_C R \to R$ (it is assumed R has a unit $\rho : C \to R$). Then one knows that $\mathrm{Hom}_C(A, R)$ has the structure of an algebra over C with unit where if $f, g \in \mathrm{Hom}_C(A, R)$ the product $f * g \in \mathrm{Hom}_C(A, R)$ is defined by

$$f * g = m \circ (f \otimes g) \circ d.$$

That is, one has a commutative diagram

$$\begin{tikzcd} A \arrow[r, "d"] \arrow[d, "f * g"'] & A \otimes A \arrow[d, "f \otimes g"] \\ R & R \otimes R \arrow[l, "m"] \end{tikzcd}$$

In particular if we put $R = C$ the dual $A' = \mathrm{Hom}_C(A, C)$ has the structure of an algebra.

Now assume that A is a Hopf algebra (A is an algebra and coalgebra such that d and ε are homomorphisms and $\varepsilon\rho$ is the identity on C).

By an antipode on A we mean an element (necessarily unique if it exists) $s \in \mathrm{Hom}_C(A, A)$ such that $I * s = s * I = \varepsilon$ where I is the identity on A and $*$ is as above with A taken for R. From now on Hopf algebra means Hopf algebra with antipode.

1.2. Now assume A is a Hopf algebra over C and R is any commutative C-algebra. Then if

$$G_R = \{f \in \mathrm{Hom}_C(A, R) | f \text{ is an algebra homomorphism}\}$$

one sees immediately that G_R is a group under $*$ where

$$f^{-1}(a) = f(sa) \qquad \text{for any } f \in G_R,\ a \in A.$$

Thus one has a functor $R \to G_R$ from all commutative algebras over R into groups and the functor is represented by A.

Now if C is the set of integers Z then we may drop the word algebra so that $R \to G_R$ is a functor from all commutative rings R to groups.

EXAMPLE. If $A = \boldsymbol{Z}[X_{ij}, 1/D]$, $i, j, = 1, 2, \cdots, n$, where the X_{ij} are indeterminates and $D = \det(X_{ij})$, then A is a Hopf algebra over $\boldsymbol{Z}$ where

$$dX_{ij} = \sum_k X_{ik} \otimes X_{kj},$$

so that $dD = D \otimes D$. Also $\varepsilon(X_{ij}) = 0$ and $s(X_{ij}) = (-1)^{i+j}$ cofactor X_{ji}/D. Here $G_R = \mathrm{Gl}(n, R)$ for any commutative ring R.

In the example above if one replaces A by its quotient with respect to the ideal generated by $D - 1$ then one obtains $G_R = \mathrm{Sl}(n, R)$ for any commutative ring R.

More generally for any semisimple Lie group G we will define a Hopf algebra $\boldsymbol{Z}(G)$ over $\boldsymbol{Z}$ with the following properties:

(1) $\boldsymbol{Z}(G)$ is a finitely generated commutative integral domain;

(2) for any field k

$$k(G) = \boldsymbol{Z}(G) \otimes_{\boldsymbol{Z}} k$$

is an affine algebra defining a semisimple algebraic group over k which is split over k, and is of the same type as G;

(3) $\boldsymbol{Q}(G)$ defines G over $\boldsymbol{Q}$, where $\boldsymbol{Q}$ is the field of rational numbers.

1.3. From now on $C = \boldsymbol{Z}$. Let B be a Hopf algebra over $\boldsymbol{Z}$. An ideal $I \subseteq B$ will be said to be of finite type if B/I is a finitely generated free $\boldsymbol{Z}$-module. If I and I' are of finite type then the kernel $I \wedge I'$ of the composed map

$$B \xrightarrow{d} B \otimes B \longrightarrow B/I \otimes B/I'$$

is again clearly of finite type defining an operation on the set of all such ideals. A family F of ideals of finite type will be said to be admissible if

(1) $\bigcap_{I \in F} I = (0)$;

(2) $s(I) \in F$ for all $I \in F$;

(3) F is closed under $\wedge$.

Now given such a family put

$$A_F = \{f \in \mathrm{Hom}(B, \boldsymbol{Z}) \big| f|I = 0 \text{ for some } I \in F\}.$$

It is immediate then that A_F has the structure of a Hopf algebra over $\boldsymbol{Z}$. The multiplication in A_F is defined as the transpose of the diagonal map in B. (It exists since F is closed under $\wedge$.) The diagonal map in A_F is defined as the transpose of the multiplication in B. (It exists since each $f \in A_F$ vanishes on an ideal of finite type in B.) The antipode is simply the transpose of the antipode in B. (It exists since F is closed under s.)

1.4. Now let G be a complex semisimple Lie group and let $\mathfrak{g}$ be its Lie algebra. Let U be the universal enveloping algebra of $\mathfrak{g}$ so that U is a Hopf algebra over $\boldsymbol{C}$ where

$$dx = x \otimes 1 + 1 \otimes x$$

for any $x \in \mathfrak{g}$. Also ε is given by $\varepsilon(x) = 0$ for any $x \in \mathfrak{g}$ and s is the anti-automorphism of U defined by $s(x) = -x$ for any $x \in \mathfrak{g}$.

We will now define a Hopf algebra B over $\boldsymbol{Z}$ where $B \subseteq U$. The family of ideals F will be defined by G and one puts

$$Z(G) = A_F.$$

2. The definition and structure of *B*. Let $\mathfrak{h}$ be a Cartan subalgebra of $\mathfrak{g}$ and let Δ be the corresponding set of roots.

Chevalley has shown (see **[1]**) the existence of a set of root vectors e_ϕ, $\phi \in \Delta$, such that if ϕ, ψ, $\phi + \psi \in \Delta$ then

$$[e_\phi, e_\psi] = \pm r e_{\phi+\psi}$$

where $r \in \boldsymbol{Z}_+$ (the set of nonnegative integers) is the minimum integer such that $(\operatorname{ad} e_{-\phi})^r e_\psi = 0$ and if $h_\phi = [e_\phi, e_{-\phi}]$ then

$$\phi(h_\phi) = 2.$$

We fix the e_ϕ as above and put $\mathfrak{g}_{\boldsymbol{Z}}$ equal to the $\boldsymbol{Z}$ span of all the e_ϕ and h_ϕ for $\phi \in \Delta$. We recall some facts from **[1]** which, in fact, are easy to check. Let Δ_+ be a system of positive roots and let $\Pi = (\alpha_1, \cdots, \alpha_l)$ be the corresponding set of simple roots. Put $h_i = h_{\alpha_i}$, $i = 1, 2, \cdots, l$, for simplicity. Then one has

PROPOSITION 1. *The elements $h_1, \cdots, h_l$ together with all e_ϕ, $\phi \in \Delta$ form a free $\boldsymbol{Z}$-basis of $\mathfrak{g}_{\boldsymbol{Z}}$.*

REMARK 1. Proposition 1 is of course only really a statement about the $\boldsymbol{Z}$-span of the h_ϕ and the statement is of course well known.

Now it is clear that $\mathfrak{g}_{\boldsymbol{Z}}$ is a Lie algebra over $\boldsymbol{Z}$. Somewhat less obvious is the following fact of **[1]**:

PROPOSITION 2. *$\mathfrak{g}_{\boldsymbol{Z}}$ is stable under $(\operatorname{ad} e_\phi)^n/n!$ for any $\phi \in \Delta$ and $n \in \boldsymbol{Z}_+$.*

REMARK 2. If h, e and f is a basis of the Lie algebra of $\mathrm{Sl}(2, \boldsymbol{C})$ where $[h, e] = 2e$, $[h, f] = -2f$ and $(e, f) = h$ then Proposition 2 in essence reduces to the following fact: If $v_1, \cdots, v_k$ is a basis of an irreducible $\mathrm{Sl}(2, \boldsymbol{C})$ module consisting of h-eigenvectors such that

$$e \cdot v_j = \pm j v_{j+1}$$

then the $\boldsymbol{Z}$-span of the v_j is stable under $e^m/m!$ and $f^n/n!$ for all $n, m \in \boldsymbol{Z}_+$.

We now define B to be the algebra generated over $\boldsymbol{Z}$ by all elements $e_\phi^n/n! \in U$ for all $\phi \in \Delta$ and $n \in \boldsymbol{Z}_+$.

2.2. To prove that B is a Hopf algebra over $\boldsymbol{Z}$ with suitable properties we shall need some multiplication relations in U.

If $h, e \in \mathfrak{g}$ where $[h, e] = \lambda e$ for some scalar λ then one easily establishes

$$p(h)e^m = e^m p(h + \lambda m) \tag{2.1.1}$$

for any $m \in Z_+$ and polynomial $p \in C[X]$.

Now if $u \in U$ is arbitrary and $m \in Z_+$ put

$$C_{u,m} = \frac{u(u-1)\cdots(u-m+1)}{m!}.$$

Somewhat less trivial than (2.1.1) is the following useful relation among the generators of the Lie algebra of $\mathrm{Sl}(2, C)$.

Lemma 1. *Let $h, e, f \in \mathfrak{g}$ where $[h, e] = 2e$, $[h, f] = -2f$* and *$[e, f] = h$. Then for any $n, m \in Z_+$ one has*

$$\frac{e^m}{m!}\frac{f^n}{n!} = \sum_{j=0}^{k} \frac{f^{n-j}}{(n-j)!} C_{h-m-n+2j,j} \frac{e^{m-j}}{(m-j)!}$$

where k is the minimum of n and m.

Proof. One first of all proves directly from the bracket relation that

$$e\frac{f^n}{n!} = \frac{f^n}{n!}e + \frac{f^{m-1}}{(m-1)!}(h - m + 1).$$

Lemma 1 is then just an exercise using (2.1.1), the relation above, and induction on m.

2.3. A sequence of C-linear independent elements to $u^{(n)} \in U$, $n = 0, 1, 2, \cdots$, where $u^{(0)} = 1$, is called a sequence of divided powers in case

$$du^{(n)} = \sum_{j=0}^{m} u^{(j)} \otimes u^{(n-j)}$$

for all n. It is clear of course that the Z-space of the $u^{(n)}$ is a coalgebra over Z.

Example. If $x \in \mathfrak{g}$ and $u^{(n)} = x^n/n!$ then clearly $u^{(n)}$ is a sequence of divided powers. Another example is obtained by putting $u^{(n)} = C_{x,n}$.

Now assume more generally that for each fixed $i = 1, 2, \cdots, k$ one is given elements $u_i^{(n)} \in U$, $n = 0, 1, 2, \cdots$, forming a sequence of divided powers and that if

$$u_N = u_1^{(n_1)} u_2^{(n_2)} \cdots u_k^{(n_k)}$$

where $N = (n_1, \cdots, n_k) \in Z_+^k$, the u_N over all $N \in Z_+^k$ are C-linearly independent. Let V be the Z-span of all u_N. It is then clear that V is a coalgebra over Z and if $D = \mathrm{Hom}_Z(V, Z)$ then D, as in §1.1, has the structure of a commutative algebra. But the point is that the algebra structure on D is particularly easy to describe.

Let $\alpha_i \in D$, $i = 1, 2, \cdots, k$, be such that $\gamma_i(u_N) = 0$ for all N except $\gamma_i(u_i^{(1)}) = 1$.

We leave it as an exercise to prove

PROPOSITION 3. *For any $N = (n_1, \cdots, n_k) \in \boldsymbol{Z}^k_+$ let $\gamma_N = \gamma_1^{n_1} \cdots \gamma_k^{n_k}$. Then one has $\gamma_N(u_M) = 0$ unless $M = N$ and $\gamma_N(u_N) = 1$ so that D is the ring of formal power series*

$$D = \boldsymbol{Z}[[\gamma_1, \cdots, \gamma_k]].$$

2.4. Now introduce the partial ordering in Δ where $\phi < \psi$ in case $\psi - \phi$ can be written as a sum of positive roots. Then simply order Δ_+ so that $\Delta_+ = (\phi_1, \phi_2, \cdots, \phi_r)$ where $\phi_i < \phi_j$ implies $i \leqq j$.

Let $\mathfrak{n}$ be the complex nilpotent Lie algebra spanned by all e_ϕ where $\phi \in \Delta_+$ and let $U(\mathfrak{n}) \subseteq U$ be the universal enveloping algebra of $\mathfrak{n}$. In each r-tuple $M = (m_1, \cdots, m_r)$ where $m_i \in \boldsymbol{Z}_+$ put

$$e_M = \frac{e_{\phi_1}^{m_1}}{m_1!} \cdots \frac{e_{\phi_r}^{m_r}}{m_r!}$$

so that the elements e_M form a Birkhoff-Witt basis of $U(\mathfrak{n})$.

Now let E be the $\boldsymbol{Z}$-algebra in $U(\mathfrak{n})$ generated over $\boldsymbol{Z}$ by $e_\phi^n/n!$ for all $\phi \in \Delta$ and $n \in \boldsymbol{Z}_+$.

LEMMA 2. *The elements e_M, over all $M \in \boldsymbol{Z}^r_+$, for a free $\boldsymbol{Z}$-basis of E.*

PROOF. Let E_1 be the $\boldsymbol{Z}$-span of all e_M for $M \in \boldsymbol{Z}^r_+$. Since the e_M are independent over $\boldsymbol{C}$ they certainly form a free $\boldsymbol{Z}$-basis of E_1 and $E_1 \subseteq E$. Since E_1 contains the generators of E, to prove $E_1 = E$ we have only to show that E_1 is closed under multiplication.

We first observe that for any $1 \leqq j \leqq r$ there exists $s_j \in \mathrm{Hom}_{\boldsymbol{C}}(\mathfrak{g}, \boldsymbol{C})$ such that (1) s_j vanishes on all root vectors e_ϕ, (2) $s_j(h_{\phi_j}) = 1$ and (3) s_j takes values in $\boldsymbol{Z}$ on $\mathfrak{g}_{\boldsymbol{Z}}$. Indeed this is clear from Proposition 1 since any root, e.g., ϕ_j can be embedded in a system of simple roots.

Now consider the adjoint representation of $\mathfrak{n}$ on $\mathfrak{g}$. Extending to $U(\mathfrak{n})$ one has that $\mathfrak{g}$ is a $U(n)$ module. If $F = \mathrm{Hom}_{\boldsymbol{C}}(U(\mathfrak{n}), \boldsymbol{C})$ and $1 \leqq j \leqq r$ let $f_j \in F$ be defined by

$$f_j(u) = s_j(u \cdot e_{-\phi_j})$$

for any $u \in U(\mathfrak{n})$. If $M_j = (m_1, \cdots, m_r)$ is defined by $m_i = 0$ for $i \neq j$ and $m_j = 1$, then clearly $f_j(e_{M_j}) = 1$, that is, $f_j(e_{\phi_j}) = 1$. On the other hand if one orders $\boldsymbol{Z}^r_+$ lexicographically it is immediate that $f_j(e_M) = 0$ for all $M > M_j$.

But now by Proposition 2 f_j must take values in $\boldsymbol{Z}$ on E. Now since $U(\mathfrak{n})$ is a coalgebra F is an algebra over $\boldsymbol{C}$. For any $N = (n_1, \cdots, n_r)$ put $f_N = f_1^{n_1} \cdots f_r^{n_r} \in F$. But now since E is the algebra generated over $\boldsymbol{Z}$ by all $e_\phi^n/n!$ it follows that dE is in the $\boldsymbol{Z}$-span of all elements in $U(\mathfrak{n}) \otimes_{\boldsymbol{C}} U(\mathfrak{n})$ of the form $u \otimes v$ where $u_1 v \in E$. Consequently f_N also takes values in $\boldsymbol{Z}$ on E for any $N \in \boldsymbol{Z}^r_+$. But $E_1 \subseteq E$ and by Proposition 3 one has $f_N(e_N) = 1$ and $f_N(e_M) = 0$ for all $M > N$.

Now assume E_1 is not an algebra. Then there exists N, M such that $e_N e_M \notin E_1$. That is, since the e_P, $P \in Z^r_+$ are a C-basis of $U(\mathfrak{n})$ and one writes

$$e_N e_M = \sum c_P e_P$$

there exists c_P such that $c_P \notin Z$. Let L be minimal with this property. But then $f_L(e_N e_M) \notin Z$. This however contradicts the fact that f_L takes integral values on E.

REMARK 3. We note here that Lemma 2 may be strengthened in that the same conclusion is true when we use *any* ordering in Δ_+. Indeed if f_M is defined in the same way as e_M except with respect to a different ordering in Δ_+ and

$$|M| = \sum_{i=1}^{r} m_i$$

for $M = (m_1, \cdots, m_r)$ then by the Birkhoff-Witt theorem there exists $M' \in Z^r_+$ such that $|M'| = |M|$ and

$$e_M - f_{M'} = \sum c_N e_N$$

where the sum is over N such that $|N| < |M|$. But the c_N lie in Z by Lemma 2. The result then follows by induction on $|M|$.

2.5. If X is an indeterminate one knows that $C_{X,n}$ for all $n \in Z_+$ form a free Z-basis of the Z-ring R of all polynomials p in $C[X]$ such that $p(n) \in Z$ for all $n \in Z$. Since $C_{X-m,n} \in R$ for any $m \in Z$ and is of degree n it is clear that the polynomial $C_{X-m,n}$ is an integral combination of $C_{X,d}$ for $0 \leqq j \leqq n$.

Now for any $K = (k_1, \cdots, k_1) \in Z^l_+$ let $h_K = C_{h_1,k_1} \cdots C_{h_l,k_l}$. It is then clear that the h_K over all $K \in Z^l_+$ is a C-basis of the universal enveloping algebra $U(\mathfrak{h})$ of $\mathfrak{h}$. On the other hand from above and §2.3 it is also clear that the Z-span H of all h_K is a Hopf algebra over Z. Also from above, H contains $C_{h_i-n_i,k}$ for any $k \in Z_+$ and $m_i \in Z$.

We have defined $e_M \in U(\mathfrak{n})$ for any $M \in Z^r_+$. Now similarly define

$$f_N = e^{n_1}_{-\phi_1}/n_1! \cdots e^{n_r}_{-\phi_r}/n_r!$$

for any $N \in Z^r_+$.

Recall that B is the Z-algebra generated over Z by all $e^n_\phi/n!$ for $\phi \in \Delta$, $n \in Z_+$.

THEOREM 1. *The elements*

$$f_N h_K e_M$$

for all $N, M \in Z^r_+$ *and* $K \in Z^l_+$ *form a free* Z*-basis of* B.

PROOF. For convenience put $n = 2r + l$ and for any $P \in Z^n_+$ write $P = (N, K, M)$ and put $b_P = f_N h_K e_M$. By the Birkhoff-Witt theorem it is clear that the b_P form a C-basis of U. Let U_Z be the Z-span of all b_P. We first show that $U_Z \subseteq B$. For this it is clearly enough to show that if $h = h_i$, $1 \leqq i \leqq l$ and $k \in Z_+$ then $C_{h,k} \in B$. Put $e = e_{\alpha_i}$ and $f = e_{-\alpha_i}$ so that h, e and f satisfy the conditions of Lemma 1.

Assume inductively that $C_{h,j} \in B$ for all $j < k$. Then by Lemma 1 one has $(e^k/k!)(f^k/k!) = C_{h,k}$ plus terms all involving $e^p/p!$, $f^q/q!$ and $C_{h-m,j}$ where $p, q \in Z_+$, $m \in Z$ and $j < k$. By induction therefore $C_{h,k} \in B$ so that $U_Z \subseteq B$.

With the same definition of h, e, f as above we now show that U_Z is stable under right multiplication by $e^n/n!$, $f^n/n!$ and $C_{h,n}$ for any $n \in Z_+$. For the case of $e^n/n!$ the result is immediate by Lemma 2. For $C_{h,n}$ the result follows from (2.1.1) since $\phi(h) \in Z$ for all roots of $\phi \in \Delta$ so that $e_M C_{h,n} = C_{h-m,n} e_M$ for some $m \in Z$.

Finally we want to show $b_P f^n/n! = f_N h_K e_M f^n/n!$ lies in U_Z for all P. Since the argument above shows that U_Z is stable under left multiplication by f_N and h_K it is enough to show that $e_M f^n/n! \in U_Z$ for all M. But by Remark 3 we can change the order of the roots in Δ_+ without changing E. Order the roots in Δ_+ so that $\phi_r = \alpha_i$ and let S be the set of all $M \in Z^r_+$ where $m_r = 0$. We must therefore show

$$e_M \frac{e^m}{m!} \frac{f^n}{n!} \in U_Z$$

for all $M \in S$, m, $n \in Z_+$. But by Lemma 1, $(e^m/m!)(f^n/n!)$ can be rewritten as an integral sum of elements of the form

$$\frac{f^i}{i!} C_{h,k} \frac{e^j}{j!}.$$

Hence we have only to show $e_M f^n/n! \in U_Z$ where $M \in S$.

But now one knows that the set $(\phi_1, \cdots, \phi_{r-1}, -\alpha_i)$ forms a new system of positive roots (obtained from Δ_+ by the reflection corresponding to α_i). Hence Lemma 2 and particularly Remark 3 apply to this new system. Thus $e_M f^n/n!$ can be written as an integral sum of elements of the form $(f^j/j!)e_N$ where again $N \in S$. But these all lie in U_Z. Thus U_Z is stable under right multiplication by $e^n/n!$, $f^n/n!$ and $C_{h,k}$. By symmetry the same is true for left multiplication.

Now consider the adjoint representation of $\mathfrak{g}$ on U. This extends to U so that U is a U-module and if U^j is the finite dimensional subspace spanned by all products of $\mathfrak{g}$ with itself at most j times then one knows that U^j is a U-submodule. It is also clear that if $U^j_Z = U_Z \cap U^j$ then U^j_Z is a Z-form of U_Z with a free Z-basis consisting of all b_P where $|P| \leqq j$.

But if $x \in \mathfrak{g}$ and $u \in U$ then $\operatorname{ad} x(u) = xu - ux$. Hence

$$\operatorname{ad}\left(\frac{e^n}{n!}\right)u = \sum_{j=0}^{n} (-1)^j \frac{e^{n-j}}{(n-j)!} u \frac{e^j}{j!}.$$

Thus U^j_Z is stable under $\operatorname{ad}(e^n/n!)$ and similarly $\operatorname{ad}(f^n/n!)$ for all n. It follows therefore if π_i (recall $e = e_{\alpha_i}$) is the representation of $SL(2, C)$ on U defined by $\operatorname{ad} h$, $\operatorname{ad} e$ and $\operatorname{ad} f$ and we let $\sigma_i = \pi_i(e_{12} - e_{21})$ where e_{ij}, $i = 1, 2$, are the matrix units in $M_2(C)$ then U^j_Z and hence U_Z is stable under σ_i. If X is the group generated by the σ_i for all i then U_Z is stable under X and one knows there is a homomorphism $\sigma \to \bar{\sigma}$ of X onto the Weyl group W such that $\sigma e_{\phi} = \pm e_{\bar{\sigma}\phi}$ for all $\sigma \in X$. Since every root is W-conjugate to a simple root it follows therefore that U_Z is stable under right multiplication by $e_{\phi}^n/n!$ for all $\phi \in \Delta$ and $n \in Z_+$. This implies $U_Z = B$.

2.6. If we regard $U(\mathfrak{h})$ as the algebra of all polynomials on the dual space $\mathfrak{h}'$ to $\mathfrak{h}$, then for any $f \in \mathfrak{h}'$ one has that

$$h_M(f) = C_{f(h_1),m_1}, C_{f(h_2),m_2} \cdots C_{f(h_l),m_l}$$

Thus if $L \subseteq h'$ is the group of all integral linear forms on $\mathfrak{h}$ then $h_M(f) \in Z$ for all $M \in Z_+^l$. In fact, using the standard basis of L it follows easily that H is exactly the set of all $p \in U(\mathfrak{h})$ which take integral values on L. Furthermore (since the same is true for R and Z; see §2.5) given any finite subset $F \subseteq L$ and $\lambda \in F$ there exists $p \in H$ such that $p(\lambda) = 1$ and $p(\mu) = 0$ for $u \in F$ and $\mu \neq \lambda$.

Now assume that V is an arbitrary finite dimensional U-module. Let $\Delta(V) \subseteq L$ be the set of weights of V and for each $\mu \in \Delta(V)$ let V^{μ} be the corresponding weight space.

A Z-form V_Z of $V(V = V_Z \otimes_Z C)$ is called admissible if it is stable under B.

COROLLARY 1 TO THEOREM 1. *There exists an admissible Z-form U_Z in V. Moreover if V_Z is any admissible Z-form in V and $V_Z^{\mu} = V_Z \cap V^{\mu}$ for $\mu \in \Delta(V)$ then*

$$V_Z = \bigoplus_{\mu \in \Delta(V)} V_Z^{\mu}.$$

PROOF. To prove the existence of an admissible Z-form it is enough to assume V is U-irreducible. Let v be a highest weight vector and put $V_Z = B \cdot v$. Since $f_M \cdot v \neq 0$ for only a finite number of M it is clear that V_Z is finitely generated over Z, stable under B and generates V over C. Furthermore V_Z is a direct sum of the $V_Z^{\mu} = V_Z \cap V^{\mu}$ for $\mu \in \Delta(V)$. To prove V_Z is a Z-form of V we have only to show that if $c_1, \cdots, c_k \in C$ are independent over Z and $v_1, \cdots, v_k \in V_Z^{\mu}$ are such that $\sum c_i v_i = 0$ then one already has $v_i = 0$ for all i. Indeed if, say, $v_1 \neq 0$, there exists $p \in E$ (see §2.4) of weight $\lambda - \mu$ (where λ is the highest weight of V) such that $p \cdot v_1 \neq 0$. But for all i, $p \cdot v_i = m_i v$ for some $m_i \in Z$ since $p \cdot v_i$ is of the form $q_i v$ where $q_i \in H$ by Theorem 1. Hence

$$0 = p \cdot \left(\sum c_i v_i\right) = \left(\sum c_i m_i\right) v$$

contradicting the fact that the c_i are Z-independent since we have $m_1 \neq 0$. Thus V_Z is a Z-form of V.

Now assume V_Z is any Z-form of V. For each $\mu \in \Delta(V)$ let $p_{\mu} \in H$ be such that $p_{\mu}(\mu) = 1$ and $p_{\mu}(\gamma) = 0$ for all $\gamma \in \Delta(V), \gamma \neq \mu$. But then $\sum_{\mu} p_{\mu}$ operates as the identity on V and if $w \in V_Z$ and $w_{\mu} = p_{\mu} \cdot w$ then $w = \sum_{\mu} w_{\mu}$ and $w_{\mu} \in V_Z^{\mu}$. This proves the direct sum decomposition stated in the corollary.

It follows from its definition but clearer from Theorem 1 that B is a Hopf algebra over Z.

THEOREM 2. *If $J \subseteq U$ is any ideal of finite codimension in U then $I = B \cap U$ is an ideal of finite type in B.*

PROOF. Put $V = U/I$ so that by left multiplication V is a finite dimensional U-module. Since an admissible $\boldsymbol{Z}$-form exists B is represented by $m \times m$ matrices with coefficients in $\boldsymbol{Z}$ where $m = \dim V$. This implies J is an ideal of finite type in B.

Now let Λ index all equivalence classes of finite dimensional modules for G. Regard these as modules for U and let $J_\alpha \subseteq U$, for $\alpha \in \Lambda$, be the corresponding kernels. If $I_\alpha = J_\alpha \cap B$ then it follows easily from Theorem 2 that the $I_\alpha, \alpha \in \Lambda$, form an admissible family F of ideals of finite type in B. One puts $\boldsymbol{Z}(G) = A_F$, (see §1.4) defining the Hopf algebra $\boldsymbol{Z}(G)$.

If V is any one of these modules and $V_{\boldsymbol{Z}}$ is an admissible $\boldsymbol{Z}$-form in V with $\boldsymbol{Z}$ basis v_i and w_j is the dual basis then one always has $f_{ij} \in \boldsymbol{Z}(G)$ where

$$f_{ij}(u) = \langle u \cdot v_i, w_j \rangle$$

for $u \in B$. The fact that $\boldsymbol{Z}(G)$ is finitely generated is a consequence of the following theorem of Chevalley.

THEOREM 3. *If G is faithfully represented in V then $\boldsymbol{Z}(G)$ is exactly the algebra generated over Z by the f_{ij}.*

REMARK 4. The definition given here for $\boldsymbol{Z}(G)$ provides the following normal form for $\boldsymbol{Z}(G)$. Let b_P be the basis of B given in Theorem 1 (see proof). Let $S = \mathrm{Hom}_{\boldsymbol{Z}}(B, \boldsymbol{Z})$ and let $\gamma_i \in S, i = 1, 2, \cdots, n$, be orthogonal to all b_P except the basis e_ϕ, h_i of $\mathfrak{g}_{\boldsymbol{Z}}$ and the γ_i define a dual basis to this basis of $\mathfrak{g}_{\boldsymbol{Z}}$ in the order indicated by Theorem 1. Then (by §2.3) if $\gamma_P = \gamma_1^{p_1} \cdots \gamma_n^{p_n}$ where $P = (p_1, \cdots p_n)$ one has $\gamma_P(b_Q) = \delta_{PQ}$. Furthermore $\boldsymbol{Z}(G) \subseteq S$ and S is the ring of formal power series

$$S = \boldsymbol{Z}[[\gamma_1 \cdots \gamma_n]].$$

REFERENCE

1. C. Chevalley, *Sur certaines groupes simples*, Tôhoku Math. J. (2) 7 (1955), 14–66.

Subgroups of Finite Index in Certain Arithmetic Groups

BY

H. MATSUMOTO

Introduction. Let k be an algebraic number field and $\mathfrak{o}$ the ring of integers of k. Let G be a connected algebraic group defined over k and $G_{\mathfrak{o}}$ its subgroup of integral points. For every ideal $\mathfrak{q} \neq (0)$ of $\mathfrak{o}$, the full congruence subgroup $G_{\mathfrak{o}}(\mathfrak{q})$ modulo $\mathfrak{q}$ is obviously of finite index in $G_{\mathfrak{o}}$.

The purpose of this talk is to discuss a converse to this for certain groups. We have the following theorem:

THEOREM. *Let G be a connected simply connected simple group of rank $\geqslant 2$ and split over $\boldsymbol{Q}$. Then every subgroup of finite index of $G_{\boldsymbol{Z}}$ contains $G_{\boldsymbol{Z}}(\mathfrak{q})$ for some ideal $\mathfrak{q} \neq (0)$ of $\boldsymbol{Z}$.*

This means that the set of all full congruence subgroups of G is cofinal in the set of all arithmetic subgroups of G. This is of much interest especially when G is a symplectic group. As is well known, the analogous statement is false for $\boldsymbol{SL}_2$.

The theorem was given for $\boldsymbol{SL}_n$ ($n \geqq 3$) and $\boldsymbol{Sp}_{2n}$ ($n \geqq 2$), independently, in [2], [6], [7]. Mennicke (yet unpublished) has proved it for all simple groups, but his original proof involves a case-by-case discussion. His arguments are essentially as follows: he reduces the problem first to the cases where $G = \boldsymbol{SL}_3, \boldsymbol{Sp}_4$, and then, by means of clever matrix computations, to some arithmetic properties of $\boldsymbol{Z}$, which are verified in virtue of Dirichlet's theorem on arithmetic progressions.

In this talk, we shall show how the problem can be reduced to cases of lower rank, making use of the theory of semisimple group schemes over $\boldsymbol{Z}$ due to Chevalley [5], discussed by Cartier and Kostant [3] at this Institute.

REMARK. It seems likely that the theorem is in fact true if $\boldsymbol{Q}$ and $\boldsymbol{Z}$ are replaced by a number field k and its ring of integers $\mathfrak{o}$. In fact, for a given k, the reduction theorem whose proof is sketched below shows that if the theorem is true for $G = \boldsymbol{SL}_{3,\mathfrak{o}}, \boldsymbol{Sp}_{4,\mathfrak{o}}$, then it is true for any G which is simple, simply connected, and splits over k. Moreover, Mennicke has shown that the theorem is true for $G = \boldsymbol{SL}_{3,\mathfrak{o}}, \boldsymbol{Sp}_{4,\mathfrak{o}}$, if $\mathfrak{o}$ verifies the following condition, which we state for a commutative ring A: for $x, y \in A$, let us denote by $n(x, y)$ the smallest positive integer n such that y^n is congruent mod x to a unit of A. If x, y are coprime in A, then the g.c.d. of the numbers $n(x + ty, y)\,(t \in A)$ is equal to one.

1. **Groups over $\boldsymbol{Z}$.** Let us recall briefly some definitions and results in [3].

Let G be a connected semisimple algebraic group of automorphisms of a vector space U over $\boldsymbol{C}$ and H a maximal torus of G. Let $\mathfrak{g}$, $\mathfrak{h}$ be the Lie algebras of G, H respectively, Φ the system of roots of G relative to H and Δ a system of simple roots in Φ. We take, as in Cartier's lecture, a Chevalley lattice $\mathfrak{g}_{\mathbf{Z}}$ of $\mathfrak{g}$ and an admissible lattice $U_{\mathbf{Z}}$ of U, $g_{\mathbf{Z}} = \mathfrak{g} \cap \mathrm{End}(U_{\mathbf{Z}}) = \mathfrak{h}_{\mathbf{Z}} + \sum_{\alpha\in\Phi} \mathbf{Z}x_\alpha$, $\mathfrak{g}_\alpha = \mathbf{C}x_\alpha$, and we define a Hopf algebra $\mathbf{Z}[G]$ over $\mathbf{Z}$ of G. $\mathbf{Q}[G] = \mathbf{Z}[G] \otimes_{\mathbf{Z}} \mathbf{Q}$ induces a $\mathbf{Q}$-structure of G.

If X is a connected subgroup of G defined over $\mathbf{Q}$, the inclusion map $\iota: X \rightarrow G$ induces a Hopf algebra homomorphism $\tilde{\iota}: \mathbf{C}[G] \rightarrow \mathbf{C}[X]$, and $\mathbf{Z}[X]$ will denote the subalgebra $\tilde{\iota}(\mathbf{Z}[G])$ over $\mathbf{Z}$ of $\mathbf{C}[X]$. For the semisimple subgroups X of G considered later, this $\mathbf{Z}[X]$ will be exactly the Hopf algebra associated with X viewed as a semisimple group.

Now let ρ be an irreducible rational representation of G in V and $V_{\mathbf{Z}}$ an admissible lattice of V with respect to $\mathfrak{g}_{\mathbf{Z}}$ and $\mathfrak{h}_{\mathbf{Z}}$. We have $V_{\mathbf{Z}} = \sum_\lambda V_{\mathbf{Z}} \cap V^\lambda$ where λ runs through the weights of ρ with respect to H and V^λ is the weight space of λ. Let us take a basis of $V_{\mathbf{Z}}$, $\{v_1, v_2, \ldots, v_m\}$, compatible with the above decomposition and such that $v_1 \in V^{\lambda_1}$ with λ_1 the highest weight of ρ relative to Δ. When we express ρ in terms of this basis, $\rho(g)v_j = \sum_{i=1}^m t_{ij}(g)v_i$, we have $t_{ij} \in \mathbf{Z}[G]$ and the action of G on V induces a ring homomorphism $\tilde{\rho}$ of $\mathbf{Z}[V]$ into $\mathbf{Z}[G] \otimes \mathbf{Z}[V]$.

Let us introduce some subgroups of G. Let P be the stabilizer in G of V^{λ_1}, N^+ the unipotential radical of P, S the maximal reductive subgroup of P containing H and G' the derived group of S. Denote by $\mathfrak{n}^+, \mathfrak{s}, \mathfrak{g}'$ the Lie algebras of N^+, S, G' respectively. We can write $\mathfrak{n}^+ = \sum_{\alpha\in\Phi(\mathfrak{n}^+)} \mathfrak{g}_\alpha$, $\mathfrak{s} = \mathfrak{h} + \sum_{\alpha\in\Phi(\mathfrak{s})} \mathfrak{g}_\alpha$, and $\mathfrak{g}' = \mathfrak{g}' \cap \mathfrak{h} + \sum_{\alpha\in\Phi(\mathfrak{s})} \mathfrak{g}_\alpha$. Let $\mathfrak{m}$ be the subalgebra of $\mathfrak{g}$ generated by $\mathfrak{g}_{\pm\alpha}$, $\alpha \in \Delta \cap \Phi(\mathfrak{n}^+)$, and put $\mathfrak{n}^- = \sum_{\alpha\in\Phi(\mathfrak{n}^+)} \mathfrak{g}_{-\alpha}$ and $\mathfrak{h}' = \mathfrak{m} \cap \mathfrak{h}$. Let N^- and H' be the connected subgroups of G whose Lie algebras are respectively $\boldsymbol{n}^-$ and $\boldsymbol{h}'$. We have $S = H'G'$ with $H' \cap G'$ finite. These subgroups of G are all defined over $\mathbf{Q}$.

Now the map $\phi: N^- \times N^+ \times S \rightarrow G$ defined by $\phi(n^-, n^+, s) = n^-n^+s$ is an isomorphism of algebraic varieties of $N^- \times N^+ \times S$ onto an affine open set Ω in G. If $H' \cap G' = \{e\}$, the map $\psi: H' \times G' \rightarrow S$ defined by $\psi(h', g') = h'g'$ is also an isomorphism of algebraic varieties. Furthermore, we have the following

PROPOSITION 1. (i) *$\mathbf{C}[\Omega] = \mathbf{C}[G][t_{11}^{-1}]$ with $t_{11} \in \mathbf{Z}[G]$ and $t_{11}(e) = 1$. ϕ induces a ring isomorphism $\tilde{\phi}$ of $\mathbf{Z}[G][t_{11}^{-1}]$ to $\mathbf{Z}[N^-] \otimes \mathbf{Z}[N^+] \otimes \mathbf{Z}[S]$.*

(ii) *If $H' \cap G' = \{e\}$, then ψ induces a ring isomorphism $\tilde{\psi}$ of $\mathbf{Z}[S]$ to $\mathbf{Z}[H'] \otimes \mathbf{Z}[G']$.*

This proposition follows from a theorem in [5] and in [3]. We note that if G is simply connected one always has $H' \cap G' = \{e\}$.

2. **Reformulation of the problem.** Let $\mathfrak{o}$ be a commutative ring with unity. The set of ring homomorphisms of $\mathbf{Z}[G]$ into $\mathfrak{o}$, $G_{\mathfrak{o}} = \mathrm{Hom}(\mathbf{Z}[G], \mathfrak{o})$, has a group structure induced by the Hopf algebra structure of $\mathbf{Z}[G]$. With a connected subgroup X of G defined over $\mathbf{Q}$, we associated the homomorphism $\tilde{\iota}: \mathbf{Z}[G] \rightarrow \mathbf{Z}[X]$, and thereby we obtain an injection of $X_{\mathfrak{o}} = \mathrm{Hom}(\mathbf{Z}[X], \mathfrak{o})$ into $G_{\mathfrak{o}}$:

thus $X_{\mathfrak{o}}$ is a subgroup of $G_{\mathfrak{o}}$. In particular, for a root subgroup $N^{\alpha} = \exp \mathfrak{g}_{\alpha}, \alpha \in \Phi$, we have a subgroup $N^{\alpha}_{\mathfrak{o}}$ of $G_{\mathfrak{o}}$.

The elements in the union of $N^{\alpha}_{\mathfrak{o}}, \alpha \in \Phi$, are called *elementary unipotents* of $G_{\mathfrak{o}}$ (with respect to $\mathfrak{g}_{\boldsymbol{Z}}$ and $\mathfrak{h}_{\boldsymbol{Z}}$).

$\mathfrak{o}$ is fixed once for all and we put $\Gamma = G_{\mathfrak{o}}$. For every ideal $\mathfrak{q}$ of $\mathfrak{o}$, we get a reduction homomorphism of Γ into $G_{\mathfrak{o}/\mathfrak{q}} = \mathrm{Hom}(\boldsymbol{Z}[G], \mathfrak{o}/\mathfrak{q})$, whose kernel is denoted by $\Gamma_{\mathfrak{q}}$. One can see later that this reduction map is surjective, for example, if G is simply connected and if $\mathfrak{o}/\mathfrak{q}$ is semilocal.

Now let us define some subgroups of Γ. Let E be the subgroup of Γ generated by the elementary unipotents in Γ, and, for every ideal $\mathfrak{q}$ of $\mathfrak{o}$, let $E_{\mathfrak{q}}$ be the smallest normal subgroup of E containing the elementary unipotents in $\Gamma_{\mathfrak{q}}$.

We see easily that the theorem in the Introduction is a consequence of the following

THEOREM 1. *If G is simply connected and simple of rank $\geqq 2$ and if $\mathfrak{o} = \boldsymbol{Z}$, we have, with the above notations, $\Gamma_{\mathfrak{q}} = E_{\mathfrak{q}}$ for every ideal $\mathfrak{q}$ of $\mathfrak{o}$.*

In fact, we know that the statements of these theorems are equivalent and that this fact remains valid when $\mathfrak{o}$ is the ring of integers of an algebraic number field (cf. [1]).

3. **A reduction lemma.** In this section we shall always assume the following:

(A1) G is simply connected and simple.

(A2) $\mathfrak{o}$ is a commutative ring with unity such that, for every ideal $\mathfrak{q}$ not contained in the radical of $\mathfrak{o}$, $\mathfrak{o}/\mathfrak{q}$ is semilocal.

Under these assumptions, we shall show, for $\Gamma = \mathrm{Hom}(\boldsymbol{Z}[G], \mathfrak{o})$, how one can reduce to cases of lower rank the question whether $\Gamma_{\mathfrak{q}}$ and $E_{\mathfrak{q}}$ are equal.

For this purpose we need a representation of G satisfying certain conditions. Let us consider the following condition on an irreducible representation ρ of G:

(Pdm) Every nonzero weight of ρ (with respect to H) is transformed into the highest weight of ρ by an element of the Weyl group of G (with respect to H).

We recall a proposition in [4, exposé 20]:

PROPOSITION 2. *If ρ is a nontrivial irreducible representation of G satisfying* (Pdm), *then every nonzero weight of ρ is of multiplicity* 1 *and the multiplicity of the weight zero is the number of simple roots appearing among the nonzero weights.*

We know (loc. cit.) that there exist at least min $\{\mathrm{rk}(G), [C]\}$ fundamental representations of G satisfying (Pdm), where $\mathrm{rk}(G)$ is the rank of G and $[C]$ the order of the center C of G.

We shall fix a fundamental representation of G satisfying (Pdm) and the following supplementary condition (Deg): ρ is of degree greater than 2 and its highest weight λ_1 is not sum of any two simple roots.

One can see easily that (Deg) is automatically fulfilled by any nontrivial irreducible representation of G satisfying (Pdm) unless G is isomorphic to $\boldsymbol{SL}_2$, $\boldsymbol{SL}_3$ or $\boldsymbol{Sp}_4$. Thus, if G is of rank $\geqq 2$, there exists at least one fundamental representation of G satisfying (Pdm) and (Deg).

We shall now apply the results of §1 to such a fundamental representation ρ of G in V. First, we take an admissible lattice $V_{\mathbf{Z}}$ of V and modify it so as to coincide with $V_{\mathbf{Z}} + V_{\mathbf{Z}}^{0}$, where $V_{\mathbf{Z}}^{0'}$ is the largest lattice of the zero-weight space V^{0} such that $V_{\mathbf{Z}} + V_{\mathbf{Z}}^{0}$ remains an admissible lattice of V (cf. Proposition 2). As in §1, we have subgroups N^{-}, H', N^{+}, G' of G, defined with respect to ρ. We have $H' \cap G' = \{e\}$, $\mathbf{Z}[H'] = \mathbf{Z}[t_{11}|H, (t_{11}|H)^{-1}]$, and, since G is simply connected, so is G'. Therefore, Proposition 1 gives us the ring isomorphism

$$\tilde{\omega} = (\tilde{1} \otimes 1 \otimes \tilde{\psi}) \circ \tilde{\phi} : \mathbf{Z}[G][t_{11}^{-1}] \rightarrow \mathbf{Z}[N^{-}] \otimes \mathbf{Z}[N^{+}] \otimes \mathbf{Z}[H'] \otimes \mathbf{Z}[G'].$$

$\mathbf{Z}[G]$ is the Hopf algebra associated with G' viewed as a semisimple group and $\Gamma' = G'_{\mathfrak{o}} = \mathrm{Hom}(\mathbf{Z}[G'], \mathfrak{o})$ is a subgroup of Γ. We have $\Gamma'_{\mathfrak{q}} = \Gamma_{\mathfrak{q}} \cap \Gamma'$. For the unipotent subgroups $N^{\pm}$, we see easily that $N_{\mathfrak{o}}^{\pm} \cap \Gamma_{\mathfrak{q}} \subset E_{\mathfrak{q}}$.

The dual action $\tilde{\rho} : \mathbf{Z}[V] \rightarrow \mathbf{Z}[G] \otimes \mathbf{Z}[V]$ defines an action of Γ on $V_{\mathfrak{o}}$, where $V_{\mathfrak{o}} = \mathrm{Hom}(\mathbf{Z}[V], \mathfrak{o}) = V_{\mathbf{Z}} \otimes_{\mathbf{Z}} \mathfrak{o}$. In virtue of Proposition 2, we can see in what manner Γ and E act on $V_{\mathfrak{o}}$ in terms of our basis $\{v_1, v_2, \cdots, v_m\} : \Gamma$ acts on $V_{\mathfrak{o}}$, *grosso modo*, in as simple a manner as $SL_{n,\mathfrak{o}}$ does naturally on $V_{\mathfrak{o}}$ ($n \geqq 3$). So using arguments similar to those in [**1**] and [**2**], we can show the following

LEMMA 1. *Let v be an element of $V_{\mathfrak{o}}$ such that $v \equiv v_1 \bmod \mathfrak{q}V_{\mathfrak{o}}$. Then there exists a $g \in E_{\mathfrak{q}}$ such that $\rho(g)v - v_1 \in \sum_{j=2}^{m} \mathfrak{q}v_j$.*

This allows us to obtain our reduction lemma: namely,

THEOREM 2. *The notations and assumptions being as above, we have $\Gamma_{\mathfrak{q}} = E_{\mathfrak{q}}\Gamma'_{\mathfrak{q}}$ for every ideal $\mathfrak{q}$ of $\mathfrak{o}$.*

SKETCH OF PROOF. Let g be an element of $\Gamma_{\mathfrak{q}}$. By Lemma 1, there is a $g_1 \in E_{\mathfrak{q}}$ such that $g_1 g$ maps t_{11} to 1. Hence $g_1 g$ belongs to $\mathrm{Hom}(\mathbf{Z}[G][t_{11}^{-1}], \mathfrak{o})$ and therefore, by means of $\tilde{\omega}$, it can be written in the form $g_1 g = n^{-} n^{+} h' g'$ where $n^{-} \in N_{\mathfrak{o}}^{-}$, $n^{+} \in N_{\mathfrak{o}}^{+}$, $h' \in H'_{\mathfrak{o}}$ and $g' \in \Gamma'_{\mathfrak{o}}$. We see easily then that $h' = e$ and that n^{-}, n^{+} are in $\Gamma_{\mathfrak{q}}$, hence in $E_{\mathfrak{q}}$. This implies that g is in $E_{\mathfrak{q}}\Gamma'_{\mathfrak{q}}$.

We note some consequences of this theorem (cf. [**1**], [**6**]).

COROLLARY 1. *Assume* $\mathrm{rk}(G) \geqq 2$. *Then $E_{\mathfrak{q}}$ is a normal subgroup of Γ and we have $[\Gamma, \Gamma_{\mathfrak{q}}] \subset E_{\mathfrak{q}}$.*

COROLLARY 2. (i) *If $\mathfrak{o}$ is semilocal, $\Gamma_{\mathfrak{q}}$ is equal to $E_{\mathfrak{q}}$ for every ideal $\mathfrak{q}$ of $\mathfrak{o}$.*

(ii) *If $\mathfrak{o}$ is euclidean, Γ is equal to E.*

Now if G' has a simple factor of rank $\geqq 2$, we can apply Theorem 2 to $\Gamma'_{\mathfrak{q}}$, to obtain $\Gamma_{\mathfrak{q}} = E_{\mathfrak{q}}\Gamma''_{\mathfrak{q}}$ where Γ'' comes from a subgroup G'' of rank $\mathrm{rk}(G) - 2$. Actually, we can always take ρ in such a way that G' is simple; therefore we have $\Gamma_{\mathfrak{q}} = E_{\mathfrak{q}}\Gamma'_{\mathfrak{q}} = \cdots = E_{\mathfrak{q}}\Gamma_{\mathfrak{q}}^{(l-1)}$, where $l = \mathrm{rk}(G)$ and $\Gamma^{(l-1)}$ is isomorphic to SL_2.

Finally if G is of type G_2, we see easily that G has a subgroup G^{*} containing $G'H$ and isomorphic to SL_3. We have therefore $\Gamma_{\mathfrak{q}} = E_{\mathfrak{q}}\Gamma'_{\mathfrak{q}} = E_{\mathfrak{q}}\Gamma_{\mathfrak{q}}^{*}$.

Thus, the problem of knowing whether the equality $\Gamma_{\mathfrak{q}} = E_{\mathfrak{q}}$ holds is reduced to cases of lower ranks and, under certain circumstances, to the cases of SL_2, SL_3 and Sp_4.

These remarks, together with the results for SL_3 and Sp_4 in [2], [6] and [7], complete the proof of Theorem 1.

References

1. H. Bass, *K-theory and stable algebra*, Publ. Math. I.H.E.S. No. 22 (1964), 5–60.

2. H. Bass, M. Lazard and J.-P. Serre, *Sous-groupes d'indice fini dans SL*(n, *Z*), Bull. Amer. Math. Soc. **70** (1964), 385–392.

3. Bertram Kostant, *Groups over Z*, Proc. Sympos. Pure Math. vol. 9, Amer. Math. Soc., Providence, R. I., 1966; pp. 90–98.

4. C. Chevalley, *Séminaire sur la classification des groupes de Lie algébriques* (École Normale Supérieure, 1956/1958), Secrétariat Mathématique, Paris.

5. ———, *Certaines schémas de groupes semi-simples*. Séminaire Bourbaki 1960; 1961, éxposé **219**, Secrétariat Mathématique, Paris.

6. J. Mennicke, *Finite factor groups of the unimodular group*, Ann. of Math. **81** (1965), 31–37.

7. ———, *Zur Theorie der Siegelschen Modulgruppe*, Math. Ann. **159** (1965), 115–129.

The Problem of the Maximality of Arithmetic Groups

BY

NELO D. ALLAN

1. **Introduction.** Our purpose is to give a survey of the known results on the maximality of arithmetic groups. The problem of finding extensions of an arithmetic group was first treated by Hurwitz who found an extension of $\mathrm{Sl}_n(\mathfrak{O})$, $\mathfrak{O}$ being the ring of integers of a number field k. Later on, about 1938, Hecke proved that $\mathrm{Sl}_2(\boldsymbol{Z})$ is maximal in $\mathrm{Sl}_n(\boldsymbol{R})$. In 1955 Maass proved that the Hurwitz group is the only maximal arithmetic group containing the Hilbert-Blumental group, up to a central extension. In 1957 Gutnik solved the problem of the maximality of $G_{\boldsymbol{Z}}$ for all paramodular groups G. Recently Greenberg solved the problem of the maximality of Fuchsian groups, and Ramanathan and Christian generalized Maass results to the case of the Hilbert-Siegel modular group; also Ramanathan proved, in several cases, that an arithmetic group is contained in only finitely many maximal arithmetic groups. This result has been generalized by Borel, who also generalizes the results of Hecke and Gutnik; there is also a generalization of these results in another direction, obtained by myself. We understand that H. C. Wang has also results concerning the maximality of discrete subgroups of some Lie groups. We would like to mention that with the help of the strong approximation theorem, we can lift the results of Hijikata, Bruhat–Satake, and Iwahori–Matsumoto, from the local case to the global case, to prove the maximality of $G_{\mathfrak{O}}$ in G_k.

2. **General problems.** Let G be a connected, semisimple linear algebraic group defined over an algebraic number filed k; say $G \subset \mathrm{Sl}_n(\boldsymbol{C})$. We say that a subgroup Δ of G is *arithmetic* if Δ is commensurable to $G_{\mathfrak{O}}$, i.e., $\Delta \sim G_{\mathfrak{O}}$. We shall assume that any arithmetic group is Zariski dense in G; this is true if G has no connected normal subgroup N, defined over k, such that $(R_{k|\boldsymbol{Q}}(N))_{\boldsymbol{R}}$ is compact.

Given an arithmetic group Δ, the first problem that arises is "how many" maximal groups are there that contain Δ. The solution of this problem was first given by Ramanathan for some classical groups, and later on by Borel, in general; there are only finitely many maximal arithmetic groups containing Δ.[1] We shall sketch the proof of this result, because of its simplicity.

[1] More recently H. C. Wang proved that if G is a semisimple real Lie group without compact factors, then any discrete subgroup of G with fundamental domain of finite measure is contained in only finitely many maximal discrete subgroups of G.

Let $L = A(\Delta, \mathfrak{O})$ be the enveloping algebra of Δ, i.e., the $\mathfrak{O}$-order generated by the elements of Δ in $M_n(k)$. The Zariski density of Δ implies the existence of $\lambda, \lambda' \in \mathfrak{O}$ such that

$$(1) \qquad \lambda M_n(\mathfrak{O}) \subset \lambda' L \subset M_n(\mathfrak{O}).$$

We shall prove first the following lemma:

Lemma (Borel). *If G is centerless and G is irreducible as a matrix group, then any arithmetic group is contained in G_k.*

Proof. First we can find $\Delta_0 \subset G_{\mathfrak{O}}$ such that $\Delta \subset N(\Delta_0)$, where $N(\Delta_0)$ is the normalizer of Δ_0 in G. The Zariski density of Δ_0 is equivalent to the existence of n^2 independent elements, over k, in Δ_0, say $M_1, \cdots, M_n \in \Delta_0$ and with the help of these elements we can define a representation Ψ of G in $M_n(C)$ by assigning to every $g \in G$ the matrix $\Psi(g) = (\alpha_{ij}(g))$ where α_{ij} is defined by $g^{-1}M_i g = \sum \alpha_{ij} M_j$. Since G is centerless, Ψ is faithful, hence it is an isomorphism over k, and consequently $\Psi(G_k) = (\Psi(G))_k$. Now our assertion follows from the fact that $\Psi(\Delta) \subset \Psi(N(\Delta_0)) \subset (\Psi(G))_k$.

With a slight modification of this argument we obtain the following results:

(a) Under the same hypothesis as in lemma, the commensurability group of Δ is G_k.

(b) In general (G not necessarily centerless), $N_k(\Delta) \sim \Delta$, for all $\Delta \subset G_k$, where $N_k(\Delta) = N(\Delta) \cap G_k$.

Now we are in the position to prove our assertion. We first observe that the property of being a maximal arithmetic group remains unchanged under an isogeny; hence we may assume that G is centerless. Since the enveloping algebra of an arithmetic group contained in G_k is an $\mathfrak{O}$-order in the algebra $M_n(k)$, and every such order is contained in only finitely many maximal orders, it follows that Δ is contained in only finitely many maximal arithmetic groups, and these groups are among the groups obtained by intersecting the maximal orders containing L, with G.

If G is not centerless, we have the following result: if Δ is maximal in G_k, then there exists a unique maximal arithmetic group containing Δ, namely the normalizer $N(\Delta)$ of Δ in G. Moreover $N(\Delta)/\Delta$ is an abelian group such that the order of each one of its elements divides n.

This result is obtained from the following lemma, which also tell us the "shape" of any element in $N(\Delta)$.

Lemma. *Let Ω be an algebraically closed field, G be a matrix subgroup of $\mathrm{Sl}_n(\Omega)$, and k be the quotient field of a Dedekind domain $\mathfrak{O}$ contained in Ω. Let Δ be a subgroup of G_k such that for any $\Delta' \sim \Delta$ the formula* (1) *is satisfied for some $\lambda, \lambda' \in \mathfrak{O}$, and $N_k(\Delta) = \Delta$. Then every $g \in N(\Delta)$ can be written as (g_{ij}) and $g^n_{ij} \in k$ for all $i, j = 1, \cdots, n$. Moreover the ideal (g^n_{ij}) can be written as $\mathfrak{A}^n_{ij}/\mathfrak{D}$ where $\mathfrak{A}_{ij}$ and $\mathfrak{D}$ are ideals in $\mathfrak{O}$ such that the ideal class of $\mathfrak{A}_{ij}$ is independent of i and $j, g_{ij} \neq 0$, and $\mathfrak{D}$ divides λ^{n-1}. In particular $g = g' \sqrt[n]{a}$, with $g' \in M_n(k)$ and $a \in k$.*

If we denote by $\mathcal{U}$ the subgroup of $N(\Delta)$ consisting of those g where a can be taken as a unit of $\mathfrak{D}$, then we have a natural injection of $\mathcal{U}/\Delta$ into $U_n = U/U \cap \mathfrak{D}$, where U is the group of all nth roots of all units of $\mathfrak{D}$. If we assume that λ is divisible only by principal primes, and if we denote by $D(n, \lambda)$ the group D/D^n where D is the free abelian group generated by all prime divisors of λ, then there exists an injection of $N(\Delta)/\mathcal{U}$ into the direct product of the subgroup $\mathrm{IC}(n, k)$ of the ideal class group of k, consisting of those ideal classes whose order divides n by the group $D(n, \lambda)$. This injection is the mapping which associates to every $g \in G$ the pair (ideal class of $\mathfrak{A}_{ij}$, class of $\mathfrak{D}$ in $D(n, \lambda)$).

3. **Relation with the local theory.** We shall investigate the relation between global and local maximality. First we observe that a maximal arithmetic group contained in G_k is the intersection of maximal compact subgroups of $G_{k_\mathfrak{P}}$. For, if Δ is maximal in G_k, then for every finite spot $\mathfrak{P}$, the $\mathfrak{p}$-adic closure $(\Delta)^\mathfrak{P}$ of Δ is contained in only finitely many maximal compact subgroups of $G_{k_\mathfrak{P}}$; we choose one among them and call it $\Delta_\mathfrak{P}$; now the intersection of all $\Delta_\mathfrak{P}$ for $\mathfrak{P}$ finite, intersected with G_k, gives Δ. We observe that if $\mathfrak{P}$ does not divide λ, then $\Delta_\mathfrak{P} = G_{\mathfrak{D}_\mathfrak{P}}$; also the intersection with G_k of maximal compact $\mathfrak{P}$-adic groups may not be a maximal arithmetic group.

One would like to find conditions under which local maximality at all finite spots, implies global maximality, because the local problem is easier to handle; in particular we want to find conditions on the representation of G such that $G_\mathfrak{D}$ is maximal in G_k if and only if $G_{\mathfrak{D}_\mathfrak{P}}$ is maximal in $G_{k_\mathfrak{P}}$ for all finite $\mathfrak{P}$. This is true, for instance, if G is simply connected, because here we can use the approximation theorem. We observe that to prove the "only if" part, we need the trivial condition $(G_\mathfrak{D})^\mathfrak{P} = G_{\mathfrak{D}_\mathfrak{P}}$ for all $\mathfrak{P}$; which is a consequence of the strong approximation theorem, and is also verified in most of the examples listed in the next section.

As an application, we consider an admissible lattice for a simply connected Chevalley type group over k, then $G_\mathfrak{D}$ is maximal in G_k because the local maximality condition holds here (Borel-Matsumoto-Iwahori). More generally we consider a maximal k-torus T and a set of simple roots $\alpha_1, \cdots, \alpha_r$ with respect to T; we choose a Chevalley basis $\{X_\alpha, H_\alpha\}$ for the Lie Algebra $\mathfrak{g}$ of G. If

$$\alpha_0 = \sum_{i=1}^{r} m_i \alpha_i,$$

is the maximal root of G, then for every root $\alpha = \sum_{i=1}^{r} q_i \alpha_i$, we can define the Bruhat exponents $\mu_i(\alpha)$ as being 1, 0, or -1, according as whether $q_i = m_i$, $0 \leqq q_i < m_i$, or $q_i < 0$, respectively. Now we choose numbers n_α in $\mathfrak{D}$ such that at every prime $\mathfrak{P}$ the lattice generated by $n_\alpha^{\mu i(\alpha)} X_\alpha, H_\alpha\}$ is the Bruhat lattice in $\mathfrak{g}$; consequently the groups $G_\mathfrak{D}$ of units of t in this lattice are maximal in G_k because $G_{\mathfrak{D}_\mathfrak{P}}$ is maximal in $G_{k_\mathfrak{P}}$ for all $\mathfrak{P}$. It is conjectured that this result holds for any split group over k. Also it is conjectured that any maximal arithmetic group contained in G_k is conjugate to one of such groups, provided that the class number of k is one. This is a generalization of the Example 3 of the next section.

4. **Known results on the maximality of $G_{\mathfrak{D}}$.**

(1) *General results.* If L is an admissible lattice for G, a Chevalley type group over k, then $G_{\mathfrak{D}}$ is maximal in G_k provided that the class number of k is one. G_Z is maximal in G_R (Borel-Matsumoto).

(2) $G = \mathrm{Sl}_n(C)$. In this case $G_{\mathfrak{D}}$ is maximal in G_k for any k, and $\mathscr{U}/G_{\mathfrak{D}} \sim U_n$, $N(G_{\mathfrak{D}})/\mathscr{U} \sim \mathrm{IC}(n, k)$. In the case of $G_{\mathfrak{D}} = \mathrm{Sl}_2(\mathfrak{D})$, we can describe $N(G_{\mathfrak{D}})$ as follows: If $g \in \mathrm{Gl}_2(\mathfrak{D})$ and $\det(g) = \varepsilon$ is a unit of $\mathfrak{D}$, then $g/\sqrt{(\varepsilon)}$, hence $\mathscr{U}/G_{\mathfrak{D}} \sim U_2$. If $\mathscr{C}$ is an ideal class in $\mathrm{IC}(2, k)$, $\mathscr{C}^2 = 1$, and if $\mathfrak{P}_1$ and $\mathfrak{P}_2$ are two distinct primes in $\mathscr{C}$, then $\mathfrak{P}_1^2 = (w_1)$, $\mathfrak{P}_2^2 = (w_2)$, with $w_1, w_2 \in \mathfrak{D}$; hence we can find $a, b \in \mathfrak{D}$, such that $aw_1 - bw_2 = 1$. Therefore the matrix

$$g = \begin{pmatrix} a\sqrt{(w_1)} & b\sqrt{(w_2)} \\ \sqrt{(w_2)} & \sqrt{(w_1)} \end{pmatrix}$$

lies in $N(G_{\mathfrak{D}})$ provided the choice of the $w_1, w_2 \in \mathfrak{D}$ is such that $\sqrt{(w_1)} \cdot \sqrt{(w_2)} \in \mathfrak{D}$, because we can easily verify that $g = (g_{ij})$, with $(g_{ij}^2) = \mathfrak{A}_{ij}^2$, where $\mathfrak{A}_{ij}$ are non-principal ideals in $\mathfrak{D}$ lying in $\mathscr{C}$ for all $i, j = 1, 2$.

(3) $G = \mathrm{Sp}(F)$, where
$$'F = -F, \qquad F = \begin{pmatrix} 0 & \delta \\ -\delta & 0 \end{pmatrix},$$
and δ is diagonal $\{1, d_2, \cdots, d_p\}$, $\delta \in M_p(\mathfrak{D})$, and d_i divide d_{i+1} for all $i = 1, \cdots, p-1$. $G_{\mathfrak{D}}$ is maximal in G_k if and only if d_p is square free, in this case $\mathscr{U}/G_{\mathfrak{D}} \sim U_2$ and $N(G_{\mathfrak{D}})/\mathscr{U} \sim \mathrm{IC}(2, k) \times T$ where $T = \{e\}$ if p is odd, and $T = D(2, d_{s+1}/d_s)$ if $p = 2s$ is even and d_p is divisible only by principal primes. To get the ideal classes and units in $N(G_{\mathfrak{D}})$ we just embed $N(\mathrm{Sl}_2(\mathfrak{D}))$ in $N(G_{\mathfrak{D}})$ in a natural way. These results generalize the results of Gutnik ($k = Q$) and the results of Ramanathan–Christian (δ = identity).

(4) $G = \mathrm{SU}(F)$ = *the Special Unitary Group of* F. In this case k is an imaginary quadratic extension of a real number field k_0 and F is the same matrix as in (3) but now $\delta \in M_p(\mathfrak{D}_0)$ where $\mathfrak{D}_0$ is the ring of integers of k_0. We have that $G_{\mathfrak{D}}$ is maximal in G_k if for every prime $\mathfrak{P}$ dividing d_p, neither $\mathfrak{P}^2$ divides d_p, nor $\mathfrak{P}\overline{\mathfrak{P}}$ divides d_p. The converse is true if d_p is only divisible by principal primes. The image of $\mathscr{U}/G_{\mathfrak{D}}$ is contained in the subgroup U' of U_n consisting of the classes of all $\sqrt[n]{\varepsilon}$ where $\sqrt[n]{(\varepsilon)} \cdot \sqrt[n]{(\bar{\varepsilon})} \in k_0$; also this image contains the group

$$(U_0)_2 = U_0/U_0 \cap \mathfrak{D}_0$$

where U_0 is the group of all square roots of units of $\mathfrak{D}_0$. If d_p is only divisible by invariant primes and it is square free, then $N(G_{\mathfrak{D}})/\mathscr{U} \sim \mathrm{IC}(n, k)' \times T$, where $T = \{e\}$ or $D(2, d_{s+1}/d_s)$ according as whether p is odd, or p is even, $p = 2s$. Here $\mathrm{IC}(n, k)'$ denotes the subgroup of $\mathrm{IC}(n, k)$ consisting of all classes $\mathscr{C}$ such that $\mathscr{C}^n = \mathscr{C}\overline{\mathscr{C}} = 1$, and there exists $\mathfrak{P} \in \mathscr{C}$, $\mathfrak{P}^n = (w)$, and $w\bar{w} = \lambda^n$, for some $\lambda \in \mathfrak{D}_0$.

(5) $G = \mathrm{SO}(S)$ = *the Special Orthogonal Group of* S, where $S \in M_n(\mathfrak{D})$, is the matrix $(s_{ij}), i, j = 1, 2, 3$ with $s_{i3} = s_{31} = E_p$, the p by p identity, $s_{22} = V$,

$V = {}^tV \in M_r(\mathfrak{O})$ is positive definite, $\det(V)$ is a unit, and $s_{ij} = 0$, otherwise; also $n = 2p + r$ and $p > 1$. We shall assume that 2 is square free in k. In this case we may always assume, by replacing V by ${}^tf\,Vf, f \in \mathrm{Gl}_n(\mathfrak{O})$, if necessary, that $V = (v_{ij})$, $V^{-1} = (w_{ij})$, and either 2 divides all v_{ii} and all w_{jj}, or 2 divides all v_{ii} and all w_{jj} with the exception of $i = r$ and $j = r - 1$ or else r. In the first case $G_{\mathfrak{O}}$ is always maximal in G_k. In the second case the same is true provided that for any prime $\mathfrak{P}$ dividing 2, $\mathfrak{P}^2$ does not divide w_{rr} and $\mathfrak{P}^2$ does not divide $v_{r-1\,r-1}$ or else v_{rr}. Under these conditions, every element of $N(G_{\mathfrak{O}})$ is a matrix with algebraic integral entries only. In particular, if n is odd, then $G_{\mathfrak{O}}$ is maximal in G, because in this case G is centerless. If V is the r by r identity matrix, then $G_{\mathfrak{O}}$ is maximal in G_k if 4 does not divide r, and $G_{\mathfrak{O}}$ is not maximal in G_k if $r = 4$.

(6) $G = \mathrm{SU}(S)$, where S is taken as in (5), but here we assume that V is hermitian positive, and k is an imaginary quadratic extension of a real number field k_0. If r is even and there exists an element of $\mathfrak{O}$ with trace one, then $G_{\mathfrak{O}}$ is maximal in G_k, and every matrix in $N(G_{\mathfrak{O}})$ has only algebraic integral entries. If r is odd and $\mathscr{T}$ denotes the ideal $\mathrm{tr}_{k|k_0}(\mathfrak{O})$, then if $\mathscr{T}$ is prime in k_0 we always may assume that $\mathscr{T}$ divides v_{ii} and w_{jj} with exception of v_{rr} and w_{rr}, and in this case the same result, as above, is true.

(7) $G =$ *Group of units of a quaternion form.* Let $\boldsymbol{D}$ be an involutorial quaternion algebra of first kind over a real number field k and let $\boldsymbol{D}^{\#} = \boldsymbol{D} \otimes_k \boldsymbol{R}$. Let $\boldsymbol{O}$ be a maximal order in $\boldsymbol{D}$ and $\boldsymbol{H} \in M_n(\boldsymbol{O})$ be a quaternion hermitian or skew hermitian matrix. Let $G = \mathrm{SU}(\boldsymbol{H}) = \{g \in M_n(\boldsymbol{D}^{\#}) | g^*\boldsymbol{H}g = \boldsymbol{H}\}$ where * denotes the extension of the involution of $\boldsymbol{D}$ to $M_n(\boldsymbol{D}^{\#})$. Again if Δ is any subgroup of $G_{\boldsymbol{D}}$, $\Delta \sim G_{\boldsymbol{O}}$, then we can find a number $\lambda, \lambda' \in \mathfrak{O}$ such that

$$\lambda M_n(\boldsymbol{O}) \subset \lambda' \boldsymbol{L} \subset M_n(\boldsymbol{O})$$

where $\boldsymbol{L} = A(\Delta, \mathfrak{O})$ is the $\mathfrak{O}$-order of Δ in $M_n(\ D)$, provided that G is noncompact. We also have that, if Δ is maximal in $G_{\boldsymbol{D}}$, then there exists a unique maximal arithmetic group containing Δ and this group is $N(\Delta)$. $N(\Delta)/\Delta$ is finite abelian and everyone of its elements has order dividing 2. Every $g \in N(\Delta)$ can be written as $g'\sqrt{a}$, with $g' \in M_n(\boldsymbol{D})$ and $a \in k$. If we denote by $\mathscr{U}$ the subgroup of $N(\Delta)$ consisting of those elements g where a can be taken as a unit of $\mathfrak{O}$ then $\mathscr{U}/\Delta \sim U_2$. Also there exists a number $\lambda_1 \in \mathfrak{O}$ depending only on λ and $\boldsymbol{O}$ such that, if λ_1 is only divisible by principal primes, then $N(\Delta)/\mathscr{U}$ is isomorphic to a subgroup of $\mathrm{IC}(2, k) \times D(2, \lambda_1)$. We fix now a basis of $\boldsymbol{D}$ over k consisting of $1, w_1, w_2, w_1w_2 \in \boldsymbol{O}$ such that $w_1^2 = a$, $w_2^2 = b$, $a, b \in \mathfrak{O}$, and $w_1w_2 + w_2w_1 = 0$. Then we can take $\lambda_1 = 2ab\lambda$. In particular, if $a, b \neq \pm 1$ and $2ab$ is only divisible by principal primes, and $\boldsymbol{H}$ is the matrix $\boldsymbol{F}$ considered in (3) with δ being the identity matrix, then $G_{\boldsymbol{O}}$ is maximal in $G_{\boldsymbol{D}}, \mathscr{U}/G_{\boldsymbol{O}} \sim U_2$ and $N(G_{\boldsymbol{O}})/\mathscr{U} \sim \mathrm{IC}(2, k) \times T$ where T is a subgroup of $D(2, 2ab)$ with order at least 4. If $\boldsymbol{H}$ is the matrix $\boldsymbol{S}$ considered in (5). Then $G_{\boldsymbol{O}}$ is maximal in $G_{\boldsymbol{D}}$, provided that there exists in $\boldsymbol{O}$ an element with trace one; $\mathscr{U}/G_{\boldsymbol{O}}$ is isomorphic to a subgroup of U_2 and $N(G_{\boldsymbol{O}})/\mathscr{U}$ is isomorphic to a subgroup of $\mathrm{IC}(2, k) \times D(2, 2ab)$.

5. **Applications to bounded domains.** We would like to point out how to find maximal discontinuous groups acting in some bounded domains. If G is a connected semisimple linear group defined over k such that G/K is a bounded domain where K is a maximal compact subgroup of G, then $G_{\mathfrak{O}}$ acts discontinuously in the product, $\mathscr{D}$, of $s = [k:Q]$ copies of irreducible bounded domains. In general $N(G_{\mathfrak{O}})$ is too big in the sense that it cannot be embedded in the identity component, $\mathrm{T}(\mathscr{D})^0$, of the group of isometries of $\mathscr{D}$. In the case where G is either of orthogonal type or of symplectic type then the biggest subgroup of $N(G_{\mathfrak{O}})$ which can be embedded in $\mathrm{T}(\mathscr{D})^0$ consists of the elements where $g = g' \cdot \sqrt{a}$ with a being a totally positive number. We shall denote it by $N(G_{\mathfrak{O}})^*$. Then there exists a unique maximal (in $\mathrm{T}(\mathscr{D})^0$) discontinuous group containing $G_{\mathfrak{O}}$, and this group is the direct product of $N(G_{\mathfrak{O}})^*$ by the center of $\mathrm{T}(\mathscr{D})^0$.

References

1. N. Allan, *Maximality of some arithmetic groups*, forthcoming thesis, The University of Chicago.

2. A. Borel, *Density and maximality of arithmetic subgroups*, (to appear).

3. U. V. Christian, *Zur theorie der Hilbert-Siegelschen Modulfunktionen*, Math. Ann. **152** (1963), 275–341.

4. L. Greenberg, *Maximal Fuchsian groups*, Bull. Amer. Math. Soc. **69** (1963), 569–573.

5. L. Gutnik, *On the extension of integral subgroups of some groups*, Vestnik Leningrad Univ. Ser. Math. Mech. and Astr. **12** (1957), no. 19, 47–78.

6. H. Hijikata, *Maximal compact subgroups of* $\mathfrak{p}$*-adic classical groups*, Notes from Yale University.

7. N. Iwahori, *Generalized Tits system*, Proc. Sympos. Pure Math., vol. 9, Amer. Math. Soc., Providence, R.I., 1966, pp. 71–83.

8. N. Iwahori and H. Matsumoto, *On some Bruhat decompositions*, Publ. of I.H.E.S. **25** (1965), pp. 237–280.

9. H. Maass, *Über die Erweiterungsfähigkeit der Hilbertschen Modulgruppe*, Math. Ž. **51** (1948), 255–261.

10. K. Ramanathan, *Discontinuous groups*. II, Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II (1964), 145–164.

11. H. C. Wang, *On a maximality property of discrete subgroups with fundamental domain of finite measure*, Amer. J. Math. (to appear).

II. Arithmetic Properties of Algebraic Groups. Adèle Groups

Adèles

BY

TSUNEO TAMAGAWA

1. **Valuations.** Let k be an algebraic number field. Denote the r_1 real embeddings of k into C by $\{\sigma_1, \sigma_2, \cdots, \sigma_{r_1}\}$ and the $2r_2 = n - r_1$ nonreal embeddings by $\{\sigma_{r_1+1}, \sigma_{r_1+2}, \cdots, \sigma_{r_1+r_2}; \bar{\sigma}_{r_1+1}, \cdots, \bar{\sigma}_{r_1+r_2}\}$. For each real σ we define a (real) valuation of k by:

$$|\alpha|_{\mathfrak{p}_{\infty,\sigma}} = |\alpha^{\sigma}| \qquad \text{for } \alpha \in k;$$

if σ is nonreal, we define

$$|\alpha|_{\mathfrak{p}_{\infty,\sigma}} = |\alpha^{\sigma}|^2 = \alpha^{\sigma}\alpha^{\bar{\sigma}}.$$

The $r_1 + r_2$ archimedean valuations thus obtained are denoted

$$\{|\ |_{\mathfrak{p}_{\infty,1}}, \cdots, |\ |_{\mathfrak{p}_{\infty,r_1}}; |\ |_{\mathfrak{p}_{\infty,r_1+1}} \cdots, |\ |_{\mathfrak{p}_{\infty,r_1+r_2}}\}.$$

Each of these defines in k a metric with respect to which k is a topological field; the completion of k with respect to $|\ |_{\mathfrak{p}_{\infty,i}}$ is denoted by $k_{\mathfrak{p}_{\infty,i}}$ and is topologically isomorphic to the field of real numbers for $i = 1, \cdots, r_1$, and to the field of complex numbers for $i = r_1 + 1, \cdots, r_1 + r_2$.

For each (integral) prime ideal $\mathfrak{p}$ in the ring of algebraic integers $\mathcal{O}$ of k, we define a nonarchimedean valuation $|\ |_{\mathfrak{p}}$ by:

$$|\alpha|_{\mathfrak{p}} = (N_{\mathfrak{p}})^{-\mathrm{ord}_{\mathfrak{p}}\alpha} \qquad \text{for } \alpha \in k$$

where $N_{\mathfrak{p}}$ is the norm of $\mathfrak{p}$ and $\mathrm{ord}_{\mathfrak{p}}(\alpha)$ is the power to which the prime ideal $\mathfrak{p}$ occurs in the factorization of the principal ideal (α). Each such valuation defines a metric in k whose completion is denoted by $k_{\mathfrak{p}}$; the latter is a locally compact, totally-disconnected topological field. The compact, open subring $\mathcal{O}_{\mathfrak{p}}$ of $k_{\mathfrak{p}}$ defined by

$$\mathcal{O}_{\mathfrak{p}} = \{\beta \in k_{\mathfrak{p}} \,\big|\, |\beta|_{\mathfrak{p}} \leqq 1\}$$

is called the ring of integers in $k_{\mathfrak{p}}$; its unit group $U_{\mathfrak{p}}$ is defined by

$$U_{\mathfrak{p}} = \{\beta \in k_{\mathfrak{p}} \,\big|\, |\beta|_{\mathfrak{p}} = 1\}$$

and is compact.

These valuations satisfy the following Product Formula:

$$\prod_{\mathfrak{p}} |\alpha|_{\mathfrak{p}} = 1 \qquad \text{for all } \alpha \in k^*$$

where the product is taken over *all* the valuations defined above.

We call these valuations "primes"; the archimedean ones are referred to as "infinite primes."

2. **Definition of adèle ring.** Let S be a finite set of primes containing all the infinite ones. We put the product topology in the Cartesian product

$$A_S = \left(\prod_{\mathfrak{p}\notin S} \mathcal{O}_\mathfrak{p}\right)\left(\prod_{\mathfrak{g}\in S} k_\mathfrak{g}\right)$$

and get a locally compact ring (addition and multiplication component-wise). For $S \subset S'$ there is a natural injection $\phi: A_S \to A_{S'}$ with ϕ of (A_S) open in $A_{S'}$. Thus in

$$A_k \overset{\mathrm{def}^n}{=} \lim_S A_S$$

there is a unique topology such that each A_S is open. A_k is a locally compact topological ring.

3. **Adèlized variety.** Let V be an affine variety contained in Ω^n and defined over k and let $\mathfrak{P}$ be the (prime) ideal of V in $k[X_1, \cdots, X_n]$. The set of points

$$V_A = \{(a_1, a_2, \cdots, a_n) \in A_k^n \mid F(a_1, \cdots, a_n) = 0 \text{ for all } F \in \mathfrak{P}\}$$

is called the adèlized variety of V over k.

Alternately, we can define V_A as the limit of V_{A_s} where

$$V_{A_s} = \left(\prod_{\mathfrak{p}\notin S} V_{\mathcal{O}_\mathfrak{p}}\right) \times \left(\prod_{\mathfrak{p}\in S} V_{k_\mathfrak{p}}\right).$$

For the case of an abstract variety we proceed as follows. Let $V_1, \cdots, V_n$ be affine varieties. Let V be a set and f_i an injection $f_i\colon V_i \to V$ for $i = 1, 2, \cdots, n$. Suppose:

(1) $$V = \bigcup_{i=1}^{n} f_i(V_i)$$

(2) The mapping T_{ij} taking $f_i^{-1}(p)$ to $f_j^{-1}(p)$ is a birational mapping defined for all $p \in f_i(V_i) \cap f_j(V_j)$.

Then $\{(f_1, V_1), \cdots, (f_n, V_n)\}$ is called an *abstract* variety (usually just denoted V) and is said to be defined over k in case the $\{V_i\}$ and $\{T_{ij}\}$ are defined over k. Assume V is defined over k and set

$$V_{\mathcal{O}_\mathfrak{p}} = \bigcup_{i=1}^{n} f_i[(V_i)_{\mathcal{O}_\mathfrak{p}}]$$

for finite $\mathfrak{p}$,

$$V_{k_\mathfrak{p}} = \bigcup_{i=1}^{n} f_i[(V_i)_{k_\mathfrak{p}}].$$

V_{A_s} and V_A are now defined by:

$$V_{A_s} = \left(\prod_{\mathfrak{p}\notin S} V_{\mathcal{O}_\mathfrak{p}}\right) \times \left(\prod_{\mathfrak{p}\in S} V_{k_\mathfrak{p}}\right),$$

and

$$V_A = \lim_{S} V_{A_s}.$$

It can be shown that this definition is independent of the affine covering $\{(f_1, V_1), \cdots, (f_n, V_n)\}$ for V; more precisely, if F is a morphism of $V = \bigcup_{i=1}^{n} f_i(V_i)$ to $W = \bigcup_{j=1}^{m} g_j(W_j)$ and V, W, and F are defined over k, then F maps $V_{\mathcal{O}_\mathfrak{p}}$ into $W_{\mathcal{O}_\mathfrak{p}}$ for almost all $\mathfrak{p}$—thus, if F is an isomorphism, V_A is isomorphic to W_A.

EXAMPLE. Let $V = \Omega^n - \{0\}$. Define $V_i \subset \Omega^{n+1}$ by

$$V_i = \{(a_1, \cdots, a_n, 1/a_i)\}$$

for $i = 1, 2, \cdots, n$. Let $\pi : \Omega^{n+1} \to \Omega^n$ map $(x_1, \cdots, x_{n+1})$ to $(x_1, \cdots x_n)$. Then $V = \{(\pi_1, V_1), \cdots, (\pi_n, V_n)\}$ is an abstract variety defined over the prime field. $(V_i)_{\mathcal{O}_\mathfrak{p}}$ is the subset of $k_\mathfrak{p}^n$

$$(V_i)_{\mathcal{O}_\mathfrak{p}} = \left\{(a_1, a_2, \cdots, a_n, 1/a_i) \middle| \begin{array}{l}(1)\ a_i \in U_\mathfrak{p} \\ (2)\ a_j \in \mathcal{O}_\mathfrak{p} \quad j = 1, 2, \cdots, n\end{array}\right\}.$$

Moreover,

$$V_{\mathcal{O}_\mathfrak{p}} = \{(a_1, a_2, \cdots, a_n) | \text{at least one } a_i \text{ is a unit}\},$$

$$V_{k_\mathfrak{p}} = \{(a_1, a_2, \cdots, a_n) | \text{at least one } a_i \text{ is nonzero}\}.$$

For $x \in \prod_{\text{all}\,\mathfrak{p}} k_\mathfrak{p}^n$ we write $\Pi_\mathfrak{p}(x) = (a_1, a_2, \cdots, a_n)$ with $a_i \in k_\mathfrak{p}$. V_A is the set of all $x \in \prod_\mathfrak{p} k_\mathfrak{p}^n$ such that:

(1) for each $\mathfrak{p}$, at least one a_i is $\neq 0$,

(2) for almost all $\mathfrak{p}$, all a_i are integers and at least one is a unit.

4. **Adèlized group.** For a linear algebraic group G defined over k, the group operations can be extended to G_{A_k}, which is thereby a locally compact group.

EXAMPLES. (1) Let G be the additive group k^+. Then $G_{A_k} = A_k$.

(2) If G is the multiplicative group $k^* \cong Gl_1$, then G_{A_k} is the group of units of the adèle ring; i.e., G_{A_k} is the group of elements $a = (a_\mathfrak{p}) \in \prod_\mathfrak{p} k_\mathfrak{p}$ such that:

(i) $a_\mathfrak{p} \neq 0$ for all $\mathfrak{p}$,

(ii) $a_\mathfrak{p} \in U_\mathfrak{p}$ for almost all $\mathfrak{p}$.

($k^*_{A_k}$ is the "idèle group" of Chevalley.)

(3) $G = Sl(n, k)$. G_{A_k} is the set of all $x \in \prod_\mathfrak{p} Sl(n, k_\mathfrak{p})$ such that $\pi_\mathfrak{p}(x) \in Sl(n, \mathcal{O}_\mathfrak{p})$ for almost all $\mathfrak{p}$.

(4) $G = Gl(n, k)$. G_{A_k} is the set of all $x \in \prod_\mathfrak{p} Gl(n, k_\mathfrak{p})$ such that $\pi_\mathfrak{p}(x) \in Gl(n, \mathcal{O}_\mathfrak{p})$ for almost all $\mathfrak{p}$; i.e.,

(i) $\det(\pi_\mathfrak{p}(x)) \neq 0$ for all $\mathfrak{p}$,

(ii) $\det(\pi_\mathfrak{p}(x)) \in U_\mathfrak{p}$ for almost all $\mathfrak{p}$,

(iii) $\pi_\mathfrak{p}(x) \in Gl(n, \mathcal{O}_\mathfrak{p})$ for almost all $\mathfrak{p}$.

NOTE. Given a morphism $\phi: G \to G'$ we can extend to a morphism $\phi_{A_k} G_{A_k} \to G'_{A_k}$ (where G, G', and ϕ are defined over k). It is *not* always true that ϕ_{A_k} is superlative when ϕ is—nor is it true that $\phi_{A_k}(G_{A_k})$ must be open in G'_{A_k}; however, $\phi_{A_k}(G_{A_k})$ is closed in G'_{A_k}.

Let G be a connected algebraic group defined over k with algebraic subgroup H also defined over k. The morphism $\Pi: G \to G/H = S$ extends to a morphism $\Pi_{A_k}: G_{A_k} \to S_{A_k}$. In some cases Π_{A_k} is surjective and we can identify S_{A_k} with G_{A_k}/H_{A_k}; e.g., if there exists a rational cross-section ϕ defined over k on an open set ($\phi: S \to G$ and $\Pi \circ \phi$ = identity on S) then this is the case.

5. **Certain homogeneous spaces.** There is a natural injection of k into A_k; viz., $\alpha \to (\alpha, \alpha, \cdots)$. In this way, k is identified with a discrete subgroup of A_k and A_k/k is compact. More generally, we identify k^n with the diagonal in A_k^n and for any affine variety V defined over k then V_k is discrete in V_{A_k}.

NOTE. If V is not an affine variety, this is not necessarily so. However, if G is an algebraic group, G_k is a discrete subgroup of G_{A_k} because G is embedded in an affine space, the homogeneous space G_A/G_k.

Assume G connected and let $X_k(G)$ be the group of (rational) characters of G defined over k. For each $X \in X_k(G)$ and $g \in G_{A_k}$ we have an idèle g^X. We define:

$$\|g^X\| \overset{\text{def}^n}{=} \psi_X(g) \overset{\text{def}^n}{=} \prod_{\mathfrak{p}} |g_{\mathfrak{p}}^X|_{\mathfrak{p}}$$

(where $g_{\mathfrak{p}} = \pi_{\mathfrak{p}}(g)$). The mapping ψ_X sends G_{A_k} into the multiplicative group of positive real numbers, R. Now, $X_k(G)$ is a free abelian group on a finite number of generators, say $\{X_1, \cdots, X_m\}$. Set $G_{A_k}^1 = \bigcap_{i=1}^m \ker \psi_{X_i}$. By the product formula, we see that $G_{A_k}^1 \supset G_k$.

THEOREM (BOREL—HARISH-CHANDRA). *$G_{A_k}^1/G_k$ has finite invariant volume (hence $G_{A_k}^1$ is unimodular); moreover, if G_k has no unipotent elements, $G_{A_k}^1/G_k$ is compact.*

6. **Restriction of the ground field.**

DEFINITION. Let K/k be a separable extension of (finite) degree d and let $\Sigma = \{\sigma_1, \sigma_2, \cdots, \sigma_d\}$ be the distinct isomorphisms of K (over k) into the algebraic closure $\bar{k}$. Let V be a variety defined over K. Let W be a variety defined over k and $P: W \to V$ a morphism defined over K (which automatically induces a morphism $P^{\sigma_i}: W \to V^{\sigma_i}$ defined over K^{σ_i} for each $i = 1, 2, \cdots, d$) for which the morphism

$$P^{\sigma_1} \times \cdots \times P^{\sigma_d}: W \to V^{\sigma_1} \times V^{\sigma_2} \times \cdots \times V^{\sigma_d}$$

is biregular. Then we say that the pair (W, P) is the restriction of V to k and we write $(W, P) = R_{K/k}(V)$.

REMARK. (1) For any other (W', P') satisfying these conditions, there exists a morphism ϕ defined over k such that the following diagram commutes:

$$\begin{tikzcd}
W' \arrow[rr, "P'^{\sigma_1}\times\cdots\times P'^{\sigma_d}"] \arrow[dr, "\phi"'] & & V^{\sigma_1}\times\cdots\times V^{\sigma_d} \\
& W \arrow[ur, "P^{\sigma_1}\times\cdots\times P^{\sigma_d}"'] &
\end{tikzcd}$$

In particular, the restriction is unique.

(2) For any variety defined over K and K/k separable of degree $d < \infty$, the restriction exists.

(3) If $R_{K/k}(V) = W$, there is a 1-1 correspondence between the points of W_k and those of V_K.

EXAMPLE. Let $V = G_a$ be the additive group of Ω. Let $\{\alpha_1, \alpha_2, \cdots, \alpha_d\}$ be any basis for K/k. Set $W = \Omega^d = G_a \times \cdots \times G_a$, taken d times, and $P\colon W \to V$ the morphism defined by $P(u_1, u_2, \cdots, u_d) = \sum_{j=1}^{d} \alpha_i u_i$.

Let k' be an extension of k. For $\sigma_i, \sigma_j \in \Sigma$, we say

$$\sigma_i \underset{k'}{\sim} \sigma_j$$

if there exists an isomorphism σ over k' such that $\sigma_j = \sigma_i\sigma$ (note that the automorphisms operate on the right here). In this way, Σ is partitioned into the disjoint union of subsets $\Sigma = \bigcup \Sigma_i$. For each i, choose a $\sigma_i \in \Sigma_i$. Then

$$R_{K/k}(V) \cong \prod R_{K^{\sigma_i}\cdot k'/k'}(V^{\sigma_i}).$$

In case k' is $k_\mathfrak{p}$, we can use this to identify W_{A_k} with V_{A_k}.

7. **Measure on** V_{A_k}. Let V be a nonsingular variety of dimension n defined over k; and let ω be an algebraic n-form defined over k such that

(1) $\omega \neq 0$ everywhere on V.

(2) ω is holomorphic on V; i.e., choosing local uniformizing parameters $\{x_1, x_2, \cdots, x_n\}$ at a point $v \in V$ we have

$$\omega = \phi_v(x)\, dx_1 \wedge dx_2 \wedge \cdots \wedge dx_n$$

with $\phi_v(x)$ holomorphic in a neighborhood of v.

Let k be an algebraic number field. Fix a point $v \in V_{k_\mathfrak{p}}$ and local uniformizing parameters $\{x_1, \cdots, x_n\}$ with $x_i(v) = 0$. Then we can write

$$\omega = \phi_v(x)\, dx_1 \wedge dx_2 \wedge \cdots \wedge dx_n.$$

Since v is a simple point, the formal expansion

$$\phi_v(x) = \sum C_{\nu_1\cdots\nu_n} x_1^{\nu_1} \cdots x_n^{\nu_n}$$

converges in some $\mathfrak{p}$-adic neighborhood $\mathfrak{U}$ of v which can (via $\{x_1, \cdots, x_n\}$) be identified with the set of points $\mathfrak{U}_\varepsilon \subset k_\mathfrak{p}^n$ defined by:

$$\mathfrak{U}_\varepsilon = \{(C_1, C_2, \cdots, C_n);\ C_i \in k_\mathfrak{p} \text{ and } |C_i|_\mathfrak{p} < \varepsilon\}.$$

A measure is defined on $\mathfrak{U}$ as follows:

(1) normalize the Haar-measure $dx_{\mathfrak{p}}$ on $k_{\mathfrak{p}}$ by the condition that

$$\int_{\mathcal{O}_{\mathfrak{p}}} dx_{\mathfrak{p}} = 1,$$

(2) taking the product measure $|\phi_{v}(x)|_{\mathfrak{p}}|dx_1 \cdots dx_n|_{\mathfrak{p}}$ on $k_{\mathfrak{p}}$ we have a measure on $\mathfrak{U}_{\varepsilon}$,

(3) we transfer this measure back to $\mathfrak{U}$.

It can be shown that on the overlap of $\mathfrak{U}$ and $\mathfrak{U}'$, two such measures coincide and hence we get a well-defined measure $|\omega|_{\mathfrak{p}}$ on $V_{k_{\mathfrak{p}}}$.

THEOREM. *For almost all* $\mathfrak{p}$,

$$\int_{V_{\mathcal{O}_{\mathfrak{p}}}} |\omega|_{\mathfrak{p}} = (q^{-d}) \times (\text{number of points on the reduced variety } \overline{V}_{\mathfrak{p}})$$

where $q = N_{\mathfrak{p}}$.

Let G be an algebraic group defined over k and ω a left-invariant form. On $G_{k_{\mathfrak{p}}}$ we have a measure $|\omega|_{\mathfrak{p}}$ as constructed above. For each finite prime $\mathfrak{p}$ we define

$$\mu_{\mathfrak{p}} = \int_{G_{\mathcal{O}_{\mathfrak{p}}}} |\omega|_{\mathfrak{p}}.$$

If G is semisimple, the product $\prod \mu_{\mathfrak{p}}$, $\mathfrak{p}$ finite, converges absolutely. Then we can define the product measure on the open subset

$$\prod_{\mathfrak{p}\,\text{finite}} G_{\mathcal{O}_{\mathfrak{p}}} \times \prod_{\mathfrak{p}\,\text{infinite}} G_{k_{\mathfrak{p}}}$$

of G_{A_k}, and this in turn determines a measure G_{A_k}. By suitable choice of convergence factors $\lambda_{\mathfrak{p}}$, it can be arranged in many other cases that $\prod_{\mathfrak{p}}(\lambda_{\mathfrak{p}}\mu_{\mathfrak{p}})$ converges absolutely. (This will be taken up in Ono's lectures to follow.) We point out that the measure on G_{A_k} does not depend on ω, because of the product formula:

$$|C\omega|_{\mathfrak{p}} = |C|_{\mathfrak{p}}|\omega|_{\mathfrak{p}} \text{ and}$$
$$\prod_{\mathfrak{p}} |C|_{\mathfrak{p}} = 1.$$

DEFINITION. Let G be a semisimple algebraic group over k. The Tamagawa number $\tau(G)$ is defined by

$$\tau(G) = |D|^{-\dim G/2} \int_{G_{A_k}/G_k} |\omega| < \infty,$$

where D is the discriminant of k; i.e.,

$$D = \text{absolute value of } \det \begin{pmatrix} \alpha_1^{\sigma_1} \cdots \alpha_n^{\sigma_1} \\ \alpha_1^{\sigma_2} \cdots \alpha_n^{\sigma_2} \\ \vdots \qquad \vdots \\ \alpha_1^{\sigma_n} \qquad \alpha_n^{\sigma_n} \end{pmatrix}^2$$

for a minimal basis of k over Q.

REMARK.

$$\tau(\mathrm{Sl}(n)) = 1\,;\ \tau(\mathrm{Sp}(2n)) = 1\,;\ \tau(O^+(n, S)) = 2$$

where S is a symmetric $n \times n$ matrix and O^+ means the proper orthogonal group of the associated quadratic form.

8. Connection between Siegel's theory and $\tau(O^+(n, S)) = 2$. Let S be an $n \times n$ positive definite symmetric integral matrix. For every prime number p, let $A_{p^v}(S)$ be the number of solutions of the congruence

$${}^tXSX \equiv S \qquad (\mathrm{mod}\; p^v).$$

Then for sufficiently large positive integer v, $\frac{1}{2}p^{-(1/2)vn(n-1)}A_{p^v}(S)$ is independent of v, and the value will be denoted by $\alpha_p(S)$. If $p \nmid 2 \det S$, we have

$$\alpha_p(S) = \tfrac{1}{2}p^{-(1/2)n(n-1)}A_p(S).$$

For the infinite prime p_∞, we define $\alpha_\infty(S)$ as follows. Let $\mathcal{U}$ be a compact neighborhood of S, and $\mathfrak{U}$ be the set of all X with ${}^tXSX \in \mathcal{U}$. Then $\mathfrak{U}$ is also a compact set in the affine space of all $n \times n$ real matrices. We define $\alpha_\infty(S)$ by the limits

$$\tfrac{1}{2} \lim_{\mathfrak{U} \to S} \frac{\int_{\mathfrak{U}} dx}{\int_{\mathfrak{U}} dS}.$$

To explain Siegel's theorem, we have to introduce the notion of genus. Two integral symmetric matrices S_1 and S_2 are called locally equivalent if for every prime (finite or infinite) p, there exists a matrix X_p in Q_p which is integral and unimodular if p is finite, such that $S_2 = {}^tX_pS_1X_p$. The local equivalency defines the notion of genus. S_1 and S_2 are called strongly equivalent if there exists an integral unimodular matrix X of determinant $+1$ such that $S_2 = {}^tXS_1X$. This equivalency defines the notion of the class. The genus of S consists of a finite number of classes. Let $S_1, \cdots, S_g$ be a set of representatives of those classes. For each S_i, the order of the group of all proper unimodular matrices X with ${}^tXS_iX = S_i$ will be denoted by $E(s_i)$. Then Siegel's theorem asserts that

$$\prod_p \alpha_p(S)\left(\sum_{i=1}^{g} 1/E(S_i)\right) = 2.$$

Now we try to interpret this result to our language. Let G be the algebraic group of the $n \times n$ matrices with ${}^tXSX = S$ and $\det S = 1$. Let x_{ij}, $1 \leqq i, j \leqq n$ be coordinate functions of $X = (x_{ij})$ in the n^2-dimensional affine space $M(n)$ of all $n \times n$ matrices, and t_{ij}, $1 \leqq i \leqq j \leqq n$ be coordinate functions of the $\frac{1}{2}n(n+1)$-dimensional affine space of all $n \times n$ symmetric matrices. Put ${}^tXSX = T$. Then t_{ij} are polynomials of x_{ij}, so we have a $\frac{1}{2}n(n-1)$ form ϖ such that

$$\bigwedge_{i,j=1}^{n} dx_{ij} = \bigwedge_{i \leqq j} dt_{ij} \wedge \varpi.$$

Now we have the injection map ι of G into $M(n)$, so that $\delta\iota(\varpi) = \omega$ is a $\frac{1}{2}n(n-1)$-form on G. It is easy to see that

$$\int_{G_{\mathfrak{O}_p}} |\omega|_p = \alpha_p(S) \qquad p = \text{finite}$$

and

$$\int_{G_{Q_{p_\infty}}} |\omega|_\infty = \alpha_\infty(S).$$

Hence we have

$$\int_{\Pi G_{\mathfrak{O}_p} \times G_{Q_\infty}} |\omega| = \prod_p \alpha_p(S).$$

Now the group $U = \prod G_{\mathfrak{O}_p} \times G_{Q_\infty}$ is an open subgroup of G_A, and we have the double coset decomposition

$$G_A = Ua_1G_Q \cup Ua_2G_Q \cup \cdots \cup Ua_gG_Q.$$

Hence the volume of G_A/G_Q is equal to

$$\prod \alpha_p(S) \sum 1/\text{ord}(a_i^{-1}Ua_i \cap G_Q).$$

Now we study the meaning of $\text{ord}(a_i^{-1}Ua_iG_Q)$. For every $a \in G_A$, we have ${}^taSa = S$. Now there exists a rational matrix A such that $a = uA^{-1}$ where $u = (u_p)$ belongs to $GL(n)_A$ and all u_p are unimodular. Then by the definition, ${}^tASA$ belongs to the same genus of S. The class of ${}^tASA$ is uniquely determined by the double coset UaG_Q, and $E({}^tASA)$ is equal to the order of $a^{-1}Ua \cap G_Q$. Hence we have

$$\tau(G) = \text{volume}\,(G_A/G_Q) = \prod \alpha_p(S) \sum 1/E(S_i).$$

To prove that $\tau(G) = 2$, we use the induction with respect to n. For $n = 3$ and 4, we can easily calculate $\tau(G)$ because in these cases, G is of type A_1 or $A_1 \times A_1$, and $\tau(G)$ is obtained by comparing with $\tau(\tilde{G})$ where $\tilde{G}$ is the simply connected covering of G. For $n \geqq 5$, we refer to Siegel-Weil's theorem. If S indefinite, we need some modification. Namely, in this case, $\mathfrak{U}$ is not compact, and the order of the group $U(S)$ of all proper unimodular matrices X with ${}^tXSX = S$ is also infinite. However, $U(S)$ operates on $\mathfrak{U}$ from the left side, and we can construct a fundamental domain $\mathscr{F}$ of good shape. Now we define $\rho(S)$ by

$$\lim_{\mathfrak{U} \to 0} \frac{\text{Volume}\,(\mathscr{F})}{\text{Volume}\,(\mathfrak{U})} = \rho(S).$$

Siegel's theorem in this case is as follows:

$$\prod_p \alpha_p(S)(\sum \rho(S_i)) = 2.$$

If we observe the fact that

$$\rho(S) = \int_{G_\infty/U(S)} |\omega|_\infty,$$

the interpretation of this formula to our language is also easy.

Reference

A. Weil, *Adèles and algebraic groups*, Lecture Notes, The Institute for Advanced Study, Princeton, N.J., 1961.

On Tamagawa Numbers

BY

TAKASHI ONO

We want to determine the Tamagawa number of semisimple groups modulo Weil's conjecture on simply connected groups. We begin with an Appendix to Tamagawa's talk [5].

1. **Number of rational points.** Let k be an algebraic number field, G be a connected linear algebraic group defined over k. We denote by $G^{(\mathfrak{p})}$ the algebraic group defined over the residue field $k^{(\mathfrak{p})} = \mathfrak{o}/\mathfrak{p}$ obtained from G by the reduction modulo $\mathfrak{p}$. Let ω be a left invariant highest differential form on G defined over k. On each local group $G_v = G_{k_v}$, ω induces a Haar measure ω_v and we have

$$\int_{G_{\mathfrak{o}_\mathfrak{p}}} \omega_\mathfrak{p} = q^{-\dim G}[G^{(\mathfrak{p})}_{k^{(\mathfrak{p})}}] \overset{\mathrm{def}}{=} \nu_\mathfrak{p}(G)$$

for almost all $\mathfrak{p}$, where $q = N\mathfrak{p}$. We say that G has the property (C) if $\prod'_\mathfrak{p} \nu_\mathfrak{p}(G)$ is absolutely convergent, where $\prod'_\mathfrak{p}$ means the product over almost all $\mathfrak{p}$. Since k is of characteristic zero G is decomposed as $G = UTS$ where $U = R_u(G)$ (unipotent radical), $UT = R(G)$ (radical), $TS = A$ reductive, $T =$ the identity component of the center of A, $S =$ the derived group of A, $G = UA$ is semidirect product with U normal and A is isogenous to $T \times S$. Since such a decomposition commutes with the reduction modulo $\mathfrak{p}$, for almost all $\mathfrak{p}$, we have $\nu_\mathfrak{p}(G) = \nu_\mathfrak{p}(U)\nu_\mathfrak{p}(T)\nu_\mathfrak{p}(S)$ for almost all $\mathfrak{p}$. Thus the problem of finding the convergence factors is reduced to the cases in which G is unipotent, a torus or semisimple:

(1) If $G = U$ is unipotent, then G is a semidirect product of G_a's and so $\nu_\mathfrak{p}(G) = 1$. Hence all unipotent groups have the property (C) and no convergence factors are necessary.

(2) If $G = T$ is a torus, let K be a finite Galois splitting field for T over k with the Galois group $\mathfrak{G} = \mathfrak{G}(K/k)$. Then $\hat{T} = (\hat{T})_K$ is a $\boldsymbol{Z}$-free $\mathfrak{G}$-module of rank $d = \dim T$. Let $\mathfrak{p}$ be a finite prime of k, unramified relative to K/k. Let $\mathfrak{P}$ be a prime of K over $\mathfrak{p}$ and $\sigma_\mathfrak{P}$ be the Frobenius substitution of $\mathfrak{P}$. If ξ_i, $1 \leqq i \leqq d$, is a $\boldsymbol{Z}$-basis for $\hat{T}$, we have an integral representation $\sigma \to M(\sigma)$ of $\mathfrak{G}$ defined by

$$\begin{pmatrix} \xi_1^\sigma \\ \cdot \\ \cdot \\ \cdot \\ \xi_d^\sigma \end{pmatrix} = M(\sigma) \begin{pmatrix} \xi_1 \\ \cdot \\ \cdot \\ \cdot \\ \xi_d \end{pmatrix}.$$

Then, $[T^{(\mathfrak{p})}_{k(\mathfrak{p})}] = \det(qI_d - M(\sigma_{\mathfrak{P}}))$ and hence

$$v_{\mathfrak{p}}(T) = \det(I_d - q^{-1}M(\sigma_{\mathfrak{P}})) = L_{\mathfrak{p}}(1, \chi_T, K/k)^{-1}$$

where χ_T is the character of the representation $\sigma \to M(\sigma)$. Thus T has the property (C) if and only if $T = \{e\}$ or equivalently if and only if $\hat{T} = \{0\}$.

(3) If $G = S$ is semisimple, let S_c denote a maximal compact subgroup of the complex Lie group S. By Hopf, we have

$$\sum_{\nu=0}^{d} b_\nu t^\nu = \prod_{i=1}^{l} (1 + t^{2a_i - 1})$$

where b_ν (resp. l) is the Betti number (resp. rank) of S_c. From Chevalley and Steinberg's result we see that

$$q^N \prod_{i=1}^{l} (q^{a_i} - 1) \leqq [S^{(\mathfrak{p})}_{k(\mathfrak{p})}] \leqq q^N \prod_{i=1}^{l} (q^{a_i} + 1)$$

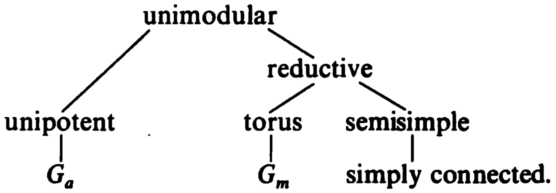
(N = the number of positive roots of S) and so

$$\prod_{i=1}^{l} (1 - q^{-a_i}) \leqq v_{\mathfrak{p}}(S) \leqq \prod_{i=1}^{l} (1 + q^{-a_i}).$$

Since $b_1 = b_2 = 0$, we have $a_i \geqq 2$ for all i, hence the property (C) holds and no convergence factors are necessary for semisimple groups.

The above argument shows that a connected algebraic group G has the property (C) if and only if $G = U \cdot S$ or equivalently if and only if $\hat{G} = \{0\}$.

2. **Definition of $\tau(G)$ for unimodular groups.** A connected algebraic group G is called unimodular if the form ω in §1 is also right invariant. We have the following chains of containment:



Hence, in defining $\tau(G)$ for a unimodular group G defined over k, it would be quite natural to require that $\tau(G) = 1$ if G is G_a, G_m or simply connected: it turns out that $\tau(G_a) = 1$ is essentially equivalent to the definition of Δ_k, the discriminant of k, and $\tau(G_m) = 1$ is equivalent to the well-known class number relation hg $= \mathrm{Res}_{s=1}\zeta_k(s)$ for k. On the other hand,

$$\tau \text{ (simply connected)} = 1$$

is the Weil's conjecture which is known to be true for a large part of classical groups (Weil, Tamagawa), for some exceptional groups (Demazure, Mars) and for Chevalley groups (Langlands), but is not yet completely solved.

We now define $\tau(G)$. Let G_A be the adele group. Put $G_A^1 = \{x \in G_A, \|\xi_A(x)\| = 1$ for all $\xi \in (\hat{G})_k\}$. Then G_A/G_A^1 is isomorphic to the vector group $\boldsymbol{R}^r$, $r = \text{rank }(\hat{G})_k$. As a measure on G_A/G_A^1 we take the usual measure of $\boldsymbol{R}^r$, which we denote by $d(G_A/G_A^1)$. Since G_k is discrete in G_A, we define dG_k to be the canonical discrete measure. We could then define the Tamagawa number, $\tau(G)$, as the measure one has to give to the measure finite space G_A^1/G_k in order that

$$dG_A = d(G_A/G_A^1)\, d(G_A^1/G_k)\, dG_k,$$

where dG_A is some canonical measure on G_A to be determined. Motivated by the classical class number relation for the case G_m mentioned above, we shall define dG_A as follows. We take a finite Galois extension K/k so that $\hat{G} = (\hat{G})_K$. As in the case of tori, $\hat{G}$ becomes a $\boldsymbol{Z}$-free $\mathfrak{G}(K/k)$-module and we denote by χ_G the character of the corresponding integral representation of $\mathfrak{G}(K/k)$. It is to be noticed that $\chi_G = \chi_T$ when $G = U \cdot T \cdot S$ in the sense of §1, because $\hat{G} \otimes_{\boldsymbol{Z}} \boldsymbol{Q} \cong \hat{T} \otimes_{\boldsymbol{Z}} \boldsymbol{Q}$ as representation spaces of $\mathfrak{G}(K/k)$. As a measure on G_A, we take

$$dG_A = \rho_G^{-1} |\Delta_k|^{-\dim G/2} \prod_{v/\infty} \omega_v \prod_{\mathfrak{p}} L_{\mathfrak{p}}(1, \chi_G)\omega_{\mathfrak{p}}$$

where $\rho_G = \lim_{s \to 1}(s-1)^r L(s, \chi_G)$. (Notice that $L(s, \chi_G)$ has a pole of order r at $s = 1$ where $r = \text{rank }(\hat{G})_k = $ multiplicity of the trivial character in χ_G.) Since $L_{\mathfrak{p}}(1, \chi_G)v_{\mathfrak{p}}(G) = L_{\mathfrak{p}}(1, \chi_T)v_{\mathfrak{p}}(T)v_{\mathfrak{p}}(S)v_{\mathfrak{p}}(U) = v_{\mathfrak{p}}(S)$ for almost all $\mathfrak{p}$, we see from §1 that dG_A is well defined. Furthermore, it is not difficult to show that dG_A is intrinsic, i.e., it is independent of the choice of K/k and ω. Thus, the definition

$$\tau(G) = \tau_k(G) = \int_{G_A^1/G_k} d(G_A^1/G_k)$$

is settled. One verifies easily the following functorial properties:

(i) $\tau(G \times G') = \tau(G)\tau(G')$,

(ii) if G is defined over a finite extension K of k, then

$$\tau_K(G) = \tau_k(R_{K/k}(G)).$$

3. **Tamagawa number of tori.** Let $\mathfrak{G}(k)$ be the full Galois group of $\bar{k}/k$, $\bar{k}$ being the algebraic closure of k. Denote by $\mathscr{C}(k)$ the category of tori defined over k and by $\hat{\mathscr{C}}(k)$ the category of finitely generated $\boldsymbol{Z}$-free continuous $\mathfrak{G}(k)$-modules. For a finite Galois extension K of k, let $\mathscr{C}(K/k)$ denote the subcategory of $\mathscr{C}(k)$ consisting of all $T \in \mathscr{C}(k)$ such that T splits over K, and $\hat{\mathscr{C}}(K/k)$ denote the category of finitely generated $\boldsymbol{Z}$-free $\mathfrak{G}(K/k)$-modules. Then $\mathscr{C}(k)$ (resp. $\hat{\mathscr{C}}(k)$) is the union of $\mathscr{C}(K/k)$ (resp. $\hat{\mathscr{C}}(K/k)$) where K runs over all finite Galois subextensions of $\bar{k}/k$. It is fundamental that $\mathscr{C}(k)$ and $\hat{\mathscr{C}}(k)$ are mutually dual under the correspondence $T \to \hat{T}$. For $T, T' \in \mathscr{C}(K/k)$,

$$T \underset{k}{\cong} T' \Leftrightarrow \hat{T} \cong \hat{T}' \quad \text{as} \quad \mathfrak{G}(K/k)\text{-modules.}$$

Furthermore,

$$T \rightleftarrows T' \ (k\text{-isogenous}) \Leftrightarrow \hat{T} \otimes_Z Q \cong \hat{T}' \otimes_Z Q \Leftrightarrow \chi_T = \chi_{T'}.$$

Let K/k be a (not necessarily Galois) finite extension and L/K be a finite extension such that L/k is Galois. We can then define the functor $\hat{R}_{K/k}: \hat{\mathscr{C}}(L/K) \to \hat{\mathscr{C}}(L/k)$ by requiring that the following diagram be commutative:

$$\begin{tikzcd}
\mathscr{C}(L/K) \arrow[r, "R_{K/k}"] \arrow[d] & \mathscr{C}(L/k) \arrow[d] \\
\hat{\mathscr{C}}(L/K) \arrow[r, "\hat{R}_{K/k}"] & \hat{\mathscr{C}}(L/k).
\end{tikzcd}$$

In view of the universal mapping property of the functor $R_{K/k}$, one can verify that $\hat{R}_{K/k}(M) = Z[\mathfrak{G}(L/k)] \otimes_{Z[\mathfrak{G}(L/K)]} M$ for $M \in \hat{\mathscr{C}}(L/K)$, i.e., the representation of $\mathfrak{G}(L/k)$ by $\hat{R}_{K/k}(M)$ is "induced" by the representation of the subgroup $\mathfrak{G}(L/K)$ by M. As an application, we can get a structure theorem on tori: namely, take a $T \in \mathscr{C}(K/k)$, K/k being Galois this time. Since χ_T is rational in the sense of finite groups, we have, by Artin, $\chi_T = \sum_\nu q_\nu \chi_{1,\nu}^*$, $q_\nu \in Q$, where $\chi_{1,\nu}^*$ is the induced character of the trivial character $\chi_{1,\nu}$ of a cyclic subgroup of $\mathfrak{G}(K/k)$. Rewrite the relation as

$$m\chi_T + \sum_\lambda m_\lambda \chi_{1,\lambda}^* = \sum_\mu m_\mu \chi_{1,\mu}^*$$

with positive integers m, m_λ, m_μ and translate in the language of tori. Then we get

$$(*)\ T^m \times \prod_\lambda (R_{K_\lambda/k} G_m)^{m_\lambda} \rightleftarrows \prod_\mu (R_{K_\mu/k} G_m)^{m_\mu} \ (k\text{-isogenous}),$$

this will be used in the following Φ-lemma.

Denote by $L_+(\mathscr{C}(k))$ the set of all positive real valued functions on $\mathscr{C}(k)$ and by Φ the set of all assignments $\phi: k \to \phi_k \in L_+(\mathscr{C}(k))$ with the following properties (Φ1), (Φ2), (Φ3):

$$(\Phi 1) \qquad \phi_k(T \times T') = \phi_k(T)\phi_k(T'),$$

$$(\Phi 2) \qquad \phi_K = \phi_k \circ R_{K/k}$$

$$(\Phi 3) \qquad \phi_k(T) = 1 \text{ when } T \in \mathscr{C}(K/k) \text{ and } \hat{T} \text{ is } \mathfrak{G}(K/k)\text{-projective.}$$

It is easily checked that Φ forms a group with the multiplication defined by $(\phi\psi)_k(T) = \phi_k(T)\psi_k(T)$ for $T \in \mathscr{C}(k)$. For a short exact sequence (E) over k of tori in $\mathscr{C}(k)$

$$(E): 0 \to T' \to T \to T'' \to 0$$

we define a function $\phi_k(E)(\phi \in \Phi)$ by the alternating product

$$\phi_k(E) = \frac{\phi_k(T')\phi_k(T'')}{\phi_k(T)}.$$

Φ-LEMMA. *If $\phi \in \Phi$ is such that for any k and for any short exact sequence (E) of $\mathscr{C}(k)$ we have $\phi_k(E) = 1$, then $\phi = 1$.*

Since this lemma is crucial in the formal aspect of our theory, we reproduce here the proof in [**2**] suggested by Tate. Take any finite Galois extension K/k and call G the Grothendieck group of $\mathscr{C}(K/k)$. By definition, the additive group G is generated by the symbol $[T]$ together with the relation $[T] = [T'] + [T'']$ whenever $0 \to T' \to T \to T'' \to 0$ (exact). By the assumption on ϕ, $\bar{\phi}[T] = \phi_k(T)$ defines a homomorphism of G into $\boldsymbol{R}_+$, the multiplicative group of positive reals. Now, by the duality, G can be viewed as the Grothendieck group of $\hat{\mathscr{C}}(K/k)$, i.e., such a group for $\boldsymbol{Z}$-representations of $\mathfrak{G}(K/k)$. Denote by $G^{\boldsymbol{Q}}$ the Grothendieck group of $\boldsymbol{Q}$-representations of $\mathfrak{G}(K/k)$ and by θ the homomorphism $G \to G^{\boldsymbol{Q}}$ given by $\theta[M] = [M \otimes_{\boldsymbol{Z}} \boldsymbol{Q}]$. Since $\boldsymbol{R}_+$ is torsion free and $\operatorname{Ker}\theta$ is finite by Swan, $\phi|\operatorname{Ker}\theta = 1$. This implies that if $T, T' \in \mathscr{C}(K/k)$ are k-isogenous, then

$$\hat{T} \otimes_{\boldsymbol{Z}} \boldsymbol{Q} \cong \hat{T}' \otimes_{\boldsymbol{Z}} \boldsymbol{Q}$$

and hence $[T] - [T'] \in \operatorname{Ker}\theta$, and consequently $\phi_k(T) = \phi_k(T')$. Applying this argument to the structure Theorem (*) for $T \in \mathscr{C}(K/k)$ and using ($\Phi 1$), ($\Phi 2$), ($\Phi 3$), we get $\phi_k(T) = 1$ for any k and any $T \in \mathscr{C}(k)$, i.e., $\phi = 1 \in \Phi$, q.e.d.

Examples of elements in Φ. First of all, $\tau \in \Phi$ (of course!). Also, the following two elements, h and i, come immediately to our mind:

$$h_k(T) = [H^1(k, \hat{T})],$$

$$i_k(T) = [\operatorname{Ker}(H^1(k, T) \to \prod_v H^1(k_v, T))].$$

An interesting fact is that those three elements τ, h and i are dependent in the torsion free group Φ: more precisely, we have

THEOREM. $\tau i h^{-1} = 1$.

SKETCH OF PROOF. In view of Φ-lemma, it is enough to show that

$$\tau_k(E) = \frac{h_k(E)}{i_k(E)}$$

for any short exact sequence

$$(E): \qquad 0 \to T' \xrightarrow{\iota} T \xrightarrow{\kappa} T'' \to 0$$

with T', T, $T'' \in C(K/k)$. Passing to the cohomology of the dual of (E), we get an exact sequence

$$(**) \qquad 0 \to \operatorname{Cok}(\hat{\iota})_k \to H^1(\hat{T}'') \xrightarrow{\xi} H^1(\hat{T}) \xrightarrow{\eta} H^1(\hat{T}') \to .$$

On the other hand, (E) induces a natural homomorphism

$$\mu: \kappa(T_{A_k})/\kappa(T_k) \to T''_{A_k}/T''_k.$$

Then,

$$\operatorname{Ind}\mu = \frac{[\operatorname{Cok}\mu]}{[\operatorname{Ker}\mu]} = \frac{[T''_{A_k} : \kappa(T_{A_k})T''_k]}{[\kappa(T_{A_k}) \cap T''_k : \kappa(T_k)]}.$$

By a Fubini type argument, we can show that

$$(***) \qquad \tau_k(E) = [\operatorname{Cok}(\hat{\imath})_k] \cdot \operatorname{Ind}\mu.$$

By chasing diagrams, we get

$$(****) \qquad \operatorname{Ind}\mu = \frac{[\operatorname{Ker}\zeta]}{i_k(E)},$$

where ζ is the homomorphism $H^1(T'_{A_K}/T'_K) \to H^1(T_{A_K}/T_K)$ induced by (E). From (**), (***), (****), there remains to prove that

$$(*****) \qquad [\operatorname{Ker}\xi][\operatorname{Ker}\zeta] = h_k(E).$$

For this purpose, the Nakayama-Tate duality is useful. It says that the pairing

$$H^{2-r}(\hat{T}) \times H^r(T_{A_K}/T_K) \to H^2(I_K/K^*)$$

induced by the natural pairing

$$\hat{T} \times T_{A_K}/T_K \to I_K/K^* \qquad \text{(idele class group of } K)$$

is dual. Applying this ($r = 1$) to the following situation:

$$\begin{tikzcd}
H^1(\hat{T}) \arrow[d, "\eta"'] & \times & H^1(T_{A_K}/T_K) \arrow[r] & H^2(I_K/K^*) \\
H^1(\hat{T}') \arrow[d] & \times & H^1(T'_{A_K}/T'_K) \arrow[r] \arrow[u, "\zeta"'] & H^2(I_K/K^*), \\
\operatorname{Cok}\eta & & \operatorname{Ker}\zeta \arrow[u] &
\end{tikzcd}$$

we get $\operatorname{Cok}\eta \cong \operatorname{Ker}\zeta$, and so

$$[\operatorname{Ker}\xi][\operatorname{Ker}\zeta] = [\operatorname{Ker}\xi][\operatorname{Cok}\eta] = \frac{\operatorname{Ind}\eta}{\operatorname{Ind}\xi}[\operatorname{Cok}\xi][\operatorname{Ker}\eta]$$

$$= \frac{h_k(T')}{h_k(T)}\,\frac{h_k(T'')}{h_k(T)}\,\frac{h_k(T)}{[\operatorname{Im}\xi]}[\operatorname{Ker}\eta] = h_k(E),$$

which proves (*****), q.e.d.

Remark. Since (***) is a basis for the characterization of τ, we see that as far as the tori are concerned, the Tamagawa number (as an element in Φ) is the *unique* solution ($\tau = h/i$) of the following axioms:

(Φ1′) For any short exact sequence (E) in $\mathscr{C}(k)$, we have

$$\tau_k(E) = [\mathrm{Cok}(\hat{\iota})_k] \cdot \mathrm{Ind}\, \mu$$

(Φ2) $\tau_K = \tau_k \circ R_{K/k}$

(Φ3) (normalization) $\tau_k(T) = 1$ when $T \in \mathscr{C}(K/k)$ and $\hat{T}$ is $\mathfrak{G}(K/k)$-projective.

REMARK. If $T \in \mathscr{C}(K/k)$ and K/k is cyclic, we can show that $i_k(T) = 1$, i.e., $\tau_k(T) = h_k(T)$. To a cyclic extension K/k, $n = [K:k]$, one can attach the exact sequence

$$0 \to \mathrm{Ker}\, N \to R_{K/k}G_m \xrightarrow{N = \mathrm{norm}} G_m \to 0.$$

One sees easily that $\tau_k(\mathrm{Ker}\, N) = n$. If K/k is quadratic ($n = 2$), Ker N is a special orthogonal group of the binary form belonging to K/k and thus we obtain a special case of Siegel's theorem on quadratic forms. For noncyclic K/k, the group Ker N still makes sense. E.g., take $k = \mathbf{Q}$ and $K = \mathbf{Q}(\sqrt{5}, \sqrt{29}, \sqrt{109}, \sqrt{281})$. Then,

$$\tau_{\mathbf{Q}}(\mathrm{Ker}\, N) = \frac{1}{2^{\sigma - \kappa}}$$

with $0 \leqq \kappa \leqq 4$, which is not an integer. This is due to the nonvalidity of the Hasse norm theorem for $K/\mathbf{Q}$.

4. **Determination of τ (semisimple) mod. Weil's conjecture.** Let G be a connected semisimple algebraic group defined over a number field k. Let $(\tilde{G}, f)$ be the universal covering group of G defined over k. Since $(\tilde{G}, f)$ is unique up to isomorphisms over k, the fundamental group $F = \mathrm{Ker} f$, which is a central finite algebraic subgroup of $\tilde{G}$ defined over k, is invariantly attached to G. Hence, it is natural to expect that the relative Tamagawa number $\tau(G)/\tau(\tilde{G})$ can be described in terms of invariants of F as a $\mathfrak{G}(k)$ ($= \mathfrak{G}(\bar{k}/k)$)-module.

EXAMPLES. (1) If $G = O^+(f)$, f being a quadratic form over k ($n \geqq 3$, n: the number of variables), then $\tilde{G} = \mathrm{Spin}(f)$. The fact that $\tau(O^+(f)) = 2$ (Siegel's theorem) and $\tau(\mathrm{Spin}(f)) = 1$ was the Tamagawa's discovery at the beginning of the theory of the Tamagawa numbers and motivated the Weil's Princeton lecture (1959–60) and others. Anyway, we have $\tau(G)/\tau(\tilde{G}) = 2 =$ the degree of the covering.

(2) If $G = \mathrm{PSL}(n)$, then $\tilde{G} = \mathrm{SL}(n)$. We have $\tau(\tilde{G}) = 1$ (Minkowski–Siegel) and $\tau(G) = n$ (Tamagawa-Weil) and so again $\tau(G)/\tau(\tilde{G}) = n = [F] =$ the degree of the covering.

(3) If $G = \mathrm{PSU}(n, K/k)$ (projective special unitary group relative to a quadratic extension K/k), then $\tilde{G} = \mathrm{SU}(n, K/k)$. We know that $\tau(\tilde{G}) = 1$ (Weil). This time, we have

$$\tau(G)/\tau(\tilde{G}) = \tau(G) = \begin{cases} 1 & n\colon \text{odd} \\ 2 & n\colon \text{even,} \end{cases}$$

and so the relative number is not equal to the degree ($= n$) of the covering. This example also shows that the fact $\tau(G) = 1$ is not characteristic for the simply connected groups.

Our formula in the Main Theorem will explain all those phenomena.

Coming back to our general situation, let $\hat{F} = \mathrm{Hom}(F, G_m) = \mathrm{Hom}(F, (\bar{k})^*)$. Then $\hat{F}$ is again a $\mathfrak{G}(k)$-module. Put

$$\mathfrak{h}_{\hat{F}} = \{\sigma \in \mathfrak{G}(k), \xi^\sigma = \xi \text{ for all } \xi \in \hat{F}\}.$$

Since $\mathfrak{h}_{\hat{F}}$ is an open normal subgroup of $\mathfrak{G}(k)$, the corresponding field $K_{\hat{F}}/k$ is a finite Galois extension. $\hat{F}$ is then a $\mathfrak{G}(K_{\hat{F}}/k)$-module. Let Γ be the group ring of $\mathfrak{G}(K_{\hat{F}}/k)$ over $\boldsymbol{Z}$. For a suitable natural number m, we have the exact sequence

$$0 \leftarrow \hat{F} \leftarrow m \cdot \Gamma \leftarrow M \leftarrow 0,$$

where $M \in \hat{C}(K_{\hat{F}}/k)$. Dualizing, we get the exact sequence over k:

$$0 \to F \to T' \to T \to 0,$$

where $T' = (R_{K_{\hat{F}}/k} G_m)^m$ and $\hat{T} = M$ with $T, T' \in \mathscr{C}(K_{\hat{F}}/k)$. Since $\hat{T}' = m\Gamma$ is $\mathfrak{G}(K_{\hat{F}}/k)$-free we have $\tau(T') = 1$ by (Φ3). This cohomological triviality of T' is crucial in the following arguments. If we imbed F into $\tilde{G} \times T'$ by the diagonal mapping and put $G^* = (\tilde{G} \times T')/F$, this being a connected reductive group, we get the commutative diagram

$$\begin{tikzcd}
 & & (V) & & \\
0 \arrow[dr] & & 0 \arrow[d] & & \\
 & F \arrow[r] \arrow[d] & T' \arrow[d, "\iota"'] \arrow[dr, "\lambda"] & & \\
(H)\,0 \arrow[r] & \tilde{G} \arrow[r] \arrow[dr, "f"'] & G^* \arrow[r, "\kappa"] \arrow[d] & T \arrow[r] & 0 \\
 & & G \arrow[d] & & \\
 & & 0 & &
\end{tikzcd}$$

where (H) (resp. (V)) denotes the horizontal (resp. vertical) short exact sequence, and everything is defined over k.

Let

$$\tau(V) = \frac{\tau(T')\tau(G)}{\tau(G^*)}$$

and

$$\tau(H) = \frac{\tau(G)\tau(T)}{\tau(G^*)}.$$

We have then

$$(\#) \qquad \frac{\tau(G)}{\tau(\tilde{G})} = \frac{\tau(T)\tau(V)}{\tau(T')\tau(H)} = \tau(T)\frac{\tau(V)}{\tau(H)}$$

since $\tau(T') = 1$. Consider now $\tau(V)$. Since $\hat{T}'$ is $\mathfrak{G}(K_{\mathfrak{f}}/k)$-free, (V) admits a rational section $(G \to G^*)$ over k. From this and the fact that $\tau(T') = 1$ it follows that

$$(\#\,\#) \qquad \tau(V) = [\mathrm{Cok}(\hat{\iota})_k]$$

by a Fubini type argument. Next, consider $\tau(H)$. The sequence (H) induces naturally a homomorphism $\mu\colon T_k/\kappa(G_k^*) \to T_A/\kappa(G_A^*)$. Again by a Fubini type argument we get

$$\tau(H) = \mathrm{Ind}\,\mu = \frac{[\mathrm{Cok}\,\mu]}{[\mathrm{Ker}\,\mu]} = \frac{[T_A : \kappa(G_A^*)T_k]}{[\kappa(G_A^*) \cap T_k : \kappa(G_k^*)]}.$$

We now claim that $[\mathrm{Ker}\,\mu] = [\mathrm{Cok}\,\mu] = 1$ by the simply connectedness of $\tilde{G}$. The following two facts are fundamental:

(K_1) $H^1(k_{\mathfrak{p}}, \tilde{G}) = 0$ ($\mathfrak{p} \neq \infty$) (Kneser).

(K_2) The Hasse map $H^1(k, \tilde{G}) \to \prod_v H^1(k_v, \tilde{G})$ is injective (Kneser and Harder).

(After my talk, I learned from Kneser that the proof of (K_2) for groups of type E_8 is not yet completed. However, as far as the relative theory is concerned, we do not have to worry about E_8 because the group of this type has no proper covering and hence the factor of type E_8 in general semisimple group G has no contribution to the relative Tamagawa number $\tau(G)/\tau(\tilde{G})$.) Now take any $t \in \kappa(G_A^*) \cap T_k$. Then $\kappa^{-1}(t)$ is a principal homogeneous space for $\tilde{G}$ over k which has a rational point over k_v for every v. Thus, by (K_2), $\kappa^{-1}(t)$ contains a $g^* \in G_k^*$, i.e., $t = \kappa(g^*) \in \kappa(G_k^*)$, which proves that $[\mathrm{Ker}\,\mu] = 1$. Next, we consider $\mathrm{Cok}\,\mu$. Denote by T_∞^0 the topological identity component of $T_\infty = \prod_{v|\infty} T_{k_v}$. It is known that $T_\infty = T_\infty^0 \cdot T_k$ (Serre and Tate). Hence, to show that $[\mathrm{Cok}\,\mu] = 1$, it is enough to see that $T_A^0 \subset \kappa(G_A^*)$ where $T_A^0 = T_\infty^0 \times \prod'_{\mathfrak{p} \neq \infty} T_{k_{\mathfrak{p}}}$. Now, the map $\kappa_A\colon G_A^* \to T_A$ is open since $\mathrm{Ker}\,\kappa = \tilde{G}$ is connected, and so $\kappa(G_{\mathfrak{o}_{\mathfrak{p}}}^*) = T_{\mathfrak{o}_{\mathfrak{p}}}$ for almost all $\mathfrak{p}$. Let S be the finitc set of finite places $\mathfrak{p}$ for which $\kappa(G_{\mathfrak{o}_{\mathfrak{p}}}^*) \not\supseteq T_{\mathfrak{o}_{\mathfrak{p}}}$. Take an adele $t = (t_v) \in T_A^0$. For $\mathfrak{p} \notin S$, we have $t_{\mathfrak{p}} = \kappa(g_{\mathfrak{p}}^*)$ with $g_{\mathfrak{p}}^* \in G_{\mathfrak{o}_{\mathfrak{p}}}^*$. For $\mathfrak{p} \in S$, we can find a $g_{\mathfrak{p}}^* \in G_{k_{\mathfrak{p}}}^*$ such that $t_{\mathfrak{p}} = \kappa(g_{\mathfrak{p}}^*)$ since the principal homogeneous space $\kappa^{-1}(t_{\mathfrak{p}})$ for $\tilde{G}$ over $k_{\mathfrak{p}}$ has a rational point in $G_{k_{\mathfrak{p}}}^*$ by (K_1). For $v|\infty$, we again have $t_v = \kappa(g_v^*)$ because T_∞^0 is connected. Thus $t = \kappa(g_A^*)$ with $g_A^* = (g_v^*) \in G_A^*$, which proves that $[\mathrm{Cok}\,\mu] = 1$. Hence,

$$(\#\,\#\,\#) \qquad \tau(H) = 1$$

From $(\#)$, $(\#\,\#)$, $(\#\,\#\,\#)$ and Theorem in §3 we get

$$(\#\,\#\,\#\,\#) \qquad \frac{\tau(G)}{\tau(\tilde{G})} = \frac{h(T)}{i(T)}[\mathrm{Cok}(\hat{\iota})_k]$$

where $h(T) = [H^1(k, \hat{T})]$, $i(T) = [\mathrm{Ker}(H^1(k, T) \to \prod_v H^1(k_v, T))]$. We can simplify $(\#\,\#\,\#\,\#)$ a little by noticing that since

$$0 \to \hat{T} \xrightarrow{\hat{\iota}} \hat{T}' \to \hat{F} \to 0$$

is exact we have the exact sequence

$$0 \to (\hat{T})_k \xrightarrow{(\hat{\lambda})k} (\hat{T}')_k \to (\hat{F})_k \to H^1(\hat{T}) \to H^1(\hat{T}') = 0$$

relative to $\mathfrak{G}(K_{\hat{F}}/k)$ and therefore

$$[\mathrm{Cok}(\hat{\lambda})_k]h(T) = [(\hat{F})_k] \overset{\mathrm{def}}{=} h^0(\hat{F}).$$

But since $\tilde{G}$ is semisimple, it is easily checked that $[\mathrm{Cok}(\hat{\lambda})_k] = [\mathrm{Cok}(\hat{\iota})_k]$ and hence

$$(\#\#\#\#\#) \qquad \frac{\tau(G)}{\tau(\tilde{G})} = \frac{h^0(\hat{F})}{i(T)}.$$

Finally, by Hasse-Brauer-Noether theorem we get

$$i(T) = i^2(F) = \left[\mathrm{Ker}(H^2(k, F) \to \prod_v H^2(k_v, F))\right]$$

and

$$i^2(F) = i^1(\hat{F}) = \left[\mathrm{Ker}(H^1(k, \hat{F}) \to \prod_v H^1(k_v, \hat{F}))\right]$$

by Tate duality. From $(\#\#\#\#\#)$ we get our

MAIN THEOREM.

$$\frac{\tau(G)}{\tau(\tilde{G})} = \frac{h^0(\hat{F})}{i^1(\hat{F})}.$$

COROLLARY 1. *If $K_{\hat{F}}/k$ is cyclic, then $\tau(G)/\tau(\tilde{G}) = h^0(\hat{F})$.*

COROLLARY 2. *If G is of Chevalley type over k, then $\tau(G)/\tau(\tilde{G}) = [F]$.*

In fact, F is contained in any k-trivial maximal torus of $\tilde{G}$. So the action of $\mathfrak{G}(k)$ on F is the same as the action of $\mathfrak{G}(k)$ on the roots of unity. Then, clearly $\hat{F}$ is $\mathfrak{G}(k)$-trivial and hence $K_{\hat{F}} = k$. Thus we get $i^1(\hat{F}) = i(T) = 1$ and $h^0(\hat{F}) = [\hat{F}] = [F]$, q.e.d. Corollary 2 explains Example (2) since $G = \mathrm{PSL}(n)$ is of Chevalley type.

COROLLARY 3. *If $[F] = 2$, then $\tau(G)/\tau(\tilde{G}) = 2$.*

In fact, evidently $\hat{F}$ is $\mathfrak{G}(k)$-trivial. Corollary 3 explains Example (1) since Spin (f) is the double covering of $O^+(f)$.

Absolutely simple groups. Let G be absolutely simple. For this case we can check, case by case, that $i^1(\hat{F}) = 1$. Thus, $\tau(G)/\tau(\tilde{G}) = h^0(\hat{F})$. We shall of course be interested in the case where the action of $\mathfrak{G}(k)$ on $\hat{F}$ is not trivial, i.e., $\hat{F}^{\mathfrak{G}(k)} \subsetneq \hat{F}$, or equivalently $K_{\hat{F}} \supsetneq k$. Actually, such a case can happen only for groups of type A_l $(l \geq 2)$, the adjoint group of type D_l $(l \geq 4)$ and the adjoint group of type E_6. We get the following table:

Type	$[K_{\hat{F}}:k]$	$[F]$	$\tau(G)/\tau(\tilde{G}) = h^0(\hat{F})$
$A_l\,(l \geqq 2)$	2	a factor of $l+1$	1 l = even 2 l = odd
D_4	2 3, 6	4	2 1
$D_l\,(l \geqq 5)$	2	4	2
E_6	2	3	1

The group $G = \mathrm{PSU}(n, K/k)$ $(n \geqq 3)$ in Example (1) belongs to A_l with $l = n - 1$.

REMARK. It is desirable to extend the definition of $\tau(G)$ to arbitrary (nonconnected, nonunimodular) group G. In particular, how should one define $\tau(G)$ for a finite group G over k? Though I do not know the correct definition, the quantity $h^0(G)/i^1(G)$ in the main theorem will suggest something at least for G finite commutative.

REFERENCES

1. T. Ono, *Arithmetic of algebraic tori*, Ann. of Math. **74** (1961), 101–139.
2. ———, *On the Tamagawa number of algebraic tori*, Ann. of Math. **78** (1963), 47–73.
3. ———, *On the relative theory of Tamagawa numbers*, Ann. of Math. **82** (1965), 88–111.
4. A. Weil, *Adèles and algebraic groups*, Institute for Advanced Study, Princeton, N.J., 1961.
5. T. Tamagawa, *Adèles*, Proc. Sympos. Pure Math., vol. 9, Amer. Math. Soc., Providence, R.I., 1966, pp. 113–121.

The Siegel Formula for Orthogonal Groups. I

BY

J. G. M. MARS

1. Let k be an algebraic numberfield, Q a nondegenerate quadratic form on a vector space X_k over k, $\dim_k X_k = m \geqq 5$. X will denote the algebraic variety defined over k such that $X_K = K \otimes_k X_k$ for any extension K of k; the extension of Q to X will be denoted by Q. Let $G = \mathrm{SO}(Q)$ be the special orthogonal group of Q. So G is a semisimple algebraic group defined over k.

As a consequence of Witt's theorem, two points $x, y \in X_K$, $\neq 0$, belong to a same orbit of G_K if and only if $Q(x) = Q(y)$. Hence the orbits of G in X which contain points of X_k are the sets $U(i) = \{x \in X | Q(x) = i, x \neq 0\}$ ($i \in k$ such that $U(i)_k$ is not empty) and $\{0\}$. If $i \in k$ and $\xi_i \in U(i)_k$, the isotropy group of ξ_i in G is an algebraic group H_i defined over k and the mapping $g \to g(\xi_i)$ induces an isomorphism of G/H_i onto $U(i)$. Using Witt's theorem we see that $G_K/H_{i,K} = U(i)_K$ for any extension K of k; moreover, $G_A/H_{i,A} = U(i)_A$ (with topology); here G_A is the adelic group attached to G etc., and the identifications are obtained from the mapping $g \to g(\xi_i)$.

Let dg, dh_i be invariant gaugeforms on G, H_i (gaugeform = differential form of maximal degree defined over k without zeros or poles); then $\mathfrak{D}_i = dg/dh_i$ is defined and is an invariant gaugeform on $G/H_i = U(i)$. Let $|dg|_A, |dh_i|_A, |\mathfrak{D}_i|_A$ be the Tamagawa measures derived from $dg, dh_i, \mathfrak{D}_i$ and the convergence factors 1. Then $|dg|_A = |\mathfrak{D}_i|_A |dh_i|_A$. Now we have

$$\int_{G_A/H_A} |\mathfrak{D}_i|_A \int_{H_A/H_k} F(gh)|dh|_A = \int_{G_A/G_k} |dg|_A \sum_{G_k/H_k} F(g\gamma)$$

for $F \in L^1(G_A/H_k), H = H_i$.

Taking $\Phi(g(\xi_i))$ instead of $F(g)$, with appropriate function Φ on X_A, we get

$$\tau(H_i) \int_{U(i)_A} \Phi|\mathfrak{D}_i|_A = \int_{G_A/G_k} |dg|_A \sum_{\xi \in U(i)_k} \Phi(g(\xi)), \tag{1}$$

where $\tau(H_i)$ is the Tamagawa number of H_i. Now H_i is either the special orthogonal group of a nondegenerate quadratic form in m-1 variables or an extension by a unipotent group of the special orthogonal group of a nondegenerate quadratic form in m-2 variables. Assuming that the Tamagawa number of any special orthogonal group in m-1 or m-2 variables is 2 we are going to prove that the Tamagawa number of G is 2. Then the Tamagawa number of any special orthogonal group is 2, provided we know that this is so in dimension 3 and 4.

The latter is proved by Weil in [1] using the classical isomorphisms for the groups in question and zeta-functions.

It follows from the Hasse principle for quadratic forms ($U(i)_k$ empty $\Rightarrow$ $U(i)_A$ empty) that formula (1) is valid for *all* $i \in k$. Summation over $i \in k$ then gives (modulo convergence):

$$(2)\qquad I(\Phi) = \int_{G_A/G_k} \sum_{\xi \in X_k} \Phi(g(\xi))|dg|_A = 2\sum_{i \in k} \int_{U(i)_A} \Phi|\mathfrak{D}_i|_A + \tau(G)\Phi(0).$$

It is clear that $I(\Phi) = I(\hat{\Phi})$, if $\hat{\Phi}$ is defined by

$$\hat{\Phi}(y) = \int_{X_A} \Phi(x)\chi([x, y])|dx|_A,$$

where $[x, y] = Q(x + y) - Q(x) - Q(y)$ and χ is a character of A such that the bicharacter $\chi(xy)$ defines an isomorphism between A and its dual group such that the discrete subgroup k of A corresponds to itself by duality. We define χ_v by $\chi(x) = \prod \chi_v(x_v)$ if $x = (x_v) \in A$. If Φ is of Schwartz–Bruhat type it will follow from considerations below that the sum over $i \in k$ in (2) converges absolutely; we also know that $\tau(G)$ is finite, so $I(\Phi)$ is defined for Φ of Schwartz–Bruhat type. We recall that if Φ is of Schwartz–Bruhat type, so is $\hat{\Phi}$.

2. Applying Proposition 1 of [2] to the map $Q\colon X_{k_v} = X_v \rightarrow k_v$ we find the following. There exists a uniquely determined family of positive measures $(\mu_i)_{i \in k_v}$ on X_v such that

(a) support $\mu_i \subset \{x \in X_v | Q(x) = i\}$,

(b) for any continuous function Φ with compact support on X_v the function F_Φ on k_v defined by $F_\Phi(i) = \int \Phi\, d\mu_i$ is continuous and satisfies $\int F_\Phi |di|_v = \int \Phi |dx|_v$. Moreover, for any Φ of Schwartz–Bruhat type F_Φ (defined as above) is continuous, integrable over k_v, satisfies $\int F_\Phi |di|_v = \int \Phi |dx|_v$ and has as Fourier transform the function $\hat{F}_\Phi$ defined by

$$\hat{F}_\Phi(i) = \int_{X_v} \Phi(x)\chi_v(iQ(x))|dx|_v \qquad (i \in k_v).$$

LEMMA 1. *The measures μ_i are carried by the sets*

$$U_v(i) = \{x \in X_v | Q(x) = i, x \neq 0\}.$$

PROOF. For $i \neq 0$ there is nothing to prove. μ_0 is the sum of a measure carried by $U_v(0)$ and a measure with support $\{0\}$, but the latter must be 0 since

$$\mu_0(tx) = |t|^{m-2}\mu_0(x) \qquad (t \in k_v^*).$$

Since the mapping Q from X onto the affine line is everywhere submersive except in 0, we may consider on each $U(i)$ the gaugeform $\mathfrak{D}_i$ defined by

$$(3)\qquad \mathfrak{D}_i(x) = \left(\frac{dx}{dQ(x)}\right)_i.$$

$\mathfrak{D}_i$ is invariant under G, so it differs from the form $\mathfrak{D}_i$ introduced above (viz. as quotient dg/dh_i) by a factor $\in k^*$ ($|\mathfrak{D}_i|_A$ is of course not changed when $\mathfrak{D}_i$ is replaced by $\rho\mathfrak{D}_i$, $\rho \in k^*$).

In the same way, taking k_v as groundfield and considering Q as a morphism of varieties defined over k_v one defines gaugeforms $\mathfrak{D}_{v,i}$ ($i \in k_v$) by a formula analogous to (3). The forms $\mathfrak{D}_{v,i}$ determine measures $|\mathfrak{D}_{v,i}|_v$ on $U(i)_v$ satisfying

$$\int_{X_v - \{0\}} \Phi |dx|_v = \int_{k_v} |di|_v \int_{U_v(i)} \Phi |\mathfrak{D}_{v,i}|_v$$

for continuous Φ with compact support $\subset X_v - \{0\}$. The family of measures $|\mathfrak{D}_{v,i}|_v$ ($i \in k_v$) is the only one with those properties. So, using Lemma 1 and the fact that $\{0\}$ has measure 0 for $|dx|_v$ we see that

$$\mu_i = |\mathfrak{D}_{v,i}|_v \qquad (i \in k_v).$$

Let us return to the adelic case. Take Φ of the form

$$\Phi(x) = \prod \Phi_v(x_v) \; (x = (x_v) \in X_A),$$

where Φ_v is of Schwartz–Bruhat type for all v and Φ_v is the characteristic function of X_v^0 ($= X_{0_v}$) for almost all v. It is easily seen now that

$$\hat{F}_\Phi(i) = \int_{X_A} \Phi(x)\chi(iQ(x))|dx|_A = \prod_v \int_{X_v} \Phi_v \chi_v(i_v Q(x))|dx|_v$$

($i = (i_v) \in A$) is the Fourier transform of

$$\prod_v \int_{U_v(i_v)} \Phi_v |\mathfrak{D}_{v,i_v}|_v. \tag{4}$$

If in (4) all i_v are equal to $i \in k$, (4) becomes

$$\prod_v \int_{U(i)_v} \Phi_v |\mathfrak{D}_i|_v = \int_{U(i)_A} \Phi |\mathfrak{D}_i|_A$$

since $U(i)$ has convergence factors 1. We may now apply Proposition 2 of [2] which says that the Poisson formula is valid for $\hat{F}_\Phi$:

$$\sum_{i \in k} \int_{U(i)_A} \Phi |\mathfrak{D}_i|_A = \sum_{i \in k} \int_{X_A} \Phi(x)\chi(iQ(x))|dx|_A \tag{5}$$

(both series are absolutely convergent).

Remark 1. In order to know that we are allowed to apply Propositions 1 and 2 of [2] to our case we have to verify the conditions (A) and (B) occurring in those propositions. This may be done by estimating the integrals $\int \Phi_v(x)\chi_v(i_v Q(x))|dx|_v$.

3. Put $\Phi_t(x) = \Phi(tx)$ ($t \in A^*$) and consider $I(\Phi_t)$.

Lemma 2. *Write $X_A = X_\infty \times X'$ where X_∞ is the direct product of the X_v for v infinite and X' the restricted direct product of the other X_v. Let E be a closed* *subset of X_A which does not contain any point of the form* $(0, x')$. *Let C be a compact subset of the Schwartz–Bruhat space attached to X_A and let N be a positive real number. Then there exists a function Φ_0 in the Schwartz–Bruhat space such that*

$$|\tau^N \Phi(a_\tau x)| \leqq \Phi_0(x)$$

if $\Phi \in C$, $\tau \geqq 1$, $x \in E$ (a_τ denotes the idèle of k which has the component τ at each infinite place and 1 *at the finite places).*

For a proof see [3] (Lemme 7).

From formula (2) we find

$$I(\Phi_t) = 2 \sum_{i \in k^*} \int_{U(i)_A} \Phi_t |\mathfrak{D}_i|_A + 2|t|^{2-m} \int_{U(0)_A} \Phi |\mathfrak{D}_0|_A + \tau(G)\Phi(0).$$

The sum over $i \in k^*$ here is $O(|t|^{-N})$ for any N as $|t| \to \infty$ (write $t = ca_\tau \rho$ with c in a fixed compact subset of A^* and ρ in k^*, and apply Lemma 2). So we have

$$\lim_{|t| \to \infty} I(\Phi_t) = \tau(G)\Phi(0). \tag{6}$$

On the other hand, we may put (5) into (2). That gives

$$I(\hat{\Phi}) = I(\Phi) = 2 \sum_{i \in k} \int_{X_A} \Phi(x)\chi(iQ(x))|dx|_A + \tau(G)\Phi(0).$$

Replacing Φ by $\hat{\Phi}_{-t^{-1}}$ we get

$$|t|^m I(\Phi_t) = 2 \sum_{i \in k} \int_{X_A} \hat{\Phi}(t^{-1}x)\chi(iQ(x))|dx|_A + \tau(G)\hat{\Phi}(0),$$

$$I(\Phi_t) = 2 \sum_{i \in k} \int_{X_A} \hat{\Phi}(x)\chi(it^2Q(x))|dx|_A + \tau(G)\hat{\Phi}(0)|t|^{-m}.$$

Using the estimations mentioned in Remark 1 one can prove that

$$\sum_{i \in k^*} \int_{X_A} \hat{\Phi}(x)\chi(it^2Q(x))|dx|_A \tag{7}$$

tends to 0 if $|t| \to \infty$. So

$$\lim_{|t| \to \infty} I(\Phi_t) = 2\Phi(0). \tag{8}$$

Comparison of (6) and (8) gives $\tau(G) = 2$.

Finally, here is Siegel's formula:

$$\int_{G_A/G_k} \sum_{\xi \in X_k} \Phi(g(\xi)) \frac{|dg|_A}{2} = \sum_{i \in k} \int_{X_A} \Phi(x)\chi(iQ(x))|dx|_A + \Phi(0).$$

REMARK 2. In order to prove that (7) tends to 0 if $|t| \to \infty$ one may also use Fourier transform:

$$\int_{X_A} \hat{\Phi}(x)\chi(it^2Q(x))|dx|_A = |t|^{-m}.\int_{X_A} \Phi(x)\chi(-i^{-1}t^{-2}Q(x))|dx|_A,$$

and apply (5) once more. In fact, this is what is done in [2]. The version given above, however, does not need the Fourier transform of a quadratic character and can also be given in certain cases where one has, e.g., a cubic invariant instead of the quadratic invariant Q (an example is the group of the generic cubic form of an exceptional Jordan algebra of dimension 27, see [3]).

REFERENCES

1. A. Weil, *Adèles and algebraic groups*, Lecture notes, Institute for Advanced Study, Princeton, N.J., 1961.

2. ———, *Sur la formule de Siegel dans la théorie des groupes classiques*, Acta Math. **113** (1965), 1–87.

3. J. G. M. Mars, *Les nombres de Tamagawa de certains groupes exceptionnels* (to appear).

The Siegel Formula for Orthogonal Groups. II

BY

J. G. M. MARS

This is a resume of Weil's paper *Sur la formule de Siegel dans la théorie des groupes classiques*, (Acta Math. **113** (1965), 1–87) for the case of an orthogonal group.

1. **Notations.** Let k be an algebraic numberfield, Q a nondegenerate quadratic form on k^m given by a nonsingular symmetric matrix h in $M_m(k)$ ($Q(u) = {}^t uhu$ for $u \in k^m$). Let X_k be the linear space of all linear maps $k^n \to k^m$; X_k can be identified with the space $M_{m,n}(k)$ of $m \times n$-matrices with coefficients in k. If $x \in X_k$, $Q \circ x$ is a quadratic form on k^n with matrix ${}^t xhx$. Let $I(X)_k$ be the linear space of all quadratic forms on k^n; we identify it with the space of all symmetric matrices in $M_n(k)$. X_k and $I(X)_k$ are the sets of points over k of algebraic varieties X and $I(X)$ obtained in the usual way. We define a morphism $i_X : X \to I(X)$ by

$$i_X(x) = {}^t xhx \qquad (x \in X).$$

$I(X)$ is identified with its dual by means of the symmetric bilinear form $tr(w_1 w_2)$ on $I(X) \times I(X)$.

We put $G = O(Q)$, $G_1 = \mathrm{SO}(Q)$, $\tilde{G} = \mathrm{Spin}\,(Q)$; so G, G_1 and $\tilde{G}$ are algebraic groups defined over k, G_1 is the identity component of G and $\tilde{G}$ is the simply connected covering of G_1. G and G_1 may be considered as groups of matrices in M_m.

Finally $\mathrm{Sp}(X)$ or Sp will denote the (algebraic) group of matrices $s \in M_{2n}$ satisfying ${}^t ses = e$, where

$$e = \begin{pmatrix} 0 & 1_n \\ -1_n & 0 \end{pmatrix}.$$

P is the parabolic subgroup of Sp consisting of the matrices

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathrm{Sp}.$$

2. **Unitary operators.** It can be proved that there exists a unitary representation $\mathbf{r}$ of $\mathrm{Sp}(X)_k$ on $L^2(X_A)$ such that

$$\mathbf{r}\begin{pmatrix} \alpha & 0 \\ 0 & {}^t\alpha^{-1} \end{pmatrix} \text{ is the operator } \Phi(x) \to \Phi(x\alpha) \text{ if } \alpha \in M_n(k)^*,$$

$\mathbf{r}\begin{pmatrix} 0 & \gamma \\ -{}^t\gamma^{-1} & 0 \end{pmatrix}$ is the operator $\Phi(x) \to \hat{\Phi}(x\gamma)$ if $\gamma \in M_n(k)^*$,

$\mathbf{r}\begin{pmatrix} 1 & \rho \\ 0 & 1 \end{pmatrix}$ is the operator $\Phi(x) \to \Phi(x)\chi(\frac{1}{2}\operatorname{tr}({}^txx\rho))$ if $\rho \in M_n(k)$, ${}^t\rho = \rho$.

Here $\hat{\Phi}$ is the Fourier transform of Φ defined by

$$\hat{\Phi}(y) = \int_{X_A} \Phi(x)\chi(\operatorname{tr}({}^txhy))|dx|_A \ (y \in X_A),$$

χ is a character on A such that $\chi(xy)$ brings A into duality with itself in such a way that the discrete subgroup k of A satisfies $k = k^\perp$.

The Schwartz–Bruhat space $\mathfrak{S}(X_A)$ is mapped onto itself by the operators $\mathbf{r}(s)$ $(s \in \mathrm{Sp}_k)$.

3. **A decomposition of** Sp. Suppose s is an element of Sp_k,

$$s = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}.$$

Put $X_k\gamma = Y$ and choose a subspace Z of X_k such that

(a) X_k is the direct sum of Y and Z,

(b) $M_m(k)Z = Z$.

Then s can be written in the form

$$s = \begin{pmatrix} 1_n & \rho \\ 0 & 1_n \end{pmatrix}\begin{pmatrix} \lambda & 0 \\ 0 & {}^t\lambda^{-1} \end{pmatrix}\left(\begin{pmatrix} 0 & 1_p \\ -1_p & 0 \end{pmatrix}\begin{pmatrix} 1_p & \rho_1 \\ 0 & 1_p \end{pmatrix} \otimes 1_{2q}\right),$$

where ${}^t\rho = \rho \in M_n(k)$, $\lambda \in M_n(k)^*$ and the meaning of the last part of the formula is the following. Y and Z can be identified with $M_{m,p}(k)$ and $M_{m,q}(k)$ respectively with $p + q = n$. Choose some identifications. This gives a new identification of $X_k = Y \oplus Z$ with $M_{m,n}(k)$. Now

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \otimes 1_{2q}$$

means, if $a, b, c, d \in M_p(k)$, the element of X_k which corresponds in the *new* identification to the matrix

$$\begin{pmatrix} a & 0 & b & 0 \\ 0 & 1_q & 0 & 0 \\ c & 0 & d & 0 \\ 0 & 0 & 0 & 1_q \end{pmatrix}.$$

ρ_1 is a symmetric matrix in $M_p(k)$.

In the above decomposition ρ, λ and ρ_1 are unique (when Z and the identification of Y with $M_p(k)$ have been chosen). From this one can derive a system of representatives for $P_k\backslash \mathrm{Sp}_k$.

4. The Eisenstein–Siegel series.

Definition. $E(\Phi) = \sum_{P_k\backslash \mathrm{Sp}_k} (\mathbf{r}(s)\Phi)(0)$. (It is easily seen that $(\mathbf{r}(p)\Phi)(0) = \Phi(0)$ if $p \in P_k$.)

Theorem 1. *$E(\Phi)$ converges absolutely for all $\Phi \in \mathfrak{S}(X_A)$ and uniformly on every compact subset of $\mathfrak{S}(X_A)$ provided we have $m > 2n + 2$.*

The proof can be given by using reduction theory for the symplectic group Sp. With the system of representatives for $P_k\backslash \mathrm{Sp}_k$ from §3 and the description of $\mathbf{r}$ in §2 we find that

$$E(\Phi) = \sum E_Y(\Phi),$$

the summation is extended over all subspaces Y of X_k satisfying $M_m(k)Y = Y$,

$$E_X(\Phi) = \sum_{{}^t\rho = \rho \in M_n(k)} \int_{X_A} \Phi(x)\chi(\mathrm{tr}({}^txhx\rho))|dx|_A,$$

and $E_Y(\Phi)$ for $Y \neq X$ is defined in an analogous way. Now we can apply the Poisson formula to the series which defines $E_X(\Phi)$. The summation is in fact a summation over $I(X)_k$ and the value in i of the Fourier transform of the function

$$r \to \int_{X_A} \Phi(x)\chi(\mathrm{tr}({}^txhxr))|dx|_A$$

on $I(X)_A$ is

$$\int_{U(i)_A} \Phi|\theta_i|_A \text{ if } i \in I(X)_k.$$

Here $U(i)$ is the variety $\{x \in X : i_X(x) = i,\ \mathrm{rank}\ x = n\}$ and θ is a G-invariant gauge form on $U(i)$ ($U(i)$ is an orbit of G). (For this kind of application of the Poisson formula, see A. Weil, Acta Math. **113**.)

We see that E_X, and also E, is a tempered positive measure on $\mathfrak{S}(X_A)$.

E has the following invariance properties.

(a) From the definition of $E(\Phi)$ it is clear that E is invariant under Sp_k, i.e., $E(\Phi)$ is not changed when Φ is replaced by $\mathbf{r}(s)\Phi$, $s \in \mathrm{Sp}_k$.

(b) E is invariant under G_A, i.e., $E(\Phi)$ is not changed when $\Phi(x)$ is replaced by $\Phi(gx)$, $g \in G_A$.

5. Uniqueness theorem.

Theorem 4 (A. Weil, Acta Math. **113**).[1] *Suppose $m > 2n + 2$. Let v be a place of k such that $U(0)_v$ is not empty and G'_v a subgroup of G_v acting transitively on $U(i)_v$*

[1] See the first paragraph of this paper for the complete reference.

for any $i \in I(X)_k$. Let E' be a tempered positive measure on X_A, invariant under Sp_k *and under G'_v and such that $E' - E$ is a sum of measures carried by the sets $U(i)_A$, $i \in I(X)_k$. Then $E' = E$.*

6. The Siegel formula.

DEFINITION.

$$I(\Phi) = \int_{G_A/G_k} \sum_{\xi \in X_k} \Phi(g\xi)\, dv(g),$$

where v is the Haar measure on G_A normed in such way that $v(G_A/G_k) = 1$. Let $I_1(\Phi)$ (resp. $\tilde{I}(\Phi)$) denote the analogous integral with G_1 (resp. $\tilde{G}$) instead of G.

PROPOSITION. *$I(\Phi)$ is absolutely convergent for all $\Phi \in \mathfrak{S}(X_A)$ if $r = 0$ and if $m - r > n + 1$ (r = index of Q = dimension of a maximal totally isotropic subspace). The same is true for I_1 and $\tilde{I}$.*

The proof can be given with the use of reduction theory.

THEOREM 5. *Assume $m > 2n + 2$. Then $I = E$.*

This is Siegel's formula. It is also true for I_1 and $\tilde{I}$. It follows easily from Theorem 4 by induction on n (starting with $n = 0$, in which case the formula is trivial).

Restricting the measures I and E to $U(i)_A$ we get

$$\int_{G_A/G_k} \sum_{\xi \in U(i)_k} \Phi(g\xi)\, dv(g) = \int_{U(i)_A} \Phi|\theta_i|_A \, (i \in I(X)_k).$$

COROLLARY (HASSE PRINCIPLE). *If $U(i)_k$ is empty, $U(i)_A$ is empty.*

For, if $U(i)_A$ is not empty, the Tamagawa measure $|\theta_i|_A \neq 0$.

COROLLARY 2. *The Tamagawa number of G (with respect to convergence factors λ) is equal to the Tamagawa number of the stabilizer in G of any point $\xi \in X_k$ of rank n. The same is true for G_1 and $\tilde{G}$.*

To see this, take $n = 1$ and write $U(i)_A = G_A/H_A$, $U(i)_k = G_k/H_k$ where H is the stabilizer in G of a point ξ_0 of $U(i)_k$. Then

$$\int_{U(i)_A} \Phi|\theta_i|_A = \tau_\lambda(G)\tau_\lambda(H)^{-1} \int_{G_A/H_k} \Phi(g\xi_0)\, dv(g)\cdot$$

and

$$\int_{G_A/G_k} \sum_{\xi \in U(i)_k} \Phi(g\xi)\, dv(g) = \int_{G_A/H_k} \Phi(g\xi_0)\, dv(g).$$

From Corollary 2 one deduces that there is a number τ such that the Tamagawa number of any special orthogonal group in at least 3 variables is equal to τ.

Appendix

In his paper in Acta Math. **113** Weil defined $I(\Phi)$ and $E(\Phi)$ for modules X_k over semisimple algebras with involution and he proved that $I = E$ if $E(\Phi)$ is absolutely convergent. We give here a list of Weil's results in the case of a simple module X_k over a simple algebra C_k. G is then the group of elements $c \in C$ such that $cc^{\iota} = 1$ (ι = the involution in C).

We have the following cases:

(0) $X_k = k^m$, G is the symplectic group of an alternating form on X_k, m is even.

(1) $X_k = D^m$, D a quaternion division algebra over k, G is the group of a hermitian form (with respect to the usual involution in D) on X_k.

(2) $X_k = D^m$, D a central division algebra over a quadratic extension K of k, D is supplied with an involution which induces on K the nontrivial k-automorphism (involution of the second kind), G is the group of a hermitian form on X_k.

(3) $X_k = D^m$, D a quaternion division algebra over k, G is the group of an antihermitian form (with respect to the usual involution on D) on X_k.

(4) $X_k = k^m$, G is the group of a quadratic form on X_k.

All these forms are of course supposed to be nondegenerate. The index of the form is r. In the Cases 2, 3, 4 we define G_1 to be the group of elements in G with reduced norm 1.

Case	G_1 semisimple	$I(\Phi)$ conv.	$E(\Phi)$ conv.	$E = I$	Result on Tamagawa numbers
0	$m > 0$	$m > 0$	$m > 0$	$m > 0$	$\tau(G) = 1$ $(m > 0)$
1	$m \geqq 1$	$m \geqq 1$	$m \geqq 2$	$m \geqq 2$	$\tau(G) = 1$ $(m \geqq 1)$
2	$\left\{\begin{array}{l} m \geqq 2 \\ m = 1, D \text{ not comm.} \end{array}\right.$	$\left\{\begin{array}{l} m \geqq 3 \\ m = 2, r = 0 \end{array}\right.$	$m \geqq 3$	$m \geqq 3$	$\tau(G_1) = \tau$ $(m \geqq 1)$
3	$m \geqq 2$	$\left\{\begin{array}{l} m \geqq 3 \\ m = 2, r = 0 \end{array}\right.$	$m \geqq 4$	$m \geqq 4$	$\tau(G_1) = \tau$ $(m \geqq 2)$
4	$m \geqq 3$	$\left\{\begin{array}{l} m \geqq 5 \\ m = 4, r \leqq 1 \\ m = 3, r = 0 \end{array}\right.$	$m \geqq 5$	$m \geqq 5$	$\tau(G_1) = \tau$ $(m \geqq 3)$

The Hasse principle is a consequence of the Siegel formula $E = I$, so it is proved for the same values of m as that formula.

By using the classical isomorphisms in low dimensions ($m = 1$ in Case 2 (and $[D:K] \leqq 4$), $m = 2$ in Case 3, $m = 3$ in Case 4) Weil proved in *Adeles and algebraic groups* that the number τ in Case 2 is 1 if $[D:K] \leqq 4$ and that $\tau = 2$ in Cases 3 and 4.

The Volume of the Fundamental Domain for Some Arithmetical Subgroups of Chevalley Groups

BY

R. P. LANGLANDS[1]

Let $\mathfrak{g}_Q$ be a split semisimple Lie algebra of linear transformations of the finite dimensional vector space V_Q over Q. Let $\mathfrak{h}_Q$ be a split Cartan subalgebra of $\mathfrak{g}_Q$ and choose for each root α of $\mathfrak{h}_Q$ a root vector X_α so that if $[X_\alpha, X_{-\alpha}] = H_\alpha$ then $\alpha(H_\alpha) = 2$ so that there is an automorphism θ of $\mathfrak{g}_Q$ with $\theta(X_\alpha) = -X_{-\alpha}$. Let L be the set of weights of $\mathfrak{h}_Q$ and if $\lambda \in L$ let

$$V_Q(\lambda) = \{v \in V_Q | Hv = \lambda(H)v \text{ for all } H \in \mathfrak{h}_Q\};$$

let $H_1, \cdots, H_p$ be a basis over Z of

$$\{H | \lambda(H) \in Z \text{ if } V_Q(\lambda) \neq 0\}.$$

As usual, there is associated to $\mathfrak{g}_Q$ a connected algebraic group G_C of linear transformations of $V_C = V_Q \otimes {}_Q C$. If H is some lattice in V_Q satisfying

(i) $M = \sum_{\lambda \in L} M \cap V(\lambda)$,

(ii) $(X_\alpha^n/n!)M \subseteq M$ for all α,

then we let $G_Z = \{g \in G_C | gM = M\}$. Let ω be a left invariant form on G_R of highest degree which takes the value ± 1 on $\prod_{i=1}^p \wedge H_i \wedge \prod_{\alpha>0} \wedge X_\alpha$ and let $[dg]$ be the Haar measure associated to ω. Our purpose now is to show that:

If $\zeta(\cdot)$ is the Riemann zeta function, $\prod_{i=1}^p (t^{2a_i-1} + 1)$ is the Poincaré polynomial of G_C, and c is the order of the fundamental group of G_C then

$$\int_{G_Z \backslash G_R} [dg] = c \prod_{i=1}^p \zeta(a_i).$$

The method to be used to find the volume of $G_Z \backslash G_R$ is not directly applicable to $[dg]$ so it is necessary to introduce another Haar measure on the group G_R. Let U be the connected subgroup of G_C whose Lie algebra is spanned over R by $\{X_\alpha - X_{-\alpha}, i(X_\alpha + X_{-\alpha}), iH_\alpha | \alpha \text{ a root}\}$ and let $K = G_R \cap U$. Choose an order on the roots and let $N = N_R$ be the set of real points on the connected algebraic subgroup of G_C with the Lie algebra $\sum_{\alpha>0} CX_\alpha$. Let A_R be the normalizer of $\mathfrak{h}_C$ in G_R. Let dn be the Haar measure on N defined by a form which takes the value ± 1 on $\prod_{\alpha>0} \wedge X_\alpha$ and let da be the Haar measure on A_R defined by a form which takes the value ± 1 on $\prod_{i=1}^p \wedge H_i$. Let dk be the Haar measure on K such

[1] Miller Fellow.

that the total volume of K is one. Let $\rho = \frac{1}{2}\sum_{\alpha>0}\alpha$ and let $\xi_{2\rho}(a)$ be the character of A_C associated to 2ρ. Finally let dg be such that

$$\int_{G_R} \phi(g)\,dg = \int_{N\times A_R\times K} |\xi_{2\rho}(a)|^{-1}\phi(nak)\,dn\,da\,dk.$$

If N^- is the set of real points on the group associated to $\sum_{\alpha<0} CX_\alpha$ define dn^- in the same way as we defined dn. It is easy to see that

$$\int_G \phi(g)[dg] = \int_N dn \int_{A_R} da \int_{N^-} dn^-|\xi_{2\rho}(a)|^{-1}\phi(nan^-).$$

Suppose $\phi(gk) = \phi(g)$ for all $g \in G_R$ and all $k \in K$. Then

$$\int_G \phi(g)\,dg = \int_{N\times A_R} dn\,da|\xi_{2\rho}(a)|^{-1}\phi(na).$$

On the other hand, if $n^- = n(n^-)a(n^-)k(n^-)$,

$$\int \phi(g)[dg] = \int_{N^-} dn^- \left\{\int_A da \int_N dn|\xi_{2\rho}(a)|^{-1}\phi(nan(n^-)a(n^-)k(n^-))\right\}$$

$$= \left\{\int_A da \int_N dn|\xi_{2\rho}(a)|^{-1}\phi(na)\right\}\left\{\int_{N^-} |\xi_{2\rho}a(n^-)|dn^-\right\}.$$

It follows from a formula of Gindikin and Karpelevich that the second factor equals

$$\prod_{\alpha>0}\frac{\pi^{-\frac{1}{2}}\Gamma(\rho(H_\alpha)/2)}{\Gamma((\rho(H_\alpha)+1)/2)} = \prod_{\alpha>0}\frac{\pi^{-\rho(H_\alpha)/2}\Gamma(\rho(H_\alpha)/2)}{\pi^{-(\rho(H_\alpha)+1)/2}\Gamma((\rho(H_\alpha)+1)/2)}$$

$$= \frac{\prod'_{\alpha>0}\pi^{-\rho(H_\alpha)/2}\Gamma(\rho(H_\alpha)/2)}{\prod_{\alpha>0}\pi^{-(\rho(H_\alpha)+1)/2}\Gamma((\rho(H_\alpha)+1)/2)},$$

since when α is simple $\rho(H_\alpha) = 1$ and

$$\Pi^{-\frac{1}{2}}\Gamma(\tfrac{1}{2}) = 1.$$

The product in the numerator is taken over the positive roots which are not simple. By a well-known result the numbers, with multiplicities, in the set

$$\{\rho(H_\alpha) + 1|\alpha > 0\}$$

are just the numbers $\rho(H_\alpha)$ with α positive and not simple, together with the numbers $a_1, \cdots, a_p$ so if

$$\xi(s) = \Pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s)$$

we have to show that

$$\int_{G_{\mathbf{Z}}\backslash G_{\mathbf{R}}} dg = \frac{c \prod_{\alpha>0} \xi(\rho(H_\alpha)+1)}{\prod'_{\alpha>0} \xi(\rho(H_\alpha))}.$$

By the way, it is well to keep in mind that $\rho(H_\alpha) > 1$ if α is not simple.

Let A be the connected component of $A_{\mathbf{R}}$ and let M be the points of finite order in $A_{\mathbf{R}}$. Certainly $A_{\mathbf{R}} = AM$. Moreover, by Iwasawa, $G = NAK$. If $g = nak$ and $a = \exp H$, we set $H = H(g)$.

If ϕ is an infinitely differentiable function with compact support on $N\backslash G$ such that $\phi(gk) = \phi(g)$ for all g in G and all k in K we can write ϕ as a Fourier integral.

$$\phi(g) = \frac{1}{(2\pi)^p} \int_{\operatorname{Re}\lambda=\lambda_0} \exp(\lambda(H(g)) + \rho(H(g))\Phi(\lambda)|d\lambda|;$$

λ is the symbol for an element of the dual of $\mathfrak{h}_{\mathbf{C}}$; $\Phi(\lambda)$ is an entire complex-valued function of λ; and $d\lambda = dz_1 \wedge \cdots \wedge dz_p$ with $z_i = \lambda(H_i)$. As in the lectures on Eisenstein series we can introduce

$$\phi\hat{}(g) = \sum_{\gamma\in G_{\mathbf{Z}}\cap NM\backslash G_{\mathbf{Z}}} \phi(\gamma g).$$

Our evaluation of the volume of $G_{\mathbf{Z}}\backslash G_{\mathbf{R}}$ will be based on the simple relation

$$(\phi\hat{}, 1)(1, \psi\hat{}) = (1, 1)(\Pi\phi\hat{}, \Pi\psi\hat{}).$$

The inner products are taken in $L^2(G_{\mathbf{Z}}\backslash G_{\mathbf{R}})$ with respect to dg and Π is the orthogonal projection on the space of constant functions. Since

$$(1, 1) = \int_{G_{\mathbf{Z}}\backslash G_{\mathbf{R}}} dg$$

it is enough to find an explicit formula for the other three terms. Now

$$\begin{aligned}(\phi\hat{}, 1) &= \int_{G_{\mathbf{Z}}\cap NM\backslash G_{\mathbf{R}}} \phi(g)\,dg \\ &= \mu(G_{\mathbf{Z}} \cap NM\backslash NM) \int_A |\xi_{2\rho}(a)|^{-1}\phi(a)\,da \\ &= \Phi(\rho)\end{aligned}$$

since $\mu(G_{\mathbf{Z}} \cap NM\backslash NM) = 1$. To see the latter we have to observe that $M \subseteq G_{\mathbf{Z}}$ and that, as follows from results stated in Cartier's talk, $\mu(G_{\mathbf{Z}} \cap N\backslash N) = 1$. It is also clear that $(1, \psi\hat{}) = \overline{\Psi}(\rho)$. The nontrivial step is to evaluate

$$(\Pi\phi\hat{}, \Pi\psi\hat{}).$$

From the theory of Eisenstein series we know that

$$(\phi^\wedge, \psi^\wedge) = \frac{1}{(2\pi)^p}\int_{\operatorname{Re}\lambda=\lambda_0}\sum_{s\in\Omega} M(s,\lambda)\Phi(\lambda)\overline{\Psi}(-s\bar{\lambda})|d\lambda|.$$

Ω is the Weyl group, λ_0 is any point such that $\lambda_0(H_\alpha) > 1$ for every simple root, and

$$M(s,\lambda) = \prod_{\alpha>0}\frac{\xi(1+s\lambda(H_\alpha))}{\xi(1+\lambda(H_\alpha))} = \prod_{\alpha>0;s\alpha<0}\frac{\xi(\lambda(H_\alpha))}{\xi(1+\lambda(H_\alpha))}$$

In the lectures on Eisenstein series I introduced an unbounded self-adjoint operator A on the closed subspace of $L^2(G_{\mathbf{Z}}\backslash G_{\mathbf{R}})$ generated by the functions $\phi^\wedge$ with ϕ of the form indicated above. Comparing the definition of A with the formula for $(\phi^\wedge, 1)$ we see that

$$(A\phi^\wedge, 1) = (\rho,\rho)(\phi^\wedge, 1).$$

Since the constant functions are in this space $A1 = (\rho,\rho)\cdot 1$. As a consequence, if $E(x)$, $-\infty < x < \infty$, is the spectral resolution of A the constant functions are in the range of $E((\rho,\rho)) - E((\rho,\rho) - 0) = E$. We show that this range consists precisely of the constant functions and compute $(E\phi^\wedge, \psi^\wedge) = (\Pi\phi^\wedge, \Pi\psi^\wedge)$.

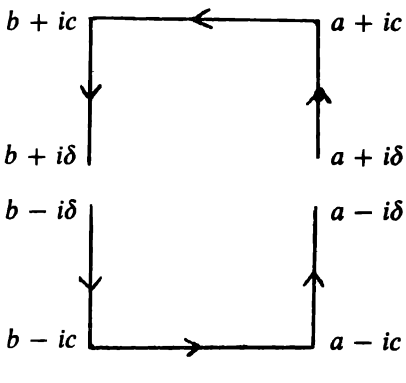
Suppose $a > (\rho,\rho) > b$ and $a - b$ is small. According to a well-known formula

$$\tfrac{1}{2}\{(E(a)\phi^\wedge,\psi^\wedge) + (E(a-0)\phi^\wedge,\psi^\wedge)\} - \tfrac{1}{2}\{(E(b)\phi^\wedge,\psi^\wedge) + (E(b-0)\phi^\wedge,\psi^\wedge)\}$$

is equal to

(a) $$\lim_{\delta\downarrow 0}\frac{1}{2\pi i}\int_{C(a,b,c,\delta)}(R(\mu,A)\phi^\wedge,\psi^\wedge)\,d\mu$$

if $C(a, b, c, \delta)$ is the following contour.



Recall that, if $\operatorname{Re}\mu > (\lambda_0, \lambda_0)$,

$$(R(\mu,A)\phi^\wedge,\psi^\wedge) = \sum_{s\in\Omega}\frac{1}{(2\pi i)^p}\int_{\operatorname{Re}\lambda=\lambda_0}\frac{1}{\mu-(\lambda,\lambda)}M(s,\lambda)\Phi(\lambda)\overline{\Psi}(-s\bar{\lambda})\,d\lambda.$$

If $w = (w_1, \cdots, w_p)$ belongs to C^p let $\lambda(w)$ be such that $\lambda(H_{\alpha_i}) = w_i$, if $\alpha_1, \cdots, \alpha_p$ are the simple roots. Set

$$\phi_p(w, s) = M(s, \lambda(w))\Phi(\lambda(w))\overline{\Psi}(-s\lambda\bar{w})),$$
$$Q_p(w) = (\lambda(w), \lambda(w))$$

then (a) is equal to

$$\frac{1}{c}\sum_{s\in\Omega}\lim_{\delta\downarrow 0}\frac{1}{2\pi i}\int_{C(a,b,c,\delta)} d\mu\left\{\frac{1}{(2\pi i)^p}\int_{\mathrm{Re}\, w = w_0}\frac{1}{\mu - Q_p(w)}\phi_p(w, s)\, dw_1 \cdots dw_p\right\}$$

provided each of these limits exist.[2] The coordinates of w_0 must all be greater than one. We shall consider the limits individually.

Let $w^q = (w_1, \cdots, w_q)$ and define $\phi_q(w^q; s)$ inductively for $0 \leqq q \leqq p$ by

$$\phi_q(w_1, \cdots, w_q; s) = \underset{w_{q+1}=1}{\mathrm{Residue}}\, \phi_{q+1}(w_1, \cdots, w_{q+1}; s).$$

It is easily seen that $\phi_q(w^q; s)$ has no singularities in the region defined by the inequalities $\mathrm{Re}\, w_i > 1$, $1 \leqq i \leqq q$; that $\phi_q(w^q; s)$ goes to zero very fast when the imaginary part of w^q goes to infinity and its real part remains in a compact subset of this region; and that there is a positive number ε so that the only singularities of $\phi_q(w^q; s)$ in

$$\{(w_1, \cdots, w_q) \big| \, |\mathrm{Re}\, w_i - 1| < \varepsilon, 1 \leqq i \leqq q\}$$

lie on the hyperplanes $w_i = 1$ and are at most simple poles. $\phi_0(s)$ is of course a constant. Set $Q_q(w^q) = Q_p(w_1, \cdots, w_q, 1, \cdots, 1)$.

Let us show by induction that the given limit equals

$$\text{(b)} \qquad \lim_{\delta\downarrow 0}\frac{1}{2\pi i}\int_{C(a,b,c,\delta)} d\mu\left\{\frac{1}{(2\pi i)^q}\int_{\mathrm{Re}\, w^q = w_0^q}\frac{1}{\mu - Q_q(w^q)}\phi_q(w^q; s)\, dw_1 \cdots dw_q\right\}$$

if $w_0^q = (w_{0,1}, \cdots, w_{0,q})$ with $w_{0,i} > 1$, $1 \leqq i \leqq q$. Of course, the above expression is independent of the choice of such a point w_0^q. Take $w_0^q = (1 + u, \cdots, 1 + u, 1 + v)$, with u and v positive but small and $w_0^{q-1} = (1 + u, \cdots, 1 + u)$. If $\Lambda_1, \cdots, \Lambda_p$ are such that $\Lambda_i(H_{\alpha j}) = \delta_{ij}$, then $(\Lambda_i, \Lambda_j) \geqq 0$. As a consequence, if u is much smaller than v, then

$$Q_q(1 + u, \cdots, 1 + u, 1 - v) < (\rho, \rho).$$

Choose (b) to be larger than the number on the left. Also

$$\mathrm{Re}\, Q_q(w^q) = Q_q(\mathrm{Re}\, w^q) - Q_p(\mathrm{Im}\, w_1, \cdots, \mathrm{Im}\, w_q, 0, \cdots, 0).$$

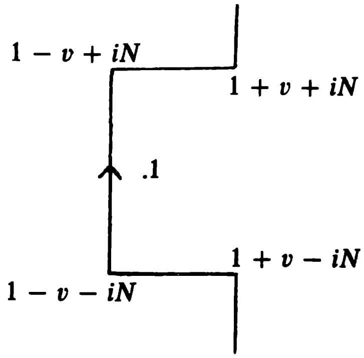
Thus there is a constant N so that if either $\mathrm{Re}\, w_i = 1 + u$, $1 \leqq i \leqq q - 1$ and $\mathrm{Re}\, w_q = 1 - v$ or $\mathrm{Re}\, w_i = 1 + u$, $1 \leqq i \leqq p$ and $|\mathrm{Re}\, w_q - 1| \leqq v$ and $|\mathrm{Im}\, w_q| > N$,

[2] The inner integral is defined for $\mathrm{Re}\, \mu > Q_p(w_0)$. However, as can be seen from the discussion to follow, the function of μ it defines can be analytically continued to a region containing $C(a, b, c, \delta)$.

then

$$\operatorname{Re} Q_q(w^q) < b - 1/N$$

In (b) we may perform the integrations in any order. Integrate first with respect to w_q. If C is the indicated contour, the result is the sum of (b) with q replaced by $q - 1$ and



The contour C

$$\lim_{\delta \downarrow 0} \frac{1}{(2\pi i)^q} \int_{\operatorname{Re} w^{q-1} = w_0^{q-1}} dw_1 \cdots$$
$$\cdots dw_{q-1} \int_C dw_q \phi_q(w^q, s) \left\{ \frac{1}{2\pi i} \int_{C(a,b,\dot{c},\delta)} \frac{1}{\mu - Q_q(w^q)} d\mu \right\}$$

which is obviously zero.

Taking $q = 0$ in (b) we get

$$\lim_{\delta \downarrow 0} \frac{\phi_0(s)}{2\pi i} \int_{C(a,b,c,\delta)} \frac{1}{\mu - (\rho, \rho)} d\mu = \phi_0(s).$$

It is clear that $\phi_0(s)$ is zero unless s sends every positive root to a negative root but that for the unique element of the Weyl group which does this

$$\phi_0(s) = \frac{\prod'_{\alpha > 0} \xi(\rho(H_\alpha)) \Phi(\rho) \overline{\Psi(\rho)}}{\prod_{\alpha > 0} \xi(\rho(H_\alpha) + 1)}$$

since $s\rho = -\rho$. This is the result required.

Finally, I remark that although the method just described for computing the volume of $\Gamma \backslash G$ has obvious limitations, it can be applied to other groups. In particular it works for Chevalley groups over a numberfield.

Galois Cohomology of Linear Algebraic Groups

BY

T. A. SPRINGER

This is the substance of three lectures; the purpose of which was to give a brief introduction to the notions and results of Galois cohomology of linear algebraic groups.

1. **Principal homogeneous spaces of algebraic groups.**

1.1. Let G be a linear algebraic group defined over a field k. Let P be a principal homogeneous space of G. This means that P is an algebraic variety along with a morphism $f: G \times P \to P$, defined over k, which defines a transformation group action of G on P which is simply transitive—that is, the mapping

$$(f, pr_2): G \times P \to P \times P$$

sending (g, p) into (gp, p) is an isomorphism. Thus if we take $P = G$ and let f be the product mapping, $G = P$ is a principal homogeneous space of G. If A is a ring containing k and $P_A \neq \emptyset$, then G_A acts simply transitively on P_A.

Two principal homogeneous spaces P, P' of G are isomorphic over k if P and P' are isomorphic as algebraic varieties under a mapping defined over k which is compatible with the action of G. If P has a k-rational point, then G and P are k-isomorphic principal homogeneous spaces of G.

The set of k-isomorphism classes of principal homogeneous spaces of G is denoted by $H^1(k, G)$. Similarly if k is perfect and K is a Galois extension of k, the set of k-isomorphism classes of principal homogeneous spaces P of G which have a K-rational point is denoted by $H^1(K/k, G)$. We have $H^1(k, G) = H^1(k_s/k, G)$ where k_s is the separable closure of k. The element of $H^1(K/k, G)$ which contains the trivial principal homogeneous space G of G is denoted by 0.

The notation $H^1(K/k, G)$ is motivated by considering the action of the Galois group $\Gamma = \mathrm{Gal}(K/k)$ on G_K and P_K. For $s \in G_K$, $x \in P_K$ we let ${}^s g$ be the image of g in G_K under s and ${}^s x$ be the image in P_K of x under s. Then ${}^s(gx) = {}^s g\, {}^s x$, since f is defined over k. Thus fixing x in P_K and denoting by g_s the unique element of G_K such that ${}^s x = g_s x$ for s in Γ, we have $g_{st} x = {}^{st}x = {}^s({}^t x) = {}^s g_t\, {}^s x = {}^s g_t g_s x$. So the mapping $s \mapsto g_s$ from into G_k satisfies

$$g_{st} = {}^s g_t g_s \qquad (s, t \in \Gamma). \tag{1}$$

If one replaces x by another point y in P_k, then $y = hx$ for some h in G_k and the function $g' = (g'_s)$ which we obtain is related to $g = (g_s)$ according to the formula

$$g'_s = {}^s h g_s h^{-1}. \tag{2}$$

Also, if we give Γ the Krull topology and G_K the discrete topology, then g is a continuous function.

Denote by $Z^1(K/k, G)$ the set of continuous functions (g_s) verifying (1). Moreover (2) defines an equivalence relation R on $Z^1(K/k, G)$. If G is abelian, $Z^1(K/k, G)$ is just the group of continuous 1-cocycles of Γ in G_K and R is the equivalence relation defined by the subgroup $B^1(K/k, G)$ of coboundaries. From what we have seen above, it follows that there exists a mapping Φ from $H^1(K/k, G)$ into $Z^1(K/k, G)/R$. We have the following result

PROPOSITION 1.1. *Φ is bijective.*

For the proof see [6, Chapter III, 1.3].

1.2. *Examples.* For details we refer to [6, Chapter III, §1].

(1) $H^1(K/k, \mathrm{GL}_n) = 0$ if K is a Galois extension of k. For $n = 1$ this is Hilbert's "theorem 90".

(2) Let k be a perfect field, V a vector space over k, x a tensor of type (p, q) over V. If y is another such tensor, y is isomorphic to x over V if some automorphism of V induces a mapping sending x into y. y is called a *K/k-form of* x if $x \otimes 1$ and $y \otimes 1$ are isomorphic in $V_K = V \otimes_k K$. Let G be the stabilizer of x in $\mathrm{GL}(V)$. Then G is defined over k, since k is perfect. And $H^1(K/k, G)$ may be identified with the isomorphism classes of K/k-forms of x. A number of important facts are special cases of this (see Examples 3, 4, 5, 6 in this section).

(3) Suppose that characteristic k is different from 2. Let x be a tensor over V belonging to a quadratic form Q on V (notation as in (2)). Let G be the orthogonal group on V with respect to Q. Then $H^1(K/k, G)$ may be identified with the set of equivalence classes of quadratic forms on V which become equivalent to Q upon extension to V_K. And $H^1(k, G)$ may be identified with the set of equivalence classes of quadratic forms on V which have the same rank as Q. More explicitly, if $S \in M_n(k)$ is a symmetric matrix defining Q and if $S' \in M_n(k)$ is a symmetric matrix having the same rank as that of S, the corresponding principal homogeneous space of G is such that for any ring A containing k we have

$$P_A = \{X \in \mathrm{GL}_n(A) | S' = {}^t XSX\}.$$

(4)$H^1(k, \mathrm{Sp}_n) = 0$ and $H^1(K/k, \mathrm{Sp}_n) = 0$ (where Sp_n denotes the symplectic group in n variables). This is seen by applying (2) and the fact that if two skew symmetric bilinear forms on V are equivalent upon extension to V_K, then they are equivalent.

(5) An algebra structure on V is determined by a tensor over V. The automorphism group of the algebra M_n of $n \times n$ matrices is PGL_n. Thus $H^1(K/k, \mathrm{PGL}_n)$ may be identified with the set of isomorphism classes of central simple algebras over k which upon extension of the base field to K become isomorphic to $M_n(K)$.

(6) Let $\mathfrak{g}$ be a Lie algebra over the perfect field k, let $G = \mathrm{Aut}(\mathfrak{g})$ be the group of automorphisms of $\mathfrak{g}$. G is an algebraic group which is defined over k. Then

$H^1(k, \mathrm{Aut}\,\mathfrak{g})$ may be identified with the isomorphism classes of k-forms of $\mathfrak{g}$ (a k-form of $\mathfrak{g}$ is a Lie algebra over k which becomes isomorphic to $\mathfrak{g}$ upon extension to $\bar{k}$). Similar results hold for the classification of forms of algebraic groups.

2. **Noncommutative cohomology.**

2.1. *Definition of* H^0 *and* H^1. Let Γ be a topological group operating continuously on a group A as a group of automorphisms, A being endowed with the discrete topology. We now define $H^i(\Gamma, A)$ for $i = 0, 1$.

Firstly, $H^0(\Gamma, A) = A^\Gamma$, the set of Γ-invariant elements of A. This definition makes sense even if A is only a set on which Γ operates, however then $H^0(\Gamma, A)$ can be empty. $H^0(\Gamma, A)$ is a group if A is a group. Next we define $Z^1(\Gamma, A)$ (the set of cocycles of Γ in A) to be the set of continuous functions $z = (z_s)$ of Γ in A such that $z_{st} = {}^sz_tz_s$ for all s in Γ (${}^sa$ denotes the image of $a \in A$ under $s \in \Gamma$). A acts on $Z^1(\Gamma, A)$, an element $a \in A$ sending the cocycle z into z', where $z'_s = {}^saz_sa^{-1}$. Denoting by R the ensuing equivalence relation, we define $H^1(\Gamma, A) = Z^1(\Gamma, A)/R$.

The element of $H^1(\Gamma, A)$ containing the cocycle which maps each element of Γ into the identity element of A is denoted by 0. So $H^1(\Gamma, A)$ is a set with a privileged point, however there is, if A is nonabelian, no canonical group structure on this set.

If B is another Γ-group, a Γ-homomorphism $f: A \to B$ induces mappings f^i_* from $H^i(\Gamma, A)$ into $H^i(\Gamma, B) (i = 0, 1)$. f^0_* is a homomorphism and f^1_* maps O into O.

2.2. *Example.* Let G be an algebraic group defined over the field k. Let K be a Galois extension of k, put $\Gamma = \mathrm{Gal}(K/k)$. Then according to Proposition 1.1 there is a bijection of $H^1(\Gamma, G_K)$ onto $H^1(K/k, G)$.

For $K = k_s$, the separable closure of k, one obtains a bijection of $H^1(\Gamma, G_K)$ onto $H^1(k, G)$.

2.3. *Twisting.* Now let X be a Γ-set on which A operates as a transformation group, in such a fashion that ${}^s(ax) = {}^sa\,{}^sx$ for s in Γ, a in A, x in X where ax denotes the image of x under a. If z is in $Z^1(\Gamma, A)$, we can get a new action of Γ on X by *twisting with* z. This action is defined as follows: set ${}_sx = z_s^{-1}({}^sx)$ for s in Γ, x in X. Then ${}_{st}x = {}_s({}_tx)$ for s, t in Γ and x in X since:

$$z_{st}^{-1}({}^{st}x) = (z_s^{-1}\,{}^s(z_t^{-1}))\,{}^s({}^tx) = z_s^{-1}\,{}^s(z_t^{-1}\,{}^tx).$$

Thus using z, X is made into a new Γ-set X_z.

2.4. *Examples of twisting.* (1) Let A play the role of X and $\mathrm{Aut}\,A$ that of A in the above discussion, where A is a Γ-group.

Let Γ operate on $\mathrm{Aut}\,A$ as follows: for s in Γ and α in $\mathrm{Aut}\,A$, define ${}^s\alpha$ by requiring that ${}^s\alpha(a) = {}^s(\alpha({}^{s^{-1}}a))$. It is clear that ${}^s(\alpha a) = {}^s\alpha\,{}^sa$ for s in Γ, a in A and α in $\mathrm{Aut}\,A$ (where $\alpha a = \alpha(a)$ for a in A and α in $\mathrm{Aut}\,A$).

If z' is a cocycle in $Z^1(\Gamma, \mathrm{Aut}\,A)$, a new Γ-group $A_{z'}$ is obtained by twisting with z'. If z is a cocycle in $Z^1(\Gamma, A)$, z and the homomorphism $\mathrm{Int}: A \to \mathrm{Aut}\,A$ determine a cocycle $z' = \mathrm{Int} \circ z$ of $Z^1(\Gamma, \mathrm{Aut}\,A)$. It is convenient to define $A_z = A_{z'}$.

Thus if A is a Γ-group and z is an element of $Z^1(\Gamma, A)$, z determines a new Γ-group A_z. We look at instances of this in the next examples.

(2) Suppose that we are in the situation of Example 2.2. Let B be the group of algebraic automorphisms of G, which are defined over K. Γ acts continuously on B, B being endowed with the discrete topology. If $z \in Z^1(\Gamma, B)$, we can form, in the manner explained above, the twisted group $(G_K)_z$. Then the following holds: there exists an algebraic group G_z, defined over k, which is isomorphic over K to G, the isomorphism being such that it identifies the Γ-groups $(G_z)_K$ and $(G_K)_z$ (a proof of this is contained in [6, Chapter III, §1]).

(3) Let k be a field of characteristic $\neq 2$, K a quadratic Galois extension of k with Galois group $\Gamma = \mathrm{Gal}(K/k)$. Choose α in k such that $K = k(\sqrt{\alpha})$. Let s be the nontrivial element of Γ. Let $A = \mathrm{SL}_n(K)$. A has an outer automorphism $\sigma : x \to {}^t x^{-1}$. And ${}^s\sigma = \sigma$ $({}^s\sigma(x) = {}^s(\sigma({}^{s^{-1}}x)) = {}^s({}^t({}^{s^{-1}}x)^{-1} = {}^t x^{-1} = \sigma(x))$. Define $z : \Gamma \to \mathrm{Aut}\, A$ by setting $z_1 = id_A, z_s = \sigma$. Then since ${}^s\sigma = \sigma$ and $\sigma^2 = 1$, z is in $Z^1(K/k, \mathrm{Aut}\, A)$. We now calculate A_z^Γ: since ${}_s x = z_s^{-1}\, {}^s x = \sigma^{-1}({}^s x) = {}^t x^{*-1}$ for x in A, we have $A_z^\Gamma = \mathrm{SU}_n(K/k)$. The algebraic group $(\mathrm{SL}_n)_z$ is isomorphic over k to the special unitary group, defined by the quadratic extension K/k.

(4) Let K, k, α, Γ, s be as in Example 2 of this section. Let $S = \mathrm{diag}(\alpha_1, \cdots, \alpha_{2n})$ in $M_{2n}(k)$. Let $v = \mathrm{diag}(1, \cdots, 1, -1)$ in $M_{2n}(k)$. Let $G = O^+(S)$. Let $\sigma : G \to G$ be defined by setting $\sigma(x) = vxv$ for x in G. Define z as before by setting $z(1) = 1$, $z(s) = \sigma$ (as before, z is in $Z^1(\Gamma, G)$). It is easily checked that $(A_z)^\Gamma = O^+(S_1)_k$, where $S_1 = \mathrm{diag}(\alpha_1, \cdots, \alpha_{2n-1}, \alpha\alpha_{2n}) \cdot G_z$ is k-isomorphic to $O^+(S_1)$.

(5) Let k be a perfect field, $\Gamma = \mathrm{Gal}(\bar{k}/k)$, $A = \mathrm{SL}_n(\bar{k})$. Let z be in $Z^1(\Gamma, \mathrm{PGL}_n(\bar{k}))$. Since $\mathrm{PGL}_n(\bar{k}) \subset \mathrm{Aut}\, A$, z determines a Γ-group A_z (see Example 1 of this section). Now $H^1(\Gamma, \mathrm{PGL}_n(\bar{k}))$ may be identified with the set of k-isomorphism classes of central simple algebras D over k of rank n^2 (see §1.2, Example (5)). z determines some central simple algebra D over k of rank n^2. Let

$$G_{\bar{k}} = \{x \in D \otimes_k \bar{k} | \text{reduced norm of } x = 1\}.$$

Then $A_z \cong G_{\bar{k}}$. The algebraic group $(\mathrm{SL}_n)_z$ is isomorphic over k to $\mathrm{SL}_1(D)$ (the group of elements of D with reduced norm 1).

2.5. Let A be a Γ-group, z and element of $Z^1(\Gamma, A)$. z determines a new Γ-group A_z (see Example 1, §2.4). We define a mapping $\tau_z : H^1(\Gamma, A_z) \to H^1(\Gamma, A)$ as follows: for x in $Z^1(\Gamma, A_z)$, set $(\tau_z x)_s = z_s x_s$ (s in Γ). It can be verified that τ_z induces a mapping $\tau_z : H^1(\Gamma, A_2) \to H^1(\Gamma, A)$ which is a bijection and maps 0 into the element ζ of $H^1(\Gamma, A)$ which contains z.

In order to consider the applications of this procedure, suppose that B is a Γ-group and $f : A \to B$ is a Γ-homomorphism. f induces a mapping f_*^1 from $H^1(\Gamma, A)$ into $H^1(\Gamma, B)$, and it is desirable to determine the fibres of f_*^1. If one has information about the fibre of f_*^1 containing 0 (e.g. by applying the following theorems on exact sequences), then one can obtain information about the fibre containing $\zeta \in H^1(\Gamma, A)$ by applying τ_z for some z in ζ. More precisely, the following diagram is commutative ($t = f^1_*(z)$):

$$\begin{tikzcd}
H^1(\Gamma, A_z) \arrow[r] \arrow[d, "\tau_z"] & H^1(\Gamma, B_t) \arrow[d, "\tau_t"] \\
H^1(\Gamma, A) \arrow[r] & H^1(\Gamma, B).
\end{tikzcd}$$

2.6. *Exact sequences.* Let B be a Γ-group, let A be a subgroup of B, which is invariant under Γ. Let f be the injection $A \to B$. f determines mappings f^i_* ($i = 0, 1$). Also the canonical projection $g: B \to A\backslash B$ induces a mapping g^0_* of $H^0(\Gamma, B)$ into $H^0(\Gamma, A\backslash B)$.

Finally there is a mapping $\delta: H^0(\Gamma, A\backslash B) \to H^1(\Gamma, A)$, which is defined as follows. If $x \in H^0(\Gamma, A\backslash B)$, then x is the coset mod A of an element $b \in B$ which satisfies ${}^sb = a_s b$, where $(a_s) \in Z^1(\Gamma, A)$. Then $\delta(x)$ is the image in $H^1(\Gamma, A)$ of the cocycle a.

PROPOSITION 2.1.

(1) $0 \longrightarrow H^0(\Gamma, A) \xrightarrow{f^0_*} H^0(\Gamma, B) \xrightarrow{g^0_*} H_0(\Gamma, A\backslash B) \xrightarrow{\delta} H^1(\Gamma, A) \xrightarrow{f^1_*} H^1(\Gamma, B)$ *is exact.*

(2) δ *induces a bijection from the set of orbits of* B^Γ *in* $(A\backslash B)^\Gamma$ *onto the kernel of* f^1_*.

(3) ζ *is in the image of* $f^1_* \Leftrightarrow H^0(\Gamma, (A\backslash B)_z) \neq 0$, *where* z *is in* ζ.

Observe that exactness makes sense in this context!

Now suppose that

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

is an exact sequence of Γ-groups (f and g are Γ-homomorphisms), so $f(A)$ is normal in B. This determines a sequence:

$$(3) \quad \begin{aligned} 0 &\longrightarrow H^0(\Gamma, A) \xrightarrow{f^0_*} H^0(\Gamma, B) \xrightarrow{g^0_*} H^0(\Gamma, C) \\ &\xrightarrow{\delta} H^1(\Gamma, A) \xrightarrow{f^1_*} H^1(\Gamma, B) \xrightarrow{g^1_*} H^1(\Gamma, C). \end{aligned}$$

PROPOSITION 2.2.

(1) (3) *is exact;*

(2) g^1_* *is proper* (*respectively injective*) *if* $H^1(\Gamma, A_z)$ *is finite* (*respectively* 0) *for each* z *in* $Z^1(\Gamma, A)$;

(3) $H^1(\Gamma, B) = 0$ *if* $H^1(\Gamma, C) = 0$ *and* $H^1(\Gamma, A) = 0$.

If $f(A)$ is central in B, one can extend (3) to an exact sequence in which $H^2(\Gamma, A)$ occurs. For the proofs of these results (which are easy) we refer to [**6**, Chapter I, §5] or [**1**, §1].

3. **Some results.** We mention here a number of recent results about the Galois cohomology of linear algebraic groups, over special ground fields.

3.1. *Fields of dimension* $\leqq 1$. We say that the field k has *dimension* $\leqq 1$, if the following holds: k has no finite dimensional division algebra extensions. In other words, the Brauer group of any finite extension of k is 0.

The following cohomological characterization explains the name. Let k be a field, let k_s denote its separable closure. Put $\Gamma = \mathrm{Gal}(k_s/k)$. Then k is a field of dimension $\leqq 1$ if and only if $H^2(\Gamma, A) = 0$ for any finite abelian group A on which Γ operates continuously. Examples of fields of dimension $\leqq 1$:

(a) finite fields (Wedderburn),

(b) the maximal unramified extension of a p-adic field (Lang [**4**]),

(c) a function field of dimension 1 whose field of constants is algebraically closed. For further details see [**6**, Chapter II, §3].

We now have the following theorem.

THEOREM 3.1. *Let k be a perfect field of dimension $\leqq 1$, let G be a connected linear algebraic group defined over k. Then $H^1(k, G) = 0$.*

This theorem is proved by Steinberg in [**7**, Theorem 1.9]. In the proof some rather delicate results about semisimple groups are used. We shall say something more about this proof in §4.

The special case of Theorem 3.1 dealing with finite fields was proved by Lang in [**5**], in this case the proof is much easier. The result is then even true for arbitrary connected algebraic groups (nonnecessarily linear).

3.2. *Local fields.* Here one has the following general result.

THEOREM 3.2. *Let k be a local field of characteristic* 0, *let G be a linear* (*not necessarily connected*) *algebraic group which is defined over k. Then $H^1(k, G)$ is finite.*

This result is due to Borel-Serre [**1**, §6]. We shall sketch the proof in §4.

In the next result, the notion of simple connectedness appears. This is defined as follows: Let G be a connected linear algebraic group defined over a field k, which we assume for simplicity to have characteristic 0. Then G is *simply connected* if any surjective homomorphism $f: G_1 \to G$ of a connected linear algebraic group G_1 onto G, which is defined over $\bar{k}$ and has finite kernel, is an isomorphism.

We can now state

THEOREM 3.3. *Let k be a local field of characteristic* 0, *let G be a connected, linear, semi-simple, simply connected algebraic group, which is defined over k. Then $H^1(k, G) = 0$.*

This theorem is due to Kneser [**2**]. His proof is by checking the result for the simple types, and is quite complicated. Another, more conceptual approach to this result was found by Bruhat and Tits. We refer to Tits' report [**8**] in these notes for more details.

Theorem 3.3 can be used to obtain the complete classification of the semisimple groups over local fields of characteristic 0.

3.3. *Number fields.* Let k be an algebraic number field, v a valuation on k, k_v the completion of k at v. Let G be an algebraic group defined over k. Then there is a natural mapping of $H^1(k, G)$ into $H^1(k_v, G)$. Thus we obtain a mapping

$$\phi : H^1(k, G) \to \prod_v H^1(k_v, G). \tag{4}$$

With these notations we have

THEOREM 3.4. *Let G be a linear algebraic group defined over the algebraic number field k. Then ϕ is a proper mapping (i.e. the fibres of ϕ are finite).*

This is also a result of [**1**, §7]. It is a global counterpart of Theorem 3.2. The global counterpart of Theorem 3.3 can only be stated as a conjecture.

CONJECTURE 3.5 (HASSE PRINCIPLE FOR SEMISIMPLE SIMPLY CONNECTED GROUPS). *Let G be a connected, linear, semisimple, simply connected algebraic group, which is defined over the algebraic number field k. Then the mapping ϕ is injective.*

Because of Theorem 3.3 we may in this case replace the product on the right side of (4) by the corresponding product taken over the real valuations of k only.

The present status of this conjecture is discussed in more detail in Kneser's report [**3**].

4. About proofs.

4.1. In this section we want to show on some examples how the machinery of noncummutative cohomology is used to prove results in Galois cohomology. We denote by k a perfect field with algebraic closure $\bar{k}$, let $\Gamma = \mathrm{Gal}(\bar{k}/k)$. If G is a linear algebraic group defined over k, we know that $H^1(k, G)$ may be identified with $H^1(\Gamma, G_{\bar{k}})$ as defined in §2. One can then apply the noncommutative cohomology to the study of $H^1(k, G)$.

As an example of the use of Proposition 2.2 we prove the following result.

PROPOSITION 4.1. *Let G be a connected unipotent linear algebraic group which is defined over the perfect field k. Then $H^1(k, G) = 0$.*

In this case G has a composition series

$$G = G_0 \supset G_1 \supset \cdots \supset G_n \supset G_{n+1} = \{e\},$$

where the G_i are normal subgroups, defined over k, such that G_i/G_{i+1} is k-isomorphic to the additive group G_a.

From Proposition 2.2 we now get an exact sequence

$$H^1(k, G_1) \to H^1(k, G) \to H^1(k, G_a).$$

Now it is well known from Galois theory that $H^1(k, G_a) = 0$. Then induction on n shows that $H^1(k, G) = 0$.

4.2. We next mention an example concerning quadratic forms.

Let k be a field of characteristic different from 2. Let $\mathrm{SO}(n)$ be the rotation group of a nondegenerate quadratic form Q in n variables. The corresponding spin group Spin (n) is defined over k, and is simply connected (for $n \geqq 3$). There is a double covering $1 \to \mu_2 \to \mathrm{Spin}\,(n) \to \mathrm{SO}(n) \to 1$, where $\mu_2 = \{1, -1\}$. Since $H^0(k, \mathrm{Spin}\,(n)) = \mathrm{Spin}\,(n)_k$, $H^0(k, SO(n)) = \mathrm{SO}(n)_k$ and $H^1(k, \mu_2) = k^*/(k^*)^2$ we obtain the exact sequence

$$\mathrm{Spin}\,(n)_k \longrightarrow \mathrm{SO}(n)_k \longrightarrow k^*/(k^*)^2 \xrightarrow{\delta^0} H^1(k, \mathrm{Spin}\,(n)) \longrightarrow H^1(k, \mathrm{SO}(n))$$
$$\xrightarrow{\delta^1} H^2(k, \mu_2).$$

Here $H^2(k, \mu_2)$ may be identified with the subgroup $\mathrm{Br}(k)_2$ of elements of order 2 in the Brauer group, δ^0 is the spinor-norm mapping and δ^1 is connected with the Hasse-invariants of quadratic forms. This sequence provides the following criteria:

$H^1(k, \mathrm{Spin}\,(n)) = 0$ *if and only if* δ^1 *is injective and* δ^0 *is surjective.*

It can be shown that this is the case if k has the following property: every quadratic form in 5 variables over k represents 0 nontrivially. Examples of fields with this property: p-adic fields, totally imaginary algebraic number fields. In this manner, one can prove Theorem 3.3 for $G = \mathrm{Spin}\,(n)$. For more details see [6, Chapter III, 3.2].

4.3. *Proof of Theorem* 3.2. The proof consists of several steps:

(i) Let G be finite and set $\Gamma = \mathrm{Gal}(\bar{k}/k)$. Then some normal subgroup Σ of finite index in Γ keeps $G_{\bar{k}}$ pointwise fixed. A (continuous) cocycle z in $Z^1(\Gamma, G_{\bar{k}})$ induces a homomorphism from Σ into $G_{\bar{k}}$. Using the fact that k has only finitely many extensions of a given degree, one obtains a normal subgroup Σ_0 of Γ of finite index, such that every homomorphism of Σ into $G_{\bar{k}}$ is trivial on Σ_0. It follows that one can identify $H^1(\Gamma, G_{\bar{k}})$ and $H^1(\Sigma_0, G_{\bar{k}})$. The latter set is finite (since Γ/Σ_0 and $G_{\bar{k}}$ are finite).

(ii) Let $G = T$ be a torus (defined over k). Let k be a finite Galois extension of k over which T splits. Let $n = [K : k]$. Let n also denote the nth power mapping from T onto T. We have an exact sequence

$$0 \longrightarrow F \xrightarrow{i} T \xrightarrow{n} T \longrightarrow 0 \qquad \text{(with } F \text{ finite).}$$

Thus the following sequence is exact:

$$H^1(k, F) \xrightarrow{i_*} H^1(k, T) \xrightarrow{n} H^1(k, T).$$

Thus to show that $H^1(k, T)$ is finite, it suffices to show that i_* is surjective. But we can identify $H^1(k, T)$ and $H^1(K/k, T)$ since $H^1(K, T) = 0$. In $H^1(K/k, T)$ the order of each element divides n, hence i^* is surjective.

(iii) Let G be connected and solvable (and defined over k). Then $G = T \cdot G_u$ (semidirect) with T, G_u defined over k (T is a maximal torus, G_u the unipotent part of G). From the exact sequence $1 \to G_u \to G \to T \to 1$ we get the exact sequence

$$H^1(k, G_u) \longrightarrow H^1(k, G) \xrightarrow{\alpha} H^1(k, T).$$

But $H^1(k, G_u) = 0$, so that α is injective (the fibre containing 0 consists of the single point 0 and by twisting, every nonempty fibre consists of a single point). And $H^1(k, T)$ is finite. Thus $H^1(k, G)$ is finite.

(iv) Let G_0 be the connected component of 1 in G. Then $H^1(k, G_0)$ is finite if and only if $H^1(k, G)$ is finite (one direction is trivial, and the other direction is easily proved by applying Proposition 2.2 to $1 \to G_0 \to G \to G/G_0 \to 1$, invoking (i) and using a twisting procedure as in (iii)).

(v) Let G be any algebraic linear group (defined over k). To show that $H^1(k, G)$ is finite, we may assume without loss of generality that G is connected. Let T be a maximal torus of G which is defined over k. Let N be the normalizer of T (thus N is defined over k). Since N_0 is solvable, $H^1(k, N)$ is finite. Thus it suffices to show that the mapping $i_*: H^1(k, N) \to H^1(k, G)$ induced by $i: N \to G$ is surjective. But for this, it suffices to show that for z in $\zeta \in H^1(k, G)$, $H^0(k, (N\backslash G)_z)$ is nonempty (see Proposition 2.1, (3)). But $(N\backslash G)_z$ in the variety of maximal tori of G_z, and since G_z is defined over k, $(N\backslash G)_z$ has a k-rational point (namely any maximal torus defined over k) and $H^0(k, (N\backslash G)_z)$ is nonempty.

4.4. *About the proof of Theorem* 3.1. The following result is proved in [7, Theorem 1.7]:

PROPOSITION 4.2. *Let k be a perfect field, let G be a connected semisimple linear algebraic group which is defined over k and quasi-split over k (i.e. has a Borel subgroup which is defined over k). Then any semisimple conjugacy class of G which is defined over k contains an element of G_k.*

From this one obtains the following result (Theorem 1.8 of [7]).

PROPOSITION 4.3. *Under the same assumptions, there exists for every $\zeta \in H^1(k, G)$ a maximal torus T of G, defined over k, such that $\zeta \in \operatorname{Im}(H^1(k, T) \to H^1(k, G))$.*

We indicate how Proposition 4.2. implies Proposition 4.3. Take $\zeta \in H^1(k, G)$ and let z be a corresponding cocycle. We wish to construct T from z. The twisted group G_z is defined over k and contains therefore a maximal torus T' which is defined over k. Since $(T')_k$ is Zariski-dense in T', we can find a regular element $x \in T'_k$. Then $x \in G_{\bar{k}}$, and for $s \in \Gamma = \operatorname{Gal}(\bar{k}/k)$ we have

$$^s x = z_s x z_s^{-1}.$$

This means that the conjugacy class of x in G is defined over k. By Proposition 4.2, there is an element y of G_k in this conjugacy class. The centralizer T of y in G is a maximal torus of G, which is defined over k, and it follows that z is cohomologous with a cocycle which takes its values in $T_{\bar{k}}$.

From Proposition 4.3 one obtains that, in order to prove Theorem 3.1 for a semisimple group which is quasi-split over k, it suffices to prove Theorem 3.1 for the case that G is a *torus*. In that case one can use an argument like that of 4.3, (ii). The case of a general G now follows without too much difficulty.

References

1. A. Borel and J.-P. Serre, *Théorèmes de finitude en cohomologie galoisienne*, Comme. Math. Helv. **39** (1964), 111-164.

2. M. Kneser, *Galois-Kohomologie halbeinfacher algebraischer Gruppen über p-adischen Körpern.* I, Math. Z. **88** (1965), 40–47; II, ibid. **89** (1965), 250–272.

3. ———, *Hasse principle for H^1 of simply connected groups*, Proc. Sympos. Pure Math., vol. 9, Amer. Math. Soc., Providence, R.I., 1966, pp. 159–163.

4. S. Lang, *On quasi-algebraic closure*, Ann. of Math. **55** (1952), 373–390.

5. ———, *Algebraic groups over finite fields*, Amer. J. Math. **78** (1956), 555–563.

6. J.-P. Serre, *Cohomologie galoisienne*, Springer Verlag, Berlin, 1964.

7. R. Steinberg, *Regular elements of semi-simple algebraic groups*, Publ. Math. I. H. E. S. no. 25 (1965), 49–80.

8. J. Tits, *Classification of algebraic semisimple groups*, Proc. Sympos. Pure Math., vol. 9, Amer. Math. Soc., Providence, R.I., 1966, pp. 33–62.

Hasse Principle for H^1 of Simply Connected Groups

BY

MARTIN KNESER

Let G be a simply connected algebraic group defined over the number field k.

CONJECTURE. *The canonical mapping*

$$H^1(k, G) \to \prod_{v \in \infty} H^1(k_v, G)$$

is injective.

The finite places can be omitted from the product because in that case

$$H^1(k_v, G) = 0.$$

It is not hard to show that the map is also surjective.

The proof of the conjecture is easily reduced to the absolutely almost simple case. This has been done in all cases except E_8, and we shall sketch some of these proofs. In [4] Veisfeiler announced the result that a group which is quasi-split locally everywhere is quasi-split globally. This would imply the Hasse principle for the case E_8 too, but the proofs for this result have not appeared as yet.

Two consequences of the Hasse principle would be:

(1) *If k is purely imaginary, then $H^1(k, G) = 0$.*

(2) *All anisotropic simple groups are of type A_n if k is purely imaginary.*

Consider first the case of inner forms of type A_n. Then G consists of the elements of reduced norm 1 in a central simple algebra A, and so we have an exact sequence

$$1 \longrightarrow G \longrightarrow A^* \xrightarrow{N} G_m \longrightarrow 1.$$

This gives rise to the commutative diagram

$$\begin{tikzcd}
A_k^* \arrow[r, "N"] \arrow[d] & k^* \arrow[r] \arrow[d] & H^1(k, G) \arrow[r] \arrow[d] & H^1(k, A^*) = 0 \arrow[d] \\
A_{k_v}^* \arrow[r, "N"] & k_v^* \arrow[r] & H^1(k_v, G) \arrow[r] & 0
\end{tikzcd}$$

with exact rows. Now suppose ζ in $H^1(k, G)$ goes onto 0 in $H^1(k_v, G)$ for all v, and let $a \in k^*$ be a pre-image of ζ. Then the image of a in k_v^* is a norm at each v, and hence a is a global norm by the norm theorem for simple algebras (see e.g. [1]). It follows that $\zeta = 0$ as required.

Next consider exterior forms of type A_n. In this case

$$G = \{x \in A | xx^I = 1, Nx = 1\}$$

where A is a central simple algebra over a quadratic extension K of k, with an involution I of the second kind.

Consider the map $x \mapsto (xx^I, Nx)$ of A^*. The image S is not a group, but is a homogeneous space under A^*:

$$S = \{(y, z) \in A^* \times A^* | y^I = y, z \in \text{center}, Ny = zz^I\}.$$

Now

$$1 \to G \to A^* \to S \to 1$$

is exact and we get the commutative diagram

$$\begin{tikzcd}
A_k^* \arrow[r] \arrow[d] & S_k \arrow[r] \arrow[d] & H^1(k, G) \arrow[r] \arrow[d] & 1 \arrow[d] \\
A_{k_v}^* \arrow[r] & S_{k_v} \arrow[r] & H^1(k_v, G) \arrow[r] & 1
\end{tikzcd}$$

with exact rows. If ζ in $H^1(k, G)$ goes onto 0 in all $H^1(k_v, G)$, and $s \in S_k$ is a preimage, then s is in the image of $A_{k_v}^* \to S_{k_v}$ for all v. The fact that s is in the image of $A_k^* \to S_k$ is a consequence of the following two lemmas.

LEMMA 1. *If $y = y^I \in A_k^*, y = x_v x_v^I (x_v \in A_{k_v}^*)$ for all v, then for some x in A_k^*, $y = xx^I$.*

This was first proved by Landherr [3]; a simpler proof using strong approximation for inner type A_n groups is due to Springer and the author.

LEMMA 2. *If $z \in K$, $zz^I = 1$, and if $z = Nx_v$ with $x_v x_v^I = 1$ $(x_v \in A_{k_v}^*)$ for all v, then $z = Nx$ for some x in A_k^* with $xx^I = 1$.*

The groups of types B_n, C_n and D_n (except the trialitarian D_4) can be handled using the isomorphisms with groups of type A_n in low dimensions, and also the known versions of the Hasse principle for quadratic forms, hermitian forms, etc. The rest of this lecture will be devoted to a sketch of the proof for the exceptional groups D_4, E_6, E_7 based on a forthcoming paper [2] of Harder. Parts of the proof are also valid for E_8. The proofs for F_4 and G_2 are comparatively easy and will not be discussed here.

The proof is by induction on the dimension of the group; we shall use consequence (2) of the Hasse principle in the induction procedure. First we state a few lemmas without proof.

LEMMA 3. *Let k be perfect and G be semisimple, connected, with a maximal torus T, all defined over k. Then if the p-primary component $H^1(k, T)_p$ is nonzero, we must have $p \in P(G)$ where $P(G)$ is the set of primes in the following table.*

Type of G	A_n	B_n, C_n, D_n	D_4, E_6, E_7, F_4, G_2	E_8
primes in $P(G)$	$p \vert (n + 1)a$	2	2, 3	2, 3, 5

with $a = 2$ for the outer type of A_n, otherwise $a = 1$, and D_n does not include the trialitarian D_4.

In the next lemma $cd_pk \leqq 1$ means that the p-primary component of the Brauer group of any finite extension of k is trivial.

LEMMA 4. *With k and G as in Lemma 3 and if $cd_pk \leqq 1$ for all $p \in P(G)$, then $H^1(k, G) = 0$ (in particular G is k-quasi-split).*

Under the stronger hypothesis of $cdk \leqq 1$, this is due to Steinberg (see Theorem 3.1 of Springer's lecture on Galois Cohomology, pp. 149–158); using Lemma 3, one can prove Lemma 4 in essentially the same way.

LEMMA 5. *If k is a number field and p is a prime, the field $k^{(p)}$ generated over k by all p^n roots of unity ($n = 1, 2, \cdots$) satisfies $cd_pk^{(p)} \leqq 1$.*

Now we return to the proof of the Hasse principle for the groups of type $D_4, E_6, E_7, (E_8)$. G is again absolutely almost simple. Suppose that G is obtained from the quasi-split group G_1 by means of an inner twist: $G = {}_aG_1$ with $a \in H^1(k, \mathrm{Ad}\, G_1)$. Given b in $H^1(k, G)$ which splits locally at each place, we must show that it splits globally, i.e. $b = 0$.

Let $\delta : H^1(k, \mathrm{Ad}\, G_1) \to H^2(k, C_1)$ be the connecting map of the cohomology sequence of the exact sequence

$$1 \to C_1 \to G_1 \to \mathrm{Ad}\, G_1 \to 1.$$

The rest of the proof consists in taking a series of extensions

$$k = k_0 \subset k_1 \subset k_2 \subset \cdots \subset k_n$$

such that each extension is cyclic of degree 2 or 3, and such that a and b split over k_n. Then one works down from k_n to k_0, one step at a time, showing at each stage that b still splits, thus finally achieving $b = 0$ over k.

The first extension k_1/k_0 is a purely imaginary one of degree 2, chosen so that $\delta a \in H^2(k, C_1)$ splits, if possible (namely in all cases but E_6).

The next extension k_2/k_1 is the quadratic extension contained in the minimal splitting field of G_1, if it exists—otherwise $k_2 = k_1$.

The third extension k_3/k_2 is of degree 3 and splits G_1 completely in case D_4 and splits δa in case E_6; in all other cases $k_3 = k_2$.

The remaining extensions k_i/k_{i-1} ($i \geqq 4$) are extensions by 2^mth and 3^mth roots of unity and are chosen (by Lemmas 4 and 5) to split a and b (so in particular G is split over k_n). It is at this point that the proof breaks down for E_8, and so it is omitted from further consideration.

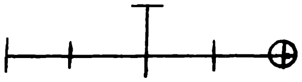
Now we begin the descent back to $k = k_0$, showing that b still splits at each stage. The procedure is to use induction on the dimension of the group, and the following lemma for the extensions $k_i/k_{i-1}, i \geqq 2$.

LEMMA 6. *Let G be simply connected of type D_4 or E_n, let l be a purely imaginary field, and let m be a cyclic quadratic or cubic extension of l. Then $H^1(m/l, G = 0$ if at least one of the following holds)*

(i) *G splits over m.*

(ii) *G is quasi-split over m, of type D_4, and $[m:l] = 2$.*
(iii) *G is isotropic over m, of type E_6, and $[m:l] = 2$.*

The proof is a lengthy case by case consideration. As a typical case we sketch the proof for E_6, $[m:l] = 3$, and G split over m. Let $b \in H^1(m/l, G)$. Let P be a maximal subgroup defined over m, corresponding to the circled root in the diagram

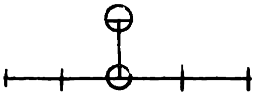


Since $\dim P = 62$, $\dim E_6 = 78$, we have

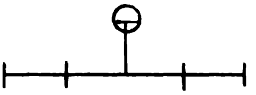
$$(*) \qquad \dim \bigcap_{\sigma\in\Gamma} P^\sigma \geqq 30$$

where Γ is the Galois group of m/l. It follows that G is isotropic over l. For if not, $\bigcap P^\sigma$ is reductive and its semisimple part is a subgroup of a group of type D_5, which yields a contradiction to (*).

By consequence (2) of the Hasse principle, the anisotropic kernel of G must consist of groups of type A_n. There are therefore two possibilities for G: it is either split over l or has Dynkin–Tits diagram



So there exists a parabolic subgroup Q defined over l corresponding to the circled root



Let Q' be a similar parabolic subgroup of ${}_bG$. Then we can change the twisting isomorphism $G \to {}_bG$ so that Q is mapped onto Q'. Then b is replaced by a cocycle of $N(Q) = Q$ and so is in $H^1(l, Q)$. This latter cohomology set is a homomorphic image of $H^1(l, Q^*)$ where Q^* is the semisimple part of Q. Since Q^* is simply connected, $H^1(l, Q^*)$ is zero by induction, and so $b = 0$ as required.

The remaining steps in the proof are concerned with descending from k_1 to k_0.

Part 7. One next finds a "nice" maximal k-torus contained in both G and ${}_bG$. More precisely there is maximal k-torus T in G and a twisting isomorphism $f: G \to {}_bG$ such that $(f^{-1} \circ {}^sf)|T = id_T$, which satisfies additional properties; for example in the case of E_7 and E_8, T is anisotropic over k and splits over k_1. One consequence is that $b = i^*(c)$ for some c in $H^1(k, T)$, where i is the inclusion map of T in G.

Part 8. Find $c' \in H^1(k, T)$ which splits in $H^1(k, G)$ and such that the local components c_v and c'_v of c and c' are equal for all infinite places v. Then twisting by means of c' reduces the proof to the special case $c_v = 0$ for all $v \in \infty$.

Part 9. To conclude the proof we must show such a c splits in $H^1(k, G)$. This is done by imbedding T in smaller subgroups, for instance in case E_7 (resp. E_8) in groups of type $A_2 \times A_5$ (resp. A_8).

References

1. M. Eichler, *Über die Idealklassenzahl hyperkomplexer Systeme*, Math. Z. **43** (1938), 481–494.

2. G. Harder, *Über die Galoiskohomologie halbeinfacher Matrizengruppen*. I, Math. Z. **90** (1965), 404–428; II (to appear).

3. W. Landherr, *Über einfache Liesche Ringe*, Abh. Math. Sem. Univ. Hamburg **11** (1936), 41–64.

4. B. Ju. Veĭsfeĭler, *Classification of semi-simple Lie algebras over a* 𝔭*-adic field*, Dokl. Akad. Nauk SSSR **158** (1964), 258–260 = Soviet Math. Dokl. **5** (1964), 1206–1208.

Nonabelian H^2 in Galois Cohomology

BY

T. A. SPRINGER

It is the purpose of the present paper to give a brief account of some results in the Galois cohomology of algebraic groups which involve the nonabelian H^2.

Such results presuppose, of course, a definition of H^2. This is a problem in itself, recent solutions of which have been given by Dedecker [2] for group cohomology and by Giraud [3] in a much more general situation.

Section 1 of the present paper contains an independent exposition of the definition and basic properties of a nonabelian H^2 in group cohomology. This definition seems to be essentially equivalent to that of Dedecker and Giraud. Section 1 also contains the definition of a relative H^1, which is useful in Galois cohomology. We develop to some extent the machinery of exact sequences for the relative H^1 and H^2.

The main result of the paper is Theorem 3.4, which states that, to a certain extent, the nonabelian H^2 in Galois cohomology can be reduced to that of finite nilpotent groups. A consequence is the theorem of Grothendieck asserting that the nonabelian Galois 2-cohomology is trivial over perfect fields of dimension $\leqq 1$.

Section 4 gives some finiteness theorems for the relative H^1 over local fields and number fields. They are rather direct consequences of the corresponding results of Borel-Serre [1] for the ordinary H^1.

The main results of this paper were obtained in 1963, after the author had heard about Grothendieck's theorem, mentioned above.

1. **Relative H^1 and H^2 in group cohomology.**

1.1. *Notations.* We follow here the notations of [1]. In particular, $\mathfrak{g}$ denotes a topological group and a $\mathfrak{g}$-set is a *discrete* topological space on which $\mathfrak{g}$ operates continuously on the left.

In discussing the properties of the relative H^1 and H^2 we shall sometimes encounter here relations (i.e. "many-valued mappings") between cohomology sets, which reduce to mappings in ordinary cohomology. As in [3], we denote a relation r between two sets A and B which is not a mapping by

$$A \overset{r}{\longrightarrow\!\!\circ}\, B.$$

If A and/or B have privileged subsets, there is an obvious way of defining an exact sequence of relations. These will occur here, however in our examples all relations but at most one will be mappings.

1.2. *Homogeneous spaces.* Let A be a $\mathfrak{g}$-group. A *right homogeneous space* of A is a nonempty $\mathfrak{g}$-set H on which A acts transitively on the right, the action being compatible with $\mathfrak{g}$. It is clear how to define the notion of isomorphism of two homogeneous spaces.

Let H be a homogeneous space, let $x \in H$. The elements $b \in A$ such that $x \cdot b = x$ form a subgroup B of A, the *isotropy group* of x. Since A acts transitively on H, the isotropy subgroups of any two points of H are conjugate in A. Now let B be any subgroup of A. We define the *relative* 1-*cohomology set of A with respect to B* as the set of isomorphism classes of homogeneous spaces of A which have B as the isotropy subgroup of one of its points. We denote this set by $H^1(\mathfrak{g}, A, B)$.

If B is reduced to the identity, $H^1(\mathfrak{g}, A, B)$ coincides with $H^1(\mathfrak{g}, A)$. If B is a $\mathfrak{g}$-invariant subgroup of A, there is a privileged element 0 in $H^1(\mathfrak{g}, A, B)$, namely the element defined by the $\mathfrak{g}$-set $B\backslash A$. Also notice that there is a canonical bijection of $H^1(\mathfrak{g}, A, B)$ onto $H^1(\mathfrak{g}, A, aBa^{-1})$.

In order for $H^1(\mathfrak{g}, A, B)$ to be nonempty, B has to satisfy certain conditions, which we will make explicit now. Let H be a homogeneous space of A; let $x \in A$ have the isotropy group B. There exists by the transitivity of A elements $a_s \in A$ such that ${}^s x = x \cdot a_s$. It is easily seen (since the isotropy subgroup of x in $\mathfrak{g}$ is an open subgroup) that we may take a_s such, that $s \mapsto a_s$ is a continuous function of $\mathfrak{g}$ into A.

We have for $b \in B$

$$x \cdot a_s = {}^s x = {}^s(xb) = x \cdot a_s {}^s b;$$

moreover

$$x \cdot a_{st} = {}^{st}x = {}^s(x \cdot a_t) = x \cdot a_s {}^s a_t (s, t \in \mathfrak{g});$$

whence

(1) $$ {}^s B = a_s^{-1} B a_s,$$

(2) $$a_s {}^s a_t a_{st}^{-1} \in B.$$

Denote by $Z^1(\mathfrak{g}, A, B)$ the set of continuous functions $a = (a_s)$ of $\mathfrak{g}$ into A satisfying (1) and (2).

Let N be the normalizer of B in A. We call two elements a, a' of $Z^1(\mathfrak{g}, A, B)$ *cohomologous* if there exists $n \in N$ such that

(3) $$a'_s \in Bn^{-1} a_s {}^s n.$$

It is readily seen that (3) defines an equivalence relation R on $Z^1(\mathfrak{g}, A, B)$.

1.3. PROPOSITION. *There is a bijection $\varepsilon: H^1(\mathfrak{g}, A, B) \to Z^1(\mathfrak{g}, A, B)/R$.*

Let H be a homogeneous space of A, suppose that $x \in H$ has isotropy group B. We have associated with x a cocycle a in $Z^1(\mathfrak{g}, A, B)$. a_s is determined by x up to the left multiplication by an element of B. On the other hand if we start instead of x with a point $y \in H$ whose isotropy subgroup is also B, then we have $y = x \cdot n$

with $n \in N$. Then if a' is defined by $a'_s = n^{-1}a_s{}^s n$ we have ${}^s y = y \cdot a'_s$. From this we infer that the class of a mod R is uniquely determined by H. This gives our map ε. The injectivity of ε follows readily. To prove surjectivity, take $a \in Z^1(\mathfrak{g}, A, B)$. Define $H = B\backslash A$ and make this into a $\mathfrak{g}$-set by defining ${}^s(Ba) = B \cdot a_s{}^s a$. The cocycle relations (1) and (2) imply that H becomes indeed a $\mathfrak{g}$-set. It is easy to check that H is mapped by ε onto the class of a.

1.4. COROLLARY. *If B is a $\mathfrak{g}$-invariant normal subgroup of A, then ε defines a bijective map of $H^1(\mathfrak{g}, A, B)$ onto $H^1(\mathfrak{g}, A/B)$.*

This follows from the cocycle description of $H^1(\mathfrak{g}, A, B)$, since now $Z^1(\mathfrak{g}, A, B)/R$ is readily seen to be the same thing as $H^1(\mathfrak{g}, A/B)$.

1.5. *Change of subgroup.* Let A be a $\mathfrak{g}$-group, let B and C be two subgroups of A. We say that the homogeneous space $H \in H^1(\mathfrak{g}, A, C)$ *dominates* the homogeneous space $K \in H^1(\mathfrak{g}, A, B)$ if there exists a mapping $f: H \to K$ of right homogeneous spaces of A, compatible with $\mathfrak{g}$.

It is easily seen that if this is the case, C must be conjugate in A to a subgroup of B. So we may assume, without loss of generality, that $C \subset B$. This we shall do from now on.

If we describe K by a cocycle a in $Z^1(\mathfrak{g}, A, B)$ then K is dominated by an $H \in H^1(\mathfrak{g}, A, C)$ if and only if a is cohomologous to a cocycle a' such that

$$(4) \qquad {}^sB = a_s'^{-1}Ba'_s, {}^sC = a_s'^{-1}Ca'_s, \ a'_s{}^s a'_t a_{st}'^{-1} \in C.$$

Domination gives a *relation* $p^1_*(B, C)$ between $H^1(\mathfrak{g}, A, C)$ and $H^1(\mathfrak{g}, A, B)$. If B and C are $\mathfrak{g}$-invariant normal subgroups of A we may identify, according to Corollary 1.4, $H^1(\mathfrak{g}, A, B)$ and $H^1(\mathfrak{g}, A, C)$ with $H^1(\mathfrak{g}, A/B)$ and $H^1(\mathfrak{g}, A/C)$, respectively. It may be shown that one may identify $p^1_*(B, C)$ with the mapping of $H^1(\mathfrak{g}, A/C)$ into $H^1(\mathfrak{g}, A/B)$, associated with the canonical homomorphism of A/C onto A/B.

A special case is that C is reduced to the identity. In that case we write $p^1_*(B)$ instead of $p^1_*(B, C)$.

The relation $p^1_*(B, C)$ enjoys "functorial" properties, we mention only that $p^1_*(B, B)$ is the identity mapping of B and that p if $D \subset C \subset B$ we have $p^1_*(B, D) = p^1_*(B, C) \circ p^1_*(C, D)$.

1.6. PROPOSITION. *Let $a = (a_s) \in Z^1(\mathfrak{g}, A)$. Let A_a be the group obtained by twisting A with a.*

(i) *If $b \in Z^1(\mathfrak{g}, A_a, B)$, then $(b_s a_s) \in Z^1(\mathfrak{g}, A, B)$ and one obtains a bijection*

$$t_a: Z^1(\mathfrak{g}, A_a, B) \to Z^1(\mathfrak{g}, A, B),$$

which defines a bijection

$$\tau_a: H^1(\mathfrak{g}, A_a, B) \to H^1(\mathfrak{g}, A, B).$$

(ii) *If $C \subset B$, then the diagram*

$$\begin{tikzcd} H^1(\mathfrak{g}, A_a, C) \arrow[r, "p^1_*(B,C)"] \arrow[d, "\tau_a"'] & H^1(\mathfrak{g}, A_a, B) \arrow[d, "\tau_a"'] \\ H^1(\mathfrak{g}, A, C) \arrow[r, "p^1_*(B,C)"] & H^1(\mathfrak{g}, A, B) \end{tikzcd}$$

is commutative.

(i) is proved like Proposition 1.5 of [1] and (ii) is a direct check.

1.7. Let A be a $\mathfrak{g}$-group, let B be a subgroup of A. We want to describe the fibers of the relation $p^1_*(B)$ between $H^1(\mathfrak{g}, A)$ and $H^1(\mathfrak{g}, A, B)$. We write now p^1_* instead of $p^1_*(B)$.

If $\beta \in H^1(\mathfrak{g}, A, B)$ is related to an element α of $H^1(\mathfrak{g}, A)$, then β can be represented by a cocycle $a \in Z^1(\mathfrak{g}, A, B)$ which lies in $Z^1(\mathfrak{g}, A)$, represents α and is such that

$$^sB = a_s^{-1}Ba_s.$$

Hence if we twist A with a, B is invariant for the twisted action of $\mathfrak{g}$ on the set A. We write B_a for the $\mathfrak{g}$-group obtained in this manner. Also, we may twist N with a, we denote the resulting $\mathfrak{g}$-group by N_a.

First assume $\alpha = 0$, so B is $\mathfrak{g}$-invariant. Now $p^1_*(0)$ consists of those elements of $H^1(\mathfrak{g}, A, B)$ which can be represented by cocycles $(b_s) \in Z^1(\mathfrak{g}, A, B)$ of the form $b_s = a^{-1}(^sa)$ with $a \in A$. From (1) we find that $a_s \in N$. It follows that there exists a surjective map

$$\rho : \mathrm{Ker}(H^1(\mathfrak{g}, N) \to H^1(\mathfrak{g}, A)) \to p^1_*(0).$$

Moreover one verifies that two elements of $H^1(\mathfrak{g}, N)$ lie in the same fiber of ρ if and only if they have the same image in $H^1(\mathfrak{g}, N/B)$ (under the mapping associated with the canonical projection of N onto N/B).

From the preceding results one obtains by twisting, using Proposition 1.6, the following result:

1.8. PROPOSITION. *Let $\alpha \in H^1(\mathfrak{g}, A)$, suppose $p^1(\alpha) \neq \varnothing$, let a be a cocycle representing α. There is a surjective map*

$$\rho_a : \mathrm{Ker}(H^1(\mathfrak{g}, N_a) \to H^1(\mathfrak{g}, A_a)) \to p^1_*(\alpha).$$

Two elements of $H^1(\mathfrak{g}, N_a)$ lie in the same fiber of ρ_a if and only if they have the same image in $H^1(\mathfrak{g}, N_a/B_a)$.

1.9. With the same notation, take now $\beta \in H^1(\mathfrak{g}, A, B)$. We want to give a description of $(p^1_*)^{-1}(\beta)$. Assume first that $\beta \in p^1_*(0)$. Let b be a cocycle representing β.

We then have

$$B = {}^sB = b_s^{-1}Bb_s.$$

Hence $b_s \in N$. Moreover we may assume that b is in $Z^1(\mathfrak{g}, N)$. We denote by A_b

(resp. B_b) the $\mathfrak{g}$-groups obtained by twisting A with the canonical image of b in $Z^1(\mathfrak{g}, A)$ (resp. obtained by twisting B with b; this makes sense since N acts on B via inner automorphisms in A).

The $\alpha \in H^1(\mathfrak{g}, A)$ which are related to β are those elements which can be represented by a cocycle of the form

$$a_s = n^{-1}c_s b_s {}^s n,$$

where $c_s \in B$. It follows that $(c_s) \in Z^1(\mathfrak{g}, B_b)$, $(a_s) \in Z^1(\mathfrak{g}, A_b)$. One then finds the following description:

1.10. Proposition. *Let $\beta \in H^1(\mathfrak{g}, A, B)$, suppose $\beta \in p_*^1(0)$; let b be a cocycle representing β which lies in $Z^1(\mathfrak{g}, N)$. There is a bijective map ρ of $(p_*^1)^{-1}(\beta)$ onto* $\operatorname{Im}(H^1(\mathfrak{g}, B_b) \to H^1(\mathfrak{g}, A_b))$.

An arbitrary fiber can be found from this result by twisting A suitably, using Proposition 1.6.

1.11. Proposition. *Let B be a $\mathfrak{g}$-invariant subgroup of the $\mathfrak{g}$-group A, denote by i the injection map $B \to A$. Then the sequence*

$$H^1(\mathfrak{g}, B) \xrightarrow{i_*^1} H^1(\mathfrak{g}, A) \xrightarrow{p_*^1} H^1(\mathfrak{g}, A, B)$$

is exact.

(Notice that $H^1(\mathfrak{g}, A, B)$ has now an element 0, so exactness makes sense.)

We leave the proof of this fact to the reader. The fibers of p_*^1 have been described in Propositions 1.8 and 1.10. i_*^1 is the induced map, defined in [**1**]. Its fibers are described in [**1**], §1.12.

1.12. *Kernels.* Let A be a group (not necessarily a $\mathfrak{g}$-group). We denote by $\operatorname{Aut}(A)$ (resp. $\operatorname{Int}(A)$) the group of automorphisms (resp. inner automorphisms) of A. We put $E(A) = \operatorname{Aut}(A)/\operatorname{Int}(A)$. Let π be the projection $\operatorname{Aut}(A) \to E(A)$.

A $\mathfrak{g}$-kernel in A is a continuous homomorphism of $\mathfrak{g}$ into $E(A)$, it being understood that $E(A)$ has the discrete topology. The $\mathfrak{g}$-kernel κ is called *trivial* if there exists a continuous homomorphism $\phi: \mathfrak{g} \to \operatorname{Aut}(A)$ such that $\kappa = \pi \circ \phi$, in other words if κ is induced by a $\mathfrak{g}$-group structure on A (in this case the one determined by ϕ). A particular case is the *kernel* 0, which corresponds to the case that ϕ is the trivial mapping (sending $\mathfrak{g}$ into the identity element of $\operatorname{Aut}(A)$). It is clear that if A is *abelian*, any $\mathfrak{g}$-kernel in A is trivial.

Let $\mathfrak{g}$ and $\mathfrak{g}'$ be two topological groups, let $\lambda: \mathfrak{g}' \to \mathfrak{g}$ be a continuous homomorphism. Let κ and κ' be a $\mathfrak{g}$-kernel in A resp. a $\mathfrak{g}'$-kernel in A'. A homomorphism $\mu: A \to A'$ is called a *homomorphism of κ into κ', compatible with λ* if the following holds: there exist continuous functions

$$\alpha: \mathfrak{g} \to \operatorname{Aut(A)} \ (\alpha': \mathfrak{g}' \to \operatorname{Aut}(A'))$$

such that

(i) $\kappa = \pi \circ \alpha$ (resp. $\kappa' = \pi \circ \alpha'$),

(ii) $\mu(\alpha(\lambda(s'))a) = \alpha'(s')\mu(a)$ if $a \in A$, $s' \in \mathfrak{g}'$.

1.13. *Group extensions.* Let A be a discrete group. A triple (E, i, p) consisting of a topological group E together with continuous homomorphisms $i: A \to E$, $p: E \to g$, is called an *extension of g* by A if

$$0 \longrightarrow A \xrightarrow{i} E \xrightarrow{p} g \longrightarrow 0$$

is an exact sequence of topological groups (hence i is an isomorphism of A onto a closed subgroup of E and p is an open mapping). A *homomorphism* of an extension (E, i, p) of g by A into the extension (E', i', p') of g by A' is a pair of continuous homomorphisms $\mu: A \to A'$, $\nu: E \to E'$, such that the following diagram commutes:

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "i"] \arrow[d, "\mu"] & E \arrow[r, "p"] \arrow[d, "\nu"] & g \arrow[r] \arrow[d, "\mathrm{id}"] & 0 \\
0 \arrow[r] & A' \arrow[r, "i'"] & E' \arrow[r, "p'"] & g \arrow[r] & 0.
\end{tikzcd}$$

An *isomorphism* of the extension (E, i, p) onto the extension (E', i', p'), both of g by A, is a homomorphism as defined above, with $\mu = \mathrm{id}$. Isomorphy of extensions is an equivalence relation.

The extension (E, i, p) of g by A is called a *split extension* if there exists a continuous homomorphism $q: g \to E$ such that $p \circ q = \mathrm{id}$.

We assume in the sequel always that the group extensions (E, i, p) satisfy the following condition:

(CS) *There exists a continuous section $\sigma: g \to E$.*

(This condition is automatically verified if g is discrete or profinite.)

One can then, as is well known, describe the extension by means of a factor system. We shall return to this in §1.14.

First we want to observe that an extension of g by A defines a g-kernel κ in A. As is also well known one defines $\kappa(s)$ to be the image in $E(A)$ of the automorphism of A, determined by the automorphism

$$x \mapsto \sigma(s)^{-1} x \sigma(s)$$

of E, where σ is a continuous section.

We call this kernel κ the g-kernel in A *associated* with the given extension.

A kernel which is associated with some extension is called *extendible.* (In order for κ to be extendible it is necessary and sufficient that a certain element of $H^3(g, C)$ vanishes, where C is the center of A.)

Examples of extendible kernels are the *trivial* ones (which are associated with the split extensions), in particular the zero kernel.

1.14. *Definition of H^2.* Let A be a group, let κ be a g-kernel in A. We define as follows the cohomology set $H^2(g, A, \kappa)$ of g in A with respect to the kernel κ : *$H^2(g, A, \kappa)$ is the set of isomorphy classes of extensions of g by A, which satisfy* (CS) *and whose associated kernel is κ.*

Notice that $H^2(\mathfrak{g}, A, \kappa)$ may be empty, viz. if κ is not extendible. If κ is trivial $H^2(\mathfrak{g}, A, \kappa)$ has a privileged element 0, namely the class of the split extension of $\mathfrak{g}$ by A.

If A is *abelian* it is well known that our $H^2(\mathfrak{g}, A, \kappa)$ is the same thing as the usual $H^2(g, A)$, where $\mathfrak{g}$ acts on A via κ (which is now a homomorphism of $\mathfrak{g}$ into $\operatorname{Aut}(A)$; hence makes A into a $\mathfrak{g}$-group).

We come now to the cocycle description of $H^2(\mathfrak{g}, A, \kappa)$. Let $Z^2(\mathfrak{g}, A, \kappa)$ be the set of pairs (f, g) of continuous mappings

$$f : \mathfrak{g} \times A \to A, \; g : \mathfrak{g} \times \mathfrak{g} \to A$$

(denoted by $(s, a) \mapsto f_s(a)$, $(s, t) \mapsto g_{s,t}$), such that

(i) for $s \in \mathfrak{g}$, $a \mapsto f_s(a)$ is an automorphism of A, whose class mod $\operatorname{Int}(A)$ is $\kappa(s)$;

(5) (ii) $f_s(f_t(a)) = g_{s,t} f_{st}(a) g_{s,t}^{-1}$;

(iii) $f_r(g_{s,t}) g_{r,st} = g_{r,s} g_{rs,t}$.

Define an equivalence relation R on $Z^2(\mathfrak{g}, A, \kappa)$ as follows: (f, g) is equivalent to (f', g') if there exists a continuous function $h : \mathfrak{g} \to A$, such that

(6) (i) $f'_s(a) = h_s f_s(a) h_s^{-1}$,

(ii) $g'_{s,t} = h_s f_s(h_t) g_{s,t} h_{st}^{-1}$.

1.15. Proposition. *There exists a bijective mapping of* $H^2(\mathfrak{g}, A, \kappa)$ *onto* $Z^2(\mathfrak{g}, A, \kappa)/R$.

This is a familiar result from the theory of group extensions, so we omit the proof.

Henceforth we identify $H^2(\mathfrak{g}, A, \kappa)$ and $Z^2(\mathfrak{g}, A, \kappa)/R$.

1.16. Let κ be a $\mathfrak{g}$-kernel in A. Let C be the center of A. Then κ determines a g-kernel in C, which is a *trivial* one (since the inner automorphisms of A act trivially on C). We denote this kernel in C also by κ. $H^2(\mathfrak{g}, C, \kappa)$ is then an ordinary cohomology group.

1.17. Proposition. $H^2(\mathfrak{g}, A, \kappa)$, *if nonempty, is a principal homogeneous space over* $H^2(\mathfrak{g}, C, \kappa)$.

In other words, $H^2(\mathfrak{g}, C, \kappa)$ acts on $H^2(\mathfrak{g}, A, \kappa)$ in a simply transitive way.

Take two cocycles (f, g) and (f', g') in $Z^2(\mathfrak{g}, A, \kappa)$. We may assume, replacing if necessary the second one by an equivalent cocycle, that $f = f'$. Then $g' = gh$, where h is a cocycle of g in the commutative $\mathfrak{g}$-group C. One verifies that the element of $H^2(\mathfrak{g}, C, \kappa)$ defined by h depends only on the cohomology classes of (f, g) and (f', g'). Conversely, if (f, g) is given and if h is a 2-cocycle of $\mathfrak{g}$ in the abelian group C, then (f', g') with $f = f'$, $g' = gh$ is in $Z^2(\mathfrak{g}, A, \kappa)$. This defines an action of $H^2(\mathfrak{g}, C, \kappa)$ on $H^2(\mathfrak{g}, A, \kappa)$, which is simply transitive.

Remark. If κ is trivial, then there exists a privileged element 0 in $H^2(\mathfrak{g}, A, \kappa)$, via which we can make a canonical identification of the set $H^2(\mathfrak{g}, A, \kappa)$ with the set $H^2(\mathfrak{g}, C, \kappa)$.

1.18. *Relation defined by homomorphism of kernels.* Let κ, κ' be a $\mathfrak{g}$-kernel in A resp. a $\mathfrak{g}'$-kernel in A', let $\lambda : \mathfrak{g}' \to \mathfrak{g}$ be a continuous homomorphism, let $\mu : A \to A'$ be a homomorphism of κ into κ', compatible with λ.

We then have a *relation* $(\lambda, \mu)^2_*$ between $H^2(\mathfrak{g}, A, \kappa)$ and $H^2(\mathfrak{g}', A', \kappa')$. Using cocycles, this relation can be defined as follows. $\xi \in H^2(\mathfrak{g}, A, \kappa)$ is related to $\xi' \in H^2(\mathfrak{g}', A', \kappa')$ if ξ and ξ' can be represented by cocycles (f, g), (f', g'), satisfying

$$f'_{s'}(\mu(a)) = \mu(f_{\lambda(s')}(a)),\ g'_{s',t'} = \mu(g_{\lambda(s'),\lambda(t')}). \tag{7}$$

In some particular cases the relation $(\lambda, \mu)^2_*$ is a *mapping* of $H^2(\mathfrak{g}, A, \kappa)$ into $H^2(\mathfrak{g}', A', \kappa')$, namely if

(i) A' is abelian, or

(ii) μ is surjective.

This is easily verified.

We mention a particular case. Let $\mathfrak{g}' = \mathfrak{g}$, let λ be the identity mapping. Let ϕ be an automorphism of A. Then ϕ defines an automorphism of $E(A)$, also denoted by ϕ. $\kappa' = \phi \circ \kappa \circ \phi^{-1}$ is a $\mathfrak{g}$-kernel in A and one verifies that ϕ is a homomorphism of κ into κ', compatible with the identity mapping of $\mathfrak{g}$. We put $(\mathrm{id}, \phi)^2_* = \phi^2_*$; this is a mapping.

1.19. PROPOSITION. *If ϕ is an inner automorphism, then $\kappa' = \kappa$ and ϕ^2_* is the identity mapping of $H^2(\mathfrak{g}, A, \kappa)$.*

That $\kappa' = \kappa$ is clear. In (7), one has now $\lambda = \mathrm{id}$, $\mu(a) = bab^{-1}$, with $b \in A$. Then it follows from (5), that (6) holds with $h_s = bf_s(b)^{-1}$.

Let us mention too that the relations $(\lambda, \mu)^2_*$ have the functorial properties which are to be expected, we leave it to the reader to make them explicit.

1.20. *The connecting map.* Let A be a $\mathfrak{g}$-group, let B be a subgroup of A. Let $a \in Z^1(\mathfrak{g}, A, B)$. Define for $s, t \in \mathfrak{g}$, $b \in B$

$$\begin{aligned} f_s(b) &= a_s {}^s b a_s^{-1}, \\ g_{s,t} &= a_s {}^s a_t a_{st}^{-1}. \end{aligned} \tag{8}$$

It follows from (1) and (2) that $b \mapsto f_s(b)$ is an automorphism of B, which defines a $\mathfrak{g}$-kernel λ_a in B. Moreover $(f, g) \in Z^2(\mathfrak{g}, B, \lambda_a)$. If we replace $a = (a_s)$ by the equivalent cocycle $(a_s b_s)$, with $b_s \in B$, then λ_a does not change and (f, g) is replaced by an equivalent cocycle. If we replace a by a' with $a'_s = n^{-1} a_s {}^s n$ (where n is in the normalizer N of B) then, denoting by ϕ_n the automorphism $b \mapsto nbn^{-1}$ of B, κ is replaced by $\kappa' = \phi_n \circ \kappa \circ \phi_n^{-1}$ and (f, g) is replaced by a cocycle (f', g') whose class is the image under $(\phi_n)^2_*$ of the cohomology class of (f, g). Let Φ be the set of $\mathfrak{g}$-kernels in B of the form λ_a.

Then N acts on $\coprod_{\lambda \in \Phi} H^2(\mathfrak{g}, B, \lambda)$ and it follows from what precedes that there is a *mapping* δ^1 of $H^1(\mathfrak{g}, A, B)$ into the set of orbits of N. Put

$$H^2(\mathfrak{g}, B \operatorname{rel} A) = \left(\coprod_{\lambda \in \Phi} H^2(\mathfrak{g}, B, \lambda) \right) / N.$$

Hence we have defined a *connecting map* δ^1 of $H^1(\mathfrak{g}, A, B)$ into $H^2(\mathfrak{g}, B \operatorname{rel} A)$.

Let $N^2(\mathfrak{g}, B \operatorname{rel} A)$ be the set of orbits of N in $\coprod_{\lambda\in\Phi} H^2(\mathfrak{g}, B, \lambda)$ whose elements correspond to split extensions of $\mathfrak{g}$ by B. We call this the set of *neutral* elements of $H^2(\mathfrak{g}, B \operatorname{rel} A)$. (It can be empty.)

1.21. We keep the notations of §1.20. It follows from (8) that the map of $\mathfrak{g} \times A$ into A, which sends (s, g) into $a_s{}^s g a_s^{-1}$ induces a $\mathfrak{g}$-group structure on N/B. We denote this $\mathfrak{g}$-group by $(N/B)_a$. Let Z denote the centralizer of B in A. Then ZB/B is a normal subgroup of N/B, which is $\mathfrak{g}$-invariant. We denote by $(ZB/B)_a$ resp. $(N/ZB)_a$ the groups ZB/B resp. N/ZB with the inherited $\mathfrak{g}$-structures.

N acts on the set Φ of $\mathfrak{g}$-kernels in B, defined in §1.20. For $\phi \in \Phi/N$ put

$$H^2(\mathfrak{g}, B \operatorname{rel} A)_\phi = \left(\coprod_{\lambda\in\phi} H^2(\mathfrak{g}, B, \lambda)\right)/N;$$

this is a subset of $H^2(\mathfrak{g}, B \operatorname{rel} A)$. With these notations we have

1.22. Proposition. (i) *There is a bijection of* Φ/N *onto* $H^1(\mathfrak{g}, (N/ZB)_a)$;

(ii) *There is a bijection of* $(\delta^1)^{-1}(H^2(\mathfrak{g}, B \operatorname{rel} A)_\phi)$ *onto the subset* $\delta^0(H^0(\mathfrak{g}, (N/ZB)_a)$ *of* $H^1(\mathfrak{g}, (ZB/B)_a)$. ($\delta^0$ *denotes the connecting map defined in* [1], §1.11.)

To prove (i), observe that an arbitary $a' \in Z^1(\mathfrak{g}, A, B)$ has the form $(a'_s) = (n_s a_s)$, with $n_s \in N$. Moreover, since $a'_s{}^s a'_t (a'_{st})^{-1}$ must be in B, it follows that we must have

$$n_s a_s{}^s n_t a_s^{-1} n_{st}^{-1} \in B,$$

moreover $(n_s a_s)$ and $(n'_s a_s)$ determine the same $\mathfrak{g}$-kernel in B if and only if $n'_s(n_s)^{-1} \in Z$. It follows that there is a bijection of Φ onto $Z^1(\mathfrak{g}, (N/ZB)_a)$ and one verifies that under this bijection the orbits of N in Φ correspond to the cohomology classes. This establishes (i). (ii) is proved in a similar way.

One can also give a description of the fibers of δ^1, but we do not need this for our applications to Galois cohomology.

1.23. With the notations of §1.20, let i be the injection map $B \to A$. Let κ be the trivial $\mathfrak{g}$-kernel in A, defined by the action of $\mathfrak{g}$ on A. For each kernel λ_a in B, i is a homomorphism of λ_a into κ (compatible with the identity map of $\mathfrak{g}$). Hence we obtain a relation between $H^2(\mathfrak{g}, B, \lambda_a)$ and $H^2(\mathfrak{g}, A, \kappa)$, which in the present situation is easily seen to be a *mapping*. From §1.20 it follows, that this mapping defines a mapping

$$i_*^2 : H^2(\mathfrak{g}, B \operatorname{rel} A) \to H^2(\mathfrak{g}, A, \kappa).$$

1.24. *Fibers of* i_*^2. Let (f, g) be a cocycle in a suitable $Z^2(\mathfrak{g}, B, \lambda)$ whose canonical image in $H^2(\mathfrak{g}, B \operatorname{rel} A)$ is α. Then there exists a continuous function a of $\mathfrak{g}$ into A such that

$$f_s(b) = a_s{}^s b a_s^{-1} \qquad (b \in B),$$

$$({}^s a_t)^{-1} a_s^{-1} g_{s,t} a_{st} \quad \text{centralizes } B.$$

We make Z into a g-group by defining

$$_{s}z = a_s{}^{s}za_s^{-1};$$

denote this $\mathfrak{g}$-group by Z_a. $Z \cap B$ is a central subgroup of Z; we denote by $(Z \cap B)_a$ this group with the inherited $\mathfrak{g}$-structure.

One then has the following result

1.25. Proposition. *There is a bijection of the fiber of α under i_*^2 onto the subset $\delta^1(H^1(\mathfrak{g}, (Z/Z \cap B)_a)$ of $H^2(\mathfrak{g}, (Z \cap B)_a)$.*

We omit the proof, which does not present any difficulty.

1.26. *Exact sequence for a subgroup.* Let A be a $\mathfrak{g}$-group, let B be a subgroup of A. We denote by i the injection homomorphism of B into A. We use the previous notations.

We now have the following result:

1.27. Proposition. *The sequence*

$$H^1(\mathfrak{g}, A) \xrightarrow{p_*^1} H^1(\mathfrak{g}, A, B) \xrightarrow{\delta^1} H^2(\mathfrak{g}, B \operatorname{rel} A) \xrightarrow{i_*^2} H^2(\mathfrak{g}, A, \kappa)$$

is exact.

Notice that $H^2(\mathfrak{g}, B \operatorname{rel} A)$ has a privileged subset $N^2(\mathfrak{g}, B \operatorname{rel} A)$ and that $H^2(\mathfrak{g}, A, \kappa)$ has an element 0, hence exactness makes sense.

If $\alpha \in H^1(\mathfrak{g}, A, B)$ and $\delta^1(\alpha) \in N^2(\mathfrak{g}, B \operatorname{rel} A)$, then α can be represented by a cocycle $a \in Z^1(\mathfrak{g}, A, B)$ which is actually in $Z^1(\mathfrak{g}, A)$ and conversely, whence exactness in $H^1(\mathfrak{g}, A, B)$.

If $\alpha \in H^2(\mathfrak{g}, B \operatorname{rel} A)$ and $i_*^2(\alpha) = 0$, then α can be represented by a cocycle (f, g) in some $Z^2(\mathfrak{g}, B, \lambda)$, such that

$$f_s(b) = h_s{}^{s}bh_s^{-1},$$

where h is a continuous function on $\mathfrak{g}$ with values in A. It follows that α is in the image of δ^1. Conversely, if α is in the image of δ^1, then α can be represented by a cocycle (f, g) of this form, which implies that $i_*^2(\alpha) = 0$.

The fibers of p^1, δ^1 and i_*^2 have been described in §§1.8, 1.10, 1.22 and 1.25, respectively.

1.28. Proposition. *Let B be a g-invariant subgroup of A. Then the sequence*

$$H^1(\mathfrak{g}, B) \xrightarrow{i_*^1} H^1(\mathfrak{g}, A) \xrightarrow{p_*^1} H^1(\mathfrak{g}, A, B) \xrightarrow{\delta^1} H^2(\mathfrak{g}, B \operatorname{rel} A) \xrightarrow{i_*^2} H^2(\mathfrak{g}, A, \kappa)$$

is exact.

As observed in §1.2, $H^1(\mathfrak{g}, A, B)$ has now an element 0, so exactness makes sense. Proposition 1.28 follows from Propositions 1.11 and 1.27.

Now let B be a normal $\mathfrak{g}$-invariant subgroup. Denote by p the canonical projection of A onto A/B. Denote by κ the trivial kernels on A and A/B, defined by the $\mathfrak{g}$-group structure. According to §1.18 we have now a mapping of $H^2(\mathfrak{g}, A, \kappa)$ into $H^2(\mathfrak{g}, A/B, \kappa)$, namely $(\mathrm{id}, p)^2_*$. We write p^2_* for this mapping. Then we have

1.29. PROPOSITION. *The sequence*

$$H^1(\mathfrak{g}, A/B) \xrightarrow{\delta^1} H^2(\mathfrak{g}, B \operatorname{rel} A) \xrightarrow{i^2_*} H^2(\mathfrak{g}, A, \kappa) \xrightarrow{p^2_*} H^2(\mathfrak{g}, A/B, \kappa)$$

is exact.

The proof is left to the reader. Observe that this sequence can be built in into a longer exact sequence, involving the H^1's and H^0's (see [**1**, §1.17]).

1.30. *Relation between H^2's of subgroups and quotients.* Let A be a group; let B be a subgroup of A. We denote by i the injection mapping. Let κ and λ be $\mathfrak{g}$-kernels in A and B, respectively. Assume that i is a homomorphism of A into B, compatible with the identity homomorphism of $\mathfrak{g}$ (in the sense of §1.12). In the present case this means, that there exists a continuous function $\alpha: \mathfrak{g} \to \mathrm{Aut}(A)$, such that $\alpha(s)(B) = B$ for all $s \in \mathfrak{g}$ and such that the canonical image of $\alpha(s)$ in $E(A)$ (resp. the canonical image of the restriction of $\alpha(s)$ to B in $E(B)$) is $\kappa(s)$ (resp. $\lambda(s)$). Then there exists, according to §1.18, a relation $(\mathrm{id}, i)^2_*$ between $H^2(\mathfrak{g}, B, \lambda)$ and $H^2(\mathfrak{g}, A, \kappa)$. We write i^2_* for this relation. With these notations, we have the following result:

1.31. PROPOSITION. *Assume that λ is a trivial kernel. Then if an element α of $H^2(\mathfrak{g}, A, \kappa)$ is in $i^2_*(0)$, κ is also a trivial kernel and $\alpha = 0$.*

The proof of this is immediate, using the description of i^2_* by means of cocycles, given in §1.18.

Now assume that B is a normal subgroup of A. Let κ be a $\mathfrak{g}$-kernel in A, let κ' be a $\mathfrak{g}$-kernel in A/B, such that the canonical projection $p: A \to A/B$ is a homomorphism of κ into κ', compatible with the identity homomorphism of $\mathfrak{g}$. Observe that if B is a *characteristic* subgroup of A, such a $\mathfrak{g}$-kernel always exists.

We denote by p^2_* the induced mapping of $H^2(\mathfrak{g}, A, \kappa)$ into $H^2(\mathfrak{g}, A/B, \kappa')$. (It is a mapping because p is surjective; see §1.18.)

1.32. PROPOSITION. *Let κ' be a trivial kernel. Assume that $\alpha \in H^2(\mathfrak{g}, A, \kappa)$, $p^2_*(\kappa) = 0$. Then there exists a $\mathfrak{g}$-kernel λ in B, such that i is a homomorphism of λ into κ, compatible with the identity, together with an element $\beta \in H^2(\mathfrak{g}, B, \lambda)$ such that $\alpha \in i^2_*(\beta)$.*

This also follows without difficulty from the description of p^2_* in terms of cocycles.

1.33. *Action of inner automorphisms.* Let A be a group, let κ be a $\mathfrak{g}$-kernel in A, which is extendible. Fix an element (f, g) in $Z^2(\mathfrak{g}, A, \kappa)$. Then any element of $Z^2(\mathfrak{g}, A, \kappa)$ is cohomologous to a cocycle of the form (f, g'). Define mappings

$$\lambda_t: \mathfrak{g} \to \mathfrak{g}, \qquad \mu_t: A \to A$$

by

$$\lambda_t(s) = t^{-1}st, \qquad \mu_t(a) = f_t(a).$$

Then μ_t is a homomorphism of A into A, compatible with λ_t in the sense of §1.12. Since μ_t is surjective, we have now by §1.18 an induced mapping $(\lambda_t, \mu_t)^2_*$ of $H^2(\mathfrak{g}, A, \kappa)$ into itself. By Proposition 1.19, this mapping does not depend on the choice of the particular cocycle (f, g). In fact, we even have the following:

1.34. Proposition. *$(\lambda_t, \mu_t)^2_*$ is the identity mapping of $H^2(\mathfrak{g}, A, \kappa)$ for all $t \in \mathfrak{g}$.*

It follows from the definition of $(\lambda_t, \mu_t)^2_*$, given in §1.18 that it is the map induced by the mapping of $Z^2(\mathfrak{g}, A, \kappa)$ into itself, which sends the cocycle (f, g') into (f', g''), where

$$f'_r(a) = f_t f_{t^{-1}rt} f_t^{-1}(a),$$

$$g''_{r,s} = f_t(g'_{t^{-1}rt,t^{-1}st}).$$

Now (5) implies that we have

$$f'_r = h_r f_r h_r^{-1},$$

with

$$h_r = g'_{t,t^{-1}rt}(g'_{r,t})^{-1}.$$

Hence, in order to establish Proposition 1.34, it suffices to prove that we have

$$g''_{r,s} = h_r f_r(h_s) g'_{r,s}(h_{rs})^{-1},$$

for $r, s \in \mathfrak{g}$. This is a relation involving only f and g', hence we may as well drop the accents and prove the corresponding relation for our fixed cocycle (f, g).

What we have to prove then is

$$f_t(g_{t^{-1}rt,t^{-1}st})g_{t,t^{-1}st}g_{rs,t}^{-1} = g_{t,t^{-1}rt}g_{r,t}^{-1}f_r(g_{t,t^{-1}st}g_{s,t}^{-1})g_{r,s}.$$

The product of the first two terms in the left side equals by (5)

$$g_{t,t^{-1}rt}g_{rt,t^{-1}st}.$$

The factor $g_{t,t^{-1}rt}$ now occurs on both sides and can be cancelled. We then have to prove

$$g_{r,t}g_{rt,t^{-1}st}g_{rs,t}^{-1} = f_r(g_{t,t^{-1}st}g_{s,t}^{-1})g_{r,s}.$$

Again, we can replace here the product of the first two terms in the left side by

$$f_r(g_{t,t^{-1}st})g_{r,st}.$$

The resulting formula is an immediate consequence of (5).

2. **Relative H^1 and H^2 in nonabelian Galois cohomology.** If k is a field, we denote by k_s (resp. $\bar{k}$) a separable (resp. algebraic) closure of k. If K/k is a Galois extension, we denote by $\mathfrak{g}(K/k)$ its Galois group (with the Krull topology).

2.1. *Homogeneous spaces.* Let A be an algebraic group which is defined over the field k. An algebraic variety X, defined over k, is called *a right homogeneous space of A over k* if A operates on X on the right, the operation being defined over k, such that the induced action of the group $A(\bar{k})$ of $\bar{k}$-rational points of A on $X(\bar{k})$, the set of $\bar{k}$-rational points of X, is transitive.

It is clear what is meant by a k-isomorphism of two right homogeneous spaces of A over k.

If B is a subgroup of A, which is also defined over k, then the quotient variety $B\backslash A$ is obviously a right homogeneous space of A over k.

Now let K/k be a separable extension. Let B be a subgroup of A which is defined over K. We denote by $H^1(K/k, A, B)$ the set of k-isomorphism classes of right homogeneous spaces of A over k, which are K-isomorphic to $B\backslash A \otimes_k K$.

Suppose that $K = k_s$. Then if X is a right homogeneous space of A over k, the $\mathfrak{g}(k_s/k)$-set $X(k_s)$ is a right homogeneous space of the group $A(K)$ in the sense of §1.2. This gives a mapping

$$\varepsilon : H^1(k_s/k, A, B) \to H^1(\mathfrak{g}(k_s/k), A(k_s), B(k_s)).$$

2.2. Proposition. *ε is bijective.*

To prove this use the cocycle description of $H^1(\mathfrak{g}(k_s/k), A(k_s), B(k_s))$, given in Proposition 1.3. The surjectivity of ε follows then by descent of the base field. We refer to Proposition 4.9 of [1], where a similar question is dealt with. The injectivity is readily verified (using cocycles).

Now let B be a subgroup of A which is also defined over k. We denote by $H^1(k, A, B)$ the set of k-isomorphism classes of homogeneous spaces of A over k, which are isomorphic to $B\backslash A$ over some separable extension of k. We then have

2.3. Proposition. *There is a bijection of $H^1(k_s/k, A, B)$ onto $H^1(k, A, B)$.*

This follows from the fact that a homogeneous space which is isomorphic to $B\backslash A$ over some separable extension of k, is isomorphic to $B\backslash A$ over k_s.

2.4. *Kernels.* Let A be an algebraic variety which is defined over the field K. Let s be an automorphism of K. An *s-semiautomorphism* of X is an automorphism α of the $\mathbf{Z}$-schema X, which satisfies the following condition: let f be the structural morphism $X \to \operatorname{Spec}(K)$, let β_s denote the automorphism of $\operatorname{Spec}(K)$ induced by s, then $f \circ \alpha = \beta_s \circ f$.

It is clear what is meant by an s-semiautomorphism of an algebraic group A which is defined over K. If the identity component A_0 of A is also defined over k, then an s-semiautomorphism of A induces one of A_0.

Let A be an algebraic group defined over K. We will assume in the rest of §2, that in this situation $A(K)$ is dense in A for the Zariski topology. Suppose that K is a Galois extension of k, let $\mathfrak{g} = \mathfrak{g}(K/k)$.

A *K/k-kernel κ in A* is a $\mathfrak{g}$-kernel in $G(K)$ in the sense of Proposition 1.10, with the following additional property: for $s \in \mathfrak{g}$, $\kappa(s)$ is the canonical image in $E(G(K))$ of an s-semiautomorphism of the algebraic group A. The density assumption on $A(K)$ implies that the s-semiautomorphism is unique.

If A' is an algebraic group defined over k, then we have on $A = A' \otimes_k K$ a trivial kernel, defined by the action of $\mathfrak{g}$ on $A(K)$. Conversely, to a trivial K/k-kernel in A there corresponds an A', as follows from well-known results about descent (see e.g. [1, §2.12]).

2.5. *Definition of* H^2. Let A be an algebraic group defined over K; let K/k be a Galois extension; let κ be a K/k-kernel in A. We then define $H^2(K/k, A, \kappa) = H^2(\mathfrak{g}(K/k), A(K), \kappa)$.

Next let A be defined over k, let κ denote the trivial k_s/k-kernel in A defined by the action of $\mathfrak{g}(k_s/k)$ on $A(k_s)$. Let k'_s denote another separable closure of k, let κ' denote the corresponding kernel. Let f be an isomorphism of k_s onto k'_s, let λ_f be the isomorphism of $\mathfrak{g}' = \mathfrak{g}(k'_s/k)$ onto $\mathfrak{g} = \mathfrak{g}(k_s/k)$ defined by f. The homomorphism $\mu_f: A(k_s) \to A(k'_s)$ defined by f is a homomorphism of κ into κ', compatible with λ_f. Since μ_f is surjective we have now, by §1.18, an induced mapping $(\lambda_f, \mu_f)^2_*$.

2.6. PROPOSITION. $(\lambda_f, \mu_f)^2_*$ *is a bijection which is independent of* f.

If f' is a second isomorphism of k_s onto k'_s, we have $\lambda_{f'} = \lambda_t \circ \lambda_f$, $\mu_{f'} = \mu_f \circ \mu_t$, where $t \in \mathfrak{g}$, $\lambda_t(s) = t^{-1}st$, $\mu_t(a) = a$. The assertion now follows from Proposition 1.34.

It follows from Proposition 2.6, that we may identify $H^2(\mathfrak{g}, A(k_s), \kappa)$ and $H^2(\mathfrak{g}', A(k'_s), \kappa')$; hence we may denote them by $H^2(k, A)$.

Let A be defined over k. Let K/k be a Galois extension with group $\mathfrak{g}$.

Let B be a subgroup of A which is defined over K. We then put $H^2(K/k, B \text{ rel } A) = H^2(\mathfrak{g}, B(K) \text{ rel } A(K))$, $N^2(K/k, B \text{ rel } A) = N^2(\mathfrak{g}, B(K) \text{ rel } A(K))$.

3. **Reduction theorem for H^2 in Galois cohomology.** In this section, we shall encounter several instances of the following situation: A is a discrete group; B is a subgroup of A; $\mathfrak{g}$ a topological group. We have a $\mathfrak{g}$-kernel κ in A and a $\mathfrak{g}$-kernel λ in B, such that the injection $i: B \to A$ is a homomorphism of λ into κ, compatible with the identity homomorphism of $\mathfrak{g}$. In this situation we shall say that λ is *compatible* with κ. This terminology will be used, in particular, for K/k kernels in algebraic groups, as defined in §2.4. We denote by i^2_* the relation between $H^2(\mathfrak{g}, B, \lambda)$ and $H^2(\mathfrak{g}, A, \kappa)$, defined in §1.30.

The main result to be proved in this section is Theorem 3.4. First we derive a number of auxiliary results.

3.1. PROPOSITION. *Let A be a finite group; let $\mathfrak{g}$ be a topological group; let κ be a $\mathfrak{g}$-kernel in A. Then for any $\alpha \in H^2(\mathfrak{g}, A, \kappa)$ there exists a nilpotent subgroup B of A and a $\mathfrak{g}$-kernel λ in B, compatible with κ, such that $\alpha \in i^2_*(H^2(\mathfrak{g}, B, \lambda))$.*

The assertion is trivially true if A itself is nilpotent. If A is not nilpotent, then it is well known that there is a Sylow-subgroup S of A, which is not a normal subgroup of A. Let A' be the normalizer of S, then $A' = A$. Take a cocycle $(f, g) \in Z^2(\mathfrak{g}, A, \kappa)$ representing α. Using the conjugacy theorem for Sylow-subgroups, we see that there is a continuous function $h: \mathfrak{g} \to A$ such that $f_s(S) = h_s^{-1}Sh_s$ for all $s \in \mathfrak{g}$. Replacing (f, g) by the equivalent cocycle (f', g') given by (6), we find that $g'_{s,t}$ normalizes S, hence lies in A'.

Denoting by κ' the g-kernel in A' such that $\kappa'(s)$ is the element of $E(A')$ containing the automorphism $a \mapsto f'_s(a)$ of A' and denoting by j the injection $A' \to A$, we see that κ' is compatible with κ and that $\alpha \in j_*^2(H^2(\mathfrak{g}, A', \kappa'))$. We now apply induction on the order of A to obtain the result.

3.2. LEMMA. *Let k be a perfect field; let A be a connected abelian algebraic group which is defined over k. Let $\mathfrak{g}$ be a profinite group; let κ be a $\mathfrak{g}$-kernel in $A(\bar{k})$. Then for any $\alpha \in H^2(\mathfrak{g}, A(\bar{k}), \kappa)$ there exists a finite subgroup B of A and a $\mathfrak{g}$-kernel λ in $B(k)$, such that $\alpha \in i_*^2(H^2(\mathfrak{g}, B(\bar{k}), \lambda))$.*

Since A is abelian, a $\mathfrak{g}$-kernel κ in $A(\bar{k})$ is simply an action of $\mathfrak{g}$ on $A(\bar{k})$. Writing $H^2(\mathfrak{g}, A(\bar{k}))$ for $H^2(\mathfrak{g}, A(\bar{k}), \kappa)$, what we must prove is that there is a finite $\mathfrak{g}$-invariant subgroup $B(\bar{k})$ of $A(\bar{k})$ such that α is in the canonical image of $H^2(\mathfrak{g}, B(\bar{k}))$ in $H^2(\mathfrak{g}, A(\bar{k}))$. Let T be the torsion subgroup of $A(\bar{k})$, then our assertion will follow if we prove that the canonical homomorphism $H^2(g, T) \to H^2(\mathfrak{g}, A(\bar{k}))$ is surjective (see [4], p. I–9, Corollary 2), which will follow if we prove that $H^2(\mathfrak{g}, A(\bar{k})/T) = 0$. However it follows from the structure theory of abelian algebraic groups that $A(\bar{k})/T$ is an abelian group in which the nth power homomorphism is an isomorphism for all integers n and it is immediate that the cohomology of a profinite group in such a group is trivial in dimensions $\geqq 1$ (loc. cit., p. I–10, Corollary 3).

The assertion about $A(\bar{k})/T$ follows from structure theory. In fact, by a theorem of Chevalley, A is an extension of an abelian variety by a connected linear group (both defined over $\bar{k}$). Moreover, the second group is a direct product of a torus and a connected unipotent group (both defined over $\bar{k}$). It then suffices to prove the assertion about $A(\bar{k})/T$ if A is either an abelian variety or a torus or a connected unipotent group. In the first two cases the required property follows from the fact that then any nth power homomorphism is surjective in $A(\bar{k})$. The same is true in the third case if the characteristic of k is 0; otherwise $A(\bar{k})$ is a torsion group in this case, so that then $A(\bar{k}) = T$.

3.3. LEMMA. *Let k be a perfect field, let A be a solvable algebraic group which is defined over $\bar{k}$. Let κ be a $\bar{k}/k$-kernel in A. For every $\alpha \in H^2(\bar{k}/k, A, \kappa)$ there exists a finite subgroup B of A and a $\bar{k}/k$-kernel λ in B, compatible with κ, such that $\alpha \in i_*^2(H^2(\bar{k}/k, B, \lambda))$.*

On account of the definition of H^2 this will follow if we prove the following: Let $\mathfrak{g} = \mathfrak{g}(\bar{k}/k)$, suppose that

$$0 \longrightarrow A(\bar{k}) \xrightarrow{h} E \xrightarrow{p} \mathfrak{g} \longrightarrow 0$$

is an extension of $\mathfrak{g}$ by $A(\bar{k})$ in the sense of §1.13, which satisfies the condition (CS). Then there exists a closed subgroup $\mathfrak{g}_1$ of E with the following properties: (a) $p(\mathfrak{g}_1) = \mathfrak{g}$, (b) $h^{-1}(\mathfrak{g}_1 \cap h(A(\bar{k}))$ is a finite subgroup of $A(\bar{k})$, (c) $E = \mathfrak{g}_1 \cdot h(A(\bar{k}))$.

Let A_1 be the last nontrivial subgroup in the commutator series of A. By induction on the length of the commutator series we may assume our assertion to be true for A/A_1. From this we infer the existence of a closed subgroup E_1 of E, possessing the properties (a) and (c) of $\mathfrak{g}_1$ and such that we have, instead of (b), only: $h^{-1}(E_1 \cap h(A(\bar{k}))$ is an extension of a finite group by $A_1(\bar{k})$. Denote by A_0

the identity component of A_1. This is a connected abelian algebraic group, which is a subgroup of A_1. Now put $\mathfrak{g}' = E_1/h(A_0(\bar{k}))$. This is an extension of $\mathfrak{g}$ by a finite group, hence $\mathfrak{g}'$ is a profinite group and we have an extension

$$0 \longrightarrow A_0(\bar{k}) \xrightarrow{h} E_1 \xrightarrow{p'} \mathfrak{g}' \longrightarrow 0, \tag{9}$$

which verifies the condition (CS). Hence there corresponds to this extension an element $\alpha' \in H^2(\mathfrak{g}', A_0(\bar{k}), \kappa')$, where κ' is a suitable kernel. Applying Lemma 3.2 to this element α', we see that there exists a closed subgroup $\mathfrak{g}_1$ of E_1 which has the properties (a), (b), (c) relative to the extension (9). It follows that $\mathfrak{g}_1$, considered now as a closed subgroup of E, has the required properties (a), (b), (c).

3.4. THEOREM. *Let k be a perfect field, let A be an algebraic group which is defined over $\bar{k}$. Let κ be a $\bar{k}/k$-kernel in A. Then for every $\alpha \in H^2(\bar{k}/k, A, \kappa)$ there exists a finite nilpotent subgroup B of A, defined over k and a $\bar{k}/k$-kernel λ in B, compatible with κ, such that $\alpha \in i_*^2(H^2(\bar{k}/k, B, \lambda))$.*

Let A_0 be the identity component of A. There exists a $\bar{k}/k$-kernel κ' in the finite algebraic group A/A_0 such that the canonical projection $p: A \to A/A_0$ induces a homomorphism of κ into κ', compatible with the identity homomorphism of $\mathfrak{g} = \mathfrak{g}(\bar{k}/k)$, as follows from what was observed in §2.4. We then have a mapping p_*^2 of $H^2(\bar{k}/k, A, \kappa)$ into $H^2(\bar{k}/k, A/A_0, \kappa')$. Applying Proposition 3.1, we find easily that we may assume, replacing A by a subgroup with the same identity component, that A/A_0 is nilpotent (hence solvable).

Let L be the greatest connected linear subgroup of A_0. Then the theorem of Chevalley mentioned in the proof of Lemma 3.2, states that L is a normal subgroup of A_0 and that A_0/L is an abelian variety. Clearly, L is invariant under an s-semiautomorphism of A (s denoting an automorphism of $\bar{k}$). Now let M be a Borel subgroup of L. Using the fact that two Borel subgroups of L are conjugate, the same argument as used in the proof of Proposition 3.1 shows that there is a $\bar{k}/k$-kernel κ' in the normalizer N of M in A, such that, j denoting the injection $N \to A$, we have $\alpha \in j^2(H^2(\bar{k}/k, N, \kappa'))$. But A/L is solvable, being an extension of the finite nilpotent group A/A_0 by an abelian variety. Hence N is also solvable. Application of Lemma 3.2 and Proposition 3.1 finishes the proof of Theorem 3.4.

From Theorem 3.4 we obtain the following result, due to Grothendieck.

3.5. THEOREM. *Let k be a perfect field of dimension $\leqq 1$. Let A be an algebraic group which is defined over $\bar{k}$. Then any $\bar{k}/k$-kernel κ in A is trivial and*

$$H^2(\bar{k}/k, A, \kappa) = 0.$$

From Theorem 3.4 and Proposition 1.31 it follows that we need only to prove this if A is a finite nilpotent group. Suppose that this is the case and let B be the commutator subgroup of A. Using Proposition 1.32 and induction on the length of the commutator series of A, we see that it suffices to prove the assertion for A

finite abelian, in which case it is a direct consequence of the definition of fields of dimension $\leqq 1$ (see [4]).

3.6. Corollary. *Let k be a perfect field of dimension $\leqq 1$; let A be an algebraic group which is defined over $\bar{k}$; let B be a subgroup of A which is defined over $\bar{k}$. Then $H^2(\bar{k}/k, B \operatorname{rel} A) = N^2(\bar{k}/k, B \operatorname{rel} A)$.*

This is a consequence of Theorem 3.5.

3.7. *Applications to homogeneous spaces.* Let k be a perfect field; let A be an algebraic group which is defined over k. If X and Y are two right homogeneous spaces of A over k then we say that *Y dominates X* if there exists a morphism $Y \rightarrow X$, defined over k, which is compatible with the action of A in X and Y. Then the homogeneous space $Y(\bar{k})$ of the $\mathfrak{g}(\bar{k}/k)$-group $A(\bar{k})$ dominates the homogeneous space $X(\bar{k})$ in the sense of §1.5.

If X is a homogeneous space of A over k and if $x \in X(\bar{k})$, then there exists an algebraic subgroup B of A, which is defined over $\bar{k}$, such that $B(\bar{k})$ is the isotropy group in $A(\bar{k})$ of x, in the sense of §1.2. B is unique. It is called the *isotropy group of x in A*.

3.8. Theorem. *Let k be a perfect field, let A be an algebraic group which is defined over k. Let X be a right homogeneous space of A over k. Then X is dominated by a right homogeneous space of A over k whose isotropy groups are finite nilpotent.*

X is given by an element α of $H^1(\bar{k}/k, A, B)$, where B is a suitable subgroup of A which is defined over $\bar{k}$. Taking a cocycle in $Z^1(\mathfrak{g}(\bar{k}/k), A(\bar{k}), B(\bar{k}))$ representing α we find, in the manner described in the beginning of §1.20, a $\bar{k}/k$-kernel λ in B and a cocycle in $Z^2(\mathfrak{g}(\bar{k}/k), B(\bar{k}), \lambda)$; hence an element β of $H^2(\bar{k}/k, B, \lambda)$. Applying Theorem 3.4 to this element we obtain a finite nilpotent subgroup C of B and a $\bar{k}/k$-kernel μ in C, compatible with λ such that, i denoting the injection $C \rightarrow B$, we have $\beta \in i_*^2(H^2(\bar{k}/k, C, \mu))$. It is now easily seen that X is dominated by a homogeneous space of A over k, which has an isotropy subgroup C.

3.9. Theorem. *Let k be a perfect field of dimension $\leqq 1$. Let A be an algebraic group which is defined over k. Let X be a right homogeneous space of A over k. Then X is dominated by a principal homogeneous space of A over k.*

This is a known result (see [4], p. III–16, Theorem 3). It can be derived now as follows. X is given by an element of a suitable $H^1(\bar{k}/k, A, B)$.

According to Proposition 1.27 we have an exact sequence

$$H^1(k, A) \xrightarrow{p_*^1} H^1(\bar{k}/k, A, B) \xrightarrow{\delta^1} H^2(\bar{k}/k, B \operatorname{rel} A).$$

But now we have, by Corollary 3.6, that $H^2(\bar{k}/k, B \operatorname{rel} A) = N^2(\bar{k}/k, B \operatorname{rel} A)$; hence the exactness shows that the relation p_*^1 is surjective, which implies the assertion of Theorem 3.9.

Remark. Theorem 3.8 can also be proved by diagram chasing, the proof indicated above is somewhat simpler, however.

3.10. If, in the situation of Theorem 3.9, A is moreover linear and connected, then it is known that every principal homogeneous space of A over k has a k-rational point, hence by Theorem 3.9 any homogeneous space of A over k has a k-rational point (see [5], Theorem 1.9). Another consequence of the triviality of H^1 for connected linear A is the following result.

3.11. PROPOSITION. *Let k be a perfect field of dimension $\leqq 1$, let A be an algebraic group which is defined over k. Let X be a right homogeneous space of A over k, whose isotropy groups are connected linear subgroups of A. Then X is dominated by a principal homogeneous space of A over k, and two such principal homogeneous spaces are isomorphic.*

The existence statement is Theorem 3.9. The uniqueness is implied by Proposition 1.10. In fact, according to Proposition 1.10, the elements of $H^1(k, A)$ such that the corresponding principal homogeneous spaces dominate X, are in a one-to-one correspondence with $\mathrm{Im}(H^1(k, C) \to H^1(k, A))$, where C and D are certain twisted forms of B and A, which are defined over k. C being connected linear, we have $H^1(k, C) = 0$, which implies the assertion.

4. Finiteness theorems for local fields and number fields.

4.1. THEOREM. *Let k be a locally compact field of characteristic 0. Let A be a linear algebraic group which is defined over k; let B be a subgroup of A which is defined over $\bar{k}$. Then $H^1(\bar{k}/k, A, B)$ is finite.*

Consider the connecting map

$$\delta^1 : H^1(\bar{k}/k, A, B) \to H^2(\bar{k}/k, B \operatorname{rel} A),$$

defined in §1.20. According to §1.21 we have

$$H^1(\bar{k}/k, A, B) = \bigcup_{\phi} (\delta^1)^{-1}(H^2(\bar{k}/k, B \operatorname{rel} A)_\phi),$$

where ϕ runs through a set Σ (denoted Φ/N in §1.21). By Proposition 1.22 there exists algebraic groups C, D_ϕ, E_ϕ, defined over k, such that

(i) there is a bijection of Σ onto $H^1(k, C)$;

(ii) E_ϕ is a normal k-subgroup of $D_\phi, C = D_\phi/E_\phi$ and there is a bijection of $(\delta^1)^{-1}(H^2(\bar{k}/k, B \operatorname{rel} A)_\phi)$ onto the subset $\delta^0(H^0(k, C))$ of $H^1(k, E_\phi)$.

4.1 then follows by invoking the theorem of Borel–Serre which states that $H^1(k, A)$ is finite for any linear algebraic group A which is defined over k [1, Theorem 6.1].

4.2. Now let k be an algebraic number field. For any place v of k let k_v denote the corresponding completion. Denote by $\bar{k}_v$ an algebraic closure of k_v containing $\bar{k}$.

Suppose that A is an algebraic group defined over k and that B is an algebraic subgroup of A which is defined over $\bar{k}$. We then have a canonical mapping

$$\omega: H^1(\bar{k}/k, A, B) \to \prod_v H^1(\bar{k}_v/k_v, A, B).$$

4.3. Theorem. *If A is a linear algebraic group defined over k then ω is a proper mapping (i.e. its fibers are finite).*

We use the same notations as in the proof of Theorem 4.1. One has then the following facts:

(i) The canonical mapping

$$H^1(k, C) \to \prod_v H^1(k_v, C)$$

is proper [**1**, Theorem 7.1].

(ii) There is a bijection of $\delta^0(H^0(k, C))$ onto the set of orbits of $D_\phi(k)$ in $C(k)$ [**1**, §1.12],

(iii) Let $x \in C(k)$; let X be the set of elements x' of $C(k)$ such that for each place v there exists $d_v \in D_\phi(k_v)$ transforming x in x', then X consists of finitely many orbits of $D_\phi(k)$ [**1**, §7.12].

Using the same method as in the proof of Theorem 4.1, §4.2 is easily derived from these facts.

4.4. *Let S be a finite set of places of k. With the notations of* §4.3, *the canonical mapping*

$$H^1(\bar{k}/k, A, B) \to \prod_{v \notin S} H^1(\bar{k}_v/k_v, A, B)$$

is proper.

This follows from Theorems 4.1 and 4.3.

References

1. A. Borel and J.-P. Serre, *Théorèmes de finitude en cohomologie galoisienne*, Comm. Math. Helv. **39** (1964), 111–164.

2. P. Dedecker, *Le foncteur* Hom *non abelian. Applications de la notion de poulpe*, C. R. Acad. Sci. Paris **258** (1964), 1117–1120, *Les foncteurs* $\mathscr{E}\mathrm{xt}_\pi$, H^2_π et H^2_π *non abéliens*, 4891–4894; *Premier dérivé du foncteur* Hom *non abélien*, **259** (1964), 2054–2057; **260** (1965), 4137–4139.

3. J. Giraud, *Cohomologie non abélienne*, C. R. Acad. Sci. Paris **260** (1965), 2392–2394, 2666–2668.

4. J.-P. Serre, *Cohomologie galoisienne*, Springer, Berlin, 1964.

5. R. Steinberg, *Regular elements of semi-simple algebraic groups*, Publ. Math. I.H.E.S. No. 25 (1965), 201–312.

Inseparable Galois Cohomology

BY

PIERRE CARTIER

The following report is a brief and elementary account of a generalized Galois cohomology for generalized algebraic groups which takes into account the inseparability as well. We assume a ground field k of characteristic $p \neq 0$, because our theory reduces entirely to the classical one in the characteristic zero case. Much more general results have been obtained by M. Artin and A. Grothendieck (see **[1]**).

1. **Definition of an algebraic group.** Our algebraic groups are the same as the affine group schemes of finite type considered by A. Grothendieck and his school. We use the functorial point of view to define them. Namely, let $\mathfrak{U}_k$ be the category of commutative k-algebras. An algebraic group G is a covariant functor from $\mathfrak{U}_k$ to the category of groups which is "representable" in the following sense: *there exists a pair* (A_0, g_0), *where* A_0 *is some finitely generated algebra in* $\mathfrak{U}_k$ *and* g_0 *an element of the group* $G(A_0)$ *such that, for any object* A *of* $\mathfrak{U}_k$ *and any* g *in* $G(A)$, *there exists a unique homomorphism* σ *from* A_0 *into* A *such that* $G(\sigma)$ *maps* g_0 *into* g. We simplify the notation by writing $\tau \cdot g$ instead of $G(\tau) \cdot g$ when g is in $G(A)$ and τ is an algebra homomorphism from A to B.

EXAMPLES. (a) Let V_k be any finite-dimensional vector space over k, and V_A denote the additive group $V_k \otimes_k A$ for any object A of $\mathfrak{U}_k$. The functor V is called the *vector group associated to* V_k.

(b) If E_k is any finite-dimensional k-algebra, commutative or not, we define $E_A^\times$ as the multiplicative group of the k-algebra $E_A = E_k \otimes_k A$. This defines the multiplicative group $E^\times$ of the "algebra-variety" E.

(c) Let n be an integer. For any object A in $\mathfrak{U}_k$, let $\mathrm{GL}_n(A)$ denote the group of invertible n by n matrices with coefficients in A. Besides the algebraic group GL_n thus defined, one can define in the same way the symplectic group, or the orthogonal group of a quadratic form with coefficients in k.

(d) The algebraic group μ_n associates to any A the multiplicative group consisting of the elements a in A with $a^n = 1$.

The algebraic group G is called commutative if the groups $G(A)$ are commutative. It can be shown that the commutative algebraic groups form an *abelian category*.

2. **Definition of the cohomology groups.** Let K be a finite-dimensional commutative algebra over k. For any A in $\mathfrak{U}_k$, let us define X_A as the set of algebra

homomorphisms from K to A. Moreover, let there be given a commutative algebraic group G. By definition, an *n-cochain* c is a collection of functions

$$(1) \qquad c_A : X_A \times \cdots \times X_A \to G_A \quad (n+1 \quad \text{factors } X_A)$$

where A runs over the objects of $\mathfrak{U}_k$, subjected to the condition

$$(2) \qquad c_B(\sigma\sigma_0, \cdots, \sigma\sigma_n) = \sigma \cdot c_A(\sigma_0, \cdots, \sigma_n)$$

for any algebra homomorphism $\sigma : A \to B$. The coboundary δc of the n-cochain c is the $(n+1)$-cochain defined by

$$(3) \quad (\delta c)_A(\sigma_0, \cdots, \sigma_{n+1}) = \sum_{0 \leqq i \leqq n+1} (-1)^i \sigma_i \cdot c_A(\sigma_0, \cdots, \sigma_{i-1}, \sigma_{i+1}, \cdots, \sigma_{n+1}).$$

As usual, we have $\delta\delta c = 0$ for any n-cochain c. We can therefore define cohomology groups in the standard fashion; they will be denoted $H^n(K/k, G)$. This definition includes as particular cases the ordinary Galois cohomology in case K/k is a finite Galois extension and G an "ordinary" algebraic group, and also the Amitsur cohomology when K/k is a finite algebraic extension and G is 'the' multiplicative group $G_m = \mathrm{GL}_1$.

The cohomology groups $H^n(K/k, G)$ depend functorially on G and also on the pair (K, k) in the sense that any commutative diagram

$$\begin{tikzcd} K \arrow[r, "\phi"] & K' \\ k \arrow[u, phantom, "\cup" rotate=90] \arrow[r, "\alpha"] & k' \arrow[u, phantom, "\cup" rotate=90] \end{tikzcd}$$

gives rise to a homomorphism α^n from $H^n(K/k, G)$ to $H^n(K'/k', G)$ *independent* of ϕ.

We can define the absolute cohomology groups $H^n(k, G)$ in two equivalent ways. The first is to replace K by the algebraic closure $\bar{k}$ of k in the previous definitions (the fact that K is finite-dimensional over k played no role); the second consists in taking the direct limit of the groups $H^n(K/k, G)$ when K runs over the finite algebraic subextensions of $\bar{k}$.

The group $G(k)$ consists of the "rational points" of G and will also be denoted $\Gamma(G)$. The functor Γ maps the category of commutative algebraic groups into the category of abelian groups; the derived functors $R^n\Gamma$ of Γ are therefore defined. It turns out [2] that $R^n\Gamma(G)$ is nothing else than $H^n(k, G)$, which fact entails among other properties the existence of an exact sequence of cohomology associated to any short exact sequence of algebraic groups.

3. **Some particular cases** (K finite algebraic extension of k). Two important results are the following:

(a) *For any vector space V_k over k and any $n \geqq 1$, one has $H^n(K/k, V) = 0$.*

(b) *For any commutative algebra E_k, one has $H^1(K/k, E^\times) = 0$* (generalization of Hilbert's Theorem 90). The assumption of commutativity of E can be dropped provided one defines the first cohomology group $H^1(K/k, G)$ for a noncommutative algebraic group G as well, which causes no difficulty. Once this is done, one can prove for instance

$$H^1(K/k, \mathrm{GL}_n) = 0. \tag{4}$$

(c) *One has* $H^1(K/k, G_m) = 0$ *and* $H^2(K/k, G_m)$ *is the relative Brauer group of the field extension* K/k (that is the group of similarity classes of normal k-algebras split by K).

Going to the limit over K, we get as a corollary:

(d) *One has* $H^1(k, G_m) = 0$ *and* $H^2(k, G_m)$ *is the Brauer group of* k.

Finally using the exact sequence

$$0 \to \mu_n \to G_m \xrightarrow{\nu} G_m \to 0$$

defining μ_n (with $\nu_A(x) = x^n$ for every A) and the associated exact sequence of cohomology, we get the following information:

(e) *The group* $H^1(k, \mu_n)$ *is isomorphic to* $k^\times/(k^\times)^n$ *and* $H^2(k, \mu_n)$ *is the subgroup of the Brauer group of* k *defined by the condition* $a^n = 1$.

4. **Comparison with standard cohomology.** Let us denote by $\bar{k}$ any algebraic closure of k, and by k_s the maximal separable subextension of $\bar{k}$; the letter g denotes the group of k-automorphisms of $\bar{k}$. If G is any commutative algebraic group, the Galois group g acts on $G(k_s)$ and $G(\bar{k})$ and corresponding cohomology groups $H^n(g, G(k_s))$ and $H^n(g, G(\bar{k}))$ are defined after Tate [4]. Moreover, there are canonical homomorphisms

$$H^n(g, G(k_s)) \xrightarrow{\alpha_G^n} H^n(k, G) \xrightarrow{\beta_G^n} H^n(g, G(\bar{k})).$$

Using recent results by Shatz [3], one can prove that α_G^n and β_G^n are isomorphisms in each of the following cases (except possibly β_G^n for $n \leqq 2$)

(a) *k is perfect.*

(b) *G is smooth*, that is the algebra $A_0 \otimes_k \bar{k}$ has no nilpotent element where A_0 is as in the definition of G (§ 1).

(c) *The integer n is distinct from* 1 *and* 2.

Moreover, for every n, the kernels and cokernels of α_G^n and β_G^n are p-torsion groups and the different cohomology groups involved have no p-torsion for $n > 2$. Finally, α_G^1 is injective and β_G^2 is surjective.

5. **Infinitesimal groups.** The algebraic group G is called *infinitesimal* in case $G(K)$ is 0 for every field K; it suffices to assume $G(\bar{k}) = 0$. These groups enter as the kernels of the purely inseparable isogenies, and any information about their cohomology enables us via the exact sequence of cohomology to compare the cohomologies of any two purely inseparably isogeneous groups.

The basic result is again due to Shatz [3] and states that $H^n(k, G)$ is 0 for $n \neq 1, 2$ and isomorphic to $H^{n-1}(g, H^1(k_s, G))$ where the Galois group g acts in the natural way on $H^1(k_s, G)$.

References

1. M. Artin, *Grothendieck topologies*, Mimeographed notes for a Harvard Seminar, Spring 1962.

2. S. Shatz, *Cohomology of artinian group schemes over local fields*, Ann. of Math. **79** (1964), 411–449.

3. ———, *The cohomological dimension of certain Grothendieck topologies*, Ann. of Math. (to appear).

4. J. Tate, *Cohomology of compact totally discontinuous groups*. See a report by A. Douady in the Bourbaki Seminar, Dec. 1959, exp. 189.

Strong Approximation

BY

MARTIN KNESER

Notation. k is an algebraic number field. S will generally be a finite set of places of k, and ∞ is the (finite) set of all infinite places of k. G is a linear algebraic group defined over k, G_A is the adèle group, $G_S(\subset G_A)$ the S-component $\prod_{v\in S} G_{k_v}$ of G_A, and $G_k(\subset G_A)$ the k-rational points of G. If $\infty \subset S$, the S-integral adèles are $A(S) = A_S \times \prod_{v\notin S} \mathfrak{o}_v$ and $\mathfrak{o}(S) = A(S) \cap k$ are the S-integers of k.

The problem of (strong) approximation is as follows: under what conditions on G and S is $G_S G_k$ dense in G_A? This is equivalent to $G_k \cap UG_S$ being nonempty for every non-empty open set U of G_A. A down-to-earth equivalent formulation in the case $S = \infty$ is the following: Given S' disjoint from S and a_v in G_{k_v} and integers t_v for each v in S', find x in G_k to satisfy

$$x \equiv a_v \operatorname{mod}_{\mathfrak{p}_v}^{t_v} \quad (v \in S'),$$

$$x \in G_{\mathfrak{o}_v} \quad (v \notin S \cup S').$$

EXAMPLE 1. $G = G_a$ (additive group of the field). Then the strong approximation theorem for (G, ∞) is simply the Chinese Remainder Theorem.

EXAMPLE 2. $G =$ group of elements of reduced norm 1 in a central simple algebra (but not a definite quaternion algebra). Then Eichler [1] showed that (G, ∞) has strong approximation.

EXAMPLE 3. If G is the special orthogonal group of an indefinite quadratic form in more than two variables, $G_S G_k$ is not dense in G_A, but its closure contains all adèles whose components have spinor norm 1 (see [2] and [4]).

Most of the other classical groups are treated in [5].

Necessary conditions for strong approximation ($G \neq \{1\}$):

(1) G_S not compact.

(2) G simply connected.

The proof of (1) is easy: if G_S is compact, then $G_S G_k$ is closed since G_k is discrete; thus if (G, S) had strong approximation, we would have $G_S G_k = G_A$. For a proof of (2), as well as for details of the following discussion up to the Main Theorem, see [5].

From now on we assume that G is simply connected. It follows immediately that the radical N of G is unipotent. Now (G, S) has strong approximation if and only if $(G/N, S)$ has. Thus we may assume that G is semisimple. Write it as a product over k of almost simple factors, and look at each factor separately. Each of these factors may be obtained from some absolutely almost simple group H defined over a finite extension l/k, by reduction of scalars (see §6 of Tamagawa's lecture on *Adèles*, pp. 113–121. Since $(R_{l/k}H, S)$ has strong approximation if and only if (H, T) has (with T the set of all places of l whose restrictions to k are in S), we are reduced to the case of an absolutely simple group.

The following theorem holds modulo the Hasse principle (Theorem IV of Springer's lecture) for all k-forms of G. Thus with the present state of affairs, it holds for all groups except possibly those of type E_8. A sketch of its proof appears later in these notes.

MAIN THEOREM. *If G is simply connected, absolutely almost simple, and if G_S is not compact, then (G, S) has strong approximation.*

Putting things together, we see that for an arbitrary linear algebraic group, (G, S) has strong approximation if and only if its radial N is unipotent, G/N is simply connected, and each of the almost simple constituents H of G/N has a noncompact S-component H_S.

To show the significance of strong approximation, we discuss one particular type of application.

Class numbers. Let G be, as before, defined over k, and suppose that $G \subset \mathrm{GL}(V)$. Fix a basis for V and use it to define $G_{\mathfrak{o}_v}$, $G_{A(\infty)}$, etc. Suppose that M is the lattice (in V_k) spanned by this basis. If v is finite, M_v is the $\mathfrak{o}_v$-lattice spanned by M in V_{k_v}.

If $g = (g_v) \in G_A$, define gM to be the lattice uniquely determined by

$$(gM)_v = g_v M_v \qquad (\text{all } v \notin \infty).$$

The orbit of M under G_A (resp. G_k) is called the *G-genus* (resp. *G-class*) of M. The number of classes in a genus is the *class number*.

EXAMPLE 3 (continued). The genus, class and class number determined by the special orthogonal group coincide with the usual proper genus, proper class and proper class number. (The integral quadratic form in question is that induced on M by the form on V_k.) The ordinary genus, class and class number of an integral quadratic form arise from the full orthogonal group in the same manner.

EXAMPLE 4. V_k is a simple algebra, M a maximal order of V_k, and G is the multiplicative group V^* (acting by left multiplication). The G-genus of M consists of right ideals. In fact it is exactly all right ideals of M since each ideal of M_v is principal. Clearly the G-classes consist of equivalent right ideals (e.g. the class of M itself consists of all principal right ideals). Thus the class number of M is simply the (right) ideal class number.

We now show how the Main Theorem can be used to calculate class numbers.

The isotropy group in G_A of the lattice M is obviously $G_{A(\infty)}$. Thus the $\mathfrak{o}$-lattices in the genus of M are in 1-1 correspondence with the left cosets $xG_{A(\infty)}$, and the G-classes of M are 1-1 correspondence with the double cosets $G_k x G_{A(\infty)}$.

Suppose for a moment that G is almost simple, simply connected, and that G_∞ is not compact. Then, $\mathrm{Cl}[\cdots]$ denoting closure,

$$\begin{aligned} G_kG_{A(\infty)} &= G_kG_\infty G_{A(\infty)} && (\text{since } G_\infty \subset G_{A(\infty)}) \\ &= \mathrm{Cl}[G_kG_\infty]G_{A(\infty)} && (\text{since } G_{A(\infty)} \text{ is open}) \\ &= G_A. \end{aligned}$$

Hence the class number is 1 in this case.

In Examples 3 and 4 this procedure cannot be applied directly since in 3 G is not simply connected, and in 4 G is reductive but not semisimple. In such cases however, the theorem can still often be applied to yield a simple formula for the class number.

Namely suppose that G is connected and reductive. Then the derived group G' is semisimple and so has a universal covering group F/k:

$$\phi : F \to G' \qquad (\text{isogeny } /k).$$

Assume also that (F, ∞) has strong approximation. Then

$$G_kxG_{A(\infty)} = G_kG_\infty xG_{A(\infty)} = \mathrm{Cl}[G_kG_\infty]xG_{A(\infty)}.$$

Also

$$\begin{aligned} \mathrm{Cl}[G_kG_\infty] &\supset \mathrm{Cl}[\phi(F_kF_\infty)] \\ &= \mathrm{Cl}[\phi(F_A)] \\ &\supset (G_A)' \qquad (\text{see [5]}). \end{aligned}$$

Therefore $\mathrm{Cl}[G_kG_\infty]xG_{A(\infty)} = x\,\mathrm{Cl}[G_kG_\infty]G_{A(\infty)}$ and so we have the desired formula

$$\text{class number} = [G_A : G_kG_{A(\infty)}].$$

Example 4 (and 2) (continued). Assume V to be central and totally indefinite (i.e., V_{k_v} is a matrix algebra over k_v for all $v \in \infty$). Let $N : V_k^* \to k^*$ be the reduced norm. Its kernel, the elements of reduced norm 1, is also the commutator subgroup G'. Since it is simply connected and almost simple, the above analysis shows that $G_kG_{A(\infty)}$ contains $(G_A)'$, the adèles of reduced norm 1. Thus taking reduced norms we get

$$\text{class number} = [N(G_A) : N(G_k)N(G_{A(\infty)})].$$

It is known that, for each v, every element of k_v^* is a reduced norm from G_{k_v}, so that $N(G_A) = I_k$ (idèles). Similarly $N(G_k) = k^*$ and $N(G_{A(\infty)}) = I_{k(\infty)}$. Thus (see [1])

$$\begin{aligned} \text{class number} &= [I_k : k^*I_{k(\infty)}] \\ &= \text{ideal class number of } k. \end{aligned}$$

A similar procedure can be applied in Example 3. One then applies the spinor norm to $[G_A : G_k G_{A(\infty)}]$ to express it is an idèle index, which turns out to be a power of 2. For details see [**4**].

We now give a sketch of the proof of the Main Theorem. As stated before, the proof depends on the validity of the Hasse principle for all k-forms of G (cf. the lectures on Galois cohomology, pp. 149–158, and Hasse principle, pp. 159–163).

It clearly suffices to prove the theorem for S consisting of one place, say w. Then G_{k_w} is not compact.

The proof consists of mapping G into an object in which the strong approximation theorem is known to hold (namely an affine space) and then "lifting" the approximation back to G.

The affine space E in question has dimension l = rank G, and if G splits over k, the map $p : G \to E$ is

$$p(g) = (\chi_1(g), \cdots, \chi_l(g))$$

where $\chi_1, \cdots, \chi_l$ are the fundamental characters of G (see [**7**]). p is then defined over k. In the general case let G_0 be the split k-form of G and let $f : G_0 \to G$ be an isomorphism over $\bar{k}$. Define $p_0 : G_0 \to E$ as above. If the cocycle

$$z_s = f^{-1} \circ {}^s f \in Z^1\,(k, \operatorname{Aut} G_0)$$

is inner, i.e., if each z_s is an inner automorphism of G_0, then we can choose p to make

$$\begin{tikzcd} G_0 \arrow[r, "p_0"] \arrow[d, "f"'] & E \\ G \arrow[ur, dashed, "p"'] & \end{tikzcd}$$

commutative, i.e., $p = p_0 \circ f^{-1}$. Then

$${}^s p = p_0 {}^s f^{-1} = p_0 z_s^{-1} f^{-1}.$$

But $p_0 z_s^{-1} = p_0$ since the characters take the same values on conjugate elements, and so ${}^s p = p$ as required.

A slightly more complicated argument (using the fact that an outer automorphism of G_0 merely permutes the fundamental characters and that

$$H^1(k, \mathrm{GL}(E)) = 0)$$

shows in general that there is a $\bar{k}$-isomorphism g of E such that the map p defined by the commutativity of the diagram

$$\begin{tikzcd} G_0 \arrow[r, "p_0"] \arrow[d, "f"'] & E \arrow[d, "g"] \\ G \arrow[r, "p"] & E \end{tikzcd}$$

is rational over k. p will also denote the induced maps $G_A \to E_A, G_S \to E_S$, etc.

We begin the proof proper by pointing out that (E, S) has strong approximation:

(1) $$\mathrm{Cl}[E_k + E_S] = E_A.$$

The rest of the proof consists of refining and lifting (1) to G in several steps.

First we show that in (1), E_k can be replaced by its subset whose S components can be lifted to G_S:

(2) $$\mathrm{Cl}[[E_k \cap \pi_S^{-1}(pG_S)] + E_S] = E_A$$

with π_S the projection $E_A \to E_S$.

It suffices to show that

$$[E_k \cap \pi_S^{-1}(pG_S)] \cap [E_S + U] \neq \phi$$

for any nonempty open set U in E_A. For some compact set C, $E_A = E_k + C$. Multiplying by $\lambda \in k^*$ we get $E_A = E_k + \lambda C$ and so $(\lambda C - x) \cap E_k \neq \phi$ for all $x \in E_A$ and all $\lambda \in k^*$. Thus (2) will be proved if we can choose λ and x so that

$$\lambda C - x \subset \pi_S^{-1}(pG_S) \cap (E_S + U).$$

We may suppose that $C = \Pi C_v$ with $C_v = E_{o_v}$ for almost all v, by enlarging it if necessary. Similarly by shrinking U we may assume that $U = a + \Pi U_v$ where each U_v is a neighborhood of 0 and $U_v = E_{o_v}$ for almost all v. The coordinates of each C_v are bounded and so we can choose λ in k^* such that $\lambda C_v \subset U_v$ for all $v \notin S$. Therefore $\lambda C + a \subset E_S + U$. Now if we keep λ fixed and vary a by elements of E_S, this last inclusion still holds. Doing this, we can achieve

$$\lambda C + a \subset \pi_S^{-1}(pG_S)$$

by applying the following lemma (where $S = \{w\}$) and therefore prove (2).

LEMMA. *There exists $x_w \in E_{k_w}$ such that $C_w - x_w \subset pG_{k_w}$.*

The proof runs as follows. Since G_{k_w} is not compact, it contains a split torus, and so there exists a nontrivial homomorphism $\phi: G_m \to G$ defined over k_w. If V is any nonempty open set in $G_{k_{w_v}}$, it can be shown that $p(\phi(t)V)$ contains a translate of C_w if $|t|_w$ is sufficiently large.

The next step is to show that those adèles in G_A which are in fibers of points of E_k are dense in G_A modulo G_S, i.e., that

(3) $$\mathrm{Cl}[p_A^{-1}(E_k)G_S] = G_A$$

where p_A has been used instead of p to emphasize the fact that it is the fibers in G_A, not G_k, which are under consideration. The following lemma is needed.

LEMMA. *Let R be the set of regular elements of G (namely those elements whose centralizer has minimum dimension), and let $i: R \to G$ be the inclusion map. Then the map*

$$(p \circ i)_A : R_A \to E_A$$

is open.

To prove it one has to show that the map is open in each local component (see Steinberg [7]) and then that $(p \circ i)G_{\mathfrak{o}_v} = E_{\mathfrak{o}_v}$ for almost all v.

Back to the proof of (3). Let U be an open set in G_A. Since R is Zariski dense in G and G is nonsingular, $i^{-1}(U)$ is open and nonempty, and so $p(U)$ contains a nonempty open set V of E_A. By (2) we can find $x \in U$ such that $p(x) = e + e'$ where $e \in E_k \cap \pi_S^{-1}(pG_S)$ and $e' \in E_S$. So for each v in S, there exists g_v in G_{k_v} such that $p(g_v) = e_v$. Let y in G_A be defined by

$$\begin{aligned} y_v &= g_v, \qquad v \in S, \\ &= x_v, \qquad v \notin S. \end{aligned}$$

Then $x = yz$ for some $z \in G_S$ and $p(y) = e$. This proves (3).

Now we refine (3) by replacing E_k by pG_k:

$$\text{(4)} \qquad \mathrm{Cl}[p_A^{-1}(pG_k)G_S] = G_A,$$

i.e., the adèlic fibers of pG_k are dense mod G_S. The proof is rather complex; it uses Galois cohomology, in particular the Hasse principle for $H^1(k, G)$. An indication of it will be given in the final section of these notes.

Now any fiber of p_A which contains a rational element $g \in G_k$ also contains all of its conjugates under G_A. We refine (4) by replacing these fibers by these conjugacy classes:

$$\text{(5)} \qquad \mathrm{Cl}[G_k^{G_A}G_S] = G_A.$$

The proof of (5) again uses Galois cohomology and will not be given in these notes.

It is easy to see that $\mathrm{Cl}[G_kG_S]^{G_A} \subset \mathrm{Cl}[G_k^{G_A}G_S]$. The next refinement is

$$\text{(6)} \qquad \mathrm{Cl}[G_kG_S]^{G_A} = G_A.$$

By reduction theory $G_A = G_kDG_S$ where D is compact (the proof is similar to that in §7 of [3] where the case $S = \infty$ is treated). It follows immediately from (5) that

$$G_A = \mathrm{Cl}[G_k{}^DG_S] = \mathrm{Cl}[(G_kG_S)^D].$$

Since $\mathrm{Cl}[G_kG_S]$ is closed and D is compact, an elementary argument shows that $\mathrm{Cl}[G_kG_S]^D$ is closed and so contains the closure of $(G_kG_S)^D$ which is G_A.

At this point we digress for a moment to show that the Weak Approximation Theorem

$$(*) \qquad \mathrm{Cl}[\pi_T(G_k)] = G_T$$

can be deduced from the results proved thus far; here G satisfies the conditions of the Main Theorem, $T \cap S = \phi$, and π_T is the projection $G_A \to G_T$.

We first show that $\mathrm{Cl}[\pi_T(G_k)]$ is of finite index in G_T; this is done by showing that it is open and has a compact set of representatives. The latter fact follows from applying π_T to $G_A = G_kDG_S$ (D as above). To show that it is open we need only show that it contains an open set of G_T. By [6] there is a rational map

$V \to G$ defined over k of an affine space V generically onto G. We choose x in V_k at which the map is nondegenerate; then some neighborhood of x in

$$V_T = \mathrm{Cl}[\pi_T(V_k)]$$

goes onto an open set in G_T.

Now applying π_T to (6) shows that $\mathrm{Cl}[\pi_T(G_k)]^{G_T} = G_T$, and so (*) follows by applying the following elementary result:

If H is a group and H_0 is a subgroup of finite index such that $H_0^H = H$, then $H_0 = H$.

We are now ready to prove the Main Theorem:

$$\mathrm{Cl}[G_k G_S] = G_A. \tag{7}$$

Since every element of G_A is a limit of elements almost all of those of whose local components are 1, it suffices to show that $G_T \subset \mathrm{Cl}[G_k G_S]$ for an arbitrary finite set T disjoint from S. Suppose $g \in G_T$. By (6) we can write $g = x^y$ with x in $\mathrm{Cl}[G_k G_S]$ and y in G_A. The components of x outside of T are necessarily 1. By (*) we can find a sequence $y_1, y_2, \cdots, y_n, \cdots$ of elements in G_k such that $\lim_v y_i = y_v$ for each v in T. Then clearly g is the limit of the sequence $x^{y_1}, x^{y_2}, \cdots, x^{y_n}, \cdots$ in the topology of G_A, and so the Main Theorem is proved.

Proof of intermediate step. We now return to the sketch of the proof that the condition

$$\mathrm{Cl}[p_A^{-1}(E_k)G_S] = G_A \tag{3}$$

implies

$$\mathrm{Cl}[p_A^{-1}(pG_k)G_S] = G_A. \tag{4}$$

Let U be any nonempty open set of G_A. Then our task is to show that

$$p_A^{-1}(pG_k) \cap UG_S$$

is nonempty, i.e., find x in UG_S such that $p(x) \in p(G_k)$.

For the background of the following discussion concerning the map p and the properties of regular elements, the reader is referred to [7].

Since the regular semisimple elements of G form a Zariski-open dense subset of G, we may replace U by a smaller set such that for some particular $v \notin S$, $\pi_v U$ contains only regular semisimple elements. It follows then that all elements of G in the fibers of points in $p(UG_S) \cap E_k$ are regular and semisimple.

Let G_1 be a k-form of G which is quasi-split (i.e., has a Borel subgroup $/k$) and which is obtained from G by an inner twist. Thus we have a commutative diagram

$$\begin{tikzcd} G_1 \arrow[d, "f"'] \arrow[dr, "p_1"] & \\ G \arrow[r, "p"'] & E \end{tikzcd}$$

where $f^{-1} \circ {}^s f$ is an inner automorphism of G_1 for each s in the Galois group Γ

of $\bar{k}/k$. We have $f^{-1} \circ {}^s f \in \dot{G}_1$ (adjoint group of G_1). The important thing about G_1 is that the map $p: G_{1,k} \to E_k$ is surjective.

By the choice of U and the fact that the above diagram is commutative, any $a \in E_k \cap p(UG_S)$ lifts to a regular point $x_1 \in G_{1,k}: p_1(x_1) = a$. If it happens that a also lifts to G_k, say $p(x) = a$, then $p(f(x_1)) = p(x)$ and so x and $f(x_1)$ are conjugate in G (over $\bar{k}$). Thus changing f by an inner automorphism of G, we may suppose that $f(x_1) = x$. Since x and x_1 are rational over k, we get $f^{-1} \circ {}^s f(x_1) = x_1$, i.e., $f^{-1} \circ {}^s f$ is in the stabilizer $\dot{Z}(x_1)$ of x_1 in $\dot{G}_1$ for all s in Γ. Conversely if a is lifted to x_1 and we can find an isomorphism $f: G_1 \to G$ such that $f^{-1} \circ {}^s f$ is in $\dot{Z}(x_1)$ then $x = f(x_1)$ is in G_k and $p(x) = a$.

Therefore it suffices to do the following:

Given a regular semisimple element x_1 in $G_{1,k}$ and ξ in $H^1(k, \dot{G}_1)$ (which we shall later require to satisfy some further conditions), show that

$$\xi \in \operatorname{Im}(H^1(k, \dot{Z}(x_1)) \to H^1(k, \dot{G}_1)).$$

Before we proceed, let us show the "invariance" of these considerations, namely:

Let G_2 also be a k-form of G obtained by an inner twist, and suppose that x_2 is a regular semisimple element of $G_{2,k}$ such that $p_2(x_2) = a$. Let $g: G_1 \to G_2$ be a twisting isomorphism such that $g(x_1) = x_2$ and

$$\begin{tikzcd} G_1 \arrow[d, "g"'] \arrow[dr, "p_1"] & \\ G_2 \arrow[r, "p_1"'] & E \end{tikzcd}$$

is commutative. Since $g^{-1} \circ {}^s g$ is an inner automorphism of G_1 and is the identity on x_1, it must be an inner automorphism by an element of $Z(x_1)$. But $Z(x_1)$ is abelian and so $g^{-1} \circ {}^s g$ is the identity on it, whence the restriction of g to $Z(x_1)$ is defined over k (and maps $Z(x_1)$ isomorphically onto $Z(x_2)$).

For any torus T we put $Y(T) = \operatorname{Hom}(G_m, T)$, the 1-parameter subgroups of T. If T/k is a maximal torus of G, the Galois group Γ acts on $Y(T)$ as a subgroup of the extended Weyl group of G.

Definition. If the canonical image of Γ in $\operatorname{Aut}(Y(T))$ contains the Weyl group of G (relative to T), then T is called highly twisted. An element a of E_k is called highly twisted if $Z(x_1)$ is highly twisted (where x_1 is a regular semisimple element of $G_{1,k}$ such that $p(x_1) = a$). As we have seen above, this depends only on a, not on x_1.

Lemma. *If V is a nonempty open set of E_A, there exists a nonempty open set $V' \subset V$ such that every element a* in *$E_k \cap (V' + E_S)$ is highly twisted.*

The proof of this lemma is quite technical and is not given here.

As we have seen earlier, pU contains an open subset V of E_A. Choose $V' \subset V$ with the property in the lemma, and replace U by the open set $U \cap p^{-1}V'$. Thus we may suppose that $p(x) \in E_k$ is highly twisted if $x \in UG_S$. With these restrictions on x, we can show that $p(x)$ lifts to G_k, which will finish the proof of (4).

As before we let x_1 be a regular semisimple element of $G_{1,k}$ such that

$$p_1(x_1) = p(x),$$

and $\xi \in H^1(k, \dot{G}_1)$ is the cohomology class of cocycles which twist G_1 into G. We must show that

$$\xi \in \operatorname{Im}(H^1(k, \dot{Z}(x_1)) \to H^1(k, \dot{G}_1)).$$

Let $T_1 = Z(x_1)$ and let C_1 be the center of G_1. If G' is any of the groups involved, we let $HV(G')$ stand for either $HV(k, G')$ or $HV(k_v, G')$ for some place it will be made clear in the context whether the global case or a local case is under consideration.

Now we have the commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & C_1 \arrow[r] \arrow[d, leftrightarrow, "\mathrm{id}"'] & T_1 \arrow[r] \arrow[d] & \dot{T}_1 \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & C_1 \arrow[r] & G_1 \arrow[r] & \dot{G}_1 \arrow[r] & 1
\end{tikzcd}$$

in which the rows are exact. This gives rise to the commutative diagram

$$\begin{tikzcd}
H^1(C_1) \arrow[r] \arrow[d, leftrightarrow, "\mathrm{id}"] & H^1(T_1) \arrow[r] \arrow[d] & H^1(\dot{T}_1) \arrow[r] \arrow[d] & H^2(C_1) \arrow[r] \arrow[d, leftrightarrow, "\mathrm{id}"] & H^2(T_1) \\
H^1(C_1) \arrow[r] & H^1(G_1) \arrow[r] & H^1(\dot{G}_1) \arrow[r] & H^2(C_1) &
\end{tikzcd}$$

in which the rows are again exact; the diagram applies to either the global case or any local case.

The following lemma is proved using the Tate-Nakayama theorem of class field theory.

Lemma. *If T_1 is a highly twisted maximal torus of the simply connected group G_1, the Hasse principle holds for $H^2(k, T_1)$: the map*

$$H^2(k, T_1) \to \prod_{\text{all } v} H^2(k_v, T_1)$$

is injective.

We shall apply this lemma to show that we may assume that ξ goes onto 0 under the map $H^1(k, \dot{G}_1) \to H^2(k, C_1)$.

Now $p(x)$ can be lifted to G_v for all v (namely to x_v) and so ξ is a local image of elements of $H^1(\dot{T}_1)$. These elements all have the same image as ξ in $H^2(C_1)$, and since they go to 0 in $H^2(T_1)$, the global image of ξ in $H^2(C_1)$ must also by the above lemma. Therefore there is ζ in $H^1(\dot{T}_1)$ globally which has the same image as ξ in $H^2(C_1)$. Let $G_2 = {}_{\zeta}G_1$ be the twisted group; suppose $g: G_1 \to G_2$ is the isomorphism corresponding to ζ. Since $g|T_1$ is defined over k, it is clear that gT_1 is defined over k. Moreover under the canonical bijection $H^1(k, \dot{T}_1) \to H^1(k, {}_{\zeta}\dot{T}_1)$ the class of ζ goes onto 0. Thus we may, upon replacing G_1 by ${}_{\zeta}G_1$, assume henceforth that ξ goes onto 0 under the map $H^1(k, \dot{G}_1) \to H^2(k, C_1)$.

Let η be a global pre-image of ξ in $H^1(G_1)$. Choose pre-images of ξ at each place v in $H^1(\dot{T}_1)$; since they also go onto 0 in $H^2(C_1)$ they in turn have pre-images in $H^1(T_1)$, and by the following lemma of Serre, these latter pre-images at the infinite places are the localizations of a global one, say $\tau \in H^1(T_1)$.

Lemma. *For any torus T defined over k, the map*

$$H^1(k, T) \to \prod_{v \in \infty} H^1(k_v, T)$$

is surjective. The same is true for any finite commutative group instead of T.

Now the infinite components of the images of τ and η in $H^1(\dot{G}_1)$ are identical, and so at each $v \in \infty$, the components of η and the image of τ in $H^1(G_1)$ differ by an element of $H^1(C_1)$. By the above lemma we may change τ by an element of $H^1(k, C_1)$ so that these latter components at ∞ are identical (and so we assume it is already true for τ).

By Hasse's principle applied to $H^1(G_1)$, the image of τ in $H^1(k, G_1)$ is equal to η, and so the required pre-image of ξ in $H^1(k, \dot{T}_1)$ is the image of τ in that cohomology set.

References

1. M. Eichler, *Allgemeine Kongruenzklasseneinteilungen der Ideale einfacher Algebren über algebraischen Zahlkörpern und ihre L-Reihen*, J. Reine Angew. Math. **179** (1938), 227–251.

2. ———, *Die Ähnlichkeitsklassen indefiniter Gitter*, Math. Zeitschrift **55** (1951–1952), 216–252.

3. R. Godement, *Domaines fondamentaux des groupes arithmétiques*, Séminaire Bourbaki 1962–1963, No. 257, Secrétariat Mathématique, Paris.

4. M. Kneser, *Klassenzahlen indefiniter quadratischer Formen in drei oder mehr Veränderlichen*, Arch. Math. 7 (1956), 323–332.

5. ———, *Starke Approximation in algebraischen Gruppen.* I, J. Reine Angew. Math. **218** (1965), 190–203.

6. M. Rosenlicht, *Some rationality questions on algebraic groups*, Ann. Mat. Pura Appl. (4) **43** (1957), 25–50.

7. R. Steinberg, *Regular elements of semi-simple algebraic groups*, Publ. Math. IHES, No. 25 (1965), 49–80.

III. Automorphic Functions and Decomposition of $L^2(G/\Gamma)$

Introduction to Automorphic Forms

BY

ARMAND BOREL

The classical notion of automorphic form in one complex variable is well known. Let Γ be a Fuchsian group: the function f, holomorphic in the upper half plane H, is called an automorphic form of weight $2k$ (k an integer) if for every $\gamma \in \Gamma$

$$f(z) = J_\gamma(z)^k \cdot f(\gamma \cdot z),$$

where

$$J_\gamma(z) = (cz + d)^{-2}, \qquad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \qquad ad - bc = 1;$$

(and if it satisfies certain regularity conditions at the cusps of Γ, when H/Γ is not compact). This notion was generalized in two directions: on the one hand to holomorphic functions of several complex variables (Poincaré, Hilbert–Blumenthal, Siegel, etc.), on the other hand to nonholomorphic functions, for instance Eisenstein series of the form $\sum_{(c,d)=1} |cz + d|^{-s}$ where s is not necessarily an integer (Maass, Selberg, etc.). Our first aim here is to define a notion of automorphic form on a semisimple Lie group, which encompasses the two types just mentioned, introduced by Harish-Chandra [6].

1. **Definition of automorphic forms.** Let G be a real semisimple Lie group. To simplify matters, we assume that it is of finite index in the set of real points of a semisimple algebraic $\boldsymbol{R}$-group. The universal enveloping algebra $U(\mathfrak{g})$ of the Lie algebra $\mathfrak{g}$ (with complex coefficients) can be identified with the algebra $D(G)$ of right invariant differential operators on G: to $y \in \mathfrak{g}$ is associated a differential operator such that

$$Yf(g) = \frac{d}{dt} f(\exp tY \cdot g)\bigg|_{t=0};$$

this linear map of $\mathfrak{g}$ into $D(G)$ extends to an isomorphism of $U(\mathfrak{g})$ onto $D(G)$. On G^0, the center $Z(\mathfrak{g})$ of $U(\mathfrak{g})$ corresponds then to the left and right invariant differential operators and is isomorphic with a polynomial ring in l letters, where l is the rank of G.

A vector valued function $f: G \to V$ is called $Z(\mathfrak{g})$-finite if $Z(\mathfrak{g}) \cdot f$ is a finite-dimensional vector space, or equivalently, if f is annihilated by an ideal I of $Z(\mathfrak{g})$

of finite codimension. The most important case is when I has codimension one, i.e. when f is an eigenfunction of every operator in $Z(\mathfrak{g})$.

DEFINITION. Let Γ be a discrete subgroup of G, K a maximal compact subgroup of G, ρ a representation of K in $GL(V)$, where V is a finite-dimensional complex vector space. The smooth vector valued function $f: G \to V$ is called an *automorphic form for* Γ if

(1) $f(k \cdot g \cdot \gamma) = \rho(k) \cdot f(g)$, f is left equivariant for K and right invariant for Γ.

(2) f is $Z(\mathfrak{g})$-finite.

(3) f satisfies a certain growth condition, to be specified later.

If I is an ideal of finite codimension in $Z(\mathfrak{g})$ which annihilates f, then f is called an automorphic form of type (ρ, I).

2. **Remark on the smoothness conditions.** The above definition makes sense for distributions. However, the $Z(\mathfrak{g})$-finiteness and the K-equivariance imply that f is a real analytic function:

PROOF: Let $\mathfrak{g} = \mathfrak{k} + \mathfrak{y}$ be a Cartan decomposition of $\mathfrak{g}$. Choosing orthonormal basis X_i of $\mathfrak{y}$ and Y_j of $\mathfrak{k}$ allows one to construct the Casimir operator $C = \sum X_i^2 - \sum Y_j^2$, which belongs to $Z(\mathfrak{g})$. The universal algebra $U(\mathfrak{k})$ is a subalgebra of $U(\mathfrak{g})$. For $D \in U(\mathfrak{k})$, $Df = d\rho(D)f$, due to the K-equivariance of f. Since ρ is a finite-dimensional representation, the function f is annihilated by an ideal of $U(\mathfrak{k})$ of finite codimension. Moreover, f being $Z(\mathfrak{g})$-finite, the vector space $Z(\mathfrak{g}) \cdot U(\mathfrak{k})f = W$ is finite dimensional. The operator $w = C + 2\sum Y_j^2 = \sum X_i^2 + \sum Y_j^2$ is elliptic and belongs to $Z(\mathfrak{g}) \cdot U(\mathfrak{k})$. Hence it keeps W invariant. Since W is finite dimensional, there exists a polynomial P such that $P(w)f = 0$. The operator $P(w)$ is an analytic elliptic operator, hence f is analytic.

3. **Geometric interpretation of condition** (1). G is a principal bundle with basis the Riemannian symmetric space $X = K\backslash G$ and structural group K. Consider the associated bundle $G \times_K V$ corresponding to the representation ρ of K in $GL(V)$: it is the quotient of $G \times V$ by the equivalence relation $(g, v) \approx (k \cdot g, \rho(k) \cdot v)$, and is a bundle with basis X and typical fibre V. Denote by $[G, V]_k$ the set of maps f from G to V that are K-equivariant: $f(kg) = \rho(k) \cdot f(g)$. The group G acts by right translations on $[G, V]_k$. The map f defines then a map $s: G \to G \times V$, such that $s(g) = (g, f(g))$, compatible with the equivalence relation defined by K. Going over to the quotient, s defines a cross section $\sigma: X \to G \times_k V$. This map is an isomorphism of $[G, V]_k$ onto the vector space $S[G \times_k V]$ of sections of $G \times_k V$. The group G operates on $S[G \times_k V]$ by right translations, and this isomorphism is compatible with the action of G. Condition (1) says then that f defines a Γ-invariant cross-section of $G \times_k V$.

4. **Automorphy factors and condition** (1). We shall start with a space X in a certain category (e.g. complex analytic, real analytic, C^∞ manifold $\cdots$), a group Γ of morphisms of X, and a group H acting on a space V. The group Γ will operate on the right on X, but not necessarily as a properly discontinuous transformation group. Denote by $[X, H]$ the set of morphisms of X into H

(i.e., holomorphic, real analytic, C^∞ maps$\cdots$). The group Γ acts on $[X, H]$ through $(\gamma \cdot \phi)(x) = \phi(x \cdot \gamma)$.

DEFINITIONS. (i). An *automorphy factor* of Γ is a 1-cocycle μ of F with value in $[X, H]$, i.e., a map $\mu: X \times \Gamma \to H$ such that

$$\mu(x, \gamma \cdot \gamma') = \mu(x, \gamma) \cdot \mu(x\gamma, \gamma'), \qquad (\dot{x} \in X; \gamma, \gamma' \in \Gamma). \tag{1}$$

(ii). An *automorphic form of type* μ is a morphism $f: X \to V$ satisfying

$$f(x) = \mu(x, \gamma) \cdot f(x \cdot \gamma), \qquad (x \in X, \gamma \in \Gamma). \tag{2}$$

The automorphy factor μ allows one to define an action of Γ on $X \times V$ by:

$$(x, v) \cdot \gamma = (x \cdot \gamma, \mu(x, \gamma) \cdot v). \tag{3}$$

Due to the cocycle condition, Γ is indeed a transformation group on $X \times V$. If Γ operates freely on X as a properly discontinuous transformation group, $(X \times V)/\Gamma$ is a fibre bundle with fibre V and basis X/Γ. The automorphic forms are the cross sections of this bundle, lifted to X via the natural projection.

Assume now that $X = K\backslash G$ as above. To express the condition (2) above, and connect the automorphic forms with geometric objects on X/Γ, we need only to have an automorphy factor on Γ. However, in order to relate such an automorphic form to a function on G satisfying condition (1) of §1, we assume the automorphy factor to be defined on G.

Let 0 be the fixed point of K in X. Then for $k, k' \in K$

$$\mu(0, kk') = \mu(0, k) \cdot \mu(0, k').$$

Thus $\rho: k \mapsto \mu(0, k) = \rho(k)$, is a homomorphism of K into H. Let $\alpha: G \to H$ be the map defined by $\alpha(g) = \mu(0, g)$. Due to the cocycle condition, α is left equivariant for the representation ρ of K: $\alpha \in [G, H]_K$. Hence, it defines a cross-section of $P = G \times_K H$. The space P is obtained by identifying in $G \times H$ the pairs (g, h) and $(k \cdot g, \rho(k) \cdot h)$ $(k \in K)$. The space P is a principal bundle with basis $X = K\backslash G$ and fibre H. The cross-section α makes it possible to identify $G \times_K H$ with $X \times H$. Assuming V to be a vector space, $E = P \times_K V$ is the vector bundle over X associated to P: $E = P \times_H V$. The identification of P with $X \times H$, by means of α, allows one to identify E with $X \times V$ and every section of E with a map from X to V:

$$[G, V]_K \xrightarrow{\sim} [X, V].$$

If $\dot{g} = 0 \cdot g = K \cdot g$ denotes the image of the left K-coset of g in X, the inverse identification is given by $f \mapsto F$, where $F(g) = \alpha(g) \cdot f(\dot{g})$. This map is obviously a G-homomorphism, where the action of G is defined on $[G, V]_K$ by right translations, and on $[X, V]$ by §4 (3). The functions that appear in condition (1) of the definition of automorphic forms are then identified with the functions from X to V which satisfy (ii).

Conversely a cross-section σ of the principal bundle $P = G \times_K H$ defines, in the usual way, a left K-equivariant map $\alpha: G \to H$, and an automorphy factor

μ: $X \times G \to H$, given by $\mu(\dot{g}, g') = \alpha(g)^{-1}$, $\alpha(g \cdot g') = \alpha(k \cdot g)^{-1} \cdot \alpha(k \cdot g \cdot g')$ where $g, g' \in G$, $k \in K$ and $\dot{g} = 0 \cdot g \in X$. It is again possible to identify $[G, V]_K$ with $[X, V]$, by means of μ.

5. **Example.** Let X be a bounded symmetric domain, $X = K\backslash G$. If $\mathfrak{g}$ and $\mathfrak{k}$ are the Lie algebras of G and K respectively, $\mathfrak{g}_C$ and $\mathfrak{k}_C$ their complexifications, then as vector space $\mathfrak{g}_C = \mathfrak{k}_C \oplus \mathfrak{p}_C = \mathfrak{k}_C \oplus \mathfrak{y}^+ \oplus \mathfrak{y}^-$, where $\mathfrak{y}^+$ and $\mathfrak{y}^-$ are commutative subalgebras of $\mathfrak{g}_C$ contained in $\mathfrak{p}_C$. Putting $P^\pm = \exp(\mathfrak{y}^\pm)$, then $G \subset P^- \cdot K_C \cdot P^+$, and the map of $P^- \times K_C \times P^+$ into G_C given by $(x, y, z) \mapsto x \cdot y \cdot z$ is biholomorphic onto a Zariski-open subset of G_C. Let $g = g_- g_0 g_+$ be the decomposition of $g \in G$ with respect to P^-, K_C, P^+. A theorem of Harish-Chandra asserts that the map $G \to \mathfrak{p}^+$, which sends g onto $\log g_+$, identifies $X = K\backslash G$ with a bounded domain D of $\mathfrak{y}^+$. The subspace $P^- \cdot K_C \cdot G$ is open in G_C. Hence

$$P^-\backslash P^- K_C G \cong K_C \times_K G,$$

is a complex analytic principal bundle over $X = K\backslash G$ with K_C as fibre. This fibre space has a natural cross-section v defined by P^+, to which corresponds an automorphy factor μ. If $x \in D \in \mathfrak{y}^+$ and $g \in G$, then

$$\exp x \cdot g = (\exp x \cdot g)_- \cdot (\exp x \cdot g)_0 \cdot (\exp x \cdot g)_+,$$

and

$$\mu(x, g) = (\exp x \cdot g)_0 \in K_C.$$

This is the "canonical automorphy factor" on X, considered in [9]. To recover completely the situation of §§1, 4, one gives a representation $\rho: K_C \to GL(V)$. Then $\mu_\rho(x, g) = \rho((\exp x \cdot g)_0)$. (To get the Jacobian determinant of the bounded realization as an automorphy factor, take $\rho: K_C \to GL_1$ defined by $\rho(k) = \det \cdot \mathrm{Ad}_{\mathfrak{y}^+} k^{-1}$.)

It is not necessary to take P^+ as cross section for the bundle $K_C \times_K G$. Let P' be conjugate to P^+, such that $G \subset P^- \cdot K_C \cdot P'$. Every element $g \in G$ can again be decomposed as $g = g^- \cdot g'_0 g'_+$. Then $\mu'(x, g) = (\exp x \cdot g)'_0$ is again an automorphy factor. There exist a number of canonical choices of P', defined by the so-called partial Cayley transforms, that give rise to unbounded realizations of X (see [1]).

Example. $G = Sp(n, R)$, $K = U(n)$, $K_C = GL(n, C)$.
If

$$g = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

and $K\backslash G$ is realized as the Siegel upper half plane, then the corresponding canonical automorphy factor is

$$\mu(Z, g) = CZ + D.$$

6. **Connection between holomorphy and condition** (2). Let $f\colon X \to V$ be a holomorphic automorphic form defined on X, with automorphy factor μ_ρ; then the corresponding automorphic form F on G is $Z(\mathfrak{g})$-finite, where $F(g) = \mu(0, g)\cdot f(\dot{g})$. This was pointed out in [11, Exp. 10]. One way to see it is to prove first that,

$$Y\cdot F(g) = \mu_\rho(0, g)(\tilde{Y}\cdot f)(\dot{g}) \qquad (Y \in \mathfrak{p}^-), \tag{4}$$

where, due to the definition of the complex structure of X, $\tilde{Y}$ is the derivative with respect to the conjugate of some coordinate-variable in X (see [2, §5]). The function f is holomorphic if and only if $\tilde{Y}f = 0$ $(Y \in \mathfrak{p}^-)$ by (4); this is equivalent to $Y\cdot F = 0$ $(Y \in \mathfrak{p}^-)$. The fact that F is then $Z(\mathfrak{g})$-finite depends now on some properties of $Z(\mathfrak{g})$. As a vector space $\mathfrak{g}_C = \mathfrak{p}^+ \oplus \mathfrak{k}_C \oplus \mathfrak{p}^-$. Hence as a vector space $U(\mathfrak{g}) = U(\mathfrak{p}^+) \otimes U(\mathfrak{k}) \otimes U(\mathfrak{p}^-)$: every $x \in U(\mathfrak{g})$ can accordingly be written as $x = \sum p_i^+ \cdot k_i \cdot p_i^-$. One shows then that if $x \in Z(\mathfrak{g})$, the only terms occurring in this sum are such that p_i^+ and p_i^- are simultaneously zero or different from zero. Hence there exists a linear map $v\colon Z(\mathfrak{g}) \to U(\mathfrak{k}_C)$ such that

$$z - v(z) \in U(\mathfrak{g}_C)\cdot \mathfrak{p}^-, \qquad \text{for } z \in Z(\mathfrak{g}).$$

Since F is annihilated by $\mathfrak{p}^-$, $z\cdot F = v(z)F$. The equivariance of F with respect to K insures that F is annihilated by an ideal in $U(\mathfrak{k})$ of finite codimension. The same will then be true in $Z(\mathfrak{g})$.

7. **Growth condition.** Let W be a finite-dimensional complex vector space and σ a locally faithful representation of G in $GL(W)$. Put on W a structure of Hilbert space invariant by $\sigma(K)$. Let $\|g\| = \operatorname{tr}(g^*\cdot g)$.

Then

$$\|g\cdot h\| \leqq \|g\|\,\|h\| \qquad (g, h \in G),$$

and

$$\|k\cdot g\cdot k'\| = \|g\| \qquad (k, k' \in K, g \in G).$$

If A is the connected component of a maximal $\boldsymbol{R}$-split torus, then $G = K\cdot A^+\cdot K$ (where A^+ is a positive Weyl chamber, for some ordering of the $\boldsymbol{R}$-roots), and the second relation shows that what matters is the behavior of the seminorm on A: for $\alpha \in A$, $\|a\| < c\cdot a^\Lambda$, where c is a constant and Λ is some weight of A^+, dominating the weights of σ ($\Lambda = \sum c_\alpha \Lambda_\alpha$ with $c_\alpha \geqq 0$, Λ_α being fundamental weights). As an example, let σ be the adjoint representation, $\mathfrak{g} = \mathfrak{k} + \mathfrak{p}$ a Cartan decomposition of the Lie algebra of G, and s the corresponding Cartan involution. Then we may put

$$\|g\| = \operatorname{Tr}(\operatorname{Ad} s(g)^{-1}\cdot \operatorname{Ad} g). \tag{5}$$

If $|\ |$ is a norm in the vector space V, and $f\colon G \to V$, the growth condition imposed on f is:

$$\exists\, c > 0 \qquad \text{and} \qquad m \in \boldsymbol{Z}, m \geqq 0,$$

such that

$$|f(g)| \leqq c\|g\|^m.$$

This growth condition really does not depend on the chosen representation σ, since it is easy to see, due to the behavior of the seminorm on A, that if τ is another locally faithful representation of G, there exists a positive integer n, $C_1 > 0$ such that

$$\|g\|_\sigma \leqq C_1\|g\|_\tau^n, \qquad (g \in G).$$

8. **Construction of automorphic forms.** Let $X = K\backslash G$, and $\mu: X \times G \to \mathrm{GL}(V)$ be an automorphy factor. For $\phi: X \to V$, consider the series

$$\sum_{\gamma\in\Gamma} \mu(x, \gamma)\cdot\phi(x\cdot\gamma). \tag{6}$$

If it converges, it will be equal to an automorphic form under suitable assumptions for ϕ (for instance, holomorphy if X is a bounded domain, and μ is itself holomorphic). One can work analogously on G instead of X. Starting from $f: G \to V$, assumed to be $Z(\mathfrak{g})$-finite and K-equivariant, then the series $\sum_\Gamma f(g\cdot\gamma)$, if properly convergent, will represent an automorphic form. It may happen that f is already invariant under some subgroup Γ_∞ of Γ. If Γ_∞ is infinite, the summation will of course be taken over Γ/Γ_∞. The analogous situation for (6) is when ϕ is invariant under Γ_∞, and $\mu(x, \gamma) = 1$ $(x \in X, \gamma \in \Gamma_\infty)$. Two standard examples are the Poincaré series and the Eisenstein series. The former are obtained by imposing on f conditions strong enough so that $\sum_\Gamma \rho(g\gamma)$ converges for any discrete group Γ. For the Eisenstein series, Γ_∞ is in general infinite, and conditions are imposed on Γ and ϕ. We now describe natural generalizations of these notions in the present context.

9. **Poincaré series.** A vector valued function f on G is said to be K-finite on the left (resp. right) if the set of right (resp. left) translates of f under elements of K is a finite-dimensional vector space.

9.1. THEOREM. *Let V be a finite-dimensional vector space, and f a function from G to V. Assume*:

(a) $f \in L^1(G) \otimes V$,

(b) f *is $Z(\mathfrak{g})$-finite,*

(c) f *is K-finite on the left* (*respectively on the right*). *Then the series*

$$P_f(g) = \sum_{\gamma\in\Gamma} f(g\cdot\gamma)$$

converges absolutely and uniformly on compact sets (*respectively, and moreover* $\sum_\Gamma |f(g\cdot\gamma)|$ *is bounded on* G).

Proof of the first assertion (Godement [**11**, Exp. 10]):

$$\int_G |f(g)|\,dg = \int_{G/\Gamma} \sum_\Gamma |f(g\cdot\gamma)|\,dg < \infty.$$

$\sum_\Gamma |f(g)\cdot\gamma)|$ converges in $L^1(G/\Gamma)$, and so converges almost everywhere and also converges in the distribution sense. Now, by assumptions (b) and (c), f is annihilated by an elliptic operator (see (2)). By a general principle (essentially an application of the closed graph theorem) the series converges then in the C^∞-topology; in particular, it converges uniformly on compact sets of G.

To prove the uniform boundedness we use the following lemma of Harish-Chandra [7, Theorem 1]:

9.2. LEMMA. *Let $f: G \to V$ be $Z(\mathfrak{g})$-finite and K-finite on the right (resp. on the left) and U be a neighborhood of e in G. Then there exists an $\alpha \in C_c^\infty(U)$ invariant by inner automorphisms of K such that $f = f * \alpha$ (resp. $f = \alpha * f$).*

(C_c^∞ refers to C^∞-functions with compact support, and $*$ to convolution. Thus

$$f * \alpha(g) = \int_G f(g \cdot u^{-1})\alpha(u)\, du).$$

Proof of uniform boundedness when f is K-finite on the right:

$$f(g \cdot \gamma) = \int_G f(g \cdot \gamma \cdot u^{-1})\alpha(u)\, du = \int_G f(g \cdot v^{-1})\alpha(v \cdot \gamma) dv,$$

$$|f(g \cdot \gamma)| \leqq M \int_{U \cdot \gamma} |f(gv^{-1})|\, dv,$$

if U is small enough $U \cdot \gamma \cap U \cdot \gamma' = \phi$ when $\gamma \neq \gamma'$. So

$$\sum_{\gamma \in \Gamma} |f(g \cdot \gamma)| \leqq M \sum_{\gamma} \int_{U \cdot \gamma} |f(gv^{-1})|\, dv$$

$$\leqq M \int_G |f(v)|\, dv = M \|f\|_{L_1}.$$

REMARK. The above proof for the uniform boundedness is due to Harish-Chandra. A slight variation of it also yields the first assertion. That $\sum f(x \cdot \gamma)$ is uniformly bounded (when f is K-finite on the *right*, and verifies (a), (b)) was proved in the holomorphic case first by Godement [11, Exp. 10]. His argument may be extended to the general case.

10. **Example of the classical Poincaré series.** Let $X = K\backslash G$ be a bounded symmetric domain. Take as automorphy factor $J(x, g)$ the determinant of the Jacobian. If f is a polynomial in $C^N \supset X$, then

$$P(x) = \sum_{\gamma \in \Gamma} J(x, \gamma)^l \cdot f(x\gamma),$$

converges absolutely and uniformly on compact sets for $l \geqq 2$, and

$$\tilde{P}(g) = J(o, g)^l \cdot P(\dot{g})$$

is uniformly bounded. More strongly:

$$\sum_{\Gamma} |J(o, g\gamma)|^{l}|f(0 \cdot g\gamma)| < C < \infty$$

where o denotes the coset K in X.

PROOF. In the identification of X with a bounded domain $\mathfrak{y}^{+} = C^{N}$ the coset o is mapped into the origin. Hence K is linear and the polynomial f is K-finite on the right. The function $F(g) = J(o, g)^{l} \cdot f(g)$ is $Z(\mathfrak{g})$-finite (cf. §6). To apply the previous theorem, it is enough to show that F belongs to $L^{1}(G) \otimes V$ for $l \geqq 2$. X being a bounded domain, f is bounded on X. So

$$\int_{G} |F(g)|\, dg \leqq C \cdot \int_{G} |J(o, g)|^{l}\, dg.$$

It is easily seen that

$$|J(o, kgk')| = |J(o, g)| \qquad (k, k' \in K; g \in G);$$

hence $|J(o, g)|$ may be viewed as a K-invariant function on X. Therefore,

$$\int |J(o, g)|^{l}\, dg \leqq C' \cdot \int_{X} |J(o, x)|^{l}\, dw,$$

where dw is an invariant measure on X. But $dw = c \cdot |J(o, x)|^{-2}\, dx\, (c > 0)$, where dx is the usual Lebesgue measure on $\boldsymbol{R}^{2n}$. Consequently, we are reduced to showing that $J(o, x)$ is bounded on X. Since $X = o \cdot A \cdot K$, it is enough to check this on $o \cdot A$, which is easy (see for instance [2, §1]).

If $\tau : K \to GL(V)$ and $\mu_{\tau}(x, g)$ is the automorphy factor of §5, then there exists an l_0 such that

$$\sum_{\gamma \in \Gamma} J(x, \gamma)^{l} \mu_{\tau}(x, \gamma) \cdot f(x \cdot \gamma)$$

converges for $l \geqq l_0$ (see [2, §5] for more details).

11. **Eisenstein series.** Let G be a connected semisimple algebraic group defined over $k \subset \boldsymbol{R}$, P a standard (not necessarily minimal) parabolic k subgroup of G, for a maximal k-split torus S. If P_0 is a minimal parabolic k-subgroup between S and P, let θ be the subset ${}_{k}\Delta$ of simple roots of $\Phi(G, S)$, for the ordering defined by P_0, such that $P = {}_{k}P_{\theta}$ (see [3, §6.5). Then

$$P_0 = Z(S_0) \cdot U_0,$$
$$P = Z(S_{\theta}) \cdot U_0 = Z(S_{\theta}) \cdot U,$$

where $U = R_{u}(P)$ and $S_{\theta} = (\bigcap_{\alpha \in \theta} \operatorname{Ker} \alpha)^{0}$. Put $\theta' = {}_{k}\Delta - \theta$ and $\chi = \det \operatorname{Ad}_{\mathfrak{u}}$, where $\mathfrak{u}$ is the Lie algebra of U: for $p \in P_{\boldsymbol{R}}$ $p^{\chi} = \det \operatorname{Ad}_{\mathfrak{u}} p$. The character χ is then a positive linear combination of the fundamental highest k-weights Λ_{α} of $G : \chi = \sum_{\alpha \in \theta'} e_{\alpha} \Lambda_{\alpha}$, $(e_{\alpha} > 0)$, where the Λ_{α} verify $(\Lambda_{\alpha}, \beta) = d_{\alpha} \delta_{\alpha\beta}$ $(\alpha, \beta \in {}_{k}\Delta, d > 0)$. Let $s = (s_{\alpha})_{\alpha \in \theta'}$ be a set of complex numbers. Put $\Lambda_{s} = \sum_{\alpha \in \theta'} s_{\alpha} \Lambda_{\alpha}$ and $p^{\Lambda_{s}} = \Pi |p^{\Lambda_{\alpha}}|^{s_{\alpha}}$:

If $A = S^0_{\mathbf{R}}$, $G_{\mathbf{R}} = K \cdot P_{\mathbf{R}} = K \cdot M_{\mathbf{R}} \cdot A \cdot U$. If $g = kmau$ is the corresponding decomposition of $g \in G$, then $k \cdot m$, a and u are uniquely determined; we let $a(g)$ denote the A-component of $g \in G$.

11.1. LEMMA (GODEMENT). *Let Γ be a discrete subgroup of $G_{\mathbf{R}}$ and Γ_∞ a subgroup of $\Gamma \cap (M \cdot U)_{\mathbf{R}}$. Assume that*

(1) *$a(\gamma)^{\Lambda_\alpha} \geqq d > 0$ for all $\gamma \in \Gamma$ and $\alpha \in \theta'$,*

(2) *$(M \cdot U)_{\mathbf{R}}/\Gamma_\infty$ has finite-invariant measure,*

(3) *$Rs_\alpha > e_\alpha$, for all $\alpha \in \theta'$.*

Then $E(g, s) = \sum_{\gamma \in \Gamma/\Gamma_\infty} a(g \cdot \gamma)^{-\Lambda_s}$ converges uniformly on any compact set of G.

(Note that, $M \cdot U$ being contained in the kernel of every k-character of P, $a(g \cdot \gamma)^{\Lambda_\alpha} = a(g)^{\Lambda_\alpha}$ for $\gamma \in \Gamma_\infty$ and $M \cdot U$ is unimodular.)

SKETCH OF THE PROOF. We may assume the s_α to be real. Let C be a compact subset of G. Then there exist $d, d' > 0$ such that

$$d \cdot a(g)^{-\Lambda_s} \leqq a(c \cdot g)^{-\Lambda_s} \leqq d' \cdot a(g)^{-\Lambda_s} \qquad (g \in G, c \in C).$$

This implies readily that the uniform convergence on compact sets is equivalent to the convergence at one point, say e. Furthermore, if C is a neighborhood of e, the convergence at e is equivalent to the convergence of the series

$$\sum_\gamma \int_C a(c \cdot \gamma)^{-\Lambda_s}\, dg.$$

Take C small enough so that $C \cdot C^{-1} \cap \Gamma = \{e\}$. Then the series is majorized by

$$I = \int_{C \cdot \Gamma/\Gamma_\infty} a(g)^{-\Lambda_s}\, dg.$$

Let

$$A(t) = \{a \in A \mid a^{\Lambda_\alpha} \geqq t \quad (\alpha \in \theta')\}.$$

By assumption $\Gamma \subset K \cdot M \cdot A(t') \cdot U$, for some $t' > 0$, whence the existence of $t > 0$ such that $C \cdot \Gamma \subset K \cdot M \cdot A(t) \cdot U$.

We have $K \cdot M \cdot A(t) \cdot U = K \cdot A(t) \cdot M \cdot U$. By assumption there exists $w \subset M \cdot U$, of finite measure, such that $M \cdot U = w \cdot \Gamma_\infty$. From this we deduce without difficulty that

$$I \leqq \delta \cdot \int_{KA(t)w} a^{-\Lambda_s}\, dg, \qquad (\delta > 0).$$

By standard facts about Haar measures, the last integral is, up to a constant, equal to

$$\int_K dk \int_w dv \int_{A(t)} a^{-\Lambda_s + \chi}\, da = d \int_{A(t)} a^{-\Lambda_s + \chi}\, da,$$

where $\chi = \sum e_\alpha \cdot \Lambda_\alpha = \det \mathrm{Ad}_u$ (see beginning of this section), and dk, dv, da, are

Haar measures on K, $M\cdot U$ and A respectively. The last integral is a product, (over $\alpha\in\theta'$) of integrals of the form

$$\int_t^\infty \exp[(-s_\alpha + e_\alpha)\cdot t]\,dt,$$

hence converges, since we assume $s_\alpha > e_\alpha$.

11.2. Theorem. *Let $f: G_{\mathbf{R}} \to V$, where V is a finite-dimensional vector space. Keeping the same notations as above, suppose that*

(i) *the assumptions* (1), (2) *and* (3) *of the lemma are satisfied,*

(ii) $f(g\cdot\gamma) = f(g)$ *for* $\gamma\in\Gamma_\infty$,

(iii) $|f(g\cdot p)|p^{\Lambda_s}$ *is bounded if g stays in a compact set of G and $p\in P_{\mathbf{R}}$.*

Then the series $E_f(g) = \sum_{\Gamma/\Gamma_\infty} f(g\cdot\gamma)$ converges absolutely and uniformly on any compact set of G.

Proof. We have $G = K\cdot P_{\mathbf{R}}$, hence

$$\begin{aligned} f(g)\cdot a(g)^{\Lambda_s} &= f(k\cdot p)\cdot a(k\cdot p)^{\Lambda_s} \\ &= f(k\cdot p)\cdot a(p)^{\Lambda_s} = f(k\cdot p)\cdot p^{\Lambda_s}, \\ |f(g)\cdot a(g)^{\Lambda_s}| &= |f(k\cdot p)|p^{\Lambda_s} \leqq C. \end{aligned}$$

Hence

$$\begin{aligned} |f(g)| &\leqq C|a(g)|^{-\Lambda_s}, \\ \sum_{\Gamma/\Gamma_\infty} |f(g\cdot\gamma)| &\leqq C\cdot \sum_{\Gamma/\Gamma_\infty} |a(g)|^{-\Lambda_s}. \end{aligned}$$

The lemma ensures that the last series converges. This proves the theorem. The series E_f will be called an Eisenstein series.

12. Special cases of Eisenstein series.

12.1. Theorem. *We keep the notation of the previous section and assume moreover that $k = \mathbf{Q}$, that Γ is an arithmetic group, and Γ_∞ a subgroup of finite index in $\Gamma\cap P$. Then the assumptions of* (1) *and* (2) *of the lemma in* §11.1 *are fulfilled.*

Proof. (1) $(M\cdot U)_{\mathbf{R}}$ has no nontrivial character defined over $\mathbf{Q}$, and Γ_∞ is an arithmetic subgroup of $(M\cdot U)_{\mathbf{R}}$. So $(M\cdot U)_{\mathbf{R}}/\Gamma_\infty$ has finite volume by reduction theory [4, Theorem 9.1].

(2) Let ρ_α be an irreducible representation of G, which is strongly rational over $\mathbf{Q}$, having Λ_α $(\alpha\in\theta')$ as highest weight [3, §7]. If e_α is a corresponding weight vector in the representation space F_α of ρ_α one has $\rho(p)(e_\alpha) = p^{\Lambda_\alpha}\cdot e_\alpha$ $(p\in P)$ because $\alpha\in\theta'$. There exists a lattice L_α in $F_{\alpha\mathbf{Q}}$ invariant under Γ. We may assume that $e_\alpha\in L_\alpha - \{0\}$. So $\rho_\alpha(\Gamma)\cdot e_\alpha\in L - \{0\}$. There exists a $d > 0$ such that $|\rho_\alpha(\gamma)\cdot e_\alpha| > d$ for every $\gamma\in\Gamma$. Write $\gamma = k\cdot m\cdot a(\gamma)u$. Since M and U lie in P and

have no Q-character, one has

$$d < |\rho_\alpha(\gamma)e_\alpha| = |\rho_\alpha(a(\gamma))\cdot e_\alpha| = a(\gamma)^{\Lambda_\alpha}.$$

This proves condition (2) of the lemma.

If $f: G_R \to V$ verifies the identity $f(g\cdot p) = f(g)p^{-\Lambda_\alpha}$, then f satisfies the hypotheses (iii) and (ii) of the convergence theorem ((ii) because Γ_∞ lies in the kernel of all Q-characters of P). One gets with such functions a straightforward generalization of the classical Eisenstein series.

If moreover f is ρ-equivariant on the left with respect to K, then it follows from standard facts about the universal enveloping algebra $U(\mathfrak{g})$ that E_f is $Z(\mathfrak{g})$-finite. Moreover, the growth condition can also be checked using reduction theory. Thus we get automorphic forms in the sense of §1.

A typical function satisfying $f(g\cdot p) = f(g)\cdot p^{-\Lambda_\alpha}$ $(p\in P)$ is given by $f(g) = |\rho_\alpha(g)\cdot e_\alpha|$. These functions are also connected with minimum properties on Siegel-domains.

EXAMPLES 1. Let $G = Sp(n, C)$, and P be the maximal parabolic group, consisting of the matrices

$$\begin{pmatrix} A & B \\ 0 & D \end{pmatrix}$$

in the standard notation. Then, as function $f(g)$, we may take $\det(C\cdot i + D)$.

2. Let $G = SL_n$, $K = SO(n)$, $= SL(n, Z)$. The fundamental representation of G are the exterior powers of the identity representation of G. For an ordering of the roots associated to the group of upper triangular matrices, the highest weight of the ith exterior power is $e_1 \wedge \cdots \wedge e_i$, where (e_i) is the canonical basis of R^n $(1 \leqq i \leqq n-1)$. The corresponding function is then

$$\Phi_i(g) = \|g\cdot e_1 \wedge \cdots \wedge g\cdot e_i\|.$$

Let P_i be the stability group of the flag

$$[e_1] \subset [e_1, e_2] \subset \cdots \subset [e_1, \cdots, e_i].$$

Then for Rs_j sufficiently big, $(1 \leqq j \leqq i)$,

$$\sum_{\gamma\in\Gamma/\Gamma\cap P_i} \Phi_1(g\cdot\gamma)^{-s_1}\cdots\Phi_i(g\cdot\gamma)^{-s_i},$$

is an Eisenstein series. Such series have been considered by Selberg [10].

3. We return to the situation of the theorem in §12.1. Let $\rho: K \to GL(V)$ be a finite-dimensional representation of K. Let $\Phi: G \to V$ be a continuous function which is ρ-equivariant, with respect to K, is right invariant with respect to $A\cdot U_R$, and is a cusp form on M_R for $\Gamma_\infty \cap M$ (for the notion of cusp form, see [5]). We may define a function $f: G \to V$ by $f(k\cdot m\cdot a\cdot u) = \Phi(k\cdot m)\cdot a^{\Lambda_\alpha}$. Since a cusp form is bounded, it is easily seen that f satisfies the condition of the theorem.

The corresponding Eisenstein series is then

$$E_f = \sum_{\gamma\in\Gamma/\Gamma_\infty} f(g\cdot\gamma) = \sum_{\gamma\in\Gamma/\Gamma_\infty} \Phi(g\cdot\gamma)\cdot a(g\cdot\gamma)^{-\Lambda_s}.$$

Such series occur in the work of Selberg, and of Langlands [**8**].

4. Finally, we note that the Poincaré–Eisenstein series which are used in [**1**; **2**] to study the compactification of X/Γ, when X is a bounded symmetric domain are special cases of the series considered in §11.2. In this case, M is the almost direct product of two normal $\boldsymbol{Q}$-subgroups M_1, M_2 and, roughly speaking, the function f, restricted to $M_{\mathbf{R}}$ is the product of a constant function on $M_{\mathbf{R}}$ by a Poincaré series (hence a cusp form) on $M_{2\mathbf{R}}$.

References

1. W. Baily, *On compactifications of orbit spaces of arithmetic discontinuous groups acting on bounded symmetric domains*. Proc. Sympos. Pure Math., vol. 9, Amer. Math. Soc., Providence, R.I., 1966, pp. 281–295.

2. W. Baily and A. Borel, *Compactification of arithmetic quotients of bounded symmetric domains*, (to appear).

3. A. Borel, *Linear algebraic groups*, Proc. Sympos. Pure Math., vol. 9, Amer. Math. Soc., Providence, R.I., 1966, pp. 3–19.

4. A. Borel and Harish-Chandra, *Arithmetic subgroups of algebraic groups*, Ann. of Math. (2) **75** (1962), 485–535.

5. R. Godement, *The spectral decomposition of cusp-forms*, Proc. Sympos. Pure Math., vol. 9, Amer. Math. Soc., Providence, R.I., 1966, pp. 225–234.

6. Harish-Chandra, *Automorphic forms on a semi-simple Lie group*, Proc. Nat. Acad. Sci. U.S.A. **45**, (1959), 570–573.

7. ———, *Discrete series for semi-simple Lie groups*. II, (to appear).

8. R. Langlands, *Eisenstein series*; Proc. Sympos. Pure Math., vol. 9, Amer. Math. Soc., Providence, R.I., 1966, pp. 235–252.

9. S. Murakami, *Cohomologies of vector-valued forms on compact, locally symmetric Riemann manifolds*, Proc. Sympos. Pure Math., vol. 9, Amer. Math. Soc., Providence, R.I., 1966, pp. 387–399.

10. A. Selberg, *Harmonic analysis and discontinuous groups*, J. Indian Math. Soc. **20** (1956), 47–87.

11. Séminaire H. Cartan, *Fonctions automorphes*, 2 vols., 10ème année (1957/1958), Paris, 1958 (Mimeographed notes).

(From Notes by F. Bingen)

The Decomposition of $L^2(G/\Gamma)$ for $\Gamma = \mathrm{SL}(2, \boldsymbol{Z})$

BY

R. GODEMENT

$$G = \mathrm{SL}(2, \boldsymbol{R}); \qquad \Gamma = \mathrm{SL}(2, \boldsymbol{Z});$$

$$U\text{: subgroup } \quad u = \begin{pmatrix} 1 & u \\ O & 1 \end{pmatrix};$$

$$H\text{: subgroup } \quad h = \begin{pmatrix} t & O \\ 0 & 1/t \end{pmatrix}, \quad t \neq 0;$$

$$M\text{: subgroup } \quad m = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}.$$

The Iwasawa decomposition is here

$$G = MHU, \qquad M \cap H = \{\pm 1\}.$$

The Haar measure of G is given by

$$(1) \qquad \int_G \phi(g)\,dg = \iiint_{M \times H \times U} \phi(mhu)\beta(h)\,dm\,dh\,du = \iiint \phi(muh)\,dm\,dh\,du$$

where

$$\beta(h) = t^2 \quad \text{if} \quad h = \begin{pmatrix} t & 0 \\ 0 & 1/t \end{pmatrix}.$$

Bruhat's decomposition is given by

$$G = HU \cup UwHU \quad \text{where} \quad w = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

2. The Laplace transform of a modular function. The principal series of irreducible unitary representations of G is obtained by letting G operate through the operators $\phi(g) \mapsto \phi(x^{-1}g)$ on the Hilbert space $\mathscr{H}(s)$ of functions ϕ on G such that

$$(2) \qquad \phi(ghu) = \phi(g)\beta(h)^{s-1}, \qquad \|\phi\|^2 = \int_M |\phi(m)|^2\,dm.$$

The representation is unitary if $\mathrm{Re}(s) = \frac{1}{2}$ and then irreducible, except for $s = \frac{1}{2}$.

Consider now a "modular function," i.e., a function $\Phi(g)$ such that $\Phi(g\gamma) = \Phi(g)$ for all $\gamma \in \Gamma$; then $u \mapsto \Phi(gu)$ is invariant under

$$\Gamma_\infty = \Gamma \cap U, \quad \text{integral matrices} \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix},$$

and one thus can consider

$$\Phi^0(g) = \int_{U/\Gamma_\infty} \Phi(gu)\,du \tag{3}$$

i.e., the "constant" term in the Fourier expansion

$$\Phi(gu) = \sum \Phi^n(g) e^{2\pi inu}. \tag{3'}$$

Define the *formal Laplace transform* of Φ as

$$\hat{\Phi}(g, s) = \int_H \Phi^0(gh)\beta(h)^{1-s}\,dh; \tag{4}$$

up to convergence this is an element $\hat{\Phi}(s)$ of $\mathscr{H}(s)$ and the map $\Phi \mapsto \hat{\Phi}(s)$ commutes with the operations of G (left translations).

As to convergence the simplest case is as follows:

(5) $\hat{\Phi}(g, s)$ *exists for* $\operatorname{Re}(s) > 1$ *if* Φ *is bounded and with compact carrier* mod Γ.

Firstly $\Phi^0(g)$ is bounded; secondly $\Phi^0(gh)$ vanishes for $|t|$ small because for every $c > 0$ the part $\{|t| < c\}$ of H is mapped *properly* into G/Γ; hence it remains to show that

$$\int_{|t| \geqq c} \beta(h)^{1-s}\,dh \sim \int_c^{+\infty} \frac{dt}{t^s}$$

converges for $\operatorname{Re}(s) > 1$.

The same result more generally holds if Φ is bounded and "rapidly decreasing" at infinity in G/Γ, i.e., if for every N

$$\Phi(mhu) = O(|t|^N) \quad \text{as} \quad |t| \to 0$$

uniformly in m and u.

3. Incomplete theta series. Let $\mathscr{D}(G/U)$ be the space of C^∞ functions on G which are invariant under U and have a compact carrier mod U; since

$$G/U \cong \boldsymbol{R}^2 - \{0\}$$

this is also the space of C^∞ functions in the real plane, vanishing around 0 and ∞.

If $\phi \in \mathscr{D}(G/U)$ we define

$$\theta_\phi(g) = \sum_{\Gamma/\Gamma_\infty} \phi(g\gamma) = \sum_{\Gamma/\Gamma_\infty} \phi[g\gamma(e_1)] = \sum_{\xi \in \boldsymbol{Z}^2;\, \xi \text{ prime}} \phi[g(\xi)] \tag{6}$$

where e_1 is the first basis vector in $\boldsymbol{R}^2$ [so that $g \mapsto g(e_1)$ induces the identification $G/U \cong \boldsymbol{R}^2 - \{0\}$]. Of course $\theta_\phi \in \mathscr{D}(G/\Gamma)$, i.e., is C^∞ with compact carrier mod Γ.

We have

$$\theta_\phi^0(g) = \int_{U/\Gamma_\infty} du \sum_{\Gamma/\Gamma_\infty} \phi(gu\gamma) = \sum_{\Gamma_\infty\backslash\Gamma/\Gamma_\infty} \int_{U/\Gamma_\infty(\gamma)} \phi(gu\gamma)\, du,$$

where

$$\begin{aligned}\Gamma_\infty(\gamma) = \Gamma_\infty \cap \gamma\Gamma_\infty\gamma^{-1} &= \Gamma_\infty \text{ if } \gamma \in \pm\Gamma_\infty \\ &= \{e\} \text{ if } \gamma \notin \pm\Gamma_\infty.\end{aligned}$$

Hence, and assuming $\phi(-g) = \phi(g)$, we get

$$\tfrac{1}{2}\theta_\phi^0(g) = \phi(g) + \sum_{(\gamma)} \int_U \phi(gu\gamma)\, du$$

where $\sum_{(\gamma)}$ is extended to the nontrivial double cosets $\pm\Gamma_\infty\gamma\Gamma_\infty$ (with γ and $-\gamma$ identified).

But then $\gamma \in UwHU$ i.e.,

$$\gamma = u_\gamma' w h_\gamma u_\gamma'',$$

from which it follows at once that

$$\begin{aligned}\tfrac{1}{2}\theta_\phi^0(g) &= \phi(g) + \sum_{(\gamma)} \int_U \phi(guwh_\gamma)\, du \\ &= \phi(g) + \sum_{(\gamma)} \int_U \phi(guh_\gamma^{-1}w)\, du,\end{aligned}$$

$$\tfrac{1}{2}\theta_\phi^0(g) = \phi(g) + \sum_{(\gamma)} \beta(h_\gamma)^{-1} \int_U \phi(gh_\gamma^{-1}uw)\, du. \tag{7}$$

Observe that

$$\begin{aligned}\|\theta_\phi\|^2 &= \int_{G/\Gamma} |\theta_\phi(g)|^2\, d\dot{g} = \int_{G/\Gamma} d\dot{g} \sum_{\Gamma/\Gamma_\infty} \theta_\phi(g)\overline{\phi(g\gamma)} \\ &= \int_{G/\Gamma} d\dot{g} \sum_{\Gamma/\Gamma_\infty} \theta_\phi(g\gamma)\overline{\phi(g\gamma)} = \int_{G/\Gamma_\infty} \theta_\phi(g)\overline{\phi(g)}\, d\dot{g} \\ &= \int_{G/U} d\dot{g} \int_{U/\Gamma_\infty} \theta_\phi(gu)\overline{\phi(gu)}\, du = \int_{G/U} \overline{\phi(g)}\, d\dot{g} \int_{U/\Gamma_\infty} \theta_\phi(gu)\, du\end{aligned}$$

so that

$$\begin{aligned}\|\theta_\phi\|^2 &= \int_{G/U} \theta_\phi^0(g)\overline{\phi(g)}\, dg = \iint \theta_\phi^0(mh)\overline{\phi(mh)}\beta(h)\, dm\, dh \\ &= \iint [\theta_\phi^0(mh)\beta(h)^{1-s}]\overline{\phi(mh)\beta(h)^{\bar{s}}}\, dm\, dh;\end{aligned}$$

defining

$$L_\phi(g, 2s) = \int_H \phi(gh)\beta(h)^s \, dh \tag{8}$$

[this is an *integral* function of s if $\phi \in \mathscr{D}(G/U)$] and applying Plancherel's formula on a line $\operatorname{Re}(s) = \sigma > 1$, we get

$$\|\theta_\phi\|^2 = \frac{1}{\pi^2}\int dm \int_{\operatorname{Re}(s)=\sigma>1} \hat{\theta}_\phi(m, s)\overline{L_\phi(m, 2\bar{s})}\, ds. \tag{9}$$

4. Eisenstein series. From (8) it follows that

$$L_\phi(ghu, 2s) = L_\phi(g, 2s)\beta(h)^{-s}$$

i.e., the function $g \mapsto L_\phi(g, 2s)$ belongs to $\mathscr{H}(1 - s)$. On the other hand the Fourier inversion formula shows that

$$\phi(g) = \frac{1}{\pi}\int_{\operatorname{Re}(s)=\sigma} L_\phi(g, 2s)\, ds$$

(note that $s \mapsto L_\phi(g, 2s)$ is rapidly decreasing in every vertical strip), so that

$$\theta_\phi(g) = \sum_{\Gamma/\Gamma_\infty} \phi(g\gamma) = \frac{1}{\pi}\int_{\operatorname{Re}(s)=\sigma} E_\phi(g, s)\, ds \tag{10}$$

where

$$E_\phi(g, s) = \sum_{\Gamma/\Gamma_\infty} L_\phi(g\gamma, 2s) \tag{11}$$

is a so-called Eisenstein series. These computations are at first purely formal; but *the series* (11) *converges for* $\operatorname{Re}(s) > 1$ *and* (10) *is justified in this range of values of* s.

To see the convergence of (11) we may assume that $g = e$ (replace ϕ by a left-translate of ϕ) and write

$$\phi(g) = \int_U F(gu)\, du$$

for some continuous function $F(g)$ with compact carrier on G. Then

$$\begin{aligned} E_\phi(e, s) &= \sum_{\Gamma/\Gamma_\infty} \iint_{H\times U} F(\gamma hu)\beta(h)^s \, dh\, du = \sum_{\Gamma/\Gamma_\infty} \iint_{H\times U} F(\gamma uh)\beta(h)^{s-1}\, dh\, du \\ &= \int_H \beta(h)^{1-s}\, dh \int_{U/\Gamma_\infty} du \sum_\Gamma F(\gamma u^{-1}h^{-1}); \end{aligned}$$

considering $\Phi(x) = \sum_\Gamma F(\gamma x^{-1})$ which is bounded with compact carrier mod Γ

one gets

$$E_\phi(e, s) = \int_H \beta(h)^{1-s}\, dh \int_{U/\Gamma_\infty} \Phi(hu)\, du = \hat{\Phi}(e, s)$$

and the convergence for Re$(s) > 1$ follows from (5).

As for the fact that

$$\int_{\mathrm{Re}(s)=\sigma>1} ds \sum_{\Gamma/\Gamma_\infty} L_\phi(g\gamma, 2s) = \sum_{\Gamma/\Gamma_\infty} \int_{\mathrm{Re}(s)=\sigma>1} L_\phi(g\gamma, 2s)\, ds,$$

it is easily justified by using uniform majorations for $L_\phi(g, 2s)$ on the line Re$(s) = \sigma$.

5. Analytic continuation of Eisenstein series. Let $\phi \in \mathscr{D}(G/U)$ and consider ϕ as a function on $\boldsymbol{R}^2$, so that $\phi(g) = \phi[g(e_1)]$. Then

$$(12) \qquad L_\phi(g, 2s) = \int \phi[g(e_1)t]t^{2s}d^*t \quad \text{where } d^*t = dt/t,$$

(we consider $\boldsymbol{R}^2$ as a *right* vector space) and thus

$$E_\phi(g, s) = \int t^{2s}d^*t \sum_{\Gamma/\Gamma_\infty} \phi[g\gamma(e_1)t] = \int t^{2s}d^*t \sum_{\xi\in\boldsymbol{Z}^2;\xi \text{ prime}} \phi[g(\xi)t].$$

But every nonzero $\xi \in \boldsymbol{Z}^2$ can be written in one and only one way as $\xi = n\eta$ where n is a positive integer and η is a primitive vector; hence

$$(13) \qquad \zeta(2s)E_\phi(g, s) = \int t^{2s}\, d^*t \sum_{\xi\in\boldsymbol{Z}^2;\,\xi\neq 0} \phi[g(\xi)t].$$

If we now consider the Fourier transform

$$(14) \qquad \hat{\phi}(x) = \int_{\boldsymbol{R}^2} \phi(y)e^{-2\pi i\langle w(x),\, v\rangle}\, dy$$

of ϕ, and if we assume

$$(15) \qquad \hat{\phi}(0) = 0 \quad \text{i.e.,} \int_{G/U} \phi(g)\, dg = 0$$

i.e., θ_ϕ orthogonal to 1 in $L^2(G/\Gamma)$, then Poisson's formula leads to

$$\sum_{\xi\in\boldsymbol{Z}^2;\,\xi\neq 0} \phi[g(\xi)t] = t^{-2} \sum_{\xi\in\boldsymbol{Z}^2;\,\xi\neq 0} \hat{\phi}[g(\xi)t^{-1}] \quad \text{since } \phi(0) = \hat{\phi}(0) = 0;$$

defining

$$\Xi_\phi(g, s) = \zeta(2s)E_\phi(g, s) = \int_{t\neq 0} \Theta_\phi(g, t)t^{2s}\, d^*t$$

where $\Theta_\phi(g, t) = \sum_{\xi \neq 0} \phi[g(\xi)t]$, one gets

$$\begin{aligned}\Xi_\phi(g, s) &= \int_{|t| \geqq 1} \Theta_\phi(g, t)t^{2s}\, d^*t + \int_{|t| \leqq 1} \Theta_\phi(g, t)t^{2s}\, d^*t \\ &= \int_{|t| \geqq 1} \Theta_\phi(g, t)t^{2s}\, d^*t + \int_{|t| \geqq 1} \Theta_{\hat\phi}(g, t)t^{2(1-s)}\, d^*t;\end{aligned}$$

hence, by the usual methods, the following result: *under* (15) *the function* $\zeta(2s)E_\phi(g, s)$ *is an integral function of s and does not change under*

$$(s, \phi) \mapsto (1 - s, \hat\phi).$$

It would have been more symmetrical to start with a function

$$\phi \in \mathscr{S}(G/U) \text{ such that } \phi(0) = \hat\phi(0) = 0$$

where $\mathscr{S}(G/U)$ means the set of rapidly decreasing functions on $\boldsymbol{R}^2$; the Fourier transform is a bijection of $\mathscr{S}(G/U)$ onto $\mathscr{S}(G/U)$ but not of course of $\mathscr{D}(G/U)$ onto $\mathscr{D}(G/U)$!

On the other hand, deleting the assumption that $\int_{G/U} \phi(g)\, dg = 0$ would lead to a pole at $s = 1$.

The classical series

$$\sum \frac{y^{s-k}}{|cz + d|^{2s-2k}(cz + d)^{2k}}$$

would be obtained by taking for instance

$$\phi(g) = (a + ic)^{2k} e^{-\pi(a^2+c^2)} \quad \text{if } g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

6. Analytic continuation of Laplace transforms. Let $\phi \in \mathscr{D}(G/U)$ so that

$$\hat\theta_\phi(g, s) = \int \theta^0_\phi(gh)\beta(h)^{1-s}\, dh$$

exists for Re(s) > 1. By Equation (7) we have

$$\begin{aligned}\tfrac{1}{2}\hat\theta_\phi(g, s) &= \int \phi(gh)\beta(h)^{1-s}\, dh + \sum_{(\gamma)} \beta(h_\gamma)^{-1} \iint \phi(ghh_\gamma^{-1}uw)\beta(h)^{1-s}\, dh\, du \\ &= L_\phi(g, 2 - 2s) + \sum_{(\gamma)} \beta(h_\gamma)^{-s} \iint \phi(ghuw)\beta(h)^{1-s}\, dh\, du \\ &= L_\phi(g, 2 - 2s) + \text{Ч}(s) \iint \phi(guwh)\beta(h)^{s}\, dh\, du\end{aligned}$$

i.e.,

$$\tfrac{1}{2}\hat{\theta}_\phi(g, s) = L_\phi(g, 2 - 2s) + \text{Ч}(s)\int L_\phi(guw, 2s)\,du \tag{16}$$

where

$$\text{Ч}(s) = \sum_{(\gamma)} \beta(h_\gamma)^{-s} = \sum_{(\gamma)} \frac{1}{c_\gamma^{2s}} \qquad \text{where } \gamma = \begin{pmatrix} a_\gamma & b_\gamma \\ c_\gamma & d_\gamma \end{pmatrix}; \tag{17}$$

since there are $\phi(n)$ (Euler's function) classes $(\gamma) = \Gamma_\infty \gamma \Gamma_\infty$ such that $c_\gamma = n$ we get

$$\text{Ч}(s) = \sum_1^\infty \frac{\phi(n)}{n^{2s}} = \frac{\zeta(2s - 1)}{\zeta(2s)}. \tag{18}$$

On the other hand let us compute for $\operatorname{Re}(s) > 1$

$$E_\phi^0(g, s) = \int_{U/\Gamma_\infty} du \sum_{\Gamma/\Gamma_\infty} L_\phi(gu\gamma, 2s);$$

the computations that led to (7) lead here to

$$\begin{aligned}\tfrac{1}{2}E_\phi^0(g, s) &= L_\phi(g, 2s) + \sum_{(\gamma)} \int L_\phi(guwh_\gamma, 2s)\,du \\ &= L_\phi(g, 2s) + \sum_{(\gamma)} \beta(h_\gamma)^{-s} \int L_\phi(guw, 2s)\,du\end{aligned}$$

i.e., to

$$\tfrac{1}{2}E_\phi^0(g, s) = L_\phi(g, 2s) + \text{Ч}(s) \int_U L_\phi(guw, 2s)\,du, \quad \operatorname{Re}(s) > 1. \tag{19}$$

Since we have seen that $\zeta(2s)E_\phi(g, s)$ is an entire * function invariant under $(\phi, s) \mapsto (\hat{\phi}, 1 - s)$ the same is true for $\zeta(2s)E_\phi^0(g, s)$, and we necessarily have

$$\zeta(2s)\text{Ч}(s)\int L_\phi(guw, 2s)\,du = \zeta(2 - 2s)L_{\hat{\phi}}(g, 2 - 2s) \tag{20}$$

i.e.,

$$\int L_\phi(guw, 2s)\,du = \frac{\zeta(2 - 2s)}{\zeta(2s - 1)} L_{\hat{\phi}}(g, 2 - 2s), \quad \operatorname{Re}(s) > 1. \tag{21}$$

Comparing with (16) we get

$$\tfrac{1}{2}\hat{\theta}_\phi(g, s) = L_\phi(g, 2 - 2s) + \frac{\zeta(2 - 2s)}{\zeta(2s)} L_{\hat{\phi}}(g, 2 - 2s). \tag{22}$$

* provided $\int_{G/U} \phi(g)\,d\dot{g} = 0$, which we shall assume henceforth.

The function

$$L_{\hat\phi}(g, 2s) = \int \hat\phi(gh)\beta(h)^s\, dh = 2\int_0^{+\infty} \hat\phi[g(e_1)t]t^{2s}\, d^*t$$

is meromorphic since $\hat\phi$ is C^∞ and rapidly decreasing at infinity; since $\hat\phi(0) = 0$, the only poles [consider $\int_0^{+\infty} = \int_0^1 + \int_1^{+\infty}$ and integrate $\int_0^1$ by parts several times so as to enlarge the domain of convergence] are at most $s = -\frac{1}{2}, -1, -\frac{3}{2}, \cdots$ and are simple; while $L_\phi(g, 2 - 2s)$ is an entire function due to the fact that $\phi(x)$ vanishes in a neighborhood of 0 in $\boldsymbol{R}^2$. It follows from (22) that $\hat\theta_\phi(g, s)$ *is meromorphic in the whole plane*, and since the poles of $L_{\hat\phi}(g, 2 - 2s)$ in (22) are killed by the trivial zeros of $\zeta(2 - 2s)$ its poles are at most the zeros of $\zeta(2s)$, so that $\hat\theta_\phi(g, s)$ *is holomorphic in* $\mathrm{Re}(s) \geqq \frac{1}{2}$, not to mention $\mathrm{Re}(s) \geqq \frac{1}{4} \cdots$.

Furthermore, since $L_\phi(g, 2 - 2s)$ and $L_{\hat\phi}(g, 2 - 2s)$ are rapidly decreasing any vertical strip, and since

$$\left|\frac{1}{\zeta(2s)}\right| = O(\log^7|t|) \quad \text{in } \mathrm{Re}(s) \geqq \tfrac{1}{2} \quad \text{if} \quad s = \sigma + it,$$

it is clear that $\hat\theta_\phi(g, s)$ *is rapidly decreasing at infinity in every vertical strip* $\frac{1}{2} \leqq \mathrm{Re}(s) \leqq \sigma < +\infty$.

The Laplace transform $\hat\theta_\phi(g, s)$ satisfies a functional equation. Consider

$$\int_U \hat\theta_\phi(guw, 1 - s)\, du; \tag{23}$$

since the function $F(g) = \hat\theta_\phi(g, 1 - s)$ satisfies

$$F(ghu) = F(g)\beta(h)^{-s}$$

we have $F(g) \asymp \|g(e_1)\|^{-2s}$ (euclidean norm in $\boldsymbol{R}^2$) outside a neighborhood of 0 in $\boldsymbol{R}^2$, and thus (for given g and variable u)

$$\hat\theta_\phi(guw, 1 - s) \asymp \|guw(e_1)\|^{-2s} \asymp \|u(e_2)\|^{-2s} \asymp (1 + u^2)^{-s},$$

so that (23) converges for $\mathrm{Re}(s) > \frac{1}{2}$.

Now it follows from (22) and (21) that

$$\begin{aligned}
\tfrac{1}{2}\int \hat\theta_\phi(guw, 1 - s)\, du &= \int L_\phi(guw, 2s)\, du + \frac{\zeta(2s)}{\zeta(2 - 2s)}\int L_{\hat\phi}(guw, 2s)\, du \\
&= \frac{\zeta(2 - 2s)}{\zeta(2s - 1)} \cdot L_{\hat\phi}(g, 2 - 2s) \\
&\quad + \frac{\zeta(2s)}{\zeta(2 - 2s)} \cdot \frac{\zeta(2 - 2s)}{\zeta(2s - 1)} \cdot L_{\hat\phi}(g, 2 - 2s) \\
&= \frac{\zeta(2s)}{\zeta(2s - 1)}\left\{\frac{\zeta(2 - 2s)}{\zeta(2s)} L_{\hat\phi}(g, 2 - 2s) + L_\phi(g, 2 - 2s)\right\},
\end{aligned}$$

and we eventually get

$$\text{(24)} \qquad \text{Ч}(s) \int_U \hat{\theta}_\phi(guw, 1 - s)\, du = \hat{\theta}_\phi(g, s), \quad \mathrm{Re}(s) > \tfrac{1}{2}.$$

7. **The scalar product of two theta series.** We now come back to formula (9), namely

$$\|\theta_\phi\|^2 = c \int dm \int_{\mathrm{Re}(s)=\sigma} \hat{\theta}_\phi(m, s)\overline{L_\phi(m, 2\bar{s})}\, ds \qquad \text{where } c = 1/\pi^2.$$

It is valid provided $\sigma > 1$, but since the integrand is holomorphic and rapidly decreasing in the strip $\frac{1}{2} \leqq \mathrm{Re}(s) \leqq \sigma$ one can replace it by

$$\|\theta_\phi\|^2 = c \int dm \int_{\mathrm{Re}(s)=\frac{1}{2}} \hat{\theta}_\phi(m, s)\overline{L_\phi(m, 2 - 2s)}\, ds$$

(observe that $\bar{s} = 1 - s$ on the critical line!). We shall now prove that we have also

$$\text{(25)} \qquad \|\theta_\phi\|^2 = c \int_M dm \int_{\substack{\mathrm{Re}(s)\ \frac{1}{2} \\ \mathrm{Im}(s) > 0}} |\hat{\theta}_\phi(m, s)|^2\, ds;$$

since the function $g \mapsto \hat{\theta}_\phi(g, s)$ belongs to the representation space $\mathscr{H}(s)$ of G ("principal series" of §2; it is unitary on the critical line) we can write (25) as

$$\text{(26)} \qquad \|\Phi\|^2 = c \int_{\substack{\mathrm{Re}(s)\ \frac{1}{2} \\ \mathrm{Im}(s) > 0}} \|\hat{\Phi}(s)\|^2\, ds \qquad (\Phi = \theta_\phi, \Phi \perp 1)$$

where $\|\hat{\Phi}(s)\|$ is the norm of the element $\hat{\Phi}(s)$ of the Hilbert space $\mathscr{H}(s)$, cf. page 1. One can view (26) as follows: *the unitary representation of G on the subspace of $L^2(G/\Gamma)$ spanned by the functions θ_ϕ, $\phi \in D(G/U)$, orthogonal to* 1, *is the continuous direct sum with respect to the Lebesgue measure of the irreducible representations of the principal series.*

Let us now prove (25). We shall first compute the scalar product

$$\int_{G/\Gamma} \theta_\phi(g)\overline{E_{\phi'}(g, \bar{s})}\, d\dot{g} = \int_{G/\Gamma} d\dot{g} \sum_{\Gamma/\Gamma_\infty} \theta_\phi(g\gamma)\overline{L_{\phi'}(g\gamma, 2\bar{s})}$$

$$= \int_{G/\Gamma_\infty} \theta_\phi(g)\overline{L_{\phi'}(g, 2\bar{s})}\, d\dot{g} = \int_{G/U} \theta_\phi^0(g)\overline{L_{\phi'}(g, 2\bar{s})}\, d\dot{g}$$

$$= \iint_{M \times H} \theta_\phi^0(mh)\overline{L_{\phi'}(m, 2\bar{s})\beta(h)^{-\bar{s}}}\beta(h)\, dm\, dh,$$

whence

$$\int_{G/\Gamma} \theta_\phi(g)\overline{E_{\phi'}(g, \bar{s})}\, dg = \int_M \hat{\theta}_\phi(m, s)\overline{L_{\phi'}(m, 2\bar{s})}\, dm$$

for $\mathrm{Re}(s) > 1$ at first, and for $\mathrm{Re}(s) \geqq \frac{1}{2}$ by analytic continuation. But we have

$$\zeta(2 - 2s)E_{\phi'}(g, 1 - s) = \zeta(2s)E_{\hat{\phi}'}(g, s)$$

so that the expression

$$\zeta(2s) \int_{G/\Gamma} \theta_\phi(g)\overline{E_{\phi'}(g, \bar{s})}\, dg = \int_M \hat{\theta}_\phi(m, s)\overline{\zeta(2\bar{s})L_{\phi'}(m, 2\bar{s})}\, dm$$

is (on the critical line) invariant under $s \to 1 - s = \bar{s}$, $\phi' \to \hat{\phi}'$; hence

$$\int \hat{\theta}_\phi(m, s)\overline{L_{\phi'}(m, 2\bar{s})}\, dm = \int \hat{\theta}_\phi(m, \bar{s})\overline{\frac{\zeta(2s)}{\zeta(2\bar{s})} L_{\hat{\phi}'}(m, 2s)}\, dm$$

from which it follows that (take now $\phi' = \phi$)

$$\begin{aligned}
&\|\theta_\phi\|^2 \\
&= c \iint \hat{\theta}_\phi(m, s)\overline{L_\phi(m, 2\bar{s})}\, dm\, ds \\
&= c \iint_{\substack{\mathrm{Re(s)} = \frac{1}{2} \\ \mathrm{Im(s)} > 0}} \hat{\theta}_\phi(m, s)\overline{L_\phi(m, 2\bar{s})}\, dm\, ds + c \iint_{\substack{\mathrm{Re(s)} = \frac{1}{2} \\ \mathrm{Im(s)} > 0}} \hat{\theta}_\phi(m, \bar{s})\overline{\left[\frac{\zeta(2s)}{\zeta(2\bar{s})} L_{\hat{\phi}}(m, 2s)\right]}\, dm\, ds \\
&= c \iint_{\substack{\mathrm{Re(s)} = \frac{1}{2} \\ \mathrm{Im(s)} > 0}} \hat{\theta}_\phi(m, s)\overline{L_\phi(m, 2\bar{s})}\, dm\, ds + c \iint_{\substack{\mathrm{Re(s)} = \frac{1}{2} \\ \mathrm{Im(s)} > 0}} \hat{\theta}_\phi(m, s)\, \overline{\frac{\zeta(2\bar{s})}{\zeta(2s)} L_{\hat{\phi}}(m, 2\bar{s})}\, dm\, ds \\
&= c \iint_{\substack{\mathrm{Re(s)} = \frac{1}{2} \\ \mathrm{Im(s)} > 0}} \hat{\theta}_\phi(m, s)\overline{\left\{L_\phi(m, 2\bar{s}) + \frac{\zeta(2\bar{s})}{\zeta(2s)} L_{\hat{\phi}}(m, 2\bar{s})\right\}}\, dm\, ds \\
&= c \iint_{\substack{\mathrm{Re(s)} = \frac{1}{2} \\ \mathrm{Im(s)} > 0}} \hat{\theta}_\phi(m, s)\hat{\theta}_\phi(m, s)\, dm\, ds
\end{aligned}$$

as follows from (22), page 8, and the fact that $\bar{s} = 1 - s$ on the critical line. We thus get (25).

8. **Inversion formula.** Let $\Phi = \theta_\phi$ be a theta series in $L^2(G/\Gamma)$; formula (26) enables us to compute its norm in $L^2(G/\Gamma)$ in terms of its "components" $\hat{\Phi}(s)$ in the various Hilbert spaces $\mathscr{H}(s)$ of the principal series; this is an analogue of Plancherel's formula in the classical theory of Fourier integrals. We shall now prove that there is an analogue of Fourier's inversion formula, i.e., a formula expressing $\Phi(g)$ in terms of its Laplace transform $\hat{\Phi}(g, s)$ on the critical line $\mathrm{Re}(s) = \frac{1}{2}$.

Since

$$\hat{\Phi}(ghu, 1 - s) = \hat{\Phi}(g, 1 - s)\beta(h)^{-s}$$

it is clear that the ratio $\hat{\Phi}(g, 1 - s)/L_\phi(g, 2s)$ is invariant under HU; since G/HU is compact we see that, for a given s,

$$\hat{\Phi}(g, 1 - s) \asymp L_\phi(g, 2s);$$

hence the Eisenstein series

$$E_\Phi(g, s) = \sum_{\Gamma/\Gamma_\infty} \hat{\Phi}(g\gamma, 1 - s) \tag{27}$$

converges for $\mathrm{Re}(s) > 1$ (multiply by $\zeta(2 - 2s)$ to kill the poles on the right hand side!); (22) shows that

$$\tfrac{1}{2}E_\Phi(g, s) = E_\phi(g, s) + \frac{\zeta(2s)}{\zeta(2 - 2s)}E_{\hat{\phi}}(g, s)$$

if $\Phi = \theta_\phi$, $\phi \in \mathscr{D}(G/U)$. But

$$\zeta(2s)E_{\hat{\phi}}(g, s) = \zeta(2 - 2s)E_{\hat{\hat{\phi}}}(g, 1 - s) = \zeta(2 - 2s)E_\phi(g, 1 - s)$$

and thus

$$\tfrac{1}{2}E_\Phi(g, s) = E_\phi(g, s) + E_\phi(g, 1 - s) \tag{28}$$

if $\Phi = \theta_\phi$. But we have seen, cf. (10), that

$$\theta_\phi(g) = \frac{1}{\pi}\int_{\mathrm{Re}(s)=\sigma} E_\phi(g, s)\,ds \quad \text{if} \quad \sigma \gg 1;$$

since $\zeta(2s)E_\phi(g, s)$ is an entire function and decreases rapidly in every vertical strip (use the Laplace integral representation of §5), the function $E_\phi(g, s)$ is holomorphic and rapidly decreasing at infinity in $\frac{1}{2} \leqq \mathrm{Re}(s) \leqq \sigma$. Hence we can shift the integration, so that

$$\begin{aligned}\theta_\phi(g) = \frac{1}{\pi}\int_{\mathrm{Re}(s)=\frac{1}{2}} E_\phi(g, s)\,ds &= \frac{1}{\pi}\int_{\mathrm{Re}(s)=\frac{1}{2}} E_\phi(g, \bar{s})\,ds \\ &= \frac{1}{2\pi}\int_{\mathrm{Re}(s)=\frac{1}{2}} [E_\phi(g, s) + E_\phi(g, 1 - s)]\,ds\end{aligned}$$

and we eventually get the analogue of Fourier inversion formula, namely

$$\Phi(g) = \frac{1}{4\pi}\int_{\mathrm{Re}(s)=\frac{1}{2}} E_\Phi(g, s)\,ds. \tag{29}$$

[We assume $\Phi = \theta_\phi$ for some $\phi \in \mathscr{D}(G/U)$, and $\Phi \perp 1$.]

9. **The space of cusp forms.** Take any $\Phi \in L^2(G/\Gamma)$ and any $\psi \in \mathscr{D}(G/U)$; then

$$\langle \Phi, \theta_\varphi \rangle = \int_{G/\Gamma} \Phi(g)\overline{\theta_\psi(g)}\, dg = \int_{G/\Gamma_\infty} \Phi(g)\overline{\psi(g)}\, dg = \int_{G/U} \Phi^0(g)\overline{\psi(g)}\, dg$$

as can be shown by using again the methods of §3 and §7. From this it follows that the subspace $L_0^2(G/\Gamma)$ of $L^2(G/\Gamma)$ orthogonal to the theta series θ_ϕ, $\phi \in \mathscr{D}(G/U)$, is the set of *cusp-forms* i.e., of $\Phi \in L^2(G/\Gamma)$ such that

$$\Phi^0(g) = \int_{U/\Gamma_\infty} \Phi(gu)\, du = 0 \quad \text{almost everywhere,} \tag{30}$$

[To see that this integral makes sense for any square integrable function $\Phi(g)$ observe that for any $c > 0$ the set $MH(c)U/\Gamma_\infty$, where $H(c)$ is the set of $h \in H$ such that $|t| < c$, covers a *finite* number of times only a part of G/Γ; hence for any $\Phi \in L^2(G/\Gamma)$ the integral

$$\int_{MH(c)U/\Gamma_\infty} |\Phi(g)|^2\, dg = \int_M dm \int_{H(c)} \beta(h)\, dh \int_{U/\Gamma_\infty} |\Phi(mhu)|^2\, du$$

is convergent; making use of Parseval-Bessel's formula for U/Γ_∞ it follows that $u \mapsto \Phi(gu)$ is in $L^2(U/\Gamma_\infty) \subset L^1(U/\Gamma_\infty)$ for almost all g and that

$$\begin{aligned}\int_M dm \int_{H(c)} |\Phi^0(mh)|^2 \beta(h)\, dh &\leqq \int_M dm \int_{H(c)} \beta(h)\, dh \sum |\Phi^n(mh)|^2 \\ &= \int_{MH(c)U/\Gamma_\infty} |\Phi(g)|^2\, dg.\end{aligned} \qquad \text{[cf. Equation (3')]}$$

Hence we even have

$$\iint_{M \times H(c)} |\Phi^0(mh)|^2 \beta(h)\, dm\, dh < +\infty$$

for any $c > 0$ and any $\Phi \in L^2(G/\Gamma)$.]

10. **Discreteness of the spectrum in $L_0^2(G/\Gamma)$.** The following lemma is easily proved: Let $x \to U_x$ be a unitary representation of a locally compact group G on a Hilbert space $\mathscr{H}$; suppose the convolution operator

$$U_F = \int_G U_x F(x)\, dx$$

is compact for every continuous function F which vanishes outside a compact neighborhood of e; then the decomposition of the given representation into irreducible ones is *discrete with finite multiplicities* (i.e., $\mathscr{H}$ is a Hilbert direct sum of countably many minimal closed-invariant subspaces and the number of irreducible components which are equivalent to a given one is finite).

Returning to $G = \mathrm{SL}(2, \boldsymbol{R})$, $\Gamma = \mathrm{SL}(2, \boldsymbol{Z})$, we shall prove that the above lemma applies to the representation of G on $\mathscr{H} = L^2(G/\Gamma)$.

Here (and denoting by F a generic continuous function with compact support on G and by Φ a generic element of $\mathscr{H}$) we have

$$U_F\Phi(g) = \int_G U_x\Phi(g)\cdot F(x)\,dx = \int_G F(x)\Phi(x^{-1}g)\,dx = F*\Phi(g),$$

a convolution product; but since $\Phi(g\gamma) = \Phi(g)$ we also get

$$\begin{aligned} U_F\Phi(g) &= \int_G F(gx^{-1})\Phi(x)\,dx = \int_{G/\Gamma_\infty} dx \sum_{\Gamma_\infty} F(g\gamma x^{-1})\Phi(x\gamma^{-1}). \\ &= \int_{G/\Gamma_\infty} K_F(g, x)\Phi(x)\,dx \end{aligned}$$

where

$$K_F(g, x) = \sum_{\eta\in\Gamma_\infty} F(g\eta x^{-1}). \tag{31}$$

But since $\Phi \in L^2_0(G/\Gamma)$ implies $U_F\Phi \in L^2_0(G/\Gamma)$ i.e.,

$$0 = \int_{U/\Gamma_\infty} U_F\Phi(gu)\,du = \int_{U/\Gamma_\infty} du \int_{G/\Gamma_\infty} K_F(gu, x)\Phi(x)\,dx,$$

we also have

$$\begin{aligned} U_F\Phi(g) &= \int_{G/\Gamma_\infty} \Phi(x)\,dx\left\{K_F(g, x) - \int_{U/\Gamma_\infty} K_F(gu, x)\,du\right\} \\ &= \int_{G/\Gamma_\infty} \Phi(x)\,dx\left\{\sum_{\Gamma_\infty} F(g\eta x^{-1}) - \int_{U/\Gamma_\infty} du \sum_{\Gamma_\infty} F(gu\eta x^{-1})\right\} \\ &= \int_{G/\Gamma_\infty} \Phi(x)\,dx\left\{\sum_{\Gamma_\infty} F(g\eta x^{-1}) - \int_U F(gux^{-1})\,du\right\}. \end{aligned}$$

It will be shown in the next set of notes that the integral $\int_U F(gux^{-1})\,du$ is the "principal" part of the kernel $K_F(g, x)$, and that by substracting it from $K_F(g, x)$ one gets for $U_F\Phi(g)$ a function which decreases rapidly at infinity in the fundamental region of Γ; the compactness of U_F in $L^2(G/\Gamma)$ will follow at once from this result.

11. **References.** No precise reference can be given because, as far as SL(2) is concerned, nobody thus far has ever published anything like a *proof* of a statement. Deep results valid for fuchsian groups have been announced long ago by A. Selberg at the Colloquium on the theory of zeta functions (Bombay, 1956), to be found in the Journal of the Indian Mathematical Society, volume XX; a first idea of the proofs, as well as extensions to more general groups (e.g. groups of rank one over Q), are to be found in Selberg's talk at the International Congress of Mathematicians, Stockholm, 1962; see also Gel'fand's paper in the Proceedings of the same Congress. In 1964, Gel'fand, Graev and Pjateckiĭ-Šapiro published a note (Doklady, volume 157) on the spectral decomposition of $L^2(G_A/G_k)$ where

G is the SL(2) group over an algebraic number field; nearly complete proofs were supplied in December 1964 at the Seminaire Bourbaki by the present author, who is thus entitled to consider himself as a striking exception to the first statement above! The method and results explained in the present paper have been the subject of a course of lectures delivered in Paris in 1964–1965; detailed lecture notes will be available within a short time.

The purely arithmetical method used here or in the author's Bourbaki talk has not been, so far, extended to general arithmetically defined discrete subgroups of semisimple Lie groups; Langlands' methods are of a quite different nature and do not rest upon the arithmetic properties of the discrete subgroups. To prove Langlands' results by arithmetical methods would probably be a quite interesting problem, and might lead to more precise results than Langlands' method does, and/or to a better understanding of the general situation.

Observe finally that when Langlands' paper will appear, it will be a second and more striking exception to our opening statement, since it will contain complete statements *and* detailed proofs for the most general case.

The Spectral Decomposition of Cusp-Forms

BY

R. GODEMENT

1. **Laplace transforms.** Let G be a connected reductive linear algebraic group defined over $k = \mathbf{Q}$, and let Γ be an arithmetic subgroup of G. We have a unitary representation of $G_{\mathbf{R}}$ on the Hilbert space $L^2(G_{\mathbf{R}}/\Gamma)$ (left translations) and one of the main problems of the theory of automorphic function is to decompose this representation into a (possibly continuous) direct sum of irreducible ones.

If we denote by

$$T_x : \Phi(g) \mapsto \Phi(x^{-1}g)$$

the operator corresponding to a generic $x \in G_{\mathbf{R}}$, the first thing to do is to construct the operator

$$T_F = \int_{G_{\mathbf{R}}} T_x F(x)\, dx$$

for every $F \in \mathscr{K}(G)$, i.e., every continuous function with compact carrier on G. It is given by

$$\begin{aligned} T_F\Phi(x) &= \int_{G_{\mathbf{R}}} T_y\Phi(x)F(y)\, dy = \int_{G_{\mathbf{R}}} F(y)\Phi(y^{-1}x)\, dy \\ &= \int_{G_{\mathbf{R}}} F(xy^{-1})\Phi(y)\, dy \end{aligned}$$

from which we get at once

$$T_F\Phi(x) = \int_{G_{\mathbf{R}}/\Gamma} K_F(x, y)\Phi(y)\, dy$$

with a kernel

$$K_F(x, y) = \sum_{\gamma\in\Gamma} F(x\gamma y^{-1})$$

which is continuous on $(G_{\mathbf{R}}/\Gamma) \times (G_{\mathbf{R}}/\Gamma)$. If $G_{\mathbf{R}}/\Gamma$ is compact, i.e., if G is *anisotropic*, the operators T_F will thus be compact, from which it follows (see the end of the SL(2) notes) that the representation T of $G_{\mathbf{R}}$ on $L^2(G_{\mathbf{R}}/\Gamma)$ has in this case a *discrete* decomposition into irreducible ones, with *finite* multiplicities, a fairly nice and simple situation, with unfortunately few results available to this day....

So we have a strong motivation for looking at the other cases. We then have in G nontrivial parabolic subgroups, and we can use them to define a kind of Laplace transform as in the SL(2) case. More specifically take in G a unipotent subgroup U and assume it is the unipotent radical of some parabolic group, necessarily the normalizer P of U in G. For every function $\Phi \in L^2(G_{\mathbf{R}}/\Gamma)$, the function $u \mapsto \Phi(gu)$ is invariant under

$$U_\Gamma = U_{\mathbf{R}} \cap \Gamma,$$

a discrete subgroup of $U_{\mathbf{R}}$ with compact factor space, so that we can construct

$$\Phi_U^0(g) = \int_{U_{\mathbf{R}}/U_\Gamma} \Phi(gu)\,du;$$

of course the function $p \mapsto \Phi_U(gp)$, $p \in P_{\mathbf{R}}$, is right invariant under $U_{\mathbf{R}}P_\Gamma$, where

$$P_\Gamma = P_{\mathbf{R}} \cap \Gamma,$$

so that we can consider it as a function on

$$P_{\mathbf{R}}/U_{\mathbf{R}} \cong (P/U)_{\mathbf{R}} = H_{\mathbf{R}}$$

invariant under the image H_Γ of Γ in $H = P/U$, which is an arithmetic subgroup of H (observe that H is reductive, algebraic, and defined over $\mathbf{Q}$). Now denote by λ any continuous homomorphism $H_{\mathbf{R}} \mapsto \mathbf{C}^*$ with the property that $\lambda = 1$ on H_Γ (these λ are closely related to the rational characters of H, of course); then the Laplace transform of Φ (corresponding to U) will be the function

$$\hat{\Phi}_U(g, \lambda) = \int_{P_{\mathbf{R}}/P_\Gamma U_{\mathbf{R}} \cong H_{\mathbf{R}}/H_\Gamma} \Phi_U^0(gp)\lambda(\dot{p})^{-1}\,d\dot{p}$$

where $p \mapsto \dot{p}$ is the canonical mapping from $P_{\mathbf{R}}$ onto $H_{\mathbf{R}}$.

It is to be expected that conversely the function Φ can be reconstructed in some canonical way from its various Laplace transforms $\hat{\Phi}_U$, but this is hopeless if $\hat{\Phi}_U = 0$ for all U, i.e., if we have

$$\int_{U_{\mathbf{R}}/U_\Gamma} \Phi(gu)\,du = 0$$

as soon as U is the unipotent radical of some parabolic subgroup. Such functions are called *cusp-forms* (the "constant term" of their "Fourier expansion" along each $U_{\mathbf{R}}$ vanishes) and they form in $L^2(G_{\mathbf{R}}/\Gamma)$ a closed invariant subspace $L_0^2(G_{\mathbf{R}}/\Gamma)$. Since our attempt to construct the "continuous" part of the spectrum failed on $L_0^2(G_{\mathbf{R}}/\Gamma)$, there is no other choice left than proving the following result:

The representation of $G_{\mathbf{R}}$ *on* $L_0^2(G_{\mathbf{R}}/\Gamma)$ *decomposes into a* discrete *sum of irreducible representations occurring with* finite *multiplicities.*

In other words, on $L_0^2(G_{\mathbf{R}}/\Gamma)$ everything looks as if G were anisotropic....

In the remainder of this lecture we shall give a proof of the above result, closely following Langlands' paper but for the use of Poisson's summation formula. The method will of course consist in proving that on $L_0^2(G_{\mathbf{R}}/\Gamma)$ the convolution operators

$$T_F\Phi(x) = F * \Phi(x) = \int_{G_{\mathbf{R}}} F(xy^{-1})\Phi(y)\,dy$$

are *compact* [we shall prove it only for $F \in \mathcal{D}(G_{\mathbf{R}})$ i.e., C^∞ with compact carrier].

2. **Notations.** We shall denote by P a fixed *minimal* parabolic subgroup of G, by U its unipotent radical, by S a maximal split torus in P and by Z its centralizer, so that $P = ZU$ (semidirect product over $\mathbf{Q}$); of course $Z \cong P/U$, and $S \cap \Gamma = S_\Gamma$ is finite. A root α of G with respect to S will be called *positive* if the subspace $\mathfrak{g}(\alpha)$ of the Lie algebra of G is contained in the Lie algebra of U; the corresponding simple positive roots will be denoted by $\alpha_1, \cdots, \alpha_r$ ($r = \dim S$). The connected component of $S_{\mathbf{R}}$ will be denoted by $S_{\mathbf{R}}^+$, and $S_{\mathbf{R}}^+(t)$ will denote the subset of $S_{\mathbf{R}}^+$ defined by the relations

$$\alpha_i(s) < t \qquad (1 \leqq i \leqq r),$$

for a strictly positive t.

We shall choose in $Z = Z(S)$ a closed subgroup M (defined over $\mathbf{Q}$) such that $Z = SM$, with $S \cap M$ finite. We then have

$$Z_{\mathbf{R}} = S_{\mathbf{R}} M_{\mathbf{R}}$$

and M is anisotropic, so that $M_{\mathbf{R}}/M_\Gamma$ is compact. We shall also choose in $G_{\mathbf{R}}$ a maximal compact subgroup K such that $S_{\mathbf{R}}$ is stable under the involution of $G_{\mathbf{R}}$ with respect to K; we then have

$$G_{\mathbf{R}} = K S_{\mathbf{R}}^+ M_{\mathbf{R}} U_{\mathbf{R}};$$

the corresponding decomposition of an $x \in G_{\mathbf{R}}$ will be written as

$$x = k_x s_x m_x u_x;$$

s_x, u_x and the product $k_x m_x$ are uniquely determined by x.

We shall denote by[1]

$$\mathfrak{S} = K S_{\mathbf{R}}^+(t) \Omega_M \Omega_U$$

a fixed Siegel's domain in $G_{\mathbf{R}}$ and by $\xi_1, \cdots, \xi_h$ elements of $G_{\mathbf{Q}}$ such that

$$G_{\mathbf{R}} = \bigcup_{i=1}^{h} \mathfrak{S}\xi_i\Gamma.$$

Finally, the Lie algebra of U will be denoted by $\mathfrak{n}$; the map

$$\exp : \mathfrak{n} \to U$$

is an isomorphism of algebraic varieties defined over $\mathbf{Q}$, and induces an isomorphism of analytic varieties $\mathfrak{n}_{\mathbf{R}} \to U_{\mathbf{R}}$; it transforms the (additive) Haar measure

[1] We shall denote by Ω_M or Ω_U or Ω_G, etc..., fixed compact subsets of M or $U_{\mathbf{R}}$ or $G_{\mathbf{R}}$, etc.... However the meaning of such a "fixed" compact set will be allowed to change a finite number of times in the course of the proof.

of $\mathfrak{n}_{\mathbf{R}}$ in that of $U_{\mathbf{R}}$. Though U_Γ is not necessarily the image under exp of some discrete subgroup of $\mathfrak{n}_{\mathbf{R}}$, it is known that there is in $\mathfrak{n}_{\mathbf{R}}$ a lattice $\mathfrak{a} \subset \mathfrak{n}_{\mathbf{Q}}$ such that $\exp(\mathfrak{a})$ *is a subgroup of finite index of* U_Γ. If $V \subset U$ is the unipotent radical of a parabolic subgroup containing P, it is clear that

$$V'_\Gamma = V \cap \exp(\mathfrak{a}) = \exp(\mathfrak{v} \cap \mathfrak{a}),$$

where $\mathfrak{v}$ is the Lie algebra of V, is a subgroup of finite index of V_Γ.

3. **Majoration of the kernel.** Let $\Phi \in L^2(G_{\mathbf{R}}/\Gamma)$; since Φ is invariant under (at least)

$$U'_\Gamma = \exp(\mathfrak{a}),$$

we get at once, for every $F \in \mathscr{D}(G_{\mathbf{R}})$,

$$T_F\Phi(x) = \int_{G_{\mathbf{R}}/U'_\Gamma} K_F(x, y)\Phi(y)\,dy \tag{1}$$

where

$$K_F(x, y) = \sum_{\eta \in U'_\Gamma} F(x\eta y^{-1}) = \sum_{v \in \mathfrak{a}} F[x \exp(v) y^{-1}]. \tag{2}$$

To get an asymptotic evaluation of $K_F(x, y)$ for $x \in \mathfrak{S}$, we shall use Poisson's summation formula on $\mathfrak{n}_{\mathbf{R}}$: for given $x, y \in G_{\mathbf{R}}$ it is clear that

$$n \mapsto F[x \exp(n) y^{-1}] \tag{3}$$

is C^∞ with compact carrier on $\mathfrak{n}_{\mathbf{R}}$, whence

$$K_F(x, y) = \sum_{\lambda \in \mathfrak{A}} \int_{\mathfrak{n}_{\mathbf{R}}} F[x \exp(n) y^{-1}] e^{2\pi i \lambda(n)}\,dn \tag{4}$$

where the summation extends to the set $\mathfrak{A}$ of all linear forms $\lambda : \mathfrak{n}_{\mathbf{R}} \mapsto \mathbf{R}$ which take integral values on $\mathfrak{a}$.

Consider now the integration domain $G_{\mathbf{R}}/U'_\Gamma$ in (1); since $U_{\mathbf{R}}/U'_\Gamma$ is compact we see that in the decomposition $y = k_y s_y m_y u_y$ of y we have $u_y \in \Omega_U$, a fixed compact set in $U_{\mathbf{R}}$. Furthermore, since F has a compact carrier, we see that

$$F(x\eta y^{-1}) \neq 0 \Rightarrow x\eta y^{-1} \in \Omega_G;$$

if $x \in \mathfrak{S}$ we have $x \in K\Omega_M s_x \Omega_U = \Omega_G s_x$ and thus

$$\begin{aligned} F(x\eta y^{-1}) \neq 0 &\Rightarrow s_x \eta y^{-1} \in \Omega_G \\ &\Rightarrow s_x \eta u_y^{-1} s_x^{-1} \cdot s_x m_y^{-1} s_y^{-1} k_y^{-1} \in \Omega_G \\ &\Rightarrow s_x \eta u_y^{-1} s_x^{-1} \cdot m_y^{-1} \cdot s_x s_y^{-1} \in \Omega_G, \end{aligned}$$

and since the decomposition

$$p = u_p m_p s_p$$

of a $p \in P_R$ is topological we conclude among other things that

$$F(x\eta y^{-1}) \neq 0 \Rightarrow m_y \in \Omega_M \quad \text{and} \quad s_y \in \Omega_S s_x. \tag{5}$$

For $x \in \mathfrak{S}$ we thus see that

$$K_F(x, y) \neq 0 \Rightarrow y \in K\Omega_M\Omega_S s_x U_R \tag{6}$$

so that we need only evaluate (4) in this range, and even for $y \in K\Omega_M\Omega_S s_x\Omega_U$, since we integrate modulo U'_Γ.

Then we get

$$\int_{\mathfrak{n}_R} F[x \cdot \exp(n) \cdot y^{-1}]e^{2\pi i\lambda(n)}\,dn = \int_{\mathfrak{n}_R} F[\omega_x \cdot s_x \exp(n)s_x^{-1} \cdot s_x y^{-1}]e^{2\pi i\lambda(n)}\,dn$$

where $\omega_x = xs_x^{-1} \in \Omega_G$; furthermore $\omega_{x,y} = s_x y^{-1}$ also remains in some fixed compact Ω_G as we have seen above.

Thus

$$\begin{aligned}\int_{\mathfrak{n}_R} & F[x \cdot \exp(n) \cdot y^{-1}]e^{2\pi i\lambda(n)}\,dn \\ &= \int_{\mathfrak{n}_R} F[\omega_x \cdot \exp(\mathrm{Ad}(s_x)n) \cdot \omega_{x,y}]e^{2\pi i\lambda(n)}\,dn \\ &= \beta(s_x)^{-1} \int_{\mathfrak{n}_R} F[\omega_x \cdot \exp(n) \cdot \omega_{x,y}]\exp[2\pi i\lambda(\mathrm{Ad}(s_x)^{-1}n)]\,dn,\end{aligned}$$

and if we define

$$\hat{F}_{x,y}(\lambda) = \int_{\mathfrak{n}_R} F[\omega_x \cdot \exp(n) \cdot \omega_{x,y}]e^{2\pi i\lambda(n)}\,dn \tag{7}$$

for any real linear form λ on $\mathfrak{n}_R$, we eventually get

$$\int_{\mathfrak{n}_R} F[x \cdot \exp(n) \cdot y^{-1}]e^{2\pi i\lambda(n)}\,dn = \beta(s_x)^{-1}\hat{F}_{x,y}[\mathrm{Ad}(s_x)\lambda] \tag{8}$$

where we still denote by $\mathrm{Ad}(s_x)$ the *contragredient* of the adjoint representation of S_R on $\mathfrak{n}_R$, and where

$$\beta(s) = \det_{\mathfrak{n}} \mathrm{Ad}(s) = \prod_{\alpha > 0} \alpha(s), \tag{9}$$

each root occurring as many times as its multiplicity.

Now since the functions

$$n \mapsto F[\omega_x \cdot \exp(n) \cdot \omega_{x,y}]$$

obviously remain in a fixed compact subset of $\mathscr{D}(\mathfrak{n}_R)$, their Fourier transforms $\hat{F}_{x,y}$ are *uniformly* rapidly decreasing at infinity; if we choose any norm $\|\lambda\|$ on the dual space of $\mathfrak{n}_{\mathbf{R}}$ we thus have for every integer N a majoration

$$|\hat{F}_{x,y}(\lambda)| \leqq C_N \cdot \|\lambda\|^{-N} \tag{10}$$

valid for all nonzero λ and all x, y under consideration. From this we get

$$\left|\int_{\mathfrak{n}_{\mathbf{R}}} F[x \cdot \exp(n) \cdot y^{-1}] e^{2\pi i \lambda(n)}\, dn\right| \prec \beta(s_x)^{-1} \|\mathrm{Ad}(s_x)\lambda\|^{-N}$$

and if we denote by λ_α the restriction of λ to the subspace of $\mathfrak{n}_{\mathbf{R}}$ corresponding to a positive root α we eventually obtain

$$\int_{\mathfrak{n}_{\mathbf{R}}} F[x \exp(n) y^{-1}] e^{2\pi i \lambda(n)}\, dn \prec \|\lambda\|^{-N} \beta(s_x)^{-1} \cdot \sup_{\lambda_\alpha \neq 0} \alpha(s_x)^N \tag{11}$$

for every integer N and $\lambda \in \mathfrak{n}_{\mathbf{R}}^*$.

4. **Majoration of $T_F\Phi(x)$ in $\mathfrak{S}$.** We now make use of the fact that Φ is a *cusp-form* to get a majoration of $T_F\Phi(x)$ for $x \in \mathfrak{S}$.

Choose a simple root α_i and let V be the subgroup of U spanned by the roots

$$\alpha = n_1\alpha_1 + \cdots + n_r\alpha_r$$

such that $n_i > 0$; hence V is the unipotent radical of a (maximal) parabolic subgroup containing P.

In the Fourier integral

$$\int_{\mathfrak{n}_{\mathbf{R}}} F[x \cdot \exp(n) \cdot y^{-1}] e^{2\pi i \lambda(n)}\, dn \tag{12}$$

assume λ vanishes on the Lie algebra $\mathfrak{v}_{\mathbf{R}}$ of $V_{\mathbf{R}}$; then (12), as a function on y, is right invariant under $V_{\mathbf{R}}$, because if $v \in V_{\mathbf{R}}$ we have (by the Campbell-Hausdorff formula)

$$\exp(n) v^{-1} = \exp[n - v(n)]$$

with $v(n) \in \mathfrak{v}_{\mathbf{R}}$; taking $n - v(n)$ as a new integration variable in (12), which replaces dn by dn, one gets at once the invariance of (12) under $V_{\mathbf{R}}$.

But since Φ is a cusp-form, we have

$$\int_{V_{\mathbf{R}}/V_\Gamma} \Phi(gv)\, dv = 0$$

hence also

$$\int_{V_{\mathbf{R}}/V'_\Gamma} \Phi(gv)\, dv = 0$$

since $V'_\Gamma = V_{\boldsymbol{R}} \cap \exp(\mathfrak{a}) \subset V_\Gamma$, and if we write formula (1) as

$$T_F\Phi(x) = \int_{G_{\boldsymbol{R}}/V_{\boldsymbol{R}}U'_\Gamma} dy \int_{V_{\boldsymbol{R}}/V'_\Gamma} K_F(x, yv)\Phi(yv)\, dv \tag{13}$$

we see that we can remove from the series

$$K_F(x, y) = \sum_{\lambda\in\mathfrak{N}} \int_{\mathfrak{n}_{\boldsymbol{R}}} F[x \cdot \exp(n) \cdot y^{-1}]e^{2\pi i\lambda(n)}\, dn \tag{4}$$

those terms for which $\lambda = 0$ on $\mathfrak{v}_{\boldsymbol{R}}$.

But if λ is not identically 0 on $\mathfrak{v}_{\boldsymbol{R}}$ then there is a root $\alpha = n_i\alpha_i + \cdots + n_r\alpha_r$ for which

$$\lambda_\alpha \neq 0, \qquad n_i > 0;$$

inequality (11) and the fact that the $\alpha_j(s_x)$ remain bounded for $x \in \mathfrak{S}$ yield for such a λ a majoration

$$\left| \int_{\mathfrak{n}_{\boldsymbol{R}}} F[x \exp(n)y^{-1}]e^{2\pi i\lambda(n)}\, dn \right| \prec \|\lambda\|^{-N}\beta(s_x)^{-1}\alpha_i(s_x)^{-N}$$

and since $\sum_{\lambda\in\mathfrak{N}} \|\lambda\|^{-N}$ converges for large N it follows that

$$K_F(x, y) = O[\alpha_i(s_x)^N/\beta(s_x)] + \cdots \tag{14}$$

where the dots do not contribute to the calculation of $T_F\Phi$, and are invariant under $V_{\boldsymbol{R}}$; furthermore it is clear from (5) that (12) vanishes unless

$$y \in K\Omega_M\Omega_S s_x U_{\boldsymbol{R}},$$

so that the kernel obtained from (14) by removing the dots still vanishes outside $K\Omega_M\Omega_S s_x U_{\boldsymbol{R}}$.

We thus get from (13)

$$T_F\Phi(x) \prec \beta(s_x)^{-1}\alpha_i(s_x)^N \int_{K\Omega_M\Omega_S s_x U_{\boldsymbol{R}}/U'_\Gamma} \Phi(y)\, dy = \beta(s_x)^{-1}\alpha_i(s_x)^N \int_{K\Omega_M\Omega_S s_x \Omega_U} \Phi(y)\, dy,$$

whence, by Cauchy-Schwarz inequality,

$$\prec \beta(s_x)^{-1}\alpha_i(s_x)^N v(K\Omega_M\Omega_S s_x\Omega_U)^{\frac{1}{2}} \left\{ \int_{K\Omega_M\Omega_S s_x\Omega_U} |\Phi(y)|^2\, dy \right\}^{\frac{1}{2}};$$

but

$$K\Omega_M\Omega_S s_x\Omega_U \subset K\Omega_M S^+_{\boldsymbol{R}}(t')\Omega_U = \mathfrak{S}',$$

a fixed Siegel's domain, and thus

$$\left\{ \int_{K\Omega_M\Omega_S s_x\Omega_U} |\Phi(y)|^2\, dy \right\}^{\frac{1}{2}} \prec \left\{ \int_{G_{\boldsymbol{R}}/\Gamma} |\Phi(y)|^2\, dy \right\}^{\frac{1}{2}} = \|\Phi\|_2;$$

on the other hand

$$v(K\Omega_M\Omega_S s_x\Omega_U) = v(K\Omega_M\Omega_S s_x\Omega_U s_x^{-1}) \asymp v(s_x\Omega_U s_x^{-1}) \asymp \beta(s_x),$$

and we eventually get

$$T_F\Phi(x) \prec \frac{\alpha_i(s_x)^N}{\beta^{\frac{1}{2}}(s_x)} \|\Phi\|_2$$

for $x \in \mathfrak{S}$. Since this is true for any $i = 1, \cdots, r$ we actually have

$$(15) \qquad T_F\Phi(x) \prec \frac{\eta(s_x)^N}{\beta^{\frac{1}{2}}(s_x)} \|\Phi\|_2 \text{ in } \mathfrak{S}$$

where

$$(16) \qquad \eta(s) = \inf[\alpha_1(s), \cdots, \alpha_r(s)].$$

Note that $\beta(s)' = \prod \alpha_i(s)^{r_i}$ with positive r_i, so that

$$\beta(s) \geqq \eta(s)^r$$

for a suitable r. From this and (15) we finally get

$$(15') \qquad T_F\Phi(x) \prec \eta(s_x)^{-N}\|\Phi\|_2$$

for all $x \in \mathfrak{S}$ and $\Phi \in L_0^2(G_{\mathbf{R}}/\Gamma)$.

5. **End of the proof.** To conclude the proof of the fact that T_F is compact on $L_0^2(G_{\mathbf{R}}/\Gamma)$ it remains to prove that the set $\mathscr{E} = \{T_F\Phi | \Phi \in L_0^2(G_{\mathbf{R}}/\Gamma),\ \|\Phi\|_2 \leqq 1\}$ is precompact in $L^2(G_{\mathbf{R}}/\Gamma)$.

First of all $G_{\mathbf{R}}/\Gamma$ is finitely covered by $\bigcup \mathfrak{S}\xi_i$ with finitely many $\xi_1, \cdots, \xi_h$, so that we need estimates not only for $T_F\Phi(x)$ but also for $T_F\Phi(x\xi_i)$ for $x \in \mathfrak{S}$; this amounts to replacing $\Phi(x)$ and Γ by $\Phi(x\xi_i)$ and $\xi_i\Gamma\xi_i^{-1}$, so that we get from (15′) a majoration

$$(15'') \qquad T_F\Phi(x\xi_i) \prec \eta(s_x)^N\|\Phi\|_2 \quad \text{if} \quad x \in \mathfrak{S},\ \Phi \in L_0^2(G_{\mathbf{R}}/\Gamma).$$

Now if X denotes any right invariant differential operator on $G_{\mathbf{R}}$ (of arbitrary order) we have

$$X(T_F\Phi) = X(F * \Phi) = (XF) * \Phi$$
$$= T_{XF}\Phi;$$

applying (15″) to XF we conclude that *the functions of $\mathscr{E}$ are uniformly bounded together with all their derivatives* on $G_{\mathbf{R}}/\Gamma$, and this obviously shows that $\mathscr{E}$ is pre-compact, which concludes the proof.

6. **A majoration of cusp-forms.** Assume a given $\Phi \in L_0^2(G_{\mathbf{R}}/\Gamma)$ is an automorphic form in Harish-Chandra's sense, i.e.,

(1) Φ is annihilated by an ideal of finite codimension in the center of the enveloping algebra of $\mathfrak{G}$.

(2) Φ transforms under $g \to kg$ according to some finite dimensional representation of K.

(If the ideal and the representation are given, those Φ remain in a finite dimensional subspace because (a) there are *finitely* many irreducible unitary representations of $G_{\mathbf{R}}$ in which the given ideal and representation occur, (b) these irreducible representations of $G_{\mathbf{R}}$ occur in $L_0^2(G_{\mathbf{R}}/\Gamma)$ with *finite* multiplicities, (c) each finite dimensional representation of K occurs *finitely* many times in such an irreducible representation.) Then it is easy to show there is an $F \in \mathscr{D}(G)$ such that $T_F\Phi = \Phi$.

We thus obtain for every automorphic form in $L_0^2(G_{\mathbf{R}}/\Gamma)$ a majoration $\Phi(x\xi_i) \prec \eta(s_x)^N \|\Phi\|_2$ in $\mathfrak{S}$ for every positive integer N.

7. **Cusp-forms on adèle groups.** Denote by A the ring of adèles of Q and consider $L^2(G_A/G_Q)$. If U is the unipotent radical of a parabolic subgroup P of G, then U_A/U_Q is compact, so that one can define

$$\Phi_U^0(g) = \int_{U_A/U_Q} \Phi(gu)\,du$$

for every function Φ invariant under G_Q; of course functions Φ_U^0 corresponding to conjugate U's are essentially the same, so there are essentially as many Φ_U^0 (for given Φ) as there are classes of parabolic subgroups.

The space $L_0^2(G_A/G_Q)$ defined by the requirement that

$$\Phi_U^0 = 0 \text{ for all } U$$

is a closed subspace of $L^2(G_A/G_Q)$, invariant under left translations by elements of G_A. We have then the same result as "at infinity," namely: for every continuous function F with compact support on G_A, the convolution operator

$$T_F\Phi(x) = \int_{G_A} F(xy^{-1})\Phi(y)\,dy$$

is *compact on* $L_0^2(G_A/G_Q)$, so that the representation of G_A on $L_0^2(G_A/G_Q)$ decomposes into a *discrete* sum of irreducible ones with *finite* multiplicities.

One could either deduce this result from the theorem "at infinity" or prove it directly (and then deduce from it the theorem "at infinity") by following the same method; one should then take

$$F(x) = \prod F_p(x_p)$$

where $F_\infty \in \mathscr{D}(G_{\mathbf{R}})$, where, for a finite p, the function F_p is locally constant with compact carrier, and where F_p is for almost all p the characteristic function of the group of integral points of G_p. One can then use Poisson's formula in the form

$$\sum_{\eta \in U_Q} F(x\eta y^{-1}) = \sum_{\lambda} \int_{\mathfrak{n}_A} F[x \exp(n) y^{-1}]\lambda(n)\,dn$$

where $\lambda(n)$ is the (Pontrjagin) character of the additive group of $\mathfrak{n}_A$ attached to a rational linear form λ on $\mathfrak{n}$, etc..... This would even be simpler in some respect than the computations at infinity.

References

1. I. M. Gel'fand and I. I. Pjateckiĭ-Šapiro, *Automorphic functions and representation theory*, Trudy Moskov. Mat. Obšč. **12** (1963). 389–412.

2. R. Langlands, *On the functional equations satisfied by Eisenstein series* (to appear).

Eisenstein Series

BY

R. P. LANGLANDS*

1. **Preliminaries.** In these lectures I want to discuss, with some indications of proofs, some of the elementary facts in the theory of Eisenstein series. Although the discussion can be carried out in more generality it is most convenient, in the context of this institute, to take for discrete group an arithmetically defined subgroup Γ of the group G of real points of a reductive group G_C defined over Q whose connected component G_Q^0 has no rational character. It is also necessary to suppose that the centralizer of a maximal Q split torus of G_C^0 meets every component of G_C. The reduction theory of Borel applies, with trivial modifications, to G; it will be convenient to assume that Γ has a fundamental set with only one cusp. Fix a minimal parabolic subgroup P_C^0 defined over Q and a maximal Q split torus A_C^0 of P_C^0 so that the standard parabolic Q-subgroups are defined. A (standard) cuspidal (percuspidal) subgroup P is the normalizer in G of a (standard) parabolic (minimal parabolic) Q-subgroup P_C of G_C^0. To each standard cuspidal subgroup P is associated a subspace $\mathfrak{A}_C$ of the Lie algebra $\mathfrak{a}_C^0$ of A_C^0; this subspace will be called the split component of P. By definition the rank of P is equal to its dimension. $\mathfrak{a}$, the set of real points on $\mathfrak{a}_C$, will also be called the split component of P. P is a product AMN where A is the analytic subgroup of G with the Lie algebra $\mathfrak{a}$, N is the set of real points in the unipotent radical of P_C, and M satisfies the same conditions as G. We identify M with $N\backslash MN$. $\Gamma \cap P \subseteq MN$ and $\Theta = \Gamma \cap N\backslash\Gamma \cap MN$ is an arithmetically defined subgroup of M. Assume that for each standard cuspidal subgroup P it also has a fundamental domain with only one cusp.

Suppose P and P' are two standard cuspidal subgroups with the split components $\mathfrak{a}$ and $\mathfrak{a}'$ respectively. If there is an element of Ω, the Weyl group (over Q) of $\mathfrak{a}_C^0$, taking $\mathfrak{a}_C$ to $\mathfrak{a}'_C$ we shall say that P and P' are associate; let $\Omega(\mathfrak{a}, \mathfrak{a}')$ be the set of distinct linear transformations from $\mathfrak{a}_C$ to $\mathfrak{a}'_C$ obtained by restricting such an element of Ω to $\mathfrak{A}_C$. The relation of being associate is an equivalence relation. The normalizer of $\mathfrak{A}(\mathfrak{A}')$ in G leaves $M(M')$ invariant and consequently acts on the centre $Z(Z')$ of the universal enveloping algebra of the Lie algebra of $M(M')$ and on the set $\mathfrak{X}(\mathfrak{X}')$ of homomorphisms of $Z(Z')$ into C. The orbits in $\mathfrak{X}(\mathfrak{X}')$ under this action are finite. If P and P' are associate, Z and Z' are isomorphic and there is a natural one-to-one correspondence between orbits in $\mathfrak{X}$ and $\mathfrak{X}'$. Every element of Z defines an unbounded operator on $L_0^2(\Theta\backslash M)$, the space of

* Miller Fellow.

cusp forms on $\Theta\backslash M$. If $\xi \in \mathfrak{X}$ let

$$V(\xi) = \{\phi \in L_0^2(\Theta\backslash M) | X\phi = \xi(X)\phi \text{ for all } X \in Z\}$$

and if Ξ is an orbit in $\mathfrak{X}$ let

$$V(\Xi) = \sum_{\xi \in \Xi} V(\xi).$$

$V(\Xi)$ is a closed subspace of $L_0^2(\Theta\backslash M)$ invariant under M and

$$L_0^2(\Theta\backslash M) = \sum_{\Xi} \oplus V(\Xi).$$

If Ξ' is the orbit in $\mathfrak{X}'$ corresponding to Ξ the space $V(\Xi')$ may be defined in a similar fashion. $V = V(\Xi)$ and $V' = V(\Xi')$ are said to be associate. We shall call such a V a simple admissible subspace. The symbol W will denote the space of functions on a fixed maximal compact subgroup K of G spanned by the matrix elements of some irreducible representation of K.

2. **Partial decomposition of** $L^2(\Gamma\backslash G)$. If V is a simple admissible subspace of $L_0^2(\Theta\backslash M)$ let $\mathscr{E}(V, W)$ be the set of all continuous functions Φ on $NA(\Gamma \cap P)\backslash G$ such that $\Phi(mg)$ belongs to V for all g and $\Phi(gk^{-1})$ belongs to W for all g. $\mathscr{E}(V, W)$ is a finite dimensional Hilbert space with the inner product

$$(\Phi, \Psi) = \int_{\Theta\backslash M \times K} \Phi(mk)\overline{\Psi}(mk)\, dm\, dk.$$

Let $\mathscr{D}(V, W)$ be the space of all continuous functions on $N(\Gamma \cap P)\backslash G$ such that $\phi(mg)$ belongs to V and $\phi(gk^{-1})$ belongs to W for each g and such that the projection of the support of ϕ on $NM\backslash G$ is compact.

LEMMA 1. *If* $\phi \in \mathscr{D}(V, W)$ *then*

$$\hat{\phi}(g) = \sum_{\Gamma \cap P\backslash\Gamma} \phi(\gamma g)$$

belongs to $L^2(\Gamma\backslash G)$.

The proof of this lemma requires the result in §6 of Godement's lecture on cusp forms.

Suppose $\{P\}$ is the set of all standard cuspidal subgroups associate to a given one and $\{V\} = \{V(P) | P \in \{P\}\}$ is a collection of associate simple admissible subspaces. Let $L(\{P\}, \{V\}, W)$ be the closed subspace of $L^2(\Gamma\backslash G)$ spanned by the functions $\phi\hat{}(\cdot)$ with ϕ in $\mathscr{D}(V(P), \{V\}, W)$ for some P in $\{P\}$.

LEMMA 2. $L^2(\Gamma\backslash G)$ *is the orthogonal direct sum of the spaces* $L(\{P\}, \{V\}, W)$ *and for a fixed* $\{P\}$ *and* $\{V\}$, $\sum_W \oplus L(\{P\}, W)$ *is invariant under* G.

This lemma is a fairly easy consequence of Lemma 3 which will be stated in a few minutes. To some extent it reduces the problem of decomposing $L^2(\Gamma\backslash G)$ to that of decomposing each of the spaces $L(\{P\}, \{V\}, W)$.

3. **Eisenstein series.** If P belongs to $\{P\}$ let $\mathfrak{a}_c$ be the split component of P. Let Λ be the generic symbol for a linear function on $\mathfrak{a}_c$. We can write any ϕ

in $\mathscr{D}(V, W)$ as a Fourier integral

$$(1) \qquad \phi(g) = \frac{1}{(2\pi)^q}\int_{\operatorname{Re}\Lambda=\Lambda_0} \exp(\Lambda(H(g)) + \rho(H(g))\Phi(\Lambda, g)|d\Lambda|.$$

Here $\Phi(\cdot)$, which I call the Fourier transform of ϕ, is an entire function on the dual of $\mathfrak{a}_c$ with values in $\mathscr{E}(V, W)$ and $\Phi(\Lambda, g)$ is the value of $\Phi(\Lambda)$ at g. The dimension of $\mathfrak{a}_c$ is q; ρ is one-half the sum of the positive roots; and $a(g) = \exp H(g)$ if $g = na(g)mk$, $n \in N$, $a(g) \in A$, $m \in M$, $k \in K$. If $(\Lambda_0, \alpha) > (\rho, \alpha)$ for every positive root α then

$$\phi^{\wedge}(g) = \frac{1}{(2\pi)^q}\int_{\operatorname{Re}\Lambda=\Lambda_0} \sum_{\Gamma\cap P\backslash\Gamma} \exp(\Lambda(H(\gamma g)) + \rho(H(\gamma g)))\Phi(\Lambda, \gamma g)|d\Lambda|.$$

To study the map $\phi \rightarrow \phi^{\wedge}$ we shall, for an arbitrary Φ in $\mathscr{E}(V, W)$, study the series

$$\sum_{\Gamma\cap P\backslash\Gamma} \exp(\Lambda(H(\gamma g)) + \rho(H(\gamma g)))\Phi(\gamma g).$$

This series is of interest for all functions Φ on $NA(\Gamma \cap P)\backslash G$ such that, for each g, $\Phi(mg)$ is an automorphic form, in the sense of Harish-Chandra, on $\Theta\backslash M$ which is square integrable on $\Theta\backslash M$ and $\Phi(gk^{-1})$ belongs to some space W. It is called an Eisenstein series. Denote its sum by $E(g, \Phi, \Lambda)$. For each g and Φ this function is defined and holomorphic in the domain $\{\Lambda | \operatorname{Re}(\Lambda, \alpha) > (\rho, \alpha) \text{ for all } \alpha > 0\}$. One of the basic facts in the theory of Eisenstein series is that it can be continued to all of the dual space of $\mathfrak{a}_c$ as a meromorphic function. This has first to be done when Φ belongs to one of the spaces $\mathscr{E}(V, W)$ and for the moment we concentrate on that.

LEMMA 3. *If P' is another standard cuspidal subgroup of rank g then*

$$(a) \qquad \int_{\Gamma\cap N'\backslash N'} E(ng, \Phi, \Lambda)\, dn = 0$$

if P and P' are not associate. However, if P and P' are associate

$$(b) \quad \int_{\Gamma\cap N'\backslash N'} E(ng, \Phi, \Lambda)\, dn = \sum_{s\in\Omega(\mathfrak{a},\mathfrak{a}')} \exp(s\Lambda(H'(g)) + \rho(H'(g)))(M(s, \Lambda)\Phi)(g)$$

where $M(s, \Lambda)$ is a linear transformation from $\mathscr{E}(V, W)$ to $\mathscr{E}(V', W)$ analytic as a function of Λ in $\{\Lambda | \operatorname{Re}(\Lambda, \alpha) > (\rho, \alpha) \text{ for } \alpha > 0\}$. V' is associate to V.

In order to gain some understanding of this lemma we consider the case that P is the standard cuspidal subgroup, $P' = P$, and Φ is a constant function. The sum on the right of (b) is then a sum over the Weyl group. The left side equals

$$\int_{\Gamma\cap N\backslash N} \sum_{\Gamma\cap P\backslash L} \exp(\Lambda(H(\gamma ng)) + \rho(H(\gamma ng)))\Phi(\gamma ng)\, dn$$

$$= \sum_{\Gamma\cap P\backslash\Gamma/\Gamma\cap N} \mu(\Gamma \cap N \cap \gamma^{-1}P\gamma\backslash N \cap \gamma^{-1}P\gamma) \int_{N\cap\gamma^{-1}P\gamma\backslash N} \exp(\Lambda(H(\gamma ng))$$

$$+ \rho(H(\gamma ng)))\Phi(\gamma ng)\, dn.$$

We consider the integrals in this sum individually. Using the Bruhat decomposition to write γ as pn_Wu (see pp. 63–70), we see that the integral equals

$$\exp(\Lambda(H(p)) + \rho(H(p))\left\{\int_{N\cap n_W^{-1}Pn_w\backslash N} \exp(\Lambda(H(n_Wng)) + \rho(H(n_Wng))\, dn\right\}\Phi(g).$$

The expression in brackets equals

$$\exp(\Lambda(\mathrm{Ad}\, n_W(H(g))) + \rho(H(g))) \int_{N\cap n_W^{-1}Pn_W\backslash N} \exp(\Lambda(H(n_Wn) + \rho(H(n_Wn)))\, dn$$

and we are done. Observe that if, as we suppose, the measure of $\Gamma\cap N\backslash N$ is one then $M(1, \Lambda) = I$.

4. **Some functional analysis.** Combining Lemma 3 with the Fourier inversion formula we obtain a formula which is basic for everything to follow.

COROLLARY. *Suppose P and P' are associate standard cuspidal subgroups, V and V' are associate admissible subspaces, ϕ belongs to $\mathcal{D}(V, W)$, and ψ belongs to $\mathcal{D}(V', W)$. If the Haar measure on G is suitably chosen, then*

$$(2) \qquad \int_{\Gamma\backslash G} \phi^\wedge(g)\bar{\psi}^\wedge(g)\, dg = \frac{1}{(2\pi)^q}\int_{\mathrm{Re}\,\Lambda=\Lambda_0} \sum_{s\in\Omega(\mathfrak{a},\mathfrak{a}')} (M(s, \Lambda)\Phi(\Lambda), \Psi(-s\bar{\Lambda}))|d\Lambda|.$$

Of course Λ_0 must be such that $(\Lambda_0, \alpha) > (\rho, \alpha)$ if α is a positive root of $\mathfrak{A}$. Simple approximation arguments now show that if $\phi(g)$ can be represented in the form (1) with a function $\Phi(\cdot)$, with values in $\mathcal{E}(V, W)$, which is defined and analytic in a tube over a ball of radius R with $R > (\rho, \rho)^{\frac{1}{2}}$ and behaves well at infinity then $\phi^\wedge(\cdot)$ is defined and square integrable and the formula (2) is valid. In particular $\Phi(\cdot)$ could be taken to lie in $\mathcal{H}(\mathcal{E}(V, W))$ the space of all functions analytic in some such tube which go to zero at infinity faster than the inverse of any polynomial.

Let $P^1, \cdots, P^r$ be the elements of $\{P\}$, let $V^i = V(P^i)$ and set

$$\mathcal{H} = \sum_{i=1}^{r} \oplus\, \mathcal{H}(\mathcal{E}(V^i, W)).$$

Let $\Phi(\cdot) = (\Phi_1(\cdot)), \cdots, \Phi_r^{(\cdot)}$, where $\Phi_i(\cdot)$ is a function in $\mathscr{H}(\mathscr{E}(V^i, W))$, be the symbol for a generic element of $\mathscr{H}$. It is clear that we can define a linear map $\Phi(\cdot) \to \phi\hat{}(\cdot)$ of $\mathscr{H}$ into $L(\{P\}, \{V\}, W)$.

Suppose that, for $1 \leqq i \leqq r, f_i(\cdot)$ is a complex valued function defined, bounded, and analytic in the tube T_R^i over some ball of radius $R > (\rho, \rho)^{\frac{1}{2}}$ with center zero in the dual of $\mathfrak{a}_c^i$ and $f_j(s\Lambda) = f_i(\Lambda)$ if $s \in \Omega(\mathfrak{a}^i, \mathfrak{a}^j)$.

$$\mathit{Set}\, f\Phi(\cdot) = (f_1(\cdot)\Phi_1(\cdot), \cdots, f_r(\cdot)\Phi_r(\cdot)).$$

The following lemma is quite useful.

LEMMA 4. *If*

$$\max_{1 \leqq i \leqq r} \sup_{\Lambda \in T_R^i} |f_i(\Lambda)| = k$$

then there is a bounded operator $\lambda(f)$ on $L(\{P\}, \{V\}, W)$ of norm at most k so that if $\Psi(\cdot) = f\Phi(\cdot)$ then $\psi\hat{} = \lambda(f)\phi\hat{}$.

Suppose $\Phi(\cdot) = (\Phi_1(\cdot), \cdots, \Phi_r(\cdot))$ and $\Psi(\cdot) = (\Psi_1(\cdot), \cdots, \Psi_r(\cdot))$ are two arbitrary elements in $\mathscr{H}$. Then $(\phi\hat{}, \psi\hat{})$ is equal to

$$\sum_{i=1}^{r} \sum_{j=1}^{r} \frac{1}{(2\pi)^q} \int_{\mathrm{Re}\,\Lambda^i = \Lambda_0^i} \sum_{s \in \Omega(\mathfrak{a}^i, \mathfrak{a}^j)} (M(s, \Lambda^i)\Phi_i(\Lambda^i), \Psi_j(-s\bar{\Lambda}_i))|d\Lambda_i|.$$

Denote this expression by $(\Phi(\cdot), \Psi(\cdot))$. It is easily verified that

$$(f\Phi(\cdot), \Psi(\cdot)) = (\Phi(\cdot), f^*\Psi(\cdot))$$

if $f^*(\cdot) = (f_1^*(\cdot), \cdots, f_r^*(\cdot))$ and $f_i^*(\cdot)$ is defined by $f_i^*(\Lambda) = \overline{f_i(-\bar{\Lambda})}$. Consequently $(f^*f\Phi(\cdot), \Phi(\cdot)) \geqq 0$. If $l > k$ there is a function $g(\cdot)$ satisfying the same conditions as $f(\cdot)$ so that $l^2 - f_i^*(\Lambda)f_i(\Lambda) = g_i^*(\Lambda)g_i(\Lambda)$, $1 \leqq i \leqq r$. Consequently

$$l^2(\Phi(\cdot), \Phi(\cdot)) - (f\Phi(\cdot), f\Phi(\cdot)) = (g\Phi(\cdot), g\Phi(\cdot)) \geqq 0.$$

The lemma is an easy consequence of this inequality. In particular take

$$f_i(\Lambda) = (\mu - (\Lambda, \Lambda))^{-1}$$

with $\mu > (\rho, \rho)$. Then $\lambda(f)$ is self-adjoint with a dense range; consequently the operator $A = \mu - \lambda(f)^{-1}$ is a self-adjoint operator, usually unbounded, on $L(\{P\}, \{V\}, W)$. If $\Psi_i(\Lambda) = (\Lambda, \Lambda)\Phi_i(\Lambda)$, $1 \leqq i \leqq r$, then $A\phi\hat{} = \psi\hat{}$. The resolvent $R(z, A) = (z - A)^{-1}$ is an analytic function of z off the infinite interval $(-\infty, (\rho, \rho)]$.

5. A theorem.

THEOREM. *For each i and each j and each s in $\Omega(\mathfrak{a}^i, \mathfrak{a}^j)$ the function $M(s, \Lambda)$ is meromorphic on the dual of $\mathfrak{a}_c^i$. For each i and each Φ in $\xi(V^i, W)$ the function $E(\cdot, \Phi, \Lambda)$ with values in the space of continuous functions on $\Gamma\backslash G$ is meromorphic* *on the dual of* $\mathfrak{a}_C^i$. *If* $s \in \Omega(\mathfrak{a}^i, \mathfrak{a}^j)$, $t \in \Omega(\mathfrak{a}^j, \mathfrak{a}^k)$ *and* $\Phi \in \mathscr{E}(V^i, W)$ *the functional equations*

$$M(ts, \Lambda) = M(t, s\Lambda)M(s, \Lambda),$$
$$E(g, M(s, \Lambda)\Phi, s\Lambda) = E(g, \Phi, \Lambda)$$

are satisfied.

The first, and most difficult, step in the proof of this theorem is to show that it is true when $\dim a^i = 1$ for one, and hence all, i. Most of the important ideas in this case have been described by Selberg in his talk at the International Congress.

6. **In which the number of variables is one.** If $\dim a^i = 1$ then r is 1 or 2. If z is a complex number let $\Lambda^i(z)$ be such that $(\alpha^i, \Lambda^i(z)) = z(\alpha^i, \alpha^i)^{\frac{1}{2}}$ if α^i is the unique simple root of a^i. Let $\mathscr{E} = \mathscr{E}(V^1, W)$ or $\mathscr{E}(V^1, W) \oplus \mathscr{E}(V^2, W)$ according as r is 1 or 2. If $r = 1$, there is an s in $\Omega(\mathfrak{a}^1, \mathfrak{a}^1)$ different from the identity; let $M(z) = M(s, \Lambda^1(z))$. If $r = 2$ and s is in $\Omega(\mathfrak{a}^1, \mathfrak{a}^2)$ then $s\Lambda^1(z) = -\Lambda^2(z)$. In this case let

$$M(z) = \begin{pmatrix} 0 & M(s^{-1}, \Lambda^2(z)) \\ M(s, \Lambda^1(z)) & 0 \end{pmatrix}.$$

In both cases $M(z)$ is a linear transformation of $\mathscr{E}$. If $\Phi = (\Phi_1)$ or (Φ_1, Φ_2) belongs to $\mathscr{E}$ let

$$E(g, \Phi, z) = \sum_i E(g, \Phi_i, \Lambda^i(z)).$$

The theorem may be restated as:

THEOREM. (i) $E(\cdot, \Phi, z)$ *and* $M(z)$ *are meromorphic in the complex plane,*
(ii) $M(z)M(-z) = I$,
(iii) $E(g, M(z)\Phi, -z) = E(g, \Phi, z)$.

If (i) and (ii) are true and P is any maximal standard cuspidal subgroup then

$$\int_{\Gamma \cap N \backslash N} E(ng, M(z)\Phi, -z) - E(ng, \Phi, z)\, dn = 0.$$

It follows from this that the integrand is a cusp form. Since on the other hand it is by construction orthogonal to the cusp forms it must vanish identically. Thus (iii) is also true.

The space $\mathscr{H}$ may be regarded as a space of functions, each of which is defined on some strip of the form $|\mathrm{Re}\, z| < (\rho, \rho)^{\frac{1}{2}} + \varepsilon, \varepsilon > 0$, by setting

$$\Phi(z) = \sum_i \oplus\, \Phi_i(\Lambda^i(Z)).$$

$\Phi(\cdot)$ takes values in $\mathscr{E}$. If c is close to but greater than $(\rho, \rho)^{\frac{1}{2}}$

$$(\phi\hat{\ }, \psi\hat{\ }) = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} (\Phi(z), \Psi(-\bar{z})) + (M(z)\Phi(z), \Psi(\bar{z}))\, dz.$$

If $c_1 > \operatorname{Re}\lambda > c$ then $(R(\lambda^2, \Lambda)\phi\hat{}, \psi\hat{})$ is the sum of

$$\text{(3)} \qquad \frac{1}{2\lambda}\{(\Phi(\lambda), \Psi(-\bar{\lambda})) + (M(\lambda)\Phi(\lambda), \Psi(\bar{\lambda}))\}$$

and

$$\text{(4)} \qquad \frac{1}{2\pi i}\int_{c_1 - i\infty}^{c_1 + i\infty} \frac{1}{\lambda^2 - z^2}\{(\Phi(z), \Psi(-\bar{z})) + (M(z)\Phi(z)\Psi(\bar{z}))\}\, dz.$$

If $\Phi(z) = \exp z^2\Phi$ and $\Psi(z) = \exp z^2\Psi$ with Φ and Ψ in $\mathscr{E}$ then (4) is an entire function of λ and (3) is equal to

$$(\exp 2\lambda^2/2\lambda)\{(\Phi, \Psi) + (M(\lambda)\Phi, \Psi)\}.$$

Consequently $M(\lambda)$ is analytic wherever $(R(\lambda^2, A)\hat{\phi}, \hat{\psi})$ is. In particular it is analytic for $\operatorname{Re}\lambda > 0$, $\lambda \notin (0, (\rho, \rho)^{\frac{1}{2}}]$.

Now we want to show that $E(\cdot, \Phi, z)$ is analytic in this region also. If $f(g)$ is a continuous function on G with compact support such that $f(kgk^{-1}) = f(g)$ for all k in K there is an entire function $\pi(f, z)$ with values in the space of linear transformations of $\mathscr{E}$ so that the convolution of $E(g, \Phi, z)$ and $f(g)$ is $E(g, \pi(f, z)\Phi, z)$. As a consequence it is enough to show that if $\psi(g)$ is any continuous function on $\Gamma\backslash G$ with compact support then

$$\int_{\Gamma\backslash G} E(g, \Phi, z)\bar{\psi}(g)\, dg$$

is analytic in this region. In doing this we are free to modify $E(g, \Phi, z)$ outside of the support of ψ. If $\Phi = \sum_i \oplus \Phi_i$ then

$$E(g, \Phi, z) = \sum_i \sum_{\Gamma\cap P_i\backslash\Gamma} F(\gamma g, \Phi_i, \Lambda^i(z))$$

with

$$F(g, \Phi_i, \Lambda^i) = \exp(\Lambda^i(H^i(g)) + \rho(H^i(g)))\Phi_i(g).$$

According to a principal stated by Borel in his lectures on reduction there is a number x so that, for $1 \leqq i \leqq r$, the inverse image in G of the support of ψ is contained in $\{g | \alpha^i(H^i(g)) < x(\alpha^i, \alpha^i)^{\frac{1}{2}}\}$. Let $F''(g, \Phi_i, z)$ equal $F(g, \Phi_i, \Lambda^i(z))$ if $\alpha^i(H^i(g)) < x(\alpha^i, \alpha^i)^{\frac{1}{2}}$ and let it equal $-F(g, \Phi_i(z), -\Lambda^i(z))$ otherwise. Here $\Phi_i(z)$ is defined by

$$M(z)\Phi = \sum_i \oplus \Phi_i(z).$$

Set

$$E''(g, \Phi, z) = \sum_i \sum_{\Gamma\cap P^i\backslash\Gamma} F''(\gamma g, \Phi_i, z).$$

The functions $E(g, \Phi, z)$ and $E''(g, \Phi, z)$ are equal on the support of ψ.

It is easy to compute the Fourier transform of $F''(g, \Phi_i, z)$. The argument of §4 allows us to show that $E''(g, \Phi, z)$ is in $L^2(\Gamma\backslash G)$ and that the inner product $(E''(\cdot, \Phi, \lambda), E''(\cdot, \Phi, \lambda))$ is equal to

$$(\lambda + \bar{\mu})^{-1}\{\exp x(\lambda + \bar{\mu})(\Phi, \Psi) - \exp(-x(\lambda + \bar{\mu}))(M(\lambda)\Phi, M(\mu)\Psi)\}$$
$$+ (\lambda - \bar{\mu})^{-1}\{\exp x(\lambda - \bar{\mu})(\Phi, M(\mu)\Psi) - \exp x(\bar{\mu} - \lambda)(M(\lambda)\Phi, \Psi)\}.$$

Call this expression $\omega(\lambda, \bar{\mu}; \Phi, \Psi)$. Suppose $E''(g, \Phi, \lambda)$ is defined at $\lambda = \lambda_0$ and that $\omega(\lambda, \bar{\mu}; \Phi, \Phi)$ is analytic in λ and $\bar{\mu}$ for $|\lambda - \lambda_0| < R$, $|\bar{\mu} - \bar{\lambda}_0| < R$. Since

$$\left|\frac{\partial^n}{\partial \lambda^n} E''(\cdot, \Phi, \lambda_0)\right|^2 = \frac{\partial^{2n}}{\partial \lambda^n \partial \bar{\mu}^n}\omega(\lambda_0, \bar{\lambda}_0; \Phi, \Phi)$$

we easily show that

$$\sum_{n=0}^{\infty} \frac{(\lambda - \lambda_0)^n}{n!} \frac{\partial^n}{\partial \lambda^n} E''(\cdot, \Phi, \lambda_0)$$

converges for $|\lambda - \lambda_0| < R$ so that $E''(\cdot, \Phi, \lambda)$ is an analytic function of λ in this region with values in $L^2(\Gamma\backslash G)$. It is easy to convince oneself that if $M(\lambda)$ is a meromorphic function of λ satisfying $M(\lambda)M(-\lambda) = I$ then $\omega(\lambda, \mu; \Phi, \Psi)$ is a meromorphic function of λ and $\bar{\mu}$ whose only singularities are on the lines $\lambda = \lambda_0$ or $\bar{\mu} = \bar{\lambda}_0$ where λ_0 is a singularity of $M(\lambda)$. In verifying this use the relation $M^*(\lambda) = M(\bar{\lambda})$. Because of this remark our only responsibility is to show that $M(\lambda)$ is meromorphic in the entire complex plane and satisfies the stated functional equation. However the functions $E''(g, \Phi, z)$ will still be used in an auxiliary role.

If $\lambda = \sigma + i\tau$ then $\omega(\lambda, \bar{\lambda}; \Phi, \Psi)$ which equals

$$(1/2\sigma)\{\exp 2x\sigma(\Phi, \Psi) - \exp(-2x\sigma)(M(\lambda)\Phi, M(\lambda)\Psi)\}$$
$$+ (1/2i\tau)\{\exp 2ix\tau(\Phi, M(\lambda)\Psi) - \exp(-2ix\tau)(M(\lambda)\Phi, \Psi)\}$$

is a positive semidefinite form in Φ and Ψ. As a consequence

$$\|M(\lambda)\| \leqq \max\left\{\sqrt{2}\exp 2x\sigma, \frac{4\sigma}{|\tau|}\exp 2x\sigma\right\}.$$

We conclude first of all that if U is a set of the form $a \leqq \tau \leqq b$, $0 < \sigma \leqq c$, with $ab > 0$, then $\|M(\lambda)\|$ is bounded uniformly for λ in U. This allows us to estimate $E(g, \Phi, \lambda)$ for λ in U and then, utilizing the close relation between $E(g, \Phi, \lambda)$ and $E''(g, \Phi, \lambda)$, to show that $\|E''(\cdot, \Phi, \lambda)\|$ is uniformly bounded for λ in U. Unfortunately the analysis required for these two steps is rather elaborate and cannot be reproduced here. It may be found in §5 of my mimeographed notes on Eisenstein Series. To continue we observe that this implies, by the very definition of $\omega(\lambda, \bar{\lambda}, \Phi, \tau)$, that, for each Φ and Ψ, $\omega(\lambda, \bar{\lambda}; \Phi, \Psi)$ is bounded in U. This can only be so if

$$\lim_{\sigma \downarrow 0} M^*(\sigma + i\tau)M(\sigma + i\tau) = M(\sigma - i\tau)M(\sigma + i\tau) = I$$

and

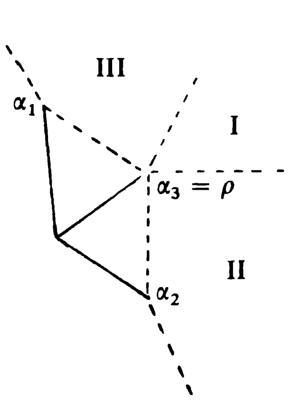
$$\lim_{\sigma \downarrow 0} M^{-1}(\sigma - i\tau) - M(\sigma + i\tau) = 0$$

uniformly for $t \in [a, b]$. Roughly speaking this means that $M(i\tau) = M^{-1}(-i\tau)$ for τ real. In any case, by an appropriate variant of the Schwarz reflection principle we can show that if we set $M(\lambda) = M^{-1}(-\lambda)$ for $\operatorname{Re} \lambda < 0$, $\lambda \notin [-(\rho, \rho)^{\frac{1}{2}}, 0]$ then $M(\lambda)$ can be extended across the imaginary axis to be meromorphic everywhere but in the interval $[-(\rho, \rho)^{\frac{1}{2}}, (\rho, \rho)^{\frac{1}{2}}]$.

Finally it must be shown that $M(\lambda)$ is also meromorphic in the interval $[-(\rho, \rho)^{\frac{1}{2}}, (\rho, \rho)^{\frac{1}{2}}]$. Since the proof of this is also based on §5 of my notes I shall not present it here.

7. **In which the number of variables is usually two.** In the proof of the functional equations for Eisenstein series in one variable there are two main points: to show that the function $M(z)$ is meromorphic and satisfies the stated functional equation and to construct the functions $E''(g, \Phi, z)$ and find the expression $\omega(\lambda, \bar{\mu}; \Phi, \Psi)$ for the inner product of two such functions. In the general case the first step is to show that the functions $M(s, \Lambda)$ are meromorphic everywhere and satisfy the equations of the theorem. After this one can proceed in two ways. Either one can find the analogues of the function $E''(g, \Phi, z)$ and the expression $\omega(\lambda, \bar{\mu}; \Phi, \Psi)$ as we shall do now or one can proceed in a more direct fashion to analytically continue the functions $E(g, \Phi, \Lambda)$ as is done at the end of §6 of the mimeographed notes referred to before. Since in proceeding the first way I work from rather rough notes you may prefer the second upon which a little more reliance can be placed. I present the first because it introduces a number of ideas and formulas likely to be of use in the attempt to obtain in the general case a trace formula in the sense of Selberg.

The first step is based on familiar ideas. It will probably be easier to understand if we discuss it in a very simple case. Let $G = SL(3, \boldsymbol{R})$, let $\Gamma = SL(3, \boldsymbol{Z})$ and let $\{P\}$ consist of one group, the group P of upper triangular matrices in G. In the diagram α_1 and α_2 are the simple roots of $\mathfrak{a}$, $\alpha_3 = \rho = \frac{1}{2}(\alpha_1 + \alpha_2 + \alpha_3)$ is the other



positive root, and I is the region $(\Lambda, \alpha_i) > (\rho, \alpha_i)$, $i = 1, 2$. The union of I and II is the convex hull of I and its reflection in the line $(\alpha_1, \Lambda) = 0$. The region III plays the same role as II with the line $(\alpha_1, \Lambda) = 0$ replaced by $(\alpha_2, \Lambda) = 0$. Let A be the tube over I, B the tube over the union of I and II, and C the tube over the union of I and III. The functions $M(s, \Lambda)$ are at first defined only in A.

Let s_i, $i = 1, 2$, be the reflection corresponding to the root α_i. For reasons to be discussed later $M(s_i, \Lambda)$ depends only on the projection of Λ on the orthogonal complement of the line $(\Lambda, \alpha_i) = 0$ and is a meromorphic function of Λ. Suppose we could show that, for all s, $M(s, \Lambda)$ is meromorphic in B and satisfies there the relation

$$M(ss_1, \Lambda) = M(s, s_1\Lambda)M(s_1, \Lambda). \tag{5}$$

Suppose we could also show the analogous facts for s_2. Then, for example,

$$M(s_1s_2, \Lambda) = M(s_1, s_2\Lambda)M(s_2, \Lambda)$$

in A. Since the right side is meromorphic in the entire two-dimensional complex plane so is the left. An easy induction can be used to show that $M(s, \Lambda)$ is meromorphic everywhere for each s and that the functional equations are satisfied.

How then do we continue $M(s, \Lambda)$ over B and prove (5). Suppose that for any Φ in $\mathscr{E}(V, W)$ we could analytically continue $E(\cdot, \Phi, \Lambda)$ over all of B (except perhaps for some poles) and show that

$$E(\cdot, M(s_1, \Lambda)\Phi, s_1\Lambda) = E(\cdot, \Phi, \Lambda) \tag{6}$$

in this region. If N is the group of upper triangular unipotent matrices and Ω is the Weyl group of G

$$\int_{\Gamma\cap N\backslash N} E(ng, \Phi, \Lambda)\, dn = \sum_{s\in\Omega} \exp(s\Lambda(H(g)) + \rho(H(g)))(M(s, \Lambda)\Phi)(g)$$

and

$$\int_{\Gamma\cap N\backslash N} E(ng, M(s_1, \Lambda)\Phi, s_1\Lambda)\, dn$$

$$= \sum_{s\in\Omega} \exp(ss_1\Lambda(H(g)) + \rho(H(g)))(M(s, s_1\Lambda)M(s_1, \Lambda)\Phi)(g).$$

The left-hand sides of these equations are meromorphic and equal in B; as a consequence the functions $M(s, \Lambda)$ are all meromorphic in the same region and the equations (5) are satisfied.

As a further simplification we shall in proving (6) assume that $\mathscr{E}(V, W)$ is the space of constant functions. $\mathfrak{a}$ is the set of diagonal matrices $D(x_1, x_2, x_3)$ of trace zero. Suppose α_1 is the linear function $x_1 - x_2$. Let $^*P$ be the group of all matrices in G of the form

$$\begin{pmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \\ 0 & 0 & x_{33} \end{pmatrix}.$$

${}^*N$ is the group of all such matrices with $x_{12} = x_{21} = 0$ and $x_{11} = x_{22} = x_{33} = 1$. ${}^*M$ is the group of all such matrices with $x_{13} = x_{23} = 0$ and $x_{33} = \pm 1$ and ${}^*\Theta = \Gamma \cap {}^*N\backslash\Gamma \cap {}^*P$ is an arithmetic subgroup of ${}^*M$. Moreover

$$\dagger P = {}^*N\backslash P \cap {}^*N{}^*M$$

is a percuspidal subgroup of ${}^*M$. We can choose $\dagger V$ and $\dagger W$ bearing the same relation to $\dagger P$ as V and W bear to P so that $\mathcal{E}(\dagger V, \dagger W)$ is also the space of constant functions. There is a natural map $\Phi \to \dagger\Phi$ of $\mathcal{E}(V, W)$ onto $\mathcal{E}(\dagger V, \dagger W)$. $\mathfrak{a}$ is the direct sum of ${}^*\mathfrak{a} = \{D(x, x, -2x)\}$ and $\dagger\mathfrak{a} = \{D(x, -x, 0)\}$ and $\dagger\mathfrak{a}$ may be regarded as the split component of $\dagger P$. The restriction $\dagger s_1$ of s_1 to $\dagger\mathfrak{a}$ belongs to the Weyl group of $\dagger\mathfrak{a}$. Corresponding to $\dagger s_1$ there is a function $M(\dagger s_1, \dagger\Lambda)$ on the dual of $\dagger\mathfrak{a}_c$ with values in the space of linear transformations of $\mathcal{E}(\dagger V, \dagger W)$. Because the dimension of $\mathfrak{a}$ is one we know that $M(\dagger s_1, \dagger\Lambda)$ is meromorphic everywhere in the dual space of $\dagger\mathfrak{a}_c$. The dual space of $\mathfrak{a}_c$ is of course isomorphic to the sum of the dual spaces of ${}^*\mathfrak{a}_c$ and $\dagger\mathfrak{a}_c$. Thus we may decompose a general Λ as a sum ${}^*\Lambda + \dagger\Lambda$. A careful study of the computations following the statement of Lemma 3 reveals that if Φ corresponds to $\dagger\Phi$ then $M(s_1, \Lambda)\Phi$ corresponds to $M(\dagger s_1, \dagger\Lambda)\dagger\Phi$. This is the fact with which we started.

By definition

$$E(g, \Phi, \Lambda) = \sum_{\Gamma\cap P\backslash\Gamma} \exp(\Lambda(H(\gamma g)) + \rho(H(\gamma g)))\Phi(\gamma g)$$

$$= \sum_{\Gamma\cap {}^*P\backslash\Gamma} \left\{ \sum_{\Gamma\cap P\backslash\Gamma\cap {}^*P} \exp(\Lambda(H(\delta\gamma g)) + \rho(H(\delta\gamma g)))\Phi(\delta\gamma g)\right\}.$$

Consider the inner sum with the argument γg replaced by g and let $g = namk$, $n \in {}^*N$, $m = m(g) \in {}^*M$, $a \in {}^*A$, and k in K. It equals

$$\exp({}^*\Lambda({}^*H(g)) + \rho({}^*H(g)))\left\{\sum_{{}^*\Theta\cap\dagger P\backslash{}^*\Theta} \exp(\dagger\Lambda(\dagger H(\theta m)) + \rho(\dagger H(\theta m)))\dagger\Phi(\theta m)\right\}$$

$$= \exp({}^*\Lambda({}^*H(g)) + \rho({}^*H(g)))E(m, \dagger\Phi, \dagger\Lambda).$$

Consequently

$$E(g, \Phi, \Lambda) = \sum_{\Gamma\cap {}^*P\backslash\Gamma} \exp({}^*\Lambda({}^*H(\gamma g)) + \rho({}^*H(\gamma g)))E(m(\gamma g), \dagger\Phi, \dagger\Lambda).$$

It can be shown that the series on the right converges at any point of $\boldsymbol{B}$ at which it is defined and that it represents a meromorphic function in $\boldsymbol{B}$. The relation (6) is an immediate consequence of the known relation

$$E(m, M(\dagger s_1, \dagger\Lambda)\dagger\Phi, \dagger s_1^{\dagger}\Lambda) = E(m, \dagger\Phi, \dagger\Lambda).$$

8. **A combinatorial lemma.** Before defining the functions $E''(g, \Phi, \Lambda)$ we had best discuss a simple combinatorial lemma. V will be a Euclidean space; V' will be its dual; $\{\lambda^1, \cdots, \lambda^p\}$ will be a basis of V' such that $(\lambda^i, \lambda^j) \leqq 0$ if $i \neq j$; and $\{\mu^1, \cdots, \mu^p\}$ will be a basis of V' dual to $\{\lambda^1, \cdots, \lambda^p\}$. Suppose $\mathfrak{p}$ is an ordered partition of $\{1, \cdots, p\}$ into $r = r(\mathfrak{p})$ nonempty subsets F_u, $1 \leqq u \leqq r$. If $i \in F_u$ let $\mu^i_{\mathfrak{p}}$ be the projection of μ^i on the orthogonal complement of the space spanned by $\{\mu^j | j \in F_v, v < u\}$ and let $\lambda^i_{\mathfrak{p}}$, $1 \leqq i \leqq p$, be such that $(\lambda^i_{\mathfrak{p}}, \mu^j_{\mathfrak{p}}) = \delta_{ij}$. A point Λ in V' will be called singular if, for some i and some $\mathfrak{p}$, $(\Lambda, \mu^i_{\mathfrak{p}}) = 0$ or $(\Lambda, \lambda^i_{\mathfrak{p}}) = 0$ and a point H in V will be called singular if $\lambda^i_{\mathfrak{p}}(H) = 0$ for some i and some $\mathfrak{p}$. Suppose Λ in V' is not singular. Define the function $\phi^\Lambda_{\mathfrak{p}}$ on V by the condition that $\phi^\Lambda_{\mathfrak{p}}(H) = 0$ unless $\lambda^i_{\mathfrak{p}}(H)(\mu^i_{\mathfrak{p}}, \Lambda) < 0$ for all i when $\phi^\Lambda_{\mathfrak{p}}(H) = 1$. Define the function $\psi^\Lambda_{\mathfrak{p}}$ by the condition that $\psi^\Lambda_{\mathfrak{p}}(H) = 0$ unless $\lambda^i_{\mathfrak{p}}(H) > 0$ for i in F_1 and $\lambda^i_{\mathfrak{p}}(H)(\mu^i_{\mathfrak{p}}, \Lambda) < 0$ for i not in F_1 when $\psi^\Lambda_{\mathfrak{p}}(H) = 1$. Let $a^u_{\mathfrak{p}}$ be the number of elements in F_u; let $b^\Lambda_{\mathfrak{p}}$ be the number of i such that $(\mu^i_{\mathfrak{p}}, \Lambda) < 0$, and let $c^\Lambda_{\mathfrak{p}}$ be the number of i in $\bigcup_{u=2}^r F_u$ such that $(\mu^i_{\mathfrak{p}}, \Lambda) < 0$. Set

$$\alpha^\Lambda_{\mathfrak{p}} = b^\Lambda_{\mathfrak{p}} + \sum_{u=1}^{r} (a^u_{\mathfrak{p}} + 1) \quad , \quad \beta^\Lambda_{\mathfrak{p}} = 1 + c^\Lambda_{\mathfrak{p}} + \sum_{u=2}^{r} (a^u_{\mathfrak{p}} + 1).$$

LEMMA 5. *If H is not singular then*

$$\sum_{\mathfrak{p}} (-1)^{\alpha^\Lambda_{\mathfrak{p}}} \phi^\Lambda_{\mathfrak{p}}(H) = \sum_{\mathfrak{p}} (-1)^{\beta^\Lambda_{\mathfrak{p}}} \psi^\Lambda_{\mathfrak{p}}(H)$$

if $(\lambda^i, \Lambda) < 0$ for some i and

$$\sum_{\mathfrak{p}} (-1)^{\alpha^\Lambda_{\mathfrak{p}}} \phi^\Lambda_{\mathfrak{p}}(H) = 1 + \sum_{\mathfrak{p}} (-1)^{\beta^\Lambda_{\mathfrak{p}}} \psi^\Lambda_{\mathfrak{p}}(H)$$

if $(\lambda^i, \Lambda) > 0$ for all i.

It is a pleasant exercise to prove this lemma.

9. **$L^2(\Gamma \backslash G)$ as the bed of Procrustes.** Suppose $\mathfrak{a} = \mathfrak{a}^{i_0}$ and $\Phi \in \mathscr{E}(V^{i_0}, W)$ (the notation is that of §4). Suppose Λ in the dual of $\mathfrak{a}_C$ is such that for all i and all s in $\Omega(\mathfrak{a}, \mathfrak{a}^i)$ the point $\operatorname{Re}(s\Lambda)$ is not singular in the sense of the previous paragraph. Take V to be $\mathfrak{a}^i$ and $\lambda^1, \cdots, \lambda^p$ to be the simple roots of $\mathfrak{a}^i$. Suppose also that $\operatorname{Re}(\Lambda, \alpha) > (\rho, \alpha)$ if α is a positive root of $\mathfrak{A}$. Choose a point H_0 in the split component of the standard percuspidal subgroup such that $\alpha(H_0)$ is very large for every positive root and let H^i_0 be its projection on $\mathfrak{a}^i$. For each i let $F''_i(g, \Phi, \Lambda)$ be the function

$$\sum_{s \in \Lambda(\mathfrak{a}, \mathfrak{a}^i)} \sum_{\mathfrak{p}} (-1)^{\alpha_{\mathfrak{p}}^{\operatorname{Re}(s\Lambda)}} \phi_{\mathfrak{p}}^{\operatorname{Re}(s\Lambda)}(H^i(g) - H^i_0) \exp(s\Lambda(Hi(g)) + \rho(Hi(g)))((M(s, \Lambda)\Phi)(g)).$$

Since the functions $\psi_{\mathfrak{p}}^{\operatorname{Re}(s\Lambda)}(H^i(g) - H^i_0)$ are zero on

$$\{g \in G | \mu^j(H^i(g) - H^i_0) < 0, 1 \leqq j \leqq p\}$$

the lemma shows that $F_i''(g, \Phi, \Lambda)$ is zero almost everywhere on this set unless $i = i_0$ and that

$$F_{i_0}''(g, \Phi, \Lambda) - \exp(\Lambda(H^{i_0}(g)) - \rho(H^{i_0}(g)))\Phi(g)$$

is zero almost everywhere on this set. Set

$$E''(g, \Phi, \Lambda) = \sum_{i=1}^{r} \sum_{\Gamma \cap P^i \backslash \Gamma} F_i''(\gamma g, \Phi, \Lambda).$$

It is a consequence of the above remarks and the minimum principle stated by Borel in his lectures on reduction theory that if U is any compact set in $\Gamma\backslash G$ the point H_0 may be so chosen that

$$E''(g, \Phi, \Lambda) = E(g, \Phi, \Lambda)$$

almost everywhere on U.

It is an easy matter to compute the Fourier transform of the functions $F_i''(g, \Phi, \Lambda)$. The arguments of §4 may be used to show that $E''(g, \Phi, \Lambda)$ is square integrable. The relation (2) may be used to evaluate

$$(E''(g, \Phi, \Lambda), E''(g, \Psi, \mathrm{M}))$$

if Ψ lies in $\mathscr{E}(V^{i_0'}, W)$ and M in the dual of $\mathfrak{A}_c' = \mathfrak{A}_c^{i_0'}$ satisfies the same conditions as Λ. If $\alpha_{\mathfrak{p}} = \sum_{u=1}^{r}(a_{\mathfrak{p}}^u + 1)$ the result is

$$\sum_{j=1}^{r} \sum_{s \in \Omega(\mathfrak{a}, \mathfrak{a}^j)} \sum_{t \in \Omega(\mathfrak{a}', \mathfrak{a}^j)} \sum_{\mathfrak{p}} (-1)^{\alpha_{\mathfrak{p}}} \frac{\exp(t\Lambda + s\bar{\mathrm{M}})(H_0^j)}{\prod_{m=1}^{p} (\mu_{\mathfrak{p}}^m, t\Lambda + s\bar{\mathrm{M}})} (M(t, \Lambda)\Phi, M(s, M)\Psi).$$

The notation is poor because the linear functions $\mu_{\mathfrak{p}}^m$ depend, of course, on j. Since it can be shown that the functional equations for the functions $M(t, \Lambda)$ imply that this expression is an analytic function of Λ and $\bar{\mathrm{M}}$ wherever all the functions $M(t, \Lambda)$ and $M^*(s, M)$ are we can proceed as in the rank one case to complete the proof of the theorem.

10. **More Eisenstein series.** Once one knows that the functions $E(g, \Phi, \Lambda)$ and $M(s, \Lambda)$ are meromorphic everywhere one can try to use the formula

$$(\phi^\wedge, \psi^\wedge) = \frac{1}{(2\pi)^q} \int_{\mathrm{Re}\,\Lambda = \Lambda_0} \sum (M(s, \Lambda)\Phi(\Lambda), \Psi(-s\bar{\Lambda}))|d\Lambda|$$

to analyze the space $L(\{P\}, \{V\}, W)$. In order to get some idea of what actually happens let us look at a particular case. We shall study the case that $G = \mathrm{SL}(3, \boldsymbol{R})$, $\Gamma = \mathrm{SL}(3, \boldsymbol{Z})$, P is the percuspidal subgroup introduced in §7, and V and W, and hence $\mathscr{E}(V, W)$ are the space of constant functions. As a preliminary let us look at the same situation with $\mathrm{SL}(3, \boldsymbol{R})$ replaced by $\mathrm{SL}(2, \boldsymbol{R})$ and with the other objects of our attention modified accordingly. Godement has already done this in his first lecture. However, he was not concerned with the discrete spectrum in $L(\{P\}, \{V\}, W)$ and we shall be.

To remind you of the notation:

$$N = \left\{\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \middle| x \in \boldsymbol{R}\right\} A_{\boldsymbol{R}} = \left\{\begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix} \middle| \alpha \in \boldsymbol{R}_* \right\} K = \left\{\begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \middle| \theta \in \boldsymbol{R}\right\}.$$

Take $dn = dx$, $da = |\alpha|^{-1}\,d\alpha$, $dk = d\theta/2\pi$, and take dg to be such that

$$\int_G \phi(g)\,dg = \int_N dn \int_{A_R} da \int_K dk |\alpha|^{-2} \phi(nak).$$

Then the inner product of $\phi^\wedge$ and $\psi^\wedge$ is equal to

$$\text{(a)} \qquad \frac{1}{2\pi i} \int_{\operatorname{Re} z = z_0} \Phi(z)\overline{\Psi}(-\bar{z}) + \frac{\xi(z)}{\xi(1+z)} \Phi(z)\overline{\Psi}(\bar{z})\,dz \qquad (z_0 > 1).$$

Here $\Phi(z) = \Phi(\Lambda(z))$ where $\Lambda(z)$ is the linear function such that $\Lambda(H_\alpha) = z$ if

$$H_\alpha = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

In the present situation $\Phi(\cdot)$ is a scalar valued function so inner products are replaced by products and if s is the nontrivial element of the Weyl group $M(s, \Lambda(z))$ is a scalar valued function equal to $\xi(z)/\xi(1+z)$ if

$$\xi(z) = \pi^{-z/2}\Gamma(z/2)\zeta(z).$$

Using the residue theorem we see that the expression (a) is the sum of two terms

$$\text{(b)} \qquad \frac{1}{2\pi i} \int_{\operatorname{Re} z = 0} \Phi(z)\overline{\Psi}(-\bar{z}) + \frac{\xi(z)}{\xi(z+1)} \Phi(z)\overline{\Psi}(\bar{z})\,dz$$

and

$$\text{(c)} \qquad \frac{1}{\xi(2)} \Phi(1)\overline{\Psi}(1).$$

The estimates of §6 justify this application of the residue theorem. We immediately see that $L(\{P\}, \{V\}, W)$ is the direct sum of two subspaces $L_i(\{P\}, \{V\}, W)$, $i = 0, 1$. $L_0(\{P\}, \{V\}, W)$ is the space of constant functions and the inner product of the projection of $\phi^\wedge$ and $\psi^\wedge$ on this space is given by (c). The inner product of the projection of $\phi^\wedge$ and $\psi^\wedge$ on $L_1(\{P\}, \{V\}, W)$ is given by (b) which equals

$$\frac{1}{\pi} \int_{-\infty}^{\infty} \tfrac{1}{2}\left\{\Phi(iy) + \frac{\xi(-iy)}{\xi(1-iy)}\Phi(-iy)\right\} \cdot \tfrac{1}{2}\overline{\left\{\Psi(iy) + \frac{\xi(-iy)}{\xi(1-iy)}\Psi(-iy)\right\}}\,dy.$$

As a consequence $L_1(\{P\}, \{V\}, W)$ is isometric to the space of all functions Υ, square integrable on the imaginary axis with respect to the measure dy/π, which satisfy

$$\Upsilon(-iy) = \frac{\xi(iy)}{\xi(1+iy)}\Upsilon(iy).$$

The term (c) comes from the pole of $\xi(z)/\xi(1+z)$ at $z = 1$. As it happens $E(g, \Phi, z)$ also has a pole at $z = 1$; to see what the residue is we observe that

(a) $$\int_{\Gamma \cap N \backslash N} \operatorname*{Res}_{z=1} E(ng, \Phi, z)\, dn = \operatorname*{Res}_{z=1} \int_{\Gamma \cap N \backslash N} E(ng, \Phi, z)\, dn.$$

This of course is equal to

$$\operatorname*{Res}_{z=1}\left\{\exp((\Lambda(z) + \rho)(H(g))) + \frac{\xi(z)}{\xi(1+z)}\exp((-\Lambda(z) + \rho)(H(g)))\right\}\Phi = \frac{1}{\xi(2)}\Phi$$

if $\Phi(g) \equiv \Phi$. Thus

$$\operatorname*{Res}_{z=1} E(g, \Phi, z) - \frac{1}{\xi(2)}\Phi$$

is a cusp form. Since it is also orthogonal to all cusp forms it must be zero.

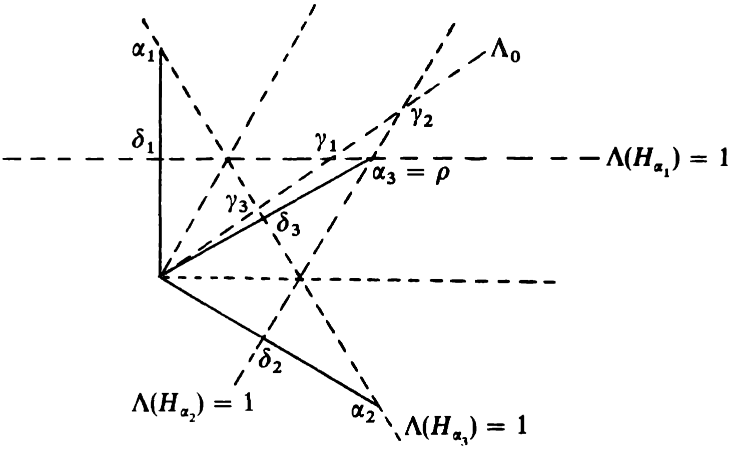
The analogue of the expression (a) when $G = \mathrm{SL}(3, \boldsymbol{R})$ is

(d) $$\frac{1}{(2\pi)^2}\int_{\operatorname{Re}\Lambda = \Lambda_0} \sum_{s \in \Omega} M(s, \Lambda)\Phi(\Lambda)\bar{\Psi}(-s\bar{\Lambda})|d\Lambda|$$

with

$$M(s, \Lambda) = \prod_{\alpha > 0;\, s\alpha < 0} \frac{\xi(\Lambda(H_\alpha))}{\xi(1 + \Lambda(H_\alpha))}$$

(for notation, see my lecture on the volume of fundamental domains).



The only singularities of the functions $M(s, \Lambda)$ which meet the tube over the positive Weyl chamber are simple poles on the lines $\Lambda(H_{\alpha_i}) = 1$, $i = 1, 2, 3$. If

$\Phi(\Lambda)$ vanishes on these three lines then (d) is equal to

$$\text{(e)} \qquad \frac{1}{(2\pi)^2}\int_{\operatorname{Re}\Lambda=0}\sum_{s\in\Omega} M(s,\Lambda)\Phi(\Lambda)\bar{\Psi}(-s\bar{\Lambda})|d\Lambda|.$$

Call the closed subspace generated by the functions $\hat{\phi}$ corresponding to $\Phi(\cdot)$ of this sort $L_2(\{P\},\{V\},W)$. As before, $L_2(\{P\},\{V\},W)$ is isometric to the space of square integrable functions on the (real) plane, $\operatorname{Re}\Lambda = 0$, which satisfy certain functional equations. Under this isometry convolution by K-invariant functions on G becomes multiplication by scalar-valued functions. The inner product of the projection of any $\hat{\phi}$ and $\hat{\psi}$ on $L_2(\{P\},\{V\},W)$ is given by (e).

The difference between (d) and (e) is nothing but the inner product of the projection of $\hat{\phi}$ and $\hat{\psi}$ on the orthogonal complement of $L_2(\{P\},\{V\},W)$. If $\mathfrak{s}_i$ is the complex line $\Lambda(H_{\alpha_i}) = 1$, $1 \leqq i \leqq 3$, then by the residue theorem the difference will be a sum of three integrals taken respectively over the real lines $\operatorname{Re}\Lambda = \gamma_i$ in $\mathfrak{s}_i$. To describe the exact form of the integrals we need a little notation. Let $\Omega(\mathfrak{s}_i,\mathfrak{s}_j)$ be the set of distinct affine transformations from $\mathfrak{s}_i$ to $-\mathfrak{s}_j$ obtained by restricting those elements of Ω which take $\mathfrak{s}_i$ to $-\mathfrak{s}_j$ to $\mathfrak{s}_i$. The difference we spoke of can be written as

$$\text{(f)} \qquad \sum_{i=1}^{3}\sum_{j=1}^{3}\sum_{s\in\Omega(\mathfrak{s}_i,\mathfrak{s}_j)}\frac{1}{2\pi}\int_{\operatorname{Re}\Lambda=\gamma_i} M(s,\Lambda)\Phi(\Lambda)\bar{\Psi}(-s\Lambda)|d\Lambda|.$$

Here $M(s,\Lambda)$ is a certain scalar valued function on $\mathfrak{s}_i$. In a moment I shall give the explicit form of these functions. First we observe that $\Omega(\mathfrak{s}_1,\mathfrak{s}_2)$ contains exactly one element ρ, the restriction to $\mathfrak{s}_1$ of the reflection in $\Lambda(H_{\alpha_1}) = 0$, that $\Omega(\mathfrak{s}_1,\mathfrak{s}_2)$ contains exactly one element σ, the restriction to $\mathfrak{s}_1$ of the reflection in $\Lambda(H_{\alpha_3}) = 0$, and that $\Omega(\mathfrak{s}_1,\mathfrak{s}_3)$ contains exactly one element τ, the restriction to $\mathfrak{s}_1$ of the rotation through an angle of $2\pi/3$. From these three elements we can obtain for each i and j the unique element of $\Omega(\mathfrak{s}_i,\mathfrak{s}_j)$. For example, the unique element of $\Omega(\mathfrak{s}_3,\mathfrak{s}_2)$ is $\sigma\rho\tau^{-1}$. Observe that, for example, $\tau\rho$ takes $\mathfrak{s}_1$ to $\mathfrak{s}_3$. If Λ is in $\mathfrak{s}_1$ and $\Lambda(H_{\beta_3}) + \frac{1}{2} = z$ the number in the second row and third column of the following table is $M(\sigma\rho\tau^{-1},\tau\rho\Lambda)$. The other entries are interpreted accordingly.

	ρ	σ	τ
ρ	$\frac{1}{\xi(2)}$	$\frac{1}{\xi(2)}\frac{\xi(-z-\frac{1}{2})}{\xi(-z+\frac{3}{2})}$	$\frac{1}{\xi(2)}\frac{\xi(\frac{1}{2}-z)}{\xi(\frac{3}{2}-z)}$
σ	$\frac{1}{\xi(2)}\frac{\xi(z-\frac{1}{2})}{\xi(z+\frac{3}{2})}$	$\frac{1}{\xi(2)}$	$\frac{\xi 1}{\xi(2)}\frac{\xi(\frac{1}{2}+z)}{\xi(\frac{3}{2}+z)}$
τ	$\frac{1}{\xi(2)}\frac{\xi(z+\frac{1}{2})}{\xi(z+\frac{3}{2})}$	$\frac{1}{\xi(2)}\frac{\xi(-z+\frac{1}{2})}{\xi(-z+\frac{3}{2})}$	$\frac{1}{\xi(2)}\frac{\xi(\frac{1}{2}-z)}{\xi(\frac{3}{2}-z)}\frac{\xi(\frac{1}{2}+z)}{\xi(\frac{3}{2}+z)}$

The matrix defined by this table is of rank one.

The integral (f) is the sum of

$$\text{(g)} \qquad \sum_{i=1}^{3}\sum_{j=1}^{3}\sum_{s\in\Omega(\mathfrak{s}_i,\mathfrak{s}_j)}\frac{1}{2\pi}\int_{\operatorname{Re}\Lambda=\delta_i} M(s,\Lambda)\Phi(\Lambda)\bar{\Psi}(-s\bar{\Lambda})|d\Lambda|$$

and

$$\text{(h)} \qquad \frac{1}{\xi(2)\xi(3)}\Phi(\rho)\bar{\Psi}(\rho).$$

The points δ_i are shown on the diagram. Correspondingly the orthogonal complement of $L_2(\{P\},\{V\},W)$ in $L(\{P\},\{V\},W)$ is the direct sum of $L_1(\{P\},\{V\},W)$ and $L_0(\{P\},\{V\},W)$ and the inner product of the projections of $\phi^\wedge$ and $\psi^\wedge$ on these two spaces are given respectively by (g) and (h). $L_0(\{P\},\{V\},W)$ is just the space of constant functions. There is an isometry of $L_1(\{P\},\{V\},W)$ with a subspace of the direct sum of the spaces of square-integrable functions on $\operatorname{Re}\Lambda_1=\delta_1$ and $\operatorname{Re}\Lambda_1=\delta_2$ which is such that convolution by K-invariant functions corresponds to multiplication by scalar valued functions.

The functions $E(g,\Phi,\Lambda)$ also have poles on the lines $\mathfrak{s}_i$. To compute the residue of $E(g,\Phi,\Lambda)$ on the line $\mathfrak{s}_1$ we combine our earlier result for SL(2, **R**) with the formula of §7. The result is

$$\frac{1}{\xi(2)}\sum_{\Gamma\cap{}^*P\backslash\Gamma}\exp({}^*\Lambda({}^*H(\gamma g))+\rho({}^*H(\gamma g)))\Phi=\frac{1}{\xi(2)}E'(g,\Phi,{}^*\Lambda);$$

the sum of an Eisenstein series belonging to the cuspidal subgroup ${}^*P$. The Eisenstein series on the left is, unlike those we have dealt with up to now, not an Eisenstein series associated to a cusp form. An automatic consequence of the above is that the function defined by the sum on the left is everywhere meromorphic.

Denote the residue of $E(g,\Phi,\Lambda)$ on $\mathfrak{s}_i$ by $E_i(g,\Phi,\Lambda)$. Then

$$\int_{\Gamma\cap N\backslash N} E_i(ng,\Phi,\Lambda)\,dn=\sum_{j=1}^{3}\sum_{s\in\Omega(\mathfrak{s}_i,\mathfrak{s}_j)}\exp(s\Lambda(H(g))+\rho(H(g)))(M(s,\Lambda)\Phi)(g).$$

Since the matrix introduced above is of rank one this implies that

$$E_2(g,\Phi,\sigma\rho\Lambda)=\frac{\xi(-z-\frac{1}{2})}{\xi(-z+\frac{3}{2})}E_1(g,\Phi,\Lambda),$$

$$E_3(g,\Phi,\tau\rho\Lambda)=\frac{\xi(\frac{1}{2}-z)}{\xi(\frac{3}{2}-z)}E_1(g,\Phi,\Lambda).$$

In the general case one can show that $L(\{P\},\{V\},W)$ is a direct sum

$$\sum_{i=0}^{g}\oplus L_i(\{P\},\{V\},W)$$

with g equal to the rank of the elements of $\{P\}$. In the course of doing this one sees that all Eisenstein series define functions which are everywhere meromorphic and satisfy functional equations of the expected type. The spectrum of $L_i(\{P\}, \{V\}, W)$ is again continuous of dimension i. Beyond this, however, the situation is very foggy.

Dimension of Spaces of Automorphic Forms[1]

BY

R. P. LANGLANDS[2]

I will first formulate a problem in the theory of group representations and show how to solve it; then I will discuss the relation of this problem to the theory of automorphic forms. Since there is no point in striving for maximum generality I start with a connected semisimple group G with finite center. An irreducible unitary representation π of G on the Hilbert space H is said to be square-integrable if for one, and hence, as one can show, every pair u and v of nonzero vectors in H the function $(\pi(g)u, v)$ is square-integrable on G. It is said to be integrable if for one such pair $(\pi(g)u, v)$ is integrable.

Suppose Γ is a discrete subgroup of G and $\Gamma\backslash G$ is compact. As was shown by Godement in an earlier lecture the representation π of the previous paragraph occurs a finite number of times, say $N(\pi)$, in the regular representation on $L^2(\Gamma\backslash G)$. The problem is first to find a closed formula for $N(\pi)$. The method which I will now describe of obtaining such a formula is valid only when π is actually integrable.

Square integrable representations are similar in some respects to representations of compact groups; in particular they satisfy a form of the Schur orthogonality relations. There is a constant d_π called the formal degree of π so that if u', v', u, and v belong to H then

$$\int_G (\pi(g)u', v')\overline{(\pi(g)u, v)}\, dg = d_\pi^{-1}(u', u)(v, v').$$

If u and v are such that $(\pi(g)u, v)$ is integrable and π' is a unitary representation of G on H' which does not contain π, then

$$\int_G (\pi'(g)u', v')\overline{(\pi(g)u, v)}\, dg = 0$$

for all u', v' in H.

Let L_i, $1 \leqq i \leqq N(\pi)$, be a family of mutually orthogonal invariant subspaces of $L^2(\Gamma\backslash G)$ which are such that the action of G on each of them is equivalent to π. Suppose that π does not occur in the orthogonal complement of

$$\sum_{i=1}^{N(\pi)} \oplus L_i.$$

[1] Based on notes of the original lecture taken by J. Shalika.

[2] Miller fellow.

If π is integrable there is a unit vector v in H so that $(\pi(g)v, v)$ is integrable. Let v_i be a unit vector in L_i corresponding to v under some equivalence between H and L_i. The orthogonality relations imply that the operator $\Phi \to \Phi'$ with

$$\Phi'(g) = d_\pi \int_G \Phi(gh)\overline{(\pi(h)v, v)}\, dh$$
$$= \int_{\Gamma\backslash G} \Phi(h)\left\{\sum_\Gamma \xi(g^{-1}\gamma h)\right\} dh,$$

if $\xi(g) = d_\pi\overline{(\pi(g)v, v)}$, is an orthogonal projection on the space spanned by $v_1, \cdots, v_{N(\pi)}$. For our purposes it may be assumed that v transforms according to a finite-dimensional representation of some maximal compact subgroup of G. Then the argument used by Borel in a previous lecture shows that

$$\sum_\Gamma \xi(g^{-1}\gamma h)$$

converges absolutely uniformly on compact subsets of $G \times G$. Hence $v_1, \cdots, v_{N(\pi)}$ may be supposed continuous. As a consequence

$$\sum_{i=1}^{N(\pi)} v_i(g)\bar{v}_i(h) = \sum_\Gamma \xi(g^{-1}\gamma h).$$

Set $h = g$ and integrate over $\Gamma\backslash G$ to obtain

$$N(\pi) = \int_{\Gamma\backslash G} \sum_\Gamma \xi(g^{-1}\gamma g)\, dg.$$

The sum in the integrand may be rearranged at will. If Σ is a set of representatives for the conjugacy classes in Γ the integral on the right equals

$$\int_{\Gamma\backslash G} \sum_{\gamma\in\Sigma} \sum_{\delta\in\Gamma_\gamma\backslash\Gamma} \xi(g^{-1}\delta^{-1}\gamma\delta g)\, dg = \sum_{\gamma\in\Sigma} \int_{\Gamma_\gamma\backslash G} \xi(g^{-1}\gamma g)\, dg$$
$$= \sum_{\gamma\in\Sigma} \mu(\Gamma_\gamma\backslash G_\gamma) \int_{G_\gamma\backslash G} \xi(g^{-1}\gamma g)\, dg,$$

if Γ_γ and G_γ are the centralizers of γ in Γ and G respectively. The equality of $N(\pi)$ and the final expression is of course a special case of a formula of Selberg and has been known for some time.

The problem of evaluating $\mu(\Gamma_\gamma\backslash G_\gamma)$, the volume of $\Gamma_\gamma\backslash G_\gamma$, has been discussed in the lectures on Tamagawa numbers so we shall not worry about it now. Since $\Gamma\backslash G$ is compact every element of Γ is semisimple; thus our problem is to express the integral

$$\int_{G_\gamma\backslash G} \xi(g^{-1}\gamma g)\, dg$$

in elementary terms when γ is a semisimple element of G.

If π is a square-integrable representation of G on H, v is a vector in H which transforms according to a finite-dimensional representation of some maximal compact subgroup of G, and

$$\xi(g) = d_\pi \overline{(\pi(g)v, v)},$$

then a recent theorem of Harish-Chandra states that

$$\text{(a)} \qquad \int_{G_\gamma\backslash G} \xi(g^{-1}\gamma g)\,dg$$

exists for γ semisimple and vanishes unless γ is elliptic, that is, belongs to some compact subgroup of G. Since Σ contains only a finite number of elliptic elements the sum in the expression for $N(\pi)$ is finite. We still require a closed expression for the integrals appearing in it.

Let K be a maximal compact subgroup of G. Since G has a square integrable representation there is a Cartan subgroup T of G contained in K. It is enough to compute the integrable (a) for γ in T. There is a limit formula of Harish-Chandra which allows one to compute its value at the singular elements once its values at the regular elements are known. Thus we need only evaluate it when γ is regular. It should be remarked that in this limit formula there is a constant which depends on the choice of Haar measure on G_γ. The exact relation of this constant to the choice of Haar measure has never been determined; until it is, our problem cannot be regarded as completely solved.

If γ is regular and the measure on G_γ is so normalized that the volume of G_γ is one, then

$$\int_{G_\gamma\backslash G} \xi(g^{-1}\gamma g)\,dg = \chi_\pi(\gamma^{-1})$$

if χ_π is the character of π. An explicit expression for the right-hand side has recently been obtained.

Let h be the Lie algebra of T; choose an order on the roots of $\mathfrak{h}_C$; and let Λ be a linear function on $\mathfrak{h}_C$ so that $\Lambda + \rho, \rho = \frac{1}{2}\sum_{\alpha>0}\alpha$, extends to a character of T and so that $(\Lambda + \rho, \alpha) \neq 0$ for all roots α. Assume, for simplicity, that ρ also extends to a character of T. To each such Λ there is associated a square-integrable representation π_Λ and if $H \in \mathfrak{h}$

$$\chi_{\pi_\Lambda}(\exp H) = (-1)^m\varepsilon(\Lambda) \sum_{\sigma\in W} \frac{\operatorname{sgn}\sigma \exp(\sigma(\Lambda + \rho))(H)}{\prod_{\alpha>0} \{(\exp(\alpha(H)/2) - \exp(-\alpha(H)/2))\}}.$$

Here $m = \frac{1}{2}\dim G/K$, $\varepsilon(\Lambda) = \operatorname{sgn}(\prod_{\alpha>0}(\Lambda + \rho, \alpha))$, and W is the Weyl group of K. Every square-integrable representation is equivalent to π_Λ for some Λ. However the values of Λ for which π_Λ is integrable are not yet known. For some special cases see [1] and [2].

The geometrical meaning of the numbers $N(\pi_\Lambda)$ is not yet completely clear. I would like to close this lecture with some suggestions as to what it might be.

Since the evidence at present is rather meagre, they are only tentative. If $\mathfrak{g}_C$ is the complexification of the Lie algebra of $\mathfrak{g}$, the elements of $\mathfrak{g}_C$ may be regarded as left-invariant complex vector fields on G, G/T may be turned into a complex manifold in such a way that the space of antiholomorphic tangent vectors at $\bar{g} = gT$ is the image of $\mathfrak{n}_C^-$ if $\mathfrak{n}_C^-$ is the subalgebra of $\mathfrak{g}_C$ generated by root vectors belonging to negative roots. Let V^* be the bundle of antiholomorphic cotangent vectors and introduce a G-invariant metric in V^* and hence in $\Lambda^q V^*$. Let B be the line bundle over G/T associated to the character $\xi(\exp H) = \exp(\Lambda(H))$ of T. If Γ is a discrete subgroup of G let $C^q(\Lambda, \Gamma)$ be the space of Γ-invariant cross-sections of $B \otimes \Lambda^q V^*$ which are square integrable over $\Gamma \backslash G/T$. There is a unique closed operator $\bar{\partial}$ from $C^q(\Lambda, \Gamma)$ to C^{q+1} of Λ, Γ whose domain contains the infinitely differentiable cross-sections of compact support on which $\bar{\partial}$ is to have its usual meaning and whose adjoint is defined on the infinitely differentiable cross-sections of $C^{q+1}(\Lambda, \Gamma)$ with compact support.

Set $C^q(\Lambda, \{1\}) = C^q(\Lambda)$. I expect, although I do not know how to prove it, that when $\Lambda + \rho$ is nonsingular the range of $\bar{\partial}$ is closed for every q. If this is so then the cohomology groups $H^q(\Lambda)$ will be Hilbert spaces on which G acts. Is it true that they vanish for all but one value of q, say $q = q_\Lambda$, and that the representation π'_Λ of G on $H^{q_\Lambda}(\Lambda)$ is equivalent to π_Λ? The following theorem is a clue to the value of q_Λ.

THEOREM (P. GRIFFITHS). *Let a_1 be the number of noncompact positive roots for which $(\Lambda + \rho, \alpha) > 0$ and let a_2 be the number of compact positive roots for which $(\Lambda + \rho, \alpha) < 0$. There is a constant c so that if $|(\Lambda + \rho, \alpha)| > c$ for every simple root, $\Gamma \backslash G$ is compact, and Γ acts freely on G/T, then $H^q(\Lambda, \Gamma) = 0$ unless $q = a_1 + a_2$.*

It is, I think, worthy of remark that if one assumes that $H^q(\Lambda) = \{0\}$ for $q \neq q_\Lambda = a_1 + a_2$, then a formal application of the Woods Hole fixed point formula shows that if γ is a regular element of T, then the value at γ of the character of π'_Λ is $\chi_{\pi_\Lambda}(\gamma)$. By the way, it is known that $H^0(\Lambda) = 0$ unless $q_\Lambda = 0$ and that if $q_\Lambda = 0$ the representation of G on $H^0(\Lambda)$ is in fact π_Λ.

Finally one will want to show that when π_Λ is integrable and $\Gamma \backslash G$ is compact the number $N(\pi_\Lambda)$ is equal to the dimension of $H^{q_\Lambda}(\Lambda, \Gamma)$. This can be done when $q_\Lambda = 0$; in this case $H^0(\Gamma, \Lambda)$ is a space of automorphic forms.

It should be possible, although I have not done so, to test these suggestions for groups whose unitary representations are well understood, in particular, for $\mathrm{SL}(2, \boldsymbol{R})$ and the De Sitter group. To do this one might make use of an idea basic to Kostant's proof of the (generalized) Borel–Weil theorem for compact groups. Suppose σ is a unitary representation of G on a Hilbert space V. Let $C^q(V)$ be the space of all linear maps from $\Lambda^q n_C^-$ to V. $C^q(V)$ is a Hilbert space. The usual coboundary operator from $C^q(V)$ to $C^{q+1}(V)$ can be defined on those elements of $C^q(V)$ which take values in the Gårding subspace of V. The closure d of this operator is the adjoint of the restriction of its formal adjoint to those elements of $C^{q+1}(V)$ which take values in the Gårding subspace. T of course acts on $\Lambda^q n_C^-$. If $f \in C^q(V)$ define $tf = f'$ by $f'(X) = tf(t^{-1}X)$, $X \in \Lambda^q n_C^-$. There is a natural identification of $C^q(\Lambda)$ with the set of f in $C^q(L^2(G))$ such that $tf = \exp(-\Lambda(H))f$ if $t = \exp H$ belongs to T and of $C^q(\Lambda, \Gamma)$ with the set of f in $C^q(L^2(\Gamma\backslash G))$ such that $tf = \exp(-\Lambda(H))f$. Moreover the following diagrams are commutative.

$$\begin{tikzcd}
C^q(\Lambda) \arrow[r, "\bar\partial"] \arrow[d, hook] & C^{q+1}(\Lambda) \arrow[d, hook] & C^q(\Lambda, \Gamma) \arrow[r, "\bar\partial"] \arrow[d, hook] & C^{q+1}(\Lambda, \Gamma) \arrow[d, hook] \\
C^q(L^2(G)) \arrow[r, "d"] & C^{q+1}(L^2(G)) & C^q(L^2(\Gamma\backslash G)) \arrow[r, "d"] & C^{q+1}(L^2(\Gamma\backslash G)).
\end{tikzcd}$$

The point is that d is easier to study than $\bar\partial$ because to study d we can decompose V into irreducible representations and study the action of d on each part.

References

1. J. Dixmier, *Représentations intégrables du groupe de De Sitter*, Bull. Soc. Math. France **89** (1961), 9–41.
2. Harish-Chandra, *Representations of semisimple Lie groups*. VI, Amer. J. Math. **78** (1956), 564–628.
3. ———, *Discrete series for semisimple Lie groups*, II. Acta. Math. (to appear).
4. Bertram Kostant, *Lie algebra cohomology and the generalized Borel–Weil theorem*, Ann. of Math. (2) **74** (1961), 329–387.
5. R. P. Langlands, *The dimension of spaces of automorphic forms*, Amer. J. Math. **85** (1963), 99–125.

Spherical Functions and Ramanujan Conjecture[1]

BY

ICHIRO SATAKE

The following exposition has nothing to do with the proof of the conjecture, but might indicate a possible generalization of it tò the higher dimensional case.

1. Zonal spherical functions.

Let G be a locally compact unimodular group and K a compact subgroup of G. Let $L = L(G, K)$ be the associative algebra (with the convolution product) consisting of all complex-valued continuous functions on G with compact support satisfying

$$\phi(kgk') = \phi(g)$$

for all k, k' in K and g in G. We make the basic assumption that *L is commutative.*

DEFINITION. ω is called a *zonal spherical function* on G relative to K, if

(1.1) ω is a complex-valued continuous function on G satisfying $\omega(1) = 1$,

(1.2) ω is K bi-invariant, i.e., $\omega(kgk') = \omega(g)$,

(1.3) for all $\phi \in L$, one has $\phi * \omega = \lambda_\phi \omega$, i.e., ω is an eigenfunction for all (invariant) integral operators defined by ϕ in L. (In this case we automatically have $\phi * \omega = \omega * \phi$.)

Clearly the map of L into C defined by $\phi \mapsto \lambda_\phi$ is a ring homomorphism. We write $\lambda_\phi = \hat{\omega}(\phi) = \int_G \phi(g)\omega(g^{-1})\,dg$. The function ω is uniquely determined by $\hat{\omega}$.

REMARK. Condition (3) above may be replaced by the "functional equation":

$$\int_K \omega(g_1 k g_2)\,dk = \omega(g_1)\omega(g_2) \tag{1.3)$'$}$$

for all $g_1, g_2 \in G$; or in the case where G is a connected Lie group by:

(1.3)″ Let $X = G/K$ with its natural C^∞ structure, then ω, considered as a function on X, should be an eigenfunction for all G-invariant differential operators on X.

EXAMPLES. Any (quasi-)character $\chi : G \to C^*$ such that $\chi | K = 1$. In particular the constant $\mathbf{1}$ is a (positive-definite) zonal spherical function.

Let $\Omega = \Omega(G, K)$ denote the set of all zonal spherical functions (relative to K) and Ω^+ be the subset of all "positive-definite" zonal spherical functions.

[1] The same talk was once given at the University of Tokyo in the Spring of 1961.

(In general, a continuous function ω on G is called positive-definite, if for all functions ϕ of compact support on G

$$\int_G \int_G \omega(g_1^{-1}g_2)\overline{\phi(g_1)}\phi(g_2)\,dg_1\,dg_2 \geqq 0.)$$

One sees easily that ω is positive-definite implies

(1.4) $\overline{\omega(g^{-1})} = \omega(g)$, i.e., ω is self-adjoint,

(1.5) $|\omega(g)| \leqq \omega(1) = 1$.

For positive-definite zonal functions, we have [4].

Lemma. *If* $\omega \in \Omega^+$, $\phi \in L$, *then*

(1.6) ϕ *is self-adjoint implies* $\hat{\omega}(\phi) \in \boldsymbol{R}$,

(1.7) ϕ *is real and nonnegative implies* $|\hat{\omega}(\phi)| \leqq \hat{\mathbf{1}}(\phi)$.

The basic assumption that L is commutative assures us of the following

Theorem ([2]). *The set of positive-definite zonal functions* ω $(\in\Omega^+)$ *are in a one-to-one correspondence with equivalence-classes of irreducible unitary representations of* G *of class one.*

An (irreducible unitary) representation $(\mathfrak{H}, U)$ of G is called "of class one" if $U|K$ contains the trivial representation of K. It is well known [2] that the condition that $L(G, K)$ is commutative, is equivalent to saying that for any irreducible unitary representation $(\mathfrak{H}, U)$ the dimension of the subspace of all K-invariant vectors in $\mathfrak{H}$ is $\leqq 1$. For an irreducible unitary representation $(\mathfrak{H}, U)$ of class one, the corresponding zonal spherical function ω is obtained by

$$\omega(g) = \langle x_0, U_g x_0 \rangle,$$

x_0 being a K-invariant unit vector in $\mathfrak{H}$.

2. **The case of** PL(2). Let $G = \mathrm{PL}(2) = \mathrm{GL}(2)/\text{center}$,

$$G_p = \mathrm{PL}(2, \boldsymbol{Q}_p),$$
$$K_p = \begin{cases} \mathrm{O}(2)/\{\pm 1\} & \text{for } p = \infty, \\ \mathrm{GL}(2, \boldsymbol{Z}_p)/\text{center} & \text{for } p < \infty. \end{cases}$$

We have the Iwasawa and elementary divisor decompositions:

$$G_p = K_p A_p N_p = K_p A_p K_p,$$

where A_p and N_p are the respective images in PL(2, $\boldsymbol{Q}_p$) of

$$\left\{\begin{pmatrix} \xi_1 & 0 \\ 0 & \xi_2 \end{pmatrix}\right\} \text{ and } \left\{\begin{pmatrix} 1 & \eta \\ 0 & 1 \end{pmatrix}\right\}.$$

Definitions of representations of G_p of the principal series. Let $\alpha : A_p \to C^*$ be a (quasi-) character of A_p, and $\mathfrak{H}^\alpha$ be the space of all complex-valued functions on G such that $\phi(gan) = \alpha(a)\phi(g)$ for all $a \in A_p$, $n \in N_p$, $g \in G_p$ and that

$$\|\phi\|^2 = \int_K |\phi(k)|^2 \, dk < \infty.$$

Then $\mathfrak{H}^\alpha$ is a Hilbert-space (with the norm $\| \ \|$), and if we put $T^\alpha_{g_1}(\phi)(g) = \phi(g_1^{-1}g)$ for $\phi \in \mathfrak{H}^\alpha$ we obtain a representation of G_p in the bounded operators on $\mathfrak{H}^\alpha$. This representation is of class one if and only if $\alpha|(A_p \cap K_p) = 1$, in which case α has the form:

$$\alpha(a) = \left|\frac{\xi_1}{\xi_2}\right|_p^{s-\frac{1}{2}} \tag{2.1}$$

with $s \in C$ (which is determined $\operatorname{mod}(2\pi i/\log p)$ for $p < \infty$). And in this case, the function ψ_α defined by $\psi_\alpha(kan) = \alpha(a)$ is a K_p-invariant unit vector in $\mathfrak{H}^\alpha$, and the corresponding zonal spherical function is given by

$$\omega_s(g) = \langle \psi_\alpha, T^\alpha_g \psi_\alpha \rangle = \int_K \psi_\alpha(g^{-1}k) \, dk. \tag{2.2}$$

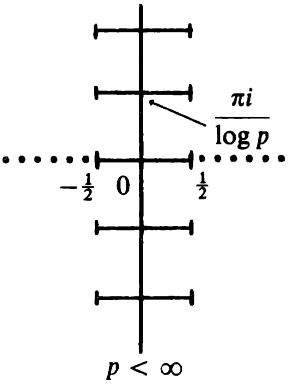
Further the representation $(\mathfrak{H}^\alpha, T^\alpha_g)$ is unitary if and only if s is purely imaginary.

THEOREM ([1], [4]). *$L(G_p, K_p)$ is commutative, and we have $\Omega_p = \Omega(G_p, K_p) = \{\omega_s\}$ with the relations*

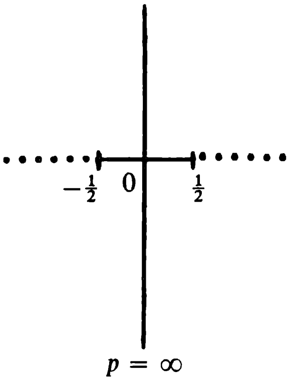
$$\omega_s = \omega_{s'} \quad \textit{if and only if}$$

$$\begin{cases} s' \equiv \pm s \left(\operatorname{mod} \dfrac{2\pi i}{\log p}\right) & \textit{for } p < \infty, \\ s' = \pm s & \textit{for } p = \infty. \end{cases}$$

Further, Ω_p^+ is described by the following diagrams:



$p < \infty$



$p = \infty$

(The solid lines correspond to those s for which ω_s is positive-definite.)

The representations corresponding to the vertical axis are called representations of the "principal series" (of class one) and those corresponding to the horizontal axis "supplementary series." The points $s = \pm\frac{1}{2}$ correspond to the identical character **1**, and for $p < \infty$ the points $s = \pm\frac{1}{2} + (\pi i/\log p)$ correspond to the character defined by $\chi(g) = (-1)^{v_p(\det g)}$. We can obtain a necessary condition for ω_s to belong to Ω_p^+ by the following considerations: For $p < \infty$, let τ_p be the characteristic function of the double coset

$$K_p\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}K_p.$$

Then (2.2) gives

$$\hat{\omega}_s(\tau_p) = p^{\frac{1}{2}}(p^s + p^{-s}) \tag{2.3}$$

and by the lemma one sees that $\hat{\omega}_s(\tau_p)$ is real and $|\hat{\omega}_s(\tau_p)| \leqq \mathbf{1}(\tau_p) = 1 + p$. It follows that s belongs to the solid-lined portion of the above figure.

For $p = \infty$, if Δ denotes the Laplacian on the upper-half plane $\mathscr{H} = G_\infty/K_\infty$, we have

$$\Delta\omega_s = (s^2 - \tfrac{1}{4})\omega_s,$$

where $s^2 - \frac{1}{4}$ should be real and nonpositive, whence the same conclusion.

3. **Spectrum of a discrete subgroup.** Again let G be a locally compact unimodular group, and Γ be a discrete subgroup such that

$$v(\Gamma\backslash G) < \infty.$$

DEFINITION. A C-valued function f on G is called *Γ-automorphic right spherical function* if

$$f(\gamma g k) = f(g) \quad \text{for} \quad \gamma \in \Gamma, g \in G, k \in K, \tag{3.1}$$

$$f * \phi = \lambda_\phi f \text{ for all } \quad \phi \in L, \tag{3.2}$$

$$\int_{\Gamma\backslash G} |f(g)|^2\, dg < \infty. \tag{3.3}$$

Here the homomorphism $\phi \mapsto \lambda_\phi$ is given by a unique positive-definite zonal function ω [**5**]; we shall then say f belongs to ω. Let $\mathfrak{M}_\Gamma(\omega)$ be the set of all Γ-automorphic right spherical functions belonging to ω $(\in \Omega^+)$ and put

$$\mathrm{Spec}(\Gamma) = \{\omega \in \Omega^+ ; \mathfrak{M}_\Gamma(\omega) \neq \{0\}\}.$$

Spec(Γ) is always discrete in the weak topology of Ω^+.

4. **Formulation of the Ramanujan–Peterson conjecture.**

Let $G = \mathrm{PL}(2)$, $G_A = \prod_p' G_p$ the corresponding adele group, and $K = \prod_p K_p$. Then one has $L(G_A, K) = \mathrm{Inj\,lim}_S \otimes_{p \in S} L(G_p, K_p)$ and so $\Omega(G_A, K) = \prod_p \Omega(G_p, K_p)$ (see [**5**]). $L(G_A, K)$ is therefore commutative.

Now G_Q is a discrete subgroup of G_A such that $v(G_Q\backslash G_A) < \infty$. For $\omega \in \mathrm{Spec}(G_Q)$, we have at each p a local $\omega_p \in \Omega_p^+$, and hence a corresponding $s_p \in C$. Then the "fake Ramanujan conjecture" says that *for all* $p < \infty$, s_p *is purely imaginary.*

To obtain a formulation of the "actual Ramanujan conjecture", we must modify the above discussion by introducing representations of K_∞.

Since

$$K_\infty = \left\{ \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \cdot \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix} \right\} \Big/ \{\pm 1\},$$

we have, for every *even* integer v, a character χ_v of K_∞ defined by

$$\chi_v(k) = e^{vi\theta}.$$

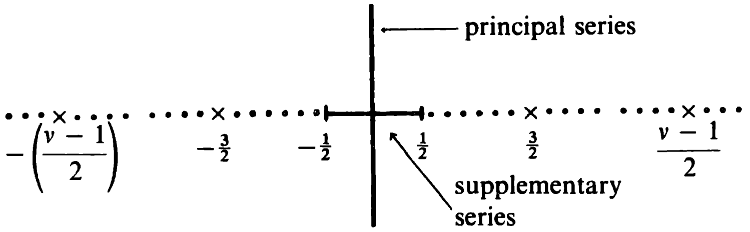
Let $L_\infty^{(v)} = L^{(v)}(G_\infty, K_\infty)$ be the algebra of all continuous functions ϕ of compact support on G_∞ satisfying

$$\phi(kgk') = \phi(g)\chi_v(k)\chi_v(k')$$

for $k, k' \in K_\infty$, $g \in G_\infty$. Then $L_\infty^{(v)}$ is again commutative. We define $\Omega_\infty^{(v)}$ (the set of all spherical functions of type χ_v) by replacing L_∞ by $L_\infty^{(v)}$ in the Definition given in §1. In our case, the condition (1.3) is equivalent to the condition that ω is an eigen-function for the Casimir operator $\mathscr{C}$ of G_∞:

$$\mathscr{C}\omega = \lambda\omega,$$

and thus we can again parametrize $\omega \in \Omega_\infty^{(v)}$ by $s \in C$ determined by $\lambda = (s^2/2) - \frac{1}{8}$. $\omega \in \Omega_\infty^{(v)+}$ (positive-definite spherical functions of type χ_v) are in a one-to-one correspondence with equivalence-classes of irreducible unitary representations $(\mathfrak{H}, U)$ of G_∞ such that $U|K_\infty$ contains the representation χ_v. $\Omega_\infty^{(v)+}$ is described by the following diagram (with the identification of s and $-s$):



where the isolated points correspond to the "discrete series" of (square-integrable) representations of G_∞ ([**1**]).

Cusp Forms. Let $\Gamma = \mathrm{GL}(2, Z)/\{\pm 1\} \subset G_\infty$, and let $\mathfrak{S}_v$ be the space of all cusp forms of weight $v\,(v > 0)$; i.e., $f \in \mathfrak{S}_v$ if and only if

(4.1) f is a holomorphic function on the upper-half plane $\mathscr{H} = G_\infty/K_\infty$, (4.2) $f(\gamma \circ z) = f(z)j(\gamma, z)^{-\nu/2}$ for $\gamma \in \Gamma$, $z \in \mathscr{H}$, where

$$j(g, z) = \frac{\det(g)}{(cz + d)^2} \quad \text{for} \quad g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G_\infty,$$

(4.3) f vanishes at the "cusps" of Γ.

Put $F(g) = f(g(i))j(g, i)^{\nu/2}$, then

(4.1)′ $F(\gamma g k) = F(g)\chi_{-\nu}(k)$ for all $\gamma \in \Gamma$, $g \in G$, $k \in K$,

(4.2)′ $\mathscr{C}F = (\nu(\nu - 1)/8)F$, where $\mathscr{C}$ is the Casimir operator of G_∞,

(4.3)′ $\int_{\Gamma\backslash G} |F|^2 < \infty$.

The condition (4.2)′ is equivalent (under the condition (4.1)′) to the condition that $F * \phi = \lambda_\phi F$ for all $\phi \in L_\infty^{(\nu)}$, and so we may express the above properties of F by saying that F belongs to $\mathfrak{M}_\Gamma(\chi_{-\nu}, \omega_{\pm(\nu-1)/2})$, the space of all Γ-automorphic right spherical functions of type $\chi_{-\nu}$ belonging to $\omega_{\pm(\nu-1)/2}$. By the correspondence $f \leftrightarrow F$, we have the isomorphism:

$$\mathfrak{S}_\nu \cong \mathfrak{M}_\Gamma(\chi_{-\nu}, \omega_{\pm(\nu-1)/2}).$$

We may also consider F as a function on G_A. More precisely: G_A has class number 1, i.e., $G_A = G_Q(K_0 \times G_\infty)$ where $K_0 = \prod_{p<\infty} K_p$. Writing $g \in G_A$ in the form $g = \xi(k_0 \times g_\infty)$ with $\xi \in G_Q$, $k_0 \in K_0$, $g_\infty \in G_\infty$, put

$$\tilde{F}(g) = \tilde{F}(\xi \cdot k_0 \times g_\infty) = F(g_\infty).$$

Then (4.1)′ assures that $\tilde{F}$ is well defined and that

$$\tilde{F}(\xi \cdot g \cdot k_0 \times k_\infty) = \tilde{F}(g)\chi^{-\nu}(k_\infty) \qquad \text{for } \xi \in G_Q, k = k_0 \times k_\infty \in K,$$

(4.2)′ that $\tilde{F}$ is an eigenfunction of $L_\infty^{(\nu)}$ belonging to $\omega_{\pm(\nu-1)/2}$, and

(4.3)′ that $\tilde{F} \in L^2(G_Q\backslash G_A)$.

These conditions uniquely determine the space $\tilde{\mathfrak{S}}_\nu$ of $\tilde{F}$'s.

Now let $L^{(\nu)}(G_A, K) = \prod_{p<\infty} L(G_p, K_p) \times L^{(\nu)}(G_\infty, K_\infty)$.

Since $\tilde{F}(gk_0) = \tilde{F}(g)$ for $g \in G_A$, $k_0 \in K_0$, the (commutative) algebra

$$L(G_0, K_0) = \prod_{p<\infty} L(G_p, K_p)$$

operates on $\tilde{\mathfrak{S}}_\nu$ by convolution from the right. Further, by the approximation theorem, $L(G_0, K_0)$ is isomorphic to the "Hecke ring" (over C) $\mathscr{R}(G_Q, G_Z)$ of G_Q with respect to G_Z, the correspondence being given by associating to each double coset $G_Z\xi G_Z$ with $\xi \in G_Q$ the characteristic function of the double coset $K_0\xi K_0$. As is well known, $\mathfrak{S}_\nu$ is a module over $\mathscr{R}(G_Q, G_Z)$ and one sees that the spaces $\mathfrak{S}_\nu$ and $\tilde{\mathfrak{S}}_\nu$ are isomorphic as modules over $\mathscr{R}(G_Q, G_Z) \cong L(G_0, K_0)$ (i.e., if $\mathfrak{S}_\nu \ni f \leftrightarrow \tilde{F} \in \tilde{\mathfrak{S}}_\nu$ and ϕ_0 is the characteristic function of $K_0\xi K_0$, then $f|(G_Z\xi G_Z) \leftrightarrow \tilde{F} * \phi_0$.)

Thus the decomposition of $\mathfrak{M}_\Gamma(\chi_{-\nu}, \omega_{\pm(\nu-1)/2}) = \tilde{\mathfrak{S}}_\nu$ into eigenspaces under the action of $L^{(\nu)}(G_A, K)$:

$$\mathfrak{M}_\Gamma(\chi_{-\nu}, \omega_{\pm(\nu-1)/2}) = \sum_j \oplus \mathfrak{M}_{G_Q}(1 \times \chi_{-\nu}, \omega_0^{(j)} \times \omega_{\pm(\nu-1)/2})$$

runs parallel to the decomposition of $\mathfrak{S}_\nu$ with respect to the action of the usual Hecke operators.

If $\tilde{F} \in \mathfrak{M}_{G_Q}(1 \times \chi_{-\nu}, \omega_0^{(j)} \times \omega_{\pm(\nu-1)/2})$ with $\omega_0^{(j)} = (\cdots, \omega_{s_p}, \cdots)$, then

$$\begin{aligned} \tilde{F} * \tau_p &= \hat{\omega}_{s_p}(\tau_p)\tilde{F} \\ &= p^{\frac{1}{2}}(p^{s_p} + p^{-s_p})\tilde{F} . \end{aligned}$$

Since, under the isomorphism $L(G_0, K_0) \cong \mathscr{R}(G_Q, G_Z)$, τ_p corresponds to $p^{1-(\nu/2)}T_p$, the corresponding $f \in \mathfrak{S}_\nu$ is an eigenfunction of all $T_p : T_p f = a_p f$. By Hecke's theory, f is then of the form:

$$f(z) = c \sum_{n>0} a_n e^{2\pi i n z}$$

where one has

$$a_p = p^{(\nu/2)-1}\hat{\omega}_{s_p}(\tau_p) = p^{(\nu-1)/2}(p^{s_p} + p^{-s_p}).$$

(Thus the spaces $\mathfrak{M}_{G_Q}(1 \times \chi_{-\nu}, \omega_0^{(j)} \times \omega_{\pm(\nu-1)/2})$ are one-dimensional.)

The Ramanujan–Peterson conjecture precisely states that *for all p one has $|a_p| \leqq 2p^{(\nu-1)/2}$, which becomes $|p^{s_p} + p^{-s_p}| \leqq 2$, or s_p is purely imaginary, i.e., $\omega_0^{(j)}$ corresponds to the principle series at each p.*

One may also demonstrate that the action of the $L_0(G_0, K_0)$ on

$$\mathfrak{M}_\Gamma(\chi_{-\nu}, \omega_{\pm(\mu-1)/2})$$

(where $\mu = 2, 4, \cdots, \nu$) is isomorphic to the action of the usual Hecke operators on $\mathfrak{S}_\mu$ and $\bar{\mathfrak{S}}_\mu$; further if s is a point corresponding to the principal or supplementary series (Diagram 2), then the action of $L_0(G_0, K_0)$ on $\mathfrak{M}_\Gamma(\chi_{-\nu}, \omega_s)$ is isomorphic to the action of the Hecke operators on the automorphic waveforms of Maass. Thus one can also make the analogous conjecture for the Fourier coefficients of these forms.

References

1. V. Bargmann, *Irreducible unitary representations of the Lorentz group*, Ann. of Math. **48** (1947), 568–640.

2. R. Godement, *A theory of spherical functions*. I, Trans. Amer. Math. Soc. **73** (1952), 496–556.

2a. ———, *Introduction aux travaux de A. Selberg*, Sèminaire Bourbaki, 1957.

3. M. Kuga, *Fibre varieties over a symmetric space whose fibres are abelian varieties*. I, II, Lecture-Notes, Univ. of Chicago, 1963–1964.

4. I. Satake, *Theory of spherical functions on reductive algebraic groups over $\mathfrak{p}$-adic fields*, Publ. Math, No. 18, Inst. Hautes Études Sci., 1963.

5. T. Tamagawa, *On Selberg's trace formula*, J. of Fac. Sci., Univ. of Tokyo **8** (1960), 363–386.

Algebraic Curves Mod 𝔭 and Arithmetic Groups

BY

YASUTAKA IHARA

As is well known, a discrete subgroup of $\mathrm{SL}(2, R)/\pm 1$ whose quotient space has finite volume determines not only Riemann surface, but also the tower of (all) finite coverings of the latter satisfying certain conditions of ramifications. For example, the modular group determines coverings of the Riemann sphere with three ramifications, and hence can be regarded as a *dense* subgroup of the Galois group of the maximum Galois extension of $C(x)$ under ramification conditions.

If we try to consider analogous problems for algebraic curves over a finite field F_q, it seems necessary to take into account not only conditions of (tame) ramifications of prime divisors, but also the conditions that a given finite number of prime divisors should be decomposed completely. For example, it seems to me that the natural analogue of the former example is the following pair:

(*) The rational j-curve over F_{p^2} with three ramifications *plus conditions of decompositions at all such primes* (j) *that elliptic curves with moduli j have no points of order p.* (Such j are called *supersingular*, and are contained in F_{p^2}.)

(*) The group

$$\Gamma = \mathrm{SL}(2, Z^{(p)})/\pm 1$$

where $Z^{(p)}$ denotes the ring of all rational numbers whose denominators are powers of p. Γ is a discrete subgroup of

$$G = \{\mathrm{SL}(2, R) \times \mathrm{SL}(2, Q_p)\}/\pm 1.$$

Thus our problem is to consider $\Gamma = \mathrm{SL}(2, Z^{(p)})/\pm 1$ as a dense subgroup of the Galois group of certain infinite Galois extension K over $k = F_{p^2}(j)$, j a variable over $F_{p^2}(j)$, K/k satisfying the above ramification and decomposition conditions. Then, the Frobenius substitution of prime divisor of k in K/k determines a conjugacy class of Γ which vanishes if and only if the prime divisor is supersingular. This connects the set of all nonsupersingular prime divisors of k and the set of all primitive and elliptic (cf. §1.1) conjugacy classes of Γ in a one-to-one manner. This holds also for finite subextension k' of k in K and "corresponding subgroup" Γ' of Γ, which implies the coincidence of congruence ζ-function of k' with ζ-function of "Selberg's type" for discrete subgroup Γ' of G—surely they are not precisely equal because of supersingular primes.

These considerations lead us to the study of ζ-functions of arbitrary discrete subgroups of our

$$G = \{\mathrm{SL}(2, R) \times \mathrm{SL}(2, Q_p)\}/\pm 1$$

whose quotient spaces have finite volumes. Our interest lies in calculating the number which, in our previous special case of Γ (or Γ'), was the number of supersingular primes (i.e. the difference between two ζ-functions). By using this result, we can prove that all supersingular primes are actually decomposed completely in the field K constructed in §1.

Proofs are omitted, and will be published elsewhere.

BRIEF OUTLINES OF EACH SECTION

1.1. To set up a one-to-one correspondence between $\mathfrak{P}(\Gamma)$ and $\mathfrak{P}(k) - \mathfrak{S}(k)$; where $\Gamma = \mathrm{SL}(2, Z^{(p)})/\pm 1$, $\mathfrak{P}(\Gamma)$: set of all elliptic and primitive (cf. §1.1) conjugacy classes of $\Gamma, k = F_{p^2}(j)$, $\mathfrak{P}(k)$ the set of all prime divisors of k, $\mathfrak{S}(k)$ the (finite) set of all supersingular primes of k, as well as (∞)-prime.

This depends wholly on Deuring's complex multiplication theory (cf. **[1]**, **[2]**, **[3]**).

1.2. To construct a certain infinite Galois extension K of k which arises from division of the elliptic curve with (variable) modulus j. The Galois group and ramifications for K/k has been determined by Igusa **[7]**. (It can be obtained also by our method, i.e. by consideration of decomposition of prime divisors, Tchebotareff's density theorem, ζ-functions in §2, etc.) The connection between the decomposition law for prime divisors of k in K and conjugacy classes of Γ (Theorem, property III) is also a consequence of "precise" complex multiplication theory. By this we obtain a one-to-one correspondence between $\mathfrak{P}(\Gamma')$ of congruence subgroups Γ' of Γ and $\mathfrak{P}(k') - \mathfrak{S}(k')$ of some finite extension k' of k in K.

Then Theorem, property III, which states that all supersingular primes of k are decomposed completely in K, is a consequence of §2; namely by calculating ζ-functions of Γ' defined analogous to that of k', we can show that the number of primes of k' which lie on supersingular primes of k is proportional to the volume of G/Γ', i.e. to the group index $[\Gamma' : \Gamma]$, which implies that all supersingular primes are decomposed completely in k.

1.3. "Monodromy problems" are two conjectures that arise from these considerations.

(A) Whether K/k is characterized as the maximum extension of k under given ramification and complete decomposition of supersingular primes, or not.

(B) Whether any subgroup of $\Gamma = \mathrm{SL}(2, Z^{(p)})/\pm 1$ with finite index contains some congruence subgroup, or not.

2.1. By Eichler–Shimura **[4]**, **[12]**, and Kuga's result **[8]**, we shall show that a necessary condition for conjecture (B) is satisfied (weaker stability property for Γ', which is true for more general discrete subgroup of

$$G = \{\mathrm{SL}(2, R) \times \mathrm{SL}(2, Q_p)\}/\pm 1$$

and *not* true for discrete subgroups of $G = \mathrm{SL}(2, Q_p)/\pm 1$; see p. 151).

2.2. Numerical example for Monodromy problems (A), (B).

2.3. Definition, and computation of ζ-functions of Γ' by using spectral decomposition of L^2 (G/Γ'). This can also be done by using Lefschetz' fixed-point theorem (and without spectral decompositions, only outlines).

1. **Frobenius' conjugacy classes.**

1.1. We consider the field of algebraic numbers as subfield of complex number field. Choose any prime factor $\wp$ of p in the former field and identify the residue class field modulo $\wp$ with algebraic closure $\bar{F}_p$ of finite field F_p. We assume in §1 that p is different from 2 or 3.

Let now $\Gamma = \mathrm{SL}(2, Z^{(p)})/\pm 1$ be as in the introduction. ($Z^{(p)}$ is the ring of all rational numbers whose denominators are p powers.) Any element γ of Γ will be called primitive if it has infinite order and if, together with some finite group, it generates its centralizor in Γ. We denote by $\mathfrak{P}(\Gamma)$ the set of all primitive and elliptic (i.e., its eigenvalues are imaginary) conjugacy classes of Γ, where γ and γ^{-1} are identified. Such γ always generate imaginary quadratic fields at which p is decomposed. So, we denote by $\deg(\gamma)$ the positive $\mathfrak{p}$-adic order of γ or γ^{-1}.

Let $\Gamma \subset \mathrm{SL}(2, R)/\pm 1$ (projection) operate on the upper half plane, let $\{\gamma\}$ be in $\mathfrak{P}(\Gamma)$, and let τ_γ be the (unique) fix point of γ in the upper half plane. Then $j(\tau_\gamma)$, where j is 12^3 times the ordinary elliptic modular function, is an algebraic integer, and its residue class mod $\wp$ is merely replaced by its conjugates over F_{p^2} when we choose other representatives of $\{\gamma\}$ (congruence relation). Applying Deuring's complex multiplication theory, (cf. [1], [2], [3]) it is easy to check that this maps $\mathfrak{P}(\Gamma)$ injectively into the set $\mathfrak{P}(k)$ of all prime divisors of the rational function field $k = F_{p^2}(\tilde{j})$, and that the image is $\mathfrak{P}(k)$ minus finite number of primes of degree one; namely (∞) and all supersingular ones.

If $\{\gamma\}$ in $\mathfrak{P}(\Gamma)$ correspond to (j) in $\mathfrak{P}(k)$, their degrees coincide, and the $Z^{(p)}$-order $Q(\gamma) \cap M(2, Z^{(p)})$ of $Q(\gamma)$ is the scalar extension by $Z^{(p)}$ of the endomorphism ring of elliptic curve with modulus j. Two elements of $\mathfrak{P}(\Gamma)$ (resp. $\mathfrak{P}(k)$) will be called equivalent and denoted by $\sim$ when they have the same orders in the above sense. We remark that if we take other choices of the prime factor $\wp$ of p, the above correspondence between $\mathfrak{P}(\Gamma)$ and $\mathfrak{P}(k)$ varies, but it does not change as a correspondence between $\mathfrak{P}(\Gamma)/\sim$ and $\mathfrak{P}(k)/\sim$.

1.2. Let $E_{\tilde{j}}: y^2 = 4x^3 - \tilde{\gamma}_2 x - \tilde{\gamma}_3$;

$$\tilde{\gamma}_2, \tilde{\gamma}_3 \in k, \qquad \tilde{j} = 12^3 \tilde{\gamma}_2^3 (\tilde{\gamma}_2^3 - 27\tilde{\gamma}_3^2)^{-1}$$

be an elliptic curve with modulus $\tilde{j}$, and let $\tilde{K}$ be the field generated over k by x coordinates of all points on $E_{\tilde{j}}$ of finite orders coprime with p. $\tilde{K}$ depends only on $\tilde{j}$ and does not depend on the special choice of $\tilde{\gamma}_2, \tilde{\gamma}_3$ in k. $\tilde{K}$ is an infinite Galois extension of k, and the Galois group $\mathfrak{g}(\tilde{K}/k)$ was determined by Igusa (cf. Igusa [7]).

$$\mathfrak{g}(\tilde{K}/k) \cong \left\{ g \in \prod_{l \neq p} \mathrm{GL}(2, Z_l);\ \det g \in \Pi^2 \right\} / \pm 1$$

where Z_l denotes the ring of l-adic integers, and Π denotes the closure in $\prod_{l \neq p} Z_l^*$ of the infinite cyclic group generated by p.

$$\therefore \quad \mathfrak{g}(\tilde{K}/k) \cong \left\{\prod_{l \neq p} \mathrm{SL}(2, Z_l)\right\}/\pm 1 \times \left\{\pm a \cdot 1 ; a \in \Pi\right\}/\pm 1.$$

The first direct factor corresponds to the subfield $\bar{F}_p(j)$ of $\tilde{K}$. Let K be the subfield of $\tilde{K}$ corresponding to the second direct factor. Then, K is the infinite Galois extension of k without constant field extension such that $\tilde{K} = K \cdot \bar{F}_p$.

THEOREM. *Any subextension k'/k of K/k has the following properties*:

(I) $(j) = (\infty)$ *is tamely ramified*, $(\bar{j}) = (12^3)$ *resp.* (0): *ramified, but ramification degree divides* 2 *resp.* 3. *All other primes are unramified* (*Igusa*).

(II) *Supersingular j are decomposed completely in K/k* (*except possibly when* $j = 12^3$ *or* 0; *in these cases, the inertia groups coincides with the decomposition groups*).

(III) *Let σ be the natural injection*:

$$\sigma : \Gamma \to \left\{\prod_{l \neq p} \mathrm{SL}(2, Z_l) \;/\pm 1\right\} \cong \mathfrak{g}(K/k).$$

For any $\{\gamma\}$ in $\mathfrak{P}(\Gamma)$, the conjugacy class of $\mathfrak{g}(K/k)$ determined by $\sigma\{\gamma\}$ is the Frobenius substitution of the corresponding prime divisor of k.[1]

The last statement implies that if k' is any finite Galois extension of k contained in K, and $\mathfrak{g}'$ the corresponding subgroup of $\mathfrak{g} = \mathfrak{g}(K/k)$, and Γ' the intersection of Γ with $\mathfrak{g}'$ (where Γ is considered as dense subgroup of $\mathfrak{g}$ by the injection of σ), the law of decomposition of $\mathfrak{P}(k)$ in k'/k is described by the order of the corresponding $\{\gamma\}$ in $\mathfrak{P}(\Gamma)$ with respect to Γ'. It is clear that we also have almost one-to-one correspondence between $\mathfrak{P}(k')$ and $\mathfrak{P}(\Gamma')$, and that proposition (II) can be proved if we can count the number of primes in $\mathfrak{P}(k')$ which does not correspond to any conjugacy class in $\mathfrak{P}(\Gamma')$ (cf. §2).

1.3. *Monodromy problems.* (A). *Is K the maximal Galois extension of k satisfying* (I) and (II) *of the previous proposition*? (B). *Is $\mathfrak{g}$ the completion of Γ with respect to all subgroups of Γ with finite indices*? *I.e., does any subgroup of Γ with finite index contain congruence subgroups*?

These two problems seem to be deeply connected with each other, and some reasons suggest that it might not be too reckless to conjecture that they are true, although the corresponding problem for characteristic zero is definitely wrong. One weak reason will be shown in §§2.1, 2.2.

2. Discrete subgroups of $G = \{\mathrm{SL}(2, R) \times \mathrm{SL}(2, k_{\mathfrak{p}})\}/\pm 1$.

2.1. Let $k_{\mathfrak{p}}$ be a p-adic field, $\mathfrak{p} + 2$, let $N_{\mathfrak{p}} = q$, and let G be as above. Let Γ be any discrete subgroup of G with compact quotient space, and whose projection on each factor is injective and dense. Let Γ_0 be the intersection of Γ with $\mathrm{SL}(2, R) \times \mathrm{SL}(2, O_{\mathfrak{p}})$, where $O_{\mathfrak{p}}$ is the ring of p-adic integers. Since Γ can be considered as subgroup of $\mathrm{SL}(2, R)/\pm 1$ (by the projection), it operates on the two dimensional real vector space, hence also on the space V_n of all symmetric tensors of degree n; $n = 0, 2, 4, \ldots$ over that vector space.

[1] For some special choice of $\cong$ which depends on $\mathfrak{P}$.

Let $H^1(\Gamma, V_n)$ be the first cohomology group. Then, we have

PROPOSITION. $H^1(\Gamma, V_n) = \{0\}$. *In particular, the case* $n = 0$ *implies that the abelianized group* $\Gamma/[\Gamma, \Gamma]$ *of* Γ *is finite, and* $n = 2$ *implies that the "infinitesimal deformation" of* Γ *in* SL(2, *R*)*-part is trivial.*

The proof of the proposition is simple.

First, the restriction map: $H^1(\Gamma, V_n) \to H^1(\Gamma_0, V_n)$ is injective. This follows from the fact that Γ_0 is maximal subgroup of $\Gamma(n = 0)$, and that for any γ in Γ, V_n is also irreducible representation space of $\Gamma_0 \cap \gamma^{-1}\Gamma_0\gamma$. (Density theorem for Fuchsian groups by Borel.)

Now, the Hecke ring $R(\Gamma_0, \Gamma)$, which is canonically isomorphic with $R(\mathrm{SL}(2,O_{\mathfrak{p}}), \mathrm{SL}(2, k_{\mathfrak{p}}))$, operates on $H^1(\Gamma_0, V_n)$ as:

$$R(\Gamma_0, \Gamma) \ni \Gamma_0\gamma\Gamma_0 = \sum_{i=1}^{d} \Gamma_0\gamma_i : a(\sigma) \to \sum_{i=1}^{d} a(\gamma_i\sigma\gamma_{\sigma(i)}^{-1})^{\gamma_i}$$

where $\gamma_i\sigma = \sigma'\gamma_{\sigma(i)}$ with $\sigma' \in \Gamma_0$. Obviously, the restriction to $H^1(\Gamma, V_n)$ of this operation coincides with the "degree representation" of $R(\Gamma_0, \Gamma)$, hence it is sufficient to show that

$$\det(\Gamma_0\gamma\Gamma_0 - d) \neq 0$$

holds on $H^1(\Gamma_0, V_n)$ for at least one double coset $\Gamma_0\gamma\Gamma_0$.

On the other hand, $H^1(\Gamma_0, V_n)$ can be identified with the space of cusp forms of weight $n + 2$ with respect to the Fuchsian group Γ_0, the latter being considered as real vector space (cf. **[4]**, **[12]**) and by this identification, the above statement is equivalent with the weakest estimation of the eigenvalues of $\Gamma_0\gamma\Gamma_0$ in the space of cusp forms, which is just the (generalization of) Kuga's result (cf. **[8]**).

If Γ' is a subgroup with finite index of our previous $\mathrm{SL}(2, Z^{(p)})/\pm 1$, G/Γ' is no longer compact, but together with the knowledge of parabolic elements of such Γ', we can see easily that the abelianized groups of such Γ' are also finite. This is a necessary condition for the validity of "Monodromy problem" (B).

2.2. The following remark seems somewhat noteworthy. When Γ' corresponds to some subfield k' of K in §1, what more precise arguments show is just the fact that the group index $(\Gamma' : [\Gamma', \Gamma'])$ does not exceed the degree of the field extension $[k'' : k']$, where k'' is (one of the) maximal abelian extension of k', without constant field extension, satisfying only the ramification conditions (I). For example, if we take Γ' as congruence subgroup modulo 2, the analogue of so-called λ-group, the previous argument shows that $(\Gamma' : [\Gamma', \Gamma'])$ does not exceed $(p^2 - 1)^2$; on the other hand, if the conjecture (A) (resp. (B)) is true, the degree of maximal abelian extension over k' satisfying (I) and (II) resp. group index $(\Gamma' : [\Gamma'\Gamma'])$ must be $3{\cdot}2^6$. It is satisfied by number of beginning p's.

2.3. *ζ-functions.* Let us go back to the situations stated at the beginning of §2. For such Γ the definition of $\mathfrak{P}(\Gamma)$—set of all elliptic, primitive conjugate classes of Γ— and of degrees stated in §1 also make sense. We assume moreover that

$$\text{if } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ is in } \Gamma, \text{ then } \begin{pmatrix} a & -b \\ -c & d \end{pmatrix} \text{ is also.}$$

Define

$$Z_\Gamma(u) = \prod_{\mathfrak{p} \in \mathfrak{P}(\Gamma)} (1 - u^{\deg \mathfrak{p}})^{-1}.$$

It is analogous in the idea to Selberg's, and in the form to congruence ζ functions. For evaluating such $Z_\Gamma(u)$, we learned from Selberg that the decomposition of $L^2(G/\Gamma)$ plays an essential role. Moreover, Gelfand and Graev established the theory of unitary representations of SL(2, $k_\mathfrak{p}$), and also we can make use of the fact that each irreducible unitary representation of our G decomposes into the tensor product of that of each factor. (The last statement is a special case of more general theorem, which I learned from R. Godement.)

By using these, we can evaluate our $Z_\Gamma(u)$. Namely;

$$Z_\Gamma(u) \doteq \frac{(1-u)^m \prod_{i=1}^{g} (1-\alpha_i u)(1-\beta_i u)}{1-q^2 u}, \quad \alpha_i \beta_i = q^2 \quad (1 \leqq i \leqq g).$$

where g is the genus of the Fuchsian group Γ_0 defined previously, and m is the multiplicity of the tensor product $\rho \otimes \sigma$ in $L^2(G/\Gamma)$ where ρ is the first member of the discrete series for SL(2, R) and σ, the so-called "special representation" of SL(2, $k_\mathfrak{p}$) (cf. [6]). Note that the special representation is not class one with respect to SL(2, $O_\mathfrak{p}$). If we put α_i, $\beta_i = q^{1 \pm s_i}$ $(1 \leqq i \leqq g)$, $q^{1 \pm s_i}$ are the parameters of the continuous series for SL(2, $k_\mathfrak{p}$) that are class one, and whose tensor product with ρ is contained in $L^2(G/\Gamma)$.

It shows that $Z_\Gamma(u)$ is different (in form) from congruence ζ functions by the factor $(1-u)^{m+1}$. This seems to suggest that if it is possible to construct an algebraic curve k over F_{p^2} out of Γ, by reduction mod $\mathfrak{p}$ of the upper half plane divided by Γ_0, so that the fix points by elements of Γ reduce to algebraic points, $\mathfrak{P}(k)$ must have $m + 1$ *more elements of degree one than* $\mathfrak{P}(\Gamma)$—decomposition primes?

Exact value of m is simple when Γ has no element of finite order. In that case,

$$m = (q-1)(g-1) - 1.$$

This shows that $m + 1$ is proportional to the volume of G/Γ. If Γ is a congruence subgroup of SL(2, $Z^{(p)}$)/±1, G/Γ is no longer compact, but by the exact knowledge of parabolic elements we can show that $m + 1$ is proportional to the volume of G/Γ, in this case too. This, together with the remark at the beginning of this note, proves Theorem, property II of §1.

References

1. M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper,* Abh. Math. Sem. Hansischen Univ. **14** (1941), 197–272.

2. ———, *Invarienten und Normalformen elliptischer Funktionenkörper,* Math. Z. **47** (1940), pp. 47–56.

3. ———, *Teilbarkeitseigenschaften der singulären Moduln der elliptischen Funktionen und Diskriminante der Klassengleichung,* Comm. Math. Helv. **19** (1947), 74–82.

4. M. Eichler, *Eine Verallgemeinerung der Abelschen Integrale,* Math. Z. **67** (1957), 267–298.

5. ———, *Quadratische Formen und Modulfunktionen,* Acta Arith. **4** (1958), 217–239.

6. I. M. Gelfand and M. I. Graev, *Representations of the group of second-order matrices with elements in a locally compact field and special functions on locally compact fields,* Uspehi Mat. Nauk **18** (1963), 29–99; English transl., Russian Math. Surveys **18** (1963), pp. 29–99.

7. J. Igusa, *Fibre systems of Jacobian varieties.* I, III, Amer. J. Math. **78** (1956), 171–191, **81** (1959), 453–476.

8. M. Kuga, *On a uniformity of distribution of positive O-cycles and the eigenvalues of Hecke's operators.* I, II, Coll. Gen. Ed. Sci. Paper, Univ. Tokyo **10** (1960), 1–16, 171–186.

9. ———, *Hecke's polynomial as a generalized congruence Artin L-function,* Proc. Sympos. Pure Math., vol. 9, Amer. Math. Soc., Providence, R. I., 1966, pp. 333–347.

10. A. Selberg, *Harmonic analysis and discrete groups in weakly symmetric Riemannian spaces with applications to Dirichlet,* J. Indian Math. Soc. N.S. **20,** (1956) 47–87.

11. G. Shimura, *Correspondances modulaires et les fonctions ζ de courbes algébriques,* J. Math. Soc. Japan **10** (1958), 1–28.

12. ———, *Sur les intégrales attachées aux formes automorphes,* J. Math. Soc. Japan **11** (1959), 291–311.

Discrete Subgroups of PL$(2, k_{\wp})$

BY

YASUTAKA IHARA

Here, we shall deal with torsion-free discrete subgroups Γ of $G = \mathrm{PL}(2, k_{\wp})$ with compact quotient spaces ($k_{\wp} = \wp$-adic fields).

We begin with the structure theorem for such Γ, which states that they are isomorphic to *free* groups with a finite number of generators.[1] Then, by making use of special free generators of Γ, we shall compute (algebraically) ζ-functions of Γ, which are defined as analogues of Selberg's ζ-functions, in $\wp$-adic cases. This, in particular, gives a relation between the number of generators of Γ and the multiplicity of certain irreducible representation of G in $L^2(G/\Gamma)$.

Finally, we shall show by example that there exists such Γ that

(i) it is commensurable with an arithmetically defined group, and that

(ii) $L^2(G/\Gamma)$ contains supplementary series.

For proofs of theorems in this note, see **[6]** which is to appear.

Notations and conventions

K: either $\wp$-adic number field or field of power series over finite constant field.

$\mathcal{O}$: the ring of integers of K.

K^* (resp. $\mathcal{O}^*$): multiplicative group of inversible elements of K (resp. $\mathcal{O}$).

$\wp$: the maximal ideal of $\mathcal{O}$.

$q = N\wp$: number of elements of the residue field $\mathcal{O}/\wp$.

G: $\mathrm{PL}(2, K) = \mathrm{GL}(2, K)/K^*$.

U: $\mathrm{PL}(2, \mathcal{O}) = \mathrm{GL}(2, O/O^* \subset G$.

For any $a, b, c, \cdots, \in K$, $(a, b, c, \cdots)$ will denote the $\mathcal{O}$-ideal generated by $a, b, c, \cdots$.

For any finite set S, $|S|$ will denote its cardinal number.

The summation symbol Σ over some subsets of a set implies disjoint union.

1. **The structure of** Γ. Here, we shall state a structure theorem for Γ. As for the proof, and for the method for construction of all such Γ, see **[6]**.

THEOREM I. *Let Γ be a torsion-free discrete subgroup of $G = \mathrm{PL}(2, K)$ with compact quotient space. Then Γ is isomorphic to the free group with $(q - 1)h/2 + 1$ generators, where $h = |U\backslash G/\Gamma|$, $U = \mathrm{PL}(2, \mathcal{O})$, and $q = N\wp$.*

We shall state the theorem in a more general form, and for that purpose, we need some definitions. By $(G', U'; \pi_0, \pi_1, \pi_2, \cdots, \pi_q)$-type, we mean any triple of

[1] This implies, in particular, that any arithmetically defined Γ contains a subgroup with finite index which does not contain any congruence subgroups (cf. §3).

abstract group G', its subgroup U' and a finite subset $\{\pi_0, \pi_1, \cdots, \pi_q\}$ of G' satisfying the following conditions.

(1) $G'_1 = \sum_{i=0}^{q} U'\pi_i$ is a disjoint union, and $G_1'^{-1} = G'_1$.

(2) G' has the disjoint union decomposition:

$$G' = \sum_{l=0}^{\infty} G'_l$$

where $G'_0 = U'$ and

$$G'_l = \sum U'\pi_{i_l} \cdots \pi_{i_1} \qquad (l \geqq 1),$$

the (disjoint) union being taken over all $(i_l, \cdots, i_1)$ such that $\pi_{i_{n+1}}\pi_{i_n} \notin U'$ for all $n (1 \leqq n \leqq l - 1)$.

From (1), it follows that for each suffix $i\,(0 \leqq i \leqq q)$, there exists one and only one suffix $j = j(i)(0 \leqq j \leqq q)$ such that $\pi_j\pi_i \in U'$, hence G'_l consists of $q^{l-1}(q + 1)$ left U' cosets. It is also easy to check that $G'_lU' = G'_l = G_l'^{-1}$ for all $l \geqq 0$. Now let $\Pi_l\,(l \geqq 0)$ be the set of all elements of the form $\pi_{i_l} \cdots \pi_{i_1}$ with $\pi_{i_{n+1}}\pi_{i_n} \notin U'$ for all n $(1 \leqq n \leqq l - 1)$, and put $\Pi = \sum_{l=0}^{\infty} \Pi_l$. Thus Π_l (resp. Π) is a complete set of representatives of $U'\backslash G'_l$ (resp. $U'\backslash G'$).

We shall introduce a lexicographic ordering in Π as follows:

(1) $x \in \Pi_l, \quad y \in \Pi_{l'}, \quad l < l' \Rightarrow x < y.$

(2) $x, y \in \Pi_l, \quad x = \pi_{i_l} \cdots \pi_{i_1}, \quad y = \pi_{j_l} \cdots \pi_{j_1}, \quad i_1 = j_1, \cdots, i_{m-1} = j_{m-1}, i_m < j_m$ for some $m \geqq 0 \Rightarrow x < y$.

Now, we can state:

THEOREM I′. *The notations being as above, let Γ' be a torsion-free subgroup of G' such that*

(1) $\Gamma' \cap x^{-1}U'x = \{1\}$ *for any* $x \in G'$.

(2) $|U'\backslash G'/\Gamma'| < \infty$.

Then, Γ' is isomorphic to the free group with $(q - 1)h/_2 + 1$ generators, where $h = |U'\backslash G'/\Gamma'|$. More precisely, let $x_1, x_2, \cdots x_h \in \Pi$ be determined by

$$G' = \Sigma U'x_i\Gamma', x_i = \mathrm{Min}(y; y \in U'x\Gamma' \cap \Pi)$$

and $1 = x_1 < \cdots < x_h$, and put $S_{ij} = x_i^{-1}G'_1x_j \cap \Gamma'$ $(1 \leqq i, j \leqq h)$, $S_{ii} = T_i \cup T_i^{-1}$ with $T_i \cap T_i^{-1} = \phi$. Then for each $j > 1$, there exists a unique suffix $i = i(j) < j$ such that $S_{ij} \ni 1$.

Now, S_{ij} $(1 \leqq i < j \leqq h, i \neq i(j))$, $S_{i(j)j} - \{1\}$ $(2 \leqq j \leqq h)$, and $T_i (1 \leqq i \leqq h)$ will be a set of free generators of Γ'.

REMARK. It is easy to check that $S_{ij}^{-1} = S_{ji}, \sum_{i=1}^{h} |S_{ij}| = q + 1$ *for each* $j\,(1 \leqq j \leqq h)$.

Theorem I′ ⇒ Theorem I. Take $G' = G, U' = U, \Gamma' = \Gamma$, and let $G_l\,(l \geqq 0)$ be the totality of elements of G which are represented modulo K^* by matrices

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

such that $a, b, c, d \in \mathcal{O}$, $(a, b, c, d) = \mathcal{O}$, and $(ad - bc)\mathcal{O} = \wp^l$. Let $\pi_0, \pi_1, \cdots, \pi_q$ be any representative of $U \backslash G_1$. Then, $(G, U; \pi_0, \pi_1, \cdots, \pi_q$ and Γ in Theorem I) satisfies the assumptions of Theorem I′, and $G'_l = G_l$ for $l = 0, 1, 2, \cdots$. The proof of Theorem I′ will be given in **[6]** and hence will be omitted here.

2. **ζ-Functions attached to Γ.** Let Γ be again a torsion-free discrete subgroup of $G = \mathrm{PL}(2, K)$ with compact quotient space. Then, for any element $\gamma \neq 1$ of Γ, the centralizer in Γ of γ is a free cyclic group (Γ is torsion-free). We shall call γ, or conjugacy class $\{\gamma\}$ in Γ containing γ, "primitive" if γ generates its centralizer in Γ. Let $\lambda_\gamma, \lambda'_\gamma$ be the eigenvalues of a representative modulo K^* of $\gamma \neq 1$ in Γ. Then $\lambda_\gamma, \lambda'_\gamma \in K$. Put $\deg\{\gamma\} = |\mathrm{ord}_\wp(\lambda_\gamma \lambda'^{-1}_\gamma)|$, where $\mathrm{ord}\,\wp$ denotes the normalized additive valuation of K.

Let $\mathfrak{P}(\Gamma)$ be the set of all primitive (non-identical) conjugacy classes of Γ, and define

$$Z_\Gamma(u) = \prod_{\{\gamma\} \in \mathfrak{P}(\Gamma)} (1 - u^{\deg\{\gamma\}})^{-1},$$

This again[2] is an analogue, in idea, of Selberg's ζ-functions and, in form, of congruence ζ-functions. With Theorem I′ in hand, it is not difficult to compute this algebraically. The result is as follows. Put $G = \sum_{i=1}^h Ux_i\Gamma$, where

$$h = |U \backslash G/\Gamma|,$$

$x_1, \cdots, x_h$ being any representatives of $|U \backslash G/\Gamma|$. Put

$$A = ((a_{ij})), \qquad a_{ij} = |x_i^{-1} G_1 x_j \cap \Gamma| \quad (1 \leqq i, j \leqq h).$$

Then $\sum_{j=1}^h a_{ij} = q + 1$ for any $i (1 \leqq i \leqq h)$; hence we can put $A \approx (q + 1) \oplus A_0$ with $h - 1 \times h - 1$ matrix A_0, where $\approx$ implies conjugacy of matrices.

Then we have:

THEOREM II. *The notation being as above, we have*

(1) $Z_\Gamma(u) = \{(1 - u)(1 - qu)(1 - u^2)^{g-1} \det(1 - A_0 u + qu^2)\}^{-1}$
where $g = (q - 1)h/_2 + 1$.

Now we shall briefly mention the connections with spectral decompositions of $L^2(G/\Gamma)$. Let

$$\Delta : G \ni x \to \det x \in K^*/K^{*2}$$

be the homomorphism given by determinant of $\mathrm{GL}(2, K)$. For the sake of simplicity, let us consider such Γ (with the condition of Theorem I) that $\Delta(\Gamma) = \pi K^{*2}/K^{*2}$ with some prime element π of K. Put $G^1 = \mathrm{PSL}(2, K) \subset G, \Gamma^1 = G^1 \cap \Gamma$ so that $[\Gamma : \Gamma^1] = 2$, and consider the connection between $Z_{\Gamma^2}(u)$ and the spectral decomposition of $L^2(G^1/\Gamma^1)$.

It is easy to see that $Z_{\Gamma^1}(u) = Z_\Gamma(u) Z_\Gamma(-u)$, hence we have

$$(1'): \qquad Z_{\Gamma^1}(u) = \left\{(1 - v)^{g_1}(1 - q^2 v) \prod_{i=1}^{h-1} (1 - \omega_i^2 v)(1 - \omega_i^{*2} v)\right\}^{-1}.$$

[2] Cf. pp. 268–270, §2.

where $Z_\Gamma(u)$ is as in (1), $v = u^2$, $g_1 = (q-1)h + 1$, and

$$\det(1 - A_0 u + qu^2) = \prod_{i=1}^{h-1}(1 - \omega_i u)(1 - \omega_i^* u), \qquad \omega_i\omega_i^* = q\,(1 \leqq i \leqq h-1).$$

By taking log of both sides of (1) and by comparing corresponding coefficients of v, (1′) is equivalent with

$$(1''): \qquad \tfrac{1}{2} \sum_{\substack{\{\gamma\}\in\wp(\Gamma^1)\\ \deg\{\gamma\}|2n}} \deg\{\gamma\} = q^{2n} + \sum_{i=1}^{h-1} (\omega_i^{2n} + \omega_i^{*2n}) + g_1$$

for any $n = 1, 2, 3, \cdots$.

First, it is well known in spherical function theory (and also easy to see) that if we put $\omega_i = q^{\frac{1}{2}+s_i}$, $\omega_i^* = q^{\frac{1}{2}-s_i}\,(1 \leqq i \leqq h-1)$, then the characters π_i of K^* defined by

$$\pi_i\colon K^* \ni x \to |x|_\wp^{2s_i} \qquad (1 \leqq i \leqq h-1, |x|_\wp = q^{-\operatorname{ord}_\wp x})$$

are precisely those characters of K^* that parametrize class-one irreducible unitary representations of G^1 contained in $L^2(G^1/\Gamma^1)$ (denoted by T_{π_i} in **[5]**).

Secondly, (1″) can also be obtained by trace-formulae for spectral decomposition of $L^2(G^1/\Gamma^1)$, where instead of g_1, the multiplicity in $L^2(G^1/\Gamma^1)$ of the "special representation" (cf. **[5]**) appears. Thus we have

$$g_1 = \textit{the multiplicity of special representation of } G^1 \textit{ in } L^2(G^1/\Gamma^1).$$

(This is, of course, an analogue of the fact that the genus of Fuchsian group $H \subset \mathrm{SL}(2, R)$ is equal to the multiplicity in $L^2(\mathrm{SL}(2, R)/H)$ of the first member of discrete series of $\mathrm{SL}(2, R)$.)

Finally, a well known remark:

(R): $L^2(G^1/\Gamma^1)$ does not contain supplementary series $\leftrightarrow$ All s_i $(1 \leqq i \leqq h-1)$ are purely imaginary $\leftrightarrow$ $|\alpha_i| \leqq 2q^{\frac{1}{2}}$ $(1 \leqq i \leqq h-1)$ $\leftrightarrow$ left hand side of (1″) $= q^{2n} + O(q^n)$ as $n \to \infty$, $\alpha_i\,(1 \leqq i \leqq h-1)$ being the set of eigenvalues of A_0. (They are real because ${}^tA = A = \bar{A}$.)

In §4, we give an example which shows that it is not always the case.

3. **Arithmetic Γ and congruence ζ-functions.** Arithmetic examples of Γ (which are more or less known) will be provided by the totally definite quarternion algebra D over the totally real algebraic number field k.

Let $\wp$ be a prime ideal of k unramified at D; i.e.

$$D \otimes_k k_\wp \cong M(2, k_\wp).$$

Put $K = k_\wp$, and let Γ be the unit group, modulo center, of any $\mathcal{O}^{(\wp)}$-order of D, where $\mathcal{O}^{(\wp)}$ is the ring of integers of k except at $\wp$ (i.e. the ring of all elements of k which are integral except at $\wp$). Then by the above isomorphism, Γ can be regarded as a discrete subgroup of $G = \mathrm{PL}(2, K)$ with compact quotient space.

In any case by taking suitable suborders, the corresponding subgroup of Γ will be torsion-free.

In particular, if $k = Q$ (the rational number field) and D has a prime discriminant $l \neq p = \wp$, and if we take maximal $Z^{(\wp)}$-order of D, then due to M. Eichler, [4], the main part of our $Z_\Gamma(u)$, namely

$$\det(1 - A_0u + qu^2), \tag{2}$$

is equal to the congruence ζ-function of an algebraic curve over Z/pZ. More precisely, by his *Zahlentheorie der Quaternionenalgebren*, the left-hand side of (1″) can be expressed by class numbers of those Z-orders of imaginary quadratic fields $\subset D$, that contain elements of norm p^n. By this, and by precise complex multiplication theory of elliptic curves (Deuring), it can be shown that (2) is equal to the numerator of congruence ζ-function of the complete nonsingular model of the elliptic transformation equation of degree l over Z/pZ.

Thus, in particular, (R) is true in this case (Riemann hypothesis for congruence ζ-functions by A. Weil).

Finally a simple remark: Let Γ be an arithmetically defined group in the above sense. We can take a suitable congruence subgroup Γ_0 which is torsion-free. Thus Γ_0 is a free group; hence $\Gamma_0/[\Gamma_0, \Gamma_0]$ is infinite, $[\Gamma_0, \Gamma_0]$ being the commutator subgroup. Let Γ_1 be a subgroup of Γ_0 with index n and containing $[\Gamma_0, \Gamma_0]$. By the structure of local unit groups, it follows that Γ_1 does not contain any congruence subgroup of Γ_0, hence of Γ, if n is sufficiently large.

4. **Other examples, failure of** (R). We begin with a simple remark on construction of all torsion-free Γ with $h = 1$ (among those are arithmetic ones in the sense of previous section), and then show that they (always) contain subgroups with finite indices for which (R) fails.

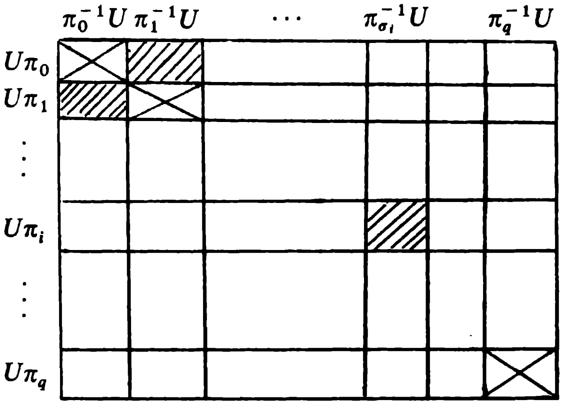
PROPOSITION. *Let G_1 (not $G^1 =$ PSL(2, K)) be as in §1, and assume that $\wp + 2$, hence $|U\backslash G_1| = q + 1$ is even. Put*

$$G_1 = \sum_{i=0}^{q} U\pi_i.$$

Let σ be any substitution on the set of indices $\{0, 1, 2, \cdots, q\}$ such that $\sigma^2 = 1$ and $\sigma(i) \neq i$ for all i $(1 \leqq i \leqq q)$. Choose any element x_i from $U\pi_i \cap \pi_{\sigma i}^{-1}U$ for each i $(0 \leqq i \leqq q)$ in such a way that $x_{\sigma i} = x_i^{-1}$ for all i $(0 \leqq i \leqq q)$. Put

$$X = \{x_0, x_1, \cdots, x_q\} = Y \cup Y^{-1}, Y \cap Y^{-1} = \phi.$$

Then Y generates a torsion-free discrete subgroup Γ of $G =$ PL(2, K) such that $G = U\Gamma$ (which is a free group over Y), and conversely, all such Γ can be constructed in this manner.



PROOF. $G, U, x_0, \cdots, x_q$ satisfies the properties of $(G, U, x_0, \cdots, x_q)$-type. [cf. §1].

Now let Γ be such; hence a free group over

$$Y = \{y_1, \cdots, y_d\}, \qquad d = (q+1)/2,$$

where $y_1, \cdots, y_d$, are as in the proposition; so,

$$G_1 \cap \Gamma = Y \cup Y^{-1}.$$

For any element γ of Γ, and for any suffix $i\,(1 \leqq i \leqq d)$, let $a_i(\gamma)$ be the sum of exponents of y_i in the expression of word γ by $y_1, \cdots, y_d$. For any nonempty subset I of $1, 2, \cdots, d$, let Γ_I be the subgroup of Γ defined by

$$\Gamma_I = \left\{\gamma \in \Gamma \,\middle|\, \sum_{i \in I} a_i(\gamma) \equiv 0 \,(\mathrm{mod}\, 2)\right\}.$$

Thus, $[\Gamma : \Gamma_I] = 2$.

It is easy to see that if $I \neq \{1, 2, \cdots, d\}$, then $\Delta(\Gamma_I) = \pi K^{*2}/K^{*2}$ for prime element $\pi = y_j\,(j \notin I)$ of K (condition in §2), and we have

$$G = U\Gamma_I + Uy_j\Gamma_I$$

by any $j \notin I$. So, the matrix $A = ((a_{ij}))$ defined in §2 will be

$$A = \begin{pmatrix} |\Gamma_I \cap G_1| & |\Gamma_I y_j \cap G_1| \\ |y_j^{-1}\Gamma_I \cap G_1| & |y_j^{-1}\Gamma_I y_j \cap G_1| \end{pmatrix} = \begin{pmatrix} 2r & q+1-2r \\ q+1-2r & 2r \end{pmatrix}$$

where $|I| = d - r, (1 \leqq r \leqq d = (q+1)/2)$.

Since the eigenvalues of A are $q+1$ and $4r - q - 1$, by the remark at the end of §2, (R) is true for $\Gamma_I^1 = \Gamma_I \cap G^1$ ($G^1 = \mathrm{PSL}(2, K)$) if and only if

$$\text{(R}')\qquad |4r - q - 1| \leqq 2q^{\frac{1}{2}}.$$

Thus (R′) cannot be true for $r = 1$, $q > 6$.

Finally, let D be the definite quaternion algebra over Q with discriminant 13. Let p be any prime $= 13$ and let Γ be the unit group modulo centre of (unique) maximal $Z^{(p)}$-order of D, where $Z^{(p)}$ is the ring of rational integers except at p. Since the class number of D is one, we have $h = 1$, and since D does not contain $Q(\sqrt{(-1)})$, $Q(\sqrt{-3}))$, Γ is torsion-free. Thus, if $p > 6$, the above argument shows that $\Gamma^1 = \Gamma \cap G^1$ has a subgroup with index 2 for which (R) fails.

References

1. M. Deuring, *Die Typen dek Multiplikatorenringe elliptischer Funktionenköper*, Abh. Math. Sem. Hansischen Univ. **14** (1941), 197–272.

2. ———, *Invarianten und Normalformen elliptischer Funktionenkörper*, Math. Z. **47** (1941), 47–56.

3. ———, *Teilbarkeitseigenschaften der singulären Moduln der elliptischen Funktionen und die Diskriminante der Klassengleichung*, Comment. Math. Helv. **19** (1946), 74–82.

4. M. Eichler, *Zur Zahlentheorie der Quaternionenalgebren*, J. Reine U. Angew. **195** (1956), 127–151.

5. Gelfand–Graev, *Representations of a group of matrices of the second order with elements from a locally compact field, etc.*, Uspehi Mat. Nauk **18** (1963) no. 4 (112), 29–99 = Russian Math. Surveys **18** (1963), 29–99.

6. Y. Ihara, *On discrete subgroups of $\wp$-adic projective linear groups of degree two*, (to appear).

7. I. Mautner, *Spherical functions over $\wp$-adic fields*, Amer. J. Math. **86** (1964).

8. I. Satake, *Theory of spherical functions on reductive algebraic groups over $\wp$-adic fields*, Paris, Inst. Hautes Études Sci. Publ. Math. **18** (1963), 229–293.

9. T. Tamagawa, *On discrete subgroups of $\wp$-adic groups*, (to appear).

IV. Bounded Symmetric Domains, Holomorphic Automorphic Forms, Moduli

On Compactifications of Orbit Spaces of Arithmetic Discontinuous Groups Acting on Bounded Symmetric Domains

BY

WALTER L. BAILY, JR.

1. **Examples.** In order to explain the nature of the methods and results of the work of Borel and myself, I wish first to give some examples of cases which may serve as motivation for our efforts.

A. Let G be the group $\mathrm{SL}(2, \boldsymbol{R})$ and Γ, the group $\mathrm{SL}(2, \boldsymbol{Z}) = G_{\boldsymbol{Z}}$. As is well known, G operates on the upper half plane $H = \{z = x + iy | y > 0\}$ by linear fractional transformations: $z \to (az + b)/(cz + d)$, and it is easy to see that Γ is a discontinuous transformation group operating on H. Hence, $\Gamma\backslash H$ is a locally compact Hausdorff, which in fact carries the complex structure of a Riemann surface. It is well known and easy to prove that this Riemann surface V is just the complex plane. V may be enlarged to a compact Riemann surface by forming its one-point compactification and introducing a suitable uniformizing parameter in a neighborhood of the new point ∞. For our purposes it will be better to construct this new Riemann surface V^* in the following way: we form the union H^* of H, $\boldsymbol{Q}$ (the set of rational points on the real axis), and the point ∞; we supply H^* with the topology in which a base of the neighborhoods of ∞ are the strips $N_\lambda = \infty \cup \{z = x + iy | y > \lambda\}$ for $\lambda > 0$, in which a base of neighborhoods of any $a/c \in \boldsymbol{Q}$ are the images of the sets N_λ under some

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \boldsymbol{Z}),$$

and in which a base of neighborhoods of any $z \in H$ is a base of neighborhoods in the usual topology of H. Then Γ operates on H^*, and $V^* = \Gamma\backslash H^*$ is a compact Hausdorff space. Let $p: H^* \to V^*$ be the natural map. Of course, $\boldsymbol{Q} \cup \infty$ is a single orbit $\overline{\infty}$ of Γ in H^*. V^* is made into a Riemann surface on which V is an open submanifold by taking as uniformizing parameter τ on $\bar{N}_1 = p(N_1)$ the function which coincides with the function induced by $e^{2\pi iz}$ on $\bar{N}_1 - \overline{\infty}$ and such that $\tau(\overline{\infty}) = 0$.

B. Let $G = \mathrm{Sp}(n, \boldsymbol{R})$, $\Gamma = \mathrm{Sp}(n, \boldsymbol{Z})$. Put $H_n = \{Z | {}^tZ = Z, Z = X + iY, Y \text{ positive definite}\}$. G operates on H_n by : If

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in G,$$

A, B, C, D being $n \times n$ real matrices, one defines

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} Z = (AZ + B)(CZ + D)^{-1}.$$

Then Γ operates discontinuously on H_n and $V_n = \Gamma \backslash H_n$ is a complex analytic space (with singularities). According to [20], the points of V_n are in natural one-to-one correspondence with the isomorphism classes of normally polarized Abelian varieties. (Normally polarized means in the notation of [20] that e is the $n \times n$ identity matrix.) Satake [18] has constructed a compactification V_n^* of V_n by supplying the set-theoretic union $V_n^* = V_n \cup V_{n-1} \cup \cdots \cup V_0$ (where V_0 is a point) with a certain topology. The elemental idea in this construction is essentially the same as that in the construction of V^* in A (above), but of course the details are much more complicated and depend on nontrivial aspects of the Minkowski reduction theory [7]. It has been proved [2] that V_n^* is, with a certain ringed structure, a normal complex analytic space, and in [2] it has also been proved that this compact, normal analytic space has a realization as a normal projective algebraic variety. It was proved in [10] that a projective imbedding of V_n^* as a normal variety may be obtained by means of automorphic forms. By combining these results with some facts from the theory of theta-functions, it was possible [3] to show that V_n^* has a projective model defined over the rational number field $\boldsymbol{Q}$ such that if x is a point of this model lying on (the part corresponding to) V_n, then $\boldsymbol{Q}(x)$ is the field of moduli of the isomorphism class of normally polarized Abelian varieties corresponding to x. More generally, by construction of compactifications of the orbit spaces in H_n of the groups Γ_e (in the notation of [20]), one may obtain similar results about the fields of moduli of Abelian varieties with polarizations which may not be normal.

C. Let k be a totally real number field and let $\mathfrak{o}$ be its ring of integers. Denote by $\sigma_1, \cdots, \sigma_m$ the distinct isomorphisms of k into $\boldsymbol{R}(m = [k:\boldsymbol{Q}])$. We let $G = \mathrm{Sp}(n, \boldsymbol{R}) \times \cdots \times \mathrm{Sp}(n, \boldsymbol{R})$ (m factors), $\Gamma' = \mathrm{Sp}(n, o)$, and define an isomorphism ϕ of Γ' into G by $\phi(g) = (g^{\sigma_1}, \cdots, g^{\sigma_m})$. Put $\Gamma = \phi(\Gamma')$. Then Γ operates discontinuously on H_n^m, and Γ is called the Hilbert-Siegel modular group. With respect to a suitable system of coordinates, G modulo its center becomes a $\boldsymbol{Q}$-simple, $\boldsymbol{Q}$-algebraic group, and Γ is then just $G_{\boldsymbol{Z}}$ ($\boldsymbol{Q}$-simple means "having no proper normal subgroups defined over $\boldsymbol{Q}$"). $\Gamma \backslash H_n^m = V_{n,m}$ has a meaning for the theory of moduli of Abelian varieties similar to that of V_n, except that now, in addition to a polarization, one must also consider an endomorphism ring containing, via some natural injection, some order in k.

D. Let $k = \boldsymbol{Q}(\sqrt{-d})$ be an imaginary quadratic number field, let G' be the group of all $2n \times 2n$ complex matrices M such that ${}^t\overline{M}HM = H$, where

$$H = \begin{pmatrix} 0 & E \\ -E & 0 \end{pmatrix},$$

and let Γ' be the group $G'_{\mathfrak{o}}$, where $\mathfrak{o}$ is the ring of integers in k. To each $M \in G'$, we assign the matrix

$$\phi_d(M) = \tfrac{1}{2}\begin{pmatrix} M + \bar{M} & \sqrt{(-d)}(M - \bar{M}) \\ \dfrac{1}{\sqrt{(-d)}}(M - \bar{M}) & M + \bar{M} \end{pmatrix} \in M_{4n}(\boldsymbol{R}).$$

Then $G = \phi_d(G')$ is a real algebraic subgroup of the symplectic group of

$$\begin{pmatrix} \begin{matrix} 0 & E \\ -E & 0 \end{matrix} & 0 \\ 0 & d\begin{pmatrix} 0 & E \\ -E & 0 \end{pmatrix} \end{pmatrix},$$

G is defined over $\boldsymbol{Q}$, and $\Gamma = \phi_d(\Gamma')$ is easily seen to be commensurable with $G_{\boldsymbol{Z}}$. The group G' is usually known as the Hermitian modular group; it operates by:

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}(Z) = (AZ + B)(CZ + D)^{-1}$$

on the symmetric space of complex $n \times n$ matrices Z such that $i^{-1}(Z - {}^t\bar{Z}) > 0$, and has been investigated under the name of the "Hermitian modular group" by, among others, Hel Braun [9] and Klingen [11]. The trivial calculations above show that this pair, consisting of a symmetric space and an arithmetrically defined discontinuous group acting on it, (together with those discussed in A, B, and C) is a special case of what we are about to discuss.

2. **The general problem.** In this section we let our transformation groups act on the right, as opposed to the convention in §1 where, for the sake of compatibility with classical notation, we let them act on the left.

Let G be a semisimple, connected, linear algebraic $\boldsymbol{Q}$-group. In this section we denote by $G_{\boldsymbol{R}}$ the group of real points of G and let $X = K\backslash G_{\boldsymbol{R}}^0$ be a symmetric space such that $G_{\boldsymbol{R}}^0$ is isogeneous tc the maximal, connected group of isometries of X; unless $G_{\boldsymbol{R}}^0$ is of noncompact type, we do not necessarily assume K to be maximal compact in $G_{\boldsymbol{R}}^0$. We now assume X to be Hermitian symmetric. Let Γ be a subgroup of $G_{\boldsymbol{R}}^0$ commensurable with $G_{\boldsymbol{Z}}$. (More generally, we may take Γ to be any subgroup of the maximal group of complex analytic automorphisms of X commensurable with $G_{\boldsymbol{Z}}$.) Our general problem consists in showing that $V = X/\Gamma$ may be realized, by a canonical procedure, as a Zariski-open subset of a projective, normal algebraic variety V^*. We begin by legitimating some simplifying assumptions. First, we may assume G to be centerless, because if Z is the center of G, then G is $\boldsymbol{Q}$-isogeneous to $G/Z = G'$, and the image of Γ in G' will, by results of [8], be commensurable with $G'_{\boldsymbol{Z}}$. If G is centerless, then G is the direct product of its absolutely simple factors, and the latter are all defined over some Galois extension k of $\boldsymbol{Q}$. Grouping together those absolutely simple factors which are conjugate (over $\boldsymbol{Q}$), we may write G as the direct product of $\boldsymbol{Q}$-simple factors:

$$G = G_1 \cdot \cdots \cdot G_m.$$

Of course, $G_{\boldsymbol{R}} = G_{1\boldsymbol{R}} \cdot \cdots \cdot G_{m\boldsymbol{R}}$ and $G_{\boldsymbol{Z}}$ is commensurable with $G_{1\boldsymbol{Z}} \cdot \cdots \cdot G_{m\boldsymbol{Z}}$; moreover, X is then the product of $X_1, \cdots, X_m$, where X_i is a Hermitian symmetric space associated to $G^0_{i\boldsymbol{R}}$. Hence, we may also assume G to be $\boldsymbol{Q}$-simple. Assuming this, there exists a totally real number field k such that if $G^{(1)}, \cdots, G^{(m)}$ are the absolutely simple factors of G and if $\sigma_1, \cdots, \sigma_m$ are the distinct isomorphisms of k into $\boldsymbol{R}$, taken in suitable order, then the smallest field of definition for $G^{(i)}$ is k^{σ_i}, and $G_{\boldsymbol{R}} = G^{(1)}_{\boldsymbol{R}} \cdot \cdots \cdot G^{(m)}_{\boldsymbol{R}}$. There are three cases to consider: (1) All simple factors $G^{(i)}_{\boldsymbol{R}}$ are compact. (2) All simple factors $G^{(i)}_{\boldsymbol{R}}$ are noncompact. (3) Some simple factors $G^{(i)}_{\boldsymbol{R}}$ are compact and some are noncompact. In case (1), X is a (nonsingular) projective variety and Γ is finite, so X/Γ is also a (normal) projective variety, and we are done. In case (3), it follows from results of Borel and Harish-Chandra **[8]** or of Mostow-Tamagawa **[14]** that X/Γ is compact. It then follows easily from a criterion, proved in **[1]**, which is a generalization of Kodaira's result **[12]** on Kähler varieties of restricted type, that X/Γ is again a projective variety. In case (2), the same results of the above-mentioned authors imply that X/Γ is compact, and therefore a projective algebraic variety, if G is $\boldsymbol{Q}$-anisotropic. Hence, we shall assume in the future that G is centerless, $\boldsymbol{Q}$-simple, of $\boldsymbol{Q}$-rank $\geqq 1$, and hence that all $G^{(i)}_{\boldsymbol{R}}$ are noncompact.

Making the assumptions indicated above, we now outline the main steps of proving the desired result.

(1) Compactification V^* of $V = X/\Gamma$ as a topological space. This requires the discussion of three subtopics:

(*a*) the natural compactification of X viewed as a bounded domain;

(*b*) the characterization of "rational boundary components" to play the rôle of $\boldsymbol{Q} \cup \{\infty\}$ in §1, A;

(c) fundamental sets and reduction theory, from which we get the topology on V^*.

(2) Introduction of a ringed structure on V^*.

(3) Proof that the ringed structure in (2) makes V^* into a normal analytic space. This requires a proof of the existence of sufficiently many functions in our ringed structure, and the latter depends on the convergence and other properties of Poincaré-Eisenstein series, including properties of the so-called Φ-operator (i.e., behaviour of Poincaré-Eisenstein series at ∞).

(4) Proof that V^* is a projective variety. This again requires information on the properties of Poincaré-Eisenstein series.

So to begin with, we need to study the natural compactification of X taken as a bounded domain in some $\boldsymbol{C}^M$, as well as properties of the unbounded realizations of X as Siegel domains of the third kind in the sense of Pyateckiĭ-Shapiro.

3. **Natural compactification and Cayley transforms of a bounded symmetric domain.** It is now our purpose to examine the "natural" compactification of a Hermitian symmetric space X of noncompact type, by which we mean the compactification of X obtained by realizing it as a bounded domain in some $\boldsymbol{C}^M$ and taking its closure there. At the same time, for later applications to Poincaré-Eisenstein series, we need to consider the unbounded realizations of X, attached to the different boundary components of X.

We may write $X = K\backslash G$, where G is a connected, reductive Lie group with compact center having a faithful linear representation. Thus, G is the identity component, in the usual topology, of the group of real points of a connected, reductive, algebraic group $G_{\boldsymbol{C}}$ defined over $\boldsymbol{R}$, which has no nontrivial rational character defined over $\boldsymbol{R}$, and K is a maximal compact subgroup of G. Let $\mathfrak{k}$ be the Lie algebra of K and let $\mathfrak{p}$ be the orthogonal complement of $\mathfrak{k}$ in the Lie algebra $\mathfrak{g}$ of G with respect to the Killing form. $\mathfrak{g} = \mathfrak{k} + \mathfrak{p}$ is a Cartan decomposition of $\mathfrak{g}$. $\mathfrak{h}$ is to be a Cartan subalgebra of $\mathfrak{k}$, and hence also of $\mathfrak{g}$ because of our assumption on X, and $\Phi = {}_{\boldsymbol{C}}\Phi$ will denote the root system of $\mathfrak{g}_{\boldsymbol{C}}$ with respect to $\mathfrak{h}_{\boldsymbol{C}}$. We may choose root vectors $E_\mu, \mu \in \Phi$, and elements H_μ of $\mathfrak{h}_{\boldsymbol{C}}$ such that

$$[E_\mu, E_{-\mu}] = H_\mu$$

and

$$\nu(H_\mu) = 2(\nu, \mu)(\mu, \mu)^{-1} \quad (\mu, \nu \in \Phi),$$

$(\, , \,)$ being the restriction of the Killing form to $\mathfrak{h}_{\boldsymbol{C}}$. If $\mu \in \Phi$, μ is called compact if it vanishes on the center of $\mathfrak{k}$, and is called noncompact otherwise. We may assume that complex conjugation of $\mathfrak{g}_{\boldsymbol{C}}$ with respect to $\mathfrak{g}$ permutes E_μ and $E_{-\mu}$ for μ noncompact. Fix a linear ordering on Φ, and let π^+ (resp. π^-) denote the set of positive (resp. negative) noncompact roots with respect to this ordering. Let $\mathfrak{p}^\pm = \sum_{\mu \in \pi^\pm} \boldsymbol{C}E_\mu$. Then $\mathfrak{p}_{\boldsymbol{C}} = \mathfrak{p}^+ + \mathfrak{p}^-$ (direct sum) and

$$\mathfrak{g}_{\boldsymbol{C}} = \mathfrak{k}_{\boldsymbol{C}} + \mathfrak{p}^+ + \mathfrak{p}^-,$$

where $\mathfrak{p}^+$ and $\mathfrak{p}^-$ are Abelian subalgebras of $\mathfrak{g}_{\boldsymbol{C}}$ normalized by $\mathfrak{k}_{\boldsymbol{C}}$. Moreover, the elements $X_\mu = (E_\mu + E_{-\mu})$, $Y_\mu = i(E_\mu - E_{-\mu}) (\mu \in \pi^+)$ form a basis of $\mathfrak{p}$ over $\boldsymbol{R}$.

Two roots $\mu, \nu \in \Phi$ are called strongly orthogonal if $\mu \pm \nu$ are not roots. We select according to Harish-Chandra a maximal set $\{\mu_1, \cdots, \mu_t\}$ of mutually strongly orthogonal elements of π^+, and write H_i, E_i, E_{-i}, X_i, and Y_i in place of $H_{\mu_i}, E_{\mu_i}, E_{-\mu_i}, X_{\mu_i}$, and Y_{μ_i}, respectively.

Let $P^\pm = \exp \mathfrak{p}^\pm$. It is well known, as has been mentioned in **[6]**, that the mapping $\phi : P^- \times K_{\boldsymbol{C}} \times P^+ \to G_{\boldsymbol{C}}$ maps the triple product biholomorphically onto a Zariski-open subset $\mathcal{O}$ of $G_{\boldsymbol{C}}$ containing G. Since $\exp : \mathfrak{p}^+ \to P^+$ is a biholomorphic isomorphism, we may form its inverse, denoted by log. Then ζ will denote the map of $\mathcal{O}$ onto $\mathfrak{p}^+$ defined as the composition of the three maps ϕ^{-1}, projection onto P^+, and log. Harish-Chandra has proved that $\zeta(G)$ is a bounded domain D in $\mathfrak{p}^+$ such that ζ induces an equivariant biholomorphic homeomorphism of $X = K\backslash G$ onto D. $\bar{D}$ is called the "natural" compactification of X.

We now wish to describe some results of Korányi and Wolf [13] on the unbounded realizations of X. These results (obtained in slightly different notation and with conventions differing slightly from the present ones, e.g., action on the left instead of on the right, etc.) generalize results of Pyateckiĭ-Shapiro on the classical domains [15]. For simplicity, we assume G henceforth to be irreducible.

For each b, $0 \leqq b \leqq t$, we define

$$c_b = \prod_{1 \leqq j \leqq b} \exp \frac{\pi i}{4} Y_j, \qquad c_0 = \text{identity of } G.$$

The elements c_b of G_C are called "partial Cayley transformations" and are analogous to the usual Cayley transformation carrying the unit disc onto the upper half H_1, of the complex plane.

Direct calculation shows:

$$\begin{aligned} &\operatorname{Ad} c_b(Y_k) = Y_k, \quad 1 \leqq k \leqq t, \\ &\operatorname{Ad} c_b(H_k) = X_k, \quad \operatorname{Ad} c_b(X_k) = -H_k, \quad 1 \leqq k \leqq b, \\ &\operatorname{Ad} c_b(H_k) = H_k, \quad \operatorname{Ad} c_b(X_k) = X_k, \quad b < k \leqq t. \end{aligned}$$

Moreover, as is substantially less obvious, $G \cdot c_b \subset \mathcal{O}$. Let $S_b = \zeta(G \cdot c_b)$. Direct calculation shows that $o_b = -(E_1 + \cdots + E_b) = \zeta(c_b) \in S_b$, and in fact $o_b \in \partial D = \bar{D} - D$. The domains S_b are the unbounded realizations we want, and the sets $o_b \cdot G$ (G acts continuously on $\bar{D}$) are precisely the distinct orbits of G in $\bar{D}$. To describe the situation more adequately, we need some further definitions.

Let $\mathfrak{a}$ be the (Abelian) subalgebra of $\mathfrak{p}$ spanned by $X_1, \cdots, X_t$. $\mathfrak{a}$ is a maximal subalgebra of $\mathfrak{g}$ contained in $\mathfrak{p}$ and is diagonalizable (over $\boldsymbol{R}$) in the adjoint representation. Let ${}_{\boldsymbol{R}}\Phi$ be the set of roots of $\mathfrak{g}$ with respect to $\mathfrak{a}$. $\mathfrak{g}$ is the direct sum of the centralizer $z(\mathfrak{a})$ of $\mathfrak{a}$ and of the root spaces

$$\mathfrak{g}_\alpha = \{x \in \mathfrak{g} | [a, x] = \alpha(a)x\}, \qquad \alpha \in {}_{\boldsymbol{R}}\Phi.$$

Let $\gamma_1, \cdots, \gamma_t$ be the coordinates in $\mathfrak{a}$ with respect to the basis $X_1, \cdots, X_t$. Then, since $\mathfrak{g}$ is simple, ${}_{\boldsymbol{R}}\Phi$ is either [5]

$$C_t = \{(\pm\gamma_i \pm \gamma_j)/2, 1 \leqq i,j \leqq t\} - \{0\}$$

or

$$BC_t = C_t \cup \{\gamma_i/2, 1 \leqq i \leqq t\}.$$

In both cases, we choose as ordering on ${}_{\boldsymbol{R}}\Phi$ the lexicographic ordering defined by the basis $\{X_i\}_{1 \leqq i \leqq t}$. Then the set ${}_{\boldsymbol{R}}\Delta$ of simple roots in ${}_{\boldsymbol{R}}\Phi$ consists of $\alpha_i = (\gamma_i - \gamma_{i+1})/2, 1 \leqq i < t$, and $\alpha_t = \gamma_t$ (resp. $\alpha_t = \frac{1}{2}\gamma_t$) if ${}_{\boldsymbol{R}}\Phi$ is of type C_t (resp. BC_t). The numbering of the simple $\boldsymbol{R}$-roots thus defined is called the *canonical numbering.*

We let ${}_{\boldsymbol{R}}\Phi^+$ (resp. ${}_{\boldsymbol{R}}\Phi^-$) denote the set of positive (resp. negative) roots in ${}_{\boldsymbol{R}}\Phi$.

Let $\mathfrak{n} = \sum_{\alpha \in {}_{\boldsymbol{R}}\Phi^+} \mathfrak{g}_\alpha$, $A = \exp \mathfrak{a}$, $N = \exp \mathfrak{n}$. Then $A \cdot N$ is a maximal connected triangulizable subgroup of G. The centralizer $Z(A)$ of A is equal to the product $A \cdot M$, where $M = Z(A) \cap K$, the normalizer $P = Z(A) \cdot N$ of N is a minimal parabolic $\boldsymbol{R}$-subgroup of G, and any minimal parabolic $\boldsymbol{R}$-subgroup of G is conjugate to P. Any maximal proper parabolic $\boldsymbol{R}$-subgroup of G is conjugate to exactly one of the form $P_b = Z(A_b)$. N, where $A_b = \exp(\boldsymbol{R}(X_1 + \cdots + X_b))$ and $Z(A_b)$ is the centralizer (in G) of A_b. Let $\mathfrak{p}_b$ be the Lie algebra of P_b. $\boldsymbol{R}(X_1 + \cdots + X_b) = \mathfrak{a}_b$ can also be described as the one-dimensional subalgebra of $\mathfrak{a}$ annihilated by all simple $\boldsymbol{R}$-roots except α_b. If σ is any subset of ${}_{\boldsymbol{R}}\Delta$, denote by $[\sigma]$ the set of $\boldsymbol{R}$-roots in its linear ($\boldsymbol{R}$-) span. Then the Lie algebra $\mathfrak{p}_b$ of P_b is the sum of

$$\mathfrak{l}_b = \sum_{\alpha \in [\alpha_{b+1}, \cdots, \alpha_t]} (\mathfrak{g}_\alpha + [\mathfrak{g}_\alpha, \mathfrak{g}_{-\alpha}]),$$

$$\mathfrak{l}'_b = \sum_{\alpha \in [\alpha_1, \cdots, \alpha_{b-1}]} (\mathfrak{g}_\alpha + [\mathfrak{g}_\alpha, \mathfrak{g}_{-\alpha}])$$

$$\mathfrak{u}_b = \sum_{\alpha \in \boldsymbol{R}\Phi^+_{\boldsymbol{R}} - [\alpha_1, \cdots, \alpha_{b-1}] - [\alpha_{b+1}, \cdots, \alpha_t]} \mathfrak{g}_\alpha,$$

of $\mathfrak{a}_b$, and of an ideal $\mathfrak{m}_b$ of $\mathfrak{m}$, the Lie algebra of M. The algebra $\mathfrak{z}_b = \mathfrak{l}'_b + \mathfrak{m}_b + \mathfrak{u}'_b + \mathfrak{a}_b$ is an ideal of $\mathfrak{p}_b$; let $U_b = \exp \mathfrak{u}_b$ and let Z_b be the inverse image in P_b of the centralizer of the identity component in P_b/Z_b^0, where Z_b^0 is the connected closed subgroup of G with (the semisimple) Lie algebra $\mathfrak{z}_b$. Then Z_b is a normal subgroup of P_b, $P_b = Z_b \cdot L_b$, and $L_b \cap Z_b$ is finite.

We have

$$\mathfrak{l}_{b,C} = \mathfrak{k}_{b,C} \oplus \mathfrak{p}_b^+ \oplus \mathfrak{p}_b^- \qquad (\mathfrak{k}_{b,C} = \mathfrak{k}_C \cap \mathfrak{l}_{b,C} \text{ and } \mathfrak{p}_b^\pm = \mathfrak{l}_{b,C} \cap \mathfrak{p}^\pm),$$

the space $X_b = K_b \backslash L_b$ is Hermitian symmetric, and $D_b = \zeta(L_b) \subset \mathfrak{p}_b^+$ is the realization of X_b as a bounded domain. $F_b = o_b + \zeta(L_b)$ is just the orbit of o_b under L_b, is contained in $\partial D = \bar{D} - D$, and is a set of imprimitivity of G in $\bar{D}$. The transforms of the F_b's by the elements of G are the *boundary components* of $\bar{D}$. D itself is a (an improper) boundary component with $b = 0$. If $\mathfrak{g}$ is not simple, then the boundary components of $\bar{D}$ are the products of the boundary components of the individual factors.

If F is a boundary component of $\bar{D}$, we define

$$N(F) = \{g \in G | Fg = F\},$$

$$Z(F) = \{g \in N(F) | xg = x \text{ for all } x \in F\},$$

and

$$G(F) = Z(F) \backslash N(F).$$

One may prove that $N(F_b) = P_b$, $Z(F_b) = Z_b$, and

$$G(F_b) = (L_b \cap Z_b)\backslash L_b, \qquad 0 \leqq b \leqq t.$$

Now we proceed to the description of the unbounded realizations S_b. We have $P_{bC} = N(F_b)_C$, a "standard" parabolic $\boldsymbol{R}$-subgroup of G_C, and $N(F_b) = Z(A_b) \cdot U_{b\boldsymbol{R}} = L_b \cdot Z_b$, where A_b is the one-dimensional subgroup of ${}_{\boldsymbol{R}}A$ on which all roots but α_b vanish, $Z(A_b)$ is its centralizer in $G^0_{\boldsymbol{R}} = G$, and U_b is the unipotent radical of P_{bC}. We may write $Z(A_b) = L_b \cdot L'_b \cdot M_b \cdot A_b$, where M_b is a compact normal subgroup of $Z(A_b)$; then $L'_b \cdot M^0_b \cdot A_b \cdot U_{b\boldsymbol{R}}$ is the identity component of Z_b. Let V be the orbit of $-io_b \in \mathfrak{p}^+$ under $L'_b \cdot M_b \cdot A_b$, let W_b be the center of U_b, and put $E_b = W_{b\boldsymbol{R}}\backslash U_{b\boldsymbol{R}}$. Since U_b is two-stage metabelian, E_b may be identified with a vector space, over $\boldsymbol{R}$ which is, in fact, even-dimensional. W_b is Abelian, connected, and contained in P^+, and therefore will be identified with its Lie algebra. It can be proved that $V \subset W_b$ (q.v. **[13]**). Let iN_2 be the smallest real subspace of W_b containing V. Then $W_b = N_2 + iN_2$ and V is a linear homogeneous convex open cone in iN_2. When speaking of real and imaginary parts of elements in W_b, it will be with reference to the real form N_2 of W_b. Then E_b (which is even-dimensional over $\boldsymbol{R}$) may be supplied with the structure of a complex vector space in a natural way depending on $t \in D_b$ such that the following is true: There exists for each $t \in D_b \subset \mathfrak{p}_b^+$ a quasi-Hermitian $\boldsymbol{R}$-bilinear mapping $L_t: E_b \times E_b \rightarrow W_b$ (depending in a real analytic manner on t) such that $S_b = \{(z, u, t) \in W_b \times E_b \times D_b | \operatorname{Im} z - \operatorname{Re} L_t(u, u) \in V\}$. (A quasi-Hermitian mapping in the sense of Pyateckiĭ-Shapiro is one which is the sum of a Hermitian mapping and of a symmetric one.) Moreover, L_t is nondegenerate for each $t \in D_b$ in the sense that $L_t(u, v) = 0$ for all $v \in E_b$, fixed u implies $u = 0$. One needs these facts in the discussion of Fourier-Jacobi series. We need, moreover, the following facts about the operation of P_b on S_b: If $n \in U_{b\boldsymbol{R}}$, n acts by a unipotent linear transformation on $E_b + W_b$ and leaves $\mathfrak{p}_b^+$ pointwise fixed. Each element of $A_b \cdot L'_b \cdot M_b$ acts by linear transformations with constant Jacobian determinant, leaving D_b pointwise fixed. And if $g \in L_b$, then the Jacobian determinant of the action of g on D_b is a positive rational power ($\geqq 1$) of the Jacobian determinant of its action on S_b.

In closing this section, we point out the following useful fact, (the inspiration for which is due essentially to Pyateckiĭ-Shapiro **[16]**): Let C_b be the connected centralizer of $W_{b\boldsymbol{R}}$ in P_b. Then its Lie algebra $\mathfrak{C}_b$ is equal to $\mathfrak{l}_b + \mathfrak{u}_b + (\mathfrak{C}_b \cap \mathfrak{z}(\mathfrak{a}) \cap \mathfrak{k})$. In particular, $C_b/L_b \cdot U_b$ is compact.

4. **The topological compactification of** X/Γ. We carry over the assumptions of §2. We shall also assume that G_C is absolutely simple. This is not essential for our proofs, but is intended to avoid obscuring the main points with technical details. All our results are indeed valid without this assumption and the fact mentioned at the end of §3 is useful in making the step to the more general case. Moreover, many things also become simpler if we assume that the $\boldsymbol{Q}$-rank of G_C is the same as its $\boldsymbol{R}$-rank. While we shall not explicitly assume this to be the case, we shall usually state without proof those propositions which enable us to

deal with the case $rk_{\boldsymbol{R}}G_{\boldsymbol{C}} > rk_{\boldsymbol{Q}}G_{\boldsymbol{C}}$ in the same general manner as with the simpler case $rk_{\boldsymbol{R}}G_{\boldsymbol{C}} = rk_{\boldsymbol{Q}}G_{\boldsymbol{C}}$.

We choose once for all a maximal $\boldsymbol{Q}$-trivial torus S in $G_{\boldsymbol{C}}$, let ${}_{\boldsymbol{Q}}M$ be the $\boldsymbol{Q}$-anisotropic part of $Z(S)$, and let ${}_{\boldsymbol{Q}}N$ be the connected, unipotent subgroup of $G_{\boldsymbol{C}}$ with Lie algebra equal to the sum of those $\boldsymbol{Q}$-root spaces corresponding to the positive $\boldsymbol{Q}$-roots with respect to some linear ordering on the vector space containing the $\boldsymbol{Q}$-roots. Put ${}_{\boldsymbol{Q}}A = S^0_{\boldsymbol{R}}$. We have the following:

Proposition. *There exist a maximal $\boldsymbol{Q}$-torus T of $G_{\boldsymbol{C}}$ and a maximal $\boldsymbol{R}$-trivial torus ${}_{\boldsymbol{R}}T$ of $G_{\boldsymbol{C}}$ (${}_{\boldsymbol{R}}T$ is not necessarily defined over $\boldsymbol{Q}$) such that $S \subset {}_{\boldsymbol{R}}T \subset T$.*

We omit the proof.

Let Φ, ${}_{\boldsymbol{R}}\Phi$, and ${}_{\boldsymbol{Q}}\Phi$ be the sets of roots of G with respect to T, ${}_{\boldsymbol{R}}T$, and S, respectively, and we suppose these are supplied with compatible orderings; e.g., if $r: X^*({}_{\boldsymbol{R}}T) \rightarrow X^*(S)$ is the restriction from the rational character group of ${}_{\boldsymbol{R}}T$ to that of S, and if $\alpha \in {}_{\boldsymbol{R}}\Phi$, then $\alpha > 0$, $r(\alpha) \neq 0$ imply $r(\alpha) > 0$; similarly for the compatibility of the orderings on the roots of the other pairs of tori. Let Δ, ${}_{\boldsymbol{R}}\Delta$, and ${}_{\boldsymbol{Q}}\Delta$ be the corresponding sets of positive simple roots. We have ${}_{\boldsymbol{Q}}\Delta = r({}_{\boldsymbol{R}}\Delta) - \{0\}$. Let ${}_{\boldsymbol{R}}\Delta = \{\alpha_1, \cdots, \alpha_t\}$ with the canonical numbering described in §3. If $\beta \in {}_{\boldsymbol{Q}}\Delta$, let $m(\beta)$ be the greatest index i such that $r(\alpha_i) = \beta$. We number the elements $\beta_1, \cdots, \beta_s$ of ${}_{\boldsymbol{Q}}\Delta$ in such a way that $i < j$ if and only if $m(\beta_i) < m(\beta_j)$. We have the

Proposition. (a) *${}_{\boldsymbol{Q}}\Delta$ is of type BC_s if either ${}_{\boldsymbol{R}}\Phi$ is of type BC_t or ${}_{\boldsymbol{R}}\Phi$ is of type C_t and $r(\alpha_t) = 0$, and is of type C_s otherwise. The numbering of $\beta_1, \cdots, \beta_s$ described above is the canonical one.*

(b) *Each $\beta \in {}_{\boldsymbol{Q}}\Delta$ is the restriction of exactly one $\alpha \in {}_{\boldsymbol{R}}\Delta$.*

The roots $\alpha \in {}_{\boldsymbol{R}}\Delta$ such that $r(\alpha) \neq 0$ are called "critical".

Corollary. *The proper maximal parabolic $\boldsymbol{Q}$-subgroups of $G_{\boldsymbol{C}}$ are also proper maximal among parabolic $\boldsymbol{R}$-subgroups.*

This is true, roughly speaking, because both ${}_{\boldsymbol{Q}}\Delta$ and ${}_{\boldsymbol{R}}\Delta$ are chains (i.e., have no branching), and for each $\beta \in {}_{\boldsymbol{Q}}\Delta$ there is just one $\alpha \in {}_{\boldsymbol{R}}\Delta$ with $r(\alpha) = \beta$. Therefore, if P is a proper, maximal, "standard" parabolic $\boldsymbol{Q}$-subgroup of $G_{\boldsymbol{C}}$, and if $\beta \in {}_{\boldsymbol{Q}}\Delta$ is the unique simple $\boldsymbol{Q}$-root which is not a $\boldsymbol{Q}$-root of the quotient of P by its unipotent radical, then P is also the proper, maximal, "standard" parabolic $\boldsymbol{R}$-subgroup such that the $\alpha \in {}_{\boldsymbol{R}}\Delta$ with $r(\alpha) = \beta$ is not a root of the quotient of P by its unipotent radical.

Let D be "the" realization of X as a bounded symmetric domain. If F is any boundary component of $\bar{D}$, then $N(F)_{\boldsymbol{C}}$ is maximal, proper $\boldsymbol{R}$-parabolic.

Definition. A boundary component F of $\bar{D}$ is called rational if $N(F)_{\boldsymbol{C}}$ is defined over $\boldsymbol{Q}$.

We note that in [4] a definition of broader apparent applicability is taken, which in our case is equivalent to the above.

Let S, ${}_{\boldsymbol{R}}T$, and T be as above and let F_b be a standard boundary component, so that $P_{b\boldsymbol{C}} = N(F_b)_{\boldsymbol{C}}$ is a maximal proper standard parabolic $\boldsymbol{R}$-subgroup of $G_{\boldsymbol{C}}$.

One sees from the description of the standard parabolic groups that P_b is defined over Q if and only if α_b is critical, and in that case, L_b, Z_b, and U_b are also defined over Q. Then, in that case, the mapping $N(F_b)_C \to Z(F_b)_C \backslash N(F_b)_C$ is defined over Q, and so if Γ is an arithmetic subgroup of G, then $(Z(F_b) \cap \Gamma) \backslash (N(F_b) \cap \Gamma)$ is a discrete transformation group of F_b (it is, in fact, an arithmetic subgroup of $G(F_b) = Z(F_b) \backslash N(F_b)$).

Let η, ω resp. be relatively compact, open neighborhoods of the identity in ${}_QM_R$, ${}_QN_R$ resp., and let $t > 0$ be given. Define

$$ {}_QA_t = \{a \in {}_QA \mid \beta(a) < e^t, \beta \in {}_Q\Delta\}, $$

and put $\mathfrak{S}_{t,\eta,\omega} = K \cdot {}_QA_t \cdot \eta \cdot \omega$ (where, of course, we take the Lie algebras of ${}_QA$ and K orthogonal to each other). Denote by $\Omega_{t,\eta,\omega}$ the natural image of $\mathfrak{S}_{t,\eta,\omega}$ in X and let $\bar{\Omega}_{t,\eta,\omega}$ be the closure of $\Omega_{t,\eta,\omega}$ in the natural compactification of X as a bounded domain D. $\Omega_{t,\eta,\omega}$ is called a "Siegel set" in X. One verifies readily that: (a) if F is a boundary component of $\bar{D}$ meeting $\bar{\Omega}_{t,\eta,\omega}$, then F is rational; (b) if F is rational, then there exists $g \in G_Q$ such that $\bar{\Omega}_{t,\eta,\omega} \cap Fg$ is nonempty; and (c) if $F \cap \bar{\Omega}_{t,\eta,\omega}$ is nonempty, then $F \cap \bar{\Omega}_{t,\eta,\omega} = \bar{\Omega}(F)_{t,\eta',\omega'}$ is a Siegel set on F, where η' and ω' can be made as large as desired by taking η and ω sufficiently large.

Now let Γ be a subgroup of G_R^0 commensurable with G_Z. Let D^* be the union of D and all rational boundary components of $\bar{D}$. It is not difficult to verify that the hypotheses of Theorem 1′ of [19] are satisfied. Thus, D^* may be supplied with a topology $\mathscr{T}$ such that $\mathscr{T}$ induces the usual topology on $\bar{\Omega}_{t,\eta,\omega}$, every element of G_Q is a continuous transformation in $\mathscr{T}$, and D^*/Γ supplied with the quotient topology $\mathscr{T}_0$ is a compact Hausdorff space. Let $\pi: D^* \to D^*/\Gamma$, $\sigma_b: \mathfrak{p}^+ \to \mathfrak{p}_b^+$ (with kernel $\mathfrak{q}_b$ equal to the sum of the root spaces in $\mathfrak{p}^+$ not contained in $\mathfrak{p}_b^+$), and $p_b: P_b \to L_b$ be the natural quotient mappings, where b is chosen such that $F_b (\subset D^*)$ is a rational boundary component. Let $x_b \in \bar{\Omega}_{t,\eta,\omega} \cap F_b$, $x_b = o_b \cdot g_b$ with $g_b \in L_b$, and let $\{\mathscr{E}_\alpha\}$ be a basis of connected relatively compact neighborhoods of g_b. For any α and $\lambda > 0$, define (here $a \in {}_QA$):

$$ \mathfrak{S}_{t,\eta,\omega}(\mathscr{E}_\alpha, \lambda) = \{g = kamn \in \mathfrak{S}_{t,\eta,\omega} \mid p_b(amn) \in \mathscr{E}_\alpha, \beta_b(a) < e^{-\lambda}\}, $$

and denote by $\Omega_{t,\eta,\omega}(\mathscr{E}_\alpha, \lambda)$ the image of this in X. By using such "truncated Siegel sets", we may prove the existence of a basis of neighborhoods $\mathscr{N}_{\alpha,\lambda}$ of $\pi(x_b)$ in $V^* = D^*/\Gamma$ such that each of the sets $\mathscr{N}_{\alpha,\lambda} \cap (D/\Gamma)$ is connected. We define $V = D/\Gamma$.

5. **The ringed structure.** If F is a rational boundary component, let

$$ \Gamma(F) = (Z(F) \cap \Gamma) \backslash (N(F) \cap \Gamma). $$

If F_b is a standard rational boundary component, of course $L_b \cap \Gamma$ is isogenous to $\Gamma(F_b)$. We may write $D^*/\Gamma = \bigcup_F F/\Gamma(F)$, where F runs over a complete set of Γ-inequivalent rational boundary components, including D itself. Each of the spaces $F/\Gamma(F) = V_F$ carries a natural complex structure. If $\mathscr{O}$ is an open subset of $D^*/\Gamma = V^*$, and if f is a continuous complex-valued function on $\mathcal{O}$, we say f is an $\mathfrak{A}$-function on $\mathcal{O}$ if $f|V_F \cap \mathcal{O}$ is analytic for each rational F. Our purpose is to prove that V^* supplied with the ringed structure of $\mathfrak{A}$-functions is a normal complex analytic space.

6. **Poincaré-Eisenstein series.** Again, let $F_b = F$ be a "standard" rational boundary component and denote by Γ a subgroup of $G = G_{\boldsymbol{R}}^0$ commensurable with $G_{\boldsymbol{Z}}$. Put $P = P_{b\boldsymbol{C}}$ and let $X_0 \colon P \to \boldsymbol{C}^*$ be the rational character defined by $X_0(p) = \det(\mathrm{Ad}_{\mathfrak{u}} p)$, where u is the Lie algebra of $U = U_b$. We take X_0 to be the fundamental highest weight of P. For any positive real number s, let $\Delta(p, s) = |X_0(p)|^{-s}$ and let f be a continuous function, $f \colon G \to \boldsymbol{C}$ such that

$$f(gp) = f(g)\Delta(p, s),\ g \in G,\ p \in P \cap G.$$

Then (Godement)

$$E_f(g) = \sum_{\gamma \in \Gamma/(\Gamma \cap P)} f(g\gamma) \qquad (g \in G)$$

converges absolutely uniformly on compact subsets of G if $s > 1$.

We now apply a slight modification of this criterion to certain series on $S_b = \zeta(G \cdot c_b)$, notation being as in §3. As remarked in [6], it is in fact sufficient to replace the hypothesis of Godement's convergence theorem by:

(a) $m(g) = \sup_{p \in P \cap G} |f(gp)| \, |X_0(p)|^s$ is finite for each $g \in G$ and is bounded on compact sets, and

(b) $f(g\gamma) = f(g)$ for all $\gamma \in \Gamma \cap P$.

Following previous notation, we let $\sigma_b \colon \mathfrak{p}^+ \to \mathfrak{p}_b^+$ be the projection with kernel $\mathfrak{q}_b$. Then $\sigma_b(S_b) = D_b \subset \mathfrak{p}_b^+$. Let ϕ be any polynomial function on D_b, let $\Gamma_0 = \Gamma \cap Z_b$, and define

$$E(x) = E_{\phi,l,\Gamma}(x) = \sum_{\gamma \in \Gamma/\Gamma_0} \phi(\sigma_b(x \cdot \gamma)) J_b(x, \gamma)^l,$$

for $x \in S_b$, where l is a suitable positive even integer and J_b is the functional determinant in S_b (of the transformation γ at $x \in S_b$). To see that this is well defined, we note that for $\gamma \in \Gamma_0$ we have $\phi(\sigma_b(x \cdot \gamma)) = \phi(\sigma_b(x))$, because Γ_0 acts trivially on F_b; and $J_b(x, \gamma)^l = 1$ for $x \in S_b$ and $\gamma \in \Gamma_0$, if l is divisible by $n!$ for a sufficiently large positive integer n, because $J_b(x, \gamma)$ takes only finitely many values for $\gamma \in \Gamma_0$, as one may easily see. Such series as these are called Poincaré-Eisenstein series (P.-E. series for short). Because of the facts indicated at the end of §3 and by our preceding discussion, we have for $p \in P \cap G$:

$$|J_b(x, p)| = |j_b(\sigma_b(x), p)|^{q_b} |X_0(p)|^{-n_b},$$

where j_b is the functional determinant of a transformation of D_b, and q_b and n_b are positive rational numbers, $q_b > 1$; thus $lq_b > 2$. We now assume that $ln_b > 1$. We may write

$$(1) \qquad E(x) = \sum_{\gamma \in \Gamma/\Gamma_\infty} \left(\sum_{\lambda \in \Gamma_\infty/\Gamma_0} \phi(\sigma_b(x \cdot \gamma\lambda)) J_b(x, \gamma\lambda)^l \right),$$

where $\Gamma_\infty = \Gamma \cap P$. We define for $g \in G$:

$$r(g) = \phi(\sigma_b(o_b \cdot g))J_b(0, g)^l,$$

and

(2)
$$\mathscr{P}(g) = \sum_{\lambda \in \Gamma_\infty/\Gamma_0} |r(g\lambda)|,$$

and for $x \in S_b$ put

(3)
$$\mathscr{P}^*(x) = \sum_{\lambda \in \Gamma_\infty/\Gamma_0} |\phi(\sigma_b(x \cdot \lambda))J_b(x, \lambda)^l|.$$

The relationship between $\mathscr{P}$ and $\mathscr{P}^*$ is that if $x = o_b \cdot g$, then

$$\mathscr{P}^*(x) = |J_b(o_b, g)^{-l}|\mathscr{P}(g).$$

Then the series of the absolute values of the terms in (1) is equal to

(4)
$$|J_b(o_b, g)^{-l}| \sum_{\gamma \in \Gamma/\Gamma_\infty} \mathscr{P}(g\gamma).$$

We define

(5)
$$E'(g) = \sum_{\gamma \in \Gamma/\Gamma_\infty} \mathscr{P}(g\gamma).$$

It is obviously sufficient to prove the convergence of the series in (5). To do this, it is enough to verify the conditions (a) and (b) above with $f = \mathscr{P}$ and $s = ln_b$. Condition (b) is clearly satisfied by virtue of the definition (2). We now check (a). We use $\mathbf{a}(g)$ to denote $J_b(o_b, g)^l$, $g \in G$. If $p \in Z_b$, $\mathbf{a}(gp) = \mathbf{a}(g)|X_0(p)|^{-s}$ $(s = ln_b)$, while if $v \in L_b, X_0(v^{-1}pv) = X_0(p)$, because P_b operates trivially on its own character group by inner automorphisms. Therefore $\mathscr{P}(gp) = \mathscr{P}(g)|X_0(p)|^{-s}$. Since $P_b = L_b \cdot Z_b$, and $|X_0(v)| = 1$ for $v \in L_b$, it suffices to prove, finally, that $\mathscr{P}(gv)$ remains bounded for $v \in L_b$, g in a compact subset C of G. For each $g \in C$, we choose an element $m_g \in L_b$ such that $\sigma_b(o_b \cdot g) = o_0 \cdot m_g (o_0 \in D_b$, being the origin of coordinates). Of course, m_g is determined up to an element of the compact group $K \cap L_b$, and so m_g remains in a compact set as g runs over C. Then for $\lambda \in \Gamma_\infty$, let $\bar{\lambda}$ be the image of λ in $Z_b\backslash N(F) = G(F)$, and if $v \in L_b$, let $\bar{v}$ be its image in $G(F)$. We have

$$J_b(o_b, g \cdot v \cdot \lambda) = J_b(o_b, g)j_b(0, m_g)^{-q_b}j_b(0, m_g \cdot \bar{v} \cdot \bar{\lambda})^{q_b},$$

as follows from the "cocycle relation" for functional determinants, so that

$$\mathscr{P}(g \cdot v) = J_b(o_b, g)^l j_b(0, m_g)^{-lq_b}\hat{\mathscr{P}}(m_g\bar{v}),$$

where $\hat{\mathscr{P}}$ is a Poincaré series on F "lifted" to the group $G(F)$, and hence, by **[6]**, is bounded on $G(F)$. Hence, $\mathscr{P}(gv)$ is bounded for $g \in C$, $v \in L_b$, as we wanted to show. Thus the series in (5) converges (absolutely and) uniformly on compact sets.

In what follows, $c_1, c_2, \cdots$ will denote suitable constants and will be so understood without further explanation. Our purpose here is to obtain a normal majorant for the series of absolute values of the terms in $E(x)$ in some Siegel set contained in a neighborhood of some $x_0 \in F_b$. The details for dealing with translates of such a Siegel set by elements of G_Q, and for dealing with the automorphic form corresponding to E in other unbounded realizations are close to what is given in our discussion here.

Let E^0 denote the series whose terms are the absolute values of the terms of the series for E. For $s \in G$ we have

$$E^0(o_b \cdot s) = \mathbf{a}(s)^{-1} \sum_{\gamma \in \Gamma/\Gamma_\infty} \mathscr{P}(s\gamma). \tag{6}$$

We take an irreducible *left* linear, rational representation ρ defined over Q, of G, with highest weight X_0^s (we may as well assume $s = ln_b$ to be an integer), such that P is the full subgroup of G leaving the line spanned by a highest weight vector e_1 invariant, and put $c'(g) = \|\rho(g)e_1\|^{-1}$, where $\| \ \|$ is some Euclidean norm with respect to which $\rho(S)$ consists of self-adjoint transformations (S is the maximal Q-trivial torus). Then the eigenspaces of $\rho(S)$ corresponding to distinct Q-weights of ρ are mutually orthogonal. If $p \in P$, we have clearly

$$c'(gp)|X_0(p)|^s = c'(g), \qquad c'(g) > 0, \qquad g \in G, \tag{7}$$

and so $\mathscr{P}(g) < c_1 \cdot c'(g)$ for all $g \in G$ by a well-known argument (using the fact that $G = KP$). Hence, E^0 is majorized by the series

$$c_1\mathbf{a}(s)^{-1} \sum_{\gamma \in \Gamma/\Gamma_\infty} c'(s\gamma). \tag{8}$$

We now want to estimate the behaviour of (8) for s in some Siegel set $\mathfrak{S}_{t,\eta,\omega}$. For $s \in \mathfrak{S}_{t,\eta,\omega}$, $s = kamn = kmn'a$, with $a \in {}_QA_t$, $m \in \eta$, $n \in \omega$, $k \in K$. By an argument in [7] $a\omega a^{-1}$ is relatively compact in ${}_QN_R$ if ω is; of course, $n' \in a\omega a^{-1}$. If $g \in G$, we have $\rho(g)e_1 = K_1e_1 + \sum_\mu f_\mu$, where f_μ is in the eigenspace corresponding to the Q-weight μ, and letting $X = X_0^s$, we have

$$\|\rho(a)\rho(g)e_1\| = \|K_1X(a)e_1 + \sum_\mu \mu(a)f_\mu\|.$$

Also, since kmn' runs over a relatively compact set C_1, we have

$$c_2\|x\| \leqq \|\rho(e)x\| \leqq c_3\|x\|$$

for all $e \in C_1$ and x in the representation space of ρ. Hence, as a simple calculation shows,

$$c_4|\mathbf{a}(s)| \leqq X(a)^{-1} \leqq c_5|\mathbf{a}(s)| \tag{9}$$

for $s = kamn \in \mathfrak{S}_{t,\eta,\omega}$. Moreover,

$$c'(ag)^{-2}|X(a)|^{-2} = \|K_1e_1\|^2 + \sum_\mu \|f_\mu\|^2|(X^{-1} \cdot \mu)(a)|^2, \tag{10}$$

where each μ is of the form

$$X\beta_1^{m_1} \cdots \beta_s^{m_s}, \qquad m_i \leqq 0, \qquad {}_Q\Delta = \{\beta_1, \cdots, \beta_s\}.$$

Combining the above, we have for $s \in \mathfrak{S}_{t,\eta,\omega}$:

$$(11)\qquad |\mathbf{a}(s)^{-1}\mathscr{P}(s \cdot g)| \leqq c_6 \Big\|K_1 e_1 + \sum_{\mu} (X^{-1} \cdot \mu)(a) f_\mu\Big\|^{-1} \leqq c_7 c'(ag)|X(a)|,$$

for $g \in G_{\boldsymbol{Q}}$. Choose $a_0 \in {}_{\boldsymbol{Q}}\bar{A}_t$ such that $|\beta_i(a_0)| = e^t$ for all $\beta_i \in {}_{\boldsymbol{Q}}\Delta$. Then for this value a_0 of a, $c'(a\gamma)^{-1}|X(a)|^{-1}$ attains a minimum for $a \in \mathfrak{S}_{t,\eta,\omega}$. For $g \in G_{\boldsymbol{Q}}$, put $c(g) = c'(a_0 g)|X(a_0)|$. It follows from the Godement criterion that $\sum_{\gamma \in \Gamma/\Gamma_\infty} c(g\gamma)$ converges, and from the things we have just said that $c_8 \sum_{\gamma \in \Gamma/\Gamma_\infty} c(\gamma)$ is an absolute majorant for the series E^0 in the image Ω in S_b of any F_b-adapted truncated Seigel domain $\mathfrak{S}$.

Now, to investigate the limit of E as we approach $F = F_b$ from within Ω, we need to estimate the terms $c'(a\gamma)|X(a)|$ as $\beta_b(a)$ tends to zero. We can easily prove, in fact, that $\lim_{\beta_b(a) \to 0} c'(a\gamma)|X(a)| = 0$ if $\gamma \in G_{\boldsymbol{Q}} - N(F)$. Let $\gamma \in G_{\boldsymbol{Q}}$. We may write $\gamma = nwhn'$ with $n, n' \in {}_{\boldsymbol{Q}}N_{\boldsymbol{Q}}$, $w \in N(S)_{\boldsymbol{Q}}$, $h \in S_{\boldsymbol{Q}}$ (Bruhat decomposition). We have

$$\begin{aligned} c'(a\gamma)^{-1} &= \|\rho(anwhn')e_1\| = \|\rho(ana^{-1}awh)(e_1)\| \\ &= \|\rho(ana^{-1}wh)(e_1)\|\,|X(w^{-1}aw)|. \end{aligned}$$

Moreover, $X(w^{-1}aw) = w(X)(a)$. One sees that $w(X) = X\beta_1^{m_1} \cdots \beta_s^{m_s}$, where all $m_i \leqq 0$, and $m_b < 0$ precisely if $\gamma \notin N(F)_{\boldsymbol{Q}}$. Hence,

$$(12)\qquad |X(a)|c'(a\gamma) = \|\rho(ana^{-1}wh)(e_1)\|^{-1}\beta_1(a)^{-m_1} \cdots \beta_s(a)^{-m_s}.$$

As $a\omega a^{-1}$ is relatively compact, the term $\| \;\|^{-1}$ remains bounded as a runs over ${}_{\boldsymbol{Q}}A_t$. Therefore, all factors on the right are bounded, and $\beta_b(a)$ appears with the positive exponent $-m_b$, whence our assertion: $|X(a)|c'(a\gamma) \to 0$ as $\beta_b(a) \to 0$ if $\gamma \notin N(F)_{\boldsymbol{Q}}$.

It now follows rather easily that the limit of E on $F = F_b$ exists and is a Poincaré series of weight lq_b with respect to a certain discontinuous group on D_b. And for suitably divisible weights, we get all such Poincaré series as limits of such P.-E. series E. Of course to prove this one must also deal with translates of E and of $\mathfrak{S}$ by elements of $G_{\boldsymbol{Q}}$, but the general ideas are the same. More generally, one may also show that E has a well-defined limit on every rational boundary component F' (in the topology $\mathscr{T}$), and if $\Phi_{F'}E$ denotes this limit, then one may prove:

(a) if $\dim F' < \dim F$, $\Phi_{F'}E = 0$.

(b) if $\dim F' = \dim F$ and $F' \not\subset F \cdot \Gamma$,
then $\Phi_{F'}E = 0$.

Using these facts, one may prove the local separation of points of V^* by $\mathfrak{A}$-functions. Then an easy prolongation theorem shows that V^*, supplied with the ringed structure indicated previously, is a normal analytic space. This prolongation theorem may be proved using the theorem on removable singularities of analytic sets of Remmert and Stein [**17**], using ideas on prolongations due to myself [**1**], and using subsequent ideas of H. Cartan [**10**; Exp. 11] on prolongations which succeeded in removing a superfluous weakening hypothesis from my earlier theorem. However, the theorem used here is not a direct application of the theorems originally proved by myself and Cartan, but needs some changes because of complications stemming from the fact that the set $V^* - V$ is not necessarily locally irreducible, so that the induction on dimension must be modified. Moreover, the properties of P.-E. series just indicated make it possible to show without great difficulty that V^* may be imbedded as a normal variety in some projective space by means of automorphic forms. Results similar to those formulated here were announced in [16] with sketches of some proofs.

References

1. W. L. Baily, Jr., *On the imbedding of V-manifolds in projective space*, Amer. J. Math. **79** (1957), 403–430.

2. ———, *On Satake's compactification of V_n*, Amer. J. Math. **80** (1958), 348–364.

3. ———, *On the theory of θ-functions, the moduli of Abelian Varieties, and the moduli of curves*, Ann. of Math., **75** (1962), 342–381.

4. W. L. Baily, Jr. and A. Borel, *Compactification of arithmetic quotients of bounded symmetric domains* (to appear).

5. A. Borel, *Linear algebraic groups*, Proc. Sympos. Pure Math., vol. 9, Amer. Math. Soc., Providence, R.I., 1966, pp. 3–19.

6. ———, *Introduction to automorphic forms*, Proc. Sympos. Pure Math., vol. 9, Amer. Math. Soc., Providence, R.I., 1966, pp. 199–210.

7. ———, *Reduction theory for arithmetic groups*, Proc. Sympos. Pure Math., vol. 9, Amer. Math. Soc., Providence, R.I., 1966, pp. 20–25.

8. A. Borel and Harish-Chandra, *Arithmetic subgroups of algebraic groups*, Ann. of Math. (2) **75** (1962), 485–535.

9. H. Braun, *Hermitian modular functions*. I, II, III, Ann. of Math. (2) **50** (1949), 827–855; (2) **51** (1950), 92–104; (2) **53** (1951), 143–160.

10. H. Cartan Séminaire, *Fonctions automorphes*, 2 vols., 10ième annèe (1957/1958), Paris, 1958. (Mimeographed notes).

11. H. Klingen, *Eisensteinreihen zur Hilbertschen Modulgruppe n-ten Grades*, Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl.II, (1960), 87–104.

12. K. Kodaira, *On Kähler varieties of restricted type*, Ann. of Math. (2) **60** (1954), 38–48.

13. A. Korányi and J. Wolf, *Generalized Cayley transformations of bounded symmetric domains* (to appear).

14. G. D. Mostow and T. Tamagawa, *On the compactness of arithmetically defined homogeneous spaces*, Ann. of Math. (2) **76** (1962), 446–463.

15. I. I. Pyateckiĭ-Shapiro, *Geometry of the classical domains and the theory of automorphic functions* Fĭzmatgiz, Moscow, 1961. (Russian)

16. ———. *Arithmetic groups in complex domains*, Uspehi Mat. Nauk **19** (1964), no. 6 (120), 93–120 = Russian Math. Surveys **19** (1964), 831.

17. R. Remmert and K. Stein, *Über die wesentlichen Singularitäten analytischer Mengen*, Math. Ann. **126** (1953), 263–306.

18. I. Satake, *On the compactification of the Siegel space*, J. Indian Math. Soc. **20** (1956), 259–281.

19. ——— *On compactifications of the quotient spaces for arithmetically defined discontinuous groups*, Ann. of Math. (2) **72** (1960), 555–580.

20. G. Shimura, *Moduli and fibre systems of abelian varieties*. Proc. Sympos. Pure Math., vol. 9, Amer. Soc., Providence, R.I., 1966, pp. 312–332.

Fourier–Jacobi Series

BY

WALTER L. BAILY, JR.

It is our purpose here to discuss the so-called Fourier–Jacobi series which are introduced and dealt with by Pyateckiĭ-Shapiro in his book *The geometry of the classical domains and the theory of automorphic functions.* This book will be referred to as PS [**5**].

My discussion is mainly an exposition of some of the ideas related to Fourier–Jacobi series developed in PS, in such language, we hope, as to make clear their relationship to some ideas in [**1**]. Of course, as regards the exceptional domains, we must rely on some of the general results of Korányi and Wolf [**4**] on partial Cayley transforms and Siegel domains of the third kind. However, the latter authors do not concern themselves with Fourier–Jacobi series, and once the main facts on Siegel domains are assumed, the principal ideas are still those of PS.

The main point of original motivation for these developments is to show how some results of Koecher [3] on Siegel modular forms can be extended to the general case of automorphic forms with respect to a fairly broad class of arithmetic discontinuous groups. Specifically, let $G_{\boldsymbol{C}}$ be a centerless, connected, linear algebraic group defined over $\boldsymbol{Q}$ which is $\boldsymbol{Q}$-simple, such that $G_{\boldsymbol{R}}^0$ has no compact simple factors, and such that $X = K\backslash G_{\boldsymbol{R}}^0$ is Hermitian symmetric (K is a maximal compact group in $G_{\boldsymbol{R}}^0$) and therefore equivalent to a bounded symmetric domain D. Suppose $\dim G > 3$ and suppose F is a proper rational boundary component of $\bar{D}$. Let f be a holomorphic automorphic form of some even weight on D with respect to some arithmetic subgroup Γ of $G_{\boldsymbol{R}}^0$. Then in a certain natural sense, f has an extension to F. It is not our purpose here to discuss the precise manner in which, in the topology $\mathscr{T}_0$ (see [**1**]), f becomes a cross-section of some coherent sheaf and such questions are left to the taste of the reader.

1. **Cylindrical sets.** As before, we choose in $G_{\boldsymbol{C}}$ a maximal $\boldsymbol{Q}$-trivial torus S, a maximal $\boldsymbol{R}$-trivial torus ${}_{\boldsymbol{R}}T$, and a maximal $\boldsymbol{Q}$-torus T with $S \subset {}_{\boldsymbol{R}}T \subset T$, and denote by ${}_{\boldsymbol{Q}}\Phi$, ${}_{\boldsymbol{R}}\Phi$, and Φ the respective root systems. Choosing compatible orderings on these, we let ${}_{\boldsymbol{Q}}\Delta = \{\beta_1, \cdots, \beta_s\}$, ${}_{\boldsymbol{R}}\Delta = \{\alpha_1, \cdots, \alpha_t\}$, and Δ be the respective sets of simple roots. (As before, it is not necessary to assume $G_{\boldsymbol{C}}$ to be absolutely simple, and if we appeal to such an assumption in what follows, it is only to simplify the discussion, and not for any intrinsic reason.) Let b be fixed, $1 \leq b \leq s$, and let F_b be the standard rational boundary component defined in

previous lectures. Then[1] $N(F_b)_{\mathbf{C}} = P_b = R \cdot U$, where U is the unipotent radical of P_b and R is a reductive complement which may be taken as $A \cdot B \cdot S_b$, where S_b is the one-dimensional, central, $\mathbf{Q}$-trivial torus in R, A and B are defined over $\mathbf{Q}$, $A_{\mathbf{R}}$ contains all the simple factors in $R_{\mathbf{R}}$ acting nontrivially on F_b, while $(B \cdot S)_{\mathbf{R}} \subset Z_b$ and $(B \cdot S \cdot U)_{\mathbf{R}} \backslash Z_b$ is compact.

We recall some facts from [**1**, §3] and from PS about $S_b = \zeta(G \cdot c_b)$ (which are true even if $G_{\mathbf{C}}$ is not irreducible). Let W be the center of $U, E = W_{\mathbf{R}} \backslash U_{\mathbf{R}}$, and identify the Abelian, connected, simply-connected Lie groups W and E with their Lie algebras once and for all. V is a convex cone contained in N_2 and $W = N_2 + iN_2$, E and W are supplied with certain complex structures, that of E depending on t, for each $t \in D_b$, and a certain quasi-(V-)Hermitian mapping $L_t : E \times E \to W$. Then

$$(1) \qquad S_b = \{(z, u, t) \in W \times E \times D_b | t \in D_b,\ \operatorname{Im} z - \operatorname{Re} L_t(u, u) \in V\}.$$

A cylindrical set $S(Q, r)$ in S_b is defined in S_b by PS as follows: Let Q be a compact subset of D_b, let $r \in V$, and define

$$(2) \qquad S(Q, r) = \{(z, u, t) \in S_b | t \in Q,\ \operatorname{Im} z - \operatorname{Re} L_t(u, u) - r \in V\}.$$

By pp. 28–29 of PS, the function $\operatorname{Im} z - \operatorname{Re} L_t(u, u)$ is invariant under $U_{\mathbf{R}}$. Hence, $S(Q, r) \cdot U_{\mathbf{R}} = S(Q, r)$. We supply N_2 with a partial ordering by: $x_1 > x_2$ if $x_1 - x_2 \in V$. The cylindrical sets are used in PS in defining a topology for D^*/Γ. This topology is at least as coarse as the topology $\mathscr{T}_0$ (q.v. [**1**]), as indicated by the Lemma given shortly below. First, we must "invert" our usual truncated Siegel sets. With $t, \eta, \omega, E, \lambda$ given as in the discussion of the latter, let $\mathfrak{S}^*_{t,\eta,\omega}(E, \lambda)$ be the set defined by all the same inequalities as those defining $\mathfrak{S}_{t,\eta,\omega}(E, \lambda)$ *except* that in giving the restrictions prescribed by t and λ on the simple roots we precisely reverse the signs of all exponents of e as well as all signs of inequality (so ${}_{\mathbf{Q}}A_t^* = \{a \in {}_{\mathbf{Q}}A | \beta(a) > e^{-t},\ \beta \in {}_{\mathbf{Q}}\Delta\}$, and we want $\beta_b(a) > e^{\lambda}, \lambda \to +\infty$). Then we have:

LEMMA. *Let $t \in \mathbf{R}$, $\omega \subset {}_{\mathbf{Q}}N_{\mathbf{R}}$, $\eta \subset {}_{\mathbf{Q}}M_{\mathbf{R}}$ be given with ω and η both relatively open and relatively compact. Let Q and r be given as above. Then there exist E and λ such that $\mathfrak{S}^*_{t,\eta,\omega}(E, \lambda) \subset S(Q, r)$.*

We omit most of the proof except to remark that it is significantly simplified by the observation that $\operatorname{Im} z - \operatorname{Re} L_t(u, u)$ is invariant under $U_{\mathbf{R}}$ and hence we may take $u = 0$ and therefore $L_t(u, u) = 0$ throughout our argument. The rest of the details are left to the thoughtful reader.

2. **The skew-symmetric form Q.** We identify W and E with their Lie algebras. Then (see PS) the group extension $U_{\mathbf{R}}$ of E by $W_{\mathbf{R}}$ is defined by the multiplication rule

$$(3) \qquad (e, w) \times (e', w') = (e + e', w + w' + Q(e, e')),$$

[1] P_b was $P_{b,\mathbf{C}}$ in [**1**].

where Q is a nondegenerate skew-symmetric bilinear mapping of $E \times E$ into W. The nondegeneracy of Q follows from that of L_t (for every t) mentioned in **[1]**. Γ is a subgroup of $G_{\mathbf{R}}^0$ commensurable with $G_{\mathbf{Z}}$. Since U and W, and hence E, are all defined over $\mathbf{Q}$, it follows that $U_\Gamma = U \cap \Gamma$, $W_\Gamma = W \cap \Gamma$, and $E_\Gamma = W_\Gamma \backslash U_\Gamma$ are respectively lattices in $U_{\mathbf{R}}$, in $W_{\mathbf{R}}$, and in E. Then Q has the further evident property (because U_Γ is a group) that $2Q(E_\Gamma \times E_\Gamma) \subset W_\Gamma$.

3. **Automorphic forms.** Let f be a holomorphic, automorphic form of weight $2k$ on S_b with respect to Γ. For $\gamma \in U_F$, $f(x\gamma) = f(x)$, $x \in S_b$, because $J_b(x, \gamma)^{2k} = 1$. In particular this is true for $\gamma \in W_\Gamma$. We denote the lattice W_Γ by $\Lambda, \Lambda \subset N_2$. Then f has a Fourier expansion:

$$f(x) = f(z, u, t) = \sum_{\rho \in \Lambda'} \psi_\rho(u, t)\varepsilon(\langle \rho, z \rangle), \tag{4}$$

where $\langle\ \rangle$ is some Euclidean inner product on W mapping $N_2 \times N_2$ into N_2, Λ' is the dual lattice of Λ with respect to $\langle\ \rangle$, and $\varepsilon(\ ) = e^{2\pi i(\ )}$. Since $f(x\gamma) = f(x)$ for $\gamma \in U_\Gamma, x \in S_b$, one may prove, using the uniqueness of the Fourier coefficients ψ_ρ in (4), that for $(e, w) \in U_\Gamma$ we have

$$\psi_\rho(u + e(t), t) = \varepsilon(-\langle \rho, w + 2iL_t(u, e(t)) + iL_t(e(t), e(t))\rangle)\psi_\rho(u, t) \tag{5}$$

(where, in the coordinates of S_b, (e, w) is represented by the transformation:

$$\begin{aligned} & t \to t, \\ & u \to u + e(t), \\ & z \to z + w + 2iL_t(u, e(t)) + iL_t(e(t), e(t)), \end{aligned} \tag{6}$$

and $e(t)$ is the complex vector representing e in the complex structure on E associated to t). For fixed t, the equations (5) for all $(e, w) \in U_\Gamma$ imply that $\psi_\rho(u, t)$ is a θ-function of u with period lattice $\{e(t)\}$ depending on t. If $\rho = 0$, we have $\psi_0(u + e(t), t) = \psi_0(u, t)$, hence by Liouville's theorem ψ_0 is independent of u. For other values of ρ, the existence of θ-functions $\psi_\rho \not\equiv 0$ satisfying (5) depends exactly on the Riemann conditions. As is shown on pp. 138–140 of PS, one part of the Riemann conditions is expressed by the condition $2Q(E_\Gamma \times E_\Gamma) \subset W_\Gamma$, which was mentioned at the end of §2, and the other part by the requirement that a certain Hermitian matrix be nonnegative semidefinite, which is finally reduced in terms of ρ to the requirement

$$\langle \rho, L_t^{(2)}(u, u)\rangle \geq 0 \tag{7}$$

for all $u \in E$, where $L_t^{(2)}$ is the Hermitian part of L_t. It follows from the nondegeneracy of L_t that the real, positive convex hull of the vectors $L_t^{(2)}(u, u)$ is just $\bar{V}$, and hence (7) becomes the requirement that $\rho \in \bar{V}'$, where V' is the dual cone of V, of which the closure is defined by

$$\bar{V}' = \{y \in N_2 | \langle y, v\rangle \geq 0, v \in V\}.$$

Hence, we may write, if $\dim E > 0$,

$$f(z, u, t) = \sum_{\rho \in \Lambda' \cap \overline{V}'} \psi_\rho(u, t)\varepsilon(\langle \rho, z \rangle).$$

If $\dim E = 0$, i.e., if U is Abelian, it is easy to see that for a proper rational boundary component F_b we must have $\dim F_b = 0$, i.e., $b = s$ and F_s is a point. In this case, all ψ_ρ are constant, and we may write

$$f(z) = \sum_{\rho \in \Lambda'} C_\rho \varepsilon(\langle \rho, z \rangle),$$

where all C_ρ are constants. We fix a point $y_0 \in V$. Then we must have that $\sum C_\rho \varepsilon(\langle \rho, iy_0 + x \rangle) = g(x)$ converges uniformly for x in any compact set. Integrating $|g(x)|^2$ over a period parallelepiped of Λ', we get

$$\sum |C_\rho|^2 e^{-4\pi\langle \rho, y_0 \rangle} < +\infty. \tag{8}$$

Suppose $\rho_0 \notin \overline{V}'$, and denote by M_0 the set all $\rho = \rho_0 \gamma'_\beta, \gamma_\beta \in \boldsymbol{B_R} \cap \Gamma$, where γ'_β is the adjoint of γ_β with respect to $\langle\,,\rangle$. For $\gamma_\beta \in \boldsymbol{B_R} \cap \Gamma, f(z\gamma_\beta) = f(z)$, and so $C_{\rho\gamma'_\beta} = C_\rho$. Therefore, $|C|^2 \sum_{\rho \in M_0} \exp(-4\pi\langle \rho, y_0 \rangle) < +\infty$, where C is the common value of all $C_{\rho\gamma'_\beta}$. Since $\dim G > 3$, $\dim V > 1$, and so $\dim \boldsymbol{B_R} > 0$. Moreover B is defined over $\boldsymbol{Q}$, has no rational characters defined over $\boldsymbol{Q}$, and so $\boldsymbol{B_R}/(\Gamma \cap \boldsymbol{B_R})$ has finite volume. But $\boldsymbol{B_R}$ is not compact, and in fact one can, e.g. by a case-by-case examination of homogeneous cones, find a one-parameter group $\beta(\tau), \tau \in \boldsymbol{R}$, in $\boldsymbol{B_R}$ such that for suitable fixed $y_0 \in V$ we have

$$\lim_{\tau \to +\infty} \langle \rho_0, y_0\beta(\tau) \rangle = -\infty.$$

By the density properties [2] of $\Gamma \cap \boldsymbol{B_R}$ in $\boldsymbol{B_R}$, we can for any pre-assigned small neighborhood N of the identity in $\boldsymbol{B_R}$, find sequences $\tau_1, \tau_2, \cdots \to +\infty$ in $\boldsymbol{R}$, $\{a_n\}$ and $\{b_n\}$ in N, such that $a_n\beta(\tau_n)b_n = \gamma_n \in \Gamma \cap \boldsymbol{B_R}$. If we take N small enough, we can obtain, finally, that $\lim_{n \to +\infty} \langle \rho_0, y_0\gamma_n \rangle \to -\infty$, which contradicts the convergence of (8), unless $C = 0$.

Hence, in all cases we have, if $\dim G > 3$,

$$f(z, u, t) = \sum_{\rho \in \Lambda' \cap \overline{V}'} \psi_\rho(u, t)\varepsilon(\langle \rho, z \rangle). \tag{9}$$

Now PS shows (Lemma 2, p. 119 of PS) that such a function has an absolute majorant on any part $S(Q, r, K_0)$ of a cylindrical set $S(Q, r)$ where $|u|$ is less than some constant K_0. Let f^* be the sum of all the terms in (9) with $\rho \neq 0$. Then $f^*(x\gamma) = f^*(x)$ for $\gamma \in U_\Gamma$, $|f^*|$ is bounded in $S(Q, r, K_0)$, and hence on all of $S(Q, r)$ by translation by elements of U_Γ, if we choose K_0 so large that the set $\{|u| < K_0\}$ contains a period parallelogram of the lattice of vectors $e(t), (e, w) \in U_\Gamma$, for all $t \in Q$ (Q being relatively compact). Moreover, we can make $|f^*|$ arbitrarily small in $S(Q, r, K_0)$ by choosing r large in the partial ordering on N_2 mentioned previously. Hence $f \to \psi_0$ as $r \nearrow \infty$ in this partial ordering, i.e., $\lim_{x \to t \in F_b} f(x) = \psi_0(t)$. (One still needs to check the effect of translating Siegel domains by some elements of $N(F_b)_Q$, but this is not serious, because then we are still discussing the limit of an automorphic form with respect to some other arithmetic discontinuous group.) Therefore, the limit of f on F_b is ψ_0, i.e., in the notation of the Φ operator [**1**], $\Phi_{F_b}f = \psi_0$, which is an automorphic form with respect to some arithmetic discontinuous group on F_b. This is true for any rational boundary component (the "standard" boundary components are such only by the choice of S, and any rational boundary component is "standard" with respect to a suitable S and suitable ordering on ${}_Q\Phi$). Thus every modular form is an "integral modular form" if $\dim G > 3$.

References

1. Walter L. Baily, Jr., *On compactifications of orbit spaces of arithmetic discontinuous groups acting on bounded symmetric domains*, Proc. Sympos. Pure Math., vol. 9, Amer. Math. Soc., Providence, R.I., 1966, pp. 281–295.

2. A Borel, *Density properties for certain subgroups of semi-simple groups without compact components*, Ann. of Math. (2) **72** (1960), 179–188.

3. M. Koecher, *Zur Theorie der Modulformen n-ten Grades*. I, Math. Z., **59** (1954), 399–416.

4. A. Korányi and J. Wolf, *Generalized Cayley transformations of bounded symmetric domains*, Amer. J. Math. **87** (1965), 899–939.

5. I. I. Pyateckiĭ-Shapiro, *Geometry of the classical domains and the theory of automorphic functions*, Fīzmatgiz, Moscow, 1961. (Russian).

On the Desingularization of Satake Compactifications

BY

JUN-ICHI IGUSA

1. **The problem of desingularization.** Let X denote a subdomain in a complex vector space which is complex-analytically isomorphic to a bounded symmetric domain. It is known that there exists a semisimple, linear algebraic group G' defined over $\boldsymbol{Q}$ such that the identity component of the Lie group of complex-analytic automorphisms of X is isomorphic to the quotient group of the identity component G of $G'_{\boldsymbol{R}}$ by a finite central subgroup. Denote by $\mathscr{C}$ the set of all subgroups Γ of G which are commensurable with the group $G_{\boldsymbol{Z}}$. If we denote by $G_{\boldsymbol{Z}}(l)$ the *principal congruence group* of level l, it is a member of $\mathscr{C}$ for $l = 1, 2, \cdots$.

Now, after Baily and Borel [**1**], we know how to construct the so-called *Satake compactification* $\mathscr{S}(\Gamma)$ of the quotient variety X/Γ for every Γ in $\mathscr{C}$. In the first place, $\mathscr{S}(\Gamma)$ has the structure of a normal projective variety in which X/Γ is Zariski-open. Furthermore, if Γ is contained in Γ', there exists a morphism $\mathscr{S}(\Gamma) \to \mathscr{S}(\Gamma')$, which is a covering (in the sense that it is proper and the fiber over each point of $\mathscr{S}(\Gamma')$ is a nonempty finite set). If Γ' is contained in Γ'', the composite morphism $\mathscr{S}(\Gamma) \to \mathscr{S}(\Gamma') \to \mathscr{S}(\Gamma'')$ is the same as the morphism $\mathscr{S}(\Gamma) \to \mathscr{S}(\Gamma'')$. A point of a normal analytic space is called *almost nonsingular* if it possesses a neighborhood which admits a nonsingular covering. If all points are almost nonsingular, the space is called almost nonsingular. While every point of X/Γ is almost nonsingular, we shall see that, in general, all points of $\operatorname{bd}\mathscr{S}(\Gamma) = \mathscr{S}(\Gamma) - X/\Gamma$ are *not* almost nonsingular. This is a serious matter if one wants to investigate geometry on$\mathscr{S}(\Gamma)$.

The problem of desingularization is to find another compactification of X/Γ which has less complicated singularities. More precisely, one seeks for every Γ in $\mathscr{C}$ a normal projective variety $\mathscr{D}(\Gamma)$ which contains X/Γ as a Zariski-open set and such that $\mathscr{D}$ satisfies the following conditions:

(0) $\mathscr{D}$ has the functorial properties similar to those of $\mathscr{S}$;

(1) For every Γ in $\mathscr{C}$, there exists a morphism $\mathscr{D}(\Gamma) \to \mathscr{S}(\Gamma)$ which is an isomorphism over X/Γ and which commutes with the covering morphisms induced by inclusions;

(2) There exists an l_0 such that $\mathscr{D}(G_{\boldsymbol{Z}}(l))$ is nonsingular for $l \geqq l_0$,

(2′) For every Γ in $\mathscr{C}$, there exists a subgroup Γ' of Γ in $\mathscr{C}$ such that $\mathscr{D}(\Gamma')$ is nonsingular,

(2″) $\mathscr{D}(\Gamma)$ is almost nonsingular for every Γ.

The condition (2) in general implies the condition (2′) and (2′) implies the condition (2″). Since we are still at an experimental stage, it is premature to make any general conjecture. However, it is probable that a good solution exists at least in the case when $G = \mathrm{Sp}(g, \boldsymbol{R})$.

REMARK 1. If $\mathscr{D}(\Gamma_0)$ is known for some Γ_0 in $\mathscr{C}$, then $\mathscr{D}$ is uniquely determined by the conditions (0) and (1). In fact, $\mathscr{D}(\Gamma)$ will be obtained from $\mathscr{D}(\Gamma_0)$ by the processes of taking a derived normal model and of taking a quotient variety by a finite group.

REMARK 2. It is almost certain that we can not make $\mathscr{D}(\Gamma)$ nonsingular for every small Γ. In fact, according to Abhyankar, an algebraic function field and its finite algebraic extension do *not* in general possess nonsingular projective models such that one is a covering of the other. This shows also that our desingularization problem, even in the above loosely defined form, is not solved by the desingularization theorem of Hironaka.

2. **Partial desingularization.** Let $\mathscr{F}$ denote an irreducible component of $\mathrm{bd}\,\mathscr{S}(\Gamma)$ with points belonging to all other irreducible components removed. Let F denote a boundary component of X in the sense of Pyatetski–Shapiro which projects to $\mathscr{F}$. Put

$N(F)$ = normalizer of F, $\quad$ $Z(F)$ = centralizer of F,

$U(F)$ = identity component of the unipotent radical of $N(F)$ or of $Z(F)$,

cent $U(F)$ = center of $U(F)$.

We know that cent $U(F)$ is isomorphic to a vector space over $\boldsymbol{R}$ and that the quotient group $U(F)/\mathrm{cent}\, U(F)$ is isomorphic to an even dimensional vector space over $\boldsymbol{R}$. The following theorems can be proved:

THEOREM 1. *The Satake compactification* $\mathscr{S}(\Gamma)$ *is not almost non-singular at any point of the closure of* $\mathscr{F}$ *provided that* (1) Γ *operates without fixed points on* X *and* (2) $\dim U(F) \geqq 2$ *and* $\dim(U(F)/\mathrm{comt}\, U(F)) \geqq 1$, *in which* comt $U(F)$ *denotes the commutator group of* $U(F)$.

THEOREM 2. *Suppose that* $\dim \mathrm{cent}\, U(F) = 1$, i.e., *suppose that* F *is a maximal boundary component of* X. *Then* $\mathscr{S}(\Gamma)$ *can be desingularized along* $\mathscr{F}$ *to an almost nonsingular analytic space which is projective over the subset* $X/\Gamma \cup \mathscr{F}$ *of* $\mathscr{S}(\Gamma)$. *Moreover, if a point* t_0 *of* F *is not a fixed point of* $N(F)_\Gamma/Z(F)_\Gamma$, *the fiber over the projection to* $\mathscr{F}$ *of* t_0 *is a generalized Kummer variety.*

One may call them "singularity theorem" and "partial desingularization theorem" respectively. The singularity theorem can be stated more generally, and it will cover all known results obtained in special cases. On the other hand, the fiber in the partial desingularization theorem can be described as follows. For every t in F, there exists an isomorphism ϕ_t over $\boldsymbol{R}$ of $U(F)/\mathrm{cent}\, U(F)$ to a complex vector space. The map ϕ_t carries $U(F)_\Gamma/\mathrm{cent}\, U(F)_\Gamma$ to a lattice, and this gives rise to a complex torus $\mathscr{A}_t$ which turns out to be a polarized abelian variety. The quotient group $Z(F)_\Gamma/U(F)_\Gamma$ operates on $\mathscr{A}_t$ as a group of automorphisms, and the corresponding quotient variety is the generalized Kummer variety. We refer to (4) for further details.

3. **The Siegel case** $G = \mathrm{Sp}(g, \boldsymbol{R})$. In the case when $G = \mathrm{Sp}(g, \boldsymbol{R})$ and $G_{\boldsymbol{Z}} = \mathrm{Sp}(g, \boldsymbol{Z})$, we shall use the familiar notations $\Gamma_g(l), \mathfrak{S}_g$ instead of $G_{\boldsymbol{Z}}(l), X$. We shall exclude the trivial case $g = 1$. Then the singularity theorem implies that $\mathscr{S}(\Gamma_g(l))$ is *not* almost nonsingular at every point of bd $\mathscr{S}(\Gamma_g(l))$ except for the case when $(g, l) = (2, 1), (2, 2)$. We note that the singular locus of $\mathscr{S}(\Gamma_g(l))$ was determined also by Christian [2]. On the other hand, the structure of $\mathscr{S}(\Gamma_g(l))$ is completely known in those two cases, and it is almost nonsingular [3]. A good desingularization functor $\mathscr{D}$ was obtained in the case $g = 2$ in the following way. First of all, bd $\mathscr{S}(\Gamma_2(1)) = \mathscr{F} \cup \mathscr{F}_0$ is a projective line over $\boldsymbol{C}$, simply $P_1(\boldsymbol{C})$, where $\mathscr{F}$ is an affine line over $\boldsymbol{C}$ and $\mathscr{F}_0$ is a single point. The partial desingularization of $\mathscr{S}(\Gamma_2(1))$ along $\mathscr{F}$ is a monoidal transformation along $\mathscr{F}$ except at the two points corresponding to fixed points of the elliptic modular group. These are the singular points of $\mathscr{S}(\Gamma_2(1))$ carried by $\mathscr{F} \cup \mathscr{F}_0$. We tentatively defined $\mathscr{D}(\Gamma_2(1))$ by extending the partial desingularization as a monoidal transformation along $\mathscr{F} \cup \mathscr{F}_0$ in the neighborhood of $\mathscr{F}_0$. We then extended $\mathscr{D}$ to all Γ in $\mathscr{C}$ by Remark 1, and were able to show that $\mathscr{D}$ satisfies the conditions (0), (1) and (2) for $l_0 = 2$. It was then discovered that the morphism $\mathscr{D}(\Gamma_2(l)) \rightarrow \mathscr{S}(\Gamma_2(l))$ is a monoidal transformation along the singular locus of $\mathscr{S}(\Gamma_2(l))$ for $l \geqq 2$.

Encouraged by this situation, we have investigated the *monoidal transformation* $\mathscr{M}(\Gamma_g(l)) \rightarrow \mathscr{S}(\Gamma_g(l))$ for $\lambda \geqq 3$ along the singular locus bd $\mathscr{S}(\Gamma_g(l))$ of $\mathscr{S}(\Gamma_g(l))$. We note that this is the blowing up of $\mathscr{S}(\Gamma_g(\lambda))$ with respect to the coherent sheaf of ideals defined by all *cusp forms*. The main theorem we have obtained in this way can be stated in the following way:

THEOREM 3. *Decompose g as $g = g_0 + g_1$. Then the point ω of $\mathscr{M}(\Gamma_g(l))$ which corresponds to a sequence in $\mathfrak{S}_g$ with a typical term*

$$\tau = \begin{pmatrix} t & z \\ {}^t z & w \end{pmatrix} \qquad (t \in \mathfrak{S}_{g_0})$$

such that t, z converge to t_0, z_0, say, while $\mathrm{Im}(w) \rightarrow \infty$ *under the restriction that*

$$\mathrm{Im}(w)_{ij}\,(i \neq j), \qquad -\sum_{j=1}^{g_1} \mathrm{Im}(w)_{ij}$$

bounded above, is simple. Furthermore, local coordinates at t_0, z_0 and

$$e((1/l)(-w_{ij})) \quad (1 \leqq i < j \leqq g_1)$$

$$e\left((1/l) \sum_{j=1}^{g_1} w_{ij}\right) \quad (1 \leqq i \leqq g_1)$$

form a set of analytic local coordinates of $\mathscr{M}(\Gamma_g(l))$ at ω.

COROLLARY. *The projection to $\mathscr{S}(\Gamma_g(l))$ of the singular locus of $\mathscr{M}(\Gamma_g(l))$ is precisely the union of the images in $\mathscr{S}(\Gamma_g(l))$ of the rational boundary components of $\mathfrak{S}_g$ whose genus g_0 is smaller than $g - 3$.*

In particular, $\mathscr{M}(\Gamma_g(l))$ is nonsingular not only for $g = 2$ but also for $g = 3$. In this case, we can show that the functor $\mathscr{D}$ defined by $\mathscr{D}(\Gamma_3(l)) = \mathscr{M}(\Gamma_3(l))$ for any $l \geqq 3$ is independent of λ, and it satisfies the conditions (0), (1) and (2) for $l_0 = 3$. Therefore, the problem of desingularization is solved for $g \leqq 3$.

REMARK 3. The morphism $\mathscr{D}(\Gamma) \rightarrow \mathscr{S}(\Gamma)$ is not, in general, a monoidal transformation. In fact, for Γ' contained in Γ, we do not have a natural covering morphism $\mathscr{M}(\Gamma') \rightarrow \mathscr{M}(\Gamma)$, not even a morphism (if $\mathscr{M}(\Gamma')$, $\mathscr{M}(\Gamma)$ denote monoidal transforms of $\mathscr{S}(\Gamma')$, $\mathscr{S}(\Gamma)$). Also $\mathscr{D}(\Gamma)$ is almost nonsingular but, in general, it has singularity (cf. Remark 2).

About the *fibers* of $\mathscr{M}(\Gamma_g(l)) \rightarrow \mathscr{S}(\Gamma_g(l))$, we have the following theorem:

THEOREM 4. *The fiber of $\mathscr{M}(\Gamma_g(l)) \rightarrow \mathscr{S}(\Gamma_g(l))$ over the image point of t_0 in $\mathfrak{S}_{g_0}$ is an abelian variety complex-analytically isomorphic to the complex torus*

$$T_{g_0}(t_0) = C^{g_0}/(t_0 1_{g_0})(lZ)^{2g_0}$$

for $g_0 = g - 1$, and an extension of the abelian variety (complex-analytically isomorphic to) $T_{g_0}(t_0)^2$ for $g_0 = g - 2$ by a reducible rational variety composed of

$$(\tfrac{1}{4})l^3 \prod_{p|l} (1 - p^{-2})$$

projective lines $P_1(C)$ meeting three at each one of the

$$(\tfrac{1}{6})l^3 \prod_{p|l} (1 - p^{-2})$$

points just like three coordinate axes in C^3. Moreover, the combinatorial schema of the reducible variety is like edges of a tetrahedron for $l = 3$, a cube for $l = 4$, a dodecahedron for $l = 5$ and of a polyhedral decomposition of the Riemann surface associated with the elliptic modular function field of level l in

$$(\tfrac{1}{2})l^2 \prod_{p|l} (1 - p^{-2})$$

l-gons for $l \geqq 3$.

In the case when $g_0 = g - 3$, we can show that the fiber is an extension of the abelian variety $T_{g_0}(t_0)^3$ by a reducible rational variety which is a union of

$$(\tfrac{1}{24})l^8 \prod_{p|l} (1 - p^{-2})(1 - p^{-3})$$

copies of the monoidal transform of $P_1(C)^3$ along

$$(0, 0, \infty) \cup (0, \infty, 0) \cup (\infty, 0, 0) \cup (\infty, \infty, \infty).$$

Complete proofs of Theorems 3, 4 are contained in [5]. The following references do not include those which will become necessary in proving the results stated in this note.

References

1. W. L. Baily and A. Borel, *Compactifications of arithmetically defined quotients of bounded symmetric domains*, (to appear).

2. U. Christian, *Zur Theorie der Hilbert–Siegelschen Modulfunktionen*, Math. Ann. **152** (1963), 275–341.

3. J. Igusa, *On Siegel modular forms of genus two*, Amer. J. Math. **84** (1962), 175–200; (II), ibid. **86** (1964), 392–412.

4. ———, *On the theory of compactifications*, Summer Institute on Algebraic Geometry. 1964, Lecture Notes.

5. ———, *A desingularization problem in the theory of Siegel modular functions*, (to appear).

Classical Theory of θ-Functions

BY

WALTER L. BAILY, JR.

1. **Introduction and elementary properties.** One of the most direct means of introducing θ-functions is to consider the problem of constructing a projective imbedding of an Abelian variety $A = C^n/L$, where L is some lattice. Of course, L has $2n$, R-independent generators $\omega_1, \cdots, \omega_{2_n} \in C^n$, and these may be taken as the columns of an $n \times 2n$ complex matrix Ω. In order for A actually to be an Abelian variety, Ω must satisfy the Riemann conditions; namely, there must exist a nonsingular, skew-symmetric matrix J with rational entries such that $\Omega J^t\Omega = 0$ and $i^{-1}\bar{\Omega}J^t\Omega > 0$ (i.e., is a positive definite Hermitian matrix). The set of all such matrices J (called principal matrices) is an open cone over the rational numbers, and the choice of a polarization for A amounts to the choice of a (rational) ray in this cone, or (equivalently) to the choice of a distinguished class of projective imbeddings for A. If such a J exists, then by an appropriate choice of coordinates in C^n and an appropriate choice of basis $\omega_1, \cdots, \omega_{2n}$ for L, we may assume Ω and J to take the forms

$$(1) \qquad \Omega = (e^{-1}, Z), \qquad J = \begin{pmatrix} 0 & e \\ -e & 0 \end{pmatrix},$$

where e is a diagonal $(n \times n)$-matrix with diagonal entries $e_1, \cdots, e_n$ such that $e_i | e_{i+1}$, and where Z is a symmetric $n \times n$ complex matrix with positive definite imaginary part, i.e., $Z \in H_n$.

If Ω and J are as above, then it is possible to construct holomorphic functions in C^n which are actually automorphic forms of the lattice L with respect to certain exponential factors of automorphy, and which are called θ-functions. If the factor of automorphy is suitably chosen, then a basis of the corresponding (finite-dimensional) module of θ-functions may be used as the homogeneous coordinates for a projective imbedding of A. In order to simplify things, and without great loss of generality as regards the θ-functions themselves, *we shall assume that e is the $n \times n$ identity matrix E.* Assuming this and taking Ω and J in the standard form (1) given above, let m be a positive integer and let $g, h \in R^n$. Then by a θ-function of the mth order and characteristic (g, h), we mean an entire function θ in C^n which satisfies

$$(2) \qquad \theta(\zeta + Z\lambda_1 + \lambda_2) = \varepsilon\left(-\frac{m}{2}({}^t\lambda_1 Z\lambda_1 + 2{}^t\lambda_1\zeta) + {}^tg\lambda_2 - {}^th\lambda_1\right)\theta(\zeta)$$

for all $\lambda_1, \lambda_2 \in Z^n$, where $\varepsilon(\ ) = e^{2\pi i(\ )}$.

If we expand θ in an appropriate Fourier series, it is seen that the relation (2) implies a recursion relation on the Fourier coefficients from which it follows easily that the number of C-linearly independent θ-functions of the mth order and fixed characteristic is exactly m^n.

If we are interested in fiber systems of Abelian varieties, we must consider the θ-functions as functions of Z, as well as of ζ. In this case, it is useful to normalize the θ-functions of mth order as entire functions on $H_n \times C^n$ which, in addition to (2), also satisfy the heat equation:

$$(3) \qquad \frac{\partial^2 \theta}{\partial \zeta_j \partial \zeta_l} = \frac{4\pi i m}{2 - \delta_{jl}} \frac{\partial \theta}{\partial z_{jl}}, \qquad 1 \leqq j, l \leqq n,$$

where $Z = (z_{ij})_{i,j=1,\cdots,n}$. We now introduce the following "standard" θ-functions of the first order of characteristic (g, h):

$$(4) \qquad \theta[g, h](\zeta, Z) = \sum_{\lambda_1 \in \mathbf{Z}^n} \varepsilon(\tfrac{1}{2}Z[\lambda_1 + g] + {}^t(\lambda_1 + g)(\zeta + h)),$$

where $Z[a] = {}^t aZa$ for any $n \times l$ matrix a. It is easy to verify that the function defined in (4) satisfies (2) (with $m = 1$) and (3). More generally, if m is any positive integer, then a particular basis of the module $\Theta(m; g, h)$ of θ-functions of mth order and characteristic (g, h) is given by the functions:

$$(5) \qquad \theta\left[\frac{g + \mu}{m}, h\right](m\zeta, mZ),$$

where μ runs over a complete system of incongruent integral n-vectors modulo m. If $m \geqq 3$, and if $\theta_\mu, \mu = 1, \cdots, m^n$ is a basis of $\Theta(m; g, h)$, then the functions θ_μ may be taken as the coordinates of a biregular injection of A into the complex projective space $CP^{m^n - 1}$. This is a well-known result of Lefschetz [7] which we refer to as the Lefschetz imbedding theorem. In particular, the functions θ have no common zeros as functions of ζ for each fixed Z; therefore, we see that the functions $\theta[\mu/m, 0](0, Z)$ have no common zeros on H_n. In fact, if one is only interested in this latter property, it is enough to take $m \geqq 2$, as has been remarked in [**4**, p. 233].

2. **Transformation theory.** Using the standardized notation of §1, with $e = E$, etc., we now wish to consider the action of $\mathrm{Sp}(n, \mathbf{Z})$ on the θ-functions. If

$$\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{Sp}(n, \mathbf{Z}), \qquad Z \in H_n, \qquad \text{and} \qquad \zeta \in C^n,$$

we define

$$(6) \qquad \gamma(\zeta, Z) = ({}^t(CZ + D)^{-1}\zeta, (AZ + B)(CZ + D)^{-1}).$$

Then we have the θ-transformation formula:

$$(7) \qquad \theta[g, h](\zeta, Z) = c \cdot e^{-U}\theta[g', h'](\gamma(\zeta, Z)),$$

where $U = \pi i^t\zeta(CZ + D)^{-1}C\zeta$, $c = (\det(CZ + D))^{-1/2}X(\gamma)(\frac{1}{2}\psi_\gamma(g, h))$, $X(\gamma)$ being a root of unity of bounded order, $\psi_r(g, h)$ being an integral quadratic function of g and h such that $\psi_\gamma(0, 0) = 0$, and where

$$g' = \tfrac{1}{2}\delta({}^tDC) + Dg - Ch \qquad \text{and} \qquad h' = \tfrac{1}{2}\delta({}^tBA) - Bg + Ah,$$

$\delta(M)$ denoting for any $n \times n$ matrix M the n-vector made up of the diagonal elements of M. For the proof of this, see [5] and [6]; see also [2, §2] for some of the details in notation more compatible with that used here. In what follows, d_0 will denote a fixed positive integer such that $X(\gamma)^{d_0} = 1$ for all $\gamma \in \mathrm{Sp}(n, Z)$ and such that for some even m_0 with the property that $\theta[\mu/m_0, 0](0, Z)$ have no common zeros, d_0 is divisible by $[\Gamma(1):\Gamma(8m_0^2)]$, where $\Gamma(l)$ denotes the group of all $\gamma \in \mathrm{Sp}(n, Z)$ such that $\gamma \equiv E_{2n} \pmod l$. Put $\Gamma = \Gamma(1) = \mathrm{Sp}(n, Z)$.

3. **θ-functions and modular forms.** Let d be an integer >0 such that $d_0|d$. In the following discussion, we assume g and h to have rational components, and for our more immediate purposes we shall assume g and h to have bounded denominators dividing a fixed positive even integer t (which may vary according to the context). We also assume $m_0|t$.

By a modular form of even weight $2k$ with respect to Γ, we mean a holomorphic function f on H_n such that for all $\gamma \in \Gamma$ and all $Z \in H_n$, we have

$$f(\gamma Z) = \det(CZ + D)^{2k}f(Z), \qquad \gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix}. \tag{8}$$

It follows from (7) that if P is a homogeneous polynomial of degree d in the functions $\theta[g, h](0, Z)(tg, th \in Z^n)$, then P is a modular form of weight $\frac{1}{2}d$ with respect to $\Gamma(8t^2)$. Hence, the homogeneous polynomials of suitable high degree in the "Thetanullwerthe" $\theta[g, h](0, Z)$ are modular forms with respect to some congruence subgroup of Γ.

On the other hand, it follows from the Lefschetz imbedding theorem and from consideration of points of sufficiently high finite order [2] that if $Z_1, Z_2 \in H_n$, then there exist, for some sufficiently large t, polynomials P and P' as above such that $P(Z_1):P'(Z_1) \neq P(Z_2):P'(Z_2)$. (One may also prove, using the Lefschetz imbedding theorem, and the heat equation, that if $t = 6$, then the differentials of the functions $\theta[g, h](0, Z)$ span the dual of the tangent space to every point of H_n.) Let d be as above and let R_d denote the graded ring of polynomials spanned by the monomials of degrees divisible by d in the functions $\theta[g, h](0, Z)$, where the grading is that in which the homogeneous polynomials of degree d are counted as the ring elements of degree 1. Let $R_{d,l}$ be the subring of those elements of R_d satisfying (8) with $k = \frac{1}{4}d$ for $\gamma \in \Gamma(l)$. Clearly $R_{d,l} \supset R_{d,1}$ for all l. By our choice of d and from elementary properties of the polynomial invariants of a finite group of linear transformations (which are an immediate consequence of the fact that the elementary symmetric functions or the elementary power sums of functions without common zeros have again the same property), it follows that the elements of degree one of $R_{d,1}$ have no common zeros. Let $\theta_0, \cdots, \theta_m$ be a basis of the elements of degree one of $R_{d,1}$, and let θ be the mapping [3] with these coordinates of $(H_n/\Gamma)^* = V^*$ into CP^m. By the argument of [**1**, pp. 353–354], we see that θ is nondegenerate everywhere, i.e., $\theta^{-1}(x)$ is at most finite for any point x of CP^m. Therefore, as one sees by an easy argument from algebraic geometry, the ring of modular forms of weights divisible by $d/2$ with respect to $\Gamma(l)$ is integral over $R_{d,l}$ and, for sufficiently large t, is contained in the quotient field of $R_{d,l}$.

For more details on such matters (except for the parenthetical remark about $t = 6$), please see [**2**], especially pp. 380–383, where one considers, more generally, θ-functions associated to a lattice in k^{2p}, where k is a totally real number field. Facts similar to these and in certain nontrivial respects more precise, were also proved independently and utilized by Igusa in his investigation of the structure of the ring of Thetanullwerthe [**4**].

4. **Algebraic dependences among θ-functions.** Let $\theta_1, \cdots, \theta_{m^n}$ be the basis (5) of the module of mth order θ-functions of characteristic (0, 0). Choose the numbering of this basis such that for some fixed Z the ratios $\theta_1/\theta_{n+1}, \cdots, \theta_n/\theta_{n+1}$ are analytically and hence algebraically independent as functions of ζ. Let θ be any other θ_μ. For any positive integer l, the number of monomials of degree l in $\theta_1, \cdots, \theta_{n+1}, \theta$ is

$$\binom{l+n+1}{n+1} = \frac{1}{(n+1)!} l^{n+1} + \cdots,$$

while for fixed Z, the number of linearly independent monomials of degree l is $< cl^n$, where c is a fixed constant depending only on m and n. Choose l such that

$$cl^n < \binom{l+n+1}{n+1}.$$

By construction there is no $Z \in H_n$ such that $\theta_{n+1}(\zeta, Z) \equiv 0$ (as a function of ζ). By consideration of an appropriate functional determinant, it is easy to see that the set of Z for which $\theta_1/\theta_{n+1}, \cdots, \theta_n/\theta_{n+1}$ are analytically independent (as functions of ζ) contains an open subset $\mathcal{O}$ of H_n. Let Z_0 be a point of $\mathcal{O}$ such that the number $N_0 = N(Z_0)$ of linearly independent monomials of degree l in $\theta_1, \cdots, \theta_{n+1}, \theta$ (as functions of ζ, Z_0 being fixed) is maximum in $\mathcal{O}$. Let $m_1, \cdots, m_{N_0}$ be linearly independent monomials of degree l, and let m_{N_0+1} be any other monomial of degree l. Then there exist constants $C_1, \cdots, C_{N_0+1}$ not all zero such that $\sum_{\alpha=1}^{N_0+1} C_\alpha m_\alpha(\zeta; Z_0) = 0$ for all ζ. Of course, $C_{N_0+1} \neq 0$, and we may assume $C_{N_0+1} = 1$. $\sum_1^{N_0} C_\alpha m_\alpha(\zeta, Z_0) \not\equiv 0$ as a function of ζ for any nonzero choice of C_α, so there exist $\zeta_1, \cdots, \zeta_{N_0}$ such that the N_0-vectors $(m_1(\zeta_i, Z_0), \cdots, m_{N_0}(\zeta_i, Z_0))$, $i = 1, \cdots, N_0$, are linearly independent. Put $\zeta_i = Z_0 a_i + b_i, a_i, b_i \in \boldsymbol{R}^n$. We have

$$\det(m_i(Z_0 a_j + b_j, Z_0)) \neq 0,$$

so there exists a neighborhood $U \subset \mathcal{O}$ of Z_0 such that

$$\phi(Z) = \det(m_i(Z a_j + b_j, Z)) \neq 0$$

for $Z \in U$. For each $Z \in U$, there exist $C_\alpha(Z), \alpha = 1, \cdots, N_0 + 1$, not all zero such that

$$\sum_{1}^{N_0+1} C_\alpha(Z) m_\alpha(\zeta, Z) = 0 \qquad \text{for all } \zeta.$$

Since $\phi(Z) \neq 0$ on U, we must have $C_{N_0+1}(Z) \neq 0$ for $Z \in U$ and for any such nontrivial solution $C_1, \cdots, C_{N_0+1}$. Hence we may assume for all $Z \in U$ that $C_{N_0+1}(Z) = 1$. Then, by Kramer's rule, $C_\alpha(Z) = \phi_\alpha(Z)/\phi(Z), \alpha = 1, \cdots, N_0$, where $\phi_\alpha(Z)$ is a polynomial in $m_\alpha(Za_j + b_j, Z)$. Thus, the functions $\phi_\alpha(Z), \alpha = 1, \cdots, N_0$, and $\phi_{N_0+1} = \phi(Z)$ are analytic in all of H_n and $\sum_\alpha C_\alpha(Z) m_\alpha(\zeta, Z)$, being identically zero on $U \times C^n$, is $\equiv 0$ on $H_n \times C^n$. Therefore $\theta_1, \cdots, \theta_{n+1}, \theta$ satisfy a nontrivial algebraic equation of which the coefficients are analytic in all of H_n. Let $\sum b_\alpha(Z) m_\alpha(\zeta, Z) = 0$ be a shortest such equation. We assume $8d_0 | l$. Then for a sufficiently divisible t (i.e., $k! | t$ for large enough k), the monomials $m_\alpha(\zeta, Z)$ all transform by the same factor according to (7) if $\gamma \in \Gamma(t)$. By the hypothesis that the equation is a shortest one, it follows that the ratios $b_\alpha(Z)/b_{\alpha'}(Z)$ are invariant under $\Gamma(t)$. To avoid a special case which must (apparently) be treated differently using the classical theory of elliptic functions, we assume $n > 1$. Then by various results on compactifications [3] it follows that the ratios $b_\alpha(Z)/b_{\alpha'}(Z)$ belong to the field of quotients of integral modular forms.

Now it is known that if $\psi_0, \cdots, \psi_n$ are integral modular forms of a suitable high weight, then the mapping $\Psi : x \to (\psi_0(x) : \cdots : \psi_n(x))$ is an injection of the Satake compactification $V_n(t)^*$ of $\Gamma(t) \backslash H_n = V_n(t)$ (supplied with the natural ringed structure that makes it a normal compact complex analytic space) into CP^n. (See [3].) Let $N = m^n - 1$. Define $\Theta : H_n \times C^n \to CP^N$ by

$$\Theta(\zeta, Z) = [\theta_1(\zeta, Z) : \cdots : \theta_{m^n}(\zeta, Z)],$$

and define $\Phi : H_n \times C^n \to CP^M \times CP^N$ by $\Phi = \Psi \times \Theta$. Let π be the projection of $CP^M \times CP^N$ onto its first factor. Let P be the smallest algebraic subvariety of $CP^M \times CP^N$ containing $\Phi(H_n \times C^n)$. By the result we have just proved on algebraic dependence, $\dim P \leqq n + n(n+1)/2$. Also,

$$\dim P \geqq \dim \Phi(H_n \times C^n) = \dim(H_n \times C^n) = n + \frac{n(n+1)}{2}$$

(because Φ is *locally* a biholomorphic injection). Hence, $\dim P = \dim(H_n \times C^n)$, and, as is now easy to see, $\pi^{-1}(V_n(t)^* - V_n(t)) \cap P = P - \Phi(H_n \times C^n)$, $\Phi(H_n \times C^n)$ is a Zariski-open subset of P, and for $x \in V_n(t)$, $\pi^{-1}(x) \cap P$ is the Abelian variety with period matrix (EZ), Z belonging to the orbit x of $\Gamma(t)$. The fiber system of Abelian varieties just constructed was used in [1] in proving certain facts about the moduli of Abelian varieties.

5. **Cusp forms and θ-functions.** As a closing remark we note the following: If the monomial

$$m = \prod_{i=1}^{d} \theta[g_i, h_i](0, Z)$$

is a modular form with respect to $\Gamma(t)$, and if some g_i has the property that all its components g_{ij}, $j = 1, \cdots, n$, are $\not\equiv 0 \pmod{\boldsymbol{Z}}$, then m tends to zero at all the standard rational boundary components. It is left as an exercise to determine just which such monomials are cusp forms, and which tend to zero on all boundary components of given rank.

References

1. W. L. Baily, Jr., *On the theory of θ-functions, the moduli of Abelian varieties, and the moduli of curves*, Ann. of Math. **75** (1962), 342–381.

2. ———, *On the moduli of Abelian varieties with multiplications*, J. Math. Soc. Japan (4) **15** (1963), 367–386.

3. ———, *On compactifications of orbit spaces of arithmetic discontinuous groups acting on bounded symmetric domains*, Proc. Sympos. Pure Math., vol. 9, Amer. Math. Soc., Providence, R.I., 1966; pp. 281–295.

4. J. Igusa, *On the graded ring of theta-constants*, Amer. J. Math., **86** (1964), 219–246.

5. A. Krazer, *Lehrbuch der Thetafunctionen*, B. G. Teubner, Leipzig, 1903.

6. A. Krazer and F. Prym, *Neue Grundlagen einer Theorie der Allgemeiner Thetafunctionen*, B. G. Teubner, Leipzig, 1903.

7. S. Lefschetz, *On certain numerical invariants of algebraic varieties with application to Abelian varieties*, Trans. Amer. Math. Soc., **22** (1921), 327–482.

Moduli of Abelian Varieties and Number Theory

BY

GORO SHIMURA

There are many arithmetically defined discontinuous groups Γ operating on a bounded symmetric domain S such that S/Γ parametrizes a family of abelian varieties. For such a Γ and S, one can naturally consider a fibre variety of which the base space is S/Γ and the fibres are the abelian varieties of the family. The cohomological or analytical aspects of the theory will be discussed in the lectures of Kuga and Satake (cf. also the articles by Baily and Mumford). Therefore my talk will be confined to the algebro-geometric and number-theoretical aspects. I shall consider a family $\Sigma_\Omega = \{\mathcal{Q}_z | z \in S\}$ of abelian varieties $\mathcal{Q}_z$ with a prescribed type Ω of structures. Here Ω describes the type of polarization, endomorphism-ring and points of finite order on an abelian variety. My main purpose is to provide a brief account of principal results concerning the following three problems.

(i) The existence of a "nice moduli-variety" and a "nice fibre variety" for the family Σ_Ω, defined over a well-defined algebraic number field k_Ω.

(ii) The description of k_Ω as a class-field.

(iii) The Hasse zeta-function of the fibre variety in a special case (collaboration with Kuga).

All the results will be stated without proofs. For the detailed proofs of (i), (ii) and (iii), see **[12]**, **[11]** and **[4]**, respectively. I devote (partly by the chairman's request) the first three sections to an exposition of basic notions and some elementary results on abelian varieties (mostly over C), Riemann forms, and the maximal families of abelian varieties.

1. **Abelian varieties** (cf. **[5]**, **[16]**, **[17]**). A projective variety A defined over a field k of characteristic $p \geqq 0$ is an *abelian variety* if there exist morphisms (of algebraic varieties) $f: A \times A \to A$ and $g: A \to A$ which define a group structure on A by $f(x, y) = x + y, g(x) = -x$. Additive notation is used since any such group structure on a projective variety can be shown to be commutative. The neutral element is accordingly denoted by 0. If f and g are defined over k, then we say that the abelian variety A *is defined over* k. This is so if and only if the neutral element is rational over k.

Let A and B be two abelian varieties defined over k. By a *homomorphism* of A into B, or an *endomorphism* when $A = B$, we shall always understand a morphism λ of A into B, satisfying $\lambda(x + y) = \lambda(x) + \lambda(y)$; if λ is birational, we call it an *isomorphism*, or an *automorphism* when $A = B$. Suppose that A and B have the same dimension. Then a homomorphism λ of A into B is surjective if and only if the kernel of λ is finite. Such a λ is called an *isogeny* of A to B. If there exists an isogeny of A to B, A and B are said to be *isogenous*.

We denote by $\mathrm{Hom}(A, B)$ the module of all homomorphisms of A into B, and put $\mathrm{End}(A) = \mathrm{Hom}(A, A)$, $\mathrm{End}_{\boldsymbol{Q}}(A) = \mathrm{End}(A) \otimes_{\boldsymbol{Z}} \boldsymbol{Q}$. Then $\mathrm{Hom}(A, B)$ is a finitely generated free $\boldsymbol{Z}$-module, and $\mathrm{End}_{\boldsymbol{Q}}(A)$ with a natural structure of ring is a semisimple algebra over $\boldsymbol{Q}$ of finite rank. Moreover it can be shown that $\mathrm{End}_{\boldsymbol{Q}}(A)$ has a positive involution. Here by an *involution* of an algebra L over $\boldsymbol{Q}$, we mean a $\boldsymbol{Q}$-linear map $\rho: L \to L$ such that $(xy)^\rho = y^\rho x^\rho$ and $(x^\rho)^\rho = x$; ρ is said to be *positive* if $\mathrm{Tr}_{L/\boldsymbol{Q}}(xx^\rho) > 0$ for every $x \in L$, $\neq 0$, where $\mathrm{Tr}_{L/\boldsymbol{Q}}$ denotes the reduced trace from L to $\boldsymbol{Q}$. We shall discuss in §4 an explicit way of obtaining a positive involution of $\mathrm{End}_{\boldsymbol{Q}}(A)$ in the case of characteristic 0.

An abelian variety A is said to be *simple* if A and $\{0\}$ are the only abelian subvarieties of A. Every abelian variety is isogenous to a product of simple abelian varieties. An abelian variety A is simple if and only if $\mathrm{End}_{\boldsymbol{Q}}(A)$ is a division algebra.

We shall now consider the case where the universal domain is $\boldsymbol{C}$. Every abelian variety defined over a subfield of $\boldsymbol{C}$, viewed as a complex manifold, is isomorphic to a complex torus. But the converse is not necessarily true. To describe the condition, let $\boldsymbol{C}^n/D$ be a complex torus, with a lattice D in $\boldsymbol{C}^n$ (i.e., a discrete subgroup of $\boldsymbol{C}^n$ of rank $2n$). An $\boldsymbol{R}$-valued $\boldsymbol{R}$-bilinear form $E(x, y)$ on $\boldsymbol{C}^n$ is called a *Riemann form* on $\boldsymbol{C}^n/D$ if it satisfies the following three conditions.

(1.1) *The value $E(x, y)$ is an integer for every $(x, y) \in D \times D$.*

(1.2) $E(x, y) = -E(y, x)$.

(1.3) *The $\boldsymbol{R}$-bilinear form $E(x, \sqrt{(-1)}y)$ in (x, y) is symmetric and positive definite.*

Then one knows that a complex torus has a structure of abelian variety if and only if there exists a Riemann form on it.

Let A be an abelian variety of dimension n defined over a subfield of $\boldsymbol{C}$, and η an isomorphism of A to a complex torus $\boldsymbol{C}^n/D$. The pair $(\boldsymbol{C}^n/D, \eta)$ is called an *analytic coordinate system* of A. Take a basis $\{g_1, \cdots, g_{2n}\}$ of D over $\boldsymbol{Z}$ and define real coordinate functions $x_i: \boldsymbol{C}^n \to \boldsymbol{R}$ by $u = \sum_{i=1}^{2n} x_i(u)g_i$ for $u \in \boldsymbol{C}^n$. Then, given a Riemann form E on $\boldsymbol{C}^n/D$, there exists a divisor X of A such that

$$\sum_{i<j} E(g_i, g_j)\, dx_i \wedge dx_j$$

represents the cohomology class of $\eta(X)$. (A *divisor* of an algebraic variety V is an element of the free $\boldsymbol{Z}$-module formally generated by all the subvarieties of V of codimension one.) In this case we say that X *determines* E (with respect to η). If two divisors X and X' on A determine Riemann forms E and E' respectively, then X is algebraically equivalent to X' if and only if $E = E'$. (If the reader does not know what algebraic equivalence means, he can adopt this as a definition of algebraic equivalence.)

Let A and A' be two abelian varieties with analytic coordinate-systems $(\boldsymbol{C}^n/D, \eta)$ and $(\boldsymbol{C}^m/D', \eta')$ respectively. For every homomorphism $\lambda: A \to A'$ there exists a C-linear mapping $\Lambda: C^n \to C^m$ such that $\Lambda(D) \subset D'$ with the relation $\eta'\lambda = \Lambda\eta$, and conversely every such linear mapping $\Lambda: C^n \to C^m$ corresponds to a homomorphism of A into A'. Assume especially $A = A'$, $(C^n/D, \eta) = (C^m/D', \eta')$. Then the mapping $\lambda \mapsto \Lambda$ is uniquely extended to a representation $\Phi: \mathrm{End}_Q(A) \to \mathrm{End}(C^n)$, which is called the *analytic representation* of $\mathrm{End}_Q(A)$. Further we observe that $Q \cdot D$ is a vector space of dimension $2n$ over Q, and Λ gives an endomorphism of $Q \cdot D$. Therefore, with respect to a basis of $Q \cdot D$ over Q, we get a representation Ψ of $\mathrm{End}_Q(A)$ by matrices of size $2n$ with entries in Q. We call Ψ the *rational representation* of $\mathrm{End}_Q(A)$. Since a basis of $Q \cdot D$ over Q is a basis of C^n over R, it can be easily shown that Ψ is equivalent to the direct sum of the analytic representation Φ and its complex conjugate $\bar{\Phi}$.

2. **Polarized abelian varieties.** Let A be an abelian variety defined over a subfield of C with an analytic coordinate system $(C^n/D, \eta)$. A *polarization* of A is a set $\mathscr{C}$ of divisors of A satisfying the following three conditions.

(2.1) *Every X in $\mathscr{C}$ determines a Riemann form on C^n/D.*

(2.2) *If X and X' are in $\mathscr{C}$, then there exist positive integers m and m' such that mX is algebraically equivalent to (i.e. homologous to) $m'X'$.*

(2.3) *$\mathscr{C}$ is a maximal set of divisors satisfying* (2.1, 2.2). (If the universal domain is not necessarily of characteristic 0, one can define polarization by replacing (2.1) with (2.1′) *$\mathscr{C}$ contains an ample divisor.*) Now a *polarized abelian variety* is a pair $(A, \mathscr{C})$ formed by an abelian variety A and a polarization $\mathscr{C}$ of A. One can find a divisor Y in $\mathscr{C}$ such that every divisor in $\mathscr{C}$ is algebraically equivalent to a multiple hY with a positive integer h. We call Y a *basic divisor* in $\mathscr{C}$.

An isomorphism (resp. isogeny) λ of A to A' is called an *isomorphism* (resp. *isogeny*) of $(A, \mathscr{C})$ to $(A', \mathscr{C}')$ if $\lambda^{-1}(X') \in \mathscr{C}$ for every $X' \in \mathscr{C}'$. If a Riemann form E on a complex torus C^n/D is given, then C^n/D and E determine a polarized abelian variety $\mathscr{P}$ up to isomorphism. Let E' be a Riemann form on another complex torus C^n/D' of the same dimension, and let $\mathscr{P}'$ be a polarized abelian variety determined by C^n/D' and E'. Then an element Λ of $\mathrm{End}(C^n)$ gives an isogeny of $\mathscr{P}$ to $\mathscr{P}'$ if and only if $\Lambda(D) \subset D'$ and $E'(\Lambda x, \Lambda y) = c \cdot E(x, y)$ with a positive rational number c. Now we recall a classical

LEMMA 1 (FROBENIUS). *Let B be an invertible alternating matrix of size $2n$ with entries in Z. Then there exists an element U of $\mathrm{GL}_{2n}(Z)$ such that*

$$ {}^tUBU = \begin{bmatrix} 0 & -e \\ e & 0 \end{bmatrix}, \qquad e = \begin{bmatrix} e_1 & & \\ & \ddots & \\ & & e_n \end{bmatrix}, $$

where the e_i are positive integers satisfying $e_{i+1} \equiv 0 \bmod (e_i)$.

A and $(C^n/D, \eta)$ being as above, let X be a divisor in a polarization $\mathscr{C}$ of A, and let E be the Riemann form determined by X. In view of (1.1) and (1.2), E can be represented by an alternating matrix B with entries in Z, with respect to a basis of D over Z. Applying Lemma 1 to B, we get n integers $e_1, \cdots, e_n$, which may be called *the elementary divisors* of X. Then X is a basic divisor in $\mathscr{C}$ if and only if $e_1 = 1$. Thus we are led to the following definition. Let e be as in Lemma 1 with positive integers $e_1, \cdots, e_n$ such that $e_1 = 1, e_{i+1} \equiv 0 \bmod(e_i)$, and

$$B = \begin{bmatrix} 0 & -e \\ e & 0 \end{bmatrix}.$$

Define an alternating form $B(x, y)$ on $\boldsymbol{R}^{2n}$ by $B(x, y) = {}^txBy$, regarding the elements of $\boldsymbol{R}^{2n}$ as column vectors. A polarized abelian variety $(A, \mathscr{C})$ is said to be of type (e) if there exist a lattice D in $\boldsymbol{C}^n$ and a commutative diagram

(2.4)
$$\begin{tikzcd}
0 \arrow[r] & \boldsymbol{Z}^{2n} \arrow[r] \arrow[d] & \boldsymbol{R}^{2n} \arrow[r] \arrow[d, "f"'] & \boldsymbol{R}^{2n}/\boldsymbol{Z}^{2n} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & D \arrow[r] & \boldsymbol{C}^n \arrow[r, "\xi"] & A \arrow[r] & 0
\end{tikzcd}$$

satisfying the following three conditions:

(2.5) *ξ gives a holomorphic isomorphism of $\boldsymbol{C}^n/D$ to A.*

(2.6) *f is an $\boldsymbol{R}$-linear isomorphism, and $f(\boldsymbol{Z}^{2n}) = D$.*

(2.7) *$\mathscr{C}$ has a basic divisor X which determines a Riemann form $E(x, y)$ on $\boldsymbol{C}^n/D$ such that $E(f(x), f(y)) = B(x, y)$ $((x, y) \in \boldsymbol{R}^{2n} \times \boldsymbol{R}^{2n})$.*

From the above discussion we see that every polarized abelian variety is of type (e) for some unique (e).

3. **Maximal families of abelian varieties.** Let $(A, \mathscr{C})$ be a polarized abelian variety of type (e). Let $\{d_1, \cdots, d_{2n}\}$ be the standard basis of $\boldsymbol{Z}^{2n}$ over $\boldsymbol{Z}$. Regard the elements of $\boldsymbol{C}^n$ as column vectors. Let f be as in the diagram (2.4). Define an $n \times 2n$ matrix w by $w = (f(d_1) \cdots f(d_{2n}))$, and write $w = (u \quad v)$ with square matrices u and v of size n. Put $z = ev^{-1}u$. By a simple calculation we can verify that ${}^tz = z$ and $\mathrm{Im}(z) > 0$ (positive definite). We put

$$S_n = \{z \in M_n(\boldsymbol{C}) | {}^tz = z, \mathrm{Im}(z) > 0\},$$

and call S_n the *Siegel space of degree n*. If we define an element g of $\mathrm{End}(\boldsymbol{C}^n)$ by $g(x) = ev^{-1}x$ for $x \in \boldsymbol{C}^n$, and take $\{\xi \circ g^{-1}, g \circ f, g(D), E(g^{-1}(x), g^{-1}(y))\}$ in place of $\{\xi, f, D, E\}$, then we have a diagram similar to (2.4), and $(g \circ f(d_1) \cdots g \circ f(d_{2n}))$ $= (z \quad e)$. In other words, if $(A, \mathscr{C})$ is of type (e), then we can choose the diagram (2.4) so that $(f(d_1) \cdots f(d_{2n})) = (z \quad e)$ with a point z of S_n.

Conversely, for any $z \in S_n$, define $f_z \colon \boldsymbol{R}^{2n} \to \boldsymbol{C}^n$ by $f_z(a) = f(a, z) = (e \quad z)a$ for $a \in \boldsymbol{R}^{2n}$ and let $D_z = f_z(\boldsymbol{Z}^{2n})$, $E_z(x, y) = B(f_z^{-1}(x), f_z^{-1}(y))$. Then E_z is a Riemann form on $\boldsymbol{C}^n/D_z$, so that we get an abelian variety A_z isomorphic to $\boldsymbol{C}^n/D_z$. Let $\mathscr{C}_z$ be the polarization of A_z determined by E_z, and let $\mathscr{P}_z = (A_z, \mathscr{C}_z)$. Thus we obtain a family $\Sigma_e = \{\mathscr{P}_z | z \in S_n\}$ of polarized abelian varieties of type (e). The above discussion shows that every polarized abelian variety of type (e) is isomorphic to a member of Σ_e. In this sense Σ_e may be called a maximal family of polarized abelian varieties. (For the moment we do not consider any specific projective embeddings of A_z.)

To determine the isomorphism classes of $\mathscr{P}_z$, let

$$P_e = \begin{bmatrix} 1 & 0 \\ 0 & e \end{bmatrix},$$

$$\Gamma'_e = \{T \in \mathrm{GL}_{2n}(Z) \mid {}^tTBT = B\}, \qquad \Gamma_e = \{P_e^{-1} \cdot {}^tTP_e \mid T \in \Gamma'_e\}.$$

Then Γ_e is a discrete subgroup of $\mathrm{Sp}(n, \boldsymbol{R})$ commensurable with $\mathrm{Sp}(n, \boldsymbol{Z})$. If $e = 1_n$, we have $\Gamma_e = \Gamma'_e = \mathrm{Sp}(n, \boldsymbol{Z})$. For an element T of Γ'_e, let

$$P_e^{-1} \cdot {}^tT^{-1}P_e = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

with $a, b, c, d \in M_n(\boldsymbol{R})$, and define the action of T on S_n by $T(z) = (az + b)(cz + d)^{-1}$ for $z \in S_n$. Now two members $\mathscr{P}_z$ and $\mathscr{P}_w$ of Σ_e, with z and w in S_n, are isomorphic if and only if there exists an element T of Γ'_e such that $T(z) = w$. Hence S_n/Γ'_e is in one-to-one correspondence with all the isomorphism classes of polarized abelian varieties of type (e).

4. **Families of abelian varieties with a prescribed type of polarization and endomorphisms.** If A is an abelian variety defined over a subfield of $\boldsymbol{C}$, every polarization $\mathscr{C}$ of A determines a positive involution ρ of $\mathrm{End}_{\boldsymbol{Q}}(A)$ as follows. Take a complex torus $\boldsymbol{C}^n/D$ isomorphic to A. Then $\mathscr{C}$ determines a Riemann form E on $\boldsymbol{C}^n/D$ up to rational factors. If $\phi(\lambda)$ denotes the element of $\mathrm{End}(\boldsymbol{C}^n)$ corresponding to an element λ of $\mathrm{End}_{\boldsymbol{Q}}(A)$, then, for every $\lambda \in \mathrm{End}_{\boldsymbol{Q}}(A)$, there exists an element λ^ρ of $\mathrm{End}_{\boldsymbol{Q}}(A)$ such that

$$E(\phi(\lambda)x, y) = E(x, \phi(\lambda^\rho)y) \qquad ((x, y) \in \boldsymbol{C}^n \times \boldsymbol{C}^n).$$

It can be easily shown that ρ is a positive involution of $\mathrm{End}_{\boldsymbol{Q}}(A)$. Therefore, writing $\mathscr{L}$ for $\mathrm{End}_{\boldsymbol{Q}}(A)$, we see that any polarized abelian variety $(A, \mathscr{C})$ determines a triple $(\mathscr{L}, \phi, \rho)$ formed by a semisimple algebra $\mathscr{L}$ over $\boldsymbol{Q}$, a representation ϕ of $\mathscr{L}$ by complex matrices, and a positive involution ρ of $\mathscr{L}$.

This observation motivates the following problem. Let L be a semisimple algebra over $\boldsymbol{Q}$ with a positive involution ρ, and Φ a representation of L by complex matrices. Determine all families of polarized abelian varieties $(A, \mathscr{C})$ such that: (i) $\mathrm{End}_{\boldsymbol{Q}}(A)$ contains L, (ii) $\mathscr{C}$ gives the involution ρ on L, and (iii) Φ is equivalent to the restriction (to L) of the analytic representation of $\mathrm{End}_{\boldsymbol{Q}}(A)$. Since L or $\mathrm{End}_{\boldsymbol{Q}}(A)$ may have many automorphisms and we shall deal with many distinct A's, it is convenient to take L outside $\mathrm{End}_{\boldsymbol{Q}}(A)$, and specify an isomorphism of L into $\mathrm{End}_{\boldsymbol{Q}}(A)$. To be more precise, we say that a triple $\mathscr{P} = (A, \mathscr{C}, \theta)$ is a polarized abelian variety of type $\{L, \Phi, \rho\}$, or more briefly, $\mathscr{P}$ belongs to $\{L, \Phi, \rho\}$, if the following three conditions are satisfied:

(4.1) *A is an abelian variety defined over a subfield of $\boldsymbol{C}$.*

(4.2) *θ is an isomorphism of L into* $\mathrm{End}_{\boldsymbol{Q}}(A)$*; if ψ is the analytic representation of* $\mathrm{End}_{\boldsymbol{Q}}(A)$*, then $\psi \circ \theta$ is equivalent to Φ.*

(4.3) *$\mathscr{C}$ is a polarization of A; and the involution of* $\mathrm{End}_{\boldsymbol{Q}}(A)$ *determined by $\mathscr{C}$ coincides on $\theta(L)$ with the involution $\theta(a) \mapsto \theta(a^\rho)$.*

In the following treatment, we always assume

(4.4) *Φ maps the identity element of L to the identity matrix,*

(4.5) *L is a division algebra,*

though a more general case is worth while considering. If n is the degree of Φ, (4.4) implies $\dim(A) = n$.

The representation Φ cannot be arbitrary in order to ensure the existence of a polarized abelian variety of type $\{L, \Phi, \rho\}$. In fact, if $(A, \mathscr{C}, \theta)$ belongs to $\{L, \Phi, \rho\}$, then the rational representation of $\mathrm{End}_{\boldsymbol{Q}}(A)$ induces a rational representation of L of degree $2n$, equivalent to the sum of Φ and $\bar{\Phi}$, where $n = \dim(A)$. Therefore $\Phi + \bar{\Phi}$ must contain all the absolutely irreducible representations of L with the same multiplicity. In view of (4.5), $[L:\boldsymbol{Q}]$ must divide $2n$.

Now we shall determine the polarized abelian varieties of type $\{L, \Phi, \rho\}$. Let $(A, \mathscr{C}, \theta)$ belong to $\{L, \Phi, \rho\}$. Take a complex torus $\boldsymbol{C}^n/D$ isomorphic to A. By the action of $\Phi(L)$, $\boldsymbol{Q} \cdot D$ can be considered as an L-module, whose rank is obviously $2n/[L:\boldsymbol{Q}]$. Let us take and fix a (left) L-module V of rank m, where $m = 2n/[L:\boldsymbol{Q}]$. Then there is an L-isomorphism $f\colon V \to \boldsymbol{Q} \cdot D$. Put $\mathfrak{M} = f^{-1}(D)$. Then $\mathfrak{M}$ is a free $\boldsymbol{Z}$-module of rank $2n$ in V. Let X be a divisor in $\mathscr{C}$, and E the Riemann form on $\boldsymbol{C}^n/D$ determined by X. Put $B(x, y) = E(f(x), f(y))$ for $(x, y) \in V \times V$. Then $B\colon V \times V \to \boldsymbol{Q}$ is a $\boldsymbol{Q}$-bilinear form satisfying

$$(4.6)\qquad B(x, y) = -B(y, x), B(ax, y) = B(x, a^\rho y) \qquad (x, y \in V; a \in L).$$

If X is a basic divisor of $\mathscr{C}$, we have $B(\mathfrak{M}, \mathfrak{M}) = \boldsymbol{Z}$.

LEMMA 2. *Let L be a division algebra over $\boldsymbol{Q}$ with an involution ρ, V a left L-module, and $B\colon V \times V \to \boldsymbol{Q}$ a $\boldsymbol{Q}$-bilinear form satisfying* (4.6). *Then there exists a $\boldsymbol{Q}$-bilinear map $T\colon V \times V \to L$ such that*

$$(4.7)\qquad B(x, y) = \mathrm{Tr}_{L/\boldsymbol{Q}}(T(x, y)),$$

$$(4.8)\quad T(x, y)^\rho = -T(y, x), \quad T(ax, by) = a \cdot T(x, y) \cdot b^\rho \qquad (x, y \in V; a, b \in L)$$

A $\boldsymbol{Q}$-bilinear map $T: V \times V \to L$ is called an *L-valued ρ-antihermitian form* on V if it satisfies (4.8). We apply this lemma to the above $\boldsymbol{Q}$-bilinear form B and obtain an L-valued ρ-antihermitian form T on V such that

$$\mathrm{Tr}_{L/\boldsymbol{Q}}(T(x, y)) = E(f(x), f(y)).$$

Thus from $(A, \mathscr{C}, \theta)$, we obtain an L-isomorphism f of V to $\boldsymbol{Q} \cdot D$, a lattice $\mathfrak{M}$ in V, and a ρ-antihermitian form T on V. As D is a lattice in $\boldsymbol{C}^n$, f can be extended to an $\boldsymbol{R}$-linear isomorphism of $V_{\boldsymbol{R}} = V \otimes_{\boldsymbol{Q}} \boldsymbol{R}$ to $\boldsymbol{C}^n$. Then f maps $V_{\boldsymbol{R}}/D$ isomorphically to A (through the isomorphism of $\boldsymbol{C}^n/D$ to A), and V/D corresponds to the set of all points of finite order on A. Therefore, if we take points $t_1, \cdots, t_s$ on A of finite order, there exist points $x_i \in V$ such that $f(x_i) \bmod D$ represents x_i.

This observation leads us to the following formulation. We call a collection of objects $\Omega = (L, \Phi, \rho; V, T, \mathfrak{M}; x_1, \cdots, x_s)$ a PEL-*type* if the objects are as follows:

L: a division algebra over $\boldsymbol{Q}$.

ρ: a positive involution of L.

Φ: a representation of L into $M_n(\boldsymbol{C})$ such that $\Phi + \bar{\Phi}$ is equivalent to a rational representation.

V: a left L-module of rank m, where $m = 2n/[L:\boldsymbol{Q}]$.

T: a nondegenerate L-valued ρ-antihermitian form on V.

$\mathfrak{M}$: a free $\boldsymbol{Z}$-submodule of V of rank $2n$.

x_i: elements of V.

The consideration of the points t_i and the x_i is motivated by the need of treating congruence subgroups of discontinuous groups. We say that $\mathcal{Q} = (A, \mathcal{C}, \theta; t_1, \cdots, t_s)$ is a PEL-*structure* if

A: an abelian variety defined over a subfield of $\boldsymbol{C}$.

$\mathcal{C}$: a polarization of A.

θ: an isomorphism of L into $\mathrm{End}_{\boldsymbol{Q}}(A)$.

t_i: points of finite order on A.

Now we say that $\mathcal{Q}$ is of type Ω if there exists a commutative diagram

$$\begin{tikzcd} 0 \arrow[r] & \mathfrak{M} \arrow[r] \arrow[d] & V_{\boldsymbol{R}} \arrow[r] \arrow[d, "f"'] & V_{\boldsymbol{R}}/\mathfrak{M} \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & D \arrow[r] & \boldsymbol{C}^n \arrow[r, "\xi"] & A \arrow[r] & 0 \end{tikzcd} \qquad (V_{\boldsymbol{R}} = V \otimes_{\boldsymbol{Q}} \boldsymbol{R}) \tag{4.9}$$

such that the following conditions (4.10–4.14) are satisfied.

(4.10) *ξ gives a holomorphic isomorphism of $\boldsymbol{C}^n/D$ to A.*

(4.11) *f is an $\boldsymbol{R}$-linear isomorphism, and $f(\mathfrak{M}) = D$.*

(4.12) *$f(\alpha x) = \Phi(\alpha)f(x)$, and $\Phi(\alpha)$ defines $\theta(\alpha)$ for every $\alpha \in L$.*

(4.13) *$\mathcal{C}$ contains a basic divisor X which determines a Riemann form E on $\boldsymbol{C}^n/D$ such that $E(f(x), f(y)) = \mathrm{Tr}_{L/\boldsymbol{Q}}(T(x, y))$ for $(x, y) \in V \times V$.*

(4.14) *$t_i = \xi(f(x_i))$ for every i.*

Since $\mathrm{Tr}_{L/\boldsymbol{Q}}(T(x, y))$ corresponds to a *basic* divisor, we have to assume

$$\mathrm{Tr}_{L/\boldsymbol{Q}}(T(\mathfrak{M}, \mathfrak{M})) = \boldsymbol{Z}. \tag{4.15}$$

(If this is not satisfied, we can replace T by a suitable rational multiple of it satisfying this condition.)

Let $\mathcal{Q} = (A, \mathcal{C}, \theta,; t_1, \cdots, t_s)$ and $\mathcal{Q}' = (A', \mathcal{C}', \theta'; t'_1, \cdots, t'_s)$ be two PEL-structures. An isomorphism $\lambda: (A, \mathcal{C}) \to (A', \mathcal{C}')$ is called an *isomorphism* of $\mathcal{Q}$ to $\mathcal{Q}'$ if $\lambda\theta(\alpha) = \theta'(\alpha)\lambda$ for every $\alpha \in L$ and $\lambda(t_i) = t'_i$ for every i.

We say that Ω is *equivalent* to another PEL-type $\Omega' = (L', \Phi', \rho'; V', T', \mathfrak{M}'; x'_1, \cdots, x'_{s'})$ if $L = L'$, $\rho = \rho'$, $V = V'$, $s = s'$, Φ and Φ' are equivalent as representations of L, and there exists an L-linear automorphism μ of V such that $T'(x\mu, y\mu) = T(x, y)$, $\mathfrak{M}\mu = \mathfrak{M}'$, $x_i\mu \equiv x'_i \bmod \mathfrak{M}'$ for every i. Let $\mathcal{Q}$ be of type Ω. Then $\mathcal{Q}$ is of type Ω' if and only if Ω is equivalent to Ω'. A PEL-type Ω is said to be *admissible* if there exists at least one PEL-structure of type Ω.

THEOREM 3. *For every admissible* PEL-*structure* $\Omega = (L, \Phi, \rho; V, T, \mathfrak{M}; x_1, \cdots, x_s)$, *there exists a bounded symmetric domain S and an analytic map $f: V_{\boldsymbol{R}} \times S \to \boldsymbol{C}^n$ holomorphic in the variable $z \in S$ with the following properties:*

(1) *If we put $f_z(x) = f(x, z)$ for $x \in V_{\boldsymbol{R}}$ and $z \in S$, then for every $z \in S$, f_z is an $\boldsymbol{R}$-linear isomorphism of $V_{\boldsymbol{R}}$ to $\boldsymbol{C}^n$. Further put $D_z = f_z(\mathfrak{M})$, $A_z = \boldsymbol{C}^n/D_z$, $E_z(u, v) = \mathrm{Tr}_{L/\boldsymbol{Q}}(T(f_z^{-1}(u), f_z^{-1}(v)))((u, v) \in \boldsymbol{C}^n \times \boldsymbol{C}^n)$, $t_i(z) = f_z(x_i) \bmod D_z$, $\theta_z(a) = \Phi(a)$ $(a \in L)$. Then E_z defines a polarization $\mathscr{C}_z$ on A_z, and*

$$\mathscr{Q}_z = (A_z, \mathscr{C}_z, \theta_z; t_1(z), \cdots, t_s(z))$$

is a PEL-*structure of type* Ω.

(2) *Every* PEL-*structure of type Ω is isomorphic to $\mathscr{Q}_z$ for some $z \in S$.*

Thus we obtain a maximal family $\Sigma_\Omega = \{\mathscr{Q}_z | z \in S\}$ of PEL-structures of type Ω. Let G be an algebraic group defined over $\boldsymbol{Q}$ such that $G_{\boldsymbol{Q}}$ can be identified with the group of all L-linear automorphisms α of V satisfying $T(x\alpha, y\alpha) = T(x, y)$. Then the bounded symmetric domain S in the above theorem can be obtained as the quotient of $G_{\boldsymbol{R}}$ by a maximal compact subgroup. Let

$$\Gamma = \{\alpha \in G_{\boldsymbol{Q}} | \mathfrak{M}\alpha = \mathfrak{M}, x_i\alpha \equiv x_i \bmod \mathfrak{M} \ (i = 1, \cdots, s)\}.$$

Then Γ is commensurable with $G_{\boldsymbol{Z}}$ and acts naturally on S.

THEOREM 4. *Two members $\mathscr{Q}_z$ and $\mathscr{Q}_w$ of Σ_Ω are isomorphic if and only if $z = \gamma(w)$ for some $\gamma \in \Gamma$.*

In other words $\Gamma\backslash S$ is in one-to-one correspondence with all the isomorphism-classes of PEL-structures of type Ω.

5. **Classification of L, Φ, ρ, S, and the admissibility of Ω.** Let F be the set of elements x in the center of L such that $x^\rho = x$. Then it can be shown that F is a totally real algebraic number field. Let g denote the degree of F over $\boldsymbol{Q}$. According to Albert, all the division algebras L with positive involution are classified into the following four types:

(Type I) $L = F$.

(Type II) L is a totally indefinite quaternion algebra over F, i.e., L has F as its center, and $L \otimes_{\boldsymbol{Q}} \boldsymbol{R} = M_2(\boldsymbol{R}) \times \cdots \times M_2(\boldsymbol{R})$ (g copies).

(Type III) L is a totally definite quaternion algebra over F, i.e., L has F as its center, and $L \otimes_{\boldsymbol{Q}} \boldsymbol{R} = \boldsymbol{K} \times \cdots \times \boldsymbol{K}$ (g copies), where $\boldsymbol{K}$ means the division ring of real quaternions.

(Type IV) The center K of L is a totally imaginary quadratic extension of F.

If $L = F$, ρ should be the identity mapping. If L is of (Type III), the standard quaternion conjugate is the only positive involution of L. If L is of (Type II, IV) and L is not commutative, L has infinitely many positive involutions. As for (Type IV), ρ must induce the nontrivial automorphism of K over F.

Now the direct sum of Φ and $\bar{\Phi}$ is equivalent to a rational representation if and only if Φ satisfies the following condition:

(5.1) (Type I, II, III) *Φ is a multiple of a reduced representation of L over $\mathbf{Q}$.*

(Type IV) *Let $\tau_1, \cdots, \tau_g$ be g isomorphisms of K into $\mathbf{C}$, such that $\tau_1, \cdots, \tau_g$, $\rho\tau_1, \cdots, \rho\tau_g$ form the set of all isomorphisms of K into $\mathbf{C}$, and let $[L:K] = q^2$. Let qr_ν resp. qs_ν be the multiplicity of τ_ν resp. $\rho\tau_\nu$ in the restriction of Φ to K. Then $r_\nu + s_\nu = mq$ for $\nu = 1, \cdots, g$, where $m = 2n/[L:\mathbf{Q}]$ (cf. definition of* PEL-*type).*

The PEL-type Ω is admissible if L is of (Type I, II, III) and the conditions (4.15) and (5.1) are satisfied. When L is of (Type IV), Ω is admissible if and only if the following condition is satisfied besides (4.15) and (5.1).

(5.2) *Let ϕ_ν be a homomorphism of $M_m(L)$ into $M_{mq}(\mathbf{C})$ such that $\phi_\nu(a) = a^{\tau_\nu}1_{mq}$ for $a \in K$ and*

$$\phi_\nu({}^tU^\rho) = {}^t\overline{\phi_\nu(U)} \quad \textit{for} \quad U \in M_m(L).$$

Then, for each ν, the complex hermitian matrix $\sqrt{(-1)}\phi_\nu(T_0)^{-1}$ has r_ν positive eigenvalues and s_ν negative eigenvalues, where T_0 is an element of $M_m(L)$ which represents T with respect to a basis of V over L.

The bounded symmetric domain S can be described as follows according to the type of L.

(Type I) $S = S_{m/2} \times \cdots \times S_{m/2}$,

(Type II) $S = S_m \times \cdots \times S_m$,

(Type III) $S = S'_m \times \cdots \times S'_m$,

(Type IV) $S = S_{r_1,s_1} \times \cdots \times S_{r_g,s_g}$.

Here the number of copies is g in each case; S_r is the Siegel space of degree r (see §3); S'_m is the space all complex *alternating* matrices z of size m such that $1 - {}^t\bar{z}z$ is positive hermitian; $S_{r,s}$ is the space of all complex matrices z with r rows and s columns such that $1 - {}^t\bar{z}z$ is positive hermitian. If either $r = 0$ or $s = 0$, we understand by $S_{r,s}$ a space consisting of only one point. Therefore, if $\Sigma_{\nu=1}^{g} r_\nu s_\nu = 0$, S consists of only one point, so that Σ_Ω has only one member. For (Type III) with $m = 1$, we have also a family with the only member. In all these families with single member, the abelian variety in question has sufficiently many complex multiplications.

6. **The moduli-variety for the family Σ_Ω.** Let V be a variety in a projective space P^N, defined by a system of equations $F_i(X_0, \cdots, X_N) = 0$ $(i \in I)$. Let σ be an automorphism of $\mathbf{C}$. Then we denote by V^σ the variety defined by $F_i^\sigma(X_0, \cdots, X_N) = 0$ $(i \in I)$, where F_i^σ is the polynomial whose coefficients are transforms of coefficients of F_i under σ. Let L and $\mathcal{Q} = (A, \mathcal{C}, \theta; t_1, \cdots, t_s)$ be as before. Then we can define $\mathcal{Q}^\sigma = (A^\sigma, \mathcal{C}^\sigma, \theta^\sigma; t_1^\sigma, \cdots, t_s^\sigma)$ as follows: $\mathcal{C}^\sigma$ is the polarization of A^σ containing a divisor X^σ for a divisor X in $\mathcal{C}$; $\theta^\sigma(a) = \theta(a)^\sigma$ for $a \in L$.

THEOREM 5. *For every* PEL-*structure* $\mathcal{Q} = (A, \mathcal{C}, \theta; t_1, \cdots, t_s)$, *there exists a unique subfield* k_0 *of* $\boldsymbol{C}$ *with the following property*: σ and τ *being two automorphisms of* $\boldsymbol{C}$, $\mathcal{Q}^\sigma$ *is isomorphic to* $\mathcal{Q}^\tau$ *if and only if* $\sigma = \tau$ *on* k_0.

We call k_0 *the field of moduli of* $\mathcal{Q}$. For example, let $L = \mathcal{Q}$, $t_1 = \cdots = t_s = 0$, and $E = \boldsymbol{C}/(\boldsymbol{Z} + \boldsymbol{Z}\tau)$ with $\operatorname{Im}(\tau) > 0$, so that E is an elliptic curve. Then the field of moduli of $(E, \mathcal{C}, \theta; 0, \cdots, 0)$, with obvious $\mathcal{C}$ and θ, is $\boldsymbol{Q}(j(\tau))$ for the value $j(\tau)$ of the classical modular function j.

We say that a PEL-type Ω is *abnormal* if (i) $\dim(S) = 1$, (ii) $\Gamma\backslash S$ is not compact, and (iii) $L \neq \boldsymbol{Q}$. Ω is said to be *normal* if at least one of these conditions is not satisfied.

THEOREM 6. *Let* Ω *be an admissible and normal* PEL-*type. For every automorphism* σ *of* $\boldsymbol{C}$, *there exists a* PEL-*type* Ω^σ *which is determined, up to equivalence, by the following property: if* $\mathcal{Q}$ *is of type* Ω, *then* $\mathcal{Q}^\sigma$ *is of type* Ω^σ. (Ω^σ *depends only on* Ω *and* σ, *and is independent of* $\mathcal{Q}$.)

THEOREM 7. *For every admissible and normal* PEL-*type* Ω, *there exists a unique algebraic number field* k_Ω *of finite degree with the following properties*:

(1) *An automorphism* σ *of* $\boldsymbol{C}$ *is the identity mapping on* k_Ω *if and only if* Ω^σ *is equivalent to* Ω. (*This property characterizes* k_Ω.)

(2) *If* $\mathcal{Q}$ *is of type* Ω, *then* k_Ω *is contained in the field of moduli of* $\mathcal{Q}$.

(3) *Let* $\Omega = (L, \Phi, \rho; V, T, \mathfrak{M}; x_1, \cdots, x_s)$, *and let* K_Φ *be the field generated over* $\boldsymbol{Q}$ *by* $\operatorname{tr}\Phi(\alpha)$ *for all* α *in the center of* L. *Then* $K_\Phi \subset k_\Omega$.

Now by a result of Baily and Borel (cf. [1] and Baily's talk), one can embed $\Gamma\backslash S$ onto a Zariski open subset of a projective variety. ($\Gamma\backslash S$ may or may not be compact.) Our first main theorem asserts that there exists a nice model for $\Gamma\backslash S$.

MAIN THEOREM I. *For every admissible and normal* PEL-*type* Ω, *there exists a couple* (V, v) *and* ψ *with the following properties*:

(1) V *is a Zariski open subset of a projective variety.*

(2) V *is defined over* k_Ω.

(3) v *is an "assignment" which assigns a point* $v(\mathcal{Q})$ *of* V *to every* PEL-*structure* $\mathcal{Q}$ *of type* Ω; *and* $\mathcal{Q}$ *is isomorphic to* $\mathcal{Q}'$ *if and only if* $v(\mathcal{Q}) = v(\mathcal{Q}')$.

(4) *The coordinates of* $v(\mathcal{Q})$ *generate over* k_Ω *the field of moduli of* $\mathcal{Q}$.

(5) ψ *is a holomorphic mapping of* S *into a projective space which induces a biregular morphism of* $\Gamma\backslash S$ *onto* V, *and such that* $\psi(z) = v(\mathcal{Q}_z)$ *for every* $z \in S$, *where* $\mathcal{Q}_z$ *is a member of the family* Σ_Ω *defined in Theorem* 3.

(6) *Let* $\mathcal{Q}$ *and* $\mathcal{Q}'$ *be of type* Ω, *and* $\mathfrak{p}$ *a* $\boldsymbol{C}$-*valued place of a field of definition for* $\mathcal{Q}$ *such that* $\mathfrak{p}(x) = x$ *for* $x \in k_\Omega$ *and the reduction of* $\mathcal{Q}$ *modulo* $\mathfrak{p}$ *is* $\mathcal{Q}'$. *Then* $\mathfrak{p}(v(\mathcal{Q})) = v(\mathcal{Q}')$.

We call (V, v) a *moduli-variety* for PEL-structures of type Ω, understanding that $v(\mathcal{Q})$ is the "modulus" of $\mathcal{Q}$. (V, v) is uniquely determined, up to biregular isomorphisms over k_Ω, by the above properties. Let us set $V = V(\Omega)$.

THEOREM 8. *Let Ω be an admissible and normal* PEL-*type, and σ an automorphism of C. Then $k(\Omega^\sigma) = k(\Omega)^\sigma$, and $V(\Omega^\sigma)$ is biregularly isomorphic to $V(\Omega)^\sigma$ over $k(\Omega)^\sigma$.*

In general, one can make the following conjecture. Let S be a bounded symmetric domain, Γ an arithmetic discontinuous group operating on S, and σ an automorphism of C. Then (i) *$\Gamma\backslash S$ has a projective embedding V defined over an algebraic number field*; (ii) *the transform of V under σ is biregularly isomorphic to $\Gamma'\backslash S$ with another arithmetic discontinuous group Γ'.*

The above results show that this conjecture is true in the case of Γ and S obtained from an admissible and normal PEL-type.

7. The number field k_Ω as a class-field.

PROPOSITION 9. *Let K_Φ be the field defined in* (3) *of Theorem 7. Then* (i) *$K_\Phi = Q$ if Φ is equivalent to $\bar{\Phi}$*; (ii) *K_Φ is a totally imaginary quadratic extension of a totally real algebraic number field if Φ is not equivalent to $\bar{\Phi}$.*

Therefore $K_\Phi = Q$ if L is of (Type I, II, III), and both cases $K_\Phi = Q$ and $K_\Phi \neq Q$ may occur if L is of (Type IV).

MAIN THEOREM II. *The field k_Ω is an abelian extension of K_Φ in the following cases*:

(1) *L is of* (*Type* I) *or of* (*Type* II);

(2) *L is of* (*Type* IV) *and commutative.*

One can make the following general conjecture: If Ω is admissible and normal, then k_Ω is an abelian extension of K_Φ except for the case where $\dim(S) = 0$ and L is of (Type III).

THEOREM 10. *Let $\mathfrak{o}$ be an order in L defined by $\mathfrak{o} = \{a \in L | a\mathfrak{M} \subset \mathfrak{M}\}$.*

(1) *Suppose that L is of* (Type I or II), *$\mathfrak{o}$ is a maximal order in L, and $N^{-1}\mathfrak{M} = \mathfrak{M} + \sum_{i=1}^{s} \mathfrak{o}x_i$ with a positive integer N.* (*The last equality means that the x_i generate the points of order N. If $x_1 = \cdots = x_s = 0$, $N = 1$.*) *Then $k_\Omega = Q(e^{2\pi i/N})$.*

(2) *Suppose that L is of* (Type I) (*hence $L = F$*) *and $x_1 = \cdots = x_s = 0$. Let c be the smallest positive integer such that $c^{-1}\mathfrak{o}$ contains the maximal order in F. Let H be the set of all rational integers μ, prime to c, which occur as the multiplier of an F-linear similitude α of T,* i.e., *$T(x\alpha, y\alpha) = \mu T(x, y)$, such that $\mathfrak{M}\alpha \subset \mathfrak{M}$. Then k_Ω is the subfield of $Q(\zeta)$, consisting of all the elements of $Q(\zeta)$ invariant under the automorphisms $\zeta \to \zeta^\mu$ for all $\mu \in H$, where $\zeta = e^{2\pi i/c}$.*

If L is of (Type IV) and $\dim(S) = 0$, the description of k_Ω as a class-field over K_Φ is exactly the theory of complex multiplication **[15]**. One can get a similar result also in the case $\dim(S) > 0$. To explain this, we have to introduce the notion of class and genus of lattices. Let F denote, for a while, an arbitrary algebraic number field of finite degree, and K a quadratic extension of F. Let V be a vector space over K of dimension m, and T a nondegenerate K-valued antihermitian form on V. We denote by G the unitary group of T. Let $\mathfrak{o}_F$ resp. $\mathfrak{o}_K$ be the ring of integers in F resp. K. Let $\mathfrak{M}$ be an $\mathfrak{o}_K$-lattice in V. For every prime ideal $\mathfrak{p}$ in F, let $F_\mathfrak{p}$ denote the completion of F with respect to $\mathfrak{p}$, and $K_\mathfrak{p} = K \otimes_F F_\mathfrak{p}$, $V_\mathfrak{p} = V \otimes_F F_\mathfrak{p}$. Then $V_\mathfrak{p}$ is a $K_\mathfrak{p}$-module, and T is uniquely extended to a $K_\mathfrak{p}$-valued antihermitian form on $V_\mathfrak{p}$. So we can define the unitary group $G_\mathfrak{p}$ on $V_\mathfrak{p}$. By a *class* of $\mathfrak{o}_K$-lattices in V with respect to G, we understand a maximal set of $\mathfrak{o}_K$-lattices in V whose members are transformed to each other by elements of G. By a *genus* of $\mathfrak{o}_K$-lattices in V with respect to G, we understand a maximal set Λ of $\mathfrak{o}_K$-lattices with the following properties: If $\mathfrak{M}$ and $\mathfrak{N}$ are members of Λ, then, for every prime ideal $\mathfrak{p}$ in F, there exists an element $\alpha_\mathfrak{p}$ of $G_\mathfrak{p}$ such that $\mathfrak{M}_\mathfrak{p}\alpha_\mathfrak{p} = \mathfrak{N}_\mathfrak{p}$. A genus Λ consists of a finite number of classes. Let J denote the group of ideals $\mathfrak{a}$ in K such that $N_{K/F}(\mathfrak{a}) = \mathfrak{o}_F$, and J_0 the group of principal ideals $a\mathfrak{o}_K$ such that $N_{K/F}(a) = 1$. Then the number of classes in Λ equals $2^{e(\Lambda)} \cdot [J:J_0]$, where $e(\Lambda)$ is a nonnegative integer depending on Λ. If T is indefinite and $\dim_K V$ is even, there exists a genus Λ such that $e(\Lambda) = 0$. Let Λ be such a genus and $\mathfrak{M}$ an $\mathfrak{o}_K$-lattice in Λ. Then the map $\Lambda \ni \mathfrak{N} \mapsto [\mathfrak{M}/\mathfrak{N}]$ gives a one-to-one correspondence between the classes in Λ and J/J_0. Here $[\mathfrak{M}/\mathfrak{N}]$ means a fractional ideal in K generated over $\mathfrak{o}_K$ by $\det(\alpha)$ for all K-linear automorphisms α of V such that $\mathfrak{M}\alpha \subset \mathfrak{N}$. We call such a genus *nice*. (For details, see [10].)

Let us come back to a PEL-type, and assume that F is totally real, and K is totally imaginary. We take L to be K.

MAIN THEOREM III. *Let $\Omega = (K, \Phi, \rho; V, T, \mathfrak{M}; 0, \cdots, 0)$ be an admissible* PEL-*type. Suppose that T is indefinite, $K_\Phi \neq \mathbf{Q}$,* $\dim_K V$ *is even, and the genus of $\mathfrak{M}$ is nice. Let $\mathfrak{a}$ be an ideal in K_Φ, and let σ be an automorphism of $\mathbf{C}$ such that σ coincides with the Frobenius automorphism $((k_\Omega/K_\Phi)/\mathfrak{a})$ on k_Ω. Then we have*

$$\Omega^\sigma = (K, \Phi, \rho; V, T, \mathfrak{N}; 0, \cdots, 0)$$

with a lattice $\mathfrak{N}$ belonging to the same genus as $\mathfrak{M}$, and

$$[\mathfrak{M}/\mathfrak{N}] = \prod_{i\ \ 1}^{h} (\mathfrak{a}^{\sigma_i}/\mathfrak{a}^{\bar{\sigma}_i})^{v_i} \operatorname{mod}(J_0),$$

where $\{\sigma_1, \cdots, \sigma_h, \bar{\sigma}_1, \cdots, \bar{\sigma}_h\}$ is the set of all isomorphisms of K_Φ into $\mathbf{C}$, and $v_1, \cdots, v_h$ are certain integers determined only by K and Φ.

Since the class of $\mathfrak{N}$ (and hence Ω^σ) can be completely determined by $[\mathfrak{M}/\mathfrak{N}] \operatorname{mod}(J_0)$, this theorem affords an "explicit reciprocity-law" for the abelian extension k_Ω/K_Φ. One can prove an analogous and somewhat complicated relation for odd m, and also in a more general case with nonzero $x_1, \cdots, x_s$.

8. **Fibre systems of abelian varieties.** We say that $\{V, W, h, f\}$ is a *fibre system of abelian varieties* defined over a field k, if the following conditions are satisfied:

(8.1) V and W are nonsingular varieties defined over k.

(8.2) h is a morphism of W into V, f is a morphism of V into W, both defined over k, such that $h \circ f$ is the identity mapping of V.

(8.3) If $Z \subset W \times V$ is the graph of h, then for every $u \in V$, Z and $W \times u$ intersect properly on $W \times V$, and $Z \cdot (W \times u) = A_u \times u$ with an abelian variety A_u whose neutral element is $f(u)$.

MAIN THEOREM IV. *Let $\Omega = (L, \Phi, \rho; V, T, \mathfrak{M}; x_1, \cdots, x_s)$ be an admissible and normal* PEL-*type, and let $\mathfrak{o} = \{a \in L | a\mathfrak{M} \subset \mathfrak{M}\}$. Suppose that Γ has no element of finite order other than the identity element. Then there exists a system*

$$\mathfrak{F} = \{V, W, h, f, Y, \Theta(a)(a \in \mathfrak{o}), f_1, \cdots, f_s\}$$

with the following properties.

(1) *$\{V, W, h, f\}$ is a fibre system of abelian varieties defined over k_Ω.*

(2) *With a suitably defined v, (V, v) is a moduli-variety for* PEL-*structures of type Ω* (cf. Main Theorem I).

(3) *Y is a divisor on W, rational over k_Ω, such that $Y \cdot A_u$ defines a polarization $\mathscr{C}_u$ on A_u for every $u \in V$.*

(4) *For every $a \in \mathfrak{o}$, $\Theta(a)$ is a morphism of W to W defined over k_Ω such that the restriction of $\Theta(a)$ to A_u is an endomorphism of A_u for every $u \in V$; denote it by $\theta_u(a)$.*

(5) *The $f_i: V \rightarrow W$ $(i = 1, \cdots, s)$ are sections which are morphisms, defined over k_Ω.*

(6) *For each $u \in V$, $\mathscr{Q}_u = (A_u, \mathscr{C}_u, \theta_u; f_1(u), \cdots, f_s(u))$ is a* PEL-*structure of type Ω.*

(7) *Let $\Sigma_\Omega = \{\mathscr{Q}_z | z \in S\}$ and $\psi: S \rightarrow V$ be as in Main Theorem* I. *Then $\mathscr{Q}_{\psi(z)}$ is isomorphic to $\mathscr{Q}_z$.*

9. Families of abelian varieties characterized by a certain nonholomorphic structure.

Let F be as before a totally real algebraic number field of degree g, and B a quaternion algebra over F. Let h be the number of archimedean primes of F for which B is unramified. Then

$$B \otimes_{\boldsymbol{Q}} \boldsymbol{R} = M_2(\boldsymbol{R}) \times \cdots \times M_2(\boldsymbol{R}) \times \boldsymbol{K} \times \cdots \times \boldsymbol{K},$$

taking the $M_2(\boldsymbol{R})$, h times, and the $\boldsymbol{K}, g - h$ times, (where $\boldsymbol{K}$ is the division ring of real quaternions). Let m be a positive integer and let G be an algebraic group defined over $\boldsymbol{Q}$, which can be identified with the group

$$\{X \in \mathrm{GL}_m(B) | {}^t X^\iota \cdot X = 1_m\}$$

where ι denotes the main involution of B (ι is not a positive involution unless $h = 0$). Then the quotient S of $G_{\boldsymbol{R}}$ by a maximal compact subgroup is the product of h copies of the Siegel space of degree m. Let $\Gamma = G_{\boldsymbol{Z}}$. Now this group Γ does not occur in our theory of PEL-structure, except when $m = 1$ or $g = h$. (If $g = h$, G is exactly the group attached to a PEL-type with an algebra $L = B$, which is of (Type II). If $m = 1$, Γ is commensurable with the group obtained from an algebra of (Type IV).) However, we can still construct a family Σ' of abelian varieties parametrized by $\Gamma\backslash S$, which is actually a subfamily of Σ_Ω of (Type IV). The members of Σ' can be characterized by the possession of a certain non-holomorphic endomorphism, or a certain rational 2-cohomology class, which is not of (1, 1)-type. It should be mentioned that there are infinitely many distinct such families attached to the same S and Γ. We can also find a projective variety, isomorphic to $\Gamma\backslash S$, defined over an algebraic number field of finite degree. This field is again of *abelian* nature. The same type of discussion can be also made for the unitary group of an ι-antihermitian form over B. A full detail of all these results will be given in **[14]**.

10. **Hecke operators.** Let L be an indefinite division quaternion algebra over $\boldsymbol{Q}$, which is, by definition, a division algebra over $\boldsymbol{Q}$ such that $L \otimes_{\boldsymbol{Q}} \boldsymbol{R} = M_2(\boldsymbol{R})$. Let $\mathfrak{o}$ be a maximal order in L. (It should be noted that if $\mathfrak{o}_1$ and $\mathfrak{o}_2$ are two maximal orders in L, there exists an element a of L such that $a\mathfrak{o}_1 a^{-1} = \mathfrak{o}_2$ and $\det(a) > 0$.) Regarding L as a subring of $M_2(\boldsymbol{R})$, let

$$\Gamma_b = \{\gamma \in \mathfrak{o} | \det(\gamma) = 1, \gamma \equiv 1 \bmod b\mathfrak{o}\}$$

for every positive integer b. We denote by H the complex upper half plane $\{z \in \boldsymbol{C} | \operatorname{Im}(z) > 0\}$, and by $\mathrm{GL}_2^+(\boldsymbol{R})$ the group of elements in $M_2(\boldsymbol{R})$ with positive determinant. For

$$\alpha = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\boldsymbol{R}),$$

we put

$$\alpha' = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

Further for

$$\alpha = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2^+(\boldsymbol{R})$$

and $z \in H$, we put $\alpha(z) = (az + b)/(cz + d)$ and $j(\alpha, z) = cz + d$. Then Γ_b, regarded as a discrete subgroup of $\mathrm{SL}_2(\boldsymbol{R})$, gives a properly discontinuous group of transformations on H with compact quotient $\Gamma_b\backslash H$. Moreover, $\Gamma_b\backslash H$ is a special case of $\Gamma\backslash S$ considered in §§4–8. In fact, for every $z \in H$, define a lattice D_z in $\boldsymbol{C}^2$ by

$$D_z = \mathfrak{o} \cdot \begin{bmatrix} z \\ 1 \end{bmatrix},$$

elements of $\mathfrak{o}$ being considered as real 2×2 matrices. Then the complex torus $\boldsymbol{C}^2/D_z$ has a structure of abelian variety. Let $A_z = \boldsymbol{C}^2/D_z$. For a suitable $v \in L$ such that v^2 is a negative integer, we can define a Riemann form E on $\boldsymbol{C}^2/D_z$ by

$$E\left(x\begin{bmatrix} z \\ 1 \end{bmatrix}, y\begin{bmatrix} z \\ 1 \end{bmatrix}\right) = \mathrm{Tr}_{L/\boldsymbol{Q}}(vxy') \qquad (x, y \in M_2(\boldsymbol{R})).$$

Let $\mathscr{C}_z$ be the polarization of A_z determined by E. For every $\alpha \in L$, the linear transformation of C^2 given by the matrix α defines an element of $\mathrm{End}_Q(A_z)$, which we denote by $\theta_z(\alpha)$. Let t_z be the point on A_z corresponding to

$$b^{-1}\begin{bmatrix} z \\ 1 \end{bmatrix}.$$

Put $\mathscr{Q}_z = (A_z, \mathscr{C}_z, \theta_z; t_z)$. In this way we get a family $\Sigma = \{\mathscr{Q}_z | z \in H\}$, which is a special case of Σ_Ω considered in §4. Two members $\mathscr{Q}_z$ and $\mathscr{Q}_w$ are isomorphic if and only if $z = \gamma(w)$ for some $\gamma \in \Gamma_b$ (cf. Theorem 4).

From now on we always assume that $b > 2$. Then Γ_b has no elements of finite order other than the identity. Applying our Main Theorem IV to the present case, we get a fibre variety $W \rightarrow V$, of which the base V is biregularly isomorphic to $\Gamma_b \backslash H$, and each fibre is isomorphic to A_z. We can take the field of rationality to be $Q(\zeta)$ with $\zeta = e^{2\pi i/b}$. For every nonnegative integer m, one can construct, over $Q(\zeta)$, a fibre system of abelian varieties $W_m \rightarrow V$, whose fibre standing on $u \in V$ is the product of m copies of A_u, where A_u is a fibre of W on u. The purpose of the remaining part of this lecture is to determine the zeta-function of W_m in the sense of Hasse–Weil.

First we have to introduce the Hecke ring in L. Let

$$\Delta_b = \{\alpha \in \mathfrak{o} | \det(\alpha) > 0, (\det(\alpha), b) = 1\}.$$

Then, for every $\alpha \in \Delta_b$, one has $\Gamma_b \alpha \Gamma_b = \bigcup_i \Gamma_b \alpha_i$ for a finite number of elements α_i. Let $R(\Gamma_b, \Delta_b)$ denote the free $\boldsymbol{Z}$-module consisting of all the formal finite sums $\sum_\lambda c_\lambda \Gamma_b \alpha_\lambda \Gamma_b$ with $c_\lambda \in \boldsymbol{Z}$, $\alpha_\lambda \in \Delta_b$. The module $R(\Gamma_b, \Delta_b)$ is called the Hecke ring associated with Γ_b and Δ_b, when a law of multiplication is defined as follows: If $\Gamma_b \alpha \Gamma_b = \bigcup_i \Gamma_b \alpha_i$ and $\Gamma_b \beta \Gamma_b = \bigcup_j \Gamma_b \beta_j$ are disjoint unions, then

$$(\Gamma_b \alpha \Gamma_b) \cdot (\Gamma_b \beta \Gamma_b) = \sum \mu_\xi \cdot \Gamma_b \xi \Gamma_b,$$

where the summation is taken over all the distinct double cosets $\Gamma_b \xi \Gamma_b \subset \Gamma_b \alpha \Gamma_b \beta \Gamma_b$, and $\mu_\xi =$ the number of (i, j) such that $\Gamma_b \alpha_i \beta_j = \Gamma_b \xi$. (It can be shown that this number μ_ξ depends only on $\Gamma_b \xi \Gamma_b, \Gamma_b \alpha \Gamma_b, \Gamma_b \beta \Gamma_b$; it does not depend on the choice of representatives.) This law of multiplication is associative. In the special case $b = 1$, one can show that $R(\Gamma_1, \Delta_1)$ is commutative.

For a positive integer k, let $S_k(\Gamma_b)$ denote the set of all holomorphic functions f on H such that $f(\gamma(z))j(\gamma, z)^{-k} = f(z)$ for every $\gamma \in \Gamma_b$. An element of $S_k(\Gamma_b)$ is called a *holomorphic automorphic form of weight k* with respect to Γ_b. If $\alpha \in \Delta_b$, we can define the action $(\Gamma_b \alpha \Gamma_b)_k$ of $\Gamma_b \alpha \Gamma_b$ on $S_k(\Gamma_b)$ in the following way. Let $\Gamma_b \alpha \Gamma_b = \bigcup_{i=1}^d \Gamma_b \alpha_i$ be a disjoint union. For every $f \in S_k(\Gamma_b)$, we put

$$f|(\Gamma_b \alpha \Gamma_b)_k = \det(\alpha)^{k-1} \sum_{i=1}^{d} f(\alpha_i(z))j(\alpha_i, z)^{-k}.$$

Then $\Gamma_b \alpha \Gamma_b \rightarrow (\Gamma_b \alpha \Gamma_b)_k$ defines a representation of the ring $R(\Gamma_b, \Delta_b)$ in the complex vector space $S_k(\Gamma_b)$. The linear transformations $(\Gamma_b \alpha \Gamma_b)_k$ may be called the *Hecke operators*.

For our purpose we need also another type of Hecke operators. Let G_b denote the group of invertible elements of $\mathfrak{o}/b\mathfrak{o}$, and ρ a representation of G_b in a complex vector space U of finite dimension. Let $S_{k,\rho}(\Gamma_1)$ denote the set of all holomorphic maps $f : H \to U$ such that $f(\gamma(z))j(\gamma, z)^{-k} = \rho(\gamma)f(z)$ for every $\gamma \in \Gamma_1$. For $\Gamma_1\alpha\Gamma_1 = \bigcup_{i=1}^{d}\Gamma_1\alpha_i$ with $\alpha \in \Delta_b$, and for $f \in S_{k,\rho}(\Gamma_1)$, we define

$$f|(\Gamma_1\alpha\Gamma_1)_{k,\rho} = \det(\alpha)^{k-1}\sum_{i=1}^{d}\rho(\alpha_i^{-1})f(\alpha_i(z))j(\alpha_i, z)^{-k}.$$

Then $\Gamma_1\alpha\Gamma_1 \to (\Gamma_1\alpha\Gamma_1)_{k,\rho}$ defines a representation of $R(\Gamma_1, \Delta_b)$ in $S_{k,\rho}(\Gamma_1)$.

LEMMA 11. *Let ρ be a regular representation of G_b, $\chi(\alpha) = \operatorname{tr}\rho(\alpha)$, and let $\Gamma_1 = \bigcup_{i=1}^{N}\Gamma_b\gamma_i$, $N = [\Gamma_1 : \Gamma_b]$. Then, for $\xi \in \Delta_b$,*

$$\operatorname{tr}[(\Gamma_1\xi\Gamma_1)_{k,\rho}] = N^{-1}\sum_{i=1}^{N}\chi(\xi'\gamma_i)\cdot\operatorname{tr}[(\Gamma_b\gamma_i^{-1}\Gamma_b)_k\cdot(\Gamma_b\xi\Gamma_b)_k].$$

Now we define a Dirichlet series $D(s; k, b, \rho)$ by

$$D(s; k, b, \rho) = \sum(\Gamma_1\alpha\Gamma_1)_{k,\rho}\det(\alpha)^{-s},$$

where the summation is taken over all the distinct double cosets $\Gamma_1\alpha\Gamma_1$ with α in Δ_b. Then $D(s; k, b, \rho)$ can be expressed as an Euler product:

$$\begin{aligned} D(s; k, b, \rho) = &\prod_{p|d_0, p\nmid b}[1 - (\Gamma_1\alpha_p\Gamma_1)_{k,\rho}p^{-s}]^{-1} \\ &\times\prod_{p\nmid bd_0}[1 - (\Gamma_1\alpha_p\Gamma_1)_{k,\rho}p^{-s} + (\Gamma_1 p\Gamma_1)_{k,\rho}p^{1-2s}]^{-1}, \end{aligned}$$

where d_0 is the discriminant of L, and α_p is an element of $\mathfrak{o}$ such that $\det(\alpha_p) = p$. Moreover, $D(s; k, b, \rho)$ can be continued holomorphically to the whole s-plane, and satisfies a functional equation [7], [8].

11. **Algebraic correspondences on W_m and their congruence relations.** First we observe that the fibre variety W_m, as a real analytic manifold, can be constructed as follows (cf. Kuga's lecture). Let $L_{\boldsymbol{R}}^m$ denote the product of m copies of $L_{\boldsymbol{R}} = M_2(\boldsymbol{R})$. The product $\mathrm{GL}_2^+(\boldsymbol{R}) \times L_{\boldsymbol{R}}^m$ forms a group with respect to the law of multiplication

$$(\alpha, u)(\beta, v) = (\alpha\beta, v\beta' + u) \qquad (\alpha, \beta \in \mathrm{GL}_2^+(\boldsymbol{R}); u, v \in L_{\boldsymbol{R}}^m).$$

We let $\mathrm{GL}_2^+(\boldsymbol{R}) \times L_{\boldsymbol{R}}^m$ act on $H \times L_{\boldsymbol{R}}^m$ by

$$(\alpha, x)(z, y) = (\alpha(z), y\alpha' + x) \qquad (\alpha \in \mathrm{GL}_2^+(\boldsymbol{R}); x, y \in L_{\boldsymbol{R}}^m, z \in H).$$

(Recall that $\alpha \to \alpha'$ is the main involution of $M_2(\boldsymbol{R})$. We regard $L_{\boldsymbol{R}}^m$ as a left and right $L_{\boldsymbol{R}}$-module.) Let $\mathfrak{o}^m$ denote the product of m copies of $\mathfrak{o}$. Then $\Gamma_b \times \mathfrak{o}^m$ is a discrete subgroup of $\mathrm{GL}_2^+(\boldsymbol{R}) \times L_{\boldsymbol{R}}^m$, and W_m can be obtained as the quotient:

$W_m = (\Gamma_b \times \mathfrak{o}^m)\backslash(H \times L^m_{\boldsymbol{R}})$. We may write: $W_0 = V = \Gamma_b\backslash H$. Then we have naturally a commutative diagram:

$$\begin{tikzcd} H \times L^m_{\boldsymbol{R}} \arrow[r, "\phi_m"] \arrow[d] & W_m \arrow[d] \\ H \arrow[r, "\phi_0"] & V \end{tikzcd}$$

For an element α of Δ_b, put $\alpha^* = (\alpha, 0)$ $(\in \mathrm{GL}_2^+(\boldsymbol{R}) \times L^m_{\boldsymbol{R}})$, and

$$X_m = \{\phi_m(s) \times \phi_m(\alpha^* s) | s \in H \times L^m_{\boldsymbol{R}}\} \qquad (m \geqq 0).$$

It can be proved that X_m is an algebraic subvariety of W_m defined over $\boldsymbol{Q}(\zeta)$. Furthermore X_m is determined only by $\Gamma_b\alpha\Gamma_b$, and independent of the choice of the representative α. We write therefore $X_m = X_m(\Gamma_b\alpha\Gamma_b)$. If $m = 0$, we have

$$V \times V \supset X_0(\Gamma_b\alpha\Gamma_b) = \{\phi_0(z) \times \phi_0(\alpha(z)) | z \in H\}.$$

Still α being an element of Δ_b, let σ be an automorphism of $\boldsymbol{Q}(\zeta)$ such that $\zeta^\sigma = \zeta^{\det(\alpha)}$. Then one can find a biregular morphism $Y_m(\alpha)$: $W_m \to W_m^\sigma$ with the following properties:

(11.1)
$$\begin{tikzcd} W_m \arrow[r, "Y_m(\alpha)"] \arrow[d] & W_m^\sigma \arrow[d] \\ V \arrow[r, "Y_0(\alpha)"] & V \end{tikzcd}$$
is commutative.

(11.2) $Y_m(\alpha)$ depends only on the class of $\alpha \bmod b\mathfrak{o}$.

(11.3) If β is another element of Δ_b, then $Y_m(\beta\alpha) = Y_m(\beta)^\sigma \circ Y_m(\alpha)$, where σ is as above.

(11.4) If $\alpha \in \Gamma_1$, then $Y_m(\alpha) = X_m(\Gamma_b\alpha\Gamma_b)$.

Let p be a prime number, and $\mathfrak{p}$ a prime ideal in $\boldsymbol{Q}(\zeta)$ dividing p. We shall denote by $\mathfrak{p}(X)$ or $\tilde{X}$ the reduction modulo $\mathfrak{p}$ of an algebro-geometric object X. Now, for almost all $\mathfrak{p}$, we have a "nice reduction" $\mathfrak{p}(W_m) \to \mathfrak{p}(V)$, which forms a fibre system of abelian varieties defined over the residue field modulo $\mathfrak{p}$.

LEMMA 12. *Let p be a prime number which does not divide b, and α an element of $\mathfrak{o}$ such that* $\det(\alpha) = p$. *Then there exists an element δ of Γ_1 such that $\alpha^2 \equiv p\delta$* mod $b\mathfrak{o}$.

THEOREM 13. *Let p, α and δ be as in Lemma 12, and let $\mathfrak{p}$ be a prime ideal in $\boldsymbol{Q}(\zeta)$ dividing p. Then, for almost all $\mathfrak{p}$, we have*

$$\tilde{X}_m(\Gamma_b\alpha\Gamma_b) = {}^t\tilde{Y}_m(\alpha') \circ \Pi + \Pi^* \circ \tilde{Y}_m(\alpha),$$

$$p \cdot \tilde{X}_m(\Gamma_b p\delta\Gamma_b) = [{}^t\tilde{Y}_m(\alpha') \circ \Pi] \circ [\Pi^* \circ \tilde{Y}_m(\alpha)],$$

where Π is the Frobenius correspondence on $\tilde{W}_m \times \tilde{W}_m^p$, i.e., the locus of $v \times v^p$ with $v \in \tilde{W}_m$, and Π^* is the locus of $v^p \times p \cdot v$ on $\tilde{W}_m^p \times \tilde{W}_m$ with $v \in \tilde{W}_m$. (Here $p \cdot v = v + \cdots + v$ (p times) on the fibre abelian variety containing v.)

12. **Calculation of the zeta-function of W_m.** Let $I(X)$ denote the intersection number of an algebraic correspondence X with the diagonal.

LEMMA 14. (Kuga [3]). *Let* $d(\Gamma_b\alpha\Gamma_b)$ *denote the number of right cosets in* $\Gamma_b\alpha\Gamma_b$. *Define integers* $a(m, i, v)$ *by*

$$a(0,0,0) = 1,$$

$$\begin{aligned} a(m, i, v) &= \binom{2m}{(i+v)/2}\binom{2m}{(i-v)/2} - \binom{2m}{(i+v)/2+1}\binom{2m}{(i-v)/2-1} \\ &\qquad \textit{if} \quad i \equiv v \bmod(2), \\ &= 0 \quad \textit{if} \quad i \not\equiv v \bmod(2), \end{aligned}$$

where the expressions in parentheses mean the binomial coefficient. Then, for every $m \geqq 0$,

$$\begin{aligned} 2^{-1}I(X_m(\Gamma_b\alpha\Gamma_b)) &= \sum_{j=0}^{2m} a(m, 2j, 0)\det(\alpha)^j\, d(\Gamma_b\alpha\Gamma_b) \\ &\quad + \sum_{i=0}^{4m}\sum_{v=0}^{i} (-1)^{i+1}a(m, i, v)\det(\alpha)^{(i-v)/2}\operatorname{Re}[\operatorname{tr}(\Gamma_b\alpha\Gamma_b)]. \end{aligned}$$

The method of proof of this "trace-formula" will be indicated in Kuga's talk.

To make our later calculation smooth, we introduce the following notation. Let x, y, u be indeterminates. Define polynomials $F_n(x, y)$ (with coefficients in $\boldsymbol{Z}$) by

$$-\frac{d}{du}\log(1 - xu + yu^2) = \sum_{n=1}^{\infty} F_n(x, y)u^{n-1}.$$

If $x = z + w$ and $y = zw$, then $F_n(x, y) = z^n + w^n$. If X and Y are commuting matrices, then

$$\frac{d}{du}\log[\det(1 - Xu + Yu^2)^{-1}] = \sum_{n=1}^{\infty} \operatorname{tr}[F_n(X, Y)]u^{n-1}.$$

From Theorem 13 we obtain easily

LEMMA 15. $F_n(\tilde{X}_m(\Gamma_b\alpha\Gamma_b), p\tilde{X}_m(\Gamma_b p\delta\Gamma_b)) = ({}^t\tilde{Y}_m(\alpha') \circ \Pi)^n + (\Pi^* \circ \tilde{Y}_m(\alpha))^n$.

LEMMA 16. *Let* $\Pi_{\mathfrak{p}}^{(n)}$ *be the locus of* $v \times v^{p^n}$ *on* $\tilde{W} \times \tilde{W}^{p^n}$ *with* $v \in \tilde{W}$, *and* $\Pi_{\mathfrak{p}}^{*(n)}$ *the locus of* $v^{p^n} \times (p^n \cdot v)$ *on* $\tilde{W}^{p^n} \times \tilde{W}$ *with* $v \in \tilde{W}$. *Let* β *be an element of* $\mathfrak{o}$ *such that* $\det(\beta) = p^n$. *Then*

$$I({}^t\tilde{Y}_m(\beta) \circ \Pi_{\mathfrak{p}}^{(n)}) = I(\Pi_{\mathfrak{p}}^{*(n)} \circ \tilde{Y}(\beta)).$$

Now the zeta-function $Z_{\mathfrak{p}}(u)$ of $\mathfrak{p}(W_m)$ over the residue field modulo $\mathfrak{p}$ is defined by

$$\frac{d}{du}\log Z_{\mathfrak{p}}(u) = \sum_{n=1}^{\infty} I(\Pi_{\mathfrak{p}}^{(fn)})u^{n-1}; \qquad N(\mathfrak{p}) = p^f.$$

If $\mathfrak{q}$ is another prime ideal in $\boldsymbol{Q}(\zeta)$ dividing p, then it is easily seen that $Z_{\mathfrak{q}} = Z_{\mathfrak{p}}$.

Let χ, N and $\{\gamma_i\}$ be as in Lemma 11, and let $\phi(b) = [G_b : \Gamma_1/\Gamma_b]$. Then

$$\text{(Z)} \qquad \frac{d}{du} \log\left[\prod_{\mathfrak{p}|p} Z_{\mathfrak{p}}(u^f)\right] = \phi(b) \sum_{n=1}^{\infty} I(\Pi_{\mathfrak{p}}^{(fn)})u^{(n-1)f} \cdot u^{f-1}$$

$$= N^{-1} \sum_{n=1}^{\infty} u^{n-1} {\sum_{\sigma}}' \chi(\sigma) I({}^t\tilde{Y}_m(\sigma) \circ \Pi_{\mathfrak{p}}^{(n)}).$$

Here we write $Y_m(\sigma) = Y_m(\alpha)$ if $\alpha \bmod b\mathfrak{o}$ represents σ, and $\sum_\sigma'$ is the summation taken over all $\sigma \in G_b$ such that $\det(\alpha) = p^n$. We see easily

$$(\text{Z}) = N^{-1} \sum_{n=1}^{\infty} u^{n-1} \sum_{j=1}^{N} \chi(\alpha'^n \gamma_j) I({}^t\tilde{Y}_m(\alpha'^n \gamma_j) \circ \Pi_{\mathfrak{p}}^{(n)})$$

with an element α of $\mathfrak{o}$ such that $\det(\alpha) = p$. Similarly

$$(\text{Z}) = N^{-1} \sum_{n=1}^{\infty} u^{n-1} \sum_{j=1}^{N} \chi(\gamma_j'\alpha^n) I({}^t\tilde{Y}_m(\gamma_j'\alpha^n) \circ \Pi_{\mathfrak{p}}^{(n)})$$

$$= N^{-1} \sum_{n=1}^{\infty} u^{n-1} \sum_{j=1}^{N} \chi(\gamma_j'\alpha^n) I(\Pi_{\mathfrak{p}}^{*(n)} \circ \tilde{Y}_m(\gamma_j'\alpha^n)) \quad \text{(Lemma 16)}.$$

By (11.3) we have $\Pi_{\mathfrak{p}}^{*(n)} \circ \tilde{Y}_m(\gamma_j'\alpha^n) = {}^t\tilde{Y}_m(\gamma_j) \circ \Pi_{\mathfrak{p}}^{*(n)} \circ \tilde{Y}_m(\alpha^n)$, hence

$$\frac{d}{du} \log\left[\prod_{\mathfrak{p}|p} Z_{\mathfrak{p}}(u^f)\right] = (2N)^{-1} \sum_{n=1}^{\infty} u^{n-1} \sum_{j=1}^{N} \chi(\alpha'^n \gamma_j) I({}^t\tilde{Y}_m(\gamma_j) \circ U_n),$$

where $U_n = {}^t\tilde{Y}_m(\alpha'^n) \circ \Pi_{\mathfrak{p}}^{(n)} + \Pi_{\mathfrak{p}}^{*(n)} \circ \tilde{Y}_m(\alpha^n)$. By Lemma 15 and the property (11.4), we have $U_n = F_n(\tilde{X}_m(\Gamma_b \alpha \Gamma_b), p\tilde{X}_m(\Gamma_b p\delta\Gamma_b))$. Applying Lemma 14 to this correspondence, we find

$$\frac{d}{du} \log\left[\prod_{\mathfrak{p}|p} Z_{\mathfrak{p}}(u^f)\right] = \sum_{j=0}^{2m} a(m, 2j, 0)P_j + \sum_{i=0}^{4m} \sum_{\nu=0}^{i} (-1)^{i+1} a(m, i, \nu) Q_{i\nu}$$

with

$$P_j = N^{-1} \sum_{n=1}^{\infty} u^{n-1} \sum_{j=1}^{N} \chi(\alpha'^n \gamma_j) p^{ni} F_n(d(\Gamma_b \alpha \Gamma_b), p \cdot d(\Gamma_b p\delta\Gamma_b)),$$

$$Q_{i\nu} = N^{-1} \sum_{n=1}^{\infty} u^{n-1} \sum_{j=1}^{N} \chi(\alpha'^n \gamma_j) p^{n(i-\nu)/2}$$

$$\cdot \operatorname{Re}\{\operatorname{tr}[(\Gamma_b \gamma_j \Gamma_b)_{\nu+2} \cdot F_n((\Gamma_b \alpha \Gamma_b)_{\nu+2}, p \cdot (\Gamma_b p\delta\Gamma_b)_{\nu+2})]\}.$$

By Lemma 11, we get

$$\prod_{\mathfrak{p}|p} Z_{\mathfrak{p}}(u^f) = \prod_{j=0}^{m} \left[\prod_{\mathfrak{p}|p} (1 - N(\mathfrak{p})^j u^f)(1 - N(\mathfrak{p})^{j+1} u^f)\right]^{-a(m,2j,0)}$$

$$\cdot \prod_{i=0}^{4m} \prod_{\nu=0}^{i} \det[1 - (\Gamma_1 \alpha \Gamma_1)_{\nu+2,\rho} p^{(i-\nu)/2} u$$

$$+ (\Gamma_1 p \Gamma_1)_{\nu+2,\rho} p^{i-\nu+1} u^2]^{(-1)^i a(m,i,\nu)}.$$

Now we define the global zeta function $Z(s; W_m, Q(\zeta))$ by

$$Z(s; W_m, Q(\zeta)) = \prod_{\mathfrak{p}} Z_{\mathfrak{p}}(N(\mathfrak{p})^{-s}),$$

the product being taken over all prime ideals $\mathfrak{p}$ in $Q(\zeta)$ with nice reduction of W_m. The above calculation proves

MAIN THEOREM V. *Let $Z(s; Q(\zeta))$ denote the Dedekind zeta function of $Q(\zeta)$. Then, up to a finite number of $\mathfrak{p}$-factors, $Z(s; W_m, Q(\zeta))$ is equal to the product*

$$\prod_{j=0}^{m} [Z(s-j; Q(\zeta))Z(s-j-1; Q(\zeta)]^{a(m,2j,0)}$$

$$\times \prod_{i=0}^{4m} \prod_{\nu=0}^{i} \det[D(s-(i-\nu)/2; b, \nu+2, \rho)]^{(-1)^{i+1}a(m,i,\nu)}.$$

Here ρ is the regular representation of G_b.

COROLLARY. *Let α be an element of $\mathfrak{o}$ such that* $\det(\alpha) = p$. *If Weil's conjecture on $Z_{\mathfrak{p}}(u)$ is true, then, for every representation ψ of G_b and for every integer $k > 2$, the absolute value of the characteristic roots of $(\Gamma_1\alpha\Gamma_1)_{k,\psi}$ and $(\Gamma_b\alpha\Gamma_b)_k$ does not exceed $2p^{(k-1)/2}$, except for a finite number of exceptional p's.*

Since Weil's conjecture is true for curves, the absolute value of the characteristic roots of $(\Gamma_1\alpha\Gamma_1)_{2,\psi}$ and $(\Gamma_b\alpha\Gamma_b)_2$ do not exceed $2 \cdot p^{\frac{1}{2}}$ for almost all p.

THEOREM 17. *Suppose that b is prime to the discriminant of L. Then W_m has a model defined over Q, and the zeta-function $Z_{\mathfrak{p}}(u)$ of W_m* $\mathrm{mod}(p)$ *over the prime field is given by*

$$Z_p(u) = \prod_{j=0}^{2m} [(1-p^j u)(1-p^{j+1}u)]^{-a(m,2j,0)}$$

$$\times \prod_{i=0}^{4m} \prod_{\nu=0}^{i} \det[1-(\Gamma_b\alpha\Gamma_b)_{\nu+2}p^{(i-\nu)/2}u + (\Gamma_b p\delta\Gamma_b)_{\nu+2}p^{i-\nu+1}u^2]^{(-1)^i a(m,i,\nu)}.$$

In view of the results of Eichler [2] and Shimizu [6], we know that there are some linear relations between the Dirichlet series $D(s; b, k, \rho)$ and Hecke's Dirichlet series attached to cusp forms with respect to congruence subgroups of $SL_2(\mathbf{Z})$. Therefore, from the above corollary, one can derive an estimate for the Fourier coefficients of certain cusp forms, assuming Weil's conjecture to be true. For example, let

$$f(z) = [\Delta(z)\Delta(2z)\Delta(3z)\Delta(6z)]^{\frac{1}{6}} = \sum_{n=1}^{\infty} a_n e^{2\pi i n z},$$

where $\Delta(z) = q \cdot \prod_{n=1}^{\infty}(1-q^n)^{24}$, $q = e^{2\pi i z}$. Then $f(z)$ is a modular form of weight $k = 4$ and of level 6. One can show that $\sum_{n=1}^{\infty} a_n n^{-s}$ is among our $D(s; k, b, \rho)$ for the quaternion algebra of discriminant 6, with $k = 4, b = 1$, $\rho =$ identity representation. Hence, Weil's conjecture together with the above result implies $|a_p| < 2p^{\frac{3}{2}}$ for almost all p.

By a simple observation about the fixed points of $X_0(\Gamma_b\xi\Gamma_b)$, together with the trace-formula of Eichler and Selberg, we can obtain the following "asymptotic estimate" for the eigenvalues. Let p be a prime number not dividing b and the discriminant of L, and let α be an element of $\mathfrak{o}$ such that $\det(\alpha) = p$. Let $r = \dim S_k(\Gamma_b)$ and let $\lambda_1, \cdots, \lambda_r$ be the eigenvalues of $(\Gamma_b\alpha\Gamma_b)_k$. Suppose that $k \geqq 3$ and $b > 2$. Then

$$r^{-1}\sum_{i=1}^{r}|\lambda_i|^2 \leqq (1+p)p^{k-2}[1 + A_k(1 + (p+1)/(g-1))].$$

Here g is the genus of $\Gamma_b\backslash H$, and A_k is a positive constant which depends only on k; $A_k = 1$ if k is odd, and $A_k \leqq 1/3$ if k is even. Let us now take a sequence of positive integers $b_1, b_2, \cdots$ which tends to infinity such that all the b_ν are prime to p, and consider a sequence of groups $\Gamma_{b_1}, \Gamma_{b_2}, \cdots$. Let $v_p(b_\nu)$ denote

$$r^{-1}\sum_{i=1}^{r}|\lambda_i|^2$$

defined for $\Gamma_{b_\nu}\alpha\Gamma_{b_\nu}$. Then, for a fixed p, we have

$$\begin{aligned}\limsup_{\nu\to\infty} v_p(b_\nu) &\leqq (4/3)\cdot(1+p)p^{k-2} && \text{if } k \text{ is even,}\\ &\leqq 2(1+p)p^{k-2} && \text{if } k \text{ is odd.}\end{aligned}$$

This is neither stronger nor weaker than the conjecture $|\lambda_i| \leqq 2p^{(k-1)/2}$.

References

1. W. L. Baily, Jr. and A. Borel, *On the compactification of arithmetically defined quotients of bounded symmetric domains*, Bull. Amer. Math. Soc. **70** (1964), 588–593.

2. M. Eichler, *Quadratische Formen und Modulfunktionen*, Acta Arith. **4** (1958), 217–239.

3. M. Kuga, *Fibre varieties over a symmetric space whose fibres are abelian varieties*, Lecture Notes, University of Chicago, Chicago, Illinois, 1963–1964.

4. M. Kuga and G. Shimura, *On the zeta-function of a fibre variety whose fibres are abelian varieties*, Ann. of Math. (2) **82** (1965), 478–539.

5. S. Lang, *Abelian varieties*, Interscience, New York, 1959.

6. H. Shimizu, *On zeta-functions of quaternion algebras*, Ann. of Math. (2) **81** (1965), 166–193.

7. G. Shimura, *On the zeta-functions of the algebraic curves uniformized by certain automorphic functions*, J. Math. Soc. Japan **13** (1961), 275–331.

8. ———, *On Dirichlet series and abelian varieties attached to automorphic forms*, Ann. of Math. (2) **76** (1962), 237–294.

9. ———, *On analytic families of polarized abelian varieties and automorphic functions*, Ann. of Math. (2) **78** (1963), 149–192.

10. ———, *Arithmetic of unitary groups*, Ann. of Math. (2) **79** (1964), 369–409.

11. ———, *On the field of definition for a field of automorphic functions*, Ann. of Math. (2) (a) I, **80** (1964), 160–189; (b) II, ibid. **81** (1965), 124–165; (c) III, ibid. (to appear).

12. ———, *Moduli and fibre systems of abelian varieties*, Ann. of Math. (to appear).

13. ———, *Class-fields and automorphic functions*, Ann. of Math. (2) **80** (1964), 444–463.

14. ———, *Discontinuous groups and abelian varieties*, (to appear).

15. G. Shimura and Y. Taniyama, *Complex multiplication of abelian varieties and its applications to number theory*, Publ. Math. Soc. Japan, No. 6, Math. Soc. Japan, Tokyo, 1961.

16. A. Weil, *Variétés abéliennes et courbes algébriques*, Hermann, Paris, 1948.

17. ———, *Introduction à l'étude des variétés kählériennes*, Hermann, Paris, 1958.

Hecke's Polynomial as a Generalized Congruence Artin L-function

(A Supplement to Shimura's Lecture)

BY

MICHIO KUGA

1. **L-functions.** Let $\mathfrak{K}$ be an algebraic function field of 1 variable over a finite field κ $(= F_q)$; and let $\mathfrak{K}'$ be an unramified Galois extension of $\mathfrak{K}$, of which the Galois group is denoted by $\mathfrak{G} = \mathrm{Gal}(\mathfrak{K}'/\mathfrak{K})$. Let P be a (topological) field; and let $R : \mathfrak{G} \to GL(N, P)$ be a (continuous) representation of $\mathfrak{G}$ by $N \times N$ matrices whose entries are in P.

For a prime divisor $\mathfrak{p}$ of $\mathfrak{K}$ over κ, take an extension $\mathfrak{P}$ of $\mathfrak{p}$ in $\mathfrak{K}'$. The Frobenius-automorphism of $\mathfrak{P}$ of $\mathfrak{K}'/\mathfrak{K}$ is denoted by $\sigma_{\mathfrak{P}}$. Then, the polynomial

$$\det[1 - R(\sigma_{\mathfrak{P}})u]$$

is independent of the choice of the extension $\mathfrak{P}$ of $\mathfrak{p}$, and it depends only on the prime divisor $\mathfrak{p}$ of $\mathfrak{K}$. This polynomial will be denoted by

$$\psi_p(u).$$

Consider the formal power series

$$\begin{aligned}\psi_p(u^{f_\mathfrak{p}})^{-1} &= \det[1 - R(\sigma_{\mathfrak{P}})u^{f_\mathfrak{p}}]^{-1}\\ &= 1 + a_1u^{f_\mathfrak{p}} + a_2u^{2f_\mathfrak{p}} + \cdots,\\ &\in P[[u]]\ (= \text{the ring of formal power series over } P),\end{aligned}$$

where $f_\mathfrak{p}$ denotes the degree of $\mathfrak{p}$ over κ:

$$N(\mathfrak{p}) = q^{f_\mathfrak{p}}.$$

And consider the product

$$\prod_\mathfrak{p} \psi_\mathfrak{p}(u^{f_\mathfrak{p}})^{-1}$$

taken over all the prime divisors of $\mathfrak{K}/\kappa$. One can see easily that the product is convergent in $P[[u]]$. The formal power series $\prod_\mathfrak{p} \psi_\mathfrak{p}(u^{f_\mathfrak{p}})^{-1}$ is denoted by

$$L(\mathfrak{K}'/\mathfrak{K}, R, u) \qquad (= L(R, u)),$$

and is called an L-function.

LEMMA 1. *If the representation R is reducible and*

$$R \sim \begin{pmatrix} R_1 & * \\ 0 & R_2 \end{pmatrix},$$

then

$$L(R, u) = L(R_1, u)L(R_2, u). \tag{1}$$

Suppose for a moment that $\mathfrak{K}'/\mathfrak{K}$ is a finite extension. Denote by $\phi_1, \phi_2, \cdots, \phi_h$ the system of all irreducible ordinary representations of $\mathfrak{G}$ over C which are realizable in some algebraic number field K. For a fixed prime l, denote by $\Phi_1, \cdots, \Phi_{h'}$ the system of all irreducible modular representations of $\mathfrak{G}$ in a universal domain Ω_l of characteristic l.

Take and fix a prime divisor $\mathfrak{l}$ of l in K. For a formal power series

$$f(u) = \sum a_m u^m \in K[[u]]$$

whose coefficients are $\mathfrak{l}$-adic integer, we put

$$\tilde{f}(u) = \tilde{f}^{\mathfrak{l}}(u) = \sum \tilde{a}_m^{\mathfrak{l}} u^m \in \Omega_l[[u]],$$

where $\tilde{a}_m^{\mathfrak{l}}$ = the residue class of a_m modulo $\mathfrak{l}$.

Now we have the following assertion:

LEMMA 2. (BRAUER-NESBITT).

$$\tilde{L}^{\mathfrak{l}}(\phi_i, u) = \prod_{j=1}^{h'} L(\Phi_j, u)^{d_{ij}} \tag{2}$$

where

$$D = \begin{pmatrix} d_{11} \cdots d_{1h'} \\ \cdot \qquad \cdot \\ \cdot \qquad \cdot \\ \cdot \qquad \cdot \\ d_{h1} \cdots d_{hh'} \end{pmatrix}$$

is the decomposition matrix.

Taking an integral matrix $A = (a_{ki})$ such that $AD = 1_{h'}$ we have

$$L(\Phi_j, u) = \prod_k \tilde{L}^{\mathfrak{l}}(\phi_k, u)^{a_{kj}}. \tag{3}$$

The existence of such an A is due to Brauer-Nesbitt, **[1]**, **[2]**.

2. **Hecke polynomials as L-functions.**

Consider the polynomial

$$\det[1 - (\Gamma_b \alpha_p \Gamma_b)_k u + p(\Gamma_b p\delta\Gamma_b)_k u^2],$$

which was discussed in the last part of Shimura's lecture [3]. (All notations are the same as there.) This polynomial is denoted by $H_k(p, u)$ and will be called Heck's polynomial. We shall write Γ instead of Γ_b.

In his lecture, Shimura introduced a family of abelian varieties $W_m \to V$. Here we are going to study the case $m = 1$. $W_1 \xrightarrow{\pi} V$ is a family whose fibres are 2-dimensional abelian varieties with rings of endomorphisms isomorphic to an order $\mathfrak{O}$ in an indefinite quaternion algebra Φ over Q. Shimura constructed a model of W_1, which is defined over $Q(e^{2\pi i/b})$, and which we identify with W_1.

For almost all prime ideals $\mathfrak{p}$ of $Q(e^{2\pi i/b})$, (i) the reductions $\mathfrak{p}(W_1)$, $\mathfrak{p}(V)$, $\mathfrak{p}(\pi)$, $\mathfrak{p}(h)$, are nonsingular, and (ii) $\mathfrak{p}(\pi)$, $\mathfrak{p}(h)$, are everywhere defined, and (iii) $\mathfrak{p}(\pi)^{-1}(x)$, which we shall denote by $\tilde{A}_x$, carries the canonical structure of an abelian variety, whose zero is $0_x = \mathfrak{p}(h)(x)$, for all $x \in \mathfrak{p}(V)$.

The varieties $\mathfrak{p}(W_1)$, $\mathfrak{p}(V)$, and the maps $\mathfrak{p}(\pi)$, $\mathfrak{p}(h)$, are all defined over $\kappa = F_q =$ the finite field with $q = N(\mathfrak{p})$ elements.

Take a generic point x of $\mathfrak{p}(V)$ over κ. Put $\mathfrak{K} = \kappa(x)$, which is isomorphic to the field of rational functions of $\mathfrak{p}(V)$, defined over κ.

Take a prime number l, prime to $\mathfrak{p}$. The field generated over $\mathfrak{K} = \kappa(x)$, by all of the coordinates of all l^νth division points of $\tilde{A}_x$ $(\nu = 1, 2, \cdots)$ is denoted by $\mathfrak{K}'_l = \mathfrak{K}(\tilde{A}_x, l^\infty)$. It is a Galois extension of $\mathfrak{K}$. Moreover for a given l, there exists a set $U(l)$ of almost all prime ideals in $Q(e^{2\pi i/b})$, such that if $U(l) \ni \mathfrak{p}$, $\mathfrak{K}(\tilde{A}_x, l^\infty)$ is unramified over $\mathfrak{K}$. The Galois group of $\mathfrak{K}(\tilde{A}_x, l^\infty)/\mathfrak{K}$, which is denoted by $\mathfrak{G} = \mathfrak{G}(\tilde{A}_x, l^\infty)$, is in a well-known way, represented by a group of 4 x 4, l-adic matrices: (l-adic representation):

$$\mathfrak{G}(\tilde{A}_x, l^\infty) \ni \sigma \longmapsto M(\sigma) \in \mathrm{GL}(4, Z_l).$$

Moreover, we can see that this representation M is reducible into the sum of two copies of a representation μ:

$$\mathfrak{G} \ni \sigma \longmapsto \mu(\sigma) \in \mathrm{GL}(2, Z_l),$$

$$M \sim \begin{pmatrix} \mu & 0 \\ 0 & \mu \end{pmatrix}.$$

Denote by M_ν the symmetric tensor representation of $\mathrm{GL}(2, Q_l)$ of the degree ν; and consider the representation $M_\nu \circ \mu : \mathfrak{G} \to \mathrm{GL}(\nu + 1, Q_l)$.

PROPOSITION 1. *If $U(l) \ni \mathfrak{p}$, then*

$$Z(\mathfrak{p}(W_m), u) = \prod_{n,\nu} L(\mathfrak{K}'_l/\mathfrak{K}, M_\nu \circ \mu, p^{(n-\nu)/2}u)^{(-1)^n a(2m,n,\nu)}, \tag{4}$$

where, $a(2m, n, \nu)$ are numbers defined on Page 343.

If $U(l) \ni \mathfrak{p}$, $\mathfrak{p}|p$, $p \equiv 1 \pmod b$, then, the variety $\mathfrak{p}(W_m)$ is defined over $\kappa = F_p$ (= the prime field), and the zeta-function of $\mathfrak{p}(W_m)$ is given by

$$Z(\mathfrak{p}(W_m), u) = \frac{\prod_{n,\nu} H_{\nu+2}(p, p^{(n-\nu)/2}u)^{(-1)^n a(2m,n,\nu)}}{\prod_n [(1 - p^{n/2}u)(1 - p^{(n+2)/2}u)]^{a(2m,n,0)}} \tag{5}$$

(cf. Shimura's paper [3] in this volume [2]).

Comparing the right sides of (4), (5) for $m = 0, 1, 2, \cdots$, we have finally

THEOREM 1. *If* $U(l) \ni \mathfrak{p}$, $\mathfrak{p}|p$, $p \equiv 1(b)$, *then*

$$\begin{aligned} L(\mathfrak{K}_l'/\mathfrak{K}, M_\nu \circ \mu, u) &= H_{\nu+2}(p, u) && (\nu > 0), \\ &= \frac{H_2(p, u)}{(1-u)(1-pu)} && (\nu = 0). \end{aligned} \tag{6}$$

3. **Applications.** Assume $\mathfrak{p} \in U(l)$, $p \equiv 1(b)$ from now on. Reducing (modulo l) both sides of the equation in the last corollary; we have

$$\tilde{H}^l_{\nu+2}(p, u) = L((M_\nu \circ \mu)^\sim, u).$$

Because $(M_\nu \circ \mu)^\sim$ is a homorphism of $\mathfrak{G}$ into a finite group, the kernel $\mathfrak{G}_\nu(l)$ of $(M_\nu \circ \mu)^\sim$ is of finite index in $\mathfrak{G}$. Denote by $\mathfrak{K}_\nu(l)$ the fixed field of $\mathfrak{G}_\nu(l)$.

Denote by $\phi_1, \cdots, \phi_h$, or $\Phi_1, \cdots, \Phi_{h'}$, the system of ordinary, or modular, representations of $\mathfrak{G}/\mathfrak{G}_\nu(l)$ respectively. Then using the Brauer-Nesbitt lemma, we have

$$\tilde{H}_{\nu+2}(p, u) = \prod_j L(\mathfrak{K}_\nu(l)/\mathfrak{K}, \Phi_j, u)^{c_j} = \prod_i \tilde{L}^l(\mathfrak{K}_\nu(l)/\mathfrak{K}, \phi_i, u)^{b_i},$$

where c_j is the multiplicity of Φ_j in $(M_\nu \circ \mu)^\sim$, and $b_i = \sum_j a_{ij} b_j$. So

PROPOSITION 2.

$$H_{\nu+2}(p, u) = \prod_i L(\mathfrak{K}_\nu(l)/\mathfrak{K}, \phi_i, u)^{b_i} \quad (\text{modulo } \mathfrak{l}). \tag{7}$$

Now assume, furthermore, that $p \equiv 1(l)$.

The group $\Gamma(l) = \Gamma_{bl}$ is a normal subgroup of $\Gamma = \Gamma_b$; and hence the Riemann surface $V(l) = \Gamma(l)\backslash X$ is a normal covering of $V = \Gamma\backslash X$; where

$$X = \{\tau = x + iy \in C|, y > 0\}.$$

$V(l)$ has a good model defined over $Q(e^{2\pi i/bl})$. (See [3].) Reducing $V(l)$ modulo a prime ideal $\mathfrak{P}$ in $Q(e^{2\pi i/bl})$, we have an algebraic curve $\mathfrak{P}(V(l))$ defined over $\kappa = F_p$. And we can see that the field $\mathfrak{K}_\nu(l)$ is identified with a subfield of the function field of $\mathfrak{P}(V(l))/\kappa$.

Hence, in our case of $p \equiv 1(bl)$, the L-functions $L(\mathfrak{K}_l(V)/\mathfrak{K}, \phi_i, u)$ divide the numerator of the Zetafunction $Z(\mathfrak{P}(V(l)), u)$ of $\mathfrak{P}(V(l))/\kappa$. The latter has, as A. Weil indicated, the following interpretation:

Denote by $J(l)$ the Jacobian variety of $V(l)$, defined over $Q(e^{2\pi i/bl})$. And let $K_{l^\infty} = Q(e^{2\pi i/bl})(J(l), l^\infty)$ be the algebraic number field generated over $Q(e^{2\pi i/bl})$, by all of the coordinates for all the l^νth division points of $J(l)$, $\nu = 1, 2, \cdots$. K_{l^∞} is a normal and infinite extension of $Q(e^{2\pi i/bl})$, whose Galois group will be denoted by $G = G(K_l)$. G is represented by an l-adic representation $M_l : G \to \mathrm{GL}(2g, Z_l)$ with respect to an l-adic coordinate of $J(l)$. Then A. Weil indicated that: the numerator of $Z(\mathfrak{P}(V(l)), u) = \det[1 - M_l(S_P)u]$, where S_P is the Frobenius automorphism of a prime divisor P of $\mathfrak{P}$ in K_{l^∞}.

Combining all of these, we have:

PROPOSITION 3. *If* $p \equiv 1(bl)$, *then*

$$H_{\nu+2}(p, u) \equiv A(u)/B(u) \pmod{l}$$

where A, B *are two polynomials such that*

$$\tilde{A}^l(u) | \widetilde{\det}^l[1 - M_l(S_{\mathfrak{p}})u],$$

$$\tilde{B}^l(u) | \widetilde{\det}^l[1 - M_l(S_{\mathfrak{p}})u].$$

Denote by K_l the smallest Galois extension of Q which contains $Q(e^{2\pi i/bl})$, and the lth division points of $J(l)$. If a prime p such that $p \equiv 1(bl)$ is completely decomposed in K_l, then $M_l(S_{\mathfrak{p}}) \equiv 1 \bmod l$,

$$\tilde{A}^l(u) = (1 - u)^{\text{some power}},$$

$$\tilde{B}^l(u) = (1 - u)^{\text{some power}},$$

and, hence,

$$H_{\nu+2}(p, u) \equiv (1 - u)^{2 \dim \gamma_{\nu+2}(l)}. \tag{8}$$

Conversely we can see that (8) is true for all $\nu = 0, 1, 2, 3, \cdots$, if and only if (8) is true for $\nu = 0, 1, 2, \cdots, l - 1$, if and only if p is decomposed in K_l into a product of primes whose degrees are powers of l. Here, we used the fact that all the irreducible modular representations in the universal domain of characteristic l of the group $\mathrm{SL}(2, Z/lZ)$ are the representations in the spaces of symmetric tensors of degrees ν; $\nu = 0, 1, 2, \cdots, l - 1$.

REFERENCES

1. Brauer-Nesbitt, *On the modular characters of groups*, Ann. of Math. **42** (1941), 556–590; especially p. 588.

2. R. Brauer, *A characterization of the characters of groups of finite order*, Ann. of Math. **57** (1953), 357–377.

3. Shimura, *Moduli of abelian varieties and number theory*, Proc. Sympos. Pure Math., vol. 9, Amer. Math. Soc., Providence, R.I., 1966; pp. 312–332.

4. M. Kuga, *Fiber varieties over a symme'ric space whose fibres are Abelian varieties*, Lecture Notes, The University of Chicago, Chicago, Ill., 1963–1964.

Fiber Varieties Over a Symmetric Space Whose Fibers Are Abelian Varieties

BY

MICHIO KUGA

G. Shimura has realized the importance of the theory of families of abelian varieties with various structures and made a deep study of such families, employing his beautiful number theories of algebraic groups [7], [8].

The purpose of this talk is to give a method of analytic construction of the total space $\mathscr{W}$ of such a family, parametrized, in a certain way, by a compact symmetric space $\mathscr{V} = \Gamma\backslash X$ (X: a symmetric space, Γ a discontinuous group) and to study the cohomology of the constructed total space $\mathscr{W}$, verifying its Hodge property.

1. Let G be a connected, noncompact, semisimple real Lie group with finite center, K a maximal compact subgroup of G, and Γ a discrete subgroup of G for which the quotient space $\Gamma\backslash G$ is compact. Then the homogeneous space $X = G/K$ is a symmetric space on which Γ operates properly discontinuously. If, in addition, Γ has no element of finite order > 1, then Γ operates without fixed points on X, and the quotient space $\Gamma\backslash X = \mathscr{V}$ is a compact manifold.

Let ρ be a representation of G in $\mathrm{GL}(N, \boldsymbol{R})$, and denote the representation space $\boldsymbol{R}^N$ by V.

First Assumption. $\rho(\Gamma) \subseteq \mathrm{GL}(N, \boldsymbol{Z})$.

If one denotes by L the lattice in V corresponding to $\boldsymbol{Z}^N$ in $\boldsymbol{R}^N$, then the first assumption may be expressed as follows: For each γ in Γ the automorphism $\rho(\gamma)$ of V carries L onto itself. As a result, one obtains from $\rho(\gamma)$ an automorphism $\rho(\gamma)$ of the torus $T = V/L$. Since Γ operates on X and T, Γ operates componentwise on the product manifold $X \times T$; this operation is properly discontinuous and without fixed points. Consequently, the quotient space $\Gamma\backslash(X \times T) = \mathscr{W}$ is a compact manifold. Let $p: X \to \mathscr{V}$ and $\tilde{p}: X \times T \to \mathscr{W}$ be quotient maps, and let $\tilde{\pi}: X \times T \to X$ be the projection of $X \times T$ on X. Then there is a unique map $\pi: \mathscr{W} \to \mathscr{V}$ such that $\pi \circ \tilde{p} = p \circ \tilde{\pi}$. One sees that $\mathscr{W}$ is the fiber bundle cover $\mathscr{V}$

(i) whose structure group is Γ and whose fiber is T,

(ii) which is associated with the covering $p: X \to \mathscr{V}$ and

(iii) such that the operation of the structure group Γ on the fiber T is defined by the representation ρ.

2. Complex structure on $\mathscr{W}$.

DEFINITION. A pair $0 = (B, S)$ of real N-by-N matrices is said to be a *symplectic pair* if:

(i) ${}^tB = -B$,
(ii) ${}^tS = S$, S positive-definite,
(iii) $BS^{-1}B = -S$.

From (iii) B is nonsingular, and, therefore, N is even. Let $G_0 = \mathrm{Sp}(B)$ be the set of N-by-N real matrices m such that ${}^tmBm = B$, and let $K_0 = G_0 \cap O(S)$, where $O(S)$ is the set of all real N-by-N matrices m such that ${}^tmSm = S$. K_0 is a maximal compact subgroup of G_0, and the symmetric space $X_0 = G_0/K_0$ is isomorphic to the Siegel upper half plane of genus $N/2$. X_0 possesses two G_0-invariant complex structures. Fix the complex structure on X_0 as that associated with the one-parameter group $j_0(t) = \exp(tB^{-1}S)$ in K_0.

SECOND ASSUMPTION. *There is a nonsingular integral skew-symmetric matrix B such that $\rho(G) \subseteq \mathrm{Sp}(B)$.*

With this one can prove the following proposition:

PROPOSITION. *There is a real symmetric positive-definite matrix S such that:*
(i) (B, S) *is a symplectic pair,*
(ii) $\rho(K) \subseteq O(S)$,
(iii) ${}^td\rho(Z)S - S\,d\rho(Z) = 0$ *for each Z in the orthogonal complement* (*with respect to the Killing form in the Lie algebra of G*) *of the Lie algebra of K.*

Choose a fixed symplectic pair $0 = (B, S)$ which satisfies all of the above conditions. As above, let $G_0 = \mathrm{Sp}(B)$, $K_0 = G_0 \cap O(S)$, and $X_0 = G_0/K_0$. For each g in G define $J(g)$ in $\mathrm{GL}(N, \boldsymbol{R})$ by $J(g) = \rho(g)B^{-1}S\rho(g)^{-1}$. Then J has the following properties:

(a) For each k in K, $J(gk) = J(g)$. Consequently, $J(g) = J(x)$ is well defined for x in X.

(b) For each x in X, $J(x)^2 = -1$.

(c) For each x in X and each γ in Γ, $J(\gamma x) = \rho(\gamma)J(x)\rho(\gamma)^{-1}$.

(d) For each x in X, the matrix $A(x) = BJ(x)$ is symmetric positive-definite.

For each x in X, the matrix $J(x)$ defines the structure of a complex vector space on the real vector space $\boldsymbol{R}^N = V$. This induces the structure of a complex manifold on the torus T, and it is well known that T with the complex structure $J(x)$ is a polarized abelian variety with polarization B. In view of (c), the isomorphism class of this polarized abelian variety depends only on the class of x mod Γ, and, consequently, $\mathscr{W}$ is a fiber system of abelian varieties over $\mathscr{V}$.

THIRD ASSUMPTION. *X is a symmetric domain.*

In this case $\mathscr{V} = \Gamma\backslash X$ is a compact complex manifold which is known to be isomorphic to a projective algebraic variety. From what has been said above, the representation ρ of G sends G into G_0 and K into K_0. Hence, ρ induces a mapping $\tau: X \to X_0$. One can raise the question of whether τ is holomorphic and this will be discussed by Satake [5], [6]. This question is tied up with the existence of a "good" complex structure on $\mathscr{W}$ as follows:

Definition. A complex structure $\mathscr{J}$ on $\mathscr{W}$ is called *good* if

(i) the map $\pi : \mathscr{W} \to \mathscr{V}$ is holomorphic,

(ii) the restruction of $\mathscr{J}$ to the fiber over each point of $\mathscr{V}$ gives the complex structure of the abelian variety already identified with that fiber,

(iii) the universal covering manifold $X \times V$ of $\mathscr{W}$, fortified with the complex structure induced by $\mathscr{J}$, is a holomorphic complex vector bundle over X.

Theorem 1. *$\mathscr{W}$ possesses good complex structures if and only if the map $\tau : X \to X_0$ is holomorphic, and, in this case, there is only one good complex structure on $\mathscr{W}$. Moreover, if τ is holomorphic, then* (1) *$\mathscr{W}$ is isomorphic to a projective algebraic variety, and* (2) *$\mathscr{W}$ is a minimal model in the sense that an arbitrary rational map of any variety $\mathscr{U}$ in $\mathscr{W}$ is always regular at each simple point of $\mathscr{U}$.*

A proof of (1) of this Theorem 1, i.e. of that $\mathscr{W}$ is a Hodge variety, will be sketched in later sections.

Consequently, there arises the following important problem, which Satake [5], [6] will discuss:

Find all representations $\rho : G \to \mathrm{Sp}(N/2)$ such that (i) *τ is holomorphic and* (ii) $\rho(\Gamma) \subseteq \mathrm{GL}(N, Z)$.

3. **Cohomology of $\mathscr{W}$.** In this section only the first of the three assumptions is needed. Let $Q_0 = p(x_0)$ be a point of $\mathscr{V}$; if N is a small neighborhood of x_0, then $\tilde{p}$ defines an isomorphism $N \times T \xrightarrow{\cong} \pi^{-1}(p(N))$. One obtains, thus, for each Q in $p(N)$ an isomorphism ψ_{Q_0Q} of the fiber T_{Q_0} over Q_0 with the fiber T_Q over Q, which is independent of the neighborhood N and the point x_0. Moreover, $\psi_{Q_0Q_2} = \psi_{Q_1Q_2} \circ \psi_{Q_0Q_1}$ whenever the points Q_0, Q_1, Q_2 are near each other. These "shifts" can be continued along any path in $\mathscr{V}$, and, in particular, along any loop based at Q_0. In this way the fundamental group $\pi_1(\mathscr{V}, Q_0)$ operates on the fiber T_{Q_0}, and a representation ψ of $\pi_1(\mathscr{V}, Q_0)$ in the group of automorphisms of T_{Q_0} is given. If the point x_0 such that $p(x_0) = Q_0$ is fixed, then there are canonical isomorphisms between $\pi_1(\mathscr{V}, Q_0)$ and Γ, on the one hand, and T_{Q_0} and T, on the other. Through these isomorphisms the representation ψ of $\pi_1(\mathscr{V}, Q_0)$ may be seen to correspond to the representation ρ of Γ.

It is known that $H_1(T) = V$ and that $H_r(T) = \Lambda^r V =$ rth exterior power of V. The operation of Γ on $H_1(T)$ is given by ρ, and the operation of Γ on $H_r(T)$ is given by $\Lambda^r\rho$. The space $H^r(T)$ is the dual space $(\Lambda^r V)^*$ of $H_r(T)$, and the corresponding operation of Γ is by $(\Lambda^r\rho)^*$.

To obtain the cohomology groups of $\mathscr{W}$, one considers the spectral sequence $\{E_r^{pq}\}$ of $\pi : \mathscr{W} \to \mathscr{V}$ for which $E_2^{pq} \cong H^p(\mathscr{V}, H^q(T))$ and $H^r(\mathscr{W}) \cong \sum_{p+q=r} \{E_\infty^{pq}\}$. It can be proved, in this case, that $E_\infty^{pq} = E_2^{pq}$, and moreover, one has

$$H^p(\mathscr{V}, H^q(T)) \cong H^p(X, \Gamma, (\Lambda^q\rho)^*) \cong H^p(\Gamma, (\Lambda^q\rho)^*)$$

(for notations, see Murakami's lecture). Hence,

$$H^r(\mathscr{W}) \cong \sum_{p+q=r} H^p(X, \Gamma, (\Lambda^q\rho)^*) \cong \sum_{p+q=r} H^p(\Gamma, (\Lambda^q\rho)^*).$$

Harmonic forms in $\mathscr{W}$. Let ds_0^2 denote a fixed Riemannian metric in X. A Riemannian metric in $\mathscr{W}$ may be introduced as follows: Choose a real symmetric positive-definite matrix S such that (i) $\rho(K) \subseteq O(S)$ and (ii) ${}^t d\rho(Z)S - S\, d\rho(Z) = 0$ for each Z in the orthogonal complement of the Lie algebra of K. For each g in G define $A(g) = {}^t\rho(g)^{-1}S\rho(g)^{-1}$. Then (i) $A(gk) = A(g)$ for g in G, k in K, so that $A(x) = A(g)$ well-defines $A(x)$ for x in X; and (ii) $A(x)$ is symmetric positive-definite. The metric $ds^2 = ds_0^2 + {}^t du A(x)\, du$ in $X \times T$, where the column vector u denotes a coordinate in T, induces a Riemannian metric in $\mathscr{W}$. In the following, the symbol $\mathscr{H}$ will be used for various spaces of harmonic differential forms. In the first place, one has a subspace $\mathscr{H}^p(X, \Gamma(\Lambda^q\rho)^*)$ of harmonic forms in

$$A^p(X, \Gamma, (\Lambda^q\rho)^*) = \{\hat{\omega} \in A^p(X) \otimes \Lambda^q(V)^* | \hat{\omega} \circ \gamma = (\Lambda^q\rho(\gamma))^*\hat{\omega} \quad \text{for all} \quad \gamma \in \Gamma\}$$
$$\subset A^p(X) \otimes \Lambda^q(V)^*,$$

(see Murakami's lecture note for the notations A^p), and by "Hodge's Theorem", the inclusion of $\mathscr{H}^p$ in A^p induces an isomorphism

$$\mathscr{H}^p(X, \Gamma, (\Lambda^q\rho)^*) \cong H^p(X, \Gamma, (\Lambda^q\rho)^*).$$

Let $\mathscr{H}^r(\mathscr{W})$ denote the space of harmonic r-forms on $\mathscr{W}$.

PROPOSITION. *The space* $\mathscr{H}^r(\mathscr{W})$ *admits a direct sum decomposition*

$$\mathscr{H}^r(\mathscr{W}) = \sum_{p+q=r} \mathscr{H}^{(p,q)}(\mathscr{W})$$

in which $\mathscr{H}^{(p,q)}(\mathscr{W})$ *is isomorphic to* $\mathscr{H}^p(X, \Gamma, (\Lambda^q\rho)^*)$.

It is the purpose of this paragraph to describe the said isomorphism explicitly.

DEFINITION OF $\mathscr{H}^{(p,q)}(\mathscr{W})$. An arbitrary differential r-form on $X \times T$ can be written in the form

$$\sum_{p+q=r} \sum_{(i,j)} f_{(i,j)}(x, u)\, dx^{i_1} \wedge \cdots \wedge dx^{i_p} \wedge du^{j_1} \wedge \cdots \wedge du^{j_q},$$

so that one has:

$$A^r(X \times T) = \sum_{p+q=r} A^{(p,q)}(X \times T) \qquad \text{(direct sum)},$$

where $A^{(p,q)}(X \times T)$ be the space of $(p + q)$-forms of the form:

$$\sum_{(i,j)} f_{(i,j)}(x, u)\, dx^{i_1} \wedge \cdots \wedge dx^{i_p} \wedge du^{j_1} \wedge \cdots \wedge du^{j_q},$$

p terms taken over the dx, q terms taken over the du.

Let $P^{(p,q)}$ denote the projection $A^r \to A^{(p,q)}$. The operations of Γ on the differential forms (induced by the operations of Γ in $X \times T$) commute with each $P^{(p,q)}$

so that $A^r(\mathscr{W})$ admits a direct sum decomposition

$$A^r(\mathscr{W}) = \sum_{p+q=r} A^{(p,q)}(\mathscr{W}).$$

Since the "Laplacian" in $\mathscr{W}$ can be shown to commute with $P^{(p,q)}$, one has

$$\mathscr{H}^r(\mathscr{W}) = \sum_{p+q=r} \mathscr{H}^{(p,q)}(\mathscr{W}),$$

where

$$\mathscr{H}^{(p,q)}(\mathscr{W}) = \mathscr{H}^r(\mathscr{W}) \cap A^{(p,q)}(\mathscr{W}).$$

Definition of the isomorphism. The isomorphism

$$\mathscr{H}^{(p,q)}(\mathscr{W}) \to \mathscr{H}^p(X, \Gamma, (\Lambda^q\rho)^*)$$

will be exhibited as a map

$$\begin{cases} A^{(p,q)}(X \times T) \to A^p(X) \otimes (\Lambda^q V)^* = \operatorname{Hom}(\Lambda^q(V), A^p(X)), \\ \omega \mapsto \hat{\omega}. \end{cases}$$

Let ω be an element of $A^{(p,q)}(X \times T)$, and let z be a q-cycle in T which represents a homology class z in $H_q(T) = \Lambda^q V$. Define $\hat{\omega}(z)$ in $A^p(X)$ for

$$\omega = \sum_{(i,j)} f_{(i,j)}(x, u)\, dx^{i_1} \wedge \cdots \wedge dx^{i_p} \wedge du^{j_1} \wedge \cdots \wedge du^{j_q}$$

by

$$\hat{\omega}(z) = \sum_{(i,j)} dx^{i_1} \wedge \cdots \wedge dx^{i_p} \int_z f_{(i,j)}(x, u)\, du^{j_1} \wedge \cdots \wedge du^{j_q}.$$

4. **An example.** Let $G = \mathrm{SL}(2, R)$, $K = \mathrm{SO}(2)$, $X =$ upper half of the complex plane. Let $\mathscr{L}$ be an indefinite division quaternion algebra over $\boldsymbol{Q}$, which is, by definition, a division algebra over $\boldsymbol{Q}$ such that $\mathscr{L} \otimes_{\boldsymbol{Q}} \boldsymbol{R} = M_2(\boldsymbol{R})$. Let $\mathscr{O}$ be a maximal order in $\mathscr{L}$. Regarding $\mathscr{L}$ as a subring of $M_2(\boldsymbol{R})$, let $\Gamma = \Gamma_b$ be the set of all ξ in $\mathscr{O}$ such that (i) $\xi\mathscr{O} = \mathscr{O}$, (ii) $\det \xi = 1$, (iii) $\xi = 1 \bmod b\mathscr{O}$, where b is some integer larger than 2. Let $V_m = M_2(\boldsymbol{R})^m$, $L_m = \mathscr{O}^m$, and define $\rho_m : G \to \mathrm{GL}(V_m)$ by

$$\rho(\alpha)(\zeta_1, \cdots, \zeta_m) = (\alpha\zeta_1, \cdots, \alpha\zeta_m)$$

for each α in G, where m is any positive integer. From $T_m = V_m/L_m$, one forms $X \times T_m$ and $\mathscr{W}_m = \Gamma\backslash(X \times T_m)$ as described in §1. In this case the space $\mathscr{H}^r(\mathscr{W}_m)$ of harmonic forms can be made completely explicit in terms of automorphic forms in X associated with Γ.

It is well known that the only irreducible representations of $\mathrm{SL}(2, \boldsymbol{R})$ are the symmetric tensor representations. Let M_ν denote the symmetric tensor representation of degree ν. The representation ρ_m, and also the representation $\Lambda^q\rho_m$, can be decomposed by means of the M_ν. In fact, one has

$$\Lambda^q\rho_m \sim \sum_\nu a(2m, q, \nu)M_\nu$$

where

$$\begin{aligned} a(n, q, v) &= \binom{n}{\frac{q+v}{2}}\binom{n}{\frac{q-v}{2}} - \binom{n}{\frac{q+v}{2}+1}\binom{n}{\frac{q-v}{2}-1}, & q &\equiv v(2), \\ &= 0, & q &\not\equiv v(2). \end{aligned}$$

Consequently,

$$\mathscr{H}^p(X, \Gamma, (\Lambda^q\rho_m)^*) \cong \sum_v a(2m, q, v)\mathscr{H}^p(X, \Gamma, M_v),$$

and Shimura [9] has shown:

$$\begin{aligned} &\mathscr{H}^0(M_0) \cong C, \\ &\mathscr{H}^0(M_v) \cong \{0\} \qquad \text{for } v > 0, \\ &\mathscr{H}^1(M_v) \cong \gamma_{v+2} \oplus \bar{\gamma}_{v+2} \qquad \text{for all } v, \\ &\mathscr{H}^2(M_0) \cong C\omega_0, \\ &\mathscr{H}^2(M_v) \cong \{0\} \qquad \text{for } v > 0, \end{aligned}$$

where γ_{v+2} denotes the space of cusp forms of weight $v + 2$ belonging to Γ, $\bar{\gamma}_{v+2}$ denotes the complex conjugate space of γ_{v+2}, and $\omega_0 = y^{-2}(d\tau \wedge d\bar{\tau})$.

Combining these, we have

$$\begin{aligned} \mathscr{H}^p(\mathscr{W}_m) &\cong a(2m, p, 0)C \\ &\oplus \sum_v^{p-1} a(2m, p-1, v)(\gamma_{v+2} \oplus \bar{\gamma}_{v+2}) \qquad (1) \\ &\oplus a(2m, p-2, 0)C\omega_0. \end{aligned}$$

For the sake of simplicity, we shall identify the two sides of (1).

Now consider the "Hecke-operator" $\Gamma\alpha\Gamma$ ($= \Gamma_b\alpha\Gamma_b$ in Shimura's lecture), which is an algebraic correspondence of the variety $\mathscr{W}_m$. The Lefschetz number $I(\Gamma\alpha\Gamma)$ of the correspondence is given by the Lefschetz fixed point formula:

$$I(\Gamma\alpha\Gamma) = \sum_{p=0} (-1)^p \operatorname{tr}((\Gamma\alpha\Gamma)|\mathscr{H}^p(\mathscr{W}_m)).$$

Here $(\Gamma\alpha\Gamma|\mathscr{H}^p(\mathscr{W}_m))$ is the linear endomorphism of $\mathscr{H}^p(\mathscr{W}_m)$ induced by the correspondence $\Gamma\alpha\Gamma$. (For precise definitions see [2], [4].) And, moreover, we can see that $(\Gamma\alpha\Gamma|\mathscr{H}^p(\mathscr{W}_m))$ sends each subspace of $\mathscr{H}^p(\mathscr{W}_m)$ appearing in the decomposition (1) into itself; and this operation coincides with

(i) the scalar multiplication $c \mapsto (\det \alpha)^{p/2}\, d(\alpha)c$ on the subspace $a(2m, p, 0)C$, where $d(\alpha)$ denotes the number of left cosets in $\Gamma\alpha\Gamma$,

(ii) the scalar multiplication $c \mapsto (\det \alpha)^{(p-2)/2}\, d(\alpha)c$ on the subspace

$$a(2m, p-2, 0)C\omega_0,$$

(iii) the Hecke operator: $(\det(\alpha))^{(p-1-\nu)/2}(\Gamma\alpha\Gamma)_{\nu+2}$ (c.f. Shimura's lecture) on the subspace identified with $\gamma_{\nu+2}$.

So combining these we have finally the formula

$$I(\Gamma\alpha\Gamma) = 2\sum_{b=0}^{4m}(-1)^b a(2m, b, 0)\det(\alpha)^{b/2}\, d(\alpha)$$
$$-\,2\sum_{b=0}^{4m}\sum_{\nu=0}^{b}(-1)^b a(2m, b, \nu)(\det(\alpha))^{(b-\nu)/2}\operatorname{Re}[\operatorname{tr}(\Gamma\alpha\Gamma)_{\nu+2}].$$

REMARK. The notation of Hecke operator $\Gamma\alpha\Gamma$ is also defined in the case of higher dimensional quotients $\Gamma\backslash X$ of symmetric spaces, and an analogous formula for $I(\Gamma\alpha\Gamma)$ is calculated in terms of the operation of $\Gamma\alpha\Gamma$ on the space of vector valued harmonic forms [2].

5. **Further structure of (co-) homology groups.** By our construction of the fiber bundle $\pi\colon \mathscr{W} \to \mathscr{V}$, each fiber has the structure of an abelian group (torus) canonically. Denote by $\tilde{h}$ the section $X \to X \times T$ defined by $\tilde{h}\colon x \mapsto (x, 0)$; and let h be the uniquely determined section $h\colon \mathscr{V} \to \mathscr{W}$ satisfying $h \circ p = \tilde{p} \circ \tilde{h}$. h is the section of zeros: $h(Q) =$ the zero of T_Q. Furthermore, consider the automorphism $\tilde{\theta}$ of $X \times T$ defined by $\tilde{\theta}\colon (x, u) \mapsto (x, -u)$. Let θ be the uniquely determined automorphism of $\mathscr{W}$ which satisfies $\tilde{p} \circ \tilde{\theta} = \theta \circ \tilde{p}$ and $\pi \circ \theta = \pi$. θ is called the upside-down operator. Since $\theta^2 =$ identity map, θ induces linear automorphisms θ^* (resp. θ_* on the group $H^*(W)$ (resp. $H_*(W)$). Put

$$H^*(\mathscr{W})^+ = \{z \in H^*(\mathscr{W}) | \theta^*(z) = z\},$$
$$H^*(\mathscr{W})^- = \{z \in H^*(\mathscr{W}) | \theta^*(z) = -z\},$$
$$H_*(\mathscr{W})^+ = \{z \in H_*(\mathscr{W}) | \theta_*(z) = z\},$$
$$H_*(\mathscr{W})^- = \{z \in H_*(\mathscr{W}) | \theta_*(z) = -z\}.$$

Then,

(2) $$H^*(\mathscr{W}) = H^*(\mathscr{W})^+ + H^*(\mathscr{W})^- \quad \text{(direct sum)},$$

(3) $$H_*(\mathscr{W}) = H_*(\mathscr{W})^+ + H_*(\mathscr{W})^- \quad \text{(direct sum)}.$$

In (2) and (3), $H^*(\mathscr{W})^{\pm}$ is the annihilator of $H_*(\mathscr{W})^{\mp}$, and so $H^*(\mathscr{W})^+$ and $H_*(\mathscr{W})^+$ are dual to each other and $H^*(\mathscr{W})^-$ and $H_*(\mathscr{W})^-$ are dual to each other (namely, (2) and (3) are dual decompositions).

Because θ preserves the Riemannian metric ds^2, θ^* induces an endomorphism of $\mathscr{H}^{\nu}(\mathscr{W})$. And defining $\mathscr{H}^p(\mathscr{W})^+$, $\mathscr{H}^p(\mathscr{W})^-$ similarly, we have

$$\mathscr{H}^p(\mathscr{W})^+ = \sum_{a+b=p, b\equiv 0(2)} \mathscr{H}^{(a,b)}(\mathscr{W}) \cong \sum_{a+b=p, b\equiv 0(2)} H^a(X, \Gamma, \Lambda^b(V)^*),$$
$$\mathscr{H}^p(\mathscr{W})^- = \sum_{a+b=p, b\equiv 1(2)} \mathscr{H}^{(a,b)}(\mathscr{W}) \cong \sum_{a+b=p, b\equiv 1(2)} H^a(X, \Gamma, \Lambda^b(V)^*).$$

In particular

$$\begin{aligned} \mathscr{H}^2(\mathscr{W})^+ &= \mathscr{H}^{(2,0)}(\mathscr{W}) + \mathscr{H}^{(0,2)}(\mathscr{W}) \\ &\cong H^2(X, \Gamma, \text{trivial}) \oplus H^0(X, \Gamma, \Lambda^2(V)^*) \\ &\cong H^2(\mathscr{V}) \oplus [\Lambda^2(V)^*]^\Gamma \\ &\cong H^2(\mathscr{V}) \oplus [H^2(T_{Q_0})]^{\pi_1(V, Q_0)} \end{aligned} \tag{4}$$

where Q_0 is any point of $\mathscr{V}$.

Take a point $x_0 \in X$ such that $p(x_0) = Q_0$, and consider the injection $j: T \to \mathscr{W}$, defined by $j(u) = \tilde{p}(x_0, u)$. Obviously $j(T) = T_{Q_0}$.

PROPOSITION. $H_2(\mathscr{W})^+ = h_*(H_2(\mathscr{V})) + j_*(H_2(T))$ *(direct sum) and this is the* dual decomposition *of* (4).

In the case where $\mathscr{W}$ has a good complex structure $\mathscr{J}$ with respect to a symplectic pair $0 = (B, S)$, the Riemann metric $ds^2 = ds_0^2 + duA(x)\,du$ (where $A(x) = {}^t p(g)^{-1}\, Sp(g)^{-1}$) is Kähler with respect to that $\mathscr{J}$, and the fundamental 2-form Ω is shown to be $\Omega = \Omega_0 + {}^t du \wedge B\, du$, where Ω_0 is the fundamental 2-form of ds_0^2. Moreover, the 2-forms Ω_0 and ${}^t du \wedge B\, du$ on $X \times T$ can be considered also to be 2-forms on $\mathscr{W}$; and

$$\Omega_0 \in \mathscr{H}^{(2,0)}(\mathscr{W}), \qquad {}^t du \wedge B\, du \in \mathscr{H}^{(0,2)}(\mathscr{W}).$$

From these data we can conclude that ds^2 is a Hodge metric of $\mathscr{W}$ if we take as ds_0^2 a Hodge metric of $\mathscr{V}$; and this gives a proof that $\mathscr{W}$ is algebraic.

In fact, for any 2-cycle

$$Z = Z_1 + Z_2 + Z_3 \in H_2(\mathscr{W}, Q) = H_2(\mathscr{W}, Q)^- + h_*(H_2(\mathscr{V}, Q)) + j_*(H_2(T, Q)),$$

we have

$$\begin{aligned} \int_Z \Omega &= \int_{Z_1 + Z_2 + Z_3} \Omega_0 + {}^t du \wedge B\, du \\ &= \int_{Z_2} \Omega_0 + \int_{Z_3} {}^t du \wedge B\, du. \end{aligned}$$

Employing the Hodge properties of $\mathscr{V}$ and of abelian varieties (the latter is nothing else than the integrality of B), we see that $\int_Z \Omega \in Q$. This shows that ds^2 is a Hodge metric of $\mathscr{W}$.

6. **Several comments.** (1) Let $\pi: \mathscr{W} \to \mathscr{V}$ be an algebraic family of polarized abelian varieties defined by $G/K = X, \Gamma, \rho, B, S$ as in §1. And let k be a field of definition for $\mathscr{W}, \mathscr{V}, \pi$. Take a generic point Q_0 of $\mathscr{V}$ over k, and consider the fiber T_{Q_0} at Q_0. Taking a point x_0 in X, such that $p(x_0) = Q_0$, we can identify:

$$T_{Q_0} = x_0 \times T = T, \qquad \pi_1(\mathscr{V}, Q_0) = \Gamma.$$

In the homology group $H_{2r}(T_{Q_0}, \boldsymbol{R})$ of the abelian variety T_{Q_0}; consider the subspace $\mathfrak{a}_r(T_{Q_0}, \boldsymbol{R})$ generated by the algebraic r-cycles of T_{Q_0} (cf. Borel–Haefliger [**1**]).

On the other hand, as is described in §3, $\pi_1(\mathscr{V}, Q_0) = \Gamma$ operates on $H_{2r}(T_{Q_0}, \boldsymbol{R}) = H_{2r}(T, \boldsymbol{R}) = \Lambda^{2r}(V)$. Consider the subgroup $H_{2r}(T_{Q_0}, \boldsymbol{R})^{\pi_1(\mathscr{V}, Q_0)} = \Lambda^{2r}(V)^{\Gamma}$ of Γ-invariant elements in $H_{2r}(T_{Q_0}, \boldsymbol{R}) = \Lambda^{2r}(V)$.

THEOREM. $H_{2r}(T_{Q_0}, \boldsymbol{R})^{\pi_1(\mathscr{V}, Q_0)} \supset \mathfrak{a}_r(T_{Q_0})$ *for a generic point* Q_0, *of* $\mathscr{V}$ *over* k.

For a sketch of this theorem, see [**3**].

REMARK 1. By a theorem of Borel, $\Lambda^{2r}(V)^{\Gamma} = \Lambda^{2r}(V)^{G}$; so this is determined by the theory of tensor invariants of Lie groups.

REMARK 2. $H_{2r}(T_{Q_0}, \boldsymbol{R})^{\pi_1(\mathscr{V}, Q_0)} = \mathfrak{a}_r(T_{Q_0})$ implies the coincidence of numerical equivalence and homological equivalence of cycles of codimension r in the abelian variety T_{Q_0}.

REMARK 3. In many cases the equality $H_{2r}(T_Q, \boldsymbol{R})^{\pi_1(\mathscr{V}, Q_0)} = \mathfrak{a}_r(T_{Q_0})$ holds. For example, it holds if G is a product of $\mathrm{Sp}(n_i, \boldsymbol{R})$. There are some examples for which $H_{2r}(T_{Q_0}, \boldsymbol{R})^{\pi_1(\mathscr{V}, Q_0)} \neq \mathfrak{a}_r(T_{Q_0})$.

(2) Shimura [**9**] defined an abelian variety $A(\gamma_k(\Gamma))$ attached to the space of automorphic forms $\gamma_k(\Gamma)$ of dimension $-k$. This is interpreted as a factor of the higher Jacobian variety $J^{[r]}(\mathscr{W}_m)$, where the variety $\mathscr{W}_m$ is defined in §3:

$$J^{[r]}(\mathscr{W}_m) \underset{(\text{isogeny})}{\sim} \sum_{v=0}^{r-1} a(2m, r-1, v) A(\gamma_{v+2})$$

for odd r.

REFERENCES

1. A. Borel and A. Haefliger, *La classe d'homologie fondamentale d'un espace analytique*, Bull. Soc. Math. de France **89** (1961), 461–513.

2. M. Kuga, *Fiber varieties over a symmetric space whose fibers are abelian varieties*, Lecture notes, The University of Chicago, 1964.

3. ———, *Fibre variety over symmetric space whose fibres are abelian varieties*, Proceedings of the U.S.–Japan Seminar in Differential Geometry, Kyoto, Japan, 1965, Nippon Hyoronsha, 1966.

4. S. Lefschetz, *Topology*, Amer. Math. Soc. Colloq. Pub., vol. 12, Amer. Math. Soc., Providence, R.I., 1930, p. 389.

5. I. Satake's several papers on symplectic representations. See references in [**6**].

6. ———, *Symplectic representations of algebraic groups*, Proc. Sympos. Pure Math., vol. 9, Amer. Math Soc., Providence, R.I., 1966, pp. 352–357.

7. G. Shimura's many many papers about families of abelian varieties and/or modular forms, etc., most of them were published in the Annals. See references of [**2**], [**8**].

8. ———, *Moduli of abelian varieties and number theory*, Proc. Sympos. Pure Math., vol. 9, Amer. Math. Soc., Providence, R.I., 1966, pp. 312–332.

9. ———, *Sur les intégrales attachées aux forms automorphes*, J. Math. Soc. Japan **11** (1959), 291–311.

10. Y. Matsushima and S. Murakami, *On vector bundle valued harmonic forms and automorphic forms on symmetric Riemannian manifolds*, Ann. of Math. **78** (1963), 365–416.

Families of Abelian Varieties

BY

DAVID MUMFORD

In previous lectures, Kuga, Shimura, and Satake have considered various families of abelian varieties parametrized by the quotients of bounded symmetric domains by arithmetic subgroups. In particular, Shimura characterized certain of these families by means of the structure of the ring of endomorphisms—the "PEL-types." My purpose here is to show that an even larger class of Kuga's families can be characterized by intrinsic properties of the abelian varieties occurring in them. The properties in question involve the Kählerian geometry of the abelian varieties, but, assuming a famous conjecture of Hodge, they are equivalent to purely "algebro-geometric" properties of the abelian varieties. The results of this lecture are partly joint work with J. Tate.

1. **The Hodge group of a complex torus.** To give a complex torus A of dimension g is the same thing as giving

(i) a $2g$-dimensional rational vector space V;

(ii) a complex structure on $V_{\boldsymbol{R}} = V \otimes_{\boldsymbol{Q}} \boldsymbol{R}$;

(iii) a lattice $L \subset V$.

Here $V = H_1(A, \boldsymbol{Q})$, $L = H_1(A, \boldsymbol{Z})$, and the complex structure on $V_{\boldsymbol{R}}$ is induced by the natural isomorphism between $V_{\boldsymbol{R}}$ and the universal covering space of A. If we are only interested in the type of A up to isogenies, we can omit L. The datum (ii) is equivalent to either of the following objects:

(ii′) an endomorphism $J: V_{\boldsymbol{R}} \to V_{\boldsymbol{R}}$ such that $J^2 = -I$,

(ii″) a homomorphism of algebraic groups,

$$\phi: T \to \mathrm{GL}(V)$$

defined over $\boldsymbol{R}$ where T is the compact 1-dimensional torus over $\boldsymbol{R}$, i.e.,

$$T_{\boldsymbol{R}} = \{z \in \boldsymbol{C} \,|\, |z| = 1\};$$

and such that ϕ, as a representation of G_m, has weights $+1$ and -1, each with multiplicity g.

Starting with a complex structure on $V_{\boldsymbol{R}}$, we get data (ii′) and (ii″) as follows:

J = multiplication by i.

$\phi(e^{i\theta})$ = the element of $\mathrm{GL}(V)_{\boldsymbol{R}}$ given by multiplying in the complex structure on $V_{\boldsymbol{R}}$ by $e^{i\theta}$.

esp: $J = \phi(i)$.

DEFINITION. The *Hodge group* of A, written $Hg(A)$, is the smallest algebraic subgroup of $\mathrm{GL}(V)$ defined over Q and containing $\phi(T)$.

Since T is connected, it follows immediately that $Hg(A)$ is a connected algebraic group. A few more definitions:

DEFINITION. Let A be a complex torus, and let

$$H^k(A, C) \cong \sum_{p+q=k} H^{p,q}(A)$$

be the Kähler decomposition of the cohomology of A. Then the *Hodge ring* of A is

$$H_0^*(A) = H^*(A, Q) \cap \sum_{p=0}^{\dim A} H^{p,p}(A).$$

Hodge's conjecture asserts that $H_0^*(A)$ is the subring of $H^*(A, Q)$ given by the Q-linear combinations of the fundamental classes of algebraic subvarieties of A.

Note that: if the complex torus A equals $V_{\mathbf{R}}/L$, then there is a canonical isomorphism:

$$H^i(A \times \cdots \times A, Q) \cong \wedge^i(V^* \oplus \cdots \oplus V^*).$$

Therefore, there is a natural representation of $Hg(A)$ on $H^*(A^k, Q)$, defined over Q.

PROPOSITION 1. *For all k, the Hodge ring of A^k is the ring invariants of $Hg(A)$ in $H^*(A, Q)$.*

Using this Proposition, it is easy to give examples of abelian varieties A such that their Hodge ring is not generated by elements of degree 2 [cf. §3 for the existence of abelian varieties with various Hodge groups].

2. **The structure of the Hodge group of an abelian variety.** The result is the following:

THEOREM. *If A is an abelian variety, then*

(i) *$Hg(A)$ is a connected reductive group,*

(ii) *$\phi(-1)$ is the center of G, and centralizer $[\phi(i)]$ = centralizer $[\phi(T)]$: call this group Z,*

(iii) *$Z_{\mathbf{R}}^0$ is a maximal compact subgroup of $Hg_{\mathbf{R}}^0$ and $Hg_{\mathbf{R}}^0/Z_{\mathbf{R}}^0$ is a bounded symmetric domain.*

COROLLARY (OF (i)). *$Hg(A)$ is the largest subgroup of $\mathrm{GL}(V)$ which leaves invariant the Hodge rings of A^k for all k. Hence the Hodge group $Hg(A)$ as a subgroup of $\mathrm{GL}(V)$ and the collection of Hodge rings $H_0^*(A^k)$ as subrings of*

$$\wedge^*[V^* \oplus \cdots \oplus V^*]$$

are "equivalent" invariants of the abelian variety A: i.e., each can be computed from the other by linear algebra.

DEFINITION. The *Hodge type* of an abelian variety A of dimension g consists in the set of "equivalent" diagrams

$$T \xrightarrow{\phi} Hg(A) \subset \mathrm{GL}(2g)$$

obtained by identifying $\mathrm{GL}[H_1(A, Q)]$ with $\mathrm{GL}(2g)$ rationally over Q; where two diagrams

$$T \xrightarrow[\phi_1]{} H_1 \subset \mathrm{GL}(2g),$$

$$T \xrightarrow[\phi_2]{} H_2 \subset \mathrm{GL}(2g),$$

are considered equivalent if there are elements $\alpha \in \mathrm{GL}(2g)_Q$, $\beta \in (H_1)_R$ such that

$$H_2 = \alpha H_1 \alpha^{-1},$$

$$\phi_2(\lambda) = \alpha\beta\phi_1(\lambda)\beta^{-1}\alpha^{-1}.$$

One should notice that once the Q-rational subgroup $H \subset \mathrm{GL}(2g)$ is given, there are only a finite number of Hodge types (H, ϕ) extending H. This follows easily from the conjugacy of maximal compact tori in H via points of H_R, and from the restriction on the weights of $\phi(T)$ in this representation.

DEFINITION. Let (H, ϕ) and (H', ϕ') be two Hodge types. Then (H, ϕ) is a refinement of (H', ϕ') if these types are represented by diagrams

$$T \xrightarrow{\phi} H \subset \mathrm{GL}(2g),$$

$$T \xrightarrow{\phi'} H' \subset \mathrm{GL}(2g),$$

where $H \subset H'$ and $\phi' = \phi$.

3. **The families.** Now suppose that a Hodge type (H, ϕ) is given. We will see that the set of all abelian varieties of this Hodge type, plus the limits which have finer Hodge types will be a family over a bounded symmetric domain, such that the action of certain arithmetic groups on the domain lifts to an action on the family.

DEFINITION. *A Hermitian symmetric pair* $(\mathscr{G}, J)$ is a real connected Lie group $\mathscr{G}$ with compact center, and an element $J \in \mathfrak{G}$, its Lie algebra, such that

(i) $\mathrm{ad}\, J$ has three eigenspaces in $\mathfrak{G}_C$: $\mathfrak{K}_C$ (the complexification of a real subspace $\mathfrak{K}$), $\mathfrak{p}_+$, and $\mathfrak{p}_-$ with eigenvalues 0, $+2i$, $-2i$,

(ii) $\mathfrak{K}$ is the Lie algebra of a maximal compact subgroup $\mathscr{K}$ in $\mathscr{G}$.

DEFINITION. Let $(\mathscr{G}, J)$ be a Hermitian symmetric pair. A faithful representation

$$\rho : \mathscr{G} \to \mathrm{GL}(2g)_R$$

is *of abelian type* if

(i) $\rho(\mathscr{G})$ is contained in $\mathrm{Sp}(2g)_R$ and is an algebraic subgroup defined over Q,

(ii) $d\rho(J)$ is conjugate under $\mathrm{Sp}(2g)_{\boldsymbol{R}}$ to

$$\begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix},$$

which is the "complex structure" in $\mathrm{Sp}(2g)_{\boldsymbol{R}}$.

(ii) is equivalent to asserting that

$$(B, -B\, d\rho(J))$$

form a "symplectic pair" in Kuga's sense, where

$$B = \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix};$$

also, (ii) is condition (H_2) of Satake.

(iii) J is not contained in the Lie algebra of any *normal* subgroup $\mathscr{G}_0 \subset \mathscr{G}$ such that $\rho(\mathscr{G}_0)$ is defined over $\boldsymbol{Q}$.

An immediate consequence of this definition is that if we exponentiate J in $\mathscr{G}$ we obtain a homomorphism:

$$\phi\colon T \to \mathscr{G} \qquad \text{where} \qquad \phi(e^{i\theta}) = \exp(\theta J).$$

In fact, $(\rho(\mathscr{G}), \rho \circ \phi)$ is a Hodge type, and every Hodge type arises from an abelian representation of a symmetric pair.

Now suppose $\mathscr{G}, J$ and ρ are given. Let $\phi\colon T \to \mathscr{G}$ denote the above homomorphism. Let K be the compact subgroup of $\mathscr{G}$ which centralizes $\phi(T)$, and let K' be the compact subgroup of $\mathrm{Sp}(2g)_{\boldsymbol{R}}$ which centralizes $\rho(\phi(T))$. Then ρ induces a holomorphic map of symmetric domains

$$\mathscr{G}/K \xrightarrow{\tau} \mathrm{Sp}(2g)_{\boldsymbol{R}}/K'.$$

Via τ, the standard family of abelian varieties on Siegel's upper $\frac{1}{2}$-plane induces a family over $\mathscr{G}/K$: call it

$$\begin{tikzcd} \mathfrak{X}(\mathscr{G}, J, \rho) \arrow[d, "\pi"] \\ \mathscr{G}/K. \end{tikzcd}$$

Since ρ is defined over $\boldsymbol{Q}$, ρ maps all small enough arithmetic subgroups Γ of $\mathscr{G}$ into $\mathrm{Sp}(2g)_{\boldsymbol{Z}}$, and hence the action of such Γ on $\mathscr{G}/K$ lifts to an action on the family $\mathfrak{X}(\mathscr{G}, J, \rho)$.

PROPOSITION 2. *The abelian variety $\pi^{-1}(x)$ in the family $\mathfrak{X}(\mathscr{G}, J, \rho)$ is isogenous to $A = \boldsymbol{R}^{2g}/\boldsymbol{Z}^{2g}$, with complex structure defined by $\rho(g\phi(i)g^{-1})$ where $g \in \mathscr{G}$ represents $x \in \mathscr{G}/K$.*

COROLLARY. *An abelian variety A is isogenous to one in the family $\mathfrak{X}(\mathscr{G}, J, \rho)$ if and only if A has Hodge type equal to or finer than $(\rho(\mathscr{G}), \rho \circ \phi)$.*

Proposition 3. *The families $\mathfrak{X}(\mathcal{G}, J, \rho)$ include all the families associated by Kuga to symplectic representations $\rho: G \to \mathrm{Sp}(2g)$ of semi-simple groups G defined over Q, in the case when $G_{\mathbf{R}}$ has no compact factors.*

4. **The conjecture.** The most intriguing possibility suggested by this theory is is an arithmetic conjecture. Serre [Colloque de Clermont-Ferrand, *Groupes de Lie l-adiques attachés aux courbes elliptiques*] has defined l-adic Lie algebras acting on $H_1(A, Q_l)$, for any abelian variety A, which are essentially the Lie algebras of the Galois group of the extension obtained by adjoining all points of order l^ν to some smallest field of definition of A. Call these $\mathfrak{G}_l$. Let $\mathrm{Lg}(A)$ be the Lie algebra of $\mathrm{Hg}(A)$. It is a sub-Lie-algebra of $\mathrm{Sl}[H_1(A, Q)]$. Then one may ask whether:

$$\mathfrak{G}_l \cap \mathrm{Sl}[H_1(A, Q_l)] = \mathrm{Lg}(A) \otimes_{\mathbf{Q}} Q_l.$$

If $\dim A = 1$, and A is defined over Q, Serre has verified this. For A of CM-type, this result is apparently proven in Shimura-Tamiyama, *Complex multiplication of abelian varieties.*

Symplectic Representations of Algebraic Groups[1]

BY

ICHIRO SATAKE

1. **Kuga's problem.** The purpose of this lecture is to answer the problem posed by Kuga in his lecture (see **[1]**, **[1a]**). This problem may be formulated as follows: Let G be a connected semisimple algebraic group defined over Q of hermitian type. Then the homogeneous space $\mathscr{D} = G_R/\mathscr{K}$ of G_R by a maximal compact subgroup $\mathscr{K}$ of G_R is a symmetric domain. Let V_Q be a finite-dimensional vector space over Q, let $V = V_Q \otimes C$, and let A be a nondegenerate skew-symmetric bilinear form on V whose matrix with respect to any basis of V_Q is rational. Then the group $G' = \mathrm{Sp}(V, A)$ of all linear automorphisms of V which leave A invariant is defined over Q, and we consider (rational) representations ρ of G in G' which are defined over Q. Let $\mathscr{K}'$ be a maximal compact subgroup of G'_R which contains $\rho(\mathscr{K})$. The representation ρ is said to satisfy the condition (H_1) if the induced map of $\mathscr{D}$ into the "Siegel space" $\mathscr{D}' = G'_R/\mathscr{K}'$ is holomorphic.

Let $\mathfrak{g} = \mathfrak{k} + \mathfrak{p}$ be the Cartan decomposition of the Lie algebra $\mathfrak{g}$ of G_R. Since G is of hermitian type, there is an element H_0 in the center of $\mathfrak{k}$ such that the restriction of $\mathrm{ad}H_0$ to $\mathfrak{p}$ is a complex structure on $\mathfrak{p}$. H_0 determines the group $\mathscr{K}$ as well as the invariant complex structure on $\mathscr{D}$. For the group $G' = \mathrm{Sp}(V, A)$ we have similarly $\mathfrak{g}'$, $\mathfrak{k}'$, $\mathfrak{p}'$, H'_0. In this case it is easy to see that $H'_0 = \pm\frac{1}{2}I$ where I is a complex structure on V_R such that bilinear form $A(x, Iy)(x, y \in V_R)$ is symmetric and positive-definite. From now on we shall assume that the complex structure on $\mathscr{D}'$ is that given by $H'_0 = \frac{1}{2}I$. Let $d\rho : \mathfrak{g} \to \mathfrak{g}'$ denote the differential homomorphism of ρ. The condition (H_1) may be formulated as follows:

$$(\mathrm{H}_1) \qquad d\rho([H_0, X]) = [H'_0, d\rho(X)] \text{ for all } X \text{ in } \mathfrak{g}.$$

A slightly stronger condition (H_2), namely $d\rho(H_0) = H'_0$, occurs in our solution. The problem is to *determine all possible* V, A, ρ, *and* $H'_0 = \frac{1}{2}I$ *for given* G, H_0, *subject to the condition* (H_1). To attack this problem it is convenient to generalize the situation.

2. **A more general situation.** Let G be an algebraic group over an arbitrary field k_0 of characteristic zero ($\subset C$), and let $\mathscr{G}$ denote the Galois group of the algebraic closure $\bar{k}_0$ of k_0 over k_0. Let (V, A) be as above except that Q is replaced by k_0, and let ρ be a representation, defined over k_0, of G in $\mathrm{Sp}(V, A)$, which we assume to be completely reducible. This assumption is satisfied in the situation of §1.

[1] This report is a summary of my paper [3].

DEFINITION. The representation ρ is called *k_0-primary* if it is equivalent (over $\bar{k}_0$) to a representation of the form

$$m \sum_{i=1}^{d} \rho_1^{\tau_i} \quad \text{with } \tau_i \in \mathscr{G},$$

where m is a positive integer, ρ_1 is an absolutely irreducible representation of G, defined over $\bar{k}_0$, and $\rho_1^{\tau_i}$ ($i = 1, 2, \cdots, d$) are mutually nonequivalent conjugates of ρ_1.

It may be seen that ρ is k_0-primary if and only if ρ is equivalent (over k_0) to a representation of the form $n'\rho'_1$ where ρ'_1 is k_0-irreducible. Let ρ denote a k_0-primary representation of G, and let ρ_1 denote any absolutely irreducible representation of G which is contained in ρ.

DEFINITION. The k_0-primary representation ρ is said to be *of type* (a), (b), or (c) according to the following conditions on ρ_1:

(a) ${}^t\rho_1^{-1} \sim \rho_1$.

(b) ${}^t\rho_1^{-1} \nsim \rho_1$ but $\sim \rho_1^{\sigma_0}$ for some $\sigma_0 \neq 1$ in $\mathscr{G}$.

(c) otherwise.

It is obvious that the conditions (a), (b), and (c) do not depend on the choice of ρ_1.

THEOREM 1. *Any* (*completely reducible*) *representation ρ, defined over k_0, of G in* Sp(V, A) *is uniquely represented as the direct sum of maximal k_0-primary subrepresentations. Thus,*

$$V = V^{(1)} \oplus V^{(2)} \oplus \cdots,$$

where $V^{(i)}$ is a maximal k_0-primary subrepresentation-space. If $V^{(i)}$ is the space for a k_0-primary representation of type (a) *or* (b), *then the restriction of the alternating form A to $V^{(i)}$ is nondegenerate, and $V^{(i)}$ is an orthogonal summand of V with respect to A. If $V^{(i)}$ is a subspace of type* (c), *then the restriction of A to $V^{(i)}$ is zero, and there is a unique index i' such that the restriction of A to $V^{(i)} \oplus V^{(i')}$ is nondegenerate; moreover, $V^{(i)} \oplus V^{(i')}$ is an orthogonal summand of V.*

We note that in the situation of §1, $\boldsymbol{R}$-primary representations of type (c) do not occur. For simplicity in what follows *we shall only discuss representations of type* (a). The other case, type (b), can be given a similar treatment.

Data for the construction of a k_0-primary representation of type (a) consist of a 9-tuple (K, $\mathfrak{K}$, ι, V_1, V_2, ε, $\boldsymbol{F}_1$, $\boldsymbol{F}_2$, P_1) where:

(i) K is a finite extension field of k_0 of degree d.

(ii) $\mathfrak{K}$ is a central division algebra of rank r^2 over K.

(iii) ι is an involution "of the first kind" on $\mathfrak{K}$, i.e., ι is K-linear.

(iv) V_1 is a right $\mathfrak{K}$-vector space of dimension n.

(v) V_2 is a left $\mathfrak{K}$-vector space of dimension n'.

(vi) $\varepsilon = \pm 1$, $(+1)$-hermitian means hermitian, (-1)-hermitian means skew-hermitian, all relative to ι.

(vii) $\boldsymbol{F}_1$ is an ε-hermitian form on V_1.

(viii) $\boldsymbol{F}_2$ is a $(-\varepsilon)$-hermitian form on V_2.

(ix) P_1 is a representation of G in the subgroup $U(V_1, \boldsymbol{F}_1)$ of GL($V_1/\mathfrak{K}$) which is "absolutely irreducible" in the sense that the representation $\rho_1 = \theta_1 \circ \mathrm{P}_1$ of G is absolutely irreducible, where θ_1 denotes the unique absolutely irreducible representation of the central simple algebra $\mathrm{End}(V_1/\mathfrak{K}) \supset \mathrm{GL}(V_1/\mathfrak{K})$.

One constructs a k_0-primary representation ρ of G as follows: Let V'_K be the K-vector space $V'_K = V_1 \otimes_{\mathfrak{K}} V_2$, and define the k_0-representation-space V_{k_0} by the relation $V_{k_0} = V'_K$, or in the authorized notation, $V = R_{K/k_0}(V')$, $V' = V_K \otimes_K C$. Let $A' = \mathrm{tr}_{\mathfrak{K}}(F_1 \otimes {}^tF_2)$ where $\mathrm{tr}_{\mathfrak{K}}$ is the reduced trace of $\mathfrak{K}$, and define $A = \mathrm{tr}_{K/k_0}(A')$. The representation ρ is then defined by $\rho = R_{K/k_0}(\mathrm{P}_1 \otimes_{\mathfrak{K}} 1)$.

THEOREM 2. *Every k_0-primary representation ρ of G of type* (a) *is equivalent* (*over k_0*) *to a representation given by some 9-tuple* $(K, \mathfrak{K}, \cdots, \mathrm{P}_1)$ *which is uniquely determined by ρ in the obvious sense.*

INDICATION OF PROOF. If ρ is a k_0-primary representation of type (a), then ρ is equivalent to a representation of the form $m \sum_{i=1}^{d} \rho_1^{\tau_i}$. Let $\mathscr{G}_1$ be the subgroup of all σ in $\mathscr{G}$ such that ρ_1^σ is equivalent to ρ_1, and let K be the subfield of $\bar{k}_0$ which corresponds to $\mathscr{G}_1$. The extension degree of K over k_0 is d. For each σ in $\mathscr{G}_1$, we have an isomorphism $\phi_\sigma : V_1 \to V_1^\sigma$ of the representation-spaces of ρ_1 and ρ_1^σ; also, for each τ in $\mathscr{G}_1$, we have the isomorphism $\phi_\sigma^\tau : V_1^\tau \to V_1^{\sigma\tau}$. By Schur's lemma these isomorphisms are uniquely determined up to a scalar factor from $\bar{k}_0$. Hence, the relation $\phi_\sigma^\tau \circ \phi_\tau = \lambda_{\sigma,\tau}\phi_{\sigma\tau}$ holds for some $\lambda_{\sigma,\tau}$ in $\bar{k}_0$, and the $\lambda_{\sigma,\tau}$ form a 2-cocycle of $\mathscr{G}_1$ in $\bar{k}_0^*$. We let $\mathfrak{K}$ be the central division algebra over K associated with the cohomology class of $(\lambda_{\sigma,\tau})$ by means of the isomorphism of $H^2(\mathscr{G}_1, \bar{k}_0^*)$ with the Brauer group of the field K. The dimension of $\mathfrak{K}$ over K is a square, say r^2. The integer r divides the integer m and the dimension of V_1, and the integers n and n' are given by $\dim V_1 = rn$ and $m = rn'$. Then the representation ρ_1 of G in $\mathrm{GL}(V_1)$ can be factored through $\mathrm{GL}(V_1/\mathfrak{K})$ as $\rho_1 = \theta_1 \circ \mathrm{P}_1$. Finally, since ρ is of type (a), ρ_1 has a bilinear invariant which is symmetric or alternating, whence follows that $\mathfrak{K}$ is equipped with an involution ι of the first kind and that P_1 has an ε-hermitian invariant F_1 relative to ι. (When ρ is of type (b), ι is an involution of the second kind.)

3. **The original problem.** G is a connected semisimple algebraic group defined over Q of hermitian type. Without loss of generality we may restrict ourselves to Q-primary representations ρ, and, for simplicity, we assume that ρ is of type (a). We assume also that ρ is nontrivial. Then by Theorem 2 we may assume that ρ comes from some 9-tuple $(K, \mathfrak{K}, \cdots, \mathrm{P}_1)$. In this case P_1 is a representation of G in $\mathrm{SU}(V_1, F_1) = G'_1$, and we put $G'_2 = \mathrm{SU}(V_2, F_2)$.

THEOREM 3. *The notation being as above, ρ satisfies the condition* (H_1) *if and only if*

(i) $R_{K/Q}(G'_i)$ *is of hermitian type for* $i = 1, 2$.

(ii) $R_{K/Q}(\mathrm{P}_1)$ *satisfies the condition* (H_2).

In this case K is a totally real algebraic number field, and $\mathfrak{K}$ (with involution of the first kind) is at most a quaternion algebra over K. One of the groups

$R_{K/Q}(G'_1)$, $R_{K/Q}(G'_2)$ is of type II (or type D) and the other is of type III (or type C); and, for each i ($1 \leqq i \leqq d$), one of $(G_1'^{\tau_i})_R$, $(G_2'^{\tau_i})_R$ is noncompact and the other is compact. One has

$$H'_0 = H'_{01} \otimes 1 + 1 \otimes H'_{02}$$

where $H'_{01} = d(R_{K/Q}\mathrm{P}_1)(H_0)$ and H'_{02} is arbitrary.

REMARK 1. If G_R has no compact factor, then $R_{K/Q}(G'_2)_R$ is compact, and consequently H'_0 is uniquely determined by H_0.

REMARK 2. Under the additional condition stated in §4, it is sufficient that P_1 satisfies the condition (H_2) instead of (ii) above, provided G has no factor of type D_4.

One has similar results when ρ is Q-primary of type (b). In this case, K is a totally imaginary quadratic extension of a totally real field K_0 and $\mathfrak{K}$ is a central division algebra over K with involution of the second kind. Both groups $R_{K/Q}(G'_1)$, $R_{K/Q}(G'_2)$ are of type I (or type A).

One can see that the essential part of our problem is thus reduced to the determination of P_1. This determines $K, \mathfrak{K}, V_1, F_1$ uniquely, and one can then select V_2 arbitrarily and F_2 almost arbitrarily up to a certain condition on the distribution of signs.

4. **List of solutions.** In the first place, by lifting representations to the universal covering group of G if necessary, we may assume that G is decomposed into the direct product $G = G_1 \times G_2 \times \cdots$ where $G_1, G_2, \cdots$ are absolutely simple. Let $\rho = m \sum \rho_1^{\tau_i}$ be a nontrivial Q-primary representation of G satisfying the condition (H_1). Then one has $\rho_1 = (\rho_{11} \circ p_1) \otimes (\rho_{12} \circ p_2) \otimes \cdots$ where p_i is the projection of G on the i-th factor G_i and ρ_{1i} is an absolutely irreducible representation of G_i. We *assume that* $\rho_{12}, \rho_{13}, \cdots$ *are trivial.* This assumption is satisfied when G_R has no compact factor ([2]). Let k be the finite extension of Q whose Galois group consists of those σ in $\mathcal{G}$ for which $G_1^\sigma = G_1$. Then G_1 is defined over k, and ρ is essentially a Q-primary representation of the Q-simple group $R_{k/Q}(G_1)$. So we may assume that $G = R_{k/Q}(G_1)$. Since G_R is of hermitian type, k is a totally real field contained in K. Except for type I, $\mathfrak{K}$, $\mathfrak{k}$ will denote quaternion algebras taken with the canonical involution.

TABLE OF SOLUTIONS

Type of G	G_1	$\rho_{11} = \theta_1 \circ \mathrm{P}_{11}$	G'_1
I.	$\mathrm{SU}(V_1/\mathfrak{K}, F_1), \varepsilon = 1$	$R_{K/K_0}\mathrm{P}_{11} = id$ $(K_0 = k)$	$G'_1 = G_1$
II. ($n \geqq 5$)	$\mathrm{SU}(V_1/\mathfrak{K}, F_1), \varepsilon = -1$	$\mathrm{P}_{11} = id$	$G'_1 = G_1$
III. 1	$\mathrm{Sp}(V_1, A_1), A_1$: alt.	$\mathrm{P}_{11} = id$	$G'_1 = G_1$

Table of Solutions—*continued*[2]

Type of G	G_1	$\rho_{11} = \theta_1 \circ \mathrm{P}_{11}$	G'_1
III. 2	$\mathrm{SU}(V_1/\mathfrak{K}, \boldsymbol{F}_1), \varepsilon = 1$	$\mathrm{P}_{11} = id$	$G'_1 = G_1$
I′	Sign. of $\boldsymbol{F}_1^{\tau_i} = (p_i, q_i)$, p_i or $q_i = 0$ or 1	ρ_{11} = skew-symmetric tensor repn.	
IV. 1	$\mathrm{SO}(W, S)$, S: symmetric p_i or $q_i = 0$ or 2	ρ_{11} = spin repn.	the type depends on dim W (mod 8)
IV. 2	$\mathrm{SU}(W/\mathfrak{k}, \boldsymbol{H})$, $\mathfrak{k}$: totally indefinite, $\boldsymbol{H}$: skew-hermitian, p_i or $q_i = 0$ or 2	ρ_{11} = spin repn.	on dim W (mod 4)
II–IV. 2 (dim $W = 4$)	$\mathrm{SU}(W/\mathfrak{k}, \boldsymbol{H})$, $\boldsymbol{H}$ = skew-hermitian	ρ_{11} = 1 spin repn.	type III

There are no other solutions. By way of illustration, we cite more complete results for the case (IV. 1). Let $l = \dim W$. Then G'_1 is of type I for $l = 2$ or 6 (mod 8), type II for $l \equiv 0, 1$, or 7 (mod 8), and type III for $l \equiv 3, 4$, or 5 (mod 8). If l is odd, then $K = k$, and there is only one spin representation. If l is even, then $K = k(((-1)^{l/2} \det(S))^{\frac{1}{2}})$, and there are two spin representations, which are conjugate when $[K:k] = 2$; the number of solutions is therefore $2/[K:k]$. The group of the "mixed type" (II–IV.2) can have a solution only when $\dim W = 4$.

Remark 1. The families of abelian varieties constructed by Kuga's method in the cases I, II, III. 1, and III. 2 are the same families constructed by Shimura in his lecture ([**4**], [**5**], [**5a**]), provided $G_{\mathbf{R}}$ has no compact factors. There they are called as type IV, III, I, II, respectively.

Remark 2. There can, of course, be many solutions of the problem which do not satisfy the above condition $\rho_1 = \rho_{11} \circ \mathrm{P}_1$. To illustrate the situation, let us give a simplest example of such a solution. Let $G_1 = \mathrm{SU}(V_{11}/\mathfrak{K}, \boldsymbol{F}_{11})$ and $G_2 = \mathrm{SU}(\mathfrak{K} \backslash V_{12}, \boldsymbol{F}_{12})$ be groups of type II and III, respectively, over the same quaternion algebra $\mathfrak{K}$ with center k. Put $G = R_{k/\boldsymbol{Q}}(G_1) \times R_{k/\boldsymbol{Q}}(G_2)$ and let $\rho_1 = (\rho_{11} \circ \mathrm{p}_1) \otimes (\rho_{12} \circ \mathrm{p}_2)$ where $\rho_{1i} = \theta_i \circ \mathrm{P}_{1i}$, $\mathrm{P}_{1i} = id$. Then one has $G'_1 = \mathrm{Sp}(V_1, A_1)$ where $V_1 \; V_{11} \otimes_{\mathfrak{K}} V_{12}$, $A_1 = \mathrm{tr}_{\mathfrak{K}}(\boldsymbol{F}_{11} \otimes {}^t\boldsymbol{F}_{12})$, and one can construct a solution by taking as G'_2 any group of the form $\mathrm{SO}(V_2, S_2)$ where S_2 is a

[2] For more explicit descriptions of the solutions, see [**2**], [**3**].

totally definite symmetric bilinear form on V_2 with a certain distribution of signs. In the most general case, it is proved that any solution can be composed from absolutely irreducible representations of Q-simple factors of G satisfying the condition (H_2) through a definite rule; the determination of each one of such representations (without the above assumption) would, however, become much more complicated. The above example is the one obtained in this manner from the second and the fourth solutions in the above table.

References

1. M. Kuga, *Fibre varieties over a symmetric space whose fibres are abelian varieties.* I; II, Lecture Notes, Univ. of Chicago, 1963–1964.

1a. ———, *Fiber varieties over a symmetric space whose fibers are abelian varieties,* Proc. Sympos. Pure Math., vol. 9, Amer. Math. Soc., Providence, R.I., 1966, pp. 338–346.

2. ———, *Holomorphic imbeddings of symmetric domains into a Siegel space,* Amer. J. Math. **87** (1965), 425–461.

3. ———, *Symplectic representations of algebraic groups satisfying a certain analyticity condition,* (to appear).

4. G. Shimura, *On analytic families of polarized abelian varieties and automorphic functions,* Ann. of Math. (2) **78** (1963), 149–192.

5. ———, *On the field of definition for a field of automorphic functions,* Ann. of Math. (2) **80** (1964), 160–189; II, **81** (1965), 124–165.

5a. ———, *Moduli of abelian varieties and number theory,* Proc. Sympos. Pure Math., vol. 9, Amer. Math. Soc., Providence, R.I., 1966, pp. 312–332.

The Modular Groups of Hilbert and Siegel[1]

BY

WILLIAM F. HAMMOND

1. **Introduction.** In his lecture [5] Kuga has discussed algebraic families of polarized abelian varieties which are fibered over automorphic varieties. Kuga's families correspond, roughly, to certain analytic mappings of automorphic varieties (the base varieties) into the Siegel modular variety. It is our intention here to discuss the case of Hilbert's modular variety. On the one hand, in order to produce results, we shall introduce data which are more restrictive than Kuga's data[2] for the construction of a fiber variety. On the other hand, this is not exactly a special case since Kuga assumes that the base variety is compact and nonsingular. One hopes that the fiber systems constructed from our data will turn out to be algebraic, but I do not know whether this is true. After the discussion of our data, which are called modular imbeddings, the structure of two "quadratic" Hilbert modular varieties is determined as a consequence of the existence of modular imbeddings.

2. **Modular imbeddings.** Let k be a totally real algebraic number field of degree n, and let $\mathfrak{O}$ denote the ring of integers in k. Let X be the n-fold product $(\mathfrak{S}_1)^n$ of the upper half plane $\mathfrak{S}_1$, and let G be the n-fold product group $\mathrm{Sp}(1, \boldsymbol{R})^n$. An imbedding of k in $\boldsymbol{R}^n$ by means of the n distinct isomorphisms (over $\boldsymbol{Q}$) of k in $\boldsymbol{R}$ induces a group isomorphism of $\mathrm{Sp}(1, k)$ with a subgroup Δ of G. Let Γ denote the image in Δ of $\mathrm{Sp}(1, \mathfrak{O})$. Γ is a discrete subgroup of G which is called the Hilbert modular group of the field k. Proofs of the results stated below may be found in [3].

DEFINITION. A *modular imbedding for* k is a pair (ϕ, Φ) consisting of a holomorphic map $\phi: X \to \mathfrak{S}_n$ and a representation $\Phi: G \to \mathrm{Sp}(n, \boldsymbol{R})$ which satisfy:

(a) There is an element N in $\mathrm{Sp}(n, \boldsymbol{R})$ such that $\phi(\tau) = N\phi_0(\tau)$ and

$$\Phi(m) = N\Phi_0(m)N^{-1}$$

for τ in X and m in G, where (ϕ_0, Φ_0) is the pair of "diagonal" imbeddings.

(b) $\Phi(\Gamma) \subseteq \mathrm{Sp}(n, \boldsymbol{Z})$.

(c) If f is a Siegel modular form of weight w, then $f\phi$ is a Hilbert modular form of weight w. (The definition of modular form is recalled in §3.)

[1] The author held an ONR Postdoctoral Research Associateship at Brandeis University during the Summer Institute.

[2] The reader's attention is directed to Satake's work [7], [8] on the classification of symplectic representations occurring in Kuga's data.

DEFINITION. (ϕ, Φ) and (ϕ', Φ') are *equivalent* if there is an element M in $\mathrm{Sp}(n, \boldsymbol{Z})$ such that $\phi' = M\phi$ and $\Phi' = M\Phi M^{-1}$.

One can show that necessarily

$$N = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix},$$

so that ϕ is affine-linear. If (ϕ, Φ) is replaced by an equivalent modular imbedding, one may obtain $\phi(0) = 0$, i.e., it may be assumed that ϕ is homogeneous-linear.

EXAMPLE. Suppose that k is the real quadratic field of discriminant D, and suppose that $D = u^2 + v^2$ for some integers u, v with v even. There is a unique representation ϕ of k by symmetric rational matrices of degree 2 such that

$$\phi(\sqrt{D}) = \begin{pmatrix} u & v \\ v & -u \end{pmatrix}.$$

This ϕ is *normal* in the sense that elements of $\mathfrak{O}$ are represented by integral matrices. Moreover, ϕ has a unique $\boldsymbol{C}$-linear extension to $\boldsymbol{C}^2$ when we imagine k as a subset of $\boldsymbol{R}^2$. Define Φ by

$$\Phi\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} \phi(\alpha) & \phi(\beta) \\ \phi(\gamma) & \phi(\delta) \end{pmatrix}.$$

THEOREM. *Let k be the real quadratic field of discriminant D. Modular imbeddings exist for k if and only if D is the sum of two squares. Every modular imbedding for k is equivalent to the modular imbedding associated above to some representation of D as the sum of two squares.*

COROLLARY. *Suppose that D is the sum of two squares, and let t be the number of primes dividing D. Then the number of classes of modular imbeddings for k is 2^{t-1}.*

In the general case, one has the following results:

THEOREM (IGUSA). *The totally real algebraic number field k admits modular imbeddings if and only if the narrow ideal class of the different of k is a square. The number of classes of modular imbeddings is the product of the number of usual ideal classes whose squares are the narrow class of the different with the index of the subgroup of squares of units in the group of totally positive units.*

REMARK 1. The existence criterion just given is sufficient for the existence of

$$\Phi\colon \mathrm{Sp}(g, \mathfrak{O}) \to \mathrm{Sp}(gn, \boldsymbol{Z}).$$

REMARK 2. If (ϕ, Φ) is a modular imbedding for k, then $\Phi(\Gamma) = \Phi(G) \cap \mathrm{Sp}(n, \boldsymbol{Z})$. Since Φ is faithful, no extension of Γ in G admits modular imbeddings. On the other hand, one knows **[6]** that Γ need not be a maximal discrete subgroup of G.

3. **Modular forms.** One reason for the study of modular imbeddings is that they enable one to construct Hilbert modular forms from Siegel modular forms. These are holomorphic functions in $\mathfrak{S}_n$ (Siegel's case) or $(\mathfrak{S}_1)^n$ (Hilbert's case)

which satisfy a functional equation under the operations of the corresponding modular group as follows:

$$f(M\tau) = \det(c\tau + d)^w f(\tau), \qquad \tau \in \mathfrak{S}_n, \qquad M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Sp}(n, \boldsymbol{Z});$$

$$f(m\tau) = \mathrm{Norm}(\gamma\tau + \delta)^w f(\tau), \qquad \tau \in (\mathfrak{S}_1)^n, \qquad m = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{Sp}(1, \mathfrak{O}).$$

In each case the modular forms constitute a ring graded by the nonnegative integral weight w.

In particular, in the quadratic case ($n = 2$) the structure of the graded ring of Siegel modular forms has been determined by Igusa [4], and one might hope to produce similar results in the case of Hilbert modular forms for a quadratic field by means of modular imbeddings.

In the genus two Siegel case, a crucial role is played by the cusp form θ of weight five inasmuch as it is [cf. 2] the defining equation for the "diagonal surface." The Hilbert modular form $\theta^* = \theta \circ \phi$ (where (ϕ, Φ) is some fixed modular imbedding for a quadratic field) defines a "bunch of curves" on the Hilbert modular variety. This bunch of curves is irreducible if and only if the discriminant D is 5. In the case $D = 8$, θ^* has two irreducible components, and it is possible to factor θ^* in such a way as to separate these components. The following structure theorems are obtained [1], [3]:

THEOREM (GUNDLACH). *The graded ring of symmetric Hilbert modular forms of even weight for the quadratic field of discriminant 5 is a polynomial ring in three variables, generated by two modular forms of weights two and six and by the cusp form of weight ten.*

THEOREM. *The graded ring of symmetric Hilbert modular forms of even weight for the quadratic field of discriminant 8 is a polynomial ring in three variables generated by two modular forms of weights two and six and by the cusp form of weight four.*

REFERENCES

1. K. B. Gundlach, *Die Bestimmung der Funktionen zur Hilbertschen Modulgruppe des Zahlkörpers* $Q(\sqrt{5})$, Math. Ann. **152** (1963), 226–256.

2. W. F. Hammond, *On the graded ring of Siegel modular forms of genus two*, Amer. J. Math. **87** (1965), 502–506.

3. ———, *The modular groups of Hilbert and Siegel*, Amer. J. Math., (to appear).

4. J. Igusa, *On Siegel modular forms of genus two*, Amer. J. Math. **84** (1962), 175–200.

5. M. Kuga, *Fiber varieties over a symmetric space whose fibers are Abelian varieties*, Proc. Sympos. Pure Math., vol. 9, Amer. Math. Soc., Providence, R.I., 1966; pp. 338–346.

6. H. Maass, *Über die Erweiterungsfähigkeit der Hilbertschen Modulgruppe*, Math. Z. **51** (1949), 255–261.

7. I. Satake, *Symplectic representations of algebraic groups*, Proc. Sympos. Pure Math., vol. 9, Amer. Math. Soc., Providence, R.I., 1966; pp. 352–357.

8. ———, *Symplectic representations of algebraic groups satisfying a certain analyticity condition*, Ann. of Math., (to appear).

Quantum Mechanical Commutation Relations and Theta Functions

BY

PIERRE CARTIER

Introduction. A certain nilpotent Lie group plays an important role in the study by H. Weyl [**13**] of the foundations of quantum mechanics. The same group appeared once more in some recent number-theoretic investigations by A. Weil [**12**], whose explicit purpose was to throw the theta-functions away from those parts of analytic number theory where they have played a predominant role in the hands of Hecke and Siegel (among others), or better to replace them by appropriate group-theoretic constructions.

We would like to reverse the whole process and to show how most of the classical properties of theta functions fit into the general group-theoretic framework. The main point is that, whereas the above quoted group has essentially one *equivalence class* of irreducible unitary representations, there are a manifold of concrete realizations of them. More precisely, they can be represented in many different ways as induced representations, and a generalization of Frobenius' reciprocity law, already apparent in some recent work by I. Gelfand and I. Piateskii-Shapiro [**5**], enables us to compare the different representations. One ought to give better foundations to the results of the two last named authors, and we plan to do it at some later occasion.

The first part of the present work is a brief exposition of the Heisenberg commutation relations, and the Schrödinger's and Fock's realizations of them. We describe also H. Weyl's procedure to convene these commutation relations into the realm of group theory. Our second part is devoted to the detailed study of the Weyl's group and its irreducibl. representations and sketch the application to the theory of theta-functions. It ought to be a pleasant task to recast the whole theory of theta-functions in this framework, but what we have done is just a modest beginning.

The author extends his warmest thanks to N. Katz who wrote a preliminary version of these notes during the Boulder Conference, and to D. Mumford whose ideas about theta-functions greatly helped him to frame his own results. His debt towards A. Weil is of a more subtle kind, but nonetheless real.

I. Commutation relations

1. **Schrödinger representation.** According to the general postulates of quantum mechanics, to every physical system S there is associated a certain complex

Hilbert space $\mathscr{H}$. Every vector of norm one in $\mathscr{H}$ defines a possible state of S, and two vectors a and b define the same state if and only if there exists a constant ω of modulus one with $b = \omega \cdot a$. Moreover, every physical quantity whose measurement depends upon the observation of S is represented by a certain self-adjoint operator in $\mathscr{H}$, in most cases unbounded.

For instance consider the case where S is a mechanical system with a finite number n of degrees of freedom. Choose n position coordinates $q_1, \cdots, q_n$ and the corresponding momenta $p_1, \cdots, p_n$. We assume that any combination of values of the q_k corresponds to some physical state. In that case, the elements of $\mathscr{H} = \mathscr{H}_n$ are pairs of functions $f(q_1, \cdots, q_n)$ and $\hat{f}(p_1, \cdots, p_n)$, both assumed to be square-integrable and related to each other by the Fourier transformation formulas

$$(1) \quad f(q_1, \cdots, q_n) = h^{-n/2} \int \cdots \int \hat{f}(p_1, \cdots, p_n) \cdot e\left(\frac{p_1 q_1 + \cdots + p_n q_n}{h}\right) dp_1 \cdots dp_n,$$

$$(1') \quad \hat{f}(p_1, \cdots, p_n) = h^{-n/2} \int \cdots \int f(q_1, \cdots, q_n) \cdot e\left(-\frac{p_1 q_1 + \cdots + p_n q_n}{h}\right) dq_1 \cdots dq_n.$$

Here h is Planck's constant and $e(t)$ is an abbreviation for $e^{2\pi i t}$. Of course, each of the functions $f(q_1, \cdots, q_n)$ and $\hat{f}(p_1, \cdots, p_n)$ determines the other and the relations (1) and (1′) are equivalent, but there is some advantage putting f and $\hat{f}$ on the same footing. The scalar product in $\mathscr{H}$ is computed according to the equivalent formulas

$$(2) \qquad (f|g) = \int \cdots \int \overline{f(q_1, \cdots, q_n)} \cdot g(q_1, \cdots, q_n)\, dq_1 \cdots dq_n,$$

$$(2') \qquad (f|g) = \int \cdots \int \hat{f}(p_1, \cdots, p_n) \cdot \hat{g}(p_1, \cdots, p_n)\, dp_1 \cdots dp_n.$$

The operational meaning is the following. Assume that S is in a state corresponding to the pair $(f, \hat{f})$. In an experiment aimed at the determination of the position of S, the most we can do is to assert the existence of a probability distribution in the space of the variables $q_1, \cdots, q_n$ with probability density $|f(q_1, \cdots, q_n)|^2$. Similarly, we have a probability distribution in the momentum space with density $|\hat{f}(p_1, \cdots, p_n)|^2$. These assumptions are compatible with the convention associating self-adjoint operators $\boldsymbol{q}_k$ to q_k and $\boldsymbol{p}_k$ to p_k in the following way:[1]

$$(3) \qquad (\boldsymbol{q}_k f)(q_1, \cdots, q_n) = q_k \cdot f(q_1, \cdots, q_n),$$

$$(3') \qquad (\widehat{\boldsymbol{p}_k f})(p_1, \cdots, p_n) = p_k \cdot \hat{f}(p_1, \cdots, p_n).$$

[1] The domain of $\boldsymbol{q}_k$ consists of square-integrable functions f for which the integral

$$\int \cdots \int q_k^2 |f(q_1, \cdots, q_n)|^2 \, dq_1 \cdots dq_n$$

is finite. Similarly for $\boldsymbol{p}_k$.

Generally speaking, the commutator of two operators A and B in $\mathscr{H}$ is defined by $[A, B] = A \cdot B - B \cdot A$.[2] With the previous definitions, we have now the famous *Heisenberg commutations relations*:

$$(4) \qquad [q_j, q_k] = [p_j, p_k] \subset 0, \qquad [p_j, q_k] \subset \frac{h}{2\pi i} \cdot \delta_{jk},$$

where δ_{jk} is 0 if $j \neq k$ and the identity operator I in case $j = k$.

2. **Fock representation.** Another example of a physical system is an assembly of so-called bosons each of which is capable of n different states $e_1, \cdots, e_n$. For instance, one can consider the photons present in a beam of monochromatic light travelling in a well-defined direction; here there are two states e_1 and e_2 corresponding to two independent states of polarization. For the purpose of clarity, we shall in the subsequent discussion call $e_1, \cdots, e_n$ the polarization states of the bosons.

In this case, the Hilbert space $\mathscr{H}$ has an orthonormal basis $\{u(c_1, \cdots, c_n)\}$ where $(c_1, \cdots, c_n)$ runs over all possible combinations of positive integers.[3] In a state of the assembly (to be contrasted with the polarization states of the individual bosons) described by a vector

$$(5) \qquad f = \sum_{c_1, \cdots, c_n} f(c_1, \cdots, c_n) \cdot u(c_1, \cdots, c_n),$$

one can ascribe the probability $|f(c_1, \cdots, c_n)|^2$ to any combination of c_1 bosons in polarization state $e_1, \cdots, c_n$ bosons in polarization state e_n. This is a *bona fide* probability distribution because

$$(6) \qquad \sum_{c_1, \cdots, c_n} |f(c_1, \cdots, c_n)|^2 = \|f\|^2 = 1.$$

The meaning of $u(c_1, \cdots, c_n)$ is therefore that of a pure state in which we can observe c_k bosons in polarization state e_k for $k = 1, \cdots, n$, and a general state is a mixing of such pure states.

The occupation operators $N_1, \cdots, N_n$ are defined by[4]

$$(7) \qquad N_k \cdot u(c_1, \cdots, c_n) = c_k \cdot u(c_1, \cdots, c_n)$$

[2] Let A and B be two operators in $\mathscr{H}$ with respective domains $\mathscr{D}_A$ and $\mathscr{D}_B$. The operators $A \pm B$ are defined on the domain $\mathscr{D}_A \cap \mathscr{D}_B$ by $(A \pm B) \cdot a = A \cdot a \pm B \cdot a$ and the operator $A \cdot B$ is defined by $(A \cdot B) \cdot a = A \cdot (B \cdot a)$ on the domain consisting of those a in $\mathscr{D}_B$ for which $B \cdot a$ lies in $\mathscr{D}_A$. We write $A \subset B$ in case $\mathscr{D}_{\,1}\mathscr{D}_B$ and $A \cdot a = B \cdot a$ for every a in $\mathscr{D}_A$.

[3] We consider 0 a positive number!

[4] The domain of N_k consists of the vectors of the form (5) for which $\sum_{c_1 \cdots c_n} c_k^2 |f(c_1, \cdots, c_n)|^2$ is finite. Similarly, the common domain of a_k and a_k^* is defined by the restriction

$$\sum_{c_1 \cdots c_n} c_k |f(c_1, \cdots, c_n)|^2 < +\infty.$$

in accordance with the previous discussion. But an important role is played by the *creation operators* $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_n$ defined by

$$\boldsymbol{a}_k \cdot u(c_1, \cdots, c_n) = (c_k + 1)^{\frac{1}{2}} \cdot u(c_1, \cdots, c_k + 1, \cdots, c_n) \tag{8}$$

and their adjoints, the *annihilation operators* $\boldsymbol{a}_1^*, \cdots, \boldsymbol{a}_n^*$ given by

$$\begin{aligned} \boldsymbol{a}_k^* \cdot u(c_1, \cdots, c_n) &= 0 \qquad \text{if } c_k = 0 \\ &= c_k^{\frac{1}{2}} \cdot u(c_1, \cdots, c_k - 1, \cdots, c_n) \qquad \text{if } c_k \geqq 1. \end{aligned} \tag{9}$$

With these definitions, we have the following commutation relations:

$$[\boldsymbol{a}_j, \boldsymbol{a}_k] = [\boldsymbol{a}_j^*, \boldsymbol{a}_k^*] \subset 0, \qquad [\boldsymbol{a}_j^*, \boldsymbol{a}_k] \subset \delta_{jk}. \tag{10}$$

The role of the creation and annihilation operators is clarified by the following remarks. The vector $\Omega = u(0, \cdots, 0)$ with no bosons present in either polarization state is understandably called the *vacuum*. It is characterized up to a multiplicative constant by the following relations:

$$\boldsymbol{a}_1^* \cdot \Omega = \cdots = \boldsymbol{a}_n^* \cdot \Omega = 0. \tag{11}$$

Moreover we have

$$u(c_1, \cdots, c_n) = \boldsymbol{a}_1^{c_1} \cdots \boldsymbol{a}_n^{c_n} \cdot \Omega / (c_1 ! \cdots c_n !)^{\frac{1}{2}}. \tag{12}$$

The operators $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_n$ form a commuting family and by (12) the vectors $P(\boldsymbol{a}_1, \cdots, \boldsymbol{a}_n) \cdot \Omega$ where P runs over the polynoms in n variables with complex coefficients form a dense subspace in $\mathscr{H}$. Note also the relations

$$N_k = \boldsymbol{a}_k \cdot \boldsymbol{a}_k^*, \tag{13}$$

$$\boldsymbol{a}_k^* \cdot P(\boldsymbol{a}_1, \cdots, \boldsymbol{a}_n) \cdot \Omega = P'_k(\boldsymbol{a}_1, \cdots, \boldsymbol{a}_n) \cdot \Omega, \tag{14}$$

where P'_k is the k-th partial derivative of P.

3. **Harmonic oscillator.** We shall now relate the two previous constructions. For that purpose choose two real numbers λ, μ such that $h\lambda\mu = \pi$, and define in the space $\mathscr{H}_n$ of the Schrödinger representation operators $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_n$ by

$$\boldsymbol{a}_k = \lambda \cdot \boldsymbol{q}_k - i\mu \cdot \boldsymbol{p}_k \tag{15}$$

for $k = 1, \cdots, n$. From (4), one deduces (10) by an easy computation. By reference to (11), one looks now for solutions of the equations

$$\boldsymbol{a}_1^* \cdot f = \cdots = \boldsymbol{a}_n^* \cdot f = 0 \tag{16}$$

which are easily transformed into the differential system

$$(17) \qquad \left(\frac{\partial}{\partial q_k} + 2\lambda^2 q_k\right) \cdot f(q_1, \cdots, q_n) = 0 \qquad (k = 1, \cdots, n).$$

A normalized solution of this system is given by

$$(18) \qquad \Omega(q_1, \cdots, q_n) = (\lambda\pi^{-\frac{1}{2}})^n \exp[-\lambda^2(q_1^2 + \cdots + q_n^2)].$$

If we define the functions $u(c_1, \cdots, c_n)$ by (12), the relation (8) and (9) are satisfied and also (7) if we define N_k to be equal to $\boldsymbol{a}_k \cdot \boldsymbol{a}_k^*$. Moreover, we have

$$(19) \qquad u(c_1, \cdots, c_n)(q_1, \cdots, q_n) = H_{c_1}(q_1) \cdots H_{c_n}(q_n)$$

where the normalized Hermite functions $H_c(q)$ are defined as follows:

$$(20) \qquad H_c(q) = \frac{(-1)^c}{2^c \lambda^{c-1} \pi^{\frac{1}{2}} (c!)^{\frac{1}{2}}} e^{\lambda^2 q^2} \left(\frac{d}{dq}\right)^c (e^{-2\lambda^2 q^2}).$$

From the properties of orthonormal polynomials, one deduces that the functions $u(c_1, \cdots, c_n)$ form an orthonormal basis in the space of square-integrable functions of n real variables $q_1, \cdots, q_n$. Otherwise stated, *the Schrödinger and Fock representations are equivalent.*

The physical meaning of this equivalence is depicted by the theory of the harmonic oscillator. According to Newton's mechanics, a particle of mass m bound to a straight line with coordinate q subjected to a force $-K \cdot q$ oscillates sinusoidally with frequency $v = (1/2\pi)(K/m)^{\frac{1}{2}}$; the momentum p is $m \cdot v$ where v is the speed and the total energy is

$$(21) \qquad E = \frac{p^2}{2m} + \frac{K \cdot q^2}{2}.$$

According to the general quantum-mechanical recipes, we must consider the operator $\boldsymbol{E}$ in $\mathscr{H}_1$ obtained by replacing q by $\boldsymbol{q}$ and p by $\boldsymbol{p}$ in (21). Here the functions $H_0, \cdots, H_c, \cdots$ form an orthonormal basis in $\mathscr{H}_1$ and provided we choose λ according to

$$(22) \qquad \lambda = \left(\frac{\pi}{h}\right)^{\frac{1}{2}} (Km)^{\frac{1}{4}}$$

we have $\boldsymbol{E} = hv(\boldsymbol{a} \cdot \boldsymbol{a}^* + \frac{1}{2})$, that is

$$(23) \qquad \boldsymbol{E} \cdot H_c = (c + \tfrac{1}{2}) \cdot hv \cdot H_c \qquad \text{for } c = 0, 1, 2, \cdots.$$

This justifies Planck's initial assumption and can be expressed by saying that a quantum-mechanical harmonic oscillator is equivalent to an assembly of bosons each having one polarization state and energy hv.[5]

[5] That the vacuum is given the energy $hv/2$ is meaningless in view of the fact that *energy differences* only have a definite physical meaning.

4. **Weyl commutation relations.** We shall now transform the Heisenberg commutation relations in a form given first by H. Weyl [**13**]. Consider for that purpose two self-adjoint operators A and B in some Hilbert space $\mathscr{H}$ and the one parameter groups of unitary operators they generate according to Stone's theorem

$$U(s) = e^{isA}, \qquad V(t) = e^{itB}. \tag{24}$$

Assume now that there exists a real constant c such that[6]

$$[A, B] \subset ic \cdot I. \tag{25}$$

If we allow power series expansion of operator exponentials (which is fully justified if A is bounded but not otherwise) and use a well-known formula by Lie

$$e^X \cdot Y \cdot e^{-X} = \sum_{n=0}^{\infty} \frac{1}{n!}[X, [X, \cdots [X, Y] \cdots]], \ n \text{ factors } X \tag{26}$$

we get at once

$$U(s) \cdot B \cdot U(s)^{-1} = B - sc \cdot I. \tag{27}$$

Going to the exponentials in both sides of (27) and multiplying to the right $U(s)$, we obtain

$$U(s) \cdot V(t) = e^{-icst} V(t) \cdot U(s). \tag{28}$$

The steps going from (25) to (28) are fully reversible and the Heisenberg-like commutation relation (25) is *formally* equivalent to the Weyl-like commutation relation (28).

The previous "proof" is open to some criticism and much pain has been devoted to fulfill the gaps. While the equivalence of (27) and (28) makes no difficulty, it appears hard to justify the use of Lie's formula (26) for unbounded A. Rellich [**10**] and Dixmier [**3**] have proved the equivalence of (25) and (28) under the assumption that there exists a dense subspace V of $\mathscr{H}$ contained in the domains of A and B, stable under both A and B, such that the restriction of $A^2 + B^2$ to V be essentially self-adjoint. A general criterion, due to E. Nelson [**8**] and valid for general Lie groups, fully contains the equivalence of (25) and (28) under Rellich-Dixmier assumptions. Another method, used by the author [**2**] and generalized to the case of unbounded operators in Banach spaces by Kato [**6**], rests on the use of Laplace transform and the resolvant formula

$$\int_0^{\infty} e^{-ps} \cdot U(s)\, ds = (p \cdot I - i \cdot A)^{-1} \qquad (p \text{ real} > 0). \tag{29}$$

[6] According to our conventions, this relation means that $[A, B]$ multiply by ic any vector in its domain.

An easy and rigorous argument shows the equivalence of (27) with the relation

$$(30) \qquad (p\cdot I - i\cdot A)^{-1}\cdot B \subset B\cdot(p\cdot I - i\cdot A)^{-1} - c\cdot(p\cdot I - i\cdot A)^{-2}.$$

Right multiplication by $(p\cdot I - i\cdot A)$ gives the fully equivalent relation

$$(31) \qquad (p\cdot I - i\cdot A)^{-1}\cdot B\cdot(p\cdot I - i\cdot A) \subset B - c\cdot(p\cdot I - i\cdot A)^{-1}$$

from which one gets easily the following criterion: *The relation* (28) *holds if and only if* (25) *holds and the domain of* $B\cdot(p\cdot I - i\cdot A)$ *is contained in the domain of* $A\cdot B$ *for every* $p > 0$. It has been shown by Kato [6] that the last condition needs only to hold for one value of p.

We give now the Weyl form of the Heisenberg commutation relations (4). Using the fact that two self-adjoint operators commute if and only if their associated one-parameter groups commute, and replacing the relations $[p_k, q_k] \subset (h/2\pi i)\cdot I$ by their Weyl analogue, we obtain

$$(32) \qquad W(t, s, u)\cdot W(t', s', u') = W(t + t' + s'\cdot u, s + s', u + u').$$

Here we used the definition

$$W(t, s, u) = e\left(\frac{t}{h}\right)\cdot e\left(\frac{s_1 q_1}{h}\right)\cdots e\left(\frac{s_n q_n}{h}\right)\cdot e\left(\frac{u_1 p_1}{h}\right)\cdots e\left(\frac{u_n p_n}{h}\right)$$

for t real and two real n-vectors $s = (s_1, \cdots, s_n)$ and $u = (u_1, \cdots, u_n)$; moreover $s\cdot u$ is the scalar product $s_1u_1 + \cdots + s_nu_n$.

5. **Uniqueness of the representation of commutation relations.** The problem of uniqueness of the representation for the Heisenberg commutation relations can be formulated as follows:

Let be given in some Hilbert space $\mathscr{H}'$ *a family of self-adjoint operators* $q'_1, \cdots, q'_n, p'_1, \cdots, p'_n$ *such that*

$$(33) \qquad [q'_j, q'_k] = [p'_j, p'_k] \subset 0, \qquad [p'_j, q'_k] \subset \frac{h}{2\pi i}\delta_{jk}.$$

Assume that these operators share with the operators in Schrödinger representation the irreducibility property, viz. no closed subspace of $\mathscr{H}'$ *distinct from* 0 *and* $\mathscr{H}'$ *itself reduces simultaneously the operators* q'_j *and* p'_j. *Does there exist an isometry* U *of* $\mathscr{H}'$ *onto* $\mathscr{H}$ *such that*

$$(34) \qquad U\cdot q'_j\cdot U^{-1} = q_j, \qquad U\cdot p'_j\cdot U^{-1} = p_j \qquad (j = 1, \cdots, n)?$$

As appropriate counter-examples show, the answer may be negative.[7] The known proofs that uniqueness holds indeed under suitable auxiliary assumptions

[7] For instance, let $\mathscr{H}'$be the space of square-integrable functions on the closed interval $[0, 1]$ and let q' be the bounded operator defined by $(q'\cdot f)(x) = x\cdot f(x)$ for $0 \leqq x \leqq 1$. Let ω be a complex number of modulus one and define p'as the differential operator $(h/2\pi i)(d/dx)$ with domain the set of absolutely continuous functions f with square-integrable derivative satisfying the boundary condition $f(1) = \omega\cdot f(0)$.

proceed by reduction to the uniqueness problem for Weyl commutation relations. To formulate this problem, we first remark that in the Schrödinger representation we have

$$(35) \qquad W(t, s, u) \cdot f(q) = e\left(\frac{t + s \cdot q}{h}\right) \cdot f(q + u)$$

with vector notations, and this in turn implies (32). Moreover, the group law

$$(36) \qquad (t, s, u) \cdot (t', s', u') = (t + t' + s' \cdot u, s + s', u + u')$$

makes a real Lie group G out of the real $(2n + 1)$-space.

J. von Neumann [9] and M. Stone [11] have simultaneously proved the following uniqueness theorem:

Any two irreducible unitary representations of the group G, mapping $(t, 0, 0)$ onto the operator $e(t/h) \cdot I$ are unitarily equivalent.

This result solves completely the uniqueness problem for Weyl commutation relations.

II. A certain group and its representations

6. **Description of the group** G. We begin by giving a more invariant description of the Weyl's group. We consider a real finite-dimensional vector space V equipped with a nondegenerate alternating bilinear form B on $V \times V$. The assumptions imply that the dimension of V is an even number $2n$.

The group G is the set of pairs (t, v) where t is a real number and v a vector in V, together with the multiplication law

$$(37) \qquad (t, v) \cdot (t', v') = (t + t' + \tfrac{1}{2}B(v, v'), v + v').$$

The one-parameter subgroups in G are given by[8]

$$(38) \qquad g_{t,v}(\lambda) = (\lambda t, \lambda \cdot v) \qquad (\lambda \text{ in } \boldsymbol{R}).$$

It follows for instance that the unit element in G is $e = (0, 0)$ and the inverse of (t, v) is $(-t, -v)$. The Lie algebra of G shall be denoted by $\mathfrak{g}$; according to (38) the vector space $\mathfrak{g}$ is the direct product $\boldsymbol{R} \times V$. We imbed V in $\mathfrak{g}$ by identifying v with $(0, v)$ for any v in V, and we denote by $\mathfrak{z}$ the one-dimensional subspace of $\mathfrak{g}$ generated by $z = (1, 0)$; therefore $\mathfrak{g}$ is the direct sum of $\mathfrak{z}$ and V. Moreover, according to general recipes, we get the bracket in $\mathfrak{g}$ by antisymmetrizing the bilinear terms in the group law (37), that is $[(t, v), (t', v')] = (B(v, v'), 0)$, or with the previous conventions

$$(39) \qquad [z, v] = 0, \qquad [v, v'] = B(v, v') \cdot z$$

for v, v' in V. Since B is assumed to be nondegenerate, $\mathfrak{z}$ is the center of $\mathfrak{g}$.

[8] We use standard notations: $\boldsymbol{R}$ is the field of real numbers and $\boldsymbol{C}$ that of complex numbers.

According to (38), the exponential mapping from $\mathfrak{g}$ to G is the identity map of the set $\boldsymbol{R} \times V$. For the sake of clarity, we distinguish between a pair (t, v) considered as an element of $\mathfrak{g}$ or as an element of G. The element $(0, v)$ of G is nothing else than e^v and $(t, 0)$ denoted ι_t or $\iota(t)$ is $e^{t \cdot z}$; more generally, the pair (t, v) as element of G is $\iota_t \cdot e^v$. It is immediate that the group Z image of the homomorphism ι of $\boldsymbol{R}$ into G is both the center and the commutator subgroup of G. By definition of the group law, we get

$$e^v \cdot e^{v'} = \iota(\tfrac{1}{2}B(v, v'))e^{v+v'} \tag{40}$$

for v, v' in V. Finally we have an exact sequence

$$0 \rightarrow \boldsymbol{R} \xrightarrow{\iota} G \xrightarrow{\kappa} V \rightarrow 0 \tag{41}$$

where κ is given by $\kappa(t, v) = v$.

The characters[9] of Z are given by the formula

$$\chi_\lambda(\iota_t) = e(\lambda t) \tag{42}$$

where λ runs over $\boldsymbol{R}$. The infinitesimal character[9] associated to χ_λ is the linear form on the Lie algebra $\mathfrak{z}$ of Z given by

$$\chi'_\lambda(z) = 2\pi i \lambda. \tag{43}$$

For the purpose of explicit computations, we may introduce a symplectic basis for V with respect to B, let say $\{P_1, \cdots, P_n, Q_1, \cdots, Q_n\}$. We then get a basis $\{z, P_1, \cdots, P_n, Q_1, \cdots, Q_n\}$ of $\mathfrak{g}$ with the property that the only nonzero brackets among basic elements are

$$[P_j, Q_j] = z \qquad (j = 1, \cdots, n). \tag{44}$$

Such a basis of $\mathfrak{g}$ shall be called a *normal basis*.

7. **Infinitesimal representations.** We consider any (unitary) representation $(\pi, \mathscr{H})$ of G. That is, $\mathscr{H}$ is a Hilbert space with scalar product $(a|b)$ linear with respect to b and norm $\|a\| = (a|a)^{\frac{1}{2}}$, and π is a homomorphism of G into the group of unitary operators in $\mathscr{H}$ satisfying the following continuity condition:

(R) *For any pair a, b in $\mathscr{H}$, the function $\phi_{a,b}$ defined on G by $\phi_{a,b}(g) = (a|\pi(g) \cdot b)$ is continuous.*

We let $\mathscr{H}_\infty$ denote the vector subspace in $\mathscr{H}$ consisting of those a's for which $\phi_{a,b}$ is a function of class C^∞ whatever be b in $\mathscr{H}$; the elements in $\mathscr{H}_\infty$ are called *C^∞-vectors*. Among the C^∞-vectors are the vectors

$$\int_G \phi(g)[\pi(g) \cdot a]\, dg \tag{45}$$

[9] A character of a Lie group G is a continuous complex-valued function χ on G such that $|\chi(g)| = 1$ and $\chi(gg') = \chi(g) \cdot \chi(g')$ for g, g' in G. The associated infinitesimal character is the linear form χ' on the Lie algebra $\mathfrak{g}$ of G characterized by $\chi(\exp X) = \exp \chi'(X)$.

where a is any vector in $\mathscr{H}$ and ϕ is a C^∞-function on G with compact support, and the integral is with respect to some Haar measure on G. It has been shown by Gårding [4] that such vectors form a dense set in $\mathscr{H}$, and therefore $\mathscr{H}_\infty$ is dense in $\mathscr{H}$.

For any X in $\mathfrak{g}$, there is a (generally unbounded) operator $\tilde{\pi}(X)$ on $\mathscr{H}$ defined by

$$\tilde{\pi}(X)\cdot a = \lim_{t\to 0}\frac{1}{t}\cdot[\pi(e^{tX})\cdot a - a] \tag{46}$$

with domain the set of all a's for which the limit exists (strong or weak, it is the same). It can be shown that $\mathscr{H}_\infty$ is the intersection of the domains of all finite products $\tilde{\pi}(X_1)\cdots\tilde{\pi}(X_m)$ where $m > 0$ and $X_1,\cdots,X_m$ run independently over $\mathfrak{g}$.

Let us choose for the moment any basis $\{X_1,\cdots,X_p\}$ of $\mathfrak{g}$ (where $p = 2n + 1$). We define on $\mathscr{H}_\infty$ an increasing sequence of Hilbert norms N_m by

$$N_m(a)^2 = \sum_{|\alpha|\leq m} \|\tilde{\pi}(X_1)^{\alpha_1}\cdots\tilde{\pi}(X_p)^{\alpha_p}\cdot a\|^2 \tag{47}$$

with the standard abbreviations $\alpha = (\alpha_1,\cdots,\alpha_p)$ and $|\alpha| = \alpha_1 + \cdots + \alpha_p$. The norms depend obviously on the chosen basis of $\mathfrak{g}$, but the topology they define on $\mathscr{H}_\infty$ does not; that makes $\mathscr{H}_\infty$ a complete metrizable vector space (an (F)-space). We define $\mathscr{H}_{-\infty}$ as the set of all continuous antilinear[10] forms on $\mathscr{H}_\infty$ and we identify $\mathscr{H}$ with a subspace of $\mathscr{H}_{-\infty}$ by associating to a vector a the antilinear form $b \mapsto (b|a)$ on $\mathscr{H}_\infty$ (note that $\mathscr{H}_\infty$ is dense in $\mathscr{H}$).

It can be shown that the representation of G in $\mathscr{H}$ extends in a natural way to a representation π of G in the (nontopological) vector space $\mathscr{H}_{-\infty}$. Moreover there is a linear representation π' of the Lie algebra $\mathfrak{g}$ in the vector space $\mathscr{H}_{-\infty}$ with the following property: for any X in $\mathfrak{g}$, the domain of $\tilde{\pi}(X)$ is the set of vectors a in $\mathscr{H} \subset \mathscr{H}_{-\infty}$ for which $\pi'(X)\cdot a$ is in $\mathscr{H}$, and we have $\pi'(X)\cdot a = \tilde{\pi}(X)\cdot a$ for such an a. The following relations hold:

$$\pi'((\mathrm{Ad}\, g)\cdot X) = \pi(g)\cdot\pi'(X)\cdot\pi(g)^{-1}, \tag{48}$$

$$(a|\pi'(X)\cdot b) = -(\pi'(X)\cdot a|b) \tag{49}$$

for a, b in $\mathscr{H}_\infty$, for X in $\mathfrak{g}$ and g in G; we denoted by $\mathrm{Ad}\, g$ the automorphism of $\mathfrak{g}$ associated to the inner automorphism $g' \mapsto gg'g^{-1}$ of G. It can be shown that $\mathscr{H}_\infty$ is stable under the operators $\pi(g)$ and $\pi'(X)$.

The previous properties are valid for any representation of any Lie group. They will be considered in detail in the forthcoming paper alluded to in the introduction.[10 bis]

8. **Induced representations.** We recall the classical definition of such representations as given for instance in [1] and [7] under more general circumstances.

[10] A complex valued function F on a complex vector space is called an antilinear form in case the following relations hold $F(v + v') = F(v) + F(v')$ and $F(c\cdot v) = \bar{c}\cdot F(v)$ where $\bar{c}$ is the complex number conjugate to c.

[10 bis] *Added in proof.* L. Schwartz informs me that he defined the spaces $\mathscr{H}_\infty$ and $\mathscr{H}_{-\infty}$ and stated their main properties in his report at the "Second Colloquium on Functional Analysis" held at Liège (Belgium) in May 1966 (see Proceedings, pp. 153–163).

Let χ be a character of some closed subgroup H of G. We let $\mathscr{H}_\chi$ denote the Hilbert space consisting of all functions f on G satisfying the following conditions:

(a) *f is Borel-measurable on G;*

(b) *$f(hg) = \chi(h) \cdot f(g)$ for g in G and h in H;*

(c) *the integral $\int_M |f(g)|^2\, dg$ is finite.*

The norm on $\mathscr{H}_\chi$ is given by

$$\|f\|^2 = \int_M |f(g)|^2\, dg. \tag{50}$$

A few words of explanation are in order. First of all $M = H\backslash G$ is the space of cosets Hg in G. Since G is nilpotent, there exist biinvariant Haar measures dg on G and dh on H, and a measure m on M invariant under the right translations by the elements of G. We abuse the notations by denoting the integral $\int_M \hat{\phi}\, dm$ as $\int_M \phi(g)\, dg$ in case ϕ and $\hat{\phi}$ are related by $\phi(g) = \hat{\phi}(Hg)$. The integral in (50) makes sense because $|\chi(h)| = 1$ implies that $|f|^2$ is constant on every coset Hg by virtue of (b).

To every g in G, there is associated a unitary operator $\pi_\chi(g)$ on $\mathscr{H}_\chi$ by

$$(\pi_\chi(g) \cdot f)(g') = f(g'g) \tag{51}$$

(right translation). The pair $(\pi_\chi, \mathscr{H}_\chi)$ is a representation of G, called the *representation induced by the character χ of H.*[11]

It can be shown that $(\mathscr{H}_\chi)_\infty$ is the set of all C^∞-functions f on G satisfying condition (b) above such that $L \cdot f$ be square-integrable modulo H for every left-invariant differential operator L on G. Accordingly, $(\mathscr{H}_\chi)_{-\infty}$ can be identified with the set of distributions which can be represented as finite sums $\sum_\alpha L_\alpha \cdot f_\alpha$ where the f_α's are in $\mathscr{H}_\chi$ and L_α is a left-invariant differential operator for every α. The representation π' of $\mathfrak{g}$ in $(\mathscr{H}_\chi)_{-\infty}$ is given via the action of the left-invariant vector fields on G. The evaluation map

$$\phi \mapsto \overline{\phi(e)}$$

considered as a functional on $(\mathscr{H}_\chi)_\infty$ is an element u_χ of $(\mathscr{H}_\chi)_{-\infty}$ called the *canonical* one. It can be identified with the distribution on G given by $u_\chi(\phi) = \int_H \phi(h)\chi(h)\, dh$ for every test-function ϕ on G. It satisfies the following equation

$$\pi(h) \cdot u = \chi(h) \cdot u \qquad (h \text{ in } H) \tag{52}$$

which amounts for connected H to be equivalent to the equation

$$\pi'(Y) \cdot u = \chi'(Y) \cdot u \tag{53}$$

for every Y in the Lie algebra of H.

[11] This construction can be expressed in the framework of fibre bundles as follows. On the trivial bundle $G \times C$ over G with fiber C, the group H operates to the left by $h(g, c) = (hg, \chi(h) \cdot c)$ and G operates to the right by $(g, c) \cdot g' = (gg', c)$. The space E of the H-orbits in $G \times C$ is therefore a line bundle over $M = H\backslash G$, on which G operates to the right. Moreover, there is a function q on E taking the value $|c|^2$ on the H-orbit of any point (g, c). The space $\mathscr{H}_\chi$ can therefore be identified with the space of square-integrable sections s of E over M (square-integrable means s is measurable and $\int_M q(s) \cdot dm < \infty$). The action of G on the sections is given via the actions of G on M *and* E.

A weak form of Frobenius' reciprocity law reads as follows:

The induced representation $(\pi_\chi, \mathscr{H}_\chi)$ is irreducible[12] *in case the only solutions of the equation* (52) *are the constant multiples of the canonical element u_χ.*

9. **Classification of the representations of G.** Let $(\pi, \mathscr{H})$ be any irreducible representation of G. For any element ζ in the center Z of G, the operator $\pi(\zeta)$ on $\mathscr{H}$ commutes with every operator $\pi(g)$ and is therefore by the irreducibility assumption a scalar multiple of the identity. We know the characters of Z (cf. formula (42), page 369) and may conclude that there exists a unique real number λ with

$$\pi(\zeta) = \chi_\lambda(\zeta) \cdot I \qquad (\zeta \text{ in } Z). \tag{54}$$

According to von Neumann [9] and Stone [11] we have the following classification:

(a) For every $\lambda \neq 0$, there exists, up to unitary equivalence, exactly one irreducible representation $(\pi, \mathscr{H})$ satisfying (54).

(b) The case $\lambda = 0$ corresponds to the representations which are trivial on the center Z of G. They are the one-dimensional representations given by the characters ϖ_u of G:

$$\varpi_u(t, v) = e(B(v, u)) \tag{55}$$

(u is a fixed element of V).

Let us choose a normal basis $\{z, P_1, \cdots, P_n, Q_1, \cdots, Q_n\}$ of $\mathfrak{g}$. The relation (54) is equivalent to the following infinitesimal one:

$$\pi'(z) = 2\pi i\lambda \cdot I \qquad (\pi = 3.1415 \cdots \text{on the right-hand side!}) \tag{56}$$

(on $\mathscr{H}_\infty$ or $\mathscr{H}_{-\infty}$ at will). The operators $\mathbf{p}_j = \pi'(P_j)$ and $\mathbf{q}_j = \pi'(Q_j)$ satisfy on $\mathscr{H}_{-\infty}$ the Heisenberg commutation relations

$$[\mathbf{p}_j, \mathbf{p}_k] = [\mathbf{q}_j, \mathbf{q}_k] = 0, \qquad [\mathbf{p}_j, \mathbf{q}_k] = 2\pi i\lambda\delta_{jk}. \tag{57}$$

10. **The Schrödinger representation of G.** Let E be any n-dimensional subspace of V with the property that B is identically zero on $E \times E$. From (40) it follows that the image $\bar{E}$ of E into G under the exponential mapping from $\mathfrak{g}$ to G is a commutative subgroup of G. The invariant subgroup $H_E = Z \cdot \bar{E}$ of G is the direct product of Z and $\bar{E}$ and there exists therefore a unique character ϖ_λ of H_E inducing χ_λ on Z and the identity on $\bar{E}$. Explicitly, one has

$$\varpi_\lambda(\iota_t \cdot e^w) = e(\lambda t) \qquad (t \in \mathbf{R}, w \in E). \tag{58}$$

[12] The representation $(\pi, \mathscr{H})$ is called irreducible in case there exists no closed vector subspace of $\mathscr{H}$, except 0 and $\mathscr{H}$ itself, invariant under every operator $\pi(g)$. A useful criterion asserts that this is the case if and only if any bounded operator in $\mathscr{H}$ commuting with every $\pi(g)$ is a scalar multiple of the identity operator.

For any $\lambda \neq 0$, we denote by $\mathscr{D}_\lambda = (\sigma_\lambda, \mathscr{H}_{\lambda, E})$ the representation of G induced by the character ϖ_λ of H_E.

To further analyse this representation, let us introduce some n-dimensional subspace E' of V, such that B induces 0 on $E' \times E'$ and that V be the direct sum of E' and E. Such a subspace E' is known to exist and to be nonunique in case $n \geqq 1$. The restriction of B to $E' \times E$ put these two vector spaces into duality. Moreover, any element of G can be uniquely written in the following form

$$g = \iota_t \cdot e^w \cdot e^{w'} \qquad (t \in \boldsymbol{R}, w \in E, w' \in E'). \tag{59}$$

By definition, $\mathscr{H}_{\lambda,E}$ consists of the functions f on G which are square-integrable modulo H_E and satisfy the relation

$$f(\iota_s \cdot e^v \cdot g) = e(\lambda s) \cdot f(g) \qquad (s \in \boldsymbol{R}, v \in E, g \in G). \tag{60}$$

It is immediate to define a Hilbert space isomorphism $f \rightleftarrows \phi$ from $\mathscr{H}_{\lambda,E}$ to $L^2(E')$ by means of the equivalent formulas[13]

$$f(g) = e(\lambda t) \cdot \phi(w'), \qquad \phi(w') = f(e^{w'}) \tag{61}$$

where g is given by (59). By means of this isomorphism, the action of G is shifted to $L^2(E')$ and is given by the following relation:

$$(\sigma_\lambda(g) \cdot \phi)(v') = e(\lambda t) \cdot e(\lambda B(v', w)) \cdot \phi(v' + w'). \tag{62}$$

Now let $\{Q_1, \cdots, Q_n\}$ be any basis of E. Since B puts E' and E into duality we can define a basis $\{P_1, \cdots, P_n\}$ and a coordinate system $\{x_1, \cdots, x_n\}$ for E' by means of the formulas

$$B(P_j, Q_k) = \delta_{jk}, \tag{63}$$

$$x_k(v') = B(v', Q_k). \tag{64}$$

According to (59), any element of G is of the form

$$\omega(t, s, u) = \iota_t \cdot e^{s_1 Q_1} \cdots e^{s_n Q_n} e^{u_1 P_1} \cdots e^{u_n P_n}$$

where t is real and $s = (s_1, \cdots, s_n)$, $u = (u_1, \cdots, u_n)$ are real n-vectors. The group law is given by

$$\omega(t, s, u) \cdot \omega(t', s', u') = \omega(t + t' + s' \cdot u, s + s', u + u') \tag{65}$$

and the operator $W(t, s, u) = \sigma_\lambda(\omega(t, s, u))$ on $L^2(E')$ is given by

$$W(t, s, u) \cdot \phi(x) = e(\lambda t) \cdot e(\lambda s \cdot x) \cdot \phi(x + u). \tag{66}$$

We are back to the Schrödinger representation with parameter $\lambda = 1/h$ (see (35) and (36)).

[13] The notation $L^2(E')$ means the space of square-integrable functions on E'.

The infinitesimal operators p_k and q_k acting on $L^2(E')$ are the differential operators

$$(67) \qquad p_k \cdot \phi = \partial\phi/\partial x_k, \qquad q_k \cdot \phi = 2\pi i\lambda x_k \cdot \phi.$$

More precisely, the general theory of induced representations (see page 371) shows that the C^∞-vectors in the representation $\mathscr{D}_\lambda$ are the C^∞-functions on E' which are mapped into square-integrable functions by any finite product of the operators (67). These functions form the Schwartz' space $\mathscr{S}(E')$ whose dual is the space $\mathscr{S}'(E')$ of "tempered distributions" on E'. The action of $\mathfrak{g}$ on the space $\mathscr{S}'(E') = (\mathscr{H}_{\lambda,E'})_{-\infty}$ is still given by (67).

The irreducibility of Schrödinger representation is a familiar result, but it is instructive to derive it from our general irreducibility criterion (see page 372) and the following elementary lemma in distribution theory.

LEMMA 1. *Any distribution T on the real n-space E' satisfying the conditions*

$$(68) \qquad x_k \cdot T = 0 \qquad (k = 1, \cdots, n)$$

is a constant multiple of the Dirac distribution δ defined by $\delta(\phi) = \phi(0)$ for any test-function ϕ.

Using the classification of the irreducible representations of G given on page 372 and using the preceding result, we obtain easily the following result.

THEOREM 1. *Let $\{\varpi, \mathscr{H}\}$ be any irreducible representation of G, nontrivial on the center Z of G, and let E be any n-dimensional subspace of V on which B induces the zero form. The set of solutions of the equation*

$$(69) \qquad \varpi'(X) \cdot v = 0 \qquad \textit{for every } X \textit{ in } E$$

is a one-dimensional subspace of $\mathscr{H}_{-\infty}$.

11. **Some discrete subgroups.** Let L be a lattice[14] in V such that B take integral values on $L \times L$; the complementary lattice L' is the set of all vectors v in V such that $B(v, \lambda)$ be an integer for every λ in L; it obviously contains L. The set of elements of the form $\iota_t \cdot e^\lambda$ with t real and λ in L is an invariant subgroup Γ_L of G; the subgroup $\Gamma_{L'}$ is defined in a similar way. Let us consider also the discrete subgroup Δ of the center Z of G consisting of the elements ι_m with m an integer. The group $\Gamma_{L'}$ is nothing else than the set of all g's for which the commutator $g\gamma g^{-1}\gamma^{-1}$ lies in Δ for every γ in Γ_L.

We denote by Ξ the group of all characters of Γ_L taking the value 1 on all of Δ; we have $\Xi = \bigcup_m \Xi_m$ (disjoint union) where Ξ_m is the set of characters of Γ_L extending the character χ_m of Z (m runs over the set of integers). The general form of the elements in Ξ_m is given as follows

$$(70) \qquad \Psi_{m,F}(\iota_t \cdot e^\lambda) = e(mt) \cdot e(\tfrac{1}{2}F(\lambda)),$$

[14] That is, a discrete subgroup of V generating it as a vector space, or equivalently, the set of vectors with integral coordinates in a suitable basis of V.

where F is any real-valued function on L, defined modulo 2, satisfying the congruence:

$$F(\lambda + \mu) \equiv F(\lambda) + F(\mu) + m \cdot B(\lambda, \mu) \qquad (\text{mod } 2). \tag{71}$$

More simply, the characters in Ξ_0 are given by

$$\Psi(\iota_t \cdot e^{\lambda}) = e(B(v_0, \lambda)) \tag{72}$$

where v_0 is a fixed element of V, defined modulo L' by this relation.

Let m be nonzero and let $\Psi_{m,F}$ and $\Psi_{m,F'}$ be two elements of Ξ_m. We can write $\Psi_{m,F'} = \Psi \cdot \Psi_{m,F}$ with some Ψ in Ξ_0. Using formula (72), we get after easy manipulations

$$\Psi_{m,F'}(\gamma) = \Psi_{m,F}(g \cdot \gamma \cdot g^{-1}) \qquad (\gamma \text{ in } \Gamma_L) \tag{73}$$

where we can take for g the element $g_0 = \exp(m^{-1} \cdot v_0)$ of G; the elements g qualifying for (73) form the whole coset $g_0 \cdot \Gamma_{m^{-1}L'}$.

A more explicit description of the situation can be given as follows. According to elementary divisor theory, there exists a normal basis $\{z, P_1, \cdots, P_n, Q_1, \cdots, Q_n\}$ of $\mathfrak{g}$ and integers $e_1, \cdots, e_n$ such that the elements of L (resp. L') are the vectors

$$\lambda = t_1 \cdot P_1 + \cdots + t_n \cdot P_n + s_1 \cdot Q_1 + \cdots + s_n \cdot Q_n \tag{74}$$

whose coordinates are solutions of the congruences

$$s_j \equiv 0, \qquad e_j^{-1} \cdot t_j \equiv 0 \ (\text{mod } 1) \qquad \text{for } j = 1, \cdots, n, \tag{75}$$

(resp.

$$e_j \cdot s_j \equiv 0, \qquad t_j \equiv 0 \ (\text{mod } 1) \qquad \text{for } j = 1, \cdots, n). \tag{75'}$$

As a corollary, we get that the index $[L' : L]$ is the square of the integer $e = e_1 \cdots e_n$.

A special instance of a solution of the functional Equation (71) is given as follows

$$F_0(\lambda) = m \cdot (t_1 s_1 + \cdots + t_n s_n). \tag{76}$$

The general solution is given by

$$F(\lambda) \equiv F_0(\lambda) + a_1 s_1 + \cdots + a_n s_n + e_1^{-1} b_1 t_1 + \cdots + e_n^{-1} b_n t_n \qquad (\text{mod } 2) \tag{77}$$

where $a_1, \cdots, a_n, b_1, \cdots, b_n$ are real numbers defined modulo 1. Let us remark that for m even, we might as well take $F_0 = 0$ as a particular solution of the congruence (71).

A particularly important special case is provided by the so-called "principal lattices," that is the lattices L equal to their complementary L'. For such an L, the commutator group of Γ_L is equal to Δ, and Ξ is therefore the set of all characters of Γ_L; moreover any two characters belonging to the same Ξ_m (with $m \neq 0$) are conjugate to each other by some element of G well-defined modulo $\Gamma_{m^{-1}L}$. Finally in case of a principal lattice, the "elementary divisors" $e_1, \cdots, e_n$ are all equal to 1.

Assume L to be principal. The Equation (71) is then satisfied for at least one integral-valued F; in case m is even, it suffices to take $F = 0$. Assuming therefore m to be odd, denote by $\bar{L}$the vector space $L/2L$ over the field with two elements By reduction modulo 2, the form B defines a symmetric bilinear form $\bar{B}$ on $\bar{L} \times \bar{L}$ and the integral-valued solutions of (71) correspond via reduction modulo 2 to the quadratic forms F on $\bar{L}$ whose associated bilinear form is $\bar{B}$. These quadratic forms fall into two equivalence classes according to the value of their "Arf invariant." Using again a normal basis $\{z, P_1, \cdots, P_n, Q_1, \cdots, Q_n\}$ for which L is the set of vectors with integral coordinates in V, we get the following reduced forms for the F falling in either one of the two classes:

$$F'(\lambda) = t_1 s_1 + \cdots + t_n s_n, \tag{78}$$

$$F''(\lambda) = t_1 s_1 + \cdots + t_n s_n + s_1^2 + t_1^2. \tag{79}$$

12. **The lattice representations.** We proceed now to describe a class of representations of G which have so far played no role in quantum mechanics.

We fix a lattice L such that B takes integral values on $L \times L$, an integer $m \neq 0$ and a function F solution of (71). The representation of G induced by the character $\Psi_{m,F}$ of Γ_L shall be denoted $\mathscr{D}_{L,m,F}$. Using the correspondence $f \rightleftarrows \phi$ expressed by the equivalent relations

$$\phi(v) = f(e^v), \qquad f(\iota_t \cdot e^v) = e(mt) \cdot \phi(v), \tag{80}$$

we shift the action of G to the space $\mathscr{H}_{L,m,F}$ of functions ϕ on V subjected to the following restrictions:

(a) The function ϕ is Borel-measurable on V.

(b) The integral $\int_P |\phi(v)|^2 \, dv$ is finite for every fundamental domain P of L acting by translation on V (for instance a suitable parallelotope).

(c) Functional equation:

$$\phi(v + \lambda) = e\left(\frac{1}{2}F(\lambda) + \frac{m}{2}B(v, \lambda)\right) \cdot \phi(v) \tag{81}$$

for v in V and λ in L.

The action of G in $\mathscr{H}_{L,m,F}$ is given as follows

$$(U_{v'}\phi)(v) = \phi(v + v') \cdot e\left(\frac{m}{2}B(v, v')\right) \tag{82}$$

where $U_{v'} = \pi_m(e^{v'})$ is the operator corresponding to the element $e^{v'}$ of G. In what follows, we consider only the case where $m = 1$, the general case going easily over to that case by replacing B by $m \cdot B$ throughout. We shall omit the index 1 in the notations $\Psi_{1,F}$, $\mathscr{H}_{L,1,F}$, $\mathscr{D}_{L,1,F}$ and π_1.

We give now an analysis of irreducibility for the representation $\mathscr{D}_{L,F}$; we shall eventually prove that *the irreducibility is at hand if and only if L is a principal lattice.* To every λ' in L', we can associate an operator $A_{\lambda'}$ commuting to $\pi(G)$

and given via left translation

$$(83)\qquad (A_{\lambda'}f)(g) = f(e^{\lambda'}\cdot g)$$

or equivalently (see formula (80)) by

$$(84)\qquad (A_{\lambda'}\phi)(v) = e(\tfrac{1}{2}B(\lambda', v))\phi(v + \lambda')$$

for any function ϕ in $\mathscr{H}_{L,F}$. Using (40), we get

$$(85)\qquad A_{\lambda'}\cdot A_{\mu'} = e(\tfrac{1}{2}B(\lambda', \mu'))\cdot A_{\lambda'+\mu'}$$

while (81) takes the form

$$(86)\qquad A_{\lambda} = e(\tfrac{1}{2}F(\lambda))\cdot I \qquad (\lambda \text{ in } L).$$

LEMMA 2. *Let S be any set of representatives for the cosets of L' modulo L. The operators A_s for s in S form a basis of the algebra of all operators in $\mathscr{H}_{L,F}$ commuting to $\pi(G)$.*

The proof runs as follows. First of all, the infinitesimal representation is given by

$$(87)\qquad (\pi'(X)\cdot\phi)(v) = \theta_X\phi(v) + \pi i\cdot B(v, X)\cdot\phi(v) \qquad (X \text{ in } V)$$

where θ_X is the Lie derivative[15] associated to the constant vector field on V with value X. More precisely, $(\mathscr{H}_{L,F})_\infty$ is the set of C^∞-solutions of the functional Equations (81) such that $\pi'(X_1)\cdots\pi'(X_p)\cdot\phi$ be square integrable modulo L for every sequence of elements $X_1,\cdots,X_p$ in V, and $(\mathscr{H}_{L,F})_{-\infty}$ is the set of distributions on V which can be expressed as finite sums of derivatives $\pi'(X_1)\cdots\pi'(X_p)\cdot\phi$ of functions ϕ belonging to $\mathscr{H}_{L,F}$. These distributions satisfy the functional Equation (81) in a symbolic sense. The canonical element (see page 371) expresses the distribution u given on any test function ϕ by[16]

$$(88)\qquad u(\phi) = \sum_{\lambda\in L} e(\tfrac{1}{2}F(\lambda))\cdot\phi(\lambda).$$

The action of $A_{\lambda'}$ on the distributions belonging to $(\mathscr{H}_{L,F})_{-\infty}$ be expressed by the same formula which works foı functions, at least when suitably interpreted in a symbolic way. This entails the following formula

$$(89)\qquad (A_{\lambda'}u)(\phi) = \sum_{\lambda\in L} e(\tfrac{1}{2}F(\lambda))\cdot e(\tfrac{1}{2}B(\lambda', \lambda))\cdot\phi(\lambda - \lambda')$$

for $A_{\lambda'}u$.

[15] Defined by

$$0_X f(v) = \lim_{t\to 0}\frac{1}{t}[f(v + tX) - f(v)].$$

[16] In this case $F = 0$, this distribution deserves to be called *Poisson distribution* because of its significance for the Poisson summation formula.

According to the general theory of representations, any operator A in $\mathscr{H}_{L,F}$ commuting to $\pi(G)$ has a natural extension to $(\mathscr{H}_{L,F})_{-\infty}$ which commutes with the action of G on $(\mathscr{H}_{L,F})_{-\infty}$. If $t = A \cdot u$, we have therefore

$$\pi(e^{\lambda}) \cdot t = e(\tfrac{1}{2}F(\lambda)) \cdot t \tag{90}$$

for every λ in L. Moreover, $A \cdot u$ is 0 if and only if A is 0. It remains therefore to prove that any distribution in $(\mathscr{H}_{L,F})_{-\infty}$ solution of (90) is a linear combination of the distributions $A_s \cdot u$, which is tantamount proving the following lemma.

LEMMA 3. *Any distribution t on V satisfying the symbolic equations*

$$t(v + \lambda) = e(\tfrac{1}{2}F(\lambda)) \cdot e(\tfrac{1}{2}B(v, \lambda)) \cdot t(v), \tag{91}$$

$$e(\tfrac{1}{2}B(v, \lambda)) \cdot t(v + \lambda) = e(\tfrac{1}{2}F(\lambda)) \cdot t(v) \tag{92}$$

for every λ in L, is of the form $t = \sum_{s \in S} T(-s) \cdot A_s u$ with suitable constants $T(-s)$.

We can replace the system of equations (91) and (92) by the equivalent system consisting of (91) and

$$t(v) = e(B(v, \lambda)) \cdot t(v). \tag{92$'$}$$

Since L' is by definition the set of common zeros of the functions $e(B(v, \lambda)) - 1$ for λ in L, an easy transversality argument shows that any solution of (92′) is given by[17]

$$t(v) = \sum_{\lambda' \in L'} T(\lambda') \cdot \delta(v - \lambda') \tag{93}$$

with a suitable complex-valued function T on L'. This being so, Equation (91) amounts to the relation (for λ in L and λ' in L')

$$T(\lambda' + \lambda) = e(\tfrac{1}{2}F(\lambda)) \cdot (-1)^{B(\lambda', \lambda)} \cdot T(\lambda') \tag{94}$$

and implies therefore

$$t = \sum_{s \in S} T(-s) \sum_{\lambda \in L} e(\tfrac{1}{2}F(\lambda)) \cdot (-1)^{B(s, \lambda)} \cdot \delta(v - \lambda + s)$$

that is

$$t = \sum_{s \in S} T(-s) \cdot A_s u.$$

We can now state the main result of this section.

THEOREM 2. *Let L be any lattice in V such that B takes integral values on $L \times L$, and let F be any solution of the Equation* (71) *with $m = 1$. Let L' be the lattice complementary to L and put $[L' : L] = e^2$.*[18] *Finally, let $(\varpi, \mathscr{H})$ be any irreducible representation of G such that $\varpi(\iota_t) = e(t) \cdot I$ for every real t.*

[17] By definition, the Dirac distribution $\delta(v - a)$ takes the value $\phi(a)$ on any test-function ϕ. For instance, (88) can be written $u(v) = \sum_{\lambda \in L} e(\tfrac{1}{2}F(\lambda)) \cdot \delta(v - \lambda)$ and similarly for (89).

[18] The index $[L' : L]$ is equal to the determinant of the matrix $\{B(v_i, v_j)\}$ where $\{v_1, \cdots, v_{2n}\}$ is any basis of V for which L is the set of vectors with integral coordinates.

(a) *The induced representation $\mathcal{D}_{L,F}$ is isomorphic to the direct sum of e copies of* $(\varpi, \mathcal{H})$.

(b) *The set of solutions of the equations*

$$\varpi(e^{\lambda}) \cdot t = e(\tfrac{1}{2}F(\lambda)) \cdot t \qquad (\lambda \text{ in } L) \tag{95}$$

is an e-dimensional subspace of $\mathcal{H}_{-\infty}$.

Since the algebra of operators in $\mathcal{H}_{L,F}$ commuting to $\pi(G)$ is finite-dimensional (its dimension being in fact equal to e^2), the representation $\mathcal{D}_{L,F}$ splits into a direct sum of finitely many irreducible components $\mathcal{D}_1, \cdots, \mathcal{D}_p$. Since $\pi(\iota_t) = e(t) \cdot I$, the classification of the representations of G shows these representations are indeed equivalent to $(\varpi, \mathcal{H})$. The commuting algebra is therefore isomorphic to the algebra of all $p \times p$ matrices and a dimension argument gives $p = e$. This proves (a). As to (b), it suffices to use (a) and to remark that the set of solutions of Equation (90) is an e^2-dimensional subspace of $(\mathcal{H}_{L,F})_{-\infty}$ by Lemma 3.

13. **Fock representation.** In order to define invariantly the Fock representation, we need a real number $\lambda \neq 0$ and an operator J in V with the properties:

$$J^2 v = -v, \tag{96}$$

$$B(Jv, Jv') = B(v, v'), \tag{97}$$

$$B(v, Jv) \geqq 0, \tag{98}$$

for any pair v, v' of elements of V. We have also to consider the complexification V_c of V, that is a complex vector space containing V such that every one of its elements can be written uniquely as $x = v + iv'$ with v and v' in V. The conjugate $\bar{x}$ of the vector x is by definition $v - iv'$. The bilinear form B on $V \times V$ extends to a complex bilinear form B_c on $V_c \times V_c$. The complex extension J_c of J to V_c has a square equal to minus the identity operator; it has therefore the eigenvalues i and $-i$ with respective eigenspaces some subspace W of V_c and its conjugate $\overline{W}$ (set of all vectors $\bar{x}$ for x in W). Using (97), one sees that B_c induces the zero form on both W and $\overline{W}$.

If we replace in the definition of G the real pairs (t, v) by complex ones (that is t is a complex number and v is in V_c) and still use the rule (37) to compute the product, we define a Lie group G_c, containing G as a closed subgroup, and with Lie algebra the complexification $\mathfrak{g}_c$ of $\mathfrak{g}$. Moreover the set of pairs $(t, \bar{x})$ with t complex and x in W is a closed subgroup P of G_c such that $G \cap P = Z$ and $G \cdot P = G_c$. We define a continuous homomorphism δ_λ from P to the multiplicative group of nonzero complex numbers by

$$\delta_\lambda(t, \bar{x}) = e(\lambda t). \tag{99}$$

With all these conventions in mind, we can define the Fock representation as a kind of *holomorphic induced representation.*[19] Indeed, it acts on a Hilbert space consisting of all functions f on G_c subjected to the following restrictions:

(a) f is holomorphic;

(b) one has $f(pg) = \delta_\lambda(p) \cdot f(g)$ for p in P and g in G_c;

(c) the integral $\int_{Z\backslash G} |f(g)|^2 \, dg$ is finite.[20]

The scalar product is given by the integral

$$(f|f') = \int_{Z\backslash G} \overline{f(g)} \cdot f'(g) \, dg \tag{100}$$

and the group G acts by the right translations defined by

$$(R_h f)(g) = f(gh). \tag{101}$$

In the applications, it is more convenient to shift everything to V as follows. We denote by V_J the complex vector space having V as underlying real space in which J is the scalar multiplication by i. On V_J, there is a unique hermitian form H having B as imaginary part; explicitly, one has:

$$H(v, v') = B(v, Jv') + i \cdot B(v, v') \tag{102}$$

and, according to (98), one has $H(v, v) \geqq 0$ for any v.

The correspondence $f \rightleftarrows \phi$ devised by the formula

$$\phi(v) = e^{\pi\lambda H(v,v)/2} \cdot f(e^v) \tag{103}$$

maps isomorphically the space of the Fock representation onto the Hilbert space $\mathscr{F}_J$ whose elements are the C^∞-functions ϕ on V satisfying the properties

$$\theta_{JX}\phi = i \cdot \theta_X \phi \qquad \text{(for every } X \text{ in } V\text{)}, \tag{104}$$

$$\int_V e^{-\pi\lambda H(v,v)} |\phi(v)|^2 \, dv < \infty. \tag{105}$$

The equation (104) is nothing else than the set of Cauchy-Riemann equations in an invariant guise and expresses that ϕ is holomorphic on V_J. As to the scalar product, it is given by

$$(\phi|\phi') = \int_V e^{-\pi\lambda H(v,v)} \overline{\phi(v)} \phi'(v) \, dv \tag{106}$$

and the operator associated to $\iota_t \cdot e^v$ is $\varpi_J(\iota_t \cdot e^v) = e(\lambda t) \cdot U_v$ where U_v is expressed as follows

$$(U_v\phi)(v') = e^{-\pi\lambda[H(v,v)/2 + H(v,v')]} \cdot \phi(v + v'). \tag{107}$$

[19] I thank heartfully J. Dixmier for having pointed out to me the importance of this notion and its bearing to our problems.

[20] By condition (b) for $p = \iota_t$ we get that $|f|^2$ is constant on every coset Zg, giving a meaning to the previous integral.

The infinitesimal representation ϖ'_J associated to ϖ_J is given by

$$\varpi'_J(X)\cdot\phi = \theta_X\cdot\phi - \pi\lambda H_X\cdot\phi \tag{108}$$

where H_X is the linear function $v \mapsto H(X, v)$ on V. We have to make the usual proviso, that is $(\mathscr{F}_J)_\infty$ is the set of all holomorphic functions ϕ on V_J such that $\varpi'_J(X_1)\cdots\varpi'_J(X_p)\cdot\phi$ is in $\mathscr{F}_J$ whatever $X_1,\cdots,X_p$ is in V, and $(\mathscr{F}_J)_{-\infty}$ consists of the finite sums of functions of the form $\varpi'_J(X_1)\cdots\varpi'_J(X_p)\cdot\phi$ with $X_1,\cdots,X_p$ in V and ϕ in $\mathscr{F}_J$. Taking into account the Cauchy-Riemann equations (104) and the obvious relation $H_{JX} = -iH_X$, we can transform (108) as follows[21]

$$\varpi'_J(Y)\cdot\phi = \theta_X\phi, \tag{109}$$

$$\varpi'_J(\overline{Y})\cdot\phi = -\pi\lambda H_X\cdot\phi \tag{110}$$

where Y is the unique element in W such that $X = Y + \overline{Y}$, that is

$$Y = \tfrac{1}{2}(X - i\cdot JX). \tag{111}$$

The main result concerning the Fock representation can be stated as follows.

THEOREM 3. *Let J be any operator in V satisfying the relations* (96) *to* (98) *and $\lambda \neq 0$ be real. Let W be the subspace of the complexification V_c of V associated to the eigenvalue i of the complex extension J_c of J to V_c.*

(a) *The Fock representation $(\varpi_J, \mathscr{F}_J)$ is irreducible.*

(b) *If $(\varpi, \mathscr{H})$ is any irreducible representation of G which is nontrivial on the center Z of G, the vectors in $\mathscr{H}_{-\infty}$ annihilated by $\varpi'(W)$ form a one-dimensional subspace of $\mathscr{H}_\infty$.*

We first prove (b) in case of the Fock representation. According to the description of $(\mathscr{F}_J)_{-\infty}$ and formula (109), an element of $(\mathscr{F}_J)_{-\infty}$ annihilated by $\varpi'_J(W)$ is a holomorphic function ϕ on V_J such that $\theta_X\phi = 0$ for every X in V, that is a constant.

For every real t, one has $\varpi_J(\iota_t) = e(\lambda t)\cdot I$. We may assume $\varpi(\iota_t) = e(\lambda t)\cdot I$ in view of the arbitrariness of λ. According to von Neumann results [9], the Fock representation is therefore isomorphic to the direct sum of a certain number m (finite or not) of copies of $(\varpi, \mathscr{H})$. Accordingly, the subspace T of $(\mathscr{F}_J)_{-\infty}$ annihilated by $\varpi'_J(W)$ contains the (algebraic) direct sum of m copies of the space S in $\mathscr{H}_{-\infty}$ annihilated by $\varpi'(W)$. Since T is one-dimensional, we get $m = 1$ and $\dim S = 1$. This proves assertions (a) and (b) in Theorem 3.

We conclude by some explicit formulas. Since H is a positive nondegenerate hermitian form on V_J we can choose a (complex) basis $\{P_1,\cdots,P_n\}$ for V_J such that $H(P_k, P_l) = \delta_{kl}$ and set $Q_j = J\cdot P_j$. It is easy to see that

$$\{z, P_1,\cdots,P_n, Q_1,\cdots,Q_n\}$$

[21] We have extended in the obvious way ϖ'_J to a representation of the complex Lie algebra $\mathfrak{g}_c$.

is a normal basis of $\mathfrak{g}$. Moreover, if we denote by $z_1, \cdots, z_n$ the complex-linear functions on V_J defined by $z_k(P_l) = \delta_{kl}$, the monomials

$$M_\alpha = \lambda^{n/2}\prod_{j=1}^{n} \frac{(\pi\lambda)^{\alpha_j/2}}{(\alpha_j!)^{1/2}} z_j^{\alpha_j} \qquad \alpha = (\alpha_1, \cdots, \alpha_n) \tag{112}$$

form an orthonormal basis of $\mathcal{F}_J$.[22] According to (109) and (110), the infinitesimal operator $\varpi'_J(P_j - iQ_j)$ is twice the derivation with respect to the complex variable z_j and $\varpi'_J(P_j + iQ_j)$ is multiplication by $-2\pi\lambda z_j$.

14. **Definition of theta functions.** The whole machinery of Riemann forms can now be set up. To summarize, let be given:

—a real vector space V of finite dimension $2n$;
—a nondegenerate alternating bilinear form B on $V \times V$;
—an operator J on V satisfying to the relations (96) to (98);
—a lattice L in V such that B takes integral values on $L \times L$;
—a real-valued function F on V such that

$$F(\lambda + \mu) \equiv F(\lambda) + F(\mu) + B(\lambda, \mu) \qquad (\text{mod } 2) \tag{113}$$

for any pair λ, μ of elements of L.

By means of these data, a Fock representation $(\varpi_J, \mathcal{F}_J)$ (with $\lambda = 1$) is defined whose irreducibility follows from Theorem 3. By Theorem 2, the solutions of the equation

$$\varpi_J(e^\lambda)\cdot t = e(\tfrac{1}{2}F(\lambda))\cdot t \qquad (\text{for every } \lambda \text{ in } L) \tag{114}$$

form an e-dimensional subspace Θ of $(\mathcal{F}_J)_{-\infty}$. Made explicit, the previous equation reads as follows

$$t(v) = t(v + \lambda)\cdot \exp -\pi[\tfrac{1}{2}H(\lambda, \lambda) + H(\lambda, v) + i\cdot F(\lambda)] \tag{115}$$

and is nothing else than the well-known functional equation defining the theta functions. We get Frobenius' theorem that the dimension of the space of solutions of (115) is given as the square root of the discriminant of B with respect to L.

A few questions to conclude: The group G is nothing but a special instance of a real nilpotent algebraic group. How can one extend to the general case the three methods given here to generate irreducible representations of such a group? What kind of functions on such a group play the role of theta functions?

[22] Following Bergman's well-known procedure, we ought to introduce the kernel

$$K(v, v') = \sum_\alpha \overline{M_\alpha(v)}\cdot M_\alpha(v')$$

given here by $K(v, v') = e^{\pi\lambda H(v, v')}$. Its intrinsic meaning is as follows. For every v in V, the function $v' \mapsto K(v, v')$ is an element K_v of $\mathcal{F}_J$ and we have $(K_v | f) = f(v)$ for every function f in $\mathcal{F}_J$.

References

1. F. Bruhat, *Sur les représentations induites des gıoupes de Lie*, Bull. Soc. Math. France **84** (1956), 97–205.

2. P. Cartier, *Analyse spectrale et théorème de prédiction statistique de Wiener*, Séminaire Bourbaki, 13ᵉ année, 1960/61, exp. 218.

3. J. Dixmier, *Sur la relation* $i(PQ - QP) = I$, Compositio Math. **13** (1958), 263–269.

4. L. Gårding, *A note on continuous representations of Lie groups*, Proc. Nat. Acad. Sci. U.S.A. **33** (1947), 331–332.

5. I. Gelfand and I. Piateskii-Shapiro, *Theory of representations and theory of automorphic functions*, Amer. Math. Soc. Transl. (2) **26** (1963), 173–200.

6. T. Kato, *On the commutation relation* $AB - BA = c$, Arch. Rational Mech. Anal. **10** (1962), 273–275.

7. G. Mackey, *Induced representations of locally compact groups* I., Ann. of Math. **55** (1952), 101–139; II. **58** (1953), 193–221.

8. E. Nelson, *Analytic vectors*, Ann. of Math. **70** (1959), 572–615.

9. J. von Neumann, *Die Eindeutigkeit der Schrödingerschen Operatoren*, Math. Ann. **104** (1931), 570–578.

10. F. Rellich, *Der Eindeutigkeitssatz für die Lösungen der quantenmechanischen Vertauschungsrelationen*, Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. (1946), 107–115.

11. M. Stone, *Linear transformations in Hilbert space*, III. *Operational methods and group theory*, Proc. Nat. Acad. Sci. U.S.A. **16** (1930), 172–175.

12. A. Weil, *Sur certains groupes d'opérateurs unitaires*, Acta Math. **113** (1964), 143–211.

13. H. Weyl, *The theory of groups and quantum mechanics*, Dover Publications, New York, 1950.

V. Quotients of Symmetric Spaces. Deformations

Cohomologies of Vector-valued Forms on Compact, Locally Symmetric Riemann Manifolds

BY

SHINGO MURAKAMI

This is a report on the cohomology groups of the title. After giving their precise definitions in §1, we shall give a survey of examples and applications in various topics, which were actually the motivations for the study of these cohomology groups. In §3 we shall outline some general theorems on these cohomology groups obtained jointly by Y. Matsushima and the speaker **[19]**, **[20]**. We note that a clear survey of the same subjects is given by A. Borel **[4]** and we follow it in parts of §2.

1. **Definitions.** Let X be a symmetric Riemann space of negative curvature. We may put $X = G/K$ where G is a connected semisimple Lie group with a faithful representation and K is a maximal compact subgroup of G. Indeed, the identity component $I(X)^0$ of the group of all isometries of X is a connected semisimple Lie group whose center reduces to (e) and which acts transitively on X, and the isotropy subgroup of $I(X)^0$ at a point of X is a maximal compact subgroup; therefore, we may take, for example, this group $I(X)^0$ for G in $X = G/K$. Let Γ be a discrete subgroup of G. We always assume that the quotient $\Gamma\backslash G$ is compact. The group Γ acts on X as a properly discontinuous group and the quotient $M = \Gamma\backslash X$ is compact. In this report, we suppose always that Γ acts freely on X, i.e. that any element of Γ different from the identity acts on X without fixed point, so that M is a compact, locally symmetric Riemann manifold. This assumption, which is equivalent to that Γ has no nontrivial element of finite order, is merely conventiona' In fact, the following definitions and all theorems (such as found in §3) about the cohomology groups are valid without this assumption. The general case can be treated by depending on the results of Baily **[2]** or by using a lemma of Selberg **[23]**; according to this lemma, a discrete subgroup Γ of G with compact quotient $\Gamma\backslash G$ has a normal subgroup Γ_1 of finite index which has no nontrivial element of finite order. We note also that Γ is finitely generated **[25]**.

Let now F be a finite-dimensional real or complex vector space and let j be a GL(F)-valued automorphic factor on $G \times X$, i.e. a C^∞-mapping of $G \times X$ into GL(F) such that

$$j(st, x) = j(s, tx)j(t, x)$$

for all $s, t \in G$ and $x \in X$. We denote by $A^r(\Gamma, X, j)$ the vector space of all F-valued

C^∞-forms η of degree r on X such that

$$(1.1) \qquad (\eta \circ L_\gamma)_x = j(x, \gamma)\eta_x$$

for all $\gamma \in \Gamma$ and $x \in X$, where $\eta \circ L_\gamma$ denotes the form which results by transforming η by the transformation L_γ of X defined by γ. Under the assumption that Γ acts freely on X, the space $A^r(\Gamma, X, j)$ can be interpreted as follows. Let E_j be the quotient of $X \times F$ by the equivalence relation $(x, u) \sim (\gamma x, j(\gamma, x)u)(\gamma \in \Gamma, u \in F)$; E_j is the vector bundle over the manifold $M = \Gamma\backslash X$ associated to the bundle $X \to M$ of group Γ by the factor j. The space $A^r(\Gamma, X, j)$ is canonically identified with the space cf all C^∞-forms of degree r with values in the sections of E_j.

The cohomology groups in which we are interested are now defined in the following two cases.

(1) Suppose that j is a representation ρ of G in F, namely, $j(s, x) = \rho(s)$ for all $s \in G$ and $x \in X$. In this case the exterior differentiation d defines a coboundary operator in the graded module $A(\Gamma, X, \rho) = \sum_r A^r(\Gamma, X, \rho)$. The cohomology groups then derived will be called, for simplicity, *d-cohomology groups* (of vector valued forms) and will be denoted by $H^r(\Gamma, X, \rho)$.

(2) Suppose that X is a symmetric bounded domain in C^N, that F is a complex vector space and that $j(s, x)$ is holomorphic in $x \in X$ for each $s \in G$. In this case, the space $A^r(\Gamma, X, j)$ decomposes into the direct sum $\sum_{p+q=r} A^{p,q}(\Gamma, X, j)$ where $A^{p,q}(\Gamma, X, j)$ is the subspace consisting of forms of type (p, q). The part d'' of type $(0, 1)$ of the operator d defines a coboundary operator of type $(0, 1)$ in the bigraded module $A(\Gamma, X, j) = \sum_{p,q} A^{p,q}(\Gamma, X, j)$. The cohomology groups then defined are called *d''-cohomology groups* (of vector valued forms) and will be denoted by $H_{d''}^{p,q}(\Gamma, X, j)$.

In practice, we shall suppose in the second case that the automorphic factor j is a so-called *canonical automorphic factor* J_τ defined by a representation τ of K in F. This notion generalizes the automorphic factor $\tau(cx + d)$ on the Siegel's upper half plane, in which case $G = \mathrm{Sp}(n, \boldsymbol{R})$, $K = U(n)$ and τ is extended to a holomorphic representation of the complexified group $K^C = \mathrm{GL}(n, \boldsymbol{C})$. We refer to Matsushima and Murakumi **[19]**, Ise **[11]** and Borel **[33]** for the exact definition of canonical automorphic factors (cf. Gunning **[9]**, Langlands **[31]**).

The d- and d''-cohomology groups can be interpreted as follows. In the case $j = \rho$, let $H^p(\Gamma, F)$ be the cohomology group of the group Γ with coefficients in the Γ-module F. On the other hand, since the vector bundle E_ρ is locally constant, we can define the sheaf $\mathscr{C}(E_\rho)$ of germs of locally constant sections of E_ρ over M. Then there holds

$$(1.2) \qquad H^p(\Gamma, F) \cong H^p(\Gamma, X, \rho) \cong H^p(M, \mathscr{C}(E_\rho)).$$

The first isomorphism follows from the facts that $X \to M$ is a covering and that X is homeomorphic to a euclidean space. The second one, which may be called "de

Rham isomorphism," follows from the following resolution of the sheaf $\mathscr{C}(E\rho)$:

$$\mathscr{C}(E\rho) \xrightarrow{d} \mathscr{A}^0(\Gamma, X, \rho) \xrightarrow{d} \mathscr{A}^1(\Gamma, X, \rho) \xrightarrow{d} \cdots,$$

where $\mathscr{A}^p(\Gamma, X, \rho)$ denotes the sheaf of germs of p-forms on M with values in the sections of E_ρ. As for the d''-cohomology, we note that E_j is a holomorphic vector bundle over the complex manifold M. Let $\Omega^p(E_j)$ be the sheaf of germs of holomorphic p-forms on M with values in the sections of E_j. Then we have a "Dolbeault isomorphism":

$$H^{p,q}_{d''}(\Gamma, X, j) \cong H^q(M, \Omega^p(E_j)). \tag{1.3}$$

2. **Applications of the cohomology groups.**

2.1. *Local triviality of deformations of* Γ *in* G. Let us first define the deformation space R of a discrete group H in a Lie group P following Weil [**25**]; R is the space of all homomorphisms of H into P endowed with the compact-open topology. When H is finitely generated, R is homeomorphic to a closed subspace of the product of a certain finite number of copies of P. We say that deformations of the subgroup $r(H)$ $(r \in R)$ in P are *locally trivial* if $\{\mathrm{Int}(s) \circ r;\ s \in P\}$ forms a neighborhood of r in R. Now, take a point $r \in R$ and denote by $\mathfrak{p}$ the Lie algebra of P. Regarding $\mathfrak{p}$ as an H-module through the representation $\mathrm{ad} \circ r$ of H in $\mathfrak{p}$, Weil [**27**] has proved that if $H^1(H, \mathfrak{p}) = (0)$ then deformations of $r(H)$ in P are locally trivial. Applying this result to the case $P = G$, $H = \Gamma$ and r is the injection of Γ into G, it follows from (1.2) that deformations of Γ in G are locally trivial, if $H^1(\Gamma, X, \mathrm{ad}) = (0)$. Weil's argument in [**26**] shows that this is the case if G has finite center and if all simple components of G are noncompact and of dimension >3 (cf. [**19**]). Actually, Weil [**26**] proves moreover that deformations of Γ in G are locally trivial if G decomposes into a product of noncompact simple Lie groups of finite center and if the projection of Γ in any simple factor of dimension 3 is not discrete.

REMARK. The Weil's theorem was first given by Selberg [**23**] for the case $G = \mathrm{SL}(n, R)$. On the other hand, the group $H^1(\Gamma, X, \mathrm{ad})$ is isomorphic, via (1.2), to the first cohomology group of M with coefficients in the sheaf of germs of Killing vector fields [**19**]. Therefore, $H^1(\Gamma, X, \mathrm{ad}) = (0)$ means in a sense the rigidity of the compact locally symmetric Riemannian structure of M, and this fact was first recognized by Calabi (cf. [**5**]) for the case that X is a space of constant negative curvature of dimension >2. We note also that the vanishing of $H^1(\Gamma, X, \mathrm{ad})$ is discussed in detail by Raghunathan [**22**] as a special case of a more general result (see §3, Corollary to Theorem 1).

2.2. *Local triviality of deformations of the complex structure of* M. We consider the case that X is a symmetric bounded domain in C^N. By a famous theorem due to Fröhlicher and Nijenhuis [**10**] and Kodaira and Spencer [**15**], deformations of the complex structure of the compact complex manifold M are locally trivial if the first cohomology group $H^1(M, \Omega^0(\Theta)) = (0)$, where Θ is the holomorphic tangent bundle of M. Now, Calabi and Vesentini [**6**] establish a vanishing theorem for the cohomology groups $H^q(M, \Omega^0(\Theta))$, and in particular they show that $H^1(M, \Omega^0(\Theta)) = (0)$ if all of irreducible components of X are of complex dimension > 1.

The cohomology groups $H^p(M, \Omega^0(\Theta))$ can be treated also in the framework of the d''-cohomology of vector valued forms. In fact, let $\mathfrak{g}$ be the Lie algebra of the Lie group G acting on X and let $\mathfrak{k}$ be the subalgebra of $\mathfrak{g}$ corresponding to the subgroup K. Then the complex structure of X defines a vector space decomposition of the complexification $\mathfrak{g}^C$ of $\mathfrak{g}$:

$$\mathfrak{g}^C = \mathfrak{k}^C + \mathfrak{n}^+ + \mathfrak{n}^- \tag{2.1}$$

where $\mathfrak{n}^+$ (resp. $\mathfrak{n}^-$) consists of those elements of $\mathfrak{g}^C$ which project to complex tangent vectors of type $(1, 0)$ (resp. $(0, 1)$) at the point $\pi(e)$ by the projection $\pi: G \to X = G/K$. We know that $\mathfrak{n}^\pm$ are abelian subalgebras of $\mathfrak{g}^C$ stable under the adjoint action of K in $\mathfrak{g}^C$. Therefore, we can define representations ad_+ and ad_- of K in the complex vector spaces $\mathfrak{n}^+$ and $\mathfrak{n}^-$ respectively. Then we see that Θ is just the vector bundle over M associated to the canonical automorphic factor J_{ad_+} on $X \times G$ **[11]**, **[19]**. By (1.3) it follows

$$H^q(M, \Omega^0(\Theta)) = H^{0,q}_{d''}(\Gamma, X, J_{\mathrm{ad}_+}).$$

In this form the theorem of Calabi and Vesentini follows from a more general vanishing theorem for d''-cohomology groups (see §3, Corollary to Theorem 6).

REMARK. The local triviality of deformations of the complex structure on $M = \Gamma\backslash X$ is recently proved in a more general case by Andreotti and Vesentini **[1]**, where $\Gamma\backslash X$ is no longer compact but where Γ verifies certain conditions satisfied by arithmetic subgroups of G and the deformations are supposed "rigid at infinity."

2.3. *Betti numbers of the manifold M.* The usual real cohomology groups $H^p(M, \boldsymbol{R})$ of the manifold M are isomorphic, through the de Rham's isomorphisms, with the d-cohomology groups $H^p(\Gamma, X, 1)$, 1 denoting the 1-dimensional trivial representation of G. The general method to approaching d-cohomology groups may therefore be applied to the study of Betti numbers of M. Along this line, Matsushima **[16]** showed at first that the first Betti number of M vanishes if X is a bounded domain all of whose irreducible factors are not isomorphic to the unit open ball in $\boldsymbol{C}^N$; this implies in particular that the index of Γ over the commutator subgroup $[\Gamma, \Gamma]$ is finite in this case. Matsushima **[17]** establishes moreover a general condition, which appeared in **[16]** for the case $p = 1$, in order that the cohomology group $H^p(\Gamma, X, 1)$ be isomorphic to the relative Lie algebra cohomology group $H^p(\mathfrak{g}, \mathfrak{k})$ or, what amounts to the same, to the cohomology group $H^p(X_u, \boldsymbol{R})$ of the so-called compact form X_u of X. This condition is formulated in terms of positivity of a certain quadratic form $H_p(\mathfrak{g})$ associated to the Lie algebra $\mathfrak{g}$ of G, and the values of p for which $H_p(\mathfrak{g}) > 0$ are determined by Matsushima **[16]**, **[17]** in the case that X is an irreducible bounded symmetric domain and by Kaneyuki and Nagano **[12]**, **[13]** for the remaining cases.

Matsushima [**18**] has recently obtained the following interesting formula which expresses the pth Betti number $b_p(M)$ of M in terms of the unitary representation of G in the Hilbert space $L^2(\Gamma\backslash G)$ and which corresponds to the well-known Cartan and Hodge's theorem for the case G compact and $\Gamma = (e)$:

$$b_p(M) = \sum_{\tau\in\mathscr{D}_0} N(\Gamma, T)\left(\sum_{i=1}^{s_p} M(T_K, \tau_i^p)\right).$$

Here $\mathscr{D}_0$ denotes the set of all nonequivalent irreducible unitary representations T of G whose defining Casimir operator is trivial; $N(\Gamma, T)$ is the multiplicity of T in the unitary representation of G in the Hilbert space $L^2(\Gamma\backslash G)$; τ_i^p $(i = 1,\cdots, s_p)$ are the irreducible components of the representation ad^p of K into the space $\Lambda^p\mathfrak{m}^C$, namely $\mathrm{ad}^p = \tau_1^p + \cdots + \tau_{s_p}^p$ (cf. (3.2)); $M(T_K, \tau_i^p)$ is the multiplicity of τ_i^p in the restriction T_K of T to K. The formula implies in particular that if X is 3- (resp. 4-) dimensional hyperbolic space and if G is the proper Lorentz group (resp. de Sitter group) the first Betti number of M is equal to the multiplicity of an irreducible unitary representation of G.

2.4. *Automorphic forms.* We suppose that X is a bounded symmetric domain in C^N. The d''-closed forms belonging to $A^{0,0}(\Gamma, X, j)$ are just the holomorphic functions f on X such that

$$f(\gamma x) = j(\gamma, x)f(x)$$

for all $\gamma\in\Gamma$ and $x\in X$, and they are by definition the automorphic forms on X with respect to Γ and j. Thus the d''-cohomology group $H_{d''}^{0,0}(\Gamma, X, j)$ is nothing but the space of all automorphic forms on X with respect to Γ and j.

Suppose now that the factor j is the canonical automorphic factor J_τ defined by a representation τ of K. The canonical line bundle of M is defined by the canonical automorphic factor J_σ, where σ is the representation of K given by $\sigma(t) = \det(\mathrm{ad}_-(t))$ for $t\in K$ (cf. (2.1)). Then we get

$$H_{d''}^{N,0}(\Gamma, X, J_\tau) \cong H_{d''}^{0,0}(\Gamma, X, J_{\sigma\otimes\tau}).$$

On the other hand, as we shall see in §3, if τ is irreducible and is contained in an irreducible representation ρ of G in such a way that the lowest weight of τ coincides with that of ρ restricted to K, we have a canonical isomorphism

$$H_{d''}^{N,0}(\Gamma, X, J_\tau) \cong H^{N,0}(\Gamma, X, \rho).$$

Thus we get

$$H^{N,0}(\Gamma, X, \rho) \cong \text{"space of all automorphic forms on } X \text{ with respect to } \Gamma \text{ and the automorphic factor } J_{\sigma\otimes\tau}.\text{"}$$

This generalizes a theorem of Eichler [**8**] and Shimura [**24**].

2.5. *Determination of cohomology groups.* The d- and d''-cohomology groups are determined by Matsushima and Shimura [**21**] in the following case. Put $X = H_1 \times H_2 \times\cdots\times H_N$ and $G = G_1\times G_2\times\cdots\times G_N\times K_0$ where H_i is the upper half plane, $G_i = \mathrm{SL}(2, \boldsymbol{R})$ acting canonically on H_i $(i = 1, 2,\cdots, N)$ and

K_0 is a compact connected Lie group acting trivially on X. Then X is a homogeneous space of G. Let Γ be a discrete subgroup of G with the following properties. (1) The projection of G onto $G_0 = G_1 \times G_2 \times \cdots \times G_N$ maps Γ bijectively on a discrete subgroup Γ_0 of G_0 with compact quotient $\Gamma_0 \backslash G_0$. (2) The projection of Γ_0 into any partial factor of G_0, different from G_0 itself, is not discrete in the partial factor. (3) $\Gamma_0/(\Gamma_0 \cap Z)$ has no element of finite order different from the identity, where Z is the center of G_0. Matsushima and Shimura determine completely the d-cohomology groups $H^r(\Gamma, X, \rho)$ for all irreducible representations ρ of G and also obtain some vanishing theorems for the groups $H^{0,q}_{d''}(\Gamma, X, J_\tau)$. See **[21]** for the details.

3. **Theorems on the cohomology groups.** We retain the notations in §1. We assume throughout this section that F is a complex vector space, although all statements about d-cohomology in §3.1 hold also for real F. We confine our attention to the cases where the automorphic factor j is an *irreducible* representation ρ of G or a canonical automorphic factor J_τ defined by an *irreducible* representation τ of K.

We refer **[19]** and **[20]** for the details of this section.

3.1. *Harmonic theory.* We consider the following diagram and we get

LEMMA 1. *The vector bundle E_j is differentiably equivalent to the bundle associated to the principal bundle $\Gamma \backslash G$ over M with group K by the representation τ of K in F; here τ is defined by $\tau(t) = j(t, x_0)$ $(t \in K)$, x_0 being the point $\pi(e) \in X$.*

$$\begin{tikzcd}
 & G \arrow[dl, "\pi"'] \arrow[dr, "\varpi"] & \\
X = G/K \arrow[dr, "\varpi"'] & & \Gamma \backslash G \arrow[dl, "\pi"] \\
 & M = \Gamma \backslash X/K &
\end{tikzcd}$$

Note that if $j = J_\tau$ we have $J_\tau(t, x_0) = \tau(t)$ for all $t \in K$.

Since Γ is discrete, each left invariant vector field on G is projectable onto $\Gamma \backslash G$, and so the Lie algebra $\mathfrak{g}$ can be identified with a Lie algebra of vector fields on $\Gamma \backslash G$. The manifold $\Gamma \backslash G$ is then parallelizable by means of a basis of $\mathfrak{g}$. Now by Lemma 1 the space $A^r(\Gamma, X, j)$ can be canonically identified with the space of all F-valued r-forms η on $\Gamma \backslash G$ such that

$$(3.1)\qquad \begin{aligned} (\theta(X) + \tau(X))\eta &= 0, \\ i(X)\eta &= 0, \end{aligned}$$

for any $X \in \mathfrak{k}$, where $\theta(X)$ and $i(X)$ denote the operators of Lie derivation and the interior product by X respectively. Let $\mathfrak{m}$ be the orthogonal complement of $\mathfrak{k}$ in $\mathfrak{g}$ with respect to the Killing form ϕ of $\mathfrak{g}$. There holds

$$(3.2)\qquad \mathfrak{g} = \mathfrak{m} + \mathfrak{k}, \qquad [\mathfrak{k}, \mathfrak{m}] \subset \mathfrak{m}, \qquad [\mathfrak{m}, \mathfrak{m}] \subset \mathfrak{k}.$$

This implies in particular that $\mathfrak{m}$ defines a connection in the principal fibre bundle $\Gamma \backslash G$ of group K. We shall denote by D the covariant differentiation with respect to this connection; D is an operator of degree 1 in the graded module

$$A(\Gamma, X, j) = \sum_r A^r(\Gamma, X, j).$$

Suppose j be the factor J_τ. We can then prove that $\mathfrak{m}$ defines a connection of type $(1, 0)$ in the holomorphic principal bundle of E_{J_τ}. It follows that the coboundary operator d'' on $A(\Gamma, X, J_\tau)$ coincides just with the $(0, 1)$-part D'' of the operator D.

We consider next the case $j = \rho$. Let $\mathfrak{F}$ be the space of all F-valued C^∞-functions on $\Gamma\backslash G$; $\mathfrak{F}$ has the $\mathfrak{g}$-module structure m defined by $m(X)f = Xf + \rho(X)f$ for $X \in \mathfrak{g}$ and $f \in \mathfrak{F}$. Since $\Gamma\backslash G$ is parallelizable by $\mathfrak{g}$ an F-valued r-form on $\Gamma\backslash G$ can be regarded as an r-cochain on $\mathfrak{g}$ with values in the $\mathfrak{g}$-module $\mathfrak{F}$. Since $\tau(X) = \rho(X)$ for $X \in \mathfrak{k}$ in Lemma 1, (3.1) shows that $A^r(\Gamma, X, \rho)$ may be considered as the relative cochain group $C^r(\mathfrak{g}, \mathfrak{k}; \mathfrak{F})$ of $\mathfrak{g}$ modulo $\mathfrak{k}$. We can prove moreover that the operator d in $A(\Gamma, X, \rho)$ coincides with the coboundary operator in the relative cochain group $C(\mathfrak{g}, \mathfrak{k}; \mathfrak{F})$. We put $d_\rho = d - D$, so that $d = D + d_\rho$.

Let j be again subject only to our starting assumption. The manifold M has a Reimann metric induced from a G-invariant Riemann metric on X. On the other hand, there exists a hermitian inner product h in F invariant under $\tau(t)$ for all $t \in K$. If $j = \rho$, we may assume moreover that h is so chosen that $\rho(X)$ for $X \in \mathfrak{m}$ is a hermitian operator with respect to h. By virtue of Lemma 1, h defines canonically a hermitian metric in the fibres of E_j. Once these are introduced, we may apply harmonic theory as developed by Kodaira and Baily [2] in studying the cohomology groups in question; we define a hermitian product $(\ ,\ )$ among forms of $A(\Gamma, X, j)$ and the adjoint operators δ, D_*, δ_ρ and ∂'' of d, D, d_ρ and d'' respectively, the first three operators (resp. the last one) being defined for the case $j = \rho$ (resp. $j = J_\tau$). We define "laplacian operators" as follows:

$$\Delta = d\delta + \delta d, \qquad \Delta_D = DD_* + D_*D, \qquad \Delta_\rho = d_\rho\delta_\rho + \delta_\rho d_\rho$$

and

$$\square'' = d''\partial'' + \partial''d''.$$

Call a form η in $A(\Gamma, X, j)$ *harmonic* if $\Delta\eta = 0$ or if $\square''\eta = 0$. The fundamental theorem of harmonic theory states that $H^r(\Gamma, X, \rho)$ and $H^{p,q}_{d''}(\Gamma, X, J_\tau)$ are canonically isomorphic to the spaces of harmonic forms.

By explicit calculation of the laplacians Δ, Δ_D, and Δ_ρ, we get

THEOREM 1. $\Delta = \Delta_D + \Delta_\rho$ *and therefore a form* η *belonging to* $A(\Gamma, X, \rho)$ *is harmonic if and only if* $\Delta_D\eta = \Delta_\rho\eta = 0$.

COROLLARY. $H\rho(\Gamma, X, \rho) = (0)$ $(p \geqq 1)$ *if the following quadratic form on* $\mathrm{Hom}(\mathfrak{m}, F)$ *is positive definite.*

$$Q_p(u, v) = \sum_{i,k} h\left(\frac{1}{p}\rho(X_k)^2 u(X_i) + \rho([X_i, X_k])u(X_k), v(X_i)\right).$$

Here $\{X_1, \cdots, X_N\}$ *is a basis of* $\mathfrak{m}$ *such that* $\phi(X_i, X_j) = \delta_{ij}$, ϕ *being the Killing form of* $\mathfrak{g}$.

Indeed Corollary follows from Theorem 1, since $(\Delta_\rho\eta, \eta)$ is expressed as the integral of $\sum_{i_1\cdots i_{p-1}} Q_p(\eta_{i_1\cdots i_{p-1}}(x))$ on $\Gamma\backslash G, \eta_{i_1\cdots i_{p-1}}(x)$ being the Hom$(\mathfrak{m}, F)$-valued function on $\Gamma\backslash G$, defined for each $x \in \Gamma\backslash G$ by

$$\eta_{i_1\cdots i_{p-1}}(x)(Y) = \eta(Y, X_{i_1}, \cdots, X_{i_{p-1}})$$

for $Y \in \mathfrak{m}$.

REMARK. This corollary may be considered as a cohomological interpretation of Weil's arguments in [26]. Besides, Raghunathan [22] shows that $Q_1(u, v)$ is positive definite for almost all $(\mathfrak{g}, \rho)$.

There exists also the following expression of Δ in terms of the Casimir operator of C of $\mathfrak{g}$, which was pointed out by Kuga.

$$\Delta = -C + \rho(C). \tag{3.3}$$

More precisely, this means that if $\eta \in A^r(\Gamma, X, \rho)$

$$(\Delta\eta)(Y_1, \cdots, Y_r) = -C(\eta(Y_1, \cdots, Y_r)) + \rho(C)(\eta(Y_1, \cdots, Y_r))$$

for $Y_1, \cdots, Y_r \in \mathfrak{g}$, where C is considered as a differential operator of second order on $\Gamma\backslash G$, and $\rho(C)$ is the Casimir operator in F associated to the representation ρ. Note that $\rho(C)$ is a scalar operator, since ρ is absolutely irreducible.

3.2. *Decomposition of the d-cohomology groups.* From now on, we suppose always that X is a symmetric bounded domain in C^N. Consider the case $j = \rho$. The parts d' and d'' of types $(1, 0)$ and $(0, 1)$ of d define coboundary operators in $A^r(\Gamma, X, \rho)$. Moreover, let D', d'_ρ (resp. D'', d''_ρ) be the parts of type $(1, 0)$(resp. $(0, 1)$) of the operators D and d_ρ respectively. (Note that $d'' \neq D''$ in this case, although E_ρ is a holomorphic vector bundle.) Then $d' = D' + d'_\rho$ and $d'' = D'' + d''_\rho$. We can form the laplacians $\Delta', \Delta'', \Delta'_D, \Delta''_D, \Delta'_\rho, \Delta''_\rho$ from these operators d', d'', D', D'', d'_ρ, d''_ρ and their adjoint operators. Then we get

LEMMA 2. $\Delta = \Delta' + \Delta'' = \Delta'_D + \Delta''_D + \Delta'_\rho + \Delta''_\rho$, *and therefore a form* η *is harmonic if and only if* $\Delta'_D\eta = \Delta''_D\eta = \Delta'_\rho\eta = \Delta''_\rho\eta = 0$.

We see by this lemma that Δ preserves type of forms in $A^r(\Gamma, X, \rho)$. Thus we get

THEOREM 2. *The group* $H^r(\Gamma, X, \rho)$ *decomposes to the direct sum*:

$$H^r(\Gamma, X, \rho) = \sum_{p+q=r} H^{p,q}(\Gamma, X, \rho),$$

where $H^{p,q}(\Gamma, X, \rho)$ *is the subgroup of* $H^r(\Gamma, X, \rho)$ *consisting of all d-cohomology classes representable by a d-closed form of type* (p, q).

Let now

$$\mathfrak{g}^C = \mathfrak{k}^C + \mathfrak{n}^+ + \mathfrak{n}^- \tag{3.4}$$

be the decomposition (2.1) of $\mathfrak{g}^C$. We know that $\mathfrak{k}$ contains a Cartan subalgebra $\mathfrak{h}$ of $\mathfrak{g}$. Let Σ be the root system of $\mathfrak{g}^C$ with respect to the Cartan subalgebra $\mathfrak{h}^C$ and for each $\alpha \in \Sigma$ let X_α be an eigenvector. It is known that there is a subset Ψ

of Σ such that $\mathfrak{n}^+$ (resp. $\mathfrak{n}^-$) is spanned by $\{X_\alpha; \alpha \in \Psi\}$ (resp. $\{X_{-\alpha}; \alpha \in \Psi\}$). Moreover, one can introduce a linear ordering in the set of weights of $\mathfrak{g}^C$ such that any root $\alpha \in \Psi$ is positive and that a root β belongs to Ψ whenever $\beta > \alpha$ for some $\alpha \in \Psi$. We can choose $X_\alpha, X_{-\alpha}$ for all $\alpha \in \Psi$ so that $\phi(X_\alpha, X_{-\alpha}) = 1$ and that $X_{-\alpha} = \overline{X}_\alpha$, $-$ denoting the conjugation of $\mathfrak{g}^C$ with respect to $\mathfrak{g}$.

Lemma 3. *Let $Y_1, \cdots, Y_r$ be a basis of $\mathfrak{k}$ such that $\phi(Y_a, Y_b) = -\delta_{ab}$ $(a, b = 1, \cdots, r)$. The representation* ad_+(resp. ad_-) *of K on* $\mathfrak{n}^+$(resp. $\mathfrak{n}^-$) *induces representations* ad_+^q (resp. ad_-^p) *of $\mathfrak{k}^C$ on* $\Lambda^q\, \mathfrak{n}^+$ (resp. $\Lambda^p\, \mathfrak{n}^-$). *Then*

$$\sum_{a=1}^{r} \mathrm{ad}_+^q(Y_a)^2 = -\sum_{\alpha\in\Psi} \mathrm{ad}_+^q([X_\alpha, X_{-\alpha})] = -\frac{q}{2}\mathrm{id} \quad on \overset{q}{\Lambda}\, \mathfrak{n}^+,$$

$$\sum_{a=1}^{r} \mathrm{ad}_-^p(Y_a)^2 = \sum_{\alpha\in\Psi} \mathrm{ad}_-^p([X_\alpha, X_{-\alpha}]) = -\frac{p}{2}\mathrm{id} \quad on \overset{p}{\Lambda}\, \mathfrak{n}^-.$$

This lemma plays an important role in calculating laplacian operators. In fact, it implies in particular the following relation:

$$\Delta_D' - \Delta_\rho' = \Delta_D'' - \Delta_\rho''.$$

(This formula is given in [20] for forms of type $(0, q)$ but holds also for forms of any type.) It follows from this formula and Lemma 2:

Lemma 4. *A form η is harmonic if and only if either*

$$\Delta_D'\eta = \Delta_\rho''\eta = 0 \qquad \text{or} \qquad \Delta_D''\eta = \Delta_\rho'\eta = 0.$$

3.3. *Relations between d- and d''-cohomology groups.* We extend the representation ρ of $\mathfrak{g}$ onto $\mathfrak{g}^C$, and consider F as a $\mathfrak{g}^C$-module.

Lemma 5. *The irreducible $\mathfrak{g}^C$-module F is decomposed, as $\mathfrak{k}^C$-module, into the direct sum of $\mathfrak{k}^C$-submodules*:

$$F = S_1 + \cdots + S_m \tag{3.5}$$

with the following properties.

(1) *S_u and S_v $(u \neq v)$ are mutually orthogonal with respect to the hermitian inner product h.*

(2) *$\rho(X)S_t \subset S_{t-1}$ for all $X \in \mathfrak{n}^+$ and $\rho(Y)S_t \subset S_{t+1}$ for all $Y \in \mathfrak{n}^-$ $(t = 1, \cdots, m)$ where $S_0 = S_{m+1} = (0)$.*

(3) S_1(resp. S_m) *coincides with the subspace of F consisting of all $u \in F$ such that $\rho(X)u = 0$ for all $X \in \mathfrak{n}^+$*(resp. $X \in \mathfrak{n}^-$).

(4) S_1(resp. S_m) *is an irreducible $\mathfrak{k}^C$-submodule whose highest (resp. lowest) weight coincides with the corresponding one of ρ.*

We remark that if ρ is the adjoint representation of a simple Lie algebra $\mathfrak{g}$ the decomposition of this lemma is just given by (3.4).

Let $F = S_1 + \cdots + S_m$ be the decomposition (3.5), and let P_t be the projection of F onto S_t $(t = 1, \cdots, m)$. Then for a form $\eta \in A^r(\Gamma, X, \rho)$ we can define $P_t\eta$, η

being considered as an F-valued form on $\Gamma\backslash G$. Let $A^{p,q}(\Gamma, X, \rho)$ (resp. $A_t^{p,q}(\Gamma, X, \rho)$) be the subspace of $A^r(\Gamma, X, \rho)$ consisting of all forms of type (p, q)(resp. of type (p, q) and such that $P_t\eta = \eta$). Then $A^{p,q}(\Gamma, X, \rho) = \sum_{t=1}^m A_t^{p,q}(\Gamma, X, \rho)$ (direct sum). Moreover, it follows from Lemma 2 and (3.3) that Δ maps $A_t^{p,q}(\Gamma, X, \rho)$ into itself. Thus we get:

$$H^{p,q}(\Gamma, X, \rho) = \sum_t H_t^{p,q}(\Gamma, X, \rho),$$

where $H_t^{p,q}(\Gamma, X, \rho)$ is the subspace of $H^{p,q}(\Gamma, X, \rho)$ consisting of all d-cohomology classes representable by a d-closed form belonging to $A_t^{p,q}(\Gamma, X, \rho)$.

Let ρ_t be the representation of K into S_t induced by ρ, and consider the groups $H_{d''}^{p,q}(\Gamma, X, J_{\rho t})$ $(t = 1, \cdots, m)$. Working always on $\Gamma\backslash G$, we may identify $A_t^{p,q}(\Gamma, X, \rho)$ with $A^{p,q}(\Gamma, X, J_{\rho t})$ in view of (3.1). Because $d'' = D''$ on $A^{p,q}(\Gamma, X, J_{\rho t})$, we see that Δ_D'' on $A_t^{p,q}(\Gamma, X, \rho)$ corresponds to $\Box''$ on $A^{p,q}(\Gamma, X, J_{\rho t})$ under this identification. Thus, by Lemma 2, if $\eta \in A_t^{p,q}(\Gamma, X, \rho)$ is Δ-harmonic, η is $\Box''$-harmonic as element of $A^{p,q}(\Gamma, X, J_{\rho t})$. Therefore, there is a canonical injection

$$H_t^{p,q}(\Gamma, X, \rho) \to H_{d''}^{p,q}(\Gamma, X, J_{\rho t}).$$

Now take the case $p = 0$ or $q = 0$. By means of concrete expressions of Δ_ρ'', we can show the following results. If η is of type $(p, 0)$ (resp. $(0, q)$), then $\Delta_\rho''\eta = 0$ (resp. $\Delta_\rho'\eta = 0$) is equivalent to stating that η belongs to $A_m^{p,0}(\Gamma, X, \rho)$ (resp. to $A_1^{0,q}(\Gamma, X, \rho)$); moreover, $\Delta_D' = \Delta_D''$ on $A^{N,0}(\Gamma, X, \rho)$. Thus the above argument, combined with Lemma 4, implies:

THEOREM 4. *Notations being as above, we have canonical injections*

$$H^{p,0}(\Gamma, X, \rho) \to H_{d''}^{p,0}(\Gamma, X, J_{\rho m})$$

and

$$H^{0,q}(\Gamma, X, \rho) \to H_{d''}^{0,q}(\Gamma, X, J_{\rho 1}).$$

Moreover, these are subjective for $p = N$ and $q = 0, \cdots, N$ $(N = \dim_C X)$.

3.4. *Vanishing theorems.* We obtain the following vanishing theorems.

THEOREM 5. *Let Λ (resp. Λ') be the highest (resp. lowest) weight of ρ, and let q_ρ(resp. p_ρ) be the number of roots $\alpha \in \Psi$ such that $\langle\Lambda, \alpha\rangle > 0$ (resp. $\langle\Lambda', \alpha\rangle < 0$), where $\langle\ ,\ \rangle$ denotes the usual inner product among weights defined by the Killing form of $\mathfrak{g}^C$. Then*

$$H^{0,q}(\Gamma, X, \rho) = (0) \quad \text{for} \quad q = 0, 1, \cdots, q_\rho - 1,$$
$$H^{p,0}(\Gamma, X, \rho) = (0) \quad \text{for} \quad p = 0, 1, \cdots, p_\rho - 1.$$

COROLLARY 1. *Suppose that $\langle\Lambda, \gamma_i\rangle > 0$ for $i = 1, \cdots, s$, where $\gamma_1, \cdots, \gamma_s$ are the simple roots belonging to Ψ. Then $H^{0,q}(\Gamma, X, \rho) = (0)$ for $q < N = \dim_C X$.*

COROLLARY 2. *Let* $\mathfrak{g}^C$ *be simple and let* γ_1 *be the* (*unique*) *simple root of* $\mathfrak{g}^C$ *belonging to* Ψ. *Then* $H^{0,q}(\Gamma, X, \mathrm{ad}) = (0)$ *for* $q < 1/\langle\gamma_1, \gamma_1\rangle - 1$.

THEOREM 6. *The notation being as in Theorems* 4 *and* 5, $H^{0;q}_{d''}(\Gamma, X, J_{\rho_1}) = (0)$ *for* $q = 0, 1, \cdots, q_\rho - 1$. *If* $\langle\Lambda, \gamma_i\rangle > 0$ *for* $i = 1, \cdots, s$, *then* $H^{0;q}_{d''}(\Gamma, X, J_{\rho_1}) = (0)$ *for all* $q < N$.

COROLLARY (CALABI AND VESENTINI [6] AND BOKEL [3]). *Suppose that* $\mathfrak{g}^C$ *be simple. Then* $H^q(\Gamma\backslash X, \Omega^0(\Theta)) = (0)$ *for* $q < 1/\langle\gamma_1, \gamma_1\rangle - 1$.

THEOREM 7. *Suppose* $\mathfrak{g}^C$ *be simple. Let* Λ *be the highest weight of the representation* τ *of* $\mathfrak{k}$ *extended to* $\mathfrak{k}^C$. *We denote by* σ *the representation of K given by*

$$\sigma(t) = \det(\mathrm{ad}_-(t)) \qquad (t \in K),$$

by γ_1 *the simple root belonging to* Ψ *and by* β_0 *the highest root of* $\mathfrak{g}^C$. *Then*

(1) *if* $\langle\Lambda, \gamma_1\rangle > 0$, *then* $H^{0;q}_{d''}(\Gamma, X, J_\tau) = (0)$ *for* $q < N$.
(2) *if* $r > -2\langle\Lambda, \gamma_1\rangle$, *tgen* $H^{0;q}_{d''}(\Gamma, X, J\sigma^{-r} \otimes \tau) = (0)$ *for* $q < N$.
(3) *if* $\langle\Lambda, \beta_0\rangle < -\frac{1}{2}$, *then* $H^{0;q}_{d''}(\Gamma, X, J_\tau) = (0)$ *for* $q > 0$.

THEOREM 8. *Let* Λ *be the highest weight of* ρ. *If* $\langle\Lambda, \alpha\rangle > 0$ *for all positive root* α *of* $\mathfrak{g}^C$, *we have*

$$H^{p,q}(\Gamma, X, \rho) = (0)$$

for all p, q *such that* $p + q \neq N$.

Among these theorems, Theorems 5 and 8 are most important, and the other statements follow from Theorems 4 and 5. They are obtained by estimating minimal eigenvalues of certain laplacian operators. In more detail, at each point $x \in \Gamma\backslash G$, taking the value η_x of η, we get a mapping of $A^{p,q}(\Gamma, X, \rho)$ into the tensor product $F \otimes \Lambda^p \mathfrak{n}^- \otimes \Lambda^q \mathfrak{n}^+$. There exist degree-preserving operators L' and L'' in $F \otimes \Lambda\mathfrak{n}^- \otimes \Lambda\mathfrak{n}^+$ such that $(\Delta'_\rho\eta)_x = L'\eta_x$ and $(\Delta''_\rho\eta)_x = L''\eta_x$. Now, the operators L' and L'' are just the trivial extensions on $F \otimes \Lambda\mathfrak{n}^- \otimes \Lambda\mathfrak{n}^+$ of the operators Δ^+ in $F \otimes \Lambda\mathfrak{n}^-$ and Δ in $F \otimes \Lambda\mathfrak{n}^+$, which appeared in the work of Kostant [14]. If η is harmonic, we have $L'\eta_x = L''\eta_x = 0$ by Lemma 2. The proofs reduce then to know when Δ^+ and Δ^- are positive definite, and this is carried out using Kostant [14] (and Cartier [7]). We note that Theorem 5 can also be derived by an argument of Raghunathan's [22].

Theorem 8, combined with formulas of Hirzebruch [28], [29], implies the following

THEOREM 9. *Under the same assumptions as in Theorem* 8, *suppose that X be irreducible. Then,* $H^r(\Gamma, X, \rho) = (0)$ *for* $r \neq N$, *and*

$$\dim_C H^N(\Gamma, X, \rho) = \pi^{-N} \frac{\prod_{\alpha > 0} \langle\Lambda + \delta, \alpha\rangle}{\prod_{\alpha > 0; \alpha \notin \Psi} \langle\delta, \alpha\rangle} E(X_u)\mathfrak{v}(\Gamma\backslash X).$$

Here, δ is the one half of the sum of all positive roots, $E(X_u)$ is the Euler characteristic of the compact form X_u of X, and $\mathfrak{v}(\Gamma\backslash X)$ is the total volume of $\Gamma\backslash X$ measured by the volume element of $\Gamma\backslash X$ associated to the Bergmann metric on X.

Supplements. At this Summer Institute, the speaker has the opportunity to look at the Kuga's lecture note [30] as well as the Mountjoy's posthumous work [32]. Both of these give interesting applications of the d-cohomology groups; in particular, Mountjoy constructs generalized jacobian varieties attached to d-cohomology groups.

References

1. A. Andreotti and E. Vesentini, *On deformations of discontinuous groups*, Acta Math. **112** (1964), 249–298.

2. W. L. Baily, *The decomposition theorems for V-manifolds*, Amer. J. Math. **78** (1956), 862–888.

3. A. Borel, *On the curvature tensor of the hermitian symmetric manifolds*, Ann. of Math. (2) **71** (1960), 508–521.

4. ———, *Cohomologie et rigidité d'espaces compacts localement symétriques*, Sèminaire Bourbaki 16^e année, (1963/64), Exp. 265, Secrétariat mathèmatique, Paris, 1964.

5. E. Calabi, *On compact riemannian manifolds with constant curvature. I, Differential geometry*, Proc. Sympos. Pure Math. Vol. 3, Amer. Math. Soc., Providence, R.I., 1961, pp. 155–180.

6. E. Calabi and E. Vesentini, *On compact, locally symmetric Kähler manifolds*, Ann. of Math. (2) **71** (1960), 472–507.

7. P. Cartier, *Remarks on "Lie algebra cohomology and generalized Borel-Weil theorem" by B. Kostant*, Ann. of Math. (2) **74** (1961), 388–390.

8. M. Eichler, *Eine Verallgemeinerung der Abelschen Integrale*, Math. Z. **67** (1957), 267–298.

9. R. C. Gunning, *Homogenuous symplectic multipliers*, Illinois J. Math. **4** (1960), 575–583.

10. A. Fröhlicher and A. Nijenhuis, *A theorem of stability of complex structures*, Proc. Nat. Acad. Sci. U.S.A. **43** (1957), 239–241.

11. M. Ise, *Generalized automorphic forms and certain holomorphic vector bundles*, Amer. J. Math. **86** (1964), 70–108.

12. S. Kaneyuki and T. Nagano, *On the first Betti numbers of compact quotient spaces of complex semi-simple Lie groups by discrete subgroups*, Sci. Papers College Gen. Ed. Univ. Tokyo **12** (1962), 1–11.

13. ———, *On certain quadratic forms related to symmetric Riemannian spaces*, Osaka Math. J. **14** (1962), 241–252.

14. B. Kostant, *Lie algebra cohomology and generalized Borel-Weil theorem*, Ann. of Math. (2) **74** (1961), 329–387.

15. K. Kodaira and D. C. Spencer, *On deformations of complex analytic structures*. I, II, Ann. of Math. (2) **67** (1958), 328–401, 403–466.

16. Y. Matsushima, *On the first Betti number of compact quotient spaces of higher dimensional symmetric spaces*, Ann. of Math. (2) **75** (1962), 312–330.

17. ———, *On Betti numbers of compact, locally symmetric Riemannian manifolds*, Osaka Math. J. **14** (1962), 1–20.

18. ———, *A formula on the Betti numbers of locally symmetric Riemann manifolds* (to appear).

19. Y. Matsushima and S. Murakami, *On vector bundle valued harmonic forms and automorphic forms on symmetric Riemannian manifolds*, Ann. of Math. (2) **78** (1963), 365–416.

20. ———, *On certain cohomology groups attached to hermitian symmetric spaces*, Osaka J. Math. **2** (1965), 1–35.

21. Y. Matsushima and G. Shimura, *On the cohomology groups attached to certain vector valued differential forms on the product of the upper half planes*, Ann. of Math. (2) **78** (1963), 417–449.

22. M. S. Raghunathan, *On the first cohomology of discrete subgroups of semi-simple Lie groups*, Amer. J. Math. **78** (1965), 103–139.

23. A. Selberg, *On discontinuous groups in higher-dimensional symmetric spaces*, Contributions to Function Theory, International Colloquim on Function Theory (Bombay, 1960), pp. 147–164, Tata Institute of Fundamental Research, Bombay, 1960.

24. G. Shimura, *Sur les intégrales attachées aux formes automorphes*, J. Math. Soc. Japan **11** (1959), 291–311.

25. A. Weil, *On discrete subgroups of Lie groups*, Ann. of Math. (2) **72** (1960), 369–384.

26. ———, *On discrete subgroups of Lie groups.* II, Ann. of Maths. (2) **75** (1962), 578–602.

27. ———, *Remarks on the cohomology of groups*, Ann. of Math. (2) **80** (1964), 149–157.

28. F. Hirzebruch, *Characteristic numbers of homogeneous domains*, Seminars on Analytic Functions, vol. 2, Princeton, 1957, pp. 92–104.

29. ———, *Automorphic Formen und der Satz von Riemann-Roch*, Symposium internacional de Topologia Algebraica, Universidad Nacional Autónoma de México and UNESCO, Mexico City, 1958, pp. 129–144.

30. M. Kuga, *Fibre varieties over a symmetric space whose fibres are abelian varieties*, Lecture note at the University of Chicago, 1963–1964.

31. R. P. Langlands, *The dimension of spaces of automorphic forms*, Amer. J. Math. **85** (1963), 99–125.

32. R. H. Mountjoy, *Abelian varieties attached to representations of discontinuous groups*, Ph.D. Thesis, University of Chicago, Illinois, 1965.

33. A. Borel, *Introduction to automorphic forms*, Proc. Sympos. Pure Math. Vol. 9, Amer. Math. Soc., Providence, R.I., 1966; pp. 199–210.

On Deformations of Lattices in Lie Groups[1]

BY

HOWARD GARLAND

Throughout this discussion G will denote a connected Lie group and $\mathfrak{G}$ will denote the Lie algebra of G. We make the convention that the Lie algebra of a Lie group is the tangent space of the group at the identity.

DEFINITION 1. A subgroup $\Gamma \subset G$ is called a lattice, in case Γ is discrete and G/Γ is compact.

Γ will always denote a lattice. If $v \in G$ and $g \in G$, then $g \cdot v$ will denote $\operatorname{Ad} g(v)$. Let $H^1(\Gamma, \mathfrak{G})$ denote the first Eilenberg-MacLane group of Γ with respect to adjoint action; let $Z^1(\Gamma, \mathfrak{G})$ and $B^1(\Gamma, \mathfrak{G})$ denote the corresponding (inhomogeneous) cocycles and coboundaries, respectively; then

$$H^1(\Gamma, \mathfrak{G}) = Z^1(\Gamma, \mathfrak{G})/B^1(\Gamma, \mathfrak{G}),$$

where $Z^1(\Gamma, \mathfrak{G})$ is the set of all maps

$$f: \Gamma \to \mathfrak{G},$$

such that

$$f(\gamma_1\gamma_2) = \gamma_1 \cdot f(\gamma_2) + f(\gamma_1), \qquad \gamma_1, \gamma_2 \in \Gamma, \tag{1}$$

and $B^1(\Gamma, \mathfrak{G})$ is the set of all f in $Z^1(\Gamma, \mathfrak{G})$ such that for some $v \in \mathfrak{G}$

$$f(\gamma) = v - \gamma \cdot v, \qquad \gamma \in \Gamma. \tag{2}$$

Let $\mathscr{R}$ be the space of all homomorphisms of Γ into G and topologize $\mathscr{R}$ by pointwise convergence. Let $\iota: \Gamma \to G$ denote the inclusion map, so of course $\iota \in \mathscr{R}$. In a certain sense $Z^1(\Gamma, \mathfrak{G})$ is the tangent space to $\mathscr{R}$ at ι. Thus let r_t be a curve in $\mathscr{R}$, such that $r_0 = \iota$; (here t varies over an open interval containing 0). We assume that r_t is C^∞ in the sense that $r_t(\gamma)$ is a C^∞ curve in G for all γ in Γ. Let $r'(\gamma)$ denote the tangent vector to this curve at $t = 0$ (i.e. at γ). We can then define a map

$$f: \Gamma \to \mathfrak{G}$$

by

$$f(\gamma) = r'(\gamma)\gamma^{-1}, \qquad \gamma \in \Gamma; \tag{3}$$

[1] This research was partially supported by the National Science Foundation under contracts NSF-GP-1662 and NSF-G24154.

i.e., $f(\gamma)$ is the right translate of $r'(\gamma)$ by γ^{-1}. It is easy to verify that the f defined by (3) satisfies (1).

DEFINITION 2. Let r_t be a C^∞ curve in $\mathscr{R}$ such that $r_0 = \iota$. If we define $f: \Gamma \to \mathfrak{G}$ by (3), then $f \in Z^1(\Gamma, \mathfrak{G})$ and we call f the tangent to r_t (at ι).

It is important to point out that in general not every element in $Z^1(\Gamma, \mathfrak{G})$ is tangent to a curve of deformations. Later on, we will discuss this matter further.

Now let $\mathscr{R}^1 \subset \mathscr{R}$ be the subspace of all $r \in \mathscr{R}$ such that r is one-one and $r(\Gamma)$ is a lattice in G. Let $\mathscr{R}_0 \subset \mathscr{R}^1$ be the connected component of $\mathscr{R}^1$, containing ι. It is known that $\mathscr{R}_0$ is arcwise connected and thus the following definition is natural:

DEFINITION 3. $\mathscr{R}_0$ is called the space of deformations of Γ (in G).

The problem in which we are interested here is to describe $\mathscr{R}_0$. To start with, A. Weil has shown (see [5]) that $\mathscr{R}_0$ is an open subset of $\mathscr{R}$; thus locally we do not have to distinguish between these two spaces. Hence, keeping our earlier qualification in mind, we may think of $Z^1(\Gamma, \mathfrak{G})$ as a "tangent space" to $\mathscr{R}_0$ at ι.

We proceed to describe what is known about $\mathscr{R}_0$ in some special cases.

(i) If G is a semisimple group with no compact or three dimensional factors, A. Weil has shown that $\mathscr{R}_0$ is homeomorphic to G/Z, where Z is the centralizer of Γ in G. From this result and from known results on Fuchsian groups, Weil obtained a description of $\mathscr{R}_0$ even when G admits three dimensional factors. The essential point in the proof is to show that $H^1(\Gamma, \mathfrak{G}) = 0$ when G has no compact or three dimensional factors (see [6] and [7]).

(ii) If G is compact then Γ is finite so that $H^1(\Gamma, \mathfrak{G}) = 0$. It then follows from [7] that $\mathscr{R}_0$ is homeomorphic to G/Z.

(iii) When G is solvable and simply connected, H. C. Wang has obtained a complete description of $\mathscr{R}_0$. We shall give a more detailed account of this result later on, but for the moment let it suffice to say that $\mathscr{R}_0$ in this case is homeomorphic to a Lie group (see [4]).

At this point one might conclude that we are well on our way to obtaining a general description of $\mathscr{R}_0$; the obvious strategy is to try and glue the results in (i), (ii), and (iii) together, using the Levi decomposition. In fact, Wang did this for (i) and (iii) (see [4]). However, trouble develops when one tries to mix compact stuff in. For example, $\mathscr{R}_0$ admits a differentiable structure in each of the above cases; moreover, *this differentiable structure is in each case admissible, in the sense that if* r_t *is a smooth curve in* $\mathscr{R}_0$ *with respect to this structure, then* $r_t(\gamma)$ *is a smooth curve in* G, *for each* $\gamma \in \Gamma$. However, in general $\mathscr{R}_0$ does not have such a differentiable structure. On the other hand, we have

THEOREM 1. *If every element in* $Z^1(\Gamma, \mathfrak{G})$ *is tangent to a curve in* $\mathscr{R}_0$, *then in a neighborhood of* ι, $\mathscr{R}_0$ *has an admissible differentiable structure.*

P. A. Griffiths gave the first proof of this result. One can also obtain a proof by using the ideas in [7]. We remark that the converse of this theorem is not true.

Theorem 1, our previous remarks, and the known results in (i) and (ii) lead one to believe that cohomology theory is the natural tool for obtaining a general description of $\mathscr{R}_0$. To begin carrying out this idea I have rederived Wang's result in the solvable case, using cohomology theory; more specifically we have

THEOREM 2. *When G is solvable and simply connected, every element in $Z^1(\Gamma, \mathfrak{G})$ is tangent to a smooth curve r_t, in $\mathscr{R}_0$.*

Then from Theorem 1 and from the explicit construction of the curves r_t obtained in the proof of Theorem 2, one obtains the exact description of $\mathscr{R}_0$ given by Wang. Before giving this description we must introduce some notation.

Thus let G denote a solvable, simply connected Lie group and let $\mathfrak{N} \subset \mathfrak{G}$ denote the maximal nilpotent ideal; also, let $N \subset G$ denote the analytic subgroup corresponding to $\mathfrak{N}$. G. D. Mostow has proved the following (see [2]): $\Gamma \cap N = \Gamma_N$ is a lattice in N and ΓN is a closed subgroup of G with identity component N (it is not difficult to see that, Γ being a lattice, these two assertions are equivalent). A result of G. Hochschild (see [1]) implies that Aut(ΓN), the group of continuous automorphisms of ΓN, is a Lie group. We let A denote the identity component of Aut(ΓN).

THEOREM 3. *Let $\phi: A \to \mathscr{R}_0$ denote the restriction map. Then ϕ is a homeomorphism and the differentiable structure on A is admissible. Moreover, $\mathscr{R}_0 \subset \mathscr{R}$ is open.*

Theorem 3 follows from Theorem 2 and from the explicit construction of the curves r_t in the proof of Theorem 2. In particular, Theorem 2 implies that an appropriate C^∞ map is of maximal rank, and we then use the implicit function theorem to obtain the fact that $\mathscr{R}_0$ is an open subset of $\mathscr{R}$.

We now turn our attention to the proof of Theorem 2. The following result shows that $Z^1(\Gamma, \mathfrak{G})$ is small enough so that one can construct a curve r_t in $\mathscr{R}$, tangent to any given $f \in Z^1(\Gamma, \mathfrak{G})$.

THEOREM 4. *$f(\Gamma) \subset \mathfrak{N}$ for all $f \in Z^1(\Gamma, \mathfrak{G})$.*

One can derive Theorem 4 from

$$f(\Gamma_N) \subset \mathfrak{N}, \qquad \text{for all } f \in Z^1(\Gamma, \mathfrak{G}). \tag{4}$$

Let $H^1(\Gamma_N, \mathfrak{N})$ (respectively, $H^1(\Gamma_N, \mathfrak{G})$) denote the first Eilenberg-MacLane group of Γ_N with respect to adjoint action in $\mathfrak{N}$ (respectively, in $\mathfrak{G}$). Let $Z^1(\Gamma_N, \mathfrak{N})$ (respectively, $Z^1(\Gamma_N, \mathfrak{G})$) denote the corresponding (inhomogeneous) cocycles; then (4) is equivalent to the sequence

$$H^1(\Gamma_N, \mathfrak{N}) \to H^1(\Gamma_N, \mathfrak{G}) \to 0, \tag{5}$$

induced by the injection $\mathfrak{N} \to \mathfrak{G}$, being exact.

Let $H^1(\mathfrak{N}, \mathfrak{N})$ (respectively, $H^1(\mathfrak{N}, \mathfrak{G})$) denote the first Lie algebra cohomology group of $\mathfrak{N}$ with respect to adjoint action in $\mathfrak{N}$ (respectively, in $\mathfrak{G}$). Let $Z^1(\mathfrak{N}, \mathfrak{N})$ (respectively, $Z^1(\mathfrak{N}, \mathfrak{G})$) denote the corresponding cocycles. A result of van Est (see [3]) implies that the sequence (5) is exact if and only if the sequence

$$H^1(\mathfrak{N},\mathfrak{N}) \to H^1(\mathfrak{N},\mathfrak{G}) \to 0, \tag{6}$$

induced by the injection $\mathfrak{N} \to \mathfrak{G}$, is exact. In turn, (6) is exact if and only if

$$f(\mathfrak{N}) \subset \mathfrak{N}, \qquad \text{for all } f \in Z^1(\mathfrak{N},\mathfrak{G}). \tag{7}$$

For general solvable Lie algebras, (7) is not true. However, if G admits a lattice, then (7) is true. To be more precise we have to introduce the notion of a strongly unimodular, solvable Lie algebra. From now on $\mathfrak{G}$ will denote a solvable Lie algebra over a field F of characteristic zero. Let

$$\mathfrak{N}^1 = \mathfrak{N}, \mathfrak{N}^l = [\mathfrak{N}^{l-1},\mathfrak{N}], \qquad l > 1.$$

Let $V_l = \mathfrak{N}^l/\mathfrak{N}^{l+1}$ and let θ_l denote the representation of $\mathfrak{G}$ induced in V_l by adjoint action.

DEFINITION 4. The solvable Lie algebra, $\mathfrak{G}$, is said to be strongly unimodular in case trace $(\theta_l(r)) = 0$ for all $r \in \mathfrak{G}$ and $l > 0$.

If G is solvable and if it contains a lattice, then the Lie algebra of G can be shown to be strongly unimodular. Thus to prove Theorem 2 it suffices to prove

LEMMA 1. *If* $\mathfrak{G}$ *is strongly unimodular, then* (7) *holds.*

One can show that it suffices to prove Lemma 1 when F is algebraically closed; so we make this assumption. Moreover, we make the simplifying assumption that $\mathfrak{N}$ is abelian so that we have the representation

$$\theta_1 : \mathfrak{G} \to \operatorname{End} \mathfrak{N},$$

with $\mathfrak{N} = \text{kernel}\,\theta_1$. Hence $\theta_1(\mathfrak{G})$ is an abelian Lie algebra of endomorphisms of $\mathfrak{N}$. Since F is algebraically closed, we therefore have a weight space decomposition,

$$\mathfrak{N} = \bigoplus_{\lambda \in \Lambda} V_\lambda \qquad \text{(direct sum)}, \tag{8}$$

where Λ is a set of linear functionals on $\mathfrak{G}$, and each V_λ has a basis

$$\varepsilon_\lambda^1, \cdots, \varepsilon_\lambda^{p(\lambda)}$$

such that

$$\theta_1(x)\varepsilon_\lambda^i = \lambda(x)\varepsilon_\lambda^i + \sum_{j>i} a_j \varepsilon_\lambda^j, \tag{9}$$

where $x \in \mathfrak{G}$ and the a_j are elements in F depending on x.

Since $\mathfrak{N}$ is abelian, $Z^1(\mathfrak{N},\mathfrak{G})$ is the set of all linear maps $f: \mathfrak{N} \to \mathfrak{G}$ such that

$$[f(n), m] + [n, f(m)] = 0, \qquad n, m \in \mathfrak{N}. \tag{10}$$

Since f is linear, it suffices in order to prove (7), to prove

(11) for all $f \in Z^1(\mathfrak{N},\mathfrak{G})$, $\mu \in \Lambda$, $j = 1, \cdots, p(\mu)$, we have $f(\varepsilon_j^\mu) \in \mathfrak{N}$.

To prove (11) it suffices to prove that the $\theta_1(f(\varepsilon_j^\mu))$ are nilpotent; then from (8) and (9) it follows that in order to prove (11) it suffices to prove

(12) for all $f \in Z^1(\mathfrak{N}, \mathfrak{G})$, $\lambda, \mu \in \Lambda$, $j = 1, \cdots, p(\mu)$, we have $\lambda(f(\varepsilon_\mu^j)) = 0$.

From (10) we have

$$[f(\varepsilon_\lambda^i), \varepsilon_\mu^j] + [\varepsilon_\lambda^i, f(\varepsilon_\mu^j)] = 0.$$

From (9) we have that the first summand on the left is contained in V_μ and that the second summand equals

$$-\lambda(f(\varepsilon_\mu^j))\varepsilon_\lambda^i - \sum_{k>i} a_k \varepsilon_\lambda^k \in V_\lambda.$$

Thus, if $\mu \neq \lambda$ we obtain that this last expression is zero, since (8) is a direct sum. Since the ε_λ^k are linearly independent we thus have that $\lambda(f(\varepsilon_\mu^j)) = 0$, unless $\lambda = \mu$. But from (9) and our unimodularity assumption we have

$$0 = \operatorname{trace} \theta_1(f(\varepsilon_\mu^j)) = p(\mu)\mu(f(\varepsilon_\mu^j));$$

so $\mu(f(\varepsilon_\mu^j)) = 0$, since F has characteristic 0. This proves (12).

The proof of Lemma 1 when $\mathfrak{N}$ is not abelian does not seem to reduce to the case when $\mathfrak{N}$ is abelian. Roughly speaking, one develops a theory of weights for cocycles in $Z^1(\mathfrak{N}, \mathfrak{G})$ and then proves that when $\mathfrak{G}$ is strongly unimodular, this theory collapses; that is, one proves that (12) holds.

References

1. G. Hochschild, *The automorphism group of a Lie group*, Trans. Amer. Math. Soc. **72** (1952), 209–216.
2. G. D. Mostow, *Factor spaces of solvable groups*, Ann. of Math. (2) **60** (1954), 1–27.
3. ———, *Cohomology of topological groups and solvmanifolds*, Ann. of Math. (2) **73** (1961), 20–48.
4. H. C. Wang, *On the deformation of lattice in a Lie group*. I, Amer. J. Math. **85** (1963), 189–212.
5. A. Weil, *On discrete subgroups of Lie groups*, Ann. of Math. (2) **72** (1960), 369–384.
6. ———, *On discrete subgroups of Lie groups*. II, Ann. of Math. (2) **75** (1962), 578–602.
7. ———, *Remarks on the cohomology of groups*, Ann. of Math. (2) **80** (1964), 149–157.

On Deformations of Discrete Groups in the Noncompact Case[1]

BY

HOWARD GARLAND

1. **Introduction.** Throughout this talk we make the following assumptions and notational conventions:

(*) G is a semisimple, connected Lie group with no compact or three dimensional factors. $\Gamma \subset G$ is a finitely generated, discrete subgroup such that G/Γ has finite invariant volume.

Let $\mathscr{R}$ be the space of all one-one homomorphisms

$$r : \Gamma \to G$$

such that $r(\Gamma)$ is a discrete subgroup of G and $G/r(\Gamma)$ has finite invariant volume. We topologize $\mathscr{R}$ by pointwise convergence. Let δ be a positive real number and let $I = (-\delta, \delta)$ denote the open interval of radius δ about zero; let t vary over I and let r_t be a C^∞ curve in $\mathscr{R}$ (i.e. $r_t(\gamma)$ is a C^∞ curve in G for all γ in Γ) such that $r_0 = \iota$, the inclusion map.

CONJECTURE (SELBERG). There is a C^∞ curve c_t in G such that for all γ in Γ, t in I, we have $r_t(\gamma) = c_t \gamma c_t^{-1}$.

Let $\mathfrak{G}$ denote the Lie algebra of G and let $\mathfrak{G} = \mathfrak{K} + \mathfrak{P}$ be a Cartan decomposition of $\mathfrak{G}$; let $K \subset G$ be the analytic subgroup corresponding to $\mathfrak{K}$ and assume G is chosen so that K is compact (this being an assumption of convenience); then $K\backslash G$ is a Riemannian symmetric space and in certain cases, a Hermitian symmetric space. For the moment, assume we are in the latter case and that Γ has no elements of finite order; then $K\backslash G/\Gamma$ has a complex structure induced from that on $K\backslash G$ and speaking loosely, r_t may be thought of as giving a deformation of this complex structure (there is a point of difficulty here which we will discuss later). The thrust of the argument in [3] is to show that if this deformation of the complex structure satisfies a certain boundary condition at ∞, then it is trivial. It then follows that the deformation r_t of Γ is itself trivial in the sense of the above conjecture.

To free ourselves from the restriction that $K\backslash G$ be Hermitian symmetric we will reformulate the proof in [3]; rather than consider deformations of the complex structure on $K\backslash G/\Gamma$ we will consider deformations of the Riemannian structure. More exactly, one considers deformations of the Riemannian structure

[1] This research was partially supported by the U.S. Army Research Office, Durham.

on $K\backslash G/\Gamma$ coming from a deformation r_t of Γ, and satisfying a boundary condition at ∞ analogous to that considered in [3] in the complex case.

Our approach has certain advantages and disadvantages. First we obtain results for the non-Hermitian case, and even in the Hermitian case we do not have to make the assumption in [3] that $K\backslash G/\Gamma$ is strongly pseudoconcave. The disadvantage is that our boundary condition, rigidity at ∞ in the Riemannian sense, is stronger than the corresponding boundary condition in the complex sense. Thus our result does not imply the result in [3]. Nevertheless, there is reason to believe (reason based on some conjectures) that our cohomological results will allow us to relax these boundary conditions.[2]

S. Murakami has observed that the methods described here probably have some application in the complex case. The approach taken in this talk is based extensively on the material in [6].

2. **Preliminaries.** Rather than work directly with the Riemannian structure on $K\backslash G$ we follow *A*. Weil (see [6]) and work with a parallelism structure on G. Thus let $\mathfrak{G}$, the Lie algebra of G, be identified with the right invariant vector fields on G; let $X_1, \cdots, X_n$ be a basis of $\mathfrak{G}$ so that $X_1, \cdots, X_r$ span $\mathfrak{P}$ and $X_{r+1}, \cdots, X_n$ span $\mathfrak{K}$. We let Greek indices λ, μ, ν, range from 1 to n, Greek indices α, β, γ, range from $r + 1$ to n, and Latin indices i, j, k, range from 1 to r. We choose a basis $\omega^1, \cdots, \omega^n$ of right invariant one-forms so that

$$\langle \omega^\lambda, X_\mu \rangle = \delta^\lambda_\mu, \qquad \lambda, \mu = 1, \cdots, n.$$

We define structural constants $C^\lambda_{\mu\nu}$ by

$$d\omega^\lambda = -\tfrac{1}{2} C^\lambda_{\mu\nu} \omega^\mu \wedge \omega^\nu, \qquad \lambda, \mu, \nu = 1, \cdots, n, \tag{1}$$

where $C^\lambda_{\mu\nu} = -C^\lambda_{\nu\mu}$ and d is the exterior differentiation operator.

DEFINITION 1. An n-dimensional C^∞ manifold U together with n C^∞ everywhere independent one-forms $\omega^1, \cdots, \omega^n$ satisfying (1), is called a G-manifold; we will say that U has G-structure given by $\omega^1, \cdots, \omega^n$.

DEFINITION 2. If U_1 and U_2 are G-manifolds and if $\phi\colon U_1 \to U_2$ is a C^∞ map, then ϕ is called a G-map in case

$$\phi^* \omega^\lambda = \omega^\lambda, \qquad \lambda = 1, \cdots, n,$$

where ϕ^* is the map of forms induced by ϕ.

We note in passing that $\omega^1, \cdots, \omega^n$ (respectively, $X_1, \cdots, X_n$) induce vector fields (respectively, forms) on G/Γ which we again denote by $X_1, \cdots, X_n$ (respectively, $\omega^1, \cdots, \omega^n$).

3. **Deformations of G-structures.** Let M be a simply connected C^∞ manifold and let $t \to r_t$ be a C^∞ map from M to $\mathscr{R}$; we choose a base point $o \in M$ and assume $r_o = \iota$. We define an action of Γ on $G \times M$ by

$$(g, t)\gamma = (gr_t(\gamma), t), \qquad t \in M, \gamma \in \Gamma, g \in G. \tag{2}$$

[2] See footnote 3, at the bottom of page 408.

We then set $\mathfrak{B} = G \times M/\Gamma$ and let $\pi\colon G \times M \to \mathfrak{B}$ denote the projection. We would like to conclude that $\mathfrak{B}$ is a C^∞ manifold and that π is a covering map. This is not immediately clear from our assumption (a proof in the compact case was given in [5]), and thus *we assume r_t is admissible in the sense that $\mathfrak{B}$ is a C^∞ manifold and π is a covering map.*

Since the coordinate projection $\mathrm{pr}_2\colon G \times M \to M$ commutes with the action of Γ in (2), we have an induced C^∞ map $\varpi\colon \mathfrak{B} \to M$ of maximal rank, such that the diagram

$$\begin{tikzcd}
G \times M \arrow[r, "\mathrm{pr}_2"] \arrow[d, "\pi"'] & M \\
\mathfrak{B} \arrow[ur, "\varpi"'] &
\end{tikzcd}$$

is commutative. Now $\varpi^{-1}(t)$ may be identified with G/Γ_t where $r_t(\Gamma) = \Gamma_t$. On each G/Γ_t we have an induced G-structure from G, so that we may think of $(\mathfrak{B}, M, \varpi, \pi, o)$ as a deformation of the G-structure on G/Γ given by the parallelism $\omega^1, \cdots, \omega^n$.

DEFINITION 3. A deformation of the G-structure on G/Γ given by $\omega^1, \cdots, \omega^n$ is the data $(\mathfrak{B}, M, \varpi, \pi, o)$ given above.

DEFINITION 4. Let $A \subset G/\Gamma$ be an open subset; then the deformation $(\mathfrak{B}, M, \varpi, \pi, o)$ is C^k A-trivial in case we have a C^k map

$$\phi\colon A \times M \to \mathfrak{B}$$

such that the diagram

$$\begin{tikzcd}
A \times M \arrow[r, "\mathrm{pr}_2"] \arrow[d, "\phi"'] & M \\
\mathfrak{B} \arrow[ur, "\varpi"'] &
\end{tikzcd}$$

is commutative, for each $t \in M$ $\phi\colon A \times t \to \varpi^{-1}(t)$ is a G-map, and $\phi|(A \times o)$, the restriction of ϕ to $A \times o$, is the inclusion map.

If we can find such a ϕ after replacing M by an open neighborhood of o, we say the deformation is locally C^k A-trivial. If we can take $A = G/\Gamma$ and $k = \infty$, we say the deformation is trivial. If the deformation is C^k A-trivial for every relatively compact $A \subset G/\Gamma$, we say the deformation is C^k pseudo-trivial.

DEFINITION 5. We will say that $(\mathfrak{B}, M, \varpi, \pi, o)$ is rigid at ∞ in case we can find a compact set $C \subset G/\Gamma$ and a C^∞ diffeomorphism

$$\phi\colon (G/\Gamma - C) \times M \to \mathfrak{B},$$

onto an open subset of $\mathfrak{B}$, such that the diagram

$$\begin{tikzcd}
(G/\Gamma - C) \times M \arrow[rr, "\phi"] \arrow[dr, "\mathrm{pr}_2"'] & & \mathfrak{B} \arrow[dl, "\varpi"] \\
& M &
\end{tikzcd}$$

is commutative; $\varpi|(\mathfrak{B} -$ Image $\phi)$, the restriction of ϖ to $\mathfrak{B} -$ Image ϕ, is proper; $\phi\colon (G/\Gamma - C) \times t \to \varpi^{-1}(t)$ is a G-map, and ϕ restricted to $(G/\Gamma - C) \times o$ is the inclusion map.

We remark that one can introduce the notions of locally trivial, locally rigid at ∞, etc., in the usual manner of deformation theory.

Theorem. *Let G be a semisimple, connected Lie group with no compact or three-dimensional factors. Let $\Gamma \subset G$ be a finitely generated, discrete subgroup such that G/Γ has finite invariant volume. If the deformation $(\mathfrak{B}, M, \varpi, \pi, o)$ is rigid at ∞, it is trivial.*[3]

In the remainder of this paper, we will sketch the proof of this theorem. Since our object is to prove that certain deformations are trivial, one can prove that it suffices to assume M is an open interval $I = (-\delta, \delta)$. If one can prove local triviality in this case, then one can prove rigidity whenever M is simply connected. Hence from now on we assume that M is such an interval and whenever necessary we will shrink δ. We now assume that $r_0 = \iota$; that is, we take 0 for our distinguished point o. We will need

Proposition 1. *If $(\mathfrak{B}, M, \varpi, \pi, 0)$ is C^k pseudotrivial then it is trivial.*

Proof. We can find an open, relatively compact subset $A \subset G/\Gamma$ such that A', the inverse image of A under the projection $P\colon G \to G/\Gamma$, is connected. L. Greenberg has shown that one can find such an A, provided Γ is finitely generated. Since we are assuming the deformation is C^k pseudo-trivial we have a homotopy of maps,

$$\phi_t\colon A \to \mathfrak{B}, \qquad t \in M,$$

where $\phi_t(A) \subset \varpi^{-1}(t)$, and $\phi_t\colon A \to \varpi^{-1}(t)$ is a G-map. By the homotopy lifting theorem, we have a homotopy of G-maps

$$\phi_t'\colon A' \to G$$

which covers ϕ_t and such that ϕ_0 is the inclusion map. Since A' is connected ϕ_t' must coincide with a right translation by an element a_t in G. One can then easily see that

$$r_t(\gamma) = a_t^{-1}\gamma a_t, \qquad \gamma \in \Gamma,\ t \in M.$$

[3] We have recently strengthened this result, as follows: We need no longer assume Γ is finitely generated, and we can relax the boundary condition, rigidity at ∞, to the condition that with respect to an invariant measure on G/Γ_t, the $f_\chi'^{\mu}$ are square integrable (the $f_\chi'^{\mu}$ are defined after (8), below).

With some further argument one can show that the a_t's can be chosen so that $t \to a_t$ is a C^∞ map. It then follows that $(\mathfrak{B}, M, \varpi, \pi, 0)$ is trivial. Q.E.D.

The vector fields X_λ on G are right invariant and hence induce vector fields (again denoted by X_λ) on $\mathfrak{B}$. Similarly the ω^λ on G induce forms (again denoted by ω^λ) on $\mathfrak{B}$. Assume we could construct a C^k vector field Y on $\mathfrak{B}$ such that

$$\varpi_*(Y) = \partial/\partial t, \tag{3}$$

(where ϖ_* is the map on vector fields induced by ϖ, and where $\partial/\partial t$ is the vector field on the interval M corresponding to the parameter t), and such that on each fiber Y is a C^∞ vector field with all derivatives along the fibers being C^k on $\mathfrak{B}$, and finally such that

$$[X_\lambda, Y] = 0, \qquad \lambda = 1, \cdots, n. \tag{4}$$

Then from (3), (4), and the theory of ordinary differential equations we have that whenever $A \subset G/\Gamma$ is a relatively compact set we can find t_A such that $0 < t_A < \delta$, and a one-parameter family of maps

$$\phi_t : A \to \mathfrak{B}, \qquad |t| < t_A,$$

such that

$$\phi_t(A) \subset G/\Gamma_t,$$

ϕ_t is a G-map, and ϕ_t is jointly C^{k+1} in t and the A-variables. Thus we obtain C^{k+1} pseudo-triviality of the deformation $(\mathfrak{B}, M, \varpi, \pi, 0)$ (where we shrink δ if necessary). Hence from Proposition 1 we obtain triviality.

Thus the proof of the theorem is reduced to finding a continuous vector field Y on $\mathfrak{B}$ such that Y is C^∞ along the fibers, such that all the derivatives of Y along the fibers are continuous on $\mathfrak{B}$, and such that Y satisfies (3) *and* (4).

From the assumption that the deformation is rigid at ∞ one can prove the following:

(5) (Shrinking δ if necessary), we can find an open subset $U \subset \mathfrak{B}$ such that $\varpi|\bar{U}$ is proper, and we can find a C^∞ vector field Y on $\mathfrak{B}$ such that Y satisfies (3) and such that Y satisfies (4) on $\mathfrak{B} - \bar{U}$. Integrating by K we can assume Y is K-invariant (G acts to the left in $\mathfrak{B}$).

4. **Cohomology.** Let Y be any C^∞ vector field on $\mathfrak{B}$ satisfying (3) and define the C^∞ functions f^μ_λ on $\mathfrak{B}$ by

$$[X_\lambda, Y] = \sum_\mu f^\mu_\lambda X_\mu; \tag{6}$$

this makes sense since $\varpi_*([X_\lambda, Y]) = 0$.

From now on we will use the Eisenstein summation convention. From the Jacobi identity we have

$$(X_\mu f^\nu_\lambda - X_\lambda f^\nu_\mu) = C^\nu_{\lambda\rho} f^\rho_\mu + C^\rho_{\mu\lambda} f^\nu_\rho - f^\rho_\lambda C^\nu_{\mu\rho}. \tag{7}$$

On the other hand let Y' be a second C^∞ vector field on $\mathfrak{B}$ satisfying (3). Then $Y' - Y$ is a vertical vector field ($\varpi_*(Y' - Y) = 0$), and thus can be expressed as a linear combination of the X_λ; that is, we have

$$Y' = Y + \phi^\mu X_\mu,$$

where the ϕ^μ are C^∞ functions on $\mathfrak{B}$.

A direct computation yields

$$f'^\mu_\lambda = f^\mu_\lambda + (X_\lambda \phi^\mu) + \phi^\rho C^\mu_{\lambda\rho},$$

where the f'^μ_λ are defined as in (6), but using Y' instead of Y. *From now on we assume that Y is K-invariant* so we have

$$[X_\alpha, Y] = 0, \qquad \alpha = r + 1, \cdots, n. \tag{8}$$

Hence the f^λ_α are all zero. Moreover, for each $t \in M$ let f'^μ_λ denote the restriction of f^μ_λ to $\varpi^{-1}(t)$; then let

$$\Omega_t = f'^\mu_\lambda X_\mu \otimes \omega^\lambda.$$

One can show that $\theta(X_\alpha)\Omega_t$, the Lie derivative of Ω_t with respect to X_α, is zero. Thus using S. Murakami's notation in [4], one may identify Ω_t with an element of $A^1(\Gamma_t, X, \mathrm{ad})$ (one should note, however, that we have interchanged left and right; that is, for us K acts on the left and Γ on the right, while in [4] it is the other way around). From now on we will make free use of the material and notation introduced in [4]. Thus letting d denote the coboundary operator on the complex

$$A(\Gamma_t, X, \mathrm{ad}) = \sum A^q(\Gamma_t, X, \mathrm{ad}) \text{ (direct sum)},$$

we have that equation (7) just expresses the fact that for each $t \in M$

$$d\Omega_t = 0. \tag{9}$$

Using a suitable metric on $\mathfrak{G}$ and a suitable complete Riemannian metric on G one can introduce a positive definite inner product (,) on $A_c = A_c(\Gamma_t, X, \mathrm{ad})$, the set of all forms in $A(\Gamma_t, X, \mathrm{ad})$ with compact support. On $A(\Gamma_t, X, \mathrm{ad})$ one can now introduce a coboundary operator δ and then the Laplacian $\Delta = d\delta + \delta d$. These operators have decompositions

$$d = D + d_{\mathrm{ad}},$$

$$\delta = D_* + \delta_{\mathrm{ad}},$$

$$\Delta = \Delta_D + \Delta_{\mathrm{ad}},$$

where $\Delta_D = DD_* + D_*D$, $\Delta_{\mathrm{ad}} = d_{\mathrm{ad}}\delta_{\mathrm{ad}} + \delta_{\mathrm{ad}}d_{\mathrm{ad}}$. Restricted to A_c, d and δ are adjoints of each other and likewise D and d_{ad} are adjoints of D_* and δ_{ad}, respectively. Now if $\Lambda \in A_c$

$$(\Delta\Lambda, \Lambda) = (\Delta_D\Lambda, \Lambda) + (\Delta_{\mathrm{ad}}\Lambda, \Lambda),$$

where by our above remarks

$$(\Delta_D\Lambda, \Lambda) = (D\Lambda, D\Lambda) + (D_*\Lambda, D_*\Lambda) \geqq 0,$$

so we obtain an inequality

$$(\Delta\Lambda, \Lambda) \geqq (\Delta_{\mathrm{ad}}\Lambda, \Lambda).$$

For $\Lambda \in A_c$, let $\|\Lambda\|^2 = (\Lambda, \Lambda)$. Then $(\Delta\Lambda, \Lambda) = \|d\Lambda\|^2 + \|\delta\Lambda\|^2$, and using the computation in [6], one can find a constant $b > 0$ such that for all Λ in $A^1(\Gamma_t, X, \mathrm{ad})$

$$(\Delta_{\mathrm{ad}}\Lambda, \Lambda) \geqq b\|\Lambda\|^2.$$

Combining this with the previous inequalities, we obtain the inequality

$$\text{(10)} \qquad b\|\Lambda\|^2 \leqq \|d\Lambda\|^2 + \|\delta\Lambda\|^2, \qquad \Lambda \in A_c^1(\Gamma_t, X, \mathrm{ad}),$$

where b does not depend on Λ.

Now given any locally constant vector bundle E on a C^∞ manifold N with Riemannian metric ds^2, we can define cohomology on N with coefficients in the sheaf of germs of locally constant sections of E. Then we can resolve by differential forms with values in the sections of E, and by means of a metric on the fibers of E, introduce harmonic analysis. Let d and δ denote the corresponding boundary and coboundary operators, respectively.

Definition 6. We say E is W^q-elliptic with respect to ds^2, if we can find a metric on E and $b > 0$ such that whenever Λ is a $C^\infty q$-form on N with values in the sections of E, and with compact support, we have the inequality

$$b\|\Lambda\|^2 \leqq \|d\Lambda\|^2 + \|\delta\Lambda\|^2.$$

Thus by (10), we have W^1-ellipticity in our situation (strictly speaking, we are working with the locally constant vector bundle on $K\backslash G/\Gamma_t$ built out of Killing vector fields on that space).

When $(ds)^2$ is complete, then we have in analogy with the theory of holomorphic vector bundles (see [2] and [3]).

Lemma 1. *If E is W^q-elliptic with respect to the complete metric ds^2, if Λ is a square integrable, C^∞ q-form with values in the sections of E, and if $d\Lambda = 0$, then we can find a C^∞ $(q - 1)$-form Φ with values in the sections of E, such that $d\Phi = \Lambda$. Moreover, Φ may be chosen in a canonical manner, once given the metric on the fibers of E.*

Now choosing Y as in (5) we may assume Ω_t has compact support for all t in M. By Lemma 1 we have a canonical Φ_t in $A^0(\Gamma_t, X, \mathrm{ad})$ such that $d\Phi_t = \Omega_t$ (in our case Φ_t is unique by Borel's density theorem). Moreover, in analogy with the results in [3] we have

Lemma 2. *Φ_t, together with all its derivatives in the direction of the fibers, is jointly continuous in t and in the fiber variables on $\mathfrak{B}$.*

For fixed t, Φ_t is a vector field on G/Γ_t. Thus, letting t vary, Lemma 2 implies that Φ_t is a continuous, vertical vector field on $\mathfrak{B}(\varpi_*(\Phi_t) = 0)$ which is C^∞ along the fibers. The fact that for each fixed t in M

$$d\Phi_t = \Omega_t,$$

implies that the vector field $Y - \Phi_t$ on $\mathfrak{B}$ satisfies (3) and (4). Thus, using our previous observation, we see that Lemmas 1 and 2 imply the theorem.

References

1. A. Andreotti and E. Vesentini, *Les théorèmes fondamentaux de la théorie des espaces holomorphiquement complets.* Topologie et géométrie différentielle, Vol. IV, Seminaire C. Ehresmann (1962–1963), Institut H. Poincaré, Paris, 1963.

2. ———, *Carleman estimates for the Laplace-Beltrami equation on complex manifolds,* Inst. Hautes Études Sci. Publ. Math. No. 25 (1965), 81–130.

3. ———, *On deformations of discontinuous groups,* Acta Math. **112** (1964), 249–298.

4. S. Murakami, *Cohomologies of vector-valued forms on compact, locally symmetric Riemannian manifolds,* Proc. Sympos. Pure Math. Vol. 9, Amer. Math. Soc., Providence, R.I., 1966; pp. 387–399.

5. A. Weil, *On discrete subgroups of Lie groups,* Ann. of Math. (2) **72** (1960), 369–384.

6. ———, *On discrete subgroups of Lie groups.* II, Ann. of Math. (2) **75** (1962), 578–602.

On the Conjugacy of Subgroups of Semisimple Groups

BY

G. D. MOSTOW*

1. We sketch here a proof of a theorem which may be regarded as an intermediate result on the problem of rigidity of subgroups of semisimple groups.

Let G be a connected semisimple real Lie group having no compact normal subgroup of positive dimension. Let ρ be a faithful representation of G such that $\rho(K)$ consists of unitary matrices, K being a maximal compact subgroup of G. Then the map

$$g \rightarrow \rho(g)^t\overline{\rho(g)}$$

defines a map of the symmetric space $X = G/K$ into the real linear space S of hermitian matrices, and accordingly one gets an embedding of X into the real projective space P associated with S. The topological closure $\bar{X}$ of X in P is the Satake ρ-compactification of G/K.

THEOREM. *Let Γ and Γ' be closed subgroups of G with G/Γ and G/Γ' having finite invariant measure. Let $\theta : \Gamma \rightarrow \Gamma'$ be an isomorphism and $\phi : \bar{X} \rightarrow \bar{X}$ be a diffeomorphism such that*

$$\phi(\gamma x) = \theta(\gamma)\phi(x) \quad \textit{for all} \quad \gamma \in \Gamma, x \in \bar{X}.$$

Then θ is the restriction to Γ of an automorphism of G.

Our proof of the above theorem rests heavily on some facts about restricted root systems whose proofs entail case-by case checking of diagrams, which regrettably I have not been able to avoid. I take this opportunity to express my appreciation to N. Iwahori and T. Tamagawa with whom I have had helpful conversations.

2. Let G' be a semisimple algebraic linear group defined over the field $\boldsymbol{R}$ of real numbers, let T^* be a maximal $\boldsymbol{R}$-split torus in G' and let T be a maximal torus defined over $\boldsymbol{R}$ and containing T^*. Let Φ denote the set of roots on T and Φ^* the set of restricted roots on T^*. Let Δ^* denote a fundamental system in Φ^* and let Δ denote a fundamental system in Φ which restricts to Δ^*. Let Φ_+ and Φ^*_+ denote the positive roots in Φ and Φ^* with respect to Δ and Δ^* respectively. Let Φ^+ denote the roots in Φ which restrict to elements in Φ^*_+.

For any Lie group F we denote by F^0 the topologically connected component of the identity in F, and by $\dot{F}$ the Lie algebra of F. $Z(\ )$ denotes the centralizer of $(\ )$.

* Supported in part by NSF GP4288.

Write $G = (G'_{\boldsymbol{R}})^0$, $H = (T_{\boldsymbol{R}})^0$, and $A = (T^*_{\boldsymbol{R}})^0$. We have $Z(T^*) = L \cdot T^*$ where L is $\boldsymbol{R}$-anisotropic; that is $L_{\boldsymbol{R}}$ is compact. Set $M = L \cap G$. Write $g[x] = gxg^{-1}$ for $g, x \in G$.

Given any semisimple automorphism x of a complex linear space, one can write x uniquely in the form $x = x_M \cdot x_A$ where x_A and x_M are commuting semisimple elements whose eigenvalues are positive real and of modulus one respectively. We call x_A the *modulus* of x. Any algebraic group containing x contains x_M and x_A.

A semisimple element $x \in G$ is called $\boldsymbol{R}$-regular if and only if

$$\dim Z(x_A) \cap G \leqq \dim Z(y_A) \cap G$$

for all $y \in G$. One sees readily that a semisimple element is $\boldsymbol{R}$-regular if and only if it is conjugate to an element in MA^1 where A^1 denotes the subset of elements in A such that $\alpha(x) > 1$ for all $\alpha \in \Delta^*$.

THEOREM 1. *Let x be a semisimple $\boldsymbol{R}$-regular element of G. Then for any $y \in G$, $x^n y$ is a semisimple $\boldsymbol{R}$-regular element for all large n.*

COROLLARY 1. *Let Γ be a closed subgroup such that G/Γ has finite invariant measure. Then $G[\Gamma] \cap H$ is Zariski-dense in H.*

COROLLARY 2. *Let S be a proper Zariski-closed subset of H. Given $\gamma \in \Gamma$, there is an element $\gamma_1 \in G[H - S]$ such that $\gamma\gamma_1^n \in G[H - S]$ for all positive n.*

3. The central algebraic fact underlying our main theorem is the following

THEOREM 2. *Let t be an automorphism of T which stabilizes T^* and Φ^+. Then t stabilizes Φ.*

What must be shown is that t stabilizes $\Phi - (\pm\Phi^+)$; that is, the roots occurring in $Z(T^*)$. Our proof consists of deducing from the fact that $Z(T^*)$ has a special structure that t preserves the Killing form of G.

In greater detail, we can reduce Theorem 2 to the case that G' is simple after showing

(1) Any automorphism of a connected $\boldsymbol{R}$-restricted diagram Δ^* can be lifted to an automorphism of Δ;

(2) Given two $\boldsymbol{R}$-simple groups G_1 and G_2, let $t: T_1 \to T_2$ be an isomorphism sending T_1^* to T_2^* and Φ_1^+ to Φ_2^+. Then G_1 and G_2 are isomorphic and t can be induced by an isomorphism of G_1 to G_2.

For the case that G' is a simple group, one proves:

(3) Let W^A denote the stabilizer of T^* in the Weyl group of T, and let L denote the commutator subgroup of the connected component of the identity in $Z(T^*)$. Then $\dot{T} \cap \dot{L}$ is a direct sum of at most two irreducible subspaces of W^A. If $\dot{T} \cap \dot{L} = \dot{T}_1 + \dot{T}_2$ is the decomposition of $\dot{T} \cap \dot{L}$ into W^A irreducible subspaces, then $\dot{L} = \dot{L}_1 + \dot{L}_2$ with $\dot{L}_i \cap \dot{T} = \dot{T}_i$, and $\dot{L}_1$ simple and isomorphic to no ideal of $\dot{L}_2$.

My proof for each of these facts involves diagram checking.

Let B and B^0 denote the Killing forms of G and $Z(T^*)$ respectively. Set $B' = \sum \alpha^2$ ($\alpha \in \Phi^+$). Then $B = 2B' + B^0$. We have

$$\dot{T} = \dot{T}_1 + \dot{T}_2 + (Z(\dot{L}) \cap \dot{T}) \qquad \text{(direct)}.$$

These summands are orthogonal with respect to both B^0 and B', hence with respect to B'. Moreover, B' is proportional to B on each of the above three summands. Since t preserves B', it must therefore preserve B.

The Weyl reflections generated by the roots in Φ^+ generate the Weyl group W and hence t stabilizes W. Since any reflection in W is the reflection of a root in Φ, it follows that t stabilizes Φ.

4. The Satake ρ-compactification may be described as follows. Let Δ_ρ^* denote the subset of Δ^* consisting of all $\alpha \in \Delta^*$ satisfying:

If $\rho = \rho^1 + \cdots + \rho^n$ is the decomposition of ρ into irreducible components and μ^i is the highest restricted weight of ρ^i, then $\mu^i - \alpha$ is a restricted weight of ρ^i for some i.

Set $E_\rho = \Delta^* - \Delta_\rho^*$, the complement of Δ_ρ^* in Δ^*. Then

$$x \to \rho(x)^t\overline{\rho(x)}$$

defines a faithful embedding of X if and only if E_ρ contains no connected component of Δ^*. The Killing form induces an inner product on Φ^* and we can describe E_ρ as the set of elements in Δ^* which are orthogonal to the highest restricted weights $\mu^1, \cdots, \mu^n$.

Any subset E_0 of Δ^* containing no connected component of Δ^* has the form E_ρ for some ρ defining a faithful embedding of X. Such a subset E_0 is called *faithful.*

Let E_0 be a faithful subset of Δ^*. A subset E of Δ^* is called E_0-reduced if E_0 contains no connected components of E; if ρ is irreducible, this is equivalent to the condition that $E \cup \{\mu_\rho\}$ is connected where μ_ρ is the highest restricted weight of ρ. (This is what Satake calls ρ-open in [2] and Moore called E_0-connected in [1].) For any E_0-reduced set E, we put

$E^+ = E \cup$ all components in E_0 not connected to E. For any subset $E \subset \Delta^*$, let $N(E)$ denote the unipotent subgroup whose Lie algebra is $\sum_\alpha \dot{G}_\alpha$ ($\alpha > 0$, $\alpha \notin \{E\}$) the linear span of E being denoted by $\{E\}$. Let $P(E)$ denote the normalizer of $N(E)$ in G, and let $G(E)$ denote the analytic subgroup whose Lie algebra is the commutator subalgebra of $\sum_\alpha \dot{G}_\alpha$ ($\alpha \in \{E\}$). Let $R(E)$ denote the radical of $P(E)^0$. Then $P(E)$ contains $Z(A)$ and $P(E) = G(E) \cdot R(E) \cdot Z$ where Z is the finite group $T^* \cap M$. Let $K(E)$ denote a maximal compact subgroup of $G(E)$. Set

$$X(E) = G(E)/K(E).$$

The boundary $\bar{X} - X$ of the Satake compactification is a finite union of G-orbits each of the form $G \times_{P(E^+)} X(E)$, where the sets E range over all the E_0-reduced subsets. The topology on $\bar{X}$ is such that the subset $X(E)$ has in its closure the subsets $X(E_1)$ with $E_1 \subset E$. The subgroup $P(E^+)$ is the stabilizer of $X(E)$ and the stabilizer of a point in the orbit $G \times_{P(E^+)} X(E)$ is conjugate to

$$S(E) = K(E)(Z(G(E) \cap P(E^+)) \cdot R(E^+).$$

$P(E^+)/S(E)$ can be identified with $G(E)/K(E)$.

The lowest dimensional orbit is denoted by X_0 and may be identified with $G/P(E_0)$. Set $P_0 = P(E_0)$.

The points in X_0 can be characterized as follows:

LEMMA. *A point p of $\bar{X}$ is in X_0 if and only if there is a $g \in G$ which is contractive at P that is, there is a neighborhood U of p in $\bar{X}$ such that*

$$\lim_{n \to \infty} g^n(U) = p.$$

For any element $g \in G$, we denote by g^* the point gK in X. If g is an $\boldsymbol{R}$-regular semisimple element, then

(a) $(g^n)^*$ approaches a limit p_g in X_0,

(b) g is contractive at p_g,

(c) g has exactly m/m_0 fixed points in X_0

where m amd m_0 denote the orders of the $\boldsymbol{R}$-restricted Weyl groups of G and P_0 respectively. The point p_g is the unique coset xP_0 such that $g \in xP_0x^{-1}$ and g is contractive on X_0 at P_g. Conversely, property (c) implies that g is a semisimple $\boldsymbol{R}$-regular element. This results from the following

LEMMA. *Let G be a connected algebraic linear group defined over the field* k. *Let m and m_0 denote the orders of the* k*-restricted Weyl groups of G and P respectively. Let x be an element in G_{k} which lies in only a finite number of conjugates of P defined over* k. *Then x lies in at most m/m_0 conjugates defined over* k. *Assume moreover that P contains no normal subgroup of G containing a* k*-split torus of positive dimension. Then x is contained in exactly m/m_0 conjugates of P defined over* k *if and only if x is semisimple and the center of $Z(x)$ contains a maximal* k*-split torus of G. If* Ad *x is unipotent and x lies in only a finite number of conjugates over P over* k, *then x lies in only one. If P is a minimal parabolic subgroup over* k, *then x lies in only one conjugate of P over* k *if and only if* Ad *x is unipotent.*

The above lemma generalizes the result of Steinberg on regular elements as defined in [4].

5. Let $\phi : \bar{X} \to \bar{X}$ be a homeomorphism (not yet assumed to be a diffeomorphism) equivariant with respect to the isomorphism $\theta : \Gamma \to \Gamma'$.

Let γ be an $\boldsymbol{R}$-regular semisimple element in Γ. Then γ is contractive at $P_\gamma = \lim_{n \to \infty} (\gamma^n)^*$. Hence $\theta(\gamma)$ is contractive at $\phi(p_\gamma)$. Consequently p_γ and $\phi(p_\gamma)$

are in X_0 by the lemma above. Now Γp_γ is topologically dense in X_0 by virtue of the following

LEMMA. *Let G be a semisimple analytic group and Γ a subgroup such that G/Γ has finite invariant measure. Then ΓP is topologically dense in G for any parabolic subgroup P of G.*

Inasmuch as $\phi(\Gamma p_\gamma) = \theta(\Gamma)\phi(p_\gamma)$ we see that $\phi(X_0) = X_0$.

We now *add* the *hypothesis* that ϕ is differentiable on X_0.

LEMMA. *There is an automorphism t of H and a Zariski-dense subset*

$$H_t \subset H \cap MA^1$$

such that h and $t(h)$ operate equivalently on X_0 for any $h \in H_t$.

PROOF. Let $p_0 = \lim_{n\to\infty} (a^n)^*$, where $a \in A^1$. Let V denote the tangent space to X_0 at p_0; V may be identified with $\dot{G}/\dot{P}_0$. For any element $h \in H$, let $\bar{h}$ denote canonical image of h in $\mathrm{GL}(V)$. Let C be a Cartan subgroup of $\mathrm{GL}(V)$ which contains $\bar{H}$.

For any $\gamma \in \Gamma$, write $\gamma' = \theta(\gamma)$. For any one-to-one maps ξ and η, we write $\xi[\eta]$ for $\xi\eta\xi^{-1}$, and for any $g \in G$, we shall denote by the same letter the canonical action of g on X_0.

Given any $\boldsymbol{R}$-regular semisimple $\gamma \in \Gamma$, one can find elements g and g' in G such that $g[\gamma] \in H$ and $g'[\gamma'] \in H$. From $\phi(\gamma p) = \gamma'\phi(P)$ we see that $\phi\gamma = \gamma'\phi$ or

$$\gamma' = \phi\gamma\phi^{-1} = \phi[\gamma].$$

Hence

$$\begin{aligned} g'[\gamma'] &= g'[\phi[\gamma]] = g'[\phi[g^{-1}g[\gamma]]] \\ &= (g'\phi g^{-1})[g[\gamma]]. \end{aligned}$$

Let σ_γ denote the differential at p_0 of $g'\phi g^{-1}$. Then

$$\overline{g'[\gamma']} = \sigma_\gamma(\overline{g[\gamma]}).$$

Consequently, there is a t_γ in the Weyl group W of C such that

$$\overline{g'[\gamma']} = t_\gamma(\overline{g[\gamma]}).$$

For any $t \in W$, let H_t denote the subset of $H \cap MA^1 \cap G[\Gamma]$ on which the map $g[\gamma] \to t_\gamma$ has the constant value t. From Corollary 1 of §2 it follows that $H \cap MA^1 \cap G[\Gamma]$ is Zariski dense in H. Since W is finite, H_t is Zariski dense in H for some t. For such a t, $t(\bar{H}_t) \subset \bar{H}$ implies $t(\bar{H}) = \bar{H}$. From this the lemma follows, when we denote by t the automorphism of H induced by t.

Let S_1 denote the union of the H_t, $t \in W$, such that H_t is not Zariski dense in H. Let S denote the union of the Zariski-closure of S_1 and the set of non $\boldsymbol{R}$-regular elements in H. Then S is a proper Zariski-closed subset of H.

Now any $h \in H$ keeps fixed the finite set of points $W^A p_0$, where W^A is the normalizer of A. Any t with H_t dense in H stabilizes A and permutes the roots Φ^{E_0} occuring in the nilradical of $P(E_0)$ as well as the roots $U_w \Phi^{E_0}$ ($w \in W^A$). The latter is the set of all roots having nonconstant restrictions on T^*; indeed t permutes Φ^+. By Theorem 2, t stabilizes Φ. Hence

$$\operatorname{Tr} \operatorname{Ad} h = \operatorname{Tr} \operatorname{Ad} t(h) \text{ for all } h \in H.$$

It follows that

$$\operatorname{Tr} \operatorname{Ad} \gamma = \operatorname{Tr} \operatorname{Ad} \theta(\gamma) \text{ for all } \gamma \in G[H - S] \cap \Gamma.$$

No generality is lost in identifying γ with $\operatorname{Ad} \gamma$, that is, replacing G by its adjoint group. Given any $\gamma \in \Gamma$, we can find a $\gamma_1 \in G[H - S]$ such that $\gamma\gamma_1^n \in G[H - S]$ for all positive n, by Corollary 2 of §2. Hence

$$\operatorname{Tr} \gamma\gamma_1^n = \operatorname{Tr} \theta(\gamma\gamma_1^n) = \operatorname{Tr} \theta(\gamma)\theta(\gamma_1)^n, \qquad n > 0.$$

Since γ_1 is invertible, we may write $1 = c_1\gamma_1 + c_2\gamma_1^2 + \cdots + c_k\gamma_1 = f(\gamma_1)$. Then $\operatorname{Tr} \gamma = \operatorname{Tr} \gamma f(\gamma_1) = \operatorname{Tr} \theta(\gamma) f(\theta(\gamma_1)) = \operatorname{Tr} \theta(\gamma)$, since $f(\theta(\gamma_1)) = 1$. Reasoning as does Selberg in [3],

$$\operatorname{Tr} \sum c_\gamma \gamma = 0 \quad \text{if and only if} \quad \operatorname{Tr} \sum c_\gamma \theta(\gamma) = 0$$

for any constants c_γ. It follows that $\gamma \to \theta(\gamma)$ extends to a linear mapping of the associative enveloping algebra $\varepsilon(\Gamma) : \varepsilon(\Gamma) \to \varepsilon(\theta(\Gamma))$, that is, an automorphism of the semisimple associative algebra $\varepsilon(G)$. This automorphism sends Γ to $\theta(\Gamma)$ and hence the Zariski closure of Γ to that of $\theta(\Gamma)$; that is, the automorphism keeps G stable.

6. A few concluding remarks are in order. The proof we presented above does not use the full hypothesis that ϕ is a diffeomorphism. We use only that ϕ is a homeomorphism on $X \cup X_0$ and a diffeomorphism on X_0. I conjecture and in some cases can prove that if ϕ is a homeomorphism of X equivariant with respect to θ, then ϕ can be extended to be continuous on $X \cup X_0$. If θ_t $0 \leqq t \leqq 1$ is a deformation of Γ, and if ϕ_t, $0 \leqq t \leqq 1$, is a deformation of X, each ϕ_t being equivariant with respect to θ_t, then the unique extension of ϕ_t to $X \cup X_0$ should presumably be differentiable if G has no compact factors or factors of rank 1. In that sense the problem of rigidity is reduced to showing

(1) the existence of the deformation ϕ_t of X,

(2) the differentiability of the extension of ϕ_t to X_0.

References

1. C. Moore, *Compactifications of symmetric spaces*, Amer. J. Math. **86** (1964), 201–218.

2. I. Satake, *On representations and compactifications of Symmetric Riemannian spaces*, Ann. of Math. (2) **71** (1960), 77–110.

3. A. Selberg, *On discontinuous groups in higher-dimensional symmetric spaces*, Internat. Colloq. Function Theory, pp. 147–164. Tata Institute of Fundamental Research, Bombay, 1960.

4. R. Steinberg, *Regular elements of semi-simple algebraic groups*, Inst. Hautes Études Sci. Publ. Math. No. 25 (1965).

Index

Authors

This is a list of the authors of the various papers in the book, together with their permanent addresses.

Dr. Nelo D. Allan, Department of Mathematics, The University of Chicago, Chicago, Illinois, *and* Department of Mathematics, DePaul University, Chicago, Illinois.

Professor Walter L. Baily, Jr., Department of Mathematics, University of Chicago, Chicago, Illinois.

Professor Armand Borel, School of Mathematics, The Institute for Advanced Study, Princeton, New Jersey.

Professor François Bruhat, 80 Boulevard Pasteur, Paris XV°, France.

Professor Pierre Cartier, Department of Mathematics, University of Strasbourg, Strasbourg, France.

Professor Howard Garland, School of Mathematics, The Institute for Advanced Study, Princeton, New Jersey.

Professor R. Godement, Institut Henri Poincaré, Rue Pierre Curie, Paris, V^e, France.

William F. Hammond, 5007 Falls Road Terrace, Baltimore, Maryland 21210.

Professor Jun-ichi Igusa, 911 Breezewick Road, Towson, Maryland.

Professor Yasutaka Ihara, School of Mathematics, The Institute for Advanced Study, Princeton, New Jersey.

Professor Nagayoshi Iwahori, Department of Mathematics, University of California, Berkeley, California

Martin L. Kneser, Merkelstrasse 39, 34 Göttingen, Germany.

Professor Bertram Kostant, Department of Mathematics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139.

Professor Michio Kuga, Faculty of Science, University of Tokyo, Bunkyo-ku, Tokyo, Japan.

Dr. Robert P. Langlands, Fine Hall, Princeton University, Princeton, New Jersey.

Professor J. G. M. Mars, Mathematique Institut, Boothstraat 17, Utrecht, The Netherlands.

Professor Hideya Matsumoto, Institut Henri Poincaré, 11, Rue Pierre Curie, Paris 5^e, France.

Professor George D. Mostow, Department of Mathematics, Yale University, New Haven, Connecticut.

Professor David Mumford, Department of Mathematics, Harvard University, Cambridge, Massachusetts 02138.

Professor Shingo Murakami, Department of Mathematics, Osaka University, Osaka, Japan.

Professor Takashi Ono, Department of Mathematics, University of Pennsylvania, Philadelphia, Pennsylvania 19104.

Professor Ichiro Satake, Department of Mathematics, University of Chicago, Chicago, Illinois 60637.

Professor Goro Shimura, Department of Mathematics, Princeton University, Princeton, New Jersey.

Professor T. A. Springer, Mathematisch Instituut, Boothstraat 17, Utrecht, The Netherlands.

Professor Tsuneo Tamagawa, Department of Mathematics, Yale University, New Haven, Connecticut.

Professor Jacques L. Tits, Mathematisches Institut der Universität, Wegelerstrasse 10, 53 Bonn, Germany.