ALGEBRAIC NUMBER THEORY

Papers contributed for the
Kyoto International Symposium, 1976

Edited by

Shôkichi IYANAGA
Gakushuin University

Published by

Japan Society for the Promotion of Science

1977

Proceedings of the
Taniguchi International Symposium
Division of Mathematics, No. 2

Preface

This Volume contains account of the invited lectures at the International Symposium on Algebraic Number Theory in Commemoration of the Centennary of the Birth of Professor Teiji TAKAGI held at the Research Institute of Mathematical Sciences (RIMS), the University of Kyoto, from March 22 through March 29, 1976. This Symposium was sponsored by the Taniguchi Foundation and the Japan Society for Promotion of Sciences and was cosponsored by the RIMS, the Mathematical Society of Japan and the Department of Mathematics of the Faculty of Science of the University of Tokyo. It was attended by some 200 participants, among whom 20 from foreign countries.

The Organizing Committee of this Symposium consisted of 6 members: Y. AKIZUKI, Y. IHARA, K. IWASAWA, S. IYANAGA, Y. KAWADA, T. KUBOTA, who were helped in practical matters by 2 younger mathematicians T. IBUKIYAMA and Y. MORITA at the Department of Mathematics of the University of Tokyo. The oldest member of the Committee, Akizuki, is a close friend of Mr. T. TANIGUCHI, president of the Taniguchi Foundation, owing to whose courtesy a series of International Symposia on Mathematics is being held, of which the first was that on Finite Groups in 1974, this symposium being the second. The next oldest member, Iyanaga, was nominated to chair the Committee.

Another International Symposium on Algebraic Number Theory was held in Japan (Tokyo-Nikko) in September, 1955. Professor T. TAKAGI (1875–1960), founder of class-field theory, attended it as Honorary Chairman. During the years that passed since then, this theory made a remarkable progress. to which a host of eminent younger mathematicians, in Japan as well as in the whole world, contributed in most diversified ways. The actual date of the centennary of the birth of Professor Takagi fell on April 25, 1975. The plan of organizing this Symposium was then formed to commemorate him and his fundamental work and to encourage at the same time the younger researchers in this country.

We are most thankful to the institutions named above which sponsored or cosponsored this Symposium as well as to the foreign institutions such as the Royal Society of the United Kingdom. the National Science Foundation of the United States, the French Foreign Ministry and the Asia Foundation which provided support for the travel expenses of some of the participants. We appreciate also greatly the practical aids given by Mrs. A. HATORI at the Department of Mathematics of the University of Tokyo, Miss T. YASUDA and Miss Y. SHICHIDA at the RIMS.

In spite of all these supports, we could dispose of course of limited resources, so that we were not in a position to invite all the eminent mathematicians in this field as we had desired. Also some of the mathematicians we invited could not

come for various reasons. (Professor A. WEIL could not come because of his ill health at that time, but he sent his paper, which was read by Professor G. SHIMURA.)

The Symposium proceeded in 10 sessions, each of which was presided by senior chairman, one of whom was Professor OLGA TAUSSKY-TODD who came from the California Institute of Technology.

In addition to delivering the lectures which are published here together with some later development, we asked the participants to present their results in written form to enrich the conversations among them at the occasion of the Symposium. Thus we received 32 written communications, whose copies were distributed to the participants, some of whom used the seminar room which we had prepared for discussions.

We note that we received all the papers published here by the summer 1976, with the two exceptions: the paper by Professor TATE and the joint paper by Professors KUGA and S. IHARA arrived here a little later. We failed to receive a paper from Professor B. J. BIRCH who delivered an interesting lecture on "Rational points on elliptic curves" at the Symposium.

We hope that the Symposium made a significant contribution for the advancement of our science and should like to express once again our gratitude to all the participants for their collaboration and particularly to the authors of the papers in this Volume.

S. IYANAGA

Tokyo, June 1977

CONTENTS

ALGEBRAIC NUMBER THEORY, Papers contributed for the International Symposium, Kyoto 1976; S. Iyanaga (Ed.): Japan Society for the Promotion of Science, Tokyo, 1977

Trigonometric Sums and Elliptic Functions

J.W.S. CASSELS

Let ξ be a p-th root of unity, where $p > 0$ is a rational prime and let χ be a character on the multiplicative group modulo p. Suppose that l is the precise order of χ: so $p \equiv 1 \pmod{l}$. We denote by

$$\tau = \sum_{r=1}^{p-1} \chi(r)\xi^r \tag{1}$$

the corresponding "generalized Gauss sum". It is well-known and easy to prove that $\tau^l \in \boldsymbol{Q}(\chi)$ and there are fairly explicit formulae for τ^l in terms of the decomposition of the prime p in $\boldsymbol{Q}(\chi)$: these are the basis of the original proof of Eisenstein's Reciprocity Theorem.

When the values of χ are taken to lie in the field $\boldsymbol{C}$ of complex numbers and ξ is given an explicit complex value, say

$$\xi = e^{2\pi i/p}, \tag{2}$$

then τ is a well-defined complex number of absolute value $p^{1/2}$. It is therefore meaningful to ask if there are any general criteria for deciding in advance which of the l-th roots of the explicitly given complex number τ^l is actually the value of τ. The case $l = 2$ is the classical "Gauss sum". Here $\tau^2 = (-1)^{(p-1)/2}p$ and Gauss proved that (2) implies that $\tau = p^{1/2}(p \equiv 1 \pmod 4)$, $\tau = ip^{1/2}(p \equiv -1 \pmod 4)$, where $p^{1/2}$ denotes the positive square root. And this remains the only definitive result on the general problem.

The next simplest case, namely $l = 3$ was considered by Kummer. We denote the cube root of 1 by $\omega = (-1 + (-3)^{1/2})/2$. There is uniqueness of factorization in $\boldsymbol{Z}[\omega]$: in particular $p = \tilde{\omega}\tilde{\omega}'$ where we can normalize so that $\tilde{\omega} = (l + 3m(-3)^{1/2})/2$ with $l, m \in \boldsymbol{Z}$ and $l \equiv 1 \pmod 3$. We have

$$\tau^3 = p\tilde{\omega} \tag{3}$$

where the sign of m is determined by the normalization

$$\chi(r) \equiv r^{(p-1)/3} \pmod{\tilde{\omega}} . \tag{4}$$

Kummer evaluated τ for some small values of p. He made a statistical conjecture about the distribution of the argument of the complex number τ (with the normalization (2)). Subsequent calculations have thrown doubt on this conjecture and the most probable conjecture now is that the argument of τ is uniformly distributed.

Class-field theory tells us that the cube root of $\tilde{\omega}$ lies in the field of $\tilde{\omega}$-division values on the elliptic curve

$$y^2 = x^3 + \tfrac{1}{4} \tag{5}$$

which has complex multiplication by $\boldsymbol{Z}[\omega]$: and in fact the relevant formulae were almost certainly known to Eisenstein at the beginning of the 19th century. Let $\boldsymbol{d}$ be a $\tilde{\omega}$-th division point of (5). Then in an obvious notation

$$\prod_{r=1}^{p-1} x(r\boldsymbol{d}) = \frac{1}{\tilde{\omega}^2} . \tag{6}$$

Hence if S denotes a $\frac{1}{3}$-set modulo $\tilde{\omega}$ (i.e. the $s, \omega s, \omega^2 s$ ($s \in S$) together with 0 are a complete set of residues (mod $\tilde{\omega}$)) we see that $P_S^3 = 1/\tilde{\omega}^2$, where

$$P_S(\boldsymbol{d}) = \prod_{s \in S} x(s\boldsymbol{d}) . \tag{7}$$

We can normalize S so that

$$\prod_{s \in S} s \equiv -1 \pmod{\tilde{\omega}} \tag{8}$$

and then $P_S(\boldsymbol{d}) = P(\boldsymbol{d})$ depends only on $\boldsymbol{d}$.

In order to compare with the normalization (2) we must choose an embedding in the complex numbers and take the classical parametrization of (5) in terms of the Weierstrass $\mathscr{P}$-function. Let θ be the positive real period and denote by $\boldsymbol{d}_0$ the $\tilde{\omega}$-division point belonging to $\theta/\tilde{\omega}$. Then the following conjecture has been verified numerically for all $p < 6{,}000$:

Conjecture (first version)

$$\tau = \tilde{\omega} p^{1/3} P(\boldsymbol{d}_0) \tag{9}$$

Here $p^{1/3}$ is the real cube root.

This conjecture can be formulated in purely geometrical terms independent of the complex embeddings. Let $\boldsymbol{d}, \boldsymbol{e}$ be respectively $\tilde{\omega}$- and $\tilde{\omega}'$-division points on (5). The Weil pairing gives a well-defined p-th root of unity

$$\xi = \xi(\boldsymbol{d}, \boldsymbol{e}) , \tag{10}$$

with which we can construct the generalized Gauss sum $\tau = \tau(\xi)$ as in (1). With this notation the conjecture is equivalent to

Conjecture (second version)

$$\tau(\xi(\boldsymbol{d}, \boldsymbol{e})) = \{\chi(3)\}^2 p\tilde{\omega}\{P(\boldsymbol{d})\}^2 P'(\boldsymbol{e}) , \tag{11}$$

where $P'(\boldsymbol{e})$ is the analogue for $\boldsymbol{e}$ of $P(\boldsymbol{d})$.

The somewhat unexpected appearance of the factor $\{\chi(3)\}^2$ in the second version is explained by the fact that $e^{2\pi i/p}$ is not the Weil pairing of the points with parameters $\theta/\tilde{\omega}$ and $\theta/\tilde{\omega}'$.

We must now recall Kronecker's treatment of the ordinary Gauss sum. Let χ_2 be the unique character of order 2 on the multiplicative group of residue classes of $\boldsymbol{Z}$ modulo the odd prime p, so

$$\tau_2 = \sum_{r=1}^{p-1} \chi_r(r)\xi^r \tag{12}$$

is the ordinary Gauss sum and, as already remarked, it is a straightforward exercise to show that

$$\tau_2^2 = (-1)^{1/2(p-1)} p . \tag{13}$$

Consider also

$$\sigma = \prod_{1}^{[1/2p]} (\xi^r - \xi^{-r}) . \tag{14}$$

Then also

$$\sigma^2 = (-1)^{1/2(p-1)} p \tag{15}$$

and so

$$\tau_2 = \pm\sigma \tag{16}$$

If we make the normalization (2) it is easy to compute the argument of σ, since it is a product. Hence we can determine the argument of τ_2 if we can determine the ambiguous sign $\pm$ in (16). But (16) is a purely algebraic statement and we can proceed algebraically. The prime p ramifies completely in $\boldsymbol{Q}(\xi)$. The extension $\mathfrak{p}$ of the p-adic valuation has prime element $1 - \xi$ and $(1 - \xi)^{-1/2(p-1)}\tau_2$ and $(1 - \xi)^{-1/2(p-1)}\sigma$ are both $\mathfrak{p}$-adic units. As Kronecker showed, it is not difficult to compute their residues in the residue class field

F_p and so to determine the sign.

If, however, we attempt to follow the same path with (11) we encounter a difficulty. There are two distinct primes $\tilde{\omega}$ and $\tilde{\omega}'$ of $Q(\omega)$. The prime $\tilde{\omega}$ ramifies completely in the field of the $\tilde{\omega}$-division points and so if we work with an extension of the $\tilde{\omega}$-adic valuation there is little trouble with $P(\boldsymbol{d})$. On the other hand, $P'(\boldsymbol{e})$ remains intractable. Thus instead of obtaining a proof of (11) we obtain merely a third version of the conjecture which works in terms of the elliptic curve (5) considered over the finite field F_p of p elements and over its algebraic closure $\bar{F}$. To explain this form of the conjecture we must recall some concepts about isogenies of elliptic curves over fields of prime characteristic in our present context.

We can identify F_p with the residue class field $Z[\omega]/\tilde{\omega}$. Then complex multiplication by the conjugate $\tilde{\omega}'$ gives a separable isogeny of the curve (5) with itself. If $X = (X, Y)$ is a generic point of (5) we shall write this isogeny as

$$(X, Y) = X \xrightarrow{\tilde{\omega}'} \tilde{\omega}'X = \boldsymbol{x} = (x, y) \ . \tag{17}$$

The function field $\bar{F}(X)$ is a galois extension of $\bar{F}(\boldsymbol{x})$ of relative degree p. The galois group is, indeed, cyclic namely

$$X \longrightarrow X + \boldsymbol{e} \ , \tag{18}$$

where $\boldsymbol{e}$ runs through the kernel of (17) (that is, through the $\tilde{\omega}'$-division points). The extension $\bar{F}(X)/\bar{F}(\boldsymbol{x})$ is thus Artin-Schreier. As Deuring [3] showed, there is an explicit construction of $\bar{F}(X)$ as an Artin-Schreier extension. Since we are in characteristic p, there is by the Riemann-Roch theorem a function $f(X)$ whose only singularities are simple poles at the p points of the kernel of (17) and which has the same residue (say 1) at each of them. Then

$$f(X) \in \bar{F}(X) \tag{19}$$

but

$$f(X) \notin \bar{F}(\boldsymbol{x}) \tag{20}$$

since otherwise it would be a function of $\boldsymbol{x}$ whose only singularity is a simple pole.

For any $\boldsymbol{e}$ in the kernel, the function $f(\boldsymbol{x} + \boldsymbol{e})$ enjoys the same properties as $f(\boldsymbol{x})$, and so

$$f(\boldsymbol{x} + \boldsymbol{e}) = f(\boldsymbol{x}) + \alpha(\boldsymbol{e}) \ , \tag{21}$$

where

$$\alpha(\boldsymbol{e}) \in \bar{F} \ . \tag{22}$$

Clearly

$$\alpha(\boldsymbol{e}_1 + \boldsymbol{e}_2) = \alpha(\boldsymbol{e}_1) + \alpha(\boldsymbol{e}_2) \tag{23}$$

and so $\alpha(\boldsymbol{e})$ gives a homomorphic map of the kernel of $\tilde{\omega}'$ into the additive group of $\bar{F}$. This homomorphism is non-trivial, by (20).

Following Deuring we normalize the residue of $f(X)$ at the points of the kernel so that near the "point at infinity" it behaves like y/x ($\boldsymbol{x} = \tilde{\omega}'X$). Then

$$f^p(X) - Af(X) = F(\boldsymbol{x}) \tag{24}$$

where $F(\boldsymbol{x})$ can be given explicitly and A is the "Hasse invariant". Given $F(\boldsymbol{x})$ the roots of this equation are $f(X)$ itself and its conjugates

$$f(X + \boldsymbol{e}) = f(X) + \alpha(\boldsymbol{e}) \ . \tag{25}$$

In particular

$$\{\alpha(\boldsymbol{e})\}^{p-1} = A \ . \tag{26}$$

All the above applies generally to an inseparable isogeny with cyclic kernel of an elliptic curve with itself. In our particular case

$$A = -\{[(p-1)/3]!\}^{-3} \ . \tag{27}$$

This implies the slightly remarkable fact that one third of the points of the kernel are distinguished by the property that

$$\{\alpha(\boldsymbol{e})\}^{(p-1)/3} = -1/[(p-1)/3]! \ . \tag{28}$$

We now can carry through the analogue of Kronecker's procedure. If $\boldsymbol{d}$ is a $\tilde{\omega}$-th division point the extension $Q(\omega, \boldsymbol{d})/Q(\omega)$ is completely ramified. A prime element for the extended valuation $\mathfrak{p}$ is given by μ/λ where (λ, μ) are the co-ordinates of $\boldsymbol{d}$. We extend $\mathfrak{p}$ to a valuation $\mathfrak{P}$ of the algebraic closure of Q. Let $\boldsymbol{e}$ be a $\tilde{\omega}'$-division point and let its reduction modulo $\mathfrak{P}$ belong to $\alpha(\boldsymbol{e}) \in \bar{F}$ in the sense just described. Then it is not difficult to see that the statement that ξ is the Weil pairing of $\boldsymbol{d}$ and $\boldsymbol{e}$ is equivalent to the statement that the $\mathfrak{p}$-adic unit

$$\tilde{\omega}'(1 - \xi)\lambda/\mu \ ,$$

reduces to $\alpha(\boldsymbol{e})$ modulo $\mathfrak{P}$.

We are now in a position to enunciate the third version of the conjecture. We denote the co-ordinates of $\boldsymbol{e}$ by $(X(\boldsymbol{e}), Y(\boldsymbol{e}))$.

Conjecture (third version). *Let S be a $1/3$-set modulo p satisfying* (8) *and let $\boldsymbol{e}$ be a point of the kernel of the inseparable isogeny* (17). *Suppose that* (28) *holds. Then*

$$\prod_{s \in S} X(s\boldsymbol{e}) = 3^{(p-1)/3}\{[(p-1)/3]!\}^2 .$$

This is, of course an equation in $\bar{F}$. It is, in fact the version of the conjecture which was originally discovered. The value of $\alpha(\boldsymbol{e})$ determines $\boldsymbol{e}$ uniquely and so determines its co-ordinates $X(\boldsymbol{e}), Y(\boldsymbol{e})$. There is therefore no ambiguity in considering them as functions of α, say $X(\alpha), Y(\alpha)$ where $\alpha^{p-1} = A$. If we had a really serviceable description of $X(\alpha)$ in terms of α then one could expect to prove the conjecture. The author was unable to find such a description but did obtain one which was good enough for computer calculations. Inspection of the results of the calculation suggested the third formulation of the conjecture: the other two formulations were later. Indeed the calculations suggested a somewhat stronger conjecture which will now be described.

Consideration of complex multiplication on (5) by the 6-th roots of unity show easily that $\alpha^{-2}X(\alpha)$ depends only on α^6. Call it $X_0(\alpha^6)$. Then calculation suggests:

Conjecture (strong form)

$$\prod_{\beta} X_0(\beta) = -3^{-(p-1)/3}\{[(p-1)/3]!\}^2$$

where the product is over all roots β of

$$\beta^{(p-1)/6} = A .$$

Even if my conjectures could be proved, it is not clear whether they would contribute to the classical problem about τ, namely whether or not its argument is uniformly distributed as p runs through the primes $\equiv 1 \pmod 6$. Also it should be remarked, at least parenthetically, that in his Cambridge thesis John Loxton has debunked the miraculous-seeming identities in [2].

References

[1] Cassels, J. W. S., On Kummer sums. Proc. London Math. Soc. (3) **21** (1970), 19–27.
[2] Cassels, J. W. S., Some elliptic function identities. Acta Arithmetica **18** (1971), 37–52.

[3] Deuring, M., Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. Abh. Math. Sem. Univ. Hamburg. **14** (1941), 197–272.

Department of Pure Mathematics
and Mathematical Statistics
University of Cambridge
16 Mill Lane, Cambridge CB2 1SB
United Kingdom

ALGEBRAIC NUMBER THEORY, Papers contributed for the International Symposium, Kyoto 1976; S. Iyanaga (Ed.): Japan Society for the Promotion of Science, Tokyo, 1977

Kummer's Criterion for Hurwitz Numbers

J. COATES and A. WILES

Introduction

In recent years, a great deal of progress has been made on studying the p-adic properties of special values of L-functions of number fields. While this is an interesting problem in its own right, it should not be forgotten that the ultimate goal of the subject is to use these special values to study the arithmetic of the number fields themselves, and of certain associated abelian varieties. The first result in this direction was discovered by Kummer. Let $\boldsymbol{Q}$ be the field of rational numbers, and $\zeta(s)$ the Riemann zeta function. For each even integer $k > 0$, define

$$\zeta^*(k) = (k-1)!\,(2\pi)^{-k}\zeta(k)\ .$$

In fact, we have $\zeta^*(k) = (-1)^{1+k/2}B_k/(2k)$, where B_k is the k-th Bernoulli number, so that $\zeta^*(k)$ is rational. Let p be an odd prime number. Then it is known that $\zeta^*(k)$ $(1 \leqslant k < p-1)$ is p-integral. Let n be an integer $\geqslant 0$, and $\mu_{p^{n+1}}$ the group of p^{n+1}-th roots of unity. Let $F_n = \boldsymbol{Q}(\mu_{p^{n+1}})$, and let R_n be the maximal real subfield of F_n. We give several equivalent forms of Kummer's criterion, in order to bring out the analogy with our later work. By a $\boldsymbol{Z}/p\boldsymbol{Z}$-extension of a number field, we mean a cyclic extension of the number field of degree p.

Kummer's Criterion. *At least one of the numbers $\zeta^*(k)$ (k even, $1 \leqslant k < p-1$) is divisible by p if and only if the following equivalent assertions are valid*:— (i) *p divides the class number of F_0*; (ii) *there exists an unramified $\boldsymbol{Z}/p\boldsymbol{Z}$-extension of F_0*; (iii) *there exists a $\boldsymbol{Z}/p\boldsymbol{Z}$-extension of R_0, which is unramified outside the prime of R_0 above p, and which is distinct from R_1.*

A modified version of Kummer's criterion is almost certainly valid if we replace $\boldsymbol{Q}$ by an arbitrary totally real base field K (see [3] for partial results

in this direction). This is in accord with the much deeper conjectural relationship between the abelian p-adic L-functions of K and certain Iwasawa modules attached to the cyclotomic $\boldsymbol{Z}_p$-extension of $K(\mu_p)$.

When the base field K is not totally real, the values of the abelian L-functions of K at the positive integers do not seem to admit a simple arithmetic interpretation, and it has been the general feeling for some time that one should instead use the values of Hecke L-functions of K with Grossencharacters of type (A_0) (in the sense of Weil [15]). In the special case $K = \boldsymbol{Q}(i)$, this idea goes back to Hurwitz [4]. Indeed, let K be any imaginary quadratic field with class number 1, and $\mathcal{O}$ the ring of integers of K. Let E be any elliptic curve defined over $\boldsymbol{Q}$, whose ring of endomorphisms is isomorphic to $\mathcal{O}$. Write S for the set consisting of 2, 3, and all rational primes where E has a bad reduction. Choose, once and for all, a Weierstrass model for E

$$y^2 = 4x^3 - g_2x - g_3\,, \tag{1}$$

such that g_2, g_3 belong to $\boldsymbol{Z}$, and the discriminant of (1) is divisible only by primes in S. Let $\mathfrak{p}(z)$ be the associated Weierstrass function, and L the period lattice of $\mathfrak{p}(z)$. Since $\mathcal{O}$ has class number 1, we can choose $\Omega \in L$ such that $L = \Omega\mathcal{O}$. As usual, we suppose that K is embedded in the complex field $\boldsymbol{C}$, and we identify $\mathcal{O}$ with the endomorphism ring of E in such a way that the endomorphism corresponding to $\alpha \in \mathcal{O}$ is given by $\xi(z) \mapsto \xi(\alpha z)$, where $\xi(z) = (\mathfrak{p}(z), \mathfrak{p}'(z))$. Let ψ be the Grossencharacter of E as defined in § 7.8 of [14]. In particular, ψ is a Grossencharacter of K of type (A_0), and we write $L(\psi^k, s)$ for the primitive Hecke L-function of ψ^k for each integer $k \geqslant 1$. It can be shown (cf. [2]) that $\Omega^{-k}L(\psi^k, k)$ belongs to K for each integer $k \geqslant 1$. Let w be the number of roots of unity in K. In the present paper, we shall only be concerned with those k which are divisible by w. In this case, $\Omega^{-k}L(\psi^k, k)$ is rational for the following reason. If $k \equiv 0 \bmod w$, we have $\psi^k(\mathfrak{a}) = \alpha^k$, where α is any generator of the ideal $\mathfrak{a}$. Then, for $k \geqslant 4$,

$$L^*(\psi^k, k) = w(k-1)!\,\Omega^{-k}L(\psi^k, k) \qquad (k \equiv 0 \bmod w) \tag{2}$$

is the coefficient of $z^{k-2}/(k-2)!$ in the Laurent expansion of $\mathfrak{p}(z)$ about the point $z = 0$. A different argument has to be used to prove the rationality of (2) in the exceptional case $k = w = 2$.

It is natural to ask whether there is an analogue for the numbers (2) of Kummer's criterion. Such an analogue would provide concrete evidence that

the p-adic L-functions constructed by Katz [6], [7], Lang [8], Lichtenbaum [9], and Manin-Vishik [10] to interpolate the $L^*(\psi^k, k)$ are also related to Iwasawa modules. A first step in this direction was made by A. P. Novikov [11]. Subsequently, Novikov's work was greatly improved by G. Robert [12]. Let p be a prime number, not in the exceptional set S, which splits in K. In this case, it can be shown that the numbers

$$L^*(\psi^k, k) \qquad (1 \leqslant k < p-1,\ k \equiv 0 \bmod w) \tag{3}$$

are all p-integral. Let $\mathfrak{p}$ be one of the primes of K dividing p. For each integer $n \geqslant 0$, let $\mathfrak{R}_n$ denote the ray class field of K modulo $\mathfrak{p}^{n+1}$. Then Robert showed that the class number of $\mathfrak{R}_0$ is prime to p if p does not divide any of the numbers (3). In the present paper, we use a different method from Robert to prove the following stronger result.

Theorem 1. *Let p be a prime number, not in S, which splits in K. Then p divides at least one of the numbers* (3) *if and only if there exists a $\boldsymbol{Z}/p\boldsymbol{Z}$-extension of $\mathfrak{R}_0$, which is unramified outside the prime of $\mathfrak{R}_0$ above $\mathfrak{p}$, and which is distinct from $\mathfrak{R}_1$.*

Since this paper was written, Robert (private communication) has also proven this theorem by refining his methods in [12].

As a numerical example of the theorem, take $K = \boldsymbol{Q}(i)$, and E the elliptic curve $y^2 = 4x^3 - 4x$. Then $S = \{2, 3\}$. Define a prime $p \equiv 1 \bmod 4$ to be irregular for $\boldsymbol{Q}(i)$ if there exists a $\boldsymbol{Z}/p\boldsymbol{Z}$-extension of $\mathfrak{R}_0$, unramified outside the prime above $\mathfrak{p}$, and distinct from $\mathfrak{R}_1$. It follows from Theorem 1 and Hurwitz's table in [4] that $p = 5, 13, 17, 29, 37, 41, 53$ are regular for $\boldsymbol{Q}(i)$. On the other hand, $p = 61, 2381, 1162253$ are irregular for $\boldsymbol{Q}(i)$, since they divide $L^*(\psi^{36}, 36)$, $L^*(\psi^{40}, 40)$, $L^*(\psi^{48}, 48)$, respectively.

For completeness, we now state the analogue, in this context, of assertions (i) and (ii) of Kummer's criterion. Again suppose that p is a prime, not in S, which splits in K, say $(p) = \mathfrak{p}\bar{\mathfrak{p}}$. Put $\pi = \psi(\mathfrak{p})$, so that π is a generator of $\mathfrak{p}$. For each integer $n \geqslant 0$, let E_{π^n} be the kernel of multiplication by π^n on E. Put $\mathcal{F} = K(E_\pi)$. Thus $\mathcal{F}/K$ is an abelian extension of degree $p-1$. By the theory of complex multiplication, $\mathcal{F}$ contains $\mathfrak{R}_0$, and $[\mathcal{F} : \mathfrak{R}_0] = w$. Let Δ be the Galois group of $\mathcal{F}/\mathfrak{R}_0$, and let $\chi : \Delta \to (\boldsymbol{Z}/p\boldsymbol{Z})^\times$ be the character defined by $u^\sigma = \chi(\sigma)u$ for all $\sigma \in \Delta$ and $u \in E_\pi$. Let $E(\mathcal{F})$ be the group of points of E with coordinates in $\mathcal{F}$. If A is any module over the group ring

$\boldsymbol{Z}_p[\Delta]$, the χ^k-th component of A means the submodule of A on which Δ acts via χ^k. Consider the $\boldsymbol{Z}_p[\Delta]$-module $E(\mathcal{F})/\pi E(\mathcal{F})$. Since $E_{\pi^2} \cap E(\mathcal{F}) = E_\pi$ (because $\boldsymbol{Q}_p(E_{\pi^2})/\boldsymbol{Q}_p$ is a totally ramified extension of degree $p(p-1)$), we can view E_π as a submodule of $E(\mathcal{F})/\pi E(\mathcal{F})$. By the definition of χ, E_π lies in the χ-component of $E(\mathcal{F})/\pi E(\mathcal{F})$. Let Ш denote the Tate-Safarevic group of E over $\mathcal{F}$, i.e. Ш is defined by the exactness of the sequence

$$0 \longrightarrow Ш \longrightarrow H^1(\mathcal{F}, E) \longrightarrow \prod_{\text{all } \mathfrak{g}} H^1(\mathcal{F}_\mathfrak{g}, E) ,$$

where the cohomology is the Galois cohomology of commutative algebraic groups (cf. [13]); here $\mathfrak{g}$ runs over all finite primes of $\mathcal{F}$, and $\mathcal{F}_\mathfrak{g}$ is the completion at $\mathfrak{g}$. Let $Ш(\pi)$ denote the π-primary component of Ш.

Theorem 2. *Let p be a prime number, not in S, which splits in K. Then the following two assertions are equivalent:—* (i) *there exists a $\boldsymbol{Z}/p\boldsymbol{Z}$-extension of $\mathfrak{R}_0$, unramified outside the prime above $\mathfrak{p}$, and distinct from $\mathfrak{R}_1$;* (ii) *either the χ-component of $Ш(\pi)$ is non-trivial, or the χ-component of $E(\mathcal{F})/\pi E(\mathcal{F})$ is strictly larger than E_π.*

For brevity, we do not include the proof of Theorem 2 in this note. However, the essential ingredients for the proof can be found in [2].

Since the symposium, we have succeeded in establishing various refinements and generalizations of Theorem 1. These yield deeper connexions between the numbers $L^*(\psi^k, k)$ $(k \geqslant 1)$, and the arithmetic of the elliptic curve E. In particular, the following part of the conjecture of Birch and Swinnerton-Dyer for E is proven in [2] by these methods.

Theorem 3. *Assume that E is defined over $\boldsymbol{Q}$, and has complex multiplication by the ring of integers of an imaginary quadratic field with class number 1. If E has a rational point of infinite order, then the Hasse-Weil zeta function of E over $\boldsymbol{Q}$ vanishes at $s = 1$.*

In particular, the theorem applies to the curves $y^2 = x^3 - Dx$, D a non-zero rational number, which were originally studied by Birch and Swinnerton-Dyer. These curves all admit complex multiplication by the ring of Gaussian integers.

Proof of Theorem 1. This is divided into two parts. In the first part, we use class field theory to establish a Galois-theoretic p-adic residue formula for an arbitrary finite extension of K. The arguments in this part have been suggested by [1] (see Appendix 1), where an analogous result is established for totally real number fields. We then combine this with a function-theoretic p-adic residue formula, due to Katz and Lichtenbaum, for the p-adic zeta function of $\mathfrak{R}_0/K$. This then yields Theorem 1.

We use the following notation throughout. Let K be any imaginary quadratic field (we do not assume in this first part of the proof that K has class number 1), and F an arbitrary finite extension of K. Put $d = [F: K]$. Let p be an odd rational prime satisfying (i) p does not divide the class number of K, and (ii) p splits in K. We fix one of the primes of K lying above p, and denote it by $\mathfrak{p}$. Write $\mathcal{S}$ for the set of primes of F lying above $\mathfrak{p}$.

We now define two invariants of F/K which play an essential role in our work. The first is the $\mathfrak{p}$-adic regulator $R_\mathfrak{p}$ of F/K. Let $\boldsymbol{Q}_p$ be the field of p-adic numbers, and $\boldsymbol{C}_p$ a fixed algebraic closure of $\boldsymbol{Q}_p$. Let log denote the extension of the p-adic logarithm to the whole of $\boldsymbol{C}_p$ in the manner described in § 4 of [5]. Denote by $\phi_1, \cdots, \phi_d$ the distinct embeddings of F into $\boldsymbol{C}_p$, which correspond to primes in $\mathcal{S}$. There are d of these embeddings because the sum of the local degrees over $\boldsymbol{Q}_p$ of the primes in $\mathcal{S}$ is equal to d, because p splits in K. Let $\mathscr{E}$ be the group of global units of F. Since F is totally imaginary, the $\boldsymbol{Z}$-rank of $\mathscr{E}$ modulo torsion is equal to $d - 1$. Pick units $\varepsilon_1, \cdots, \varepsilon_{d-1}$ which represent a basis of $\mathscr{E}$ modulo torsion, and put $\varepsilon_d = 1 + p$. We then define $R_\mathfrak{p}$ to be the $d \times d$ determinant

$$R_\mathfrak{p} = (d \log \varepsilon_d)^{-1} \det (\log (\phi_i(\varepsilon_j)))_{1 \leqslant i, j \leqslant d} . \tag{4}$$

Since the norm from F to K of an element of $\mathscr{E}$ is a root of unity, and the logarithm of a root of unity is 0, it is easy to see that, up to a factor ± 1, $R_\mathfrak{p}$ is independent of the choice of $\varepsilon_1, \cdots, \varepsilon_{d-1}$, and defines an invariant of F/K. The second quantity that we wish to define is the $\mathfrak{p}$-component $\Delta_\mathfrak{p}$ of the relative discriminant of F/K. Let $\Delta_{F/K}$ be the discriminant of F over K, so that $\Delta_{F/K}$ is an ideal of K. Let $K_\mathfrak{p}$ denote the completion of K at $\mathfrak{p}$, and $\mathcal{O}_\mathfrak{p}$ the ring of integers of $K_\mathfrak{p}$. We define $\Delta_\mathfrak{p}$ to be any generator of the ideal $\Delta_{F/K}\mathcal{O}_\mathfrak{p}$. Thus, strictly speaking, $\Delta_\mathfrak{p}$ is well defined only up to a unit in $\mathcal{O}_\mathfrak{p}$. However, this will suffice for our present purposes, since we will only be interested in the valuation of $\Delta_\mathfrak{p}$. It is perhaps worth noting that, since $\Delta_{F/K}\mathcal{O}_\mathfrak{p}$ can be written as a product of local discriminants of F/K for the primes in $\mathcal{S}$ (cf. the proof of Lemma 8), one can, in fact, define $\Delta_\mathfrak{p}$ uniquely, up to the square of a unit in $\mathcal{O}_\mathfrak{p}$.

By class field theory, there is a unique $\boldsymbol{Z}_p$-extension of K which is un-

ramified outside $\mathfrak{p}$. We denote this Z_p-extension by K_∞, and write K_n for the n-th layer of K_∞/K. Since p is assumed not to divide the class number of K, the extension K_∞/K is totally ramified at $\mathfrak{p}$. For each $n \geqslant 0$, let $\mathcal{V}_n$ be the completion of K_n at the unique prime above $\mathfrak{p}$, and let V_n be the units of $\mathcal{V}_n$ which are $\equiv 1$ modulo the maximal ideal. We write $V = V_0$ for the units of $\mathcal{O}_\mathfrak{p}$ which are $\equiv 1$ modulo p. Let N_n denote the norm map from $\mathcal{V}_n$ to $K_\mathfrak{p}$.

Lemma 4. *For each $n \geqslant 0$, we have $N_n(V_n) = V^{p^n}$.*

Proof. The lemma is true for any totally ramified abelian extension of $K_\mathfrak{p}(=\boldsymbol{Q}_p)$ of degree p^n. For, pick a local parameter π_n in $\mathcal{V}_n$. Since $\mathcal{V}_n/K_\mathfrak{p}$ is totally ramified, $\tau_n = N_n(\pi_n)$ is a local parameter in $K_\mathfrak{p}$. Thus we have

$$\mathcal{V}_n^\times = \mu_{p-1} \times \{\pi_n\} \times V_n , \qquad K_\mathfrak{p}^\times = \mu_{p-1} \times \{\tau_n\} \times V ,$$

where μ_{p-1} denotes the group of $(p-1)$-th roots of unity, and $\{\pi_n\}$, $\{\tau_n\}$ are the cyclic groups generated by π_n, τ_n, respectively. Now, by local class field theory, the index of $N_n(\mathcal{V}_n^\times)$ in $K_\mathfrak{p}^\times$ is p^n. Since $N_n(\mu_{p-1}) = \mu_{p-1}$, and since $N_n(\pi_n) = \tau_n, N_n(V_n)$ must be a closed subgroup of V of index p^n. But, as $\mathcal{O}_\mathfrak{p} = Z_p, V^{p^n}$ is the only closed subgroup of V of index p^n, and the proof of the lemma is complete.

Let $F_\infty = FK_\infty$, so that F_∞/F is a Z_p-extension, which is unramified outside $\mathcal{S}$. For each $n \geqslant 0$, let F_n denote the n-th layer of F_∞/F, and write C_n for the idèle class group of F_n. For brevity, put $C = C_0$. Let $N_{F_n/F}$ be the norm map from C_n to C, and put

$$Y = \bigcap_{n \geqslant 0} N_{F_n/F} C_n .$$

For each $\mathfrak{g} \in \mathcal{S}$, $U_{\mathfrak{g},1}$ will denote the units in the completion of F at $\mathfrak{g}$, which are $\equiv 1 \bmod \mathfrak{g}$, and we put

$$U_1 = \prod_{\mathfrak{g} \in \mathcal{S}} U_{\mathfrak{g},1} .$$

We view U_1 as being embedded in the idèle class group C in the usual way, and identify it with its image in C. We write, for convenience, $N_{F/K}$ for the norm map from U_1 to V given by the product of the local norms to $K_\mathfrak{p}$ at all the $\mathfrak{g}$ in $\mathcal{S}$. Thus $N_{F/K}$ is the restriction to U_1 of the norm map from C to the idèle class group of K. Finally, if L/H is an abelian extension of local or global fields, and ξ belongs to $H^\times$, or the idèle class group of H, according as H is local or global, we denote the Artin symbol of ξ for L/H by $(\xi, L/H)$.

Lemma 5. *$Y \cap U_1$ is the kernel of $N_{F/K}$.*

Proof. Define the integer $e \geqslant 0$ by $K_e = K_\infty \cap F$. Thus, for each $n \geqslant 0$, we have $F_n = FK_{n+e}$. Suppose first that $\xi \in Y \cap U_1$. Since $\xi \in N_{F_n/F} C_n$, we have $(\xi, F_n/F) = 1$ for each $n \geqslant 0$, whence, restricting this Artin symbol to K_{n+e}, we obtain $(N_{F/K}\xi, K_{n+e}/K) = 1$. Since $N_{F/K}\xi$ lies in $K_\mathfrak{p}$, it follows from class field theory that $N_{F/K}\xi$ is a norm from $\mathcal{V}_{n+e}$; clearly it must then be a norm from V_{n+e}. Hence, by Lemma 4, $N_{F/K}\xi \in V^{p^{n+e}}$ for all $n \geqslant 0$, and so $N_{F/K}\xi = 1$. Conversely, let ξ be an element of U_1 with $N_{F/K}\xi = 1$. Let j be the restriction map from $G(F_\infty/F)$ to $G(K_\infty/K)$. Note that j is injective because $F_\infty = FK_\infty$. Now, if C_K denotes the idèle class group of K, class field theory tells us that we have the commutative diagram

$$\begin{array}{ccc} C & \longrightarrow & G(F_\infty/F) \\ {\scriptstyle N_{F/K}}\downarrow & & \downarrow{\scriptstyle j} \\ C_K & \longrightarrow & G(K_\infty/K) , \end{array}$$

where the vertical map on the left is the norm map, and the horizontal maps are the respective Artin maps. Since j is injective, $N_{F/K}\xi = 1$ implies that $(\xi, F_\infty/F) = 1$, whence $\xi \in Y$, as required.

Lemma 6. *Let L be the p-Hilbert class field of F. Let the integers e and $k \geqslant 0$ be defined by $F \cap K_\infty = K_e$ and $L \cap F_\infty = F_k$. Then $N_{F/K}(U_1) = V^{p^{e+k}}$.*

Proof. For each prime $\mathfrak{g}$ of F_n above $\mathfrak{p}$, let $U_{\mathfrak{g},1}(n)$ be the units $\equiv 1 \bmod \mathfrak{g}$ in the completion of F_n at $\mathfrak{g}$. Then, with k as defined in the statement of the lemma, the norm map from $U_1(k) = \prod_{\mathfrak{g}|\mathfrak{p}} U_{\mathfrak{g},1}(k)$ to U_1 is surjective. This is because F_k/F is unramified, and the norm map for an unramified extension of local fields is surjective on the units (and so also surjective when its domain and range are restricted to the units $\equiv 1$). It follows that

$$N_{F/K}(U_1) = N_{F_k/K}(U_1(k)) .$$

But, as F_k contains K_{k+e}, the group on the right is contained in $N_{k+e}(V_{k+e}) = V^{p^{k+e}}$ (by Lemma 4). Therefore $N_{F/K}(U_1)$, being a closed subgroup of finite index of V, is of the form V^{p^r}, where $r \geqslant e + k$. We now proceed to show that we must have $r = e + k$. We do this by showing that every element of $G(F_{r-e}/F_k)$ is 1. Let σ be any element of $G(F_{r-e}/F_k)$, and put $t = r - e$. Since $L \cap F_t = F_k$, there exists $\tau \in G(LF_t/L)$ whose restriction to F_t is σ. As

τ fixes L, class field theory shows that there exists $\xi \in U_1$ such that $(\xi, LF_t/F) = \tau$, whence $(\xi, F_t/F) = \sigma$. Now, since the restriction map from $G(F_t/F_k)$ to $G(K_r/K_{k+e})$ is injective, it suffices to show that the restriction of σ to K_r is 1. But this restriction is the Artin symbol $(N_{F/K}\xi, K_r/K)$, and this is certainly 1 because, by hypothesis, $N_{F/K}\xi$ belongs to $V^{p^r} = N_r(V_r)$. Thus σ is indeed 1, and the proof is complete.

We now make some index computations. For each $\mathfrak{g} \in \mathcal{S}$, let $F_\mathfrak{g}$ be the completion of F at $\mathfrak{g}$, $\mathcal{O}_\mathfrak{g}$ the ring of integers of $F_\mathfrak{g}$, and $e_\mathfrak{g}$ the ramification index of $F_\mathfrak{g}$ over $K_\mathfrak{p}$. Choose an integer $t \geqslant 0$ such that $p^{-t}\mathcal{O}_\mathfrak{g}$ contains $\log U_{\mathfrak{g},1}$ for each $\mathfrak{g} \in \mathcal{S}$. Define

$$\Omega = \prod_{\mathfrak{g}\in\mathcal{S}} (p^{-t}\mathcal{O}_\mathfrak{g}) , \qquad \log U_1 = \prod_{\mathfrak{g}\in\mathcal{S}} (\log U_{\mathfrak{g},1}) .$$

For each $\mathfrak{g} \in \mathcal{S}$, let $w_\mathfrak{g}$ denote the order of the group of p-power roots of unity in $F_\mathfrak{g}$. Finally, we recall that d is the degree of F over K.

Lemma 7. $[\Omega : \log U_1] = p^{td} \prod_{\mathfrak{g}\in\mathcal{S}} (w_\mathfrak{g} N\mathfrak{g})$, *where* $N\mathfrak{g}$ *is the absolute norm of* $\mathfrak{g}$.

Proof. Fix $\mathfrak{g} \in \mathcal{S}$. The kernel of the logarithm map on $U_{\mathfrak{g},1}$ is the group of p-power roots of unity of $F_\mathfrak{g}$. On the other hand, if we define $r = [e_\mathfrak{g}/(p-1)] + 1$, and let $U_{\mathfrak{g},r}$ denote the units $\equiv 1 \bmod \mathfrak{g}^r$, then the restriction of the logarithm map to $U_{\mathfrak{g},r}$ defines an isomorphism from $U_{\mathfrak{g},r}$ onto $\mathfrak{g}^r$. Therefore the kernel of the map from $U_{\mathfrak{g},1}/U_{\mathfrak{g},r}$ onto $(\log U_{\mathfrak{g},1})/(\log U_{\mathfrak{g},r})$, which is induced by the logarithm, can be identified with the group of p-power roots of unity in $F_\mathfrak{g}$. Thus

$$[\log U_{\mathfrak{g},1} : \mathfrak{g}^r] = (N\mathfrak{g})^{r-1}/w_\mathfrak{g} ,$$

whence

$$[p^{-t}\mathcal{O}_\mathfrak{g} : \log U_{\mathfrak{g},1}] = (N\mathfrak{g})^{1+te_\mathfrak{g}} w_\mathfrak{g} .$$

Since $\mathfrak{p}$ is of degree 1, we have $N_\mathfrak{g} = p^{f_\mathfrak{g}}$, where $f_\mathfrak{g}$ is the residue class degree of $\mathfrak{g}$ over $\mathfrak{p}$. Thus, taking the product over all $\mathfrak{g} \in \mathcal{S}$, and recalling that $\sum_{\mathfrak{g}\in\mathcal{S}} e_\mathfrak{g} f_\mathfrak{g} = d$, the assertion of the lemma follows.

Let $\mathcal{E}_1$ be the group of global units of F, which are $\equiv 1 \bmod \mathfrak{g}$ for each $\mathfrak{g} \in \mathcal{S}$. The torsion in $\mathcal{E}_1$ is the group of p-power roots of unity in F, and $\mathcal{E}_1$ modulo torsion is a free $\boldsymbol{Z}$-module of rank $d-1$. Let $\varphi : F \to \prod_{\mathfrak{g}\in\mathcal{S}} F_\mathfrak{g}$ be the canonical embedding. We define D to be the $\boldsymbol{Z}_p$-submodule of U_1 which is generated by $\varphi(\mathcal{E}_1)$ and $\varphi(\varepsilon_d)$, where, as before, $\varepsilon_d = 1 + p$. We write $\log D$ for the subset of $\log U_1$, which is obtained by applying the log map to each component of the vectors in D. Let $|\ |_p$ denote the valuation of $\boldsymbol{C}_p$, normalized so that $|p|_p = p^{-1}$.

Lemma 8. *The index of* $\log D$ *in* $\log U_1$ *is finite if and only if* $R_\mathfrak{p} \neq 0$. *If* $R_\mathfrak{p} \neq 0$, *then* $[\log U_1 : \log D]$ *is equal to the inverse of the p-adic valuation of*

$$\frac{dpR_\mathfrak{p}}{\sqrt{\Delta_\mathfrak{p}}} \prod_{\mathfrak{g}\in\mathcal{S}} (w_\mathfrak{g} N\mathfrak{g})^{-1} .$$

Proof. For each $\mathfrak{g} \in \mathcal{S}$, let $\varphi_\mathfrak{g}$ be the canonical embedding of F in $F_\mathfrak{g}$, $d_\mathfrak{g} = [F_\mathfrak{g} : \boldsymbol{Q}_p]$, and $\alpha_1^{(\mathfrak{g})}, \cdots, \alpha_{d_\mathfrak{g}}^{(\mathfrak{g})}$ a $\boldsymbol{Z}_p$-basis of $\mathcal{O}_\mathfrak{g}$. If $\varepsilon_1, \cdots, \varepsilon_{d-1}$ are representatives of a $\boldsymbol{Z}$-basis of $\mathcal{E}_1$ modulo torsion, we have

$$\log \varphi_\mathfrak{g}(\varepsilon_j) = \sum_{k=1}^{d_\mathfrak{g}} a_{jk}^{(\mathfrak{g})} p^{-t} \alpha_k^{(\mathfrak{g})} \qquad (1 \leqslant j \leqslant d) , \tag{5}$$

where the $a_{jk}^{(\mathfrak{g})}$ belong to $\boldsymbol{Z}_p$. Let A be the $d \times d$ matrix formed from the $a_{jk}^{(\mathfrak{g})}$ $(1 \leqslant j \leqslant d,\ 1 \leqslant k \leqslant d_\mathfrak{g},\ \mathfrak{g} \in \mathcal{S})$. Then, since $\log D$ is generated as a $\boldsymbol{Z}_p$-module by the $\log \varphi(\varepsilon_j)$ $(1 \leqslant j \leqslant d)$, it follows that the index of $\log D$ in Ω is either infinite, or finite and equal to the exact power of p dividing $\det A$, according as $\det A$ is 0 or is not 0. To compute $\det A$, let φ_j $(1 \leqslant j \leqslant d)$ run, as before, through the distinct embeddings of F in $\boldsymbol{C}_p$ which correspond to primes in $\mathcal{S}$, and let $\sigma_j^{(\mathfrak{g})}$ $(1 \leqslant j \leqslant d_\mathfrak{g})$ run through the distinct embeddings of $F_\mathfrak{g}$ in $\boldsymbol{C}_p$. Let $\Xi_\mathfrak{g}$ be the $d_\mathfrak{g} \times d_\mathfrak{g}$ matrix formed from the $\sigma_j^{(\mathfrak{g})}\alpha_k^{(\mathfrak{g})}$ $(1 \leqslant j, k \leqslant d_\mathfrak{g})$, and let Ξ be the direct sum of the $\Xi_\mathfrak{g}$ for $\mathfrak{g} \in \mathcal{S}$ (i.e. the $d \times d$ matrix with the blocks $\Xi_\mathfrak{g}$, for $\mathfrak{g} \in \mathcal{S}$, down the diagonal, and zeros outside these blocks). Let Θ be the $d \times d$ matrix formed from the $\log \varphi_k(\varepsilon_j)$ $(1 \leqslant j,\ k \leqslant d)$. It follows from (5) that $\Theta = A\Xi$. Since the index of $\mathcal{E}_1$ in $\mathcal{E}$ is prime to p, we deduce immediately from the definition of $R_\mathfrak{p}$ that $\det \Theta = (d \log \varepsilon_d) R_\mathfrak{p} u$, where u is a unit in $\mathcal{O}_\mathfrak{p} = \boldsymbol{Z}_p$. Also, by the definition of the local discriminant, the power of p occurring in $(\det \Xi_\mathfrak{g})^2$ is $p^{-2td_\mathfrak{g}}$ times the power of p occurring in the local discriminant $\mathfrak{D}_\mathfrak{g}$ of $F_\mathfrak{g}$ over $K_\mathfrak{p}$. But, in our earlier notation, we have

$$\Delta_{F/K}\mathcal{O}_\mathfrak{p} = \Delta_\mathfrak{p}\mathcal{O}_\mathfrak{p} = \prod_{\mathfrak{g}\in\mathcal{S}} \mathfrak{D}_\mathfrak{g} ,$$

where $\Delta_{F/K}$ is the relative discriminant of F over K. It follows that the power of p dividing $(\det \Xi)^2$ is the same as that dividing $p^{-2td}\Delta_\mathfrak{p}$. The first assertion of the lemma is now plain since $\log U_1$ has finite index in Ω. Moreover, assuming that $R_\mathfrak{p} \neq 0$, we conclude that

$$[\Omega : \log D] = |(d \log(\varepsilon_d) p^{td} R_\mathfrak{p}) / \sqrt{\Delta_\mathfrak{p}}|_p^{-1} .$$

Noting that the p-adic valuation of $\log \varepsilon_d$ is p^{-1}, the assertion of the lemma now follows from Lemma 7.

Lemma 9. *The index of D in U_1 is finite if and only if $R_\mathfrak{p} \neq 0$. If $R_\mathfrak{p} \neq 0$, then $[U_1 : D]$ is equal to the inverse of the p-adic valuation of*

$$\frac{dpR_\mathfrak{p}}{\omega_F \sqrt{\Delta_\mathfrak{p}}} \prod_{\mathfrak{g} \in \mathcal{S}} (N\mathfrak{g})^{-1} ,$$

where ω_F is the number of roots of unity in F.

Proof. The first assertion is plain. Assuming $R_\mathfrak{p} \neq 0$, we have the commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & D & \longrightarrow & U_1 & \longrightarrow & U_1/D & \longrightarrow & 0 \\ & & \downarrow \log & & \downarrow \log & & \downarrow & & \\ 0 & \longrightarrow & \log D & \longrightarrow & \log U_1 & \longrightarrow & \log U_1/\log D & \longrightarrow & 0 ; \end{array}$$

the kernel of the vertical map on the left is the group of p-power roots of unity in F, and the kernel of the middle vertical map is the product over all $\mathfrak{g} \in \mathcal{S}$ of the group of p-power roots of unity in $F_\mathfrak{g}$. It now follows from the snake lemma, and Lemma 8, that U_1/D has the desired order.

The Z_p-submodule of U_1 which is generated by $\varphi(\mathscr{E}_1)$ is, of course, simply the closure $\overline{\varphi(\mathscr{E}_1)}$ of $\varphi(\mathscr{E}_1)$ in U_1 in the p-adic topology. Since $p \neq 2$, and p does not ramify in K, each element of $\mathscr{E}_1$ has norm from F to K equal to 1. Thus Lemma 5 shows that $\overline{\varphi(\mathscr{E}_1)}$ is contained in $Y \cap U_1$.

Lemma 10. *The index of $\overline{\varphi(\mathscr{E}_1)}$ in $Y \cap U_1$ is finite if and only if $R_\mathfrak{p} \neq 0$. If $R_\mathfrak{p} \neq 0$, this index is equal to the inverse of the p-adic valuation of*

$$\frac{p^{e+k+1} R_\mathfrak{p}}{\omega_F \sqrt{\Delta_\mathfrak{p}}} \prod_{\mathfrak{g} \in \mathcal{S}} (1 - (N\mathfrak{g})^{-1}) ,$$

where the integers e and k are as defined in Lemma 6.

Proof. The first assertion is plain, and so we assume that $R_\mathfrak{p} \neq 0$. By Lemma 6, and the definition of D, we have the commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & Y \cap U_1 & \longrightarrow & U_1 & \xrightarrow{N_{F/K}} & V^{p^{e+k}} & \longrightarrow & 0 \\ & & \cup & & \cup & & \uparrow & & \\ 0 & \longrightarrow & \overline{\varphi(\mathscr{E}_1)} & \longrightarrow & D & \xrightarrow{N_{F/K}} & V^d & \longrightarrow & 0 . \end{array}$$

By Lemma 5, we have $D \cap Y = \overline{\varphi(\mathscr{E}_1)}$, whence the vertical map on the extreme right is clearly injective. Applying the snake lemma, and noting that $N\mathfrak{g} - 1$ is prime to p for $\mathfrak{g} \in \mathcal{S}$, Lemma 10 now follows from Lemma 9.

We can now derive the main result of these index calculations. Recall that K is any imaginary quadratic field, p is an odd prime number, which does not divide the class number of K, and which splits in K, and $\mathfrak{p}$ is one of the factors of (p) in K. Also, F is an arbitrary finite extension of K, and $\mathcal{S}$ the set of primes of F lying above $\mathfrak{p}$.

Theorem 11. *Let M be the maximal abelian p-extension of F, which is unramified outside $\mathcal{S}$. Then $G(M/F_\infty)$ is finite if and only if $R_\mathfrak{p} \neq 0$. If $R_\mathfrak{p} \neq 0$, the order of $G(M/F_\infty)$ is equal to the inverse of the p-adic valuation of*

$$\frac{p^{e+1} h_F R_\mathfrak{p}}{\omega_F \sqrt{\Delta_\mathfrak{p}}} \prod_{\mathfrak{g} \in \mathcal{S}} (1 - (N\mathfrak{g})^{-1}) ,$$

where h_F is the class number of F, ω_F is the number of roots of unity of F, and the integer e is defined by $F \cap K_\infty = K_e$.

Proof. Let J denote the idèle group of F. For each finite prime $\mathfrak{g}$, let $U_\mathfrak{g}$ be the units in the completion of F at $\mathfrak{g}$. For each archimedean prime $\mathfrak{g}$, let $U_\mathfrak{g}$ be the full multiplicative group of the completion of F at $\mathfrak{g}$. Put $U_\mathcal{S} = \prod_{\mathfrak{g} \notin \mathcal{S}} U_\mathfrak{g}$, the product being taken over all archimedean primes, and all non-archimedean primes not in $\mathcal{S}$. We can view $U_\mathcal{S}$ as a subgroup of J in the natural way, and we let $\overline{F^\times U_\mathcal{S}}$ be the closure of $F^\times U_\mathcal{S}$ in the idèle topology. Let $\mathfrak{m}$ be the maximal abelian extension of F, which is unramified outside $\mathcal{S}$. By class field theory, the Artin map induces an isomorphism

$$(6) \qquad J/(\overline{F^\times U_\mathcal{S}}) \xrightarrow{\sim} G(\mathfrak{m}/F) .$$

Now let C be the idèle class group of F, and let M be as defined in the theorem. Thus M is the maximal p-extension of F contained in $\mathfrak{m}$. Let ψ be the Artin map from C onto $G(M/F)$. Let L be the p-Hilbert class field of F. It follows from (6) by a standard argument that ψ maps U_1 onto $G(M/L)$, and that the kernel of ψ restricted to U_1 is precisely $\overline{\varphi(\mathscr{E}_1)}$. In addition, if $\xi \in C$, then

$\psi(\xi)$ fixes F_∞ if and only if ξ is in $Y = \bigcap_{n\geqslant 0} N_{F_n/F}C_n$. Thus, as $Y \cap \overline{\varphi(\mathscr{E}_1)} = \overline{\varphi(\mathscr{E}_1)}$ by Lemma 5, it follows that ψ induces an isomorphism

$$(Y \cap U_1)/\overline{\varphi(\mathscr{E}_1)} \xrightarrow{\sim} G(M/LF_\infty) .$$

Theorem 11 now follows from Lemma 10, since

$$G(LF_\infty/F_\infty) \xrightarrow{\sim} G(L/F_\infty \cap L) ,$$

and the order of this latter group is $|h/p^k|_p^{-1}$, by the definition of k.

Before proceeding to the second part of the proof of Theorem 1, we digress briefly to indicate a possible interpretation of Theorem 11 in terms of Iwasawa modules. Let M_∞ be the maximal abelian p-extension of F_∞, which is unramified outside the primes of F_∞ lying above primes in $\mathscr{S}$. Put $X_\infty = G(M_\infty/F_\infty)$. Then $\Gamma = G(F_\infty/F)$ operates on X_∞ via inner automorphisms in the usual manner. Thus, if we fix a topological generator of Γ, X_∞ is a Λ-module in a natural way, where $\Lambda = \boldsymbol{Z}_p[[T]]$ is the ring of formal power series in an indeterminate T with coefficients in $\boldsymbol{Z}_p$. It can easily be shown that X_∞ is a finitely generated Λ-module. Very probably, two further results are true about the structure of X_∞ as a Λ-module, but these are unknown at present. Firstly, X_∞ is probably always Λ-torsion (this can be proven when F is abelian over K). Secondly, it seems likely that X_∞ has no non-zero Λ-submodule of finite cardinality. If these two facts were known for X_∞, then we could interpret Theorem 11 as giving a p-adic residue formula for a function derived from the characteristic polynomial of X_∞ in a natural way (see Appendix 1 of [1], where an analogous result is established when F is a totally real number field).

We now come to the second part of the proof of Theorem 1. We begin by recalling the results of Katz [6], [7] and Lichtenbaum [9], upon which this second part of the argument is based. At present, this work has only been completely carried out when K has class number 1, and so we assume from now on that this is the case. As in the Introduction, let $\pi = \psi(\mathfrak{p})$, so that π is a generator of the ideal $\mathfrak{p}$. As before, let E_π be the kernel of multiplication by π on E, and put $\mathscr{F} = K(E_\pi)$. Let G be the Galois group of $\mathscr{F}$ over K, and let

$$\theta : G \longrightarrow (\boldsymbol{Z}/p\boldsymbol{Z})^\times \tag{7}$$

be the canonical character giving the action of G on E_π, i.e. θ is defined by

$u^\sigma = \theta(\sigma)u$ for all $u \in E_\pi$ and all $\sigma \in G$. Since E has good reduction at $\mathfrak{p}$ by hypothesis, it is well known that θ is an isomorphism. Again, let $\mathfrak{R}_0$ be the ray class field of K modulo $\mathfrak{p}$, so that $\mathfrak{R}_0 \subset \mathscr{F}$, and $[\mathscr{F} : \mathfrak{R}_0] = \omega$, where ω denotes the number of roots of unity in K. Thus, if we identify $(\boldsymbol{Z}/p\boldsymbol{Z})^\times$ with the group of $(p-1)$-th roots of unity in $\boldsymbol{Z}_p^\times$ in the natural way, we see that

$$X = \{\theta^{k\omega} : k = 1, \cdots, (p-1)/\omega - 1\}$$

is the set of all non-trivial characters, with values in $\boldsymbol{Z}_p^\times$, of the Galois group of $\mathfrak{R}_0$ over K. To each $\varphi \in X$, Katz and Lichtenbaum have associated a p-adic L-function, which we denote by $L_p(s, \varphi)$. Actually, $L_p(s, \varphi)$ is not uniquely determined by φ, but also depends on the choice of certain parameters associated with the elliptic curve E (see the discussion in [9]). However, these additional choices do not affect the properties of $L_p(s, \varphi)$ used in the proof of Theorem 1, and so we neglect them. Let A denote the ring of integers of a sufficiently large finite extension of the completion of the maximal unramified extension of $\boldsymbol{Q}_p$, and let Λ_A be the ring of formal power series in an indeterminate T with coefficients in A. Then it is shown in either [6] or [9] that the $L_p(s, \varphi)$ are holomorphic in the following strong sense. For each $\varphi \in X$, there exists $H(T, \varphi)$ in Λ_A, such that

$$L_p(s, \varphi) = H((1+p)^s - 1, \varphi) \qquad \text{for all } s \text{ in } \boldsymbol{Z}_p . \tag{8}$$

The two key properties of the $L_p(s, \varphi)$ used in the proof of Theorem 1 are summarized in the following theorem.

Theorem 12 (Katz, Lichtenbaum). (i) *Suppose that j is an integer such that θ^j belongs to X. Then, for each integer $k \geqslant 1$ with $k \equiv j \bmod (p-1)$, we have $L_p(\theta^j, 1-k) = \alpha_k L^*(\psi^k, k)$, where α_k is a unit in A.* (ii). *If h is the class number of $\mathfrak{R}_0$, and $R_\mathfrak{p}, \Delta_\mathfrak{p}$ are the invariants of $\mathfrak{R}_0/K$ defined earlier, then*

$$\prod_{\varphi \in X} L_p(1, \varphi) = \beta h R_\mathfrak{p}/\sqrt{\Delta_\mathfrak{p}} , \tag{9}$$

where β is a unit in A.

The deepest part of this theorem is (9), which is established in [9]. Its proof is based on an explicit formula, due to Katz [7], for $L_p(1, \varphi)$ in terms of the p-adic logarithms of elliptic units.

We now prove Theorem 1. In Theorem 11, we take F to be the ray class field $\mathfrak{R}_0$ modulo $\mathfrak{p}$. In this case, $\mathfrak{R}_0/K$ is totally ramified at $\mathfrak{p}$, so that $\mathscr{S}$ consists of a single prime whose absolute norm is p. Also $e = 0$, and $\mathfrak{R}_0$

contains no non-trivial p-power roots of unity (because the conjugate of $\mathfrak{p}$ is not ramified in $\mathfrak{R}_0/K$). In addition, the p-adic analogue of Baker's theorem on linear forms in the logarithms of algebraic numbers shows that $R_{\mathfrak{p}} \neq 0$. Thus, if M denotes the maximal abelian extension of $\mathfrak{R}_0$, which is unramified outside $\mathscr{S}$, and whose Galois group is a pro-p-group, Theorem 11 tells us that the order of $G(M/F_\infty)$ is equal to

$$|hR_{\mathfrak{p}}/\sqrt{\Delta_{\mathfrak{p}}}|_{\mathfrak{p}}^{-1}\,, \tag{10}$$

where h is the class number of $\mathfrak{R}_0$. Since each $L_p(1,\varphi)$ is in A by (8), it follows from (9) that $G(M/F_\infty) = 0$ if and only if $L_{\mathfrak{p}}(1,\varphi)$ is a unit for each $\varphi \in X$. But, by (8) and (i) of Theorem 12, this latter assertion is valid if and only if p divides none of the numbers (3). On the other hand, since $G(F_\infty/F)$ has no torsion, it is clear that $G(M/F_\infty) = 0$ if and only if there is no cyclic extension of $F = \mathfrak{R}_0$ of degree p, unramified outside $\mathscr{S}$, other than the first layer of F_∞/F. Since the first layer of F_∞/F is the ray class field $\mathfrak{R}_1$ of K modulo $\mathfrak{p}^2$, the proof of Theorem 1 is complete.

References

[1] Coates, J., p-adic L-functions and Iwasawa's theory, to appear in Proceedings of symposium on algebraic number theory held in Durham, England, September, 1975, A.P., London.

[2] Coates, J. and Wiles, A., On the conjecture of Birch and Swinnerton-Dyer, to appear in Invent. Math.

[3] Greenberg, R., A generalization of Kummer's criterion, Invent. Math., **21** (1973), 247–254.

[4] Hurwitz, A., Über die Entwicklungskoeffizienten der lemniskatischen Funktionen, Math. Ann., **51** (1899), 196–226 (=Werke II, 342–373).

[5] Iwasawa, K., Lectures on p-adic L-functions, Ann. Math. Studies, **74**, Princeton U.P., Princeton, 1972.

[6] Katz, N., The Eisenstein measure and p-adic interpolation, to appear in Amer. J. Math.

[7] ——, p-adic interpolation of real analytic Eisenstein series, to appear.

[8] Lang, H., Kummersche Kongruenzen fur die normierten Entwicklungskoeffizienten der Weierstrasschen $\mathfrak{p}$-Funktionen. Abh. Math. Sem. Hamburg, **33**, (1969), 183–196.

[9] Lichtenbaum, S., On p-adic L-functions associated to elliptic curves, to appear.

[10] Vishik, M. M. and Manin, J. I., p-adic Hecke series for imaginary quadratic fields, Math. Sbornik, **95** (137), No. 3 (11) (1974), 357–383.

[11] Novikov, A. P., On the regularity of prime ideals of degree 1 of an imaginary quadratic field, Izv. Akad. Nauk. Seria Math. **33** (1969), 1059–1079.

[12] Robert, G., Nombres de Hurwitz et Unités Elliptiques, to appear.

[13] Serre, J.-P., Cohomologie galoisienne, Lecture Notes in Math., **5**, Springer, Berlin, 1964.

[14] Shimura, G., Introduction to the arithmetic theory of automorphic functions, Pub. Math. Soc. Japan, **11** Iwanami, Tokyo and Princeton U.P., Princeton, 1971.

[15] Weil, A., On a certain type of characters of the idèle class group of an algebraic number field, Proc. Int. Symp. Tokyo-Nikko, 1955, 1–7, Science Council of Japan, Tokyo, 1956.

Department of Pure Mathematics
and Mathematical Statistics
University of Cambridge
16 Mill Lane
Cambridge, CB2 1SB
England

ALGEBRAIC NUMBER THEORY, Papers contributed for the International Symposium, Kyoto 1976; S. Iyanaga (Ed.): Japan Society for the Promotion of Science, Tokyo, 1977

Symplectic Local Constants and Hermitian Galois Module Structure

ALBRECHT FRÖHLICH

Introduction

Let N/K be a normal extension of algebraic number fields, always of finite absolute degree, with Galois group Γ and let $\mathfrak{O}$ be the ring of algebraic integers in N. Under the hypothesis that N/K is tame, I established in some recent work a connection between the Galois module structure of $\mathfrak{O}$ on the one hand, and the Artin root numbers and Galois Gauss sums appearing in the functional equation of Artin L-functions, and also the Artin conductor on the other hand (cf. [F3], [F4]). The present paper complements this theory. I shall now establish, under a local tameness hypothesis, a connection between the local structure of $\mathfrak{O}$ as a "Hermitian Galois module" on the one hand and the local root numbers of Langlands (we follow the exposition in [T]), the local Galois Gauss sums (cf. [M]) and the local conductors, for symplectic characters of Γ on the other hand. The deepest results are those on root numbers. The interpretation of these, for symplectic characters, on the local level, implies one on the global level, which goes a good deal further than that obtained earlier without the additional element of structure given by the Hermitian form. (Compare e.g. Theorem 14 in [F3], or Theorem 5 [F4] and the discussion in § 5 of [F4].) We moreover derive a "Hermitian interpretation" for the conductors of *all* charactors, generalising the classical one for the discriminant.

The basic notion of a Hermitian module used here is wider than that in which topologists have been interested. Thus e.g. such a module over $Z(\Gamma)$ is given by a locally free module M together with a non-degenerate Hermitian form on $M \otimes_Z Q$ over $Q(\Gamma)$. We shall take the general theory of these only as far as is needed for the immediate purpose, defining in particular the appropriate local, and adelic, class groups. The basic tool here is the Pfaffian associated with a symplectic character.

The particular form in our case is defined via the relative trace and has been considered already in [F1] and [F2]. The link between Pfaffians on the one hand and Galois Gauss sums (or conductors) on the other is provided by the generalized resolvent, and we shall use again the fundamental theorem of [F3].

1. Pfaffians of matrices

Notation. For any ring R, the ring of n by n matrices is $M_n(R)$, and the group of invertible elements is R^*. Thus $M_n(R)^* = GL_n(R)$. $M_n(R)$ acts from the right on the product R^n of n copies of R.

Let F be a field of characteristic $\neq 2$. An involution (involutory antiautomorphism) j of $M_n(F)$ is said to be *symplectic* if it is the adjoint involution of some skew form (non-degenerate skew-symmetric bilinear form) $h: F^n \times F^n \to F$, i.e. we have

$$h(vP, w) = h(v, wP^j) , \qquad \text{all } v, w \in F^n, \text{ all } P \in M_n(F) .$$

Let h and j be as above. If $S \in GL_n(F)$ is j-symmetric (i.e. $S = S^j$) then

$$S = P^j P , \tag{1.1}$$

for some $P \in GL_n(F)$. For $S = I$ the identity matrix, this implies $\det(P) = 1$. Hence in general the determinant

$$\det(P) = Pf^j(S) \tag{1.2}$$

only depends on S. It is its *Pfaffian*. Immediately

$$Pf^j(S)^2 = \mathrm{Det}(S) , \qquad \text{hence } Pf^j(S) \in F^* . \tag{1.3}$$

Also

$$Pf^j(I) = 1 , \qquad Pf^j(P^j S P) = \mathrm{Det}(P) Pf^j(S) , \tag{1.4}$$

for $P, S \in GL_n(F)$, S being j-symmetric.

Next let h' be a further skew-form on F^m, with adjoint involution j'. Write $j \perp j'$ for the adjoint involution of the orthogonal sum $h \perp h'$. If $S \in GL_n(F)$ is j-symmetric, $S' \in GL_m(F)$ is j'-symmetric then

$$Pf^{j \perp j'}\left(\begin{pmatrix} S & 0 \\ 0 & S' \end{pmatrix}\right) = Pf^j(S) Pf^{j'}(S') , \tag{1.5}$$

where the matrix on the left is of course $j \perp j'$-symmetric.

Now let $b: F^q \times F^q \to F$ be a non-singular pairing and let $k: GL^q(F) \to GL^q(F)$ be defined by $b(vT, w) = b(v, wT^k)$, for all $v, w \in F^q$, all $T \in GL_q(F)$.

We get a skew form h on F^{2q}, given by

$$h((v_1, v_2), (w_1, w_2)) = b(v_1, w_2) - b(w_1, v_2)$$

$(v_i, w_i \in F^q)$, and with respect to its adjoint involution j we get

$$Pf^j\left(\begin{pmatrix} T & 0 \\ 0 & T^k \end{pmatrix}\right) = \mathrm{Det}(T) , \tag{1.6}$$

where $T \in GL_q(F)$ and the matrix on the left is j-symmetric.

Next let k, j be two symplectic involutions of $M_n(F)$ so that for all P, and for some fixed $C \in GL_n(F)$,

$$C^{-1} P^j C = (C^{-1} P C)^k$$

(i.e. k and j are *equivalent*). If $S \in GL_n(F)$ is j-symmetric, then $C^{-1}SC$ is k-symmetric and

$$Pf^k(C^{-1}SC) = Pf^j(S) . \tag{1.7}$$

Let σ be an automorphism of F, extended to $M_n(F)$. Given j there is a symplectic involution

$$\begin{cases} k = \sigma^{-1} j \sigma , & \text{or} \\ \sigma k = j \sigma , \end{cases} \tag{1.8}$$

and with S as before,

$$Pf^k(S^\sigma) = (Pf^j(S))^\sigma . \tag{1.9}$$

The same applies to any embedding $\sigma: F \to E$ of fields (taking the second line in (1.8))

Let now A be a central simple F-algebra with involution i. Let E be a separable algebraic extension field of F and

$$g: A \otimes_F E \cong M_n(E)$$

an isomorphism of E-algebras. The equations

$$g(a^i \otimes 1) = g(a \otimes 1)^j$$

define an involution j of $M_n(E)$. If it is symplectic (and this property does not depend on E or on g) write

$$Pf^i(a) = Pf^j(a \otimes 1) .$$

By (1.7) and (1.9) (both for $\sigma: F \to E$ and for automorphisms of E) and by the

Skolem-Noether theorem, Pf^i is independent of choices and has values in F^*. If in particular A is a quaternion algebra with i as standard involution then the symmetric elements in A^* are the $c1_A, c \in F^*$ and

$$Pf^i(c1_A) = c \ . \tag{1.10}$$

Next let B be a commutative F-algebra. Extend the symplectic involution j of $M_n(F)$ to $M_n(B) = M_n(F) \otimes_F B$, letting it act trivially on B. If B is a product of fields then for any j-symmetric $S \in GL_n(B)$ the Pfaffian $Pf^j(S)$ is defined in the same way as before and lies in B^*. The same applies to certain subalgebras of products of fields and in all these cases the results of this section remain essentially valid. An important case is that of the adele ring $B = Ad(F)$ when F is a number field. Details are left to the reader.

2. Pfaffians for group rings

Throughout Γ is a finite group whose group ring over a commutative ring B will be denoted by $B(\Gamma)$. The symbol $\bar{Q}$ stands for the algebraic closure of Q in C. The term character is used in the sense of representation theory over $\bar{Q}$, i.e. each representation $T: \Gamma \to GL_n(\bar{Q})$ has an associated character $\chi: \Gamma \to \bar{Q}$. If B is a commutative K-algebra, K always a subfield of $\bar{Q}$, we can extend T to an algebra homomorphism

$$B(\Gamma) = K(\Gamma) \otimes_K B \longrightarrow M_n(\bar{Q}) \otimes_K B \longrightarrow M_n(\bar{Q} \otimes_K B) \ ,$$

and further to

$$T: M_q(B(\Gamma)) \longrightarrow M_q(M_n(\bar{Q} \otimes_K B)) = M_{nq}(\bar{Q} \otimes_K B) \ . \tag{2.1}$$

Now take determinants and restrict to invertible elements. Thus

$$\det_\chi(a) = \det(T(a)) \in (\bar{Q} \otimes_K B)^* \ , \qquad (a \in GL_q(B(\Gamma))) \tag{2.2}$$

only depends on the character χ associated with T. Let R_Γ be the additive group of functions on Γ generated by the characters, the group of "virtual characters". The function $\det_\chi(a)$ then extends to $\chi \in R_\Gamma$ by linearity. (For all this see [F3] (AI).)

We shall write $a \to \bar{a}$ for the standard involution on group rings which leaves the base ring elementwise fixed and takes $\gamma \in \Gamma$ into γ^{-1}. The character χ associated with a representation T is *symplectic* if the $T(\gamma)$ leave some skew-form h on $\bar{Q}^n$ invariant, i.e. if

$$h(vT(\gamma), wT(\gamma)) = h(v, w) \ , \qquad \text{for all } v, w \in Q^n, \text{ all } \gamma \in \Gamma \ . \tag{2.3}$$

This is equivalent with

$$T(\bar{a}) = T(a)^j \ , \qquad \text{for all } a \in K(\Gamma) \tag{2.4}$$

($K \subset \bar{Q}$), where j is the adjoint involution of h.

This last equation can be extended to T on $B(\Gamma)$ (B always a K-algebra) and then further to T as in (2.1). For the latter we need the concept of a *matrix extension of an involution* i of a ring A. This is the involution of $M_q(A)$, again denoted by i, for which

$$P^i(r, s) = (P(s, r))^i \ , \tag{2.5}$$

where $P(r, s)$ is the r, s entry of the matrix P. In other words we involute the entries and then transpose. (2.4) will now hold for the matrix extension of $^-$ to $M_q(B(\Gamma))$ and of j to $M_q(M_n(\bar{Q} \otimes_K B))$.

Assume in the sequel that (2.4) holds in the extended sense and that B is a product of fields, or $B = Ad(K)$ with K a number field (i.e. of finite degree over Q). For $a \in GL_q(B(\Gamma))$, with $a = \bar{a}$, we now get an element $Pf^j(T(a)) \in (\bar{Q} \otimes_K B)^*$. We shall show that this only depends on the character χ associated with T, not on T itself or j, and we may thus write

$$Pf^j(T(a)) = Pf_\chi(a) \ . \tag{2.6}$$

Indeed let T' be a further representation with the same character χ, leaving invariant a skew-form h' with adjoint involution j'. There then exists $C \in GL_n(\bar{Q})$ with

$$T'(\gamma) = C^{-1}T(\gamma)C \ , \qquad \text{for all } \gamma \ ,$$
$$h'(v, w) = h(vC^{-1}, wC^{-1}) \ , \qquad \text{for all } v, w \in \bar{Q}^n \ ,$$

(see e.g. [FM] for a proof in slightly different language) and hence

$$(C^{-1}PC)^{j'} = C^{-1}P^jC \ , \qquad \text{for all } P \in M_n(\bar{Q}) \ .$$

This extends also to $M_{nq}(\bar{Q} \otimes_K B)$. By (1.7), $Pf^{j'}(T'(a)) = Pf^j(T(a))$.

If χ and ψ are symplectic characters then so is $\chi + \psi$ and, by (1.5),

$$Pf_{\chi+\psi}(a) = Pf_\chi(a)Pf_\psi(a) \ . \tag{2.7}$$

Thus the map $\chi \to Pf_\chi(a)$ extends to the subgroup R^s_Γ of R_Γ generated by the symplectic characters and (2.7) goes over. Further properties of Pf_χ are deduced first for actual symplectic characters and then always extended to R_Γ by linearity.

Let in the sequel a be a symmetric element of $GL_q(B(\Gamma))$. By (1.3),

(2.8) $$Pf_\chi(a)^2 = \det_\chi(a) .$$

By (1.4), for $b \in GL_q(B(\Gamma))$,

(2.9) $$Pf_\chi(1) = 1 , \qquad Pf_\chi(\bar{b}ab) = \det_\chi(b) Pf_\chi(a) ,$$

and so in particular

(2.10) $$\mathrm{Pf}_\chi(\bar{b}b) = \det_\chi(b) .$$

For $\phi \in R_\Gamma$ with $\bar{\phi}$ the complex conjugate, or contragredient, we have $\phi + \bar{\phi} \in R_\Gamma^s$, and then by (1.6)

(2.11) $$Pf_{\phi+\bar{\phi}}(a) = \det_\phi(a) .$$

Thus the determinants of symmetric elements, or "discriminants" are known once the Pfaffians are. Next let a' be a symmetric element of $GL_m(B(\Gamma))$. By (1.5),

(2.12) $$Pf_\chi\left(\begin{pmatrix} a & 0 \\ 0 & a' \end{pmatrix}\right) = Pf_\chi(a) Pf_\chi(a') .$$

Now let σ be an automorphism of $\bar{Q}$, extended to some automorphism of $\bar{Q} \otimes_K B$, and to $B(\Gamma)$ (so that σ leaves the elements of Γ fixed.). We shall prove that

(2.13) $$(Pf_{\chi^{\sigma^{-1}}}(a))^\sigma = Pf_\chi(a^\sigma) .$$

In fact let

$$a = \sum a_\gamma \otimes \gamma , \qquad a_\gamma \in M_q(B) .$$

Let T be a representation with character χ. Then

$$T(a) = \sum a_\gamma \otimes T(\gamma) , \qquad T(\gamma) \in M_n(\bar{Q}) .$$

Also

$$a^\sigma = \sum a_\gamma^\sigma \otimes \gamma , \qquad T(a^\sigma) = \sum a_\gamma^\sigma \otimes T(\gamma) ,$$

as T on $M_q(B(\Gamma)) = M_q(B) \otimes_K K(\Gamma)$ is defined by linearity from $\Gamma \to GL_n(\bar{Q})$. Now the representation $T^{\sigma^{-1}}: \Gamma \to GL_n(\bar{Q})$ with $T^{\sigma^{-1}}(\gamma) = T(\gamma)^{\sigma^{-1}}$ has character $\chi^{\sigma^{-1}}$. Thus we get $T(a^\sigma) = (\sum a_\gamma \otimes T^{\sigma^{-1}}(\gamma))^\sigma = (T^{\sigma^{-1}}(a))^\sigma$. By (1.9) we now get (2.13).

From now on for the remainder of this paper, let K be a number field and write $\Omega_K = \mathrm{Gal}(\bar{Q}/K)$. If $\sigma \in \Omega_K$ then we may assume that σ fixes B elementwise. By (2.7) and (2.13), the map

(2.14) $$Pf(a): \chi \longrightarrow Pf_\chi(a)$$

lies in $\mathrm{Hom}_{\Omega_K}(R_\Gamma^s, (\bar{Q} \otimes_K B)^*)$. We shall consider two cases. Firstly when $B = K_\mathfrak{p}$ is the (semilocal) completion of K at a prime divisor $\mathfrak{p}$ of some subfield of K, we write $\bar{Q} \otimes_K K_\mathfrak{p} = \bar{Q}_\mathfrak{p}$. Next we also need the case $B = Ad(K)$, the adele ring. Then we write $(\bar{Q} \otimes_K Ad(K))^* = J(\bar{Q})$. This is indeed the union of the idele groups $J(L)$ for number fields $L \subset \bar{Q}$.

Remark. For both the above choices of B one can show that all elements of the group $\mathrm{Hom}_{\Omega_K}(R_\Gamma^s, (\bar{Q} \otimes_K B)^*)$ are of form $Pf(a)$, $a \in GL_q(B(\Gamma))$ for some q, and that the group is generated by such elements with q fixed.

3. Class groups

Let R be a Dedekind domain, with quotient field F. A Hermitian $R(\Gamma)$-module is a pair (M, b) where M is a locally free $R(\Gamma)$-module of finite rank and $b: V \times V \to F(\Gamma)$ is a non-degenerate Hermitian form on the $F(\Gamma)$-module V spanned by M, with respect to the standard involution of $F(\Gamma)$.

With K as before, let $\mathfrak{o}$ be the ring of algebraic integers of K. If $\mathfrak{p}$ is a prime divisor of K, or of a subfield of K, denote by $K_\mathfrak{p}$ the completion of K at $\mathfrak{p}$. The symbol $\mathfrak{o}_\mathfrak{p}$ stands for the completion of $\mathfrak{o}$ at $\mathfrak{p}$ if $\mathfrak{p}$ is finite, and $\mathfrak{o}_\mathfrak{p} = K_\mathfrak{p}$ if $\mathfrak{p}$ infinite. The *Hermitian class group* of $\mathfrak{o}_\mathfrak{p}(\Gamma)$ is defined as

(3.1) $$HCl(\mathfrak{o}_\mathfrak{p}(\Gamma)) = \mathrm{Hom}_{\Omega_K}(R_\Gamma^s, \bar{Q}_\mathfrak{p}^*) / \mathrm{Det}^s(\mathfrak{o}_\mathfrak{p}(\Gamma)^*) .$$

Here we recall (cf. (2.2) that the map $\chi \mapsto \det_\chi(a)$ $(a \in \mathfrak{o}_\mathfrak{p}(\Gamma)^*)$, with $\chi \in R_\Gamma^s$ is an Ω_K-homomorphism into $\bar{Q}_\mathfrak{p}^*$. Denote it by $\mathrm{Det}^s(a)$. Thus Det^s is a homomorphism $\mathfrak{o}_\mathfrak{p}(\Gamma)^* \to \mathrm{Hom}_{\Omega_K}(R_\Gamma^s, \bar{Q}_\mathfrak{p}^*)$, and the denominator on the right hand side of (3.1) is its image. We also define the *adelic Hermitian class group* of $\mathfrak{o}(\Gamma)$ by

(3.2) $$AHCl(\mathfrak{o}(\Gamma)) = \mathrm{Hom}_{\Omega_K}(R_\Gamma^s, J(\bar{Q})) / \mathrm{Det}^s(U(\mathfrak{o}(\Gamma))) .$$

Here $U(\mathfrak{o}(\Gamma)) = \prod_\mathfrak{p} \mathfrak{o}_\mathfrak{p}(\Gamma)^*$ (product over all prime divisors of K), with the denominator on the right hand defined analogously to that in (3.1). The embedding $\bar{Q}_\mathfrak{p}^* \to J(\bar{Q})$ yields an embedding

(3.3) $$i_{\mathfrak{o},\mathfrak{p}}: HCl(\mathfrak{o}_\mathfrak{p}(\Gamma)) \subset AHCl(\mathfrak{o}(\Gamma)) .$$

Let (M, b) be a Hermitian $\mathfrak{o}_\mathfrak{p}(\Gamma)$-module of rank q, say with a $\mathfrak{o}_\mathfrak{p}(\Gamma)$-basis $\{v_l\}$. Then $(b(v_l, v_k))$ is a symmetric matrix in $GL_q(K_\mathfrak{p}(\Gamma))$, under the matrix extension of the standard involution of $K_\mathfrak{p}(\Gamma)$, hence (cf. (2.14)) defines an element $Pf((b(v_l, v_k)))$ of $\mathrm{Hom}_{\Omega_K}(R_\Gamma^s, \bar{Q}_\mathfrak{p}^*)$, whose class $c(M, b) \in HCl(\mathfrak{o}_\mathfrak{p}(\Gamma))$ indeed

only depends on (M, b). By (2.12) the *classinvariants* $c(M, b)$ define a homomorphism of the Grothendieck group of Hermitian $\mathfrak{o}_\mathfrak{p}(\Gamma)$-modules into $HCl(\mathfrak{o}_\mathfrak{p}(\Gamma))$ which, by the remark in § 2, is surjective.

An *adelic Hermitian* $\mathfrak{o}(\Gamma)$*-module* is a pair (M, b), where M is a free $\prod_\mathfrak{p} \mathfrak{o}_\mathfrak{p}(\Gamma)$-module (product over all primedivisors of K) of finite rank, and b is a non-degenerate Hermitian form $V \times V \to Ad(K)(\Gamma)$ spanned by M. "Non-degenerate" here means that for any basis $\{v_k\}$ of M over $\prod_\mathfrak{p} \mathfrak{o}_\mathfrak{p}(\Gamma)$, the $\mathfrak{p}$-components of the matrix $(b(v_k, v_l))$ should lie in $GL(K_\mathfrak{p}(\Gamma))$, for all $\mathfrak{p}$, and in $GL(\mathfrak{o}_\mathfrak{p}(\Gamma))$ for almost all $\mathfrak{p}$. As in the local case we get a class invariant $c(M, b) \in AHCl(\mathfrak{o}(\Gamma))$, namely the class of $Pf((b(v_k, v_l))$, with $\{v_k\}$ a basis of M. The $\mathfrak{p}$-component $(M_\mathfrak{p}, b_\mathfrak{p})$ is a Hermitian $\mathfrak{o}_\mathfrak{p}(\Gamma)$-module and $c(M, b)_\mathfrak{p} = c(M_\mathfrak{p}, b_\mathfrak{p})$. Moreover the embedding (3.3) corresponds to a functor $(M, b) \mapsto (\tilde{M}, \tilde{b})$ from Hermitian $\mathfrak{o}_\mathfrak{p}(\Gamma)$-modules to adelic Hermitian $\mathfrak{o}(\Gamma)$-modules. If say M is of rank m over $\mathfrak{o}_\mathfrak{p}(\Gamma)$ we put $\tilde{M}_\mathfrak{p} = M$, $\tilde{b}_\mathfrak{p} = b$ with $M_\mathfrak{q} = \mathfrak{o}_\mathfrak{q}(\Gamma)^m$, $\tilde{b}_\mathfrak{q}$ being given by the multiplication in $\mathfrak{o}_\mathfrak{q}(\Gamma)$, for $\mathfrak{q} \neq \mathfrak{p}$.

An Hermitian $\mathfrak{o}(\Gamma)$-module (M, b) yields by tensoring with $\prod \mathfrak{o}_\mathfrak{p}(\Gamma)$ an adelic Hermitian $\mathfrak{o}(\Gamma)$-module, and we define its adelic invariant

$$Ac(M, b) \in AHCl(\mathfrak{o}(\Gamma))$$

by

$$Ac(M, b) = c\Big(\prod_\mathfrak{p} M_\mathfrak{p}, \prod_\mathfrak{p} b_\mathfrak{p}\Big) .$$

This yields again a homomorphism from the appropriate Grothendieck group into $AHCl(\mathfrak{o}(\Gamma))$.

Remark 1. This homomorphism is not in general surjective. In other words not every element of $AHCl(\mathfrak{o}(\Gamma))$ is of form $Ac(M, b)$. The theorem that the ideal class of a quadratic form discriminant is a square is a special case of this restriction. On the other hand, by the remark in § 2, every element in $HCl(\mathfrak{o}_\mathfrak{p}(\Gamma))$ is a class invariant.

Remark 2. One can define a class group $HCl(\mathfrak{o}(\Gamma))$, and class invariants yielding a surjective homomorphism from the Grothendieck group of Hermitian $\mathfrak{o}(\Gamma)$-modules to $HCl(\mathfrak{o}(\Gamma))$. The adelic invariant in turn gives then rise to a homomorphism $HCl(\mathfrak{o}(\Gamma)) \to AHCl(\mathfrak{o}(\Gamma))$ whose kernel and cokernel provide global information. Moreover one gets a homomorphism from $HCl(\mathfrak{o}(\Gamma))$ to the ordinary class group $Cl(\mathfrak{o}(\Gamma))$ which plays a central role in theory of Galois module structure (cf. [F3], [F4]). All this will be dealt with elsewhere.

Let now $U(L)$ be the group of unit ideles of a number field L, i.e. of ideles whose components at all finite prime divisors are units. Going to the limit we get a subgroup $U(\bar{Q})$ of $J(\bar{Q})$. The surjection $J(\bar{Q}) \to J(\bar{Q})/U(\bar{Q})$ (the "group of fractional ideals") yields a homomorphism

$$AHCl(\mathfrak{o}(\Gamma)) \longrightarrow \mathrm{Hom}_{\Omega_K}(R^s_\Gamma, J(\bar{Q})/U(\bar{Q})) . \tag{3.4}$$

We shall write $\chi \mapsto \mathfrak{g}((M, b)\chi)$ for the image of $c(M, b)$ under this map, both for Hermitian $\mathfrak{o}(\Gamma)$-modules and for Hermitian $\mathfrak{o}_\mathfrak{p}(\Gamma)$-modules (using the embedding (3.3)).

4. Norm and restriction of scalars

Let k be a subfield of K, and $\{\sigma\}$ always in the sequel a right transversal of Ω_K in Ω_k. We have a natural homomorphism

$$\mathcal{N}_{K/k} : \mathrm{Hom}_{\Omega_K}(R^s_\Gamma, X) \longrightarrow \mathrm{Hom}_{\Omega_k}(R^s_\Gamma, X)$$

given by

$$\mathcal{N}_{K/k} f(\chi) = \prod_\sigma f(\chi^{\sigma^{-1}})^\sigma$$

(in multiplicative notation for X). Write $\mathfrak{o}_k$ for the ring of algebraic integers in k. We adopt the same notation for completions of k as previously for K. In this section $\mathfrak{p}$ will always stand for a prime divisor of $\mathfrak{o}_k$. The map $\mathcal{N}_{K/k}$ for $X = \bar{Q}^*_\mathfrak{p}$, or $X = J(\bar{Q})$, will take $\mathrm{Det}^s(\mathfrak{o}_\mathfrak{p}(\Gamma)^*)$ into $\mathrm{Det}^s(\mathfrak{o}_{k,\mathfrak{p}}(\Gamma)^*)$, respectively $\mathrm{Det}^s(U(\mathfrak{o}(\Gamma)))$ into $\mathrm{Det}^s(U(\mathfrak{o}_k(\Gamma)))$. where we continue to write $\mathfrak{o}$ for $\mathfrak{o}_K$ (cf. [F3] (A6 Proposition 1)). We thus get induced homomorphisms

$$\mathcal{N}_{K/k} : \begin{cases} HCl(\mathfrak{o}_\mathfrak{p}(\Gamma)) \longrightarrow HCl\,(\mathfrak{o}_{k,\mathfrak{p}}(\Gamma)) , \\ AHC(\mathfrak{o}(\Gamma)) \longrightarrow AHCl(\mathfrak{o}_k(\Gamma)) , \end{cases} \tag{4.1}$$

which commute with taking components at $\mathfrak{p}$ and with embeddings (3.3).

We extend the trace map $t_{K/k} : K \to k$ to k-algebras: $t_{K/k} : K \otimes_k A \to A = k \otimes_k A$, given by $t_{K/k}(c \otimes a) = \sum_\sigma c^\sigma \otimes a$. Let now (M, b) be a Hermitian $\mathfrak{o}(\Gamma)$ — (or $\mathfrak{o}_\mathfrak{p}(\Gamma)$—) module. Restricting scalars to $\mathfrak{o}_k(\Gamma)$ (or to $\mathfrak{o}_{k,\mathfrak{p}}(\Gamma)$) we get a Hermitian $\mathfrak{o}_k(\Gamma)$ — (or $\mathfrak{o}_{k,\mathfrak{p}}(\Gamma)$—) module $(M, t_{K/k}b)_{\mathfrak{o}_{k,\mathfrak{p}}}$ where $t_{K/k}b(v, w) = t_{K/k}(b(v, w))$. Analogously for adelic modules.

4.1. Proposition. *Let (M, b) be a Hermitian $\mathfrak{o}_\mathfrak{p}(\Gamma)$-module. With $\{\sigma\}$ as above, let $\{c_i\}$ be an $\mathfrak{o}_{k,\mathfrak{p}}$-basis of $\mathfrak{o}_\mathfrak{p}$. If $c(M, b)$ is represented by $f \in \mathrm{Hom}_{\Omega_K}(R^s_\Gamma, \bar{Q}^*_\mathfrak{p})$ then $c(M, t_{K/k}b)_{\mathfrak{o}_{k,\mathfrak{p}}}$ is represented by the map*

(4.2) $$\chi \longmapsto \mathcal{N}_{K/k} f(\chi) \cdot (\det c_i^\sigma)^{\deg(\chi) r(M)} ,$$

where $\deg(\chi)$ *is the degree of* χ *and* $r(M)$ *the* $\mathfrak{o}_\mathfrak{p}(\Gamma)$*-rank of* M.

Corollary. *The corresponding result for adelic modules and for the adelic invariants* $Ac(M, b)$ *of global modules.*

Details and proof of Corollary: Exercise.

Proof of 4.1. There is a basis $\{v_r\}$ $(r = 1, \cdots, q)$ $(q = r(M))$ of M over $\mathfrak{o}_\mathfrak{p}(\Gamma)$ so that for all $\chi \in R_\Gamma^s$

(4.3) $$f(\chi) = Pf_\chi(b(v_r, v_t)) .$$

Thus $c(M, t_{K/k} b)_{\mathfrak{o}_k, \mathfrak{p}}$ is represented by f', where

(4.4) $$f'(\chi) = Pf_\chi((t_{K/k}(c_l b(v_r, v_t) c_i))) ,$$

the matrix on the right having row index (l, r), column index (i, t) with $r, t = 1, \cdots, q$ and $l, i = 1, \cdots, m$, $(m = [K : k])$.

Next let $(\alpha_{l,s,\sigma,r})$ be the matrix with row index (l, s), column index (σ, r), where $r, s = 1, \cdots, q$, $\{\sigma\}$ as before and $l = 1, \cdots, m$, and where

$$\alpha_{l,s,\sigma,r} = c_l^\sigma \delta_{r,s} \qquad (\delta \text{ the Kronecker symbol}) .$$

Viewing this as a matrix in $M_{mq}(K_\mathfrak{p}(\Gamma))$ we compute

(4.5) $$\det_\chi((\alpha_{l,s,\sigma,r})) = \det((c_l^\sigma))^{\deg(\chi) r(M)}$$

We moreover define a matrix $(\beta_{\sigma,r,\rho,t})$ over $K_\mathfrak{p}(\Gamma)$ with row index (σ, r), column index (ρ, t), with $r, t = 1, \cdots, q$, with σ and ρ running through the given transversal of Ω_K in Ω_k, and with

$$\beta_{\sigma,r,\rho,t} = b(v_r, v_t)^\sigma \delta_{\sigma,\rho} .$$

This matrix, viewed as a block matrix is formed by blocks $(b(v_r, v_t)^\sigma)$ down the main diagonal, indexed by σ, and zero blocks elsewhere. Hence by (2.12)

$$Pf_\chi((\beta_{\sigma,r,\rho,t})) = \prod_\sigma Pf_\chi((b(v_r, v_t)^\sigma))$$

and so by (2.13)

(4.6) $$Pf_\chi((\beta_{\sigma,r,\rho,t})) = \prod_\sigma (Pf_{\chi\sigma^{-1}}((b(v_r, v_t)))^\sigma) .$$

Now one verifies the matrix equation

$$(t_{K/k}(c_l b(v_r, v_t) c_i)) = (\alpha_{l,s,\sigma,r})(\beta_{\sigma,r,\rho,t})\overline{(\alpha_{l,s,\sigma,r})} .$$

By (2.9), and (4.3)–(4.6) we verify that $f'(\chi)$ is indeed given by the right hand side of (4.2), as we had to show.

Let $d(K)$ be the absolute discriminant of K. Applying the Proposition to the case $k = Q$ we can use

(4.7) $$\det(c_i^\sigma)^{\deg(\chi)} = d(K)_p^{\deg(\chi)/2}$$

where we recall that $\deg(\chi)$ is always even for $\chi \in R_\Gamma^s$. Correspondingly for adelic invariants in the global case we get a term $d(K)^{\deg(\chi)/2}$.

Remark. One can also apply the proposition to a properly local restriction of scalars. Let the prime divisor $\mathfrak{p}$ of K lie above the rational prime divisor p. Fix an embedding $Q_p \to K_\mathfrak{p}$. From a Hermitian $\mathfrak{o}_\mathfrak{p}(\Gamma)$-module (M, b) we obtain by restriction of scalars, via the above embedding, a Hermitian $Z_p(\Gamma)$-module $(M, t_{K_\mathfrak{p}/Q_p} b)$. Let $d(K_\mathfrak{p})$ be a basis discriminant for $\mathfrak{o}_\mathfrak{p}/Z_p$, and let f represent $c(M, b)$. Then (in $\mathrm{Hom}_{\Omega_Q}(R_\Gamma^s, \overline{Q}_p^*)$, or in $\mathrm{Hom}_{\Omega_Q}(R_\Gamma^s, J(\overline{Q}))$ the map $\chi \mapsto \mathcal{N}_{K/Q} f(\chi) \cdot d(K_\mathfrak{p})^{r(M)\deg(\chi)/2}$ represents $(M, t_{K_\mathfrak{p}/Q_p} b)$.

To see this let k be the decomposition field of $\mathfrak{p}$. We thus have a unique prime divisor of k below $\mathfrak{p}$ and an isomorphism $Q_p \cong k_\mathfrak{p}$ reflecting the given embedding. Now one applies the proposition to K/k. Thus e.g. $\mathrm{t}_{K_\mathfrak{p}/Q_p} b = t_{K/k} b$. One then observes that $\overline{Q}_p^*$ is the Ω_Q-module induced by the Ω_k-module $\overline{Q}_\mathfrak{p}^*$ and that we thus get an isomorphism

$$\mathrm{Hom}_{\Omega_k}(R_\Gamma^s, \overline{Q}_\mathfrak{p}^*) \cong \mathrm{Hom}_{\Omega_Q}(R_\Gamma^s, \overline{Q}_p^*)$$

which takes $\mathcal{N}_{K/k} f$ into $\mathcal{N}_{K/Q} f$, for all $f \in \mathrm{Hom}_{\Omega_K}(R_\Gamma^s, \overline{Q}_\mathfrak{p}^*)$. The details are omitted.

5. Traceform and resolvents

We now assume that we are given a surjective homomorphism with open kernel

(5.1) $$\pi : \Omega_K \longrightarrow \Gamma ,$$

i.e. an isomorphism

(5.2) $$\Gamma \cong \mathrm{Gal}(N/K)$$

where N is the fixed field of $\mathrm{Ker}\,\pi$. Thus $\mathrm{Gal}(N/K)$-modules become Γ-modules.

For every subfield k of K we get a non-degenerate Hermitian form ("trace form")

$$b_{\pi,k} = b_{N,k} \qquad \text{(abuse of notation)}$$

on N over $k(\Gamma)$, given by

$$b_{N/k}(x,y) = \sum_{\tau} t_{N/k}(x^{\tau}y)\gamma^{-1} . \tag{5.3}$$

Hence

$$b_{N/k} = t_{K/k} b_{N/K} . \tag{5.4}$$

More generally if B is a is a commutative k-algebra we get a form on $N \otimes_k B$ over $B(\Gamma)$, which for simplicity's sake we shall again denote by $b_{N/k}$.

Let now in particular B be a commutative K-algebra. Then $N \otimes_K B$ is free of rank one over $B(\Gamma)$, say on a free generator a. On the one hand we have then the resolvent $(a|\chi)$ $(\chi \in R_\Gamma)$, given by (cf. [F3] § 1)

$$(a|\chi) = \det_\chi (\sum a^{\tau}\gamma^{-1}) .$$

On the other hand $b_{N/K}(a,a)$ will be a symmetric element of $B(\Gamma)^*$, and we thus have the Pfaffian $Pf_\chi(b_{N/K}(a,a))$, for $\chi \in R_\Gamma^s$.

Theorem 1. *For all* $\chi \in R_\Gamma^s$,

$$Pf_\chi(b_{N/K}(a,a)) = (a|\chi) .$$

Proof. Verify that

$$b_{N/K}(a,a) = \overline{\sum a^{\tau}\gamma^{-1}} \cdot \sum a^{\tau}\gamma^{-1}$$

and use (2.10).

In the sequel $\mathfrak{O}$ is always the ring of algebraic integers in N, and as before $\mathfrak{o}$ that in K. A prime divisor $\mathfrak{p}$ of K is said to be *tame* in N if it is finite and at most tamely ramified in N, or if it is infinite.

Corollary 1. *Let* $\mathfrak{p}$ *be a prime divisor of* K *which is tame in* N. *Let* $a\mathfrak{o}_\mathfrak{p}(\Gamma) = \mathfrak{O}_\mathfrak{p}$. *Then* $c(\mathfrak{O}_\mathfrak{p}, b_{N/K})$ *is represented by*

$$x \longmapsto (a|\chi) .$$

Corollary 2. *Suppose* N/K *is tame. Let* $a \prod_\mathfrak{p} \mathfrak{o}_\mathfrak{p}(\Gamma) = \prod_\mathfrak{p} \mathfrak{O}_\mathfrak{p}$ *(product over all prime divisors of* K*). Then* $Ac(\mathfrak{O}, b_{N/K})$ *is represented by*

$$\chi \longmapsto (a|\chi) .$$

We get similar descriptions after restriction of scalars, using Proposition 4.1. In this context we shall always use the notation

$$\mathcal{N}_{K/k}(a|\chi) = \prod_{\sigma} (a|\chi^{\sigma^{-1}})^{\sigma} , \tag{5.5}$$

if $\{\sigma\}$ is a right transversal of Ω_K in Ω_k.

6. Relation with Artin conductors

Write $\mathfrak{f}(N/K,\chi)$ for the Artin conductor of $\chi \in R_\Gamma$, and $\mathfrak{f}_\mathfrak{p}(N/K,\chi)$ for the local Artin conductor at a prime ideal $\mathfrak{p}$ of $\mathfrak{o}$.

Theorem 2. *Let* $\mathfrak{p}$ *be a prime ideal of* $\mathfrak{o}$, *tame in* N. *Then for all* $\chi \in R_\Gamma^s$

$$\mathfrak{g}((\mathfrak{O}_\mathfrak{p}, b_{N/K}), \chi)^2 = \mathfrak{f}_\mathfrak{p}(N/K,\chi) .$$

(For the definition of $\mathfrak{g}$ *see the end of* § 3.)

Corollary 1. *If* N/K *is tame, then for all* $\chi \in R_\Gamma^s$

$$\mathfrak{g}((\mathfrak{O}, b_{N/K}), \chi)^2 = \mathfrak{f}(N/K,\chi) .$$

Note that if $\phi \in R_\Gamma$, then $\phi + \bar{\phi} \in R_\Gamma^s$, and $\mathfrak{f}_\mathfrak{p}(N/K,\phi) = \mathfrak{f}_\mathfrak{p}(N/K,\bar{\phi})$. Thus we get

Corollary 2. (i) *Let* $\mathfrak{p}$ *be a prime ideal of* K *tame in* N. *Then for all* $\phi \in R_\Gamma$

$$\mathfrak{f}_\mathfrak{p}(N/K,\phi) = \mathfrak{g}((\mathfrak{O}_\mathfrak{p}, b_{N/K}), \phi + \bar{\phi}) .$$

(ii) *Suppose* N/K *is tame. Then for all* $\phi \in R_\Gamma$

$$\mathfrak{f}(N/K,\phi) = \mathfrak{g}((\mathfrak{O}, b_{N/K}), \phi + \bar{\phi}) .$$

The theorem and Corollary 1 give a determination of the ideals $\mathfrak{g}$ for $\mathfrak{O}_\mathfrak{p}, b_{N/K}$ and for $\mathfrak{O}, b_{N/K}$ in terms of Artin conductors. One knows that, under the hypothesis of tameness, local conductors of symplectic characters are ideal squares of $\mathfrak{o}$. Hence by Theorem 2, the $\mathfrak{g}((\mathfrak{O}_\mathfrak{p}, b_{N/K}), \chi)$ are actually ideals of $\mathfrak{o}$.

On the other hand, Corollary 2 gives, under a tameness hypothesis, a description of conductors or local conductors for *all* $\chi \in R_\Gamma$, in terms of the Hermitian invariants $\mathfrak{g}$, generalising the classical description of discriminants in terms of the trace form.

Remark on notation. Strictly speaking we should have written $\mathfrak{g}((\mathfrak{O}_\mathfrak{p}, b_{N/K}), \chi) = \mathfrak{g}_{\pi,\mathfrak{p}}(\chi)$, $\mathfrak{f}_\mathfrak{p}(N/K,\chi) = \mathfrak{f}_{\pi,\mathfrak{p}}(\chi)$, and analogously in the global case. For, all these ideals depend on π (in (5.11)) and on χ. In the context of the present paper such a strict adherence to a formal notation is not necessary, as on a whole π is fixed. But for a proper understanding of our results it is important to be clear about their precise scope. Thus e.g. Theorem 2 asserts that for

all π "tame above a given $\mathfrak{p}$" the two maps $\chi \mapsto \mathfrak{f}_{\pi,\mathfrak{p}}(\chi)$, and $\chi \mapsto \mathfrak{g}_{\pi,\mathfrak{p}}(\chi)^2$ coincide —the first given by ramification, the second by Hermitian structure. In other words the tame local conductors are "Hermitian invariants".—Similar remarks apply to the contents of subsequent sections.

Proof of Theorem 2. By Theorem 1, and [F3] (Theorem 18).

7. Relation to Galois Gauss sums

Let $U_+(L)$ be the group of ideles of a number field L which are units at all finite prime divisors and are real and positive at all infinite ones, including the complex ones. This is more restrictive than the usual definition of "totally positive elements", but has the advantage of being independent of the choice of reference field L. Write $U_+(\bar{Q})$ for the union of the $U_+(L)$, all $L \subset \bar{Q}$. Note that $\mathrm{Det}^s(U(Z(\Gamma))) \subset \mathrm{Hom}_{\mathfrak{Q}_Q}(R_\Gamma^s, U_+(\bar{Q}))$. Thus the group $AHCl(Z(\Gamma))$ has a subgroup

$$G(\Gamma) = \mathrm{Hom}_{\mathfrak{Q}_Q}(R_\Gamma^s, Q^*)\,\mathrm{Hom}_{\mathfrak{Q}_Q}(R_\Gamma^s, U_+(\bar{Q}))/\mathrm{Det}^s(U(Z(\Gamma)))\ . \tag{7.1}$$

As

$$\mathrm{Hom}_{\mathfrak{Q}_Q}(R_\Gamma^s, Q^*) \cap \mathrm{Hom}_{\mathfrak{Q}_Q}(R_\Gamma^s, U_+(\bar{Q})) = 1\ ,$$

we have in fact a direct product

$$G(\Gamma) = \mathrm{Hom}_{\mathfrak{Q}_Q}(R_\Gamma^s, Q^*) \times [\mathrm{Hom}_{\mathfrak{Q}_Q}(R_\Gamma^s, U_+(\bar{Q}))/\mathrm{Det}^s(U(Z(\Gamma)))]\ . \tag{7.2}$$

In the sequel let ρ_i denote the projection on the i-th factor.

We shall write $W(N/K, \chi)$ for the Artin root number, i.e. the constant in the functional equation of the Artin L-function, and $W_\mathfrak{p}(N/K, \chi)$ for Langlands' local constants. Also $\tau(N/K, \chi)$ is the Galois Gauss sum and $\tau_\mathfrak{p}(N/K, \chi)$ the local Galois Gauss sum (cf. [T] and [M]). We know that if $\mathfrak{p}$ is finite and tame in N/K and $\chi \in R_\Gamma^s$ then $\tau_\mathfrak{p}(N/K, \chi) \in Q^*$ and $W_\mathfrak{p}(N/K, \chi) = \pm 1$ (cf. [M] (II, § 6)) or [F3] Theorem 9). Observing that $\det_z(\Gamma) = 1$, we deduce from the definition of $\tau_\mathfrak{p}$ that

$$W_\mathfrak{p}(N/K, \chi) = \mathrm{sign}\,\tau_\mathfrak{p}(N/K, \chi)\ . \tag{7.3}$$

Theorem 3. *Let $\mathfrak{p}$ be a prime divisor of K, tame in N. Then*

$$\mathcal{N}_{K/Q}c(\mathfrak{Q}_\mathfrak{p}, b_{N/K}) \in G(\Gamma)\ ,$$

and $\rho_1\mathcal{N}_{K/Q}c(\mathfrak{Q}_\mathfrak{p}, b_{N/K})$ is the map

$$\chi \longmapsto \begin{cases} \tau_\mathfrak{p}(N/K, \chi)W_\mathfrak{p}(N/K, \chi) & (\mathfrak{p}\ \textit{finite})\ , \\ W_\mathfrak{p}(N/K, \chi) & (\mathfrak{p}\ \textit{infinite})\ . \end{cases}$$

Proof. By [F3] (Theorem 4.10), (7.3) and Theorem 1 above.

Corollary 1. *Suppose N/K is tame. Then*

$$\mathcal{N}_{K/Q}Ac(\mathfrak{Q}, b_{N/K}) \in G(\Gamma)\ ,$$

and $\rho_1\mathcal{N}_{K/Q}Ac(\mathfrak{Q}, b_{N/K})$ is the map

$$\chi \longmapsto \tau(N/K, \chi)W(N/K, \chi)\ .$$

Remark. The interpretation of $\mathcal{N}_{K/Q}Ac(\mathfrak{Q}, b_{N/K})$ as "essentially" the adelic invariant of $(\mathfrak{Q}, t_{K/Q}b_{N/K})$ over $Z(\Gamma)$ is immediate from Proposition 4.1. Following the remark in § 4 we also get a similar interpretation for $\mathcal{N}_{K/Q}c(\mathfrak{Q}_\mathfrak{p}, b_{N/K})$, $\mathfrak{p}$ a prime divisor of K.

Corollary 2. *Let $\mathfrak{p}$ be a prime divisor of K tame in N. Let a $\mathfrak{o}_\mathfrak{p}(\Gamma) = \mathfrak{Q}_\mathfrak{p}$. Then $\rho_2\mathcal{N}_{K/Q}c(\mathfrak{Q}_\mathfrak{p}, b_{N/K})$ has a representative $u_\mathfrak{p}$, so that if $u_{\mathfrak{p},l}(\chi)$ denotes the semi local component of $u_\mathfrak{p}(x)$ at the finite rational prime divisor l, we have*

$$\begin{aligned} u_{\mathfrak{p},l}(\chi) &= W_\mathfrak{p}(N/K, \chi)_l,\ \mathfrak{p}\ \textit{infinite}\ , \\ u_{\mathfrak{p},l}(\chi) &= W_\mathfrak{p}(N/K, \chi)_l\tau_\mathfrak{p}(N/K, \chi)_l^{-1},\ \mathfrak{p}\ \textit{finite},\ \mathfrak{p} \nmid l\ , \\ u_{\mathfrak{p},l}(\chi) &= W_\mathfrak{p}(N/K, \chi)_l\tau_\mathfrak{p}(N/K, \chi)_l^{-1}\mathcal{N}_{K/Q}(a\,|\,\chi),\ \mathfrak{p} \mid l\ . \end{aligned}$$

This follows from from Theorem 3 and the observation that $\mathcal{N}_{K/Q}(a\,|\,\chi)_l = 1$, if $\mathfrak{p} \nmid l$.

8. Relations to root numbers

Let l be a prime number. $\mathrm{Ker}\,d_l$ is the kernel in R_Γ of "reduction mod l". More precisely

$$\mathrm{Ker}\,d_l = [\chi \in R_\Gamma\,|\,\chi(\gamma) = 0 \quad \text{if } (\mathrm{order}\,(\gamma), l) = 1]\ .$$

In the present section we restrict l to be an odd prime, except in some concluding remarks.

If $\chi \in R_\Gamma^s \cap \mathrm{Ker}\,d_l$ then for any finite $\mathfrak{p}$ of K, tame in N, $\tau_\mathfrak{p}(N/K, \chi)$ is a unit at l and

$$\tau_\mathfrak{p}(N/K, \chi) \equiv 1 \pmod{l} \tag{8.1}$$

(cf. [F3] (Theorem 13)), whence beside the characterisation of $W_\mathfrak{p}(N/K, \chi)$ as a

signature at infinity (cf. (7.3)), we now get for these χ a characterisation by congruences mod l, namely

$$W_{\mathfrak{p}}(N/K, \chi) \equiv N\mathfrak{f}_{\mathfrak{p}}(N, K, \chi)^{1/2} \pmod{l}\ , \tag{8.2}$$

for $\mathfrak{p}$ as above. Here $N\mathfrak{f}_{\mathfrak{p}}$ is the absolute norm of $\mathfrak{f}_{\mathfrak{p}}$, which we know to be a rational square. It is (8.1), or equivalently (8.2), which lies behind the characterisation of local root numbers, for $\chi \in R_\Gamma^s \cap \operatorname{Ker} d_l$, as Hermitian invariants. In addition we need a corresponding statement for resolvents. Let $\mathfrak{p}$ be a prime divisor in K, tame in N, and let $a\mathfrak{o}_{\mathfrak{p}}(\Gamma) = \mathfrak{D}_{\mathfrak{p}}$. The idele $\mathcal{N}_{K/Q}(a\,|\,\chi)$ is a unit above l and

$$\mathcal{N}_{K/Q}(a\,|\,\chi) \equiv 1 \pmod{\mathfrak{L}} \tag{8.3}$$

where $\mathfrak{L}$ is the product of prime divisors above l in some suitable field E, e.g. $E = Q(\chi)$, the field obtained by adjoining the values $\chi(\gamma)$ to Q. If $\mathfrak{p}$ does not lie above l then the semilocal component of $\mathcal{N}_{K/Q}(a\,|\,\chi)$ at l is 1, hence (8.3) holds trivially. Otherwise see [F3] (Theorem 12).

For any number field L, let $V_l(L) = (\mathfrak{o}_L/\mathfrak{L}_L)^*$ where $\mathfrak{o}_L$ is the ring of algebraic integers in L, $\mathfrak{L}_L$ the product of its prime ideals above l. Let $V_l(\bar{Q})$ be the limit of the $V_l(L)$. If g is a homomorphism $R_\Gamma^s \to U_+(\bar{Q})$ write $r_l g$ for the composition

$$R_\Gamma^s \cap \operatorname{Ker} d_l \longrightarrow R_\Gamma^s \longrightarrow U_+(\bar{Q}) \xrightarrow{\bmod \mathfrak{L}} V_l(\bar{Q})\ .$$

If $g \in \operatorname{Det}^s(U(Z(\Gamma)))$ then actually $r_l g = 1$ (cf. [F3] (AIII Proposition 2)). Thus the map r_l in turn yields a homomorphism

$$\operatorname{Hom}_{\mathfrak{Q}_Q}(R_\Gamma^s, U_+(\bar{Q}))/\operatorname{Det}^s(U(Z(\Gamma))) \longrightarrow \operatorname{Hom}_{\mathfrak{Q}_Q}(R_\Gamma^s \cap \operatorname{Ker} d_l, V_l(\bar{Q}))\ ,$$

and composing with ρ_2 (cf. (7.2)) we get a homomorphism

$$h_l : G(\Gamma) \longrightarrow \operatorname{Hom}_{\mathfrak{Q}_Q}(R_\Gamma^s \cap \operatorname{Ker} d_l, V_l(\bar{Q}))\ . \tag{8.4}$$

By Corollary 2 to Theorem 3, by (8.1) and (8.3), we conclude that

$$h_l \mathcal{N}_{K/Q} c(\mathfrak{D}_{\mathfrak{p}}, b_{N/K})$$

(for $\mathfrak{p}$ a prime divisor in K tame in N) is represented by the map

$$\chi \longmapsto W_{\mathfrak{p}}(N/K, \chi) \pmod{l}\ . \tag{8.5}$$

To give a neat formal statement of this result let $T(R_\Gamma)$ by the subgroup

of R_Γ of virtual characters $T(\phi) = \phi + \bar{\phi}$. Then $R_\Gamma^s \supset T(R_\Gamma) \supset 2R_\Gamma^s$. We have a homomorphism

$$k_l : \operatorname{Hom}_{\mathfrak{Q}_Q}(R_\Gamma^s/T(R_\Gamma), \pm 1) \longrightarrow \operatorname{Hom}_{\mathfrak{Q}_Q}(R_\Gamma^s \cap \operatorname{Ker} d_l, V_l(\bar{Q})) \tag{8.6}$$

where $k_l g$ is the composition

$$R_\Gamma^s \cap \operatorname{Ker} d_l \longrightarrow R_\Gamma^s \longrightarrow R_\Gamma^s/T(R_\Gamma) \xrightarrow{g} \pm 1 \longrightarrow V_l(\bar{Q})\ .$$

If $\mathfrak{p}$ is tame in N, then the map $W_{\mathfrak{p}}(N/K) : \chi \mapsto W_{\mathfrak{p}}(N/K, \chi)$ lies in

$$\operatorname{Hom}_{\mathfrak{Q}_Q}(R_\Gamma^s/T(R_\Gamma), \pm 1)$$

and we now have

Theorem 4. *Let $\mathfrak{p}$ be a prime divisor of K tame in N. Then*

$$h_l \mathcal{N}_{K/Q} c(\mathfrak{D}_{\mathfrak{p}}, b_{N/K}) = k_l(W_{\mathfrak{p}}(N/K))\ .$$

With the obvious definition of $W(N/K)$ we have the

Corollary. *If N/K is tame then*

$$h_l \mathcal{N}_{K/Q} Ac(\mathfrak{D}, b_{N/K}) = k_l(W(N/K))\ .$$

We add some further remarks.

Remark 1. One can restate the result of this section by interpreting, for $\chi \in R_\Gamma^s \cap \operatorname{Ker} d_l$, the value of $W_{\mathfrak{p}}(N/K, \chi)$ as the value of a rational idele class character (mod l) at a certain rational idele class, provided that $\rho_2 \mathcal{N}_{K/Q} c(\mathfrak{D}_{\mathfrak{p}}, b_{N/K})$ has a representative in $\operatorname{Hom}_{\mathfrak{Q}_Q}(R_\Gamma^s, U_+(Q))$. This is trivially true except when $\mathfrak{p}$ is finite and divides *order* (Γ). In the latter case this is an open question of some interest in resolvent theory.

Remark 2. Theorem 4 is closely related to [F3] Theorems 14 and 15. A detailed discussion, based on maps involving the Hermitian class group of $Z(\Gamma)$ (see Remark 2 in § 3) will be given elsewhere.

Remark 3. If one now varies π, for given Γ, the problem arises, which elements of $\operatorname{Hom}_{\mathfrak{Q}_Q}(R_\Gamma^s/T(R_\Gamma), \pm 1)$ can appear in the form $W_{\mathfrak{p}}(N/K)$. For the corresponding global question see e.g. [F4] (Theorem 18.).

Remark 4. Theorem 4 does not yet give a full characterisation of (local or global) symplectic root numbers as Hermitian invariants. In other words the group $\bigcap_l \operatorname{Ker} k_l$ (l odd) need not be zero (cf. (8.6)). What is still outstanding

is a satisfactory treatment for $\mathrm{Ker}\, d_2 \cap R_\Gamma^s$. For certain groups, e.g. all generalised quaternion groups (and trivially for all groups with $R_\Gamma^s = T(R_\Gamma)$) there are complete results. For the quaternion group of order 8 and $K = Q$ these connect up with computations of Martinet's (cf. [M1]).

Literature

[F1] Fröhlich, A., Resolvents, discriminants and trace invariants, J. Algebra **4** (1966), 173–198.

[F2] ——, Resolvents and trace form, Proc. Camb. Phil. Soc. **78** (1975), 185–210.

[F3] ——, Arithmetic and Galois module structure, for tame extensions, Crelle 286/287 (1976), 380–440.

[F4] ——, Galois module structure, Algebraic Number fields, Proc. Durham Symposium ed.: A. Fröhlich, A.P. London 1977.

[FM] ——, and McEvett, A. M., The representation of groups by automorphisms of forms, J. Algebra **12** (1969), 114–133.

[M] Martinet, J., Character theory and Artin L-functions, Algebraic Number fields, Proc. Durham Symposium ed.: A. Fröhlich, A.P. London 1977.

[M1] ——, H_s, Algebraic Number fields, Proc. Durham Symposium ed.: A. Fröhlich, A.P. London 1977.

[T] Tate, J., Local constants, Algebraic Number fields, Proc. Durham Symposium ed.: A. Fröhlich, A.P. London 1977.

Department of Mathematics
King's College
University of London
Strand, London WC2R 2LS
England

ALGEBRAIC NUMBER THEORY, Papers contributed for the International Symposium, Kyoto 1976; S. Iyanaga (Ed.): Japan Society for the Promotion of Science, Tokyo, 1977

Criteria for the Validity of a Certain Poisson Formula[1]

JUN-ICHI IGUSA

Introduction

We shall first recall a Poisson formula in Weil [12], p. 7: let X, G denote locally compact commutative groups, $f: X \to G$ a continuous map, Γ a lattice in G, and Γ_* the annihilator of Γ in the dual G^* of G; let $\mathscr{S}(X)$ denote the Schwartz-Bruhat space of X and put

$$F_\Phi^*(g^*) = \int_X \Phi(x)\langle f(x), g^*\rangle dx$$

for every Φ in $\mathscr{S}(X)$ and g^* in G^*; assume that the series

$$(*) \qquad \sum_{i^* \in \Gamma_*} |F_\Phi^*(g^* + i^*)|$$

is uniformly convergent on every compact subset of $\mathscr{S}(X) \times G^*$. Then there exists a unique family of tempered positive measures μ_g on X each μ_g with support in $f^{-1}(g)$ such that

$$F_\Phi(g) = \int_X \Phi d\mu_g$$

defines a continuous L^1-function F_Φ on G with F_Φ^* as its Fourier transform; and

$$\sum_{i \in \Gamma} F_\Phi(i) = \sum_{i^* \in \Gamma_*} F_\Phi^*(i^*)$$

for every Φ in $\mathscr{S}(X)$. We also recall that the later parts of Weil's paper are devoted, among other things, to the making of the above Poisson formula definitive in the case where X, G are adelized vector spaces relative to a number field k and f is defined by quadratic forms with coefficients in k. The defini-

[1] This work was partially supported by the National Science Foundation. The symposium lecture (entitled "On a Poisson formula in number theory") consisted of some material in [12], this paper, and [6].

tive Poisson formula by Weil contains some classical works of Siegel.

We have become interested in generalizing such a formula to a similar formula where f is defined by higher degree forms; at the present moment we restrict ourselves to the case of a single form. We have two things to do: one is to prove the convergence of $(*)$ under a condition on $f(x)$ similar to the classical condition on a quadratic form that "the number of variables is larger than 4"; another is to show that μ_i for each i in k is the measure defined by a "singular series". The first difficulty in carrying out such a program came, of course, from the fact that we had no criterion for the convergence of $(*)$. Consequently the proofs in some known cases were quite artificial; cf. [3], [10]. In order to improve this situation we have developed a theory of asymptotic expansions over an arbitrary local field in [4] and applied it to another case; cf. [5]. In this paper we shall prove useful criteria for the validity of the Poisson formula; we refer to § 1, Theorem 1 for the details. As an application we have outlined shorter proofs for the above-mentioned cases; cf. § 7. There are other applications; of these we have included just one; cf. § 9, Theorem 3.

§ 1. The criteria

Let X denote an irreducible non-singular algebraic variety defined over a field k and D, D' positive divisors of X rational over k such that D' is reduced and at every point a of X the irreducible components of D' passing through a are defined over $k(a)$ and transversal at a. Suppose that a morphism $h: Y \to X$ defined over k is the product of successive monoidal transformations each with irreducible non-singular center such that at every point b of Y the irreducible components of $h^*(D + D')$ passing through b are defined over $k(b)$ and transversal at b. (We recall that if $f = 0$ is a local equation for D, then $f \circ h = 0$ is a local equation for $h^*(D)$.) We further assume that h is not biregular at most at singular points of D. Then we say that h is a *resolution of* (D, D') over k; in this case h is a resolution of $(D, 0)$ over k and also of (D, D') over any extension of k. If h is a resolution of $(D, 0)$ over k, we simply say that h is a resolution of D over k. We observe that every irreducible component E of $h^*(D)$ is non-singular. We say that h is *tame* if char (k) does not divide the multiplicity $N = N_E$ of E in $h^*(D)$ for every E.

We take a point b of E, choose local coordinates $(y_1, \cdots, y_n)$ of Y around b and local coordinates $(x_1, \cdots, x_n)$ of X around $h(b)$; then the multiplicity of E in the divisor of the corresponding Jacobian determinant $\partial(x_1, \cdots, x_n)/\partial(y_1, \cdots, y_n)$ depends only on h and E. We shall denote by $\nu = \nu_E$ this multiplicity

increased by 1; and we call the pair (N, ν) the *numerical datum of h along E*. The number of all numerical data of h is equal to the number of irreducible components of $h^*(D)$. Moreover if $E_1, E_2, \cdots$ are the irreducible components of $h^*(D)$ passing through any given point b of Y, then the cardinality of $\{E_i\}_i$ is at most equal to n. If (N_i, ν_i) is the numerical datum of h along E_i, then we call $\{(N_i, \nu_i)\}_i$ the *numerical data of h at b*. We call attention to the fact that the above definition of the numerical data is slightly different from our definition in [4]–II, p. 309.

Let $f(x)$ denote a polynomial in n variables $x_1, \cdots, x_n$ with coefficients in k; then $f(x)$ gives rise to a function f on the affine n-space X defined over k. We shall denote by $S = S_f$ the *critical set* of f defined by

$$\operatorname{grad}_x f = (\partial f/\partial x_1, \cdots, \partial f/\partial x_n) = 0 .$$

For the sake of simplicity we say that $f(x)$ is *almost homogeneous* if S_f is contained in $f^{-1}(0)$; this is the case if $f(x)$ is homogeneous and char (k) does not divide deg (f).

We shall identify X with its dual space via the symmetric bilinear from

$$[x, y] = \sum_{i=1}^{n} x_i y_i$$

on $X \times X$. Also for every i in the universal field we put

$$U(i) = f^{-1}(i) - S_f ;$$

then $U(i)$ is non-singular; and $f(x)$ is almost homogeneous if and only if $U(i) = f^{-1}(i)$ for every $i \neq 0$. We shall at least assume that $S_f \neq X$; then we can write

$$dx = dx_1 \wedge \cdots \wedge dx_n = df \wedge \theta$$

with some $(n-1)$-form θ on X. Moreover for every i we can choose θ so that it becomes regular along $U(i)$, i.e., at general points of $U(i)$; then its restriction θ_i to $U(i)$ is well defined and it is regular and non-vanishing everywhere on $U(i)$.

Let k denote a global field, k_v the completion of k relative to a normalized absolute value $|\ |_v$ on k, and k_A the adele group of k; we shall also use k, v resp. A as subscripts to denote the taking of rational points over k, k_v resp. the adelization relative to k. We shall fix a non-trivial character ψ of k_A/k and denote by ψ_v its v-component; we shall identify X_v, X_A with their duals via

the bicharacters $\psi_v([x,y])$, $\psi([x,y])$ of $X_v \times X_v$, $X_A \times X_A$, respectively. We shall denote by $|dx|_v$, $|dx|_A$ the autodual measures on X_v, X_A; then $|dx|_A$ becomes the restricted product measure of all $|dx|_v$ and X_A/X_k has measure 1. If k_v is a p-field, we shall denote by $\mathfrak{o}_v, \mathfrak{p}_v$ the subsets of k_v defined by $|i|_v \leqq 1$, $|i|_v < 1$, respectively, and we put

$$q = q_v = \text{card}\,(\mathfrak{o}_v/\mathfrak{p}_v)\,, \qquad X_v^0 = \mathfrak{o}_v \times \cdots \times \mathfrak{o}_v\,.$$

Then for almost all v we have $\psi_v = 1$ on $\mathfrak{o}_v$ but not on $\mathfrak{p}_v^{-1}$; and X_v^0 has measure 1 for such a v.

Let Φ_v denote an element of the Schwartz-Bruhat space $\mathscr{S}(X_v)$ of X_v; then

$$F_{\Phi_v}^*(i^*) = \int_{X_v} \Phi_v(x)\psi_v(i^*f(x))\,|dx|_v$$

defines a bounded uniformly continuous function $F_{\Phi_v}^*$ on k_v. If k_v is a p-field and Φ_v is the characteristic function of X_v^0, then we shall write F_v^* instead of $F_{\Phi_v}^*$. Similarly as above, for every Φ in $\mathscr{S}(X_A)$

$$F_\Phi^*(i^*) = \int_{X_A} \Phi(x)\psi(i^*f(x))\,|dx|_A$$

defines a bounded uniformly continuous function F_Φ^* on k_A; the series

$$(*) \qquad \sum_{i^* \in k} F_\Phi^*(i^*) = \sum_{i^* \in k} \int_{X_A} \Phi(x)\psi(i^*f(x))\,|dx|_A$$

may or may not converge. If i is in k_v, then θ_i gives rise to a positive Borel measure $|\theta_i|_v$ on $U(i)_v$; cf. [11], pp. 14–16. The image measure of $|\theta_i|_v$ under $U(i)_v \to X_v$ may or may not exist. If i is in k, then $|\theta_i|_v$ is defined for every v; the restricted product measure $|\theta_i|_A$ of all $|\theta_i|_v$ may or may not exist. Even if it exists, the image measure of $|\theta_i|_A$ under $U(i)_A \to X_A$ may not exist.

We shall *assume* that $f(x)$ is homogeneous of degree $m \geqq 2$, char (k) does not divide m, and that a tame resolution h_0 over k of the projective hypersurface defined by $f(x) = 0$ exists; in view of Hironaka's theorem such a resolution always exists if char $(k) = 0$; cf. [2], p. 176. Since $f(x)$ is almost homogeneous, we get $U(i) = f^{-1}(i)$ for every $i \neq 0$; hence

$$F_{\Phi_v}(i) = \int_{U(i)_v} \Phi_v\,|\theta_i|_v$$

defines a continuous function F_{Φ_v} on $k_v^\times$ for every Φ_v in $\mathscr{S}(X_v)$. And F_{Φ_v} has a continuous extension to k_v if and only if

$$F_{\Phi_v}(0) = \lim_{i \to 0} F_{\Phi_v}(i)$$

exists. If k_v is a p-field and Φ_v is the characteristic function of X_v^0, then we shall write F_v instead of F_{Φ_v}.

Theorem 1. *We shall assume that the following two conditions are satisfied:*

(C1) *The critical set S_f is of codimension at least 3, i.e.,*

$$\text{codim}_{f^{-1}(0)}\,(S_f) \geqq 2\,;$$

(C2) *for almost all p-field k_v we have*

$$|F_v^*(i^*)| \leqq \max\,(1, |i^*|_v)^{-\sigma}$$

with a fixed $\sigma > 2$ for every i^* in k_v.

Then $(*)$ has a dominant series if Φ is restricted to a compact subset of $\mathscr{S}(X_A)$. Moreover for every i in k the restricted product measure $|\theta_i|_A$ on $U(i)_A$ exists, its image measure under $U(i)_A \to X_A$ also exists, the sum of all such measures is tempered, and the Poisson formula

$$\sum_{i \in k} \int_{U(i)_A} \Phi\,|\theta_i|_A = \sum_{i^* \in k} \int_{X_A} \Phi(x)\psi(i^*f(x))\,|dx|_A$$

holds. As an identity of tempered distributions it can also be written as

$$\sum_{i \in k} |\theta_i|_A = \sum_{i^* \in k} \psi(i^*f(x))\,.$$

The condition (C1) is easy to verify; it means that the hypersurface $f(x) = 0$ is irreducible and normal. The usefulness of this theorem comes from the fact that it reduces the proof of the Poisson formula to the verification of the estimate in (C2) for almost all non-archimedean valuations. It is *probable* that we can further restrict the set of valuations as follows: let k_0 denote a suitable subfield of k over which k is separably algebraic; then the estimate in (C2) holds for almost all non-archimedean valuations v on k of degree 1 relative to k_0. We might also mention the obvious fact that in proving the Poisson formula we may use any convenient non-trivial character of k_A/k as ψ and we may multiply any element of $k^\times$ to $f(x)$; if we can prove the formula under such normalizations, then it is true in general.

§ 2. Property (P)

We shall denote by $h: Y \to X$ a resolution of (D, D'), hence also of D, over an arbitrary field and by b a point of Y. Let $\{(N_i, \nu_i)\}_i$ denote the numerical

data of h at b and assume that $\nu_i \geqq N_i$ for every i where $\nu_i = N_i$ for at most one i_0; then we say that the numerical data have the *property* (P_0) at b. If we further have that $\nu_{i_0} = N_{i_0} = 1$, then we say that the numerical data have the *property* (P) at b. In the following lemma we shall assume that h is tame:

Lemma 1. *If the numerical data of $h: Y \to X$ have the property (P_0) everywhere, i.e., at every point of Y, then they have the property (P) everywhere.*

Proof. We take a Zariski open subset U of X, put $V = h^{-1}(U)$, and denote by h_V the restriction of h to V; then $h_V: V \to U$ is a resolution of the restriction of D to U. And we have only to prove the lemma for every such U. Therefore from the beginning we may assume the following: there exists a regular function f on X such that $D = (f)$, the divisor of f; there also exists a "gauge form" dx on X, i.e., a differential form dx on X of degree $n = \dim(X)$ which is regular and non-vanishing on X, i.e., everywhere on X.

If the lemma is false, there exists an irreducible component E of $h^*(D)$ such that $\nu_E = N_E \geqq 2$. Since h is tame by assumption, N_E is not divisible by the characteristic. Consequently we can write

$$h^*(dx) = d(f \circ h) \wedge \theta$$

with an $(n-1)$-form θ on Y regular along E; and then the restriction θ_E of θ to E is well defined, different from 0, and regular on E. This can be proved as follows: let b denote an arbitrary point of E; then there exist local coordinates $(y_1, \cdots, y_n)$ of Y centered at b such that

$$f \circ h = \varepsilon \cdot \prod_{i=1}^{n} y_i^{N_i}, \qquad h^*(dx) = \varepsilon' \cdot \prod_{i=1}^{n} y_i^{\nu_i - 1} \cdot dy_1 \wedge \cdots \wedge dy_n,$$

in which $\varepsilon, \varepsilon'$ are regular and non-vanishing around b; and $\{(N_i, \nu_i)\}_i$, where $N_i \geqq 1$, are the numerical data of h at b. We may assume that $y_1 = 0$ is a local equation for E; then we can take

$$\theta = (N_1\varepsilon + y_1 \cdot \partial\varepsilon/\partial y_1)^{-1}\varepsilon' \cdot \prod_{i>1} y_i^{\nu_i - N_i - 1} \cdot dy_2 \wedge \cdots \wedge dy_n,$$

and hence locally around b we get

$$\theta_E = \text{the restriction to } E \text{ of } (N_1\varepsilon)^{-1}\varepsilon' \cdot \prod_{i>1} y_i^{\nu_i - N_i - 1} \cdot dy_2 \wedge \cdots \wedge dy_n.$$

It is easy to verify that the right hand side does not depend on the choice of the local coordinates $(y_1, \cdots, y_n)$.

We recall that h is the product of successive monoidal transformations each with irreducible non-singular center:

$$Y \longrightarrow \cdots \longrightarrow Y' \longrightarrow X' \longrightarrow \cdots \longrightarrow X.$$

Since $\nu_E \geqq 2$, h is not biregular along E; hence it is "created" at some stage, say at $h': Y' \to X'$. Let Z denote the center of h' and put $E' = (h')^{-1}(Z)$; then E' is irreducible non-singular and the restriction of $Y \to Y'$ to E is a morphism $g: E \to E'$ which is birational and surjective. Let $\theta_{E'}$ denote the unique $(n-1)$-form on E' satisfying $\theta_E = g^*(\theta_{E'})$; then $\theta_{E'}$ is different from 0 and regular on E'. In fact, if $\theta_{E'}$ is not regular on E', choose any component C' of its polar divisor; then $C = g^{-1}(C')$ becomes a component of the polar divisor of θ_E, a contradiction.

Let π denote the restriction of h' to E'; then $\pi: E' \to Z$ converts E' into a fiber space with the projective space P_{r-1} as fiber; the dimension $r-1$ of the fiber is positive because r is the codimension of Z. We choose a point b' of E' where $\theta_{E'}$ does not vanish and put $a' = \pi(b')$; we then choose a local gauge form dz on Z around a' and write

$$\theta_{E'} = \pi^*(dz) \wedge \eta$$

with an $(r-1)$-form η on E' regular along $F = \pi^{-1}(a')$. This is possible and the restriction η_F of η to F is well defined, different from 0, and is regular on F; cf. [12], p. 12. On the other hand, since F is isomorphic to P_{r-1}, there is no regular form on F other than 0. We thus have a contradiction. q.e.d.

If the resolution $h: Y \to X$ is over k, then it can happen that the numerical data of h have the property (P_0), but not necessarily the property (P), at every k-rational point of Y. An example can be constructed, e.g., as follows: we choose a homogeneous polynomial $f(x)$ of degree n in n variables with coefficients in k such that the projective hypersurface defined by $f(x) = 0$ is non-singular and has no k-rational point; and we take the affine n-space as X, (f) as D, and the quadratic transformation of X centered at the origin of X as h.

§ 3. A remark on resolutions

We shall prove, for the sake of completeness, the following elementary lemma:

Lemma 2. *Let $f(x)$ denote a homogeneous polynomial of degree m in n variables $x_1, \cdots, x_n$ with coefficients in a field k; consider the projective spaces X_0, X^* with $(x_1, \cdots, x_n)$, $(1, x_1, \cdots, x_n)$ as their respective homogeneous coordi-*

nates; let $f^\sharp$ denote the rational function on $X^\sharp$ defined by $f(x)$; and assume that a resolution $h_0: Y_0 \to X_0$ of the projective hypersurface $f(x) = 0$ over k exists. Let H_∞ denote the hyperplane at infinity in $X^\sharp$ so that $(f^\sharp)_\infty = m \cdot H_\infty$; then h_0 gives rise to a resolution $h^\sharp: Y^\sharp \to X^\sharp$ of $((f^\sharp)_0, H_\infty)$ over k such that at every point of $Y^\sharp$ the numerical data of $h^\sharp$ are the numerical data of h_0 at some point of Y_0 possibly augmented by (m, n).

Proof. The correspondence $(1, x_1, \cdots, x_n) \to (x_1, \cdots, x_n)$ defines a rational map of $X^\sharp$ to X_0 over k which is regular except at the point with $(1, 0, \cdots, 0)$ as its homogeneous coordinates. Let $g: Z \to X^\sharp$ denote the quadratic transformation centered at this point; then the product of g and the above rational map gives a morphism $h_1: Z \to X_0$ defined over k. We consider the subset $Y^\sharp$ of $Y_0 \times Z$ consisting of those (y, z) where $h_0(y) = h_1(z)$, i.e., we put

$$Y^\sharp = Y_0 \times_{X_0} Z \ ;$$

and we define $h^\sharp: Y^\sharp \to X^\sharp$ as the product of $h_0 \times 1: Y^\sharp \to Z$ and $g: Z \to X^\sharp$. We shall show that $h^\sharp$ has the required property.

We first recall that if A, B are finitely generated integral resp. graded integral rings over k such that their fields of quotients are regular over k, then the k-schemes Spec (A) resp. proj (B) can be identified with the corresponding affine resp. projective varieties. We put

$$X_i = \text{Spec}\,(k[x_1/x_i, \cdots, x_n/x_i]) \ , \qquad Y_i = h_0^{-1}(X_i)$$

for $1 \leqq i \leqq n$; then $X_1, \cdots, X_n$ resp. $Y_1, \cdots, Y_n$ form k-open coverings of X_0 resp. Y_0. Furthermore

$$\text{Spec}\,(k[x_1, \cdots, x_n]) \ , \qquad \text{Spec}\,(k[1/x_i]) \times X_i$$

for $1 \leqq i \leqq n$ form a k-open covering of $X^\sharp$ and Proj $(k[t, tx_i]) \times X_i$ for $1 \leqq i \leqq n$, in which t is a new variable, form a k-open covering of Z. Finally Proj $(k[t, tx_i]) \times Y_i$ for $1 \leqq i \leqq n$ form a k-open covering of $Y^\sharp$.

After this remark we take a point $b^\sharp$ of $Y^\sharp$ and put $a^\sharp = h^\sharp(b^\sharp)$. We have only to show that the irreducible components of $(h^\sharp)^*((f^\sharp)_0 + H_\infty)$ are defined over $k(b^\sharp)$ and transversal at $b^\sharp$ and that the numerical data of $h^\sharp$ at $b^\sharp$ are as stated in the lemma. By changing indices we may assume that $b^\sharp$ is in Proj $(k[t, tx_1]) \times Y_1$; then we can write $b^\sharp = (a_1, b)$ with a_1 in the universal field or $a_1 = \infty$ and b in Y_1. We put

$$u_2 = x_2/x_1, \cdots, u_n = x_n/x_1 \ ;$$

then there exist local coordinates $(v_2, \cdots, v_n)$ of Y_0 centered at b and defined over $k(b)$ such that

$$\begin{cases} f(1, u_2, \cdots, u_n) = \varepsilon \cdot \prod_{i>1} v_i^{\nu_i} \\ du_2 \wedge \cdots \wedge du_n = \varepsilon' \cdot \prod_{i>1} v_i^{\nu_i - 1} \cdot dv_2 \wedge \cdots \wedge dv_n \ , \end{cases}$$

in which $\varepsilon, \varepsilon'$ are regular and non-vanishing around b. We shall separate two cases according as $a^\sharp$ is or is not on H_∞, i.e., according as a_1 is or is not ∞:

If $a_1 \neq \infty$, we put

$$y_1 = x_1 - a_1, \ y_2 = v_2, \ \cdots, \ y_n = v_n \ ;$$

then $(y_1, \cdots, y_n)$ form local coordinates of $Y^\sharp$ centered at $b^\sharp$ and clearly defined over $k(b^\sharp)$ such that

$$\begin{cases} f(x_1, \cdots, x_n) = \varepsilon \cdot (y_1 + a_1)^m \cdot \prod_{i>1} y_i^{\nu_i} \\ dx = \varepsilon' \cdot (y_1 + a_1)^{n-1} \cdot \prod_{i>1} y_i^{\nu_i - 1} \cdot dy \ . \end{cases}$$

Since $(x_1, \cdots, x_n)$ form local coordinates of $X^\sharp$ around $a^\sharp$ and $f(x_1, \cdots, x_n) = 0$ gives a local equation for $(f^\sharp)_0$, $h^\sharp$ has the required property at $b^\sharp$. If $a_1 = \infty$, we put

$$y_1 = 1/x_1, \ y_2 = v_2, \ \cdots, \ y_n = v_n \ ;$$

then $(y_1, u_2, \cdots, u_n)$ resp. $(y_1, \cdots, y_n)$ form local coordinates of $X^\sharp$ resp. $Y^\sharp$ around $a^\sharp$ resp. centered at $b^\sharp$ and defined over $k(b^\sharp)$. Moreover $f(1, u_2, \cdots, u_n) = 0$ resp. $y_1 = 0$ give local equations for $(f^\sharp)_0$ resp. H_∞; and we have

$$\begin{cases} f(1, u_2, \cdots, u_n) = \varepsilon \cdot \prod_{i>1} y_i^{\nu_i} \\ dy_1 \wedge du_2 \wedge \cdots \wedge du_n = \varepsilon' \cdot \prod_{i>1} y_i^{\nu_i - 1} \cdot dy \ . \end{cases}$$

Therefore $h^\sharp$ has the required property at $b^\sharp$. q.e.d.

The above proof shows that the "augmentation" becomes necessary if and only if $a_1 = 0$, i.e., if and only if $a^\sharp = h^\sharp(b^\sharp)$ has $(1, 0, \cdots, 0)$ as its homogeneous coordinates.

§ 4. A correction

We shall resume the assumption that k is a global field and denote by $\Omega(k_v^\times)$ the group of quasi-characters of $k_v^\times$. We know that the identity component $\Omega(k_v^\times)^0$ consists of quasi-characters ω_s defined by $\omega_s(i) = |i|_v^s$ for every i in $k_v^\times$, in which s is in C; even if ω is arbitrary in $\Omega(k_v^\times)$, we at least have

$$|\omega(i)| = |i|_v^{\sigma(\omega)}$$

for every i in $k_v^\times$ with $\sigma(\omega)$ in $\boldsymbol{R}$.

Suppose that $f(x)$ is an almost homogeneous polynomial in $x_1, \cdots, x_n$ with coefficients in k_v and let X denote, as before, the affine n-space defined over k; then for every Φ_v in $\mathscr{S}(X_v)$ the following integral:

$$Z_{\Phi_v}(\omega) = \int_{X_v} \omega(f(x))\Phi_v(x)\,|dx|_v$$

defines a holomorphic function Z_{Φ_v} on the subset of $\Omega(k_v^\times)$ defined by $\sigma(\omega) > 0$; and it has a meromorphic continuation to the whole $\Omega(k_v^\times)$. Furthermore the function $F_{\Phi_v}^*$ is in $L^1(k_v)$ if and only if

$$|F_{\Phi_v}^*(i^*)| \leqq \text{const. } \max(1, |i^*|_v)^{-\sigma}$$

with a fixed $\sigma > 1$ for every i^* in k_v; and this is the case if and only if $F_{\Phi_v}(0)$ exists. In terms of $Z_{\Phi_v}(\omega)$ this condition can be stated as follows: if k_v is an $\boldsymbol{R}$-field, then $Z_{\Phi_v}(\omega)$ for ω not in $\Omega(k_v^\times)^0$ and $(s+1)Z_{\Phi_v}(\omega)$ for $\omega = \omega_s$ are holomorphic on the subset $\sigma(\omega) \geqq -1$; if k_v is a p-field and $t = q^{-s}$, then $Z_{\Phi_v}(\omega)$ for ω not in $\Omega(k_v^\times)^0$ and $(1 - q^{-1}t)Z_{\Phi_v}(\omega)$ for $\omega = \omega_s$ are holomorphic on $\sigma(\omega) \geqq -1$. And if these equivalent conditions are satisfied for every Φ_v in $\mathscr{S}(X_v)$, then

$$\Phi_v \longrightarrow F_{\Phi_v}(0) - \int_{U(0)_v} \Phi_v\,|\theta_0|_v$$

defines a tempered positive measure on X_v with support contained in

$$S_v = f^{-1}(0)_v - U(0)_v\ .$$

We proved the above results in [4]–II under the following assumption: let $X^\sharp$ denote the projective space obtained from X by adding a hyperplane H_∞ and $f^\sharp$ the rational function on $X^\sharp$ which extends f; then the assumption is that a tame resolution $h^\sharp\colon Y^\sharp \to X^\sharp$ of $((f^\sharp)_0, H_\infty)$ over k_v exists; this assumption is always satisfied if $\text{char}(k_v) = 0$. We put $Y = (h^\sharp)^{-1}(X)$ and denote by h the restriction of $h^\sharp$ to Y. Then later in that paper we proved as Lemma 4 a statement to the effect that the numerical data of h have the property (P) at every point of Y_v if k_v is a p-field and if the equivalent conditions are satisfied for every Φ_v in $\mathscr{S}(X_v)$. We have found, however, that the "proof" is incomplete; therefore we shall replace "Lemma 4" by another statement and give its complete proof. We shall use the following notation: suppose that k_v is an arbitrary local field and M a k_v-analytic manifold; then we shall denote by $\mathscr{D}(M)$ the vector space of smooth, i.e., infinitely differentiable or locally constant, functions on M with compact support.

Theorem 2. *Let b denote a point of Y_v and Φ_v an element of $\mathscr{D}(X_v)$ satisfying $\Phi_v \geqq 0$, $\Phi_v(h(b)) > 0$; then the existence of $F_{\Phi_v}(0)$ implies that the numerical data of h have the property (P_0) at b; and the stronger assumption:*

$$(**) \qquad F_{\Phi_v}(0) = \int_{U(0)_v} \Phi_v\,|\theta_0|_v$$

implies that the numerical data of h have the property (P) at b. Conversely if the numerical data of h have the property (P) at every b in Y_v, then $(**)$ holds for every Φ_v in $\mathscr{D}(X_v)$; and if the numerical data of $h^\sharp$ have the property (P) at every $b^\sharp$ in $Y_v^\sharp$, then $(**)$ holds for every Φ_v in $\mathscr{S}(X_v)$.

Proof. For a moment we take Φ_v arbitrarily from $\mathscr{S}(X_v)$. Suppose that $F_{\Phi_v}(0)$ exists; then $(s+1)Z_{\Phi_v}(\omega_s)$ is bounded around -1. On the other hand, since $h\colon Y \to X$ is a resolution of (f) over k_v, there exist local coordinates $(y_1, \cdots, y_n)$ of Y centered at b and defined over k_v such that

$$f \circ h = \varepsilon \cdot \prod_{i=1}^n y_i^{N_i}, \qquad h^*(dx) = \varepsilon' \cdot \prod_{i=1}^n y_i^{\nu_i - 1} \cdot dy\ ,$$

in which $\varepsilon, \varepsilon'$ are regular and non-vanishing around b. We observe that $\varepsilon, \varepsilon'$, $y_1, \cdots, y_n$ give rise to k_v-analytic functions on a small open neighborhood, say V, of b in Y_v; we may assume that $\varepsilon\varepsilon' \neq 0$ at every point of V. Suppose that Φ_v is in $\mathscr{D}(X_v)$ and $\Phi_v \geqq 0$, $\Phi_v(h(b)) > 0$; then, by making V smaller if necessary, we may assume that

$$|\varepsilon(y)|_v^s\,|\varepsilon'(y)|_v\,\Phi_v(h(y)) \geqq c > 0$$

for $-1 \leqq s \leqq 0$ and for every y in V, in which c is a constant. And then we will have

$$Z_{\Phi_v}(\omega_s) \geqq c \cdot \int_V \prod_{i=1}^n |y_i|_v^{N_i s + \nu_i - 1} \cdot |dy|_v$$

for $-1 < s \leqq 0$. If we multiply $s+1$ to the right hand side, therefore, the product is bounded as $s \to -1$; and this clearly implies that $\nu_i \geqq N_i$ for every i where $\nu_{i_0} = N_{i_0}$ for at most one i_0.

We shall next show that $(**)$ implies $\nu_{i_0} = N_{i_0} = 1$; by changing indices we may assume that $i_0 = 1$. We put

$$\varepsilon_1 = (N_1\varepsilon + y_1 \cdot \partial\varepsilon/\partial y_1)^{-1}\varepsilon'\ ;$$

then for every $i \neq 0$ we have

$$h^*(\theta_i) = \text{the restriction to } (f \circ h)^{-1}(i) \text{ of } \varepsilon_1 \cdot \prod_{j>1} y_j^{\nu_j - N_j - 1} \cdot dy_2 \wedge \cdots \wedge dy_n .$$

Let E denote the irreducible component of $h^*((f))$ with $y_1 = 0$ as a local equation and define θ_E as in the proof of Lemma 1; then θ_E gives rise to a positive Borel measure $|\theta_E|_v$ on E_v; and $|\theta_E|_v$ has E_v as its exact support.

After this remark we take the open neighborhood V of b small enough so that $\varepsilon_1 \neq 0$ at every point of V; then for every ϕ in $\mathscr{D}(V)$ we have

$$\lim_{i \to 0} \int_{(f \circ h)^{-1}(i)} \phi \cdot |h^*(\theta_i)|_v = \int_{E \cap V} \phi \cdot |\theta_E|_v .$$

We recall that h is biregular at every point of $h^{-1}(U(0))$. Therefore if $\nu_1 = N_1 = 1$, then in V, i.e., as long as points of V are concerned, we have

$$h^{-1}(U(0)) = E \text{ minus the hyperplanes } y_j = 0 \text{ for } N_j \geqq 1 ;$$

hence we get

$$\int_{E \cap V} \phi \cdot |\theta_E|_v = \int_{h^{-1}(U(0))_v} \phi \cdot |h^*(\theta_0)|_v .$$

We take a finite covering of the preimage under h of the support of Φ_v by open sets such as V and take a partition of unity $(p_V)_V$ subordinate to this covering. Then by applying the above observation to each $\phi = (\Phi_v \circ h) p_V$ we get

$$F_{\Phi_v}(0) = \int_{U(0)_v} \Phi_v |\theta_0|_v + \sum_{\nu_E \geqq 2} \int_{E_v} (\Phi_v \circ h) |\theta_E|_v .$$

Since $|\theta_E|_v$ has E_v as its exact support, if we have (**), then no E with $\nu_E = N_E \geqq 2$ passes through b.

Finally suppose that the numerical data of h have the property (P) at every point of Y_v; then (**) certainly holds for every Φ_v in $\mathscr{D}(X_v)$. Suppose further that the numerical data of $h^\sharp$ have the property (P) at every point $b^\sharp$ of $Y_v^\sharp$; choose local coordinates $(y_1, \cdots, y_n)$ of $Y^\sharp$ centered at $b^\sharp$ and defined over k_v such that $f^\sharp \circ h^\sharp$ becomes, up to a regular and non-vanishing function around $b^\sharp$, a product of powers of $y_1, \cdots, y_n$ and $(h^\sharp)^*(dx)$ a product of powers of $y_1, \cdots, y_n$ and a local gauge form around $b^\sharp$. This time, however, some of the exponents, say the exponent of y_i in $f^\sharp \circ h^\sharp$, may become negative. Then the "infinite divisibility" of Φ_v by a local equation for H_∞ implies the infinite divisibility of $\Phi_v \circ h^\sharp$ by y_i. In this way we see that the component with $y_i = 0$ as a local equation becomes negligible and (**) holds for every Φ_v in $\mathscr{S}(X_v)$. q.e.d.

As we have said, [4]–II, Lemma 4 has to be replaced by the theorem just proved. As for Theorem 4 that follows Lemma 4, it is valid as stated; in fact it follows from the above theorem and the previous Lemma 1.

§ 5. (C2) implies (P)

We have assumed the existence of a tame resolution $h_0 : Y_0 \to X_0$ over k of the projective hypersurface defined by $f(x) = 0$ and that $\mathrm{char}(k)$ does not divide $m \geqq 2$. This implies that the resolution $h^\sharp : Y^\sharp \to X^\sharp$ in Lemma 2 is also tame and over k, hence over k_v for every v. We shall show that if (C2) is satisfied, then the numerical data of $h^\sharp$ have the property (P) everywhere. In view of the conjecture made after Theorem 1, we shall prove the following more precise statement:

Lemma 3. *Let k_0 denote a subfield of k over which k is separably algebraic and assume that F_v^* is in $L^1(k_v)$ for almost all non-archimedean valuations v on k of degree 1 relative to k_0; then the numerical data of $h^\sharp$ have the property (P) everywhere. Therefore $F_{\Phi_v}^*$ is in $L^1(k_v)$ and*

$$(**) \qquad F_{\Phi_v}(0) = \int_{U(0)_v} \Phi_v |\theta_0|_v$$

for every Φ_v in $\mathscr{S}(X_v)$ and for every valuation v on k.

Proof. Since h_0 is tame by assumption, all irreducible components of the $(h_0)^*$ of the projective hypersurface $f(x) = 0$ are defined over the separable closure k_s of k. Consider the set of all numerical data of h_0 at various points of Y_0; then by the quasi-compactness of the Zariski topology this set is finite. Let $\{(N_i, \nu_i)\}_i$ denote an element of this set and consider the subset of Y_0 consisting of those points where h_0 has $\{(N_i, \nu_i)\}_i$ as its numerical data; then at least locally it is a transversal intersection of varieties defined over k_s. Therefore the set is locally closed and its irreducible components are defined over k_s. According to a well-known elementary lemma, any irreducible variety defined over k_s has a k_s-rational point; in fact the subset of k_s-rational points is Zariski dense. Therefore we can find a point of the set which is rational over k_s. We choose such a point b_0 for each $\{(N_i, \nu_i)\}_i$ and denote by k_1 the extension of k obtained by adjoining (the coordinates of) all b_0; by construction k_1 is a separable algebraic extension of k, hence also of k_0.

We know that the set of non-archimedean valuations on k_1 of degree 1

relative to k_0 is infinite; this is a well-known consequence of the fact that the zeta function of a global field is holomorphic for $Re(s) > 1$ and has $s = 1$ as a pole. By restricting such valuations to k we get infinitely many non-archimedean valuations on k of degree 1 relative to k_0. Therefore we can certainly choose a particular valuation, say w, from the set specified in the lemma such that k_1 becomes a subfield of k_w. We have thus achieved a situation where the numerical data of $h^\sharp$ at any given point of $Y^\sharp$ are also the numerical data of h at some point of $Y_w \cap h^{-1}(X_w^0)$. The rest of the proof is as follows:

By assumption F_w^* is in $L^1(k_w)$; hence by the first part of Theorem 2 the numerical data of h have the property (P_0) at every point of $Y_w \cap h^{-1}(X_w^0)$. In view of the construction the numerical data of $h^\sharp$ have the property (P_0) everywhere. Then by Lemma 1 they have the property (P) everywhere. Therefore by the last part of Theorem 2 $(**)$ holds, hence $F_{\Phi_v}^*$ is in $L^1(k_v)$, for every Φ_v in $\mathcal{S}(X_v)$; and this is so for every valuation v on k. q.e.d.

§ 6. Proof of Theorem 1

We recall that $F_{\Phi_v}^*$ is the Fourier transform of F_{Φ_v} for every Φ_v in $\mathcal{S}(X_v)$ and that if $F_{\Phi_v}^*$ is in $L^1(k_v)$, then

$$F_{\Phi_v}(i) = \int_{k_v} F_{\Phi_v}^*(i^*)\psi_v(-ii^*)\,|di^*|_v$$

for every i in k_v. In the following two lemmas we shall assume that v is non-archimedean, $\psi_v = 1$ on $\mathfrak{o}_v$ but not on $\mathfrak{p}_v^{-1}$, and the coefficients of $f(x)$ are in $\mathfrak{o}_v$; almost all valuations on k are good in this sense.

Lemma 4. *Suppose that*

$$|F_v^*(i^*)| \leqq \max(1, |i^*|_v)^{-\sigma}$$

with a fixed $\sigma > 1$ for every i^* in k_v; then

$$|F_v(i) - 1| \leqq (1 - 2^{-(\sigma-1)})^{-1} \cdot q^{-(\sigma-1)}$$

for every i in $\mathfrak{o}_v$.

Proof. Since v is "good," $F_v^* = 1$ on $\mathfrak{o}_v$ and X_v^0 has measure 1. Since F_v^* is in $L^1(k_v)$ by assumption, we get

$$F_v(i) - 1 = \int_{k_v - \mathfrak{o}_v} F_v^*(i^*)\psi_v(-ii^*)\,|di^*|_v\ ;$$

this implies

$$\begin{aligned} |F_v(i) - 1| &\leqq \int_{k_v - \mathfrak{o}_v} |i^*|_v^{-\sigma}\,|di^*|_v \\ &= (1 - q^{-1})(1 - q^{-(\sigma-1)})^{-1} \cdot q^{-(\sigma-1)} \\ &\leqq (1 - 2^{-(\sigma-1)})^{-1} \cdot q^{-(\sigma-1)}\ . \end{aligned}$$ q.e.d.

We recall that $U(i)_v^0$, where i is in $\mathfrak{o}_v$, is a compact subset of $U(i)_v$ defined as follows: if $i \neq 0$, then $U(i)_v^0$ is simply $U(i)_v \cap X_v^0$ and if $i = 0$, it is the subset of $U(i)_v \cap X_v^0$ defined by the additional condition that $\operatorname{grad}_x f \not\equiv 0 \bmod \mathfrak{p}_v$.

Lemma 5. *Suppose that the condition in Lemma 4 is satisfied for almost all v; put $r = \operatorname{codim}_{f^{-1}(0)}(S_f)$; then for every i in $\mathfrak{o}_v$ we have*

$$\int_{U(i)_v^0} |\theta_i|_v = 1 + O(q^{-(\sigma-1)} + q^{-r})$$

uniformly in i and v.

Proof. Since the left hand side is at most equal to $F_v(i)$, by Lemma 4 it is bounded uniformly in i and v. Therefore in proving the lemma we may exclude any finite number of valuations; in particular we may assume that $m \not\equiv 0 \bmod \mathfrak{p}_v$. After this remark we shall denote an element of X_v^0 by ξ and define $N_e(i)$ resp. $N_e^0(i)$ as the number of $\xi \bmod \mathfrak{p}_v^e$ such that $f(\xi) \equiv i \bmod \mathfrak{p}_v^e$ resp. $f(\xi) \equiv i \bmod \mathfrak{p}_v^e$ and $\operatorname{grad}_\xi f \not\equiv 0 \bmod \mathfrak{p}_v$ for $e = 0, 1, 2, \cdots$; then we get

$$q^{-(n-1)e} N_e(i) = \int_{\mathfrak{p}_v^{-e}} F_v^*(i^*)\psi_v(-ii^*)\,|di^*|_v\ .$$

As in the proof of Lemma 4 this implies

$$q^{-(n-1)} N_1(i) = 1 + O(q^{-(\sigma-1)})$$

uniformly in i and v. On the other hand we have $N_1(i) = N_1^0(i)$ if $i \not\equiv 0 \bmod \mathfrak{p}_v$ and

$$N_1(i) = N_1^0(i) + O(q^s)\ ,$$

where $s = \dim(S_f) = n - 1 - r$, uniformly in i and v if $i \equiv 0 \bmod \mathfrak{p}_v$. This is an elementary result; cf. [7], Lemma 1. We also have

$$\int_{U(i)_v^0} |\theta_i|_v = q^{-(n-1)} N_1^0(i)$$

for almost all v; cf. [11], Theorem 2.2.5. Therefore we get

$$\int_{U(i)_v^0} |\theta_i|_v = 1 + O(q^{-(\sigma-1)}) + O(q^{s-(n-1)})$$

uniformly in i and v. q.e.d.

We are ready to prove Theorem 1: first of all the series

$$\sum_{i^* \in k} F_\Phi^*(i^*) = \sum_{i^* \in k} \int_{X_A} \Phi(x)\psi(i^* f(x))\,|dx|_A$$

is absolutely convergent for every Φ in $\mathscr{S}(X_A)$. This follows from (C2), Lemma 3, and from the fact (proved in [3], [5]) that the series

$$\sum_{i^* \in k} \prod_v \max(1, |i^*|_v)^{-\sigma_v}$$

is convergent if $\sigma_v > 1$ for all v and $\sigma_v \geqq \sigma > 2$ for almost all v. We also remarked elsewhere that as long as Φ remains in a compact subset of $\mathscr{S}(X_A)$, the first series has a constant multiple of the second series as a dominant series; cf. [6]. On the other hand, the correspondence $(\Phi, i^*) \to \Phi(x)\psi(i^* f(x))$ defines a continuous map of $\mathscr{S}(X_A) \times k_A$ to $\mathscr{S}(X_A)$; cf. [8]. Therefore conditions (B_0), (B_1) in Weil [12], p. 8 are satisfied. Consequently F_Φ^* is in $L^1(k_A)$ and there exists a unique family of tempered positive measures μ_i on X_A each with support in $f^{-1}(i) = f_A^{-1}(i)$ such that

$$F_\Phi(i) = \int_{X_A} \Phi d\mu_i$$

defines a continuous L^1-function F_Φ on k_A with F_Φ^* as its Fourier transform; and

$$\sum_{i \in k} F_\Phi(i) = \sum_{i^* \in k} F_\Phi^*(i^*)$$

for every Φ in $\mathscr{S}(X_A)$. The rest of the proof consists of making the measure μ_i explicit for every i in k.

We have

$$\int_{k_A} F_\Phi^*(i^*)\psi(-ii^*)\,|di^*|_A = F_\Phi(i) = \int_{X_A} \Phi d\mu_i$$

for every Φ in $\mathscr{S}(X_A)$ and i in k_A. We choose i from k; then for every special element Φ of $\mathscr{S}(X_A)$ of the form $\Phi = \otimes_v \Phi_v$ the product of all $F_{\Phi_v}(i)$ is absolutely convergent; by Lemma 4 this follows from (C2). Futhermore 1 is a set of convergence factors for $U(i)$; by Lemma 5 this follows from (C1) and (C2). Therefore the restricted product measure $|\theta_i|_A$ of all $|\theta_i|_v$ exists. Moreover if, for a moment, S denotes a large finite set of valuations on k, then

$$\begin{cases} \int_{U(i)_A} \Phi\,|\theta_i|_A = \lim_S \prod_{v \notin S} \int_{U(i)_v^0} |\theta_i|_v \cdot \prod_{v \in S} \int_{U(i)_v} \Phi_v\,|\theta_i|_v \\ \int_{X_A} \Phi d\mu_i = \lim_S \prod_{v \in S} \int_{k_v} F_{\Phi_v}^*(i^*)\psi_v(-ii^*)\,|di^*|_v\ ; \end{cases}$$

and the right hand sides are both equal to the product of all $F_{\Phi_v}(i)$. Since the C-span of functions such as Φ forms a dense subspace of $\mathscr{S}(X_A)$, therefore, we get

$$\int_{U(i)_A} \Phi\,|\theta_i|_A = \int_{X_A} \Phi d\mu_i$$

for every Φ in $\mathscr{S}(X_A)$. This completes the proof.

§ 7. Known cases retold

If k_v is a p-field and Φ_v is the characteristic function of X_v^0, then we shall write $Z_v(s)$ instead of $Z_{\Phi_v}(\omega_s)$; this is in accordance with the notation F_v, F_v^*.

Case 1. Let $f(x)$ denote a homogeneous polynomial of degree $m \geqq 2$ in n variables with coefficients in k; we shall assume that $S_f = \{0\}$, i.e., the projective hypersurface defined by $f(x) = 0$ is non-singular. In this case $h^\sharp$ is simply the quadratic transformation of $X^\sharp$ centered at the origin of X; hence it is tame if char (k) does not divide m. Moreover if $n > m$, then we have

$$|F_v^*(i^*)| \leqq \max(1, |i^*|_v)^{-n/m}$$

for every i^* in k_v and for almost all non-archimedean valuation v on k. This was proved in [5], pp. 219–222 independently of other parts (but dependently on Deligne's result). Therefore by Theorem 1 the Poisson formula holds if char (k) does not divide m and $n > 2m$. Incidentally the Euler factor $Z_v(s)$ has $(1 - q^{-1}t)(1 - q^{-n}t^m)$, where $t = q^{-s}$, as its denominator and

$$(1 - q^{-n}N_1(0)) - (q^{-1} + q^{-n} - q^{-n-1} - q^{-n}N_1(0))t$$

as its numerator.

Case 2. We shall take as X (the underlying vector space of) a simple Jordan algebra defined over k of quaternionic hermitian matrices of degree $m \geqq 2$ and as $f(x)$ its norm form. In this case the codimension of S_f in $f^{-1}(0)$ is 5. And we have

$$Z_v(s) = \prod_{i=0}^{m-1} (1 - q^{-(2i+1)})(1 - q^{-(2i+1)}t)^{-1}$$

for almost all v; this can be proved by replacing $f(x)$ by the Pfaffian of an alternating matrix of degree $2m$, which is permissible for almost all v. The details are given in [3], pp. 192–193; it only depends on what we called "elementary arithmetic" in that paper. At any rate this implies

$$F_v^*(i^*) = \sum_{i=1}^{m-1} c_i |i^*|_v^{-(2i+1)}$$

for every i^* in $k_v - \mathfrak{o}_v$, where

$$c_i = \sum_{1 \leqq j < m, j \neq i} (1 - q^{-(2j+1)})(1 - q^{-2(j-i)})^{-1}$$

for $1 \leqq i < m$. Therefore if k is a number field, then we can apply Theorem 1 with any number between 2 and 3 as σ; hence the Poisson formula holds in this case.

Case 3. We shall take as X an exceptional simple Jordan algebra defined over k and as $f(x)$ its norm form. This case was fully examined by Mars [10] by using the theory of Jordan algebras; we can also proceed as follows: the codimension of S_f in $f^{-1}(0)$ is 9 and

$$Z_v(s) = \prod_{i=1,5,9} (1 - q^{-i})(1 - q^{-i}t)^{-1}$$

for almost all v; this can be proved by replacing $f(x)$ by the classical split form ${}^t xzy - Pf(z)$, e.g., in E. Cartan's thesis, p. 143, where z is an alternating matrix of degree 6 and x, y are column vectors. The computation is tedious but elementary. At any rate this implies

$$F_v^*(i^*) = (1 - q^{-9})(1 - q^{-4})^{-1} \cdot |i^*|_v^{-5} - q^{-4}(1 - q^{-5})(1 - q^{-4})^{-1} \cdot |i^*|_v^{-9}$$

for every i^* in $k_v - \mathfrak{o}_v$. Therefore if k is a number field, then we can apply Theorem 1; hence the Poisson formula holds also in this case.

Remark. In the function-field case we have to verify the prerequisite for applying Theorem 1, i.e., the existence of a tame resolution h_0 over k of the projective hypersurface defined by $f(x) = 0$. This question, which is interesting in itself, was examined (in the fall of 1974) by G. R. Kempf over an arbitrary field. He showed, among other things, that a resolution $h_0: Y_0 \to X_0$ exists and that the numerical data of h_0 at any given point of Y_0 are subsets of $\{(i, i(2i-1))\}_{1 \leqq i < m}$ in Case 2 and of $\{(1,1),(2,10)\}$ in Case 3. Therefore in Case 2 if $\mathrm{char}(k)$ does not divide $m!$, then the Poisson formula holds. (Actually by the method in [3] we can show that the Poisson formula holds without any restriction on $\mathrm{char}(k)$; in fact the proof in the function-field case is much simpler.) Moreover in Case 3 if $\mathrm{char}(k) \neq 2, 3$, then the Poisson formula holds.

We might also mention that Kempf's result (together with our theory of asymptotic expansions) clarifies the ambiguities in [3], p. 183 and [10], p. 129: for every Φ_v in $\mathscr{S}(X_v)$ and i^* in k_v we have

$$|F_{\Phi_v}^*(i^*)| \leqq \text{const. } \max(1, |i^*|_v)^{-\sigma}$$

with $\sigma = 3$ in Case 2 and $\sigma = 5$ in Case 3; and this is so for every valuation v on k.

§ 8. Birch-Davenport's theorem

We shall give another application of Theorem 1; we shall first recall certain results of Davenport and Birch: let k denote an algebraic extension of $\boldsymbol{Q}$ of degree d and $\mathfrak{o}$ the ring of integers of k; we choose a $\boldsymbol{Z}$-basis $\{\omega_1, \cdots, \omega_d\}$ of $\mathfrak{o}$. We shall denote by $f(x)$ a homogeneous polynomial of degree $m \geqq 2$ in $x_1, \cdots, x_n$ with coefficients in $\mathfrak{o}$ and by $S = S_f$ the critical set of $f: X = \boldsymbol{C}^n \to \boldsymbol{C}$; we shall assume that $S_f \neq X$, i.e., $f \neq 0$. We put $Y = M_{n,d}(\boldsymbol{C})$ and define $\pi: Y \to X$ as

$$\pi(y) = \left(\sum_{i=1}^{d} y_{1i}\omega_i, \cdots, \sum_{i=1}^{d} y_{ni}\omega_i \right);$$

then there exists a unique set of homogeneous polynomials $g_1(y), \cdots, g_d(y)$ of degree m in y_{ij} with coefficients in $\boldsymbol{Z}$ such that

$$f(\pi(y)) = \sum_{i=1}^{d} g_i(y)\omega_i .$$

If we use the functor $R_{k/\boldsymbol{Q}}$ in Weil [11], p. 6, then

$$R_{k/\boldsymbol{Q}}(X) = (Y, \pi), \qquad R_{k/\boldsymbol{Q}}(f) = (g_1, \cdots, g_d) .$$

In the following we shall regard the number field k, the $\boldsymbol{Z}$-basis $\{\omega_1, \cdots, \omega_d\}$ of $\mathfrak{o}$, and the form $f(x)$ as fixed; and we shall introduce the following "variables": a box B in $Y_{\boldsymbol{R}}$ of sidelength 1, a vector $u = (u_1, \cdots, u_d)$ in $\boldsymbol{R}^d$, positive real numbers α, β, τ where $\beta, \tau \leqq 1$, and polynomials $r_1(y), \cdots, r_d(y)$ of degree $m-1$ in y_{ij} with coefficients in $\boldsymbol{R}$. We say that a quantity is a parameter or a constant according as it is or is not dependent on these variables.

Theorem (Birch-Davenport). *We put*

$$\sigma_0 = 2^{-(m-1)} \operatorname{codim}(S_f)$$

and assume that $\sigma_0 \beta > \alpha$; *then there exists a parameter* τ_0 *depending only on* $\sigma_0\beta - \alpha$ *such that for any* $\tau < \tau_0$ *either*

$$(1) \qquad \left|\sum_{\eta\in\tau^{-1}B\cap Y_Z} e\left(\sum_{\lambda=1}^{d} u_\lambda(g_\lambda(\eta)+r_\lambda(\eta))\right)\right| < \tau^{d(-n+\alpha)}$$

or there exist relatively prime integers $a_1,\cdots,a_d,b$ *satisfying*

$$(2) \qquad 1\leqq b\leqq c\cdot\tau^{-(m-1)d\beta}\,, \qquad |bu_\lambda-a_\lambda|\leqq c\cdot\tau^{m-(m-1)d\beta}$$

for $1\leqq\lambda\leqq d$, *in which* c *is a constant.*

A proof of the above theorem can be "extracted" from Birch [1]; we have clarified the nature of τ_0 and also we have included $r_1(y),\cdots,r_d(y)$ with variable real coefficients.

Corollary. *We put* $\sigma=(m-1)^{-1}\sigma_0$; *then for any* $\varepsilon>0$ *there exists a positive integer* b_ε *depending only on* ε *such that if* $a_1,\cdots,a_d,b$ *are relatively prime integers and* $b\geqq b_\varepsilon$, *then*

$$\left|\sum_{0\leqq\tau_{i\lambda}<b} e\left(b^{-1}\cdot\sum_{\lambda=1}^{d} a_\lambda(g_\lambda(\eta)+r_\lambda(\eta))\right)\right| < b^{dn-\sigma+\varepsilon}\,.$$

For the sake of completeness we shall give a proof: we may assume that $\varepsilon<\sigma$; put

$$\beta=1/(m-1)d-\varepsilon/2d\sigma_0\,, \qquad \alpha=\sigma_0\beta-\varepsilon/2d\,,$$

and define b_ε as the smallest integer satisfying

$$b_\varepsilon > c^{(1-(m-1)d\beta)^{-1}}\,, \qquad \tau_0^{-1}\,;$$

then b_ε depends only on ε. Define a box B in Y_R by the condition that every $y_{i\lambda}$ satisfies $0\leqq y_{i\lambda}<1$ and put $\tau=b^{-1}$, $u_\lambda=a_\lambda b^{-1}$ for $1\leqq\lambda\leqq d$. Then the alternative (2) can easily be rejected, and the estimate (1) can be rewritten as in the corollary.

A remarkable feature of this corollary is that the estimate holds uniformly in $r_1(y),\cdots,r_d(y)$; this will permit us to prove Lemma 6 in a form more general than we need in this paper.

§ 9. Case 4

We shall apply Theorem 1 to $f(x)$; clearly if

$$\sigma=\operatorname{codim}(S_f)/2^{m-1}(m-1)>1\,,$$

then (C1) is satisfied. We shall proceed to show that if $\sigma>2d$, then (C2) is also satisfied: we shall denote by e_p the product of $\boldsymbol{Q}_p\to\boldsymbol{Q}_p/\boldsymbol{Z}_p\to\boldsymbol{R}/\boldsymbol{Z}$ and $\boldsymbol{e}$; we put $Y_p=M_{n,d}(\boldsymbol{Q}_p)$, $Y_p^0=M_{n,d}(\boldsymbol{Z}_p)$, and denote by $|dy|_p$ the Haar measure on Y_p such that Y_p^0 has measure 1. Then for every Ψ_p in $\mathscr{S}(Y_p)$ the following integral:

$$G_{\Psi_p}^*(u^*)=\int_{Y_p}\Psi_p(y)e_p\left(\sum_{\lambda=1}^{d}u_\lambda^*g_\lambda(y)\right)|dy|_p$$

defines a bounded locally constant function $G_{\Psi_p}^*$ on $\boldsymbol{Q}_p^d$.

Lemma 6. *Suppose that* Ψ_p *is the characteristic function of a coset in* Y_p/Y_p^0; *then for every* u^* *in* $\boldsymbol{Q}_p^d$ *such that*

$$|u^*|_p=\max\{|u_1^*|_p,\cdots,|u_d^*|_p\}\geqq b_\varepsilon$$

we have

$$|G_{\Psi_p}^*(u^*)|\leqq|u^*|_p^{-\sigma+\varepsilon}\,.$$

Proof. We choose a representative y^0 of the coset such that y^0 is a rational matrix with a non-negative power of p as its denominator; and we replace u^* by a similar rational vector without affecting $G_{\Psi_p}^*(u^*)$ and $|u^*|_p$. In this way the lemma is reduced to the following statement: suppose that $h_1(y),\cdots,h_d(y)$ are polynomials of degree $m-1$ in $y_{i\lambda}$ with coefficients in $p^{-e_0}\boldsymbol{Z}$ and $a_1,\cdots,a_d$ are integers not all divisible by p; then we have

$$(\sharp) \qquad \left|\int_{Y_p^0} e_p\left(p^{-e}\cdot\sum_{\lambda=1}^{d}a_\lambda(g_\lambda(y)+h_\lambda(y))\right)|dy|_p\right|\leqq(p^e)^{-\sigma+\varepsilon}$$

provided that $p^e\geqq b_\varepsilon$; and the proof is as follows:

We choose $e_1\geqq e+e_0$; then the left hand side of ($\sharp$) becomes

$$\left|p^{-e_1dn}\cdot\sum_{\eta \bmod p^{e_1}} e\left(p^{-e}\cdot\sum_{\lambda=1}^{d}a_\lambda(g_\lambda(\eta)+h_\lambda(\eta))\right)\right|\,.$$

We may assume that $0\leqq\eta_{i\lambda}<p^{e_1}$ for every i,λ and we decompose η into $\eta'+\eta''$ where $0\leqq\eta'_{i\lambda}<p^e$; then for each η'' we can write

$$g_\lambda(y+\eta'')+h_\lambda(y+\eta'')=g_\lambda(y)+r_\lambda(y)\,,$$

in which $r_\lambda(y)$ is a polynomial of degree $m-1$ in $y_{i\lambda'}$ with rational coefficients. Therefore by the "corollary" we get

$$\left|\sum_{0\leqq\eta'_{i\lambda}<p^e} e\left(p^{-e}\cdot\sum_{\lambda=1}^{d}a_\lambda(g_\lambda(\eta'+\eta'')+h_\lambda(\eta'+\eta''))\right)\right|<(p^e)^{dn-\sigma+\varepsilon}\,;$$

hence the left hand side of ($\sharp$) is less than

$$p^{-e_1dn}\cdot\operatorname{card}\{\eta''\}\cdot(p^e)^{dn-\sigma+\varepsilon}=(p^e)^{-\sigma+\varepsilon}\,. \qquad \text{q.e.d.}$$

We shall denote by tr the trace from k to $\boldsymbol{Q}$ and define a $\boldsymbol{Z}$-basis $\{\bar{\omega}_1, \cdots, \bar{\omega}_d\}$ of the inverse of the different of k by the condition $\mathrm{tr}\,(\omega_i\bar{\omega}_{i'}) = \delta_{ii'}$. On the other hand we define a character e_∞ of $\boldsymbol{Q}_\infty = \boldsymbol{R}$ as $e_\infty(t) = e(-t)$ and for a moment we allow $p = \infty$. Then for every valuation v on k dividing p the product $\psi_v = e_p \circ \mathrm{tr}_v$, where tr_v denotes the trace from k_v to $\boldsymbol{Q}_p$, gives a character of k_v; and there exists a unique character ψ of k_A/k with ψ_v as its v-component.

After this remark we shall assume that $p \neq \infty$ and fix the following product isomorphism:

$$\boldsymbol{Q}_p^d \longrightarrow \boldsymbol{Q}_p \otimes_{\boldsymbol{Q}} k \longrightarrow \sum_{v|p} k_v \ ,$$

in which the first isomorphism is given by

$$u^* \longrightarrow \sum_{i=1}^{d} u_i^*(1 \otimes \bar{\omega}_i)$$

and the second isomorphism comes from the injections $k \to k_v$; we shall also fix the following product isomorphism:

$$Y_p \xrightarrow{1\otimes\pi} \boldsymbol{Q}_p \otimes_{\boldsymbol{Q}} X_k \longrightarrow \prod_{v|p} X_v \ ,$$

in which the second isomorphism comes from the injections $X_k \to X_v$. We express the above isomorphisms as $u^* \to (i_v^*)_v$ and $y \to (x_v)_v$. We choose Φ_v from $\mathscr{S}(X_v)$ for every v dividing p and define Ψ_p in $\mathscr{S}(Y_p)$ as

$$\prod_{v|p} \Phi_v(x_v) = \Psi_p(y) \ ;$$

then we get

$$\prod_{v|p} F^*_{\Phi_v}(i_v^*) = c_p \cdot G^*_{\Psi_p}(u^*) \ ,$$

in which $c_p = 1$ if p does not divide the discriminant Δ_k of k. Finally if d_v denotes the degree of k_v over $\boldsymbol{Q}_p$, then

$$\|u^*\|_p = \max_{v|p} \{|i_v^*|_v^{1/d_v}\}$$

defines a norm on $\boldsymbol{Q}_p^d$; and $\|u^*\|_p = |u^*|_p$ if p does not divide Δ_k.

Suppose that v divides $p \geqq b_\iota$, $|\Delta_k| + 1$; denote by Φ_w the characteristic function of a coset in X_w/X_w^0 for every w dividing p; then the above Ψ_p becomes the characteristic function of a coset in Y_p/Y_p^0. Therefore if we take $i_w^* = 0$ for every w dividing p but different from v, then by Lemma 6 we get

$$|F^*_{\Phi_v}(i^*)| = |G^*_{\Psi_p}(u^*)| \leqq \max(1, |u^*|_p)^{-\sigma+\varepsilon}$$
$$= \max(1, |i^*|_v)^{(-\sigma-\varepsilon)/d_v}$$

for every $i^* = i_v^*$ in k_v. This shows that (C2) is satisfied if $\sigma > 2d$. We have thus obtained the following theorem:

Theorem 3. *Let k denote an algebraic number field and $f(x)$ a homogeneous polynomial of degree $m \geqq 2$ with coefficients in k; assume that*

$$\sigma = \mathrm{codim}\,(S_f)/2^{m-1}(m-1) > 2[k:\boldsymbol{Q}] \ ;$$

then the Poisson formula

$$\sum_{i \in k} |\theta_i|_A = \sum_{i^* \in k} \psi(i^* f(x))$$

holds.

A similar Poisson formula holds also in the function-field case; the proof in that case is simpler because $\mathscr{S}(X_A)$ coincides with the $\boldsymbol{C}$-span of characteristic functions of "boxes"; cf. [9]. We might add that if our conjecture (stated after Theorem 1) is correct, then the condition $\sigma > 2[k:\boldsymbol{Q}]$ can be replaced by $\sigma > 2$.

References

[1] Birch, B. J., Forms in many variables, Proc. Royal Soc. A, **265** (1962), 245–263.
[2] Hironaka, H., Resolution of singularities of an algebraic variety over a field of characteristic zero, Ann. Math. **79** (1964), 109–326.
[3] Igusa, J., On the arithmetic of Pfaffians, Nagoya Math. J. **47** (1972), 169–198.
[4] ——, Complex powers and asymptotic expansions, I, J. reine angew, Math. **268/269** (1974), 110–130; II, ibid. **278/279** (1975), 307–321.
[5] ——, On a certain Poisson formula, Nagoya Math. J. **53** (1974), 211–233.
[6] ——, A Poisson formula and exponential sums, J. Fac. Sci. Univ. Tokyo I.A. **23** (1976), 223–244.
[7] Lang, S. and Weil, A., Number of points of varieties in finite fields, Amer. J. Math. **76** (1954), 819–827.
[8] Levin, M., A continuity problem in the Siegel-Weil formula, TR 74–10 (1974), University of Maryland.
[9] Li, I.-H., Forms in many variables with coefficients in function field, Thesis, Johns Hopkins University, 1976.
[10] Mars, J. G. M., Les nombres de Tamagawa de certains groupes exceptionnels, Bull. Soc. Math. France, **94** (1966), 97–140.
[11] Weil, A., Adeles and algebraic groups, Lecture Note, Inst. Adv. Study, Princeton, 1961.
[12] ——, Sur la formule de Siegel dans la théorie des groupes classiques, Acta Math. **113** (1965), 1–87.

Department of Mathematics
The Johns Hopkins University
Baltimore, Maryland 21218
U.S.A.

ALGEBRAIC NUMBER THEORY, Papers contributed for the International Symposium, Kyoto 1976; S. Iyanaga (Ed.): Japan Society for the Promotion of Science, Tokyo, 1977

On the Frobenius Correspondences of Algebraic Curves

YASUTAKA IHARA

Introduction

1. Our study was motivated by the desire to find all congruence relations of the form $\mathcal{T} \equiv \Pi + \Pi' \pmod{\mathfrak{p}}$, where $\mathcal{T}$ is an algebraic correspondence of an algebraic curve $\mathcal{C}$ over a $\mathfrak{p}$-adic field having a good reduction C, Π is the $N(\mathfrak{p})$-th power Frobenius correspondence of C, and Π' is its transposed correspondence. This type of relations has been known for the Hecke correspondences $\mathcal{T} = T(p)$ of modular curves by Kronecker, Eichler, Shimura and Igusa, and for the generalized Hecke correspondences associated to quaternionic modular groups, by Shimura [7] [8] (supplemented by Y. Morita). For the applications to the arithmetic of algebraic curves over finite fields as those given in [5], it is desirable that one can find all possible relations of this type, *especially starting from any given curve C over finite field*. Thus we meet the problem of finding all *deformations* $(\mathcal{C}; \mathcal{T})$ of the pair $(C; \Pi + \Pi')$ of a curve C and a divisor $\Pi + \Pi'$ on $C \times C$, including especially the deformations changing the characteristic. The purpose of this paper is to present a full exposition of our results in this direction which were announced in the Symposium.

2. We shall formulate the problem in a precise and slightly generalized form. Take a complete discrete valuation ring R with finite residue field $\boldsymbol{F}_q$. Let C be a proper smooth geometrically irreducible[1] algebraic curve of genus $g > 1$ over $\boldsymbol{F}_q$. Put $C' = C$, and consider the product $C \times C'$ over $\boldsymbol{F}_q$. Let Π (resp. Π') be the graph on $C \times C'$ of the q-th power Frobenius morphism $C \to C'$ (resp. $C' \to C$). Consider $T = \Pi + \Pi'$ as a reduced subscheme of $C \times C'$. The singularities of T consist of all geometric points of $\Pi \cap \Pi'$.

1) This assumption of *geometric* irreducibility can be dropped, with only slight modifications; see § 16.

They are the points of the form $(\bar{Q}, \bar{Q}^q)$, where $\bar{Q}$ runs over all F_{q^2}-rational points of C. In particular, $\deg(\Pi \cap \Pi')$ equals the number of F_{q^2}-rational points of C.

Problem A. *Find all triples $(\mathscr{C}, \mathscr{C}'; \mathscr{T})$ consisting of two proper smooth R-schemes $\mathscr{C}, \mathscr{C}'$ and an R-flat closed subscheme $\mathscr{T} \subset \mathscr{C} \times_R \mathscr{C}'$, such that $\mathscr{C} \otimes_R F_q = C$, $\mathscr{C}' \otimes_R F_q = C'$ and $\mathscr{T} \times_{\mathscr{S}} (C \times C') = T$, where $\mathscr{S} = \mathscr{C} \times_R \mathscr{C}'$.*

Let π be a prime element of R and put $R_n = R/\pi^{n+1}$ $(n \geq 0)$, so that $R_0 = F_q$. When X_n is an R_n-scheme and $0 \leq m \leq n$, we write $X_m = X_n \otimes_{R_n} R_m$ and call X_n an *extension* of X_m. When we speak of a *triple* $(C_n, C_n'; T_n)$ *over* R_n, it will always be assumed that C_n and C_n' are proper smooth R_n-schemes that extend C and C' respectively, and that T_n is an R_n-flat closed subscheme of $S_n = C_n \times C_n'$ (the product is over R_n) such that $T_n \times_{S_n} (C \times C') = T$. A triple $(C_n, C_n'; T_n)$ over R_n is called an *extension* of $(C_m, C_m'; T_m)$ if C_n and C_n' are extensions of C_m and C_m' respectively and if $T_m = T_n \times_{S_n} S_m$. Now by the Grothendieck existence theorem ([1] [2], or [6]), Problem A is equivalent to:

Problem $\tilde{\text{A}}$. *Find all infinite sequences $\{(C_n, C_n'; T_n)\}_{n=0}^{\infty}$ of successive extensions of triples over R_n starting from $(C, C'; T)$.*

They are equivalent because, first, C and C' being proper curves, we know by [2] III and [1] III § 5.4 that each sequence $\{C_n\}$ (resp. $\{C_n'\}$) determines $\mathscr{C}$ (resp. $\mathscr{C}'$) uniquely, and secondly by [1] III (5.1.8, 5.4.1), $\{T_n\}$ corresponds to a unique closed subscheme $\mathscr{T}$ of $\mathscr{C} \times_R \mathscr{C}'$. So our problem is reduced to solving the following problem for the general $n \geq 1$:

Problem A_n. *Find all extensions $(C_n, C_n'; T_n)$ over R_n of a given triple $(C_{n-1}, C_{n-1}'; T_{n-1})$ over R_{n-1}.*

3. We shall now describe our main results on Problem A_n, together with the organization of this paper.

In the first four sections (§§ 4 ~ 7), we shall approach the problem by the cohomological method. Let E be the kernel of the canonical sheaf-homomorphism $\Theta \to N_T$, where Θ is the tangent sheaf of $C \times C'$ and N_T is the normal sheaf of T in $C \times C'$. Our first observation is the vanishing of $H^1(E)$ (Proposition 1, § 4). This follows from the surjectivity of the Cartier operator $\gamma: W(p^{i+1}K_C) \to W(p^iK_C)$ $(i \geq 0)$ on C (Lemma 1, § 4). The vanishing of $H^1(E)$ then leads directly to a certain uniqueness theorem. To explain this, let $(C_{n-1}, C_{n-1}'; T_{n-1})$ be the given triple over R_{n-1}, let P be a point of $C \times C'$, and let

U_{n-1} be a small affine open neighborhood of P in $C_{n-1} \times C_{n-1}'$. Consider a pair $(U_n, T_n(U_n))$ of a smooth R_n-scheme U_n extending U_{n-1} and an R_n-flat closed subscheme $T_n(U_n) \subset U_n$ extending $T_{n-1} \cap U_{n-1}$. Such a pair of local extensions exists always, and up to isomorphisms over U_{n-1}, it is unique when $P \notin \Pi \cap \Pi'$, while there are $q^{\deg P}$ distinct such pairs when $P \in \Pi \cap \Pi'$. For each $P \in \Pi \cap \Pi'$, let $\mathscr{L}_P$ be the set of germs of isomorphism classes of $(U_n, T_n(U_n))$ at P, and put $\mathscr{L} = \prod_P \mathscr{L}_P$. Then our uniqueness theorem states that *for any given $l = (l_P) \in \mathscr{L}$, the solution $(C_n, C_n'; T_n)$ of* Problem A_n*, with which $(C_n \times C_n', T_n)$ belongs to l_P at each $P \in \Pi \cap \Pi'$, is at most unique* (Theorem 1, § 6)[1]. Thus, the next problem is to investigate the existence of $(C_n, C_n'; T_n)$ for each l. This existence turns out to be equivalent with the vanishing of the obstruction class $\wp(l)$ which is an element of a $4(q-1)(g-1)$ dimensional F_q-module

$$\boldsymbol{Obs} = \operatorname{Ker}(H^2(E) \longrightarrow H^2(\Theta)) \qquad (\S\, 6)\,.$$

But $\wp(l)$ does not usually vanish, and our next attention will be directed to the nature of the mapping $\beta: \mathscr{L} \to \boldsymbol{Obs}$ defined by $l \to \wp(l)$ (§ 7). Let N_T^0 be the image of $\Theta \to N_T$ and consider the $\deg(\Pi \cap \Pi')$-dimensional F_q-module $H^0(N_T/N_T^0)$. Then $\mathscr{L}$ forms a principal homogeneous space of $H^0(N_T/N_T^0)$, and β turns out to be *equivariant* with the canonical group-homomorphism $H^0(N_T/N_T^0) \to \boldsymbol{Obs}$. (By this, we observe, for example, that the solution of Problem A is at most unique if it is so for Problem A_1 (Corollary 2 of Proposition 2).) But this is not yet sufficient for our purpose, as this describes our mapping β *only up to unknown translations in* $\boldsymbol{Obs}$. The determination of β itself seems to offer a serious arithmetic question, except in the trivial case where $R_n = F_q[[t]]/t^{n+1}$ and $(C_{n-1}, C_{n-1}'; T_{n-1})$ is the obvious extension of $(C, C'; T)$. This is the starting point of the main part of our study.

To proceed further, we shall forget about l, and look closely at the *differential invariants* of the related Frobenius mappings modulo π^{n+1} (§§ 8 ~ 11). Suppose for simplicity that $R = \boldsymbol{Z}_p$ (the ring of p-adic integers) and that $C_{n-1}' = C_{n-1}$. Let $\mathfrak{R}_{n-1}$ denote the local ring at the generic point of C_{n-1}. It is a unique R_{n-1}-flat local ring having (p) as the maximal ideal and $F_p(C)$ (the function field of C) as the residue field. The finite étale extensions of $\mathfrak{R}_{n-1}$ correspond bijectively with the finite separable extensions of the residue field $F_p(C)$. Let $\tilde{\mathfrak{R}}_{n-1}$ be the maximum étale extension of $\mathfrak{R}_{n-1}$. Then our main result in

1) It is noteworthy that the familiar concept of supersingularity in $g=1$ does not appear at this stage. In this sense, there are no exceptions for $g>1$!

this case takes the following form; *there is a canonical bijection*

$$(*) \qquad (C_n, C_n'; T_n) \longrightarrow (\omega_{n-1}, \omega_{n-1}')$$

between the set of all solutions of Problem A_n *and the set of all ordered pairs* $(\omega_{n-1}, \omega_{n-1}')$ *of differentials* $\omega_{n-1}, \omega_{n-1}'$ *of* $\tilde{\mathfrak{K}}_{n-1}$ *that are "of type* T_n^P" *at every* $P \in T$; *where* $(C_n, C_n'; T_n)$ *are counted up to isomorphisms* and $(\omega_{n-1}, \omega_{n-1}')$ are up to termwise multiplications of elements of $R_{n-1}^{\times}$ (Theorem 4, § 11).

To explain this, let C_n, C_n' be any smooth extensions of C_{n-1} over R_n, $U_n \subset C_n \times C_n'$ be an affine open set, and $T_n(U_n)$ be an R_n-flat closed subscheme of U_n extending an open set of T_{n-1}. Then $T_n(U_n) - \Pi'$ (resp. $T_n(U_n) - \Pi$), unless empty, can be considered as graphs of local morphisms $C_n \to C_n'$ (resp. $C_n' \to C_n$). Let $\sigma_n : \mathfrak{K}_n' \to \mathfrak{K}_n$ (resp. $\sigma_n' : \mathfrak{K}_n \to \mathfrak{K}_n'$) be the corresponding local homomorphisms at the generic points of C_n, C_n'. Note that $\mathfrak{K}_n/p^n$ and $\mathfrak{K}_n'/p^n$ can be identified with $\mathfrak{K}_{n-1}$, and that there is an isomorphism $\iota_n : \mathfrak{K}_n \xrightarrow{\sim} \mathfrak{K}_n'$ inducing the identity of $\mathfrak{K}_{n-1}$. After identifying $\mathfrak{K}_n$ and $\mathfrak{K}_n'$ via ι_n, we may regard σ_n and σ_n' as endomorphisms of $\mathfrak{K}_n$ inducing the p-th map modulo p. Let $\tilde{\mathfrak{K}}_n$ be the maximum étale extension of $\mathfrak{K}_n$. Then σ_n (resp. σ_n') can be extended uniquely to an endomorphism of $\tilde{\mathfrak{K}}_n$ inducing the p-th power map modulo p, which we shall denote also by σ_n (resp. σ_n'). By a general argument (§ 9), we can prove that there exists a differential ω_n (resp. ω_n') of $\tilde{\mathfrak{K}}_n$, not divisible by p, such that

$$\omega_n^{\sigma_n} = p\omega_n \qquad (\text{resp. } \omega_n'^{\sigma_n'} = p\omega_n') .$$

Moreover, if ω_{n-1} (resp. ω_{n-1}') denote the differentials of $\tilde{\mathfrak{K}}_{n-1}$ obtained by reduction of ω_n (resp. ω_n') modulo p^n, then ω_{n-1} (resp. ω_{n-1}') are uniquely determined modulo multiples of elements of $R_{n-1}^{\times}$, and they are independent of the choice of ι_n. *Consider the ordered pair* $(\omega_{n-1}, \omega_{n-1}')$ *as a differential invariant of* $(C_n, C_n'; T_n(U_n))$. In particular, we can associate to each solution $(C_n, C_n'; T_n)$ of Problem A_n its invariant $(\omega_{n-1}, \omega_{n-1}')$, and this defines the map $(*)$. A pair $(\omega_{n-1}, \omega_{n-1}')$ of differentials of $\tilde{\mathfrak{K}}_{n-1}$ is called "*of type* T_n^P" *at* $P \in T$, if there exists a small affine open neighborhood U_n of P on $C_n \times C_n'$, on which we can draw a local extension $T_n(U_n)$ of T_{n-1} in such a way that the invariant $(\omega_{n-1}^P, \omega_{n-1}'^P)$ of $(C_n, C_n'; T_n(U_n))$ coincides with $(\omega_{n-1}, \omega_{n-1}')$ up to termwise multiplications of elements of $R_{n-1}^{\times}$. (Here, when $P \notin \Pi$ (resp. $P \notin \Pi'$), so that ω_{n-1}^P (resp. $\omega_{n-1}'^P$) is not defined, the corresponding coincidence condition is considered as empty.) Since this condition is local, the choice of C_n or C_n' has no influence on this. In the proof of the bijectivity of $(*)$, a certain auxiliary sheaf F on

$C \times C'$, a coherent $\mathcal{O}_{C\times C'}^p$-Module such that $E \subset F \subset \Theta$, plays a crucial role.

This is a principle which could be used effectively only after one obtains a more explicit description of the above local condition for $(\omega_{n-1}, \omega_{n-1}')$. For the general n, the author could not succeed in rewriting this in sufficiently explicit terms, perhaps because of his present unfamiliarity with the world in which these differentials live; i.e., some ramified coverings of curves mod p^n. But for $n = 1$, our principle leads directly to the solution of Problem A_1 (Theorem 5, § 12). The solutions $(C_1, C_1'; T_1)$ are in a natural one-to-one correspondence with the pairs $(\omega_0^{\otimes(p-1)}, \omega_0'^{\otimes(p-1)})$ of differentials of degree $p-1$ on C characterized by explicit conditions. This gives an effective method for calculating the number of $(C_1, C_1'; T_1)$ for any given C. For example, let C be the Madan-Queen plane quartic:

$$y^4 + (x^3 + x^2z + z^3)y + (x^4 + xz^3 + z^4) = 0 \qquad \text{over } \boldsymbol{F}_2 .$$

Then there are no solutions $(C_1, C_1'; T_1)$ over $\boldsymbol{Z}/4$; hence *a priori* no solutions of Problem A for $R = \boldsymbol{Z}_2$. On the other hand, for the plane quartic:

$$y^4 + (x + z)y^3 + xy^2z + (x + z)^3y + x^2z^2 = 0 \qquad \text{over } \boldsymbol{F}_2 ,$$

there is exactly one solution $(C_1, C_1'; T_1)$ over $\boldsymbol{Z}/4$. We do not know whether it extends further up to a solution of Problem A (although we know by Corollary 2 of Proposition 2 that such an extension is at most unique). These, and other examples are given in § 15.

We add here the following remark. In our previous work, we have shown that wherever there is a congruence relation, there is a certain differential associated to it, and then studied some properties of this differential (cf. [4], and also "Non-abelian invariant differentials and Schwarzian equations in the p-adic theory of automorphic functions", US-Japan Seminar on Number Theory, Tokyo 1971[1]). Our present work gives a *partial inverse* of this process.

It is my pleasure to express my gratitude to E. Horikawa who guided me to his theory of deformations of varieties carrying divisors ([3]) which was very helpful in the first part of this study. I am also grateful to T. Shioda and S. Iitaka for their valuable conversations with me in connection with this problem.

Notations and conventions

In addition to the basic notation introduced in § 2, we shall also frequently use the following notations and conventions.

1) Available at the Univ. of Tokyo.

For each $0 \leq m \leq n$ and an R_n-algebra A_n (resp. an R_n-scheme X_n), we write $A_m = A_n \otimes_{R_n} R_m$ (resp. $X_m = X_n \otimes_{R_n} R_m$). Similarly, for each $f_n \in A_n$, f_m will denote its image $f_n \otimes 1$ in A_m. In this case, A_n (resp. X_n, f_n) is called an *extension* of A_m (resp. X_m, f_m). If Y_n is a subscheme of X_n, we write $Y_m = Y_n \times_{X_n} X_m$, and call Y_n an extension of Y_m on X_n. Note that X_n and X_m have the same base topological spaces. For each i $(0 \leq i \leq n)$, the product $\pi^{n-i} \cdot f_i$ $(f_i \in A_i)$ makes sense as an element of A_n.

A triple $(C_n, C_n'; T_n)$ is always assumed to satisfy the conditions in Problem $\tilde{\mathrm{A}}$, i.e., C_n (resp. C_n') is a proper smooth R_n-scheme extending C (resp. C'), and T_n is an R_n-flat closed subscheme of $C_n \times C_n'$ extending T. *Solutions* $(C_n, C_n'; T_n)$ of Problem A_n are always counted up to *equivalence* $(C_n, C_n'; T_n) \sim (C_n^*, C_n^{*\prime}; T_n^*)$; which consists of two R_n-isomorphisms $\varepsilon : C_n \xrightarrow{\sim} C_n^*$ and $\varepsilon' : C_n' \xrightarrow{\sim} C_n^{*\prime}$ extending the identities of C_{n-1} and C_{n-1}' (respectively) and satisfying $(\varepsilon \times \varepsilon')(T_n) = T_n^*$.

If X is any scheme, $\mathcal{O}_X$ will denote its structure sheaf. A *point* $P, Q, \cdots \in X$ means a scheme-theoretic closed point of X. For the *geometric points*, we shall use the letters $\bar{P}, \bar{Q}, \cdots$, etc. (For example, if $P = (Q, Q')$ is a point of T with the projections Q, Q' on C, C', respectively, then $Q = Q'$ by the identification $C = C'$; but if $\bar{P} = (\bar{Q}, \bar{Q}')$ is a geometric point of T, then either $\bar{Q}' = \bar{Q}^q$ or $\bar{Q} = \bar{Q}'^q$.) The local ring of X at P will be denoted by $O_{X,P}$. When X is either a curve or a surface which is proper smooth and irreducible over F_q, and D is a divisor on X, we denote by $\mathcal{O}(D) = \mathcal{O}_X(D)$ the corresponding invertible sheaf on X (the sheaf of germs of rational functions f on X satisfying $f \succ -D$), and write

$$l(D) = \dim_{F_q} H^0(\mathcal{O}_X(D)) ,$$

as usual.

Cohomological approach

4. We shall consider here the following two sheaves on $C \times C'$;

Θ: the tangent sheaf of $C \times C'$;

E: the kernel of the canonical homomorphism $\Theta \to N_T$,

where N_T is the normal sheaf of T (in $C \times C'$). By definition, if $U = \operatorname{Spec} A$ is any affine open set of $C \times C'$ which is so small that $T \cap U$ is defined by a single equation $f = 0$ on U, then $\Gamma(U, \Theta)$ (resp. $\Gamma(U, E)$) consists of all derivations $\delta : A \to A$ over F_q (resp. all $\delta \in \Gamma(U, \Theta)$ satisfying $\delta f \in (f)$).

To express Θ and E as direct sums of invertible sheaves, take any rational function x on C which is not a p-th power in the function field of C, and let y be the corresponding function on C'. Let K_C (resp. $K_{C'}$) be the divisor of dx (resp. dy) on C (resp. C') and put

$$K = K_C \times C' , \qquad K' = C \times K_{C'} .$$

Then each local section δ of Θ can be expressed uniquely as $\delta = a(\partial/\partial x) + b(\partial/\partial y)$, where a (resp. b) is a local section of $\mathcal{O}(-K)$ (resp. $\mathcal{O}(-K')$). This decomposition will be expressed as

$$\Theta = \Theta_1 \oplus \Theta_2 = \mathcal{O}(-K)\frac{\partial}{\partial x} \oplus \mathcal{O}(-K')\frac{\partial}{\partial y} . \tag{4.1}$$

A similar decomposition is possible for E, due to the particular circumstance that Π, Π' are graphs of *inseparable* morphisms. In fact, let $P = (Q, Q') \in T$, and take a rational function x_P on C which is finite at Q, $dx_P \neq 0$ at Q, and such that the value of x_P at Q generates the residue field of Q over F_q[1]. Let y_P be the corresponding function on C' and put $h = y_P - x_P^q$, $h' = x_P - y_P^q$ and $f = hh'$. Then $h = 0$, $h' = 0$ and $f = 0$ are local equations at P for Π, Π' and T, respectively. But since $\partial h/\partial x = \partial h'/\partial y = 0$ (by the inseparability), we obtain

$$\delta f = (y_P - x_P^q)a\frac{dx_P}{dx} + (x_P - y_P^q)b\frac{dy_P}{dy} ;$$

and since a and b are local sections of $\mathcal{O}(-K)$ and $\mathcal{O}(-K')$ respectively, $a(dx_P/dx)$ and $b(dy_P/dy)$ are finite at P. Since the local ring $O_{C\times C',P}$ is regular and hence it is a unique factorization domain, $\delta f \in (f)$ holds if and only if $a(dx_P/dx)$ and $b(dy_P/dy)$ are divisible (at P) by $x_P - y_P^q$ and $y_P - x_P^q$, respectively. This implies that δ belongs to a local section of E if and only if a and b belong to the local sections of $\mathcal{O}(-K - \Pi')$ and $\mathcal{O}(-K' - \Pi)$ respectively. Therefore, (4.1) induces the decomposition

$$E = E_1 \oplus E_2 = \mathcal{O}(-K - \Pi')\frac{\partial}{\partial x} \oplus \mathcal{O}(-K' - \Pi)\frac{\partial}{\partial y} . \tag{4.2}$$

Let p_1 (resp. p_2) be the projection of $C \times C'$ to C (resp. C'), and Θ_C (resp. $\Theta_{C'}$) be the tangent sheaf of C (resp. C'). Then $\Theta_1 = p_1^*\Theta_C \otimes p_2^*\mathcal{O}_{C'}$ and

1) Such a function exists, since if z is any function on C whose value at Q generates the residue field of Q, but $dz=0$ at Q, then $x_P = z+t$ satisfies this condition for any prime element t at Q.

$\Theta_2 = p_1^*\mathcal{O}_C \otimes p_2^*\Theta_{C'}$. But since $H^0(\Theta_C) = H^0(\Theta_{C'}) = 0$ as $g \geq 2$, the Künneth formula gives the canonical isomorphisms

$$H^1(\Theta_C) \simeq H^1(\Theta_1)\ , \qquad H^1(\Theta_{C'}) \simeq H^1(\Theta_2)\ . \tag{4.3}$$

Therefore, $H^1(\Theta) \simeq H^1(\Theta_C) \oplus H^1(\Theta_{C'})$ (canonically), in which each direct summand is $3(g-1)$-dimensional over $\boldsymbol{F}_q$.

Proposition 1. *$H^1(E) = 0$.*

Proof. By $E = E_1 \oplus E_2$ and by symmetry, it suffices to prove that $H^1(E_1) = 0$. For this purpose, look at the exact sequence

$$0 \longrightarrow E_1 \longrightarrow \Theta_1 \longrightarrow \Theta_1/E_1 \longrightarrow 0\ , \tag{4.4}$$

which can be rewritten in terms of invertible sheaves as

$$0 \longrightarrow \mathcal{O}_{C\times C'}(-K - \Pi') \longrightarrow \mathcal{O}_{C\times C'}(-K) \xrightarrow{r} \mathcal{O}_{\Pi'}(-qK_{\Pi'}) \longrightarrow 0\ , \tag{4.5}$$

where r is defined by the *restriction to* Π', and $K_{\Pi'}$ is the canonical divisor of Π'. Since $l(-qK_{\Pi'}) = 0$, it suffices to prove the injectivity of $H^1(r)$: $H^1(\mathcal{O}_{C\times C'}(-K)) \to H^1(\mathcal{O}_{\Pi'}(-qK_{\Pi'}))$. Replace $H^1(\mathcal{O}_{C\times C'}(-K))$ by $H^1(\mathcal{O}_C(-K_C))$ (via (4.3)), and $H^1(\mathcal{O}_{\Pi'}(-qK_{\Pi'}))$ by $H^1(\mathcal{O}_C(-qK_C))$ (via $\Pi' \overset{p_2}{\sim} C' = C$). Then $H^1(r)$ is replaced by $\rho: H^1(\mathcal{O}_C(-K_C)) \to H^1(\mathcal{O}_C(-qK_C))$. But by the definition of Π', ρ is nothing but the homomorphism induced by the q-th power Frobenius operation $(a_{\lambda\mu}) \to (a_{\lambda\mu}^q)$ on 1-cocycles. Therefore, the dual of ρ has an interpretation as an iterate of the Cartier operator γ. In fact, put $q = p^f$ (p: a prime number). Then ρ is the dual of the homomorphism

$$\gamma^f: W(qK_C) \longrightarrow W(K_C)\ , \tag{4.6}$$

where, in general, $W(D)$ (for a divisor D on C) denotes the space of differentials ξ on C satisfying $\xi \succ -D$. Therefore, the proof is reduced to the surjectivity of (4.6), and hence to the following lemma:

Lemma 1. *Let C be a proper smooth irreducible algebraic curve over a perfect field κ of characteristic p, K_C be its canonical divisor, and D be any divisor of C satisfying $l(D) > 0$, $l(K_C - pD) = 0$. Then the Cartier operator*

$$\gamma: W(pD) \longrightarrow W(D) \tag{4.7}$$

is surjective.

To prove this, we may replace D by a positive divisor which is linearly

equivalent with D; so, we can assume that $D \succ 0$. Take any $\xi \in W(D)$ and express ξ as $\xi = u\,dv/v$. Put $\eta = u^p\,dv/v$. Then $\gamma(\eta) = \xi$. For each point $Q \in C$, let κ_Q be the residue field, let $t = t_Q$ be a local uniformization, and expand as $\eta = \sum_n c_n(Q)t_Q^n dt_Q$ with $c_n(Q) \in \kappa_Q$. Then since $\sum_Q tr_{\kappa_Q/\kappa}(c_{-1}(Q)) = 0$, there exists a differential ζ on C such that

$$\zeta - \sum_{i\geq 0} c_{-ip-1}(Q)t_Q^{-ip-1}dt_Q$$

is finite at all Q, which implies that $\gamma(\eta) - \gamma(\zeta)$ is a differential of the first kind. On the other hand, it follows directly from the condition $\xi = \gamma(\eta) \succ -D$ that $\zeta \succ -pD$. Therefore, $W(D)$ is covered by the sum of $\gamma(W(pD))$ and the space of differentials of the first kind. Therefore, it suffices to check that $\gamma(W(pD))$ contains all differentials of the first kind. To check this, take any differential ξ_1 of the first kind. By the same reason as above, there exists a differential η_1 such that $\gamma(\eta_1) = \xi_1$. Put $\eta_1 = \sum_n b_n(Q)t_Q^n dt_Q$. Then since ξ_1 is of the first kind, we have $b_{-ip-1}(Q) = 0$ for all $i \geq 0$; hence $\eta_1 - dw_Q$ is finite at Q for some rational function w_Q. Obviously, we can choose w_Q in such a way that (w_Q) belongs to the adele ring of the function field of C. Since $l(K_C - pD) = 0$, we can find a rational function w such that $w - (w_Q) \succ -pD$ for the adele (w_Q). Since the differentiation annihilates the p-th power elements, this implies that $dw - \eta_1 \succ -pD$. Therefore if we put $\eta_2 = \eta_1 - dw$, we have $\eta_2 \in W(pD)$ and $\gamma(\eta_2) = \xi_1$. This completes the proof of Lemma 1 and hence also that of Proposition 1.

Let

$$0 = H^1(E) \longrightarrow H^1(\Theta) \xrightarrow{\varphi} H^1(\Theta/E) \longrightarrow H^2(E) \xrightarrow{\psi} H^2(\Theta) \longrightarrow H^2(\Theta/E) = 0$$

be the cohomology exact sequence induced by $0 \to E \to \Theta \to \Theta/E \to 0$. We shall call

$$\boldsymbol{Obs} = \mathrm{Ker}\,(H^2(E) \xrightarrow{\psi} H^2(\Theta))\ . \tag{4.8}$$

It is canonically isomorphic to $\mathrm{Coker}\,(H^1(\Theta) \xrightarrow{\varphi} H^1(\Theta/E))$. Since

$$\dim H^1(\mathcal{O}_C(-qK_C)) = (2q+1)(g-1)\ ,$$

we have

$$\begin{aligned}\dim(\boldsymbol{Obs}) &= \dim H^1(\Theta/E) - \dim H^1(\Theta)\\ &= 2\{(2q+1)(g-1) - 3(g-1)\} = 4(q-1)(g-1)\ .\end{aligned}$$

Corollary. *$\dim(\boldsymbol{Obs}) = 4(q-1)(g-1)$.*

Since $\dim H^2(\Theta) = 6g(g-1)$ by the Künneth formula, we have:

(4.9) $\dim H^i(\Theta) = 0,\ 6(g-1),\ 6g(g-1)$ for $i = 0, 1, 2$,

(4.10) $\dim H^i(E) = 0,\ 0,\ (6g+4q-4)(g-1)$ for $i = 0, 1, 2$,

respectively.

5. Here, the *local questions* on the infinitesimal extensions of the pair $(C_{n-1} \times C'_{n-1}, T_{n-1})$ will be discussed. We start with some general remarks (R1) $\sim$ (R3).

Let A_n be any R_n-algebra. According to our conventions made above, we write $A_m = A_n \otimes_{R_n} R_m$ and $f_m = f_n \otimes 1$ $(f_n \in A_n)$ for any $0 \leq m \leq n$. (R1): An element $a_n \in A_n$ is a unit of A_n if and only if a_0 is a unit of A_0. This follows immediately from the fact that every element of A_n of the form $1 + \pi b_n$ $(b_n \in A_n)$ is a unit of A_n (because $\pi^{n+1} = 0$). (R2): Recall that A_n is flat over R_n if and only if $\mathrm{Ker}\,[\pi^i] = \mathrm{Image}\,[\pi^{n+1-i}]$ holds for all $i = 1, \cdots, n$; or equivalently, for $i = n$; where $[\pi^j]$ denotes the multiplication of π^j in A_n. (R3): Let $X_n = \mathrm{Spec}\, A_n$ be flat over R_n and Y_0 be a closed subscheme of X_0 defined by a single equation $f_0 = 0$, where f_0 is assumed to be a *non-zero-divisor* of A_0. Let Y_n be a closed subscheme of X_n. Then the following two conditions (i) (ii) for Y_n are equivalent;

(i) Y_n is flat over R_n and $Y_n \times_{X_n} X_0 = Y_0$,

(ii) there exists $f_n \in A_n$ extending f_0 such that Y_n is defined by a single equation $f_n = 0$ in X_n.

In fact, assuming (ii) we obtain directly that A_n/f_n is flat over R_n, which gives the implication (ii) $\Rightarrow$ (i). To verify the implication (i) $\Rightarrow$ (ii), assume (i) and let $\mathfrak{a}$ be the ideal of A_n defining Y_n. Since $(\mathfrak{a}, \pi)$ corresponds to Y_0, there is some $f \in A_n$ extending f_0 such that $(\mathfrak{a}, \pi) = (f, \pi)$, and we may choose f from $\mathfrak{a}$. Take any $\alpha \in \mathfrak{a}$ and write $\alpha = fg + \pi h$ $(g, h \in A_n)$, so that $\pi h \in \mathfrak{a}$. By the R_n-flatness of Y_n, this implies that $h \equiv \pi^n h' \pmod{\mathfrak{a}}$ with some $h' \in A_n$. Therefore, $\alpha \in (f) + \pi\mathfrak{a}$; therefore, $\mathfrak{a} \subset (f) + \pi\mathfrak{a}$ which leads to $\mathfrak{a} = (f)$, as $\pi^{n+1} = 0$ in A_n. This implies (ii).

Now suppose that a triple $(C_{n-1}, C'_{n-1}; T_{n-1})$ $(n \geq 1)$ is given. Let $U_{n-1} = \mathrm{Spec}\, A_{n-1}$ be an affine open set of $C_{n-1} \times C'_{n-1}$. By the general theory [2] Exp. III, there exists a smooth R_n-scheme U_n that extends U_{n-1}, and U_n is unique up to such R_n-isomorphisms that extend the identity of U_{n-1}. Moreover, if $\mathrm{Aut}\,(U_n/U_{n-1})$ denotes the group of all R_n-automorphisms of U_n that extend the identity of U_{n-1} (called *infinitesimal automorphisms* of U_n), then there is an isomorphism

(5.1) $\mathrm{Aut}\,(U_n/U_{n-1}) \simeq \Gamma(U_0, \Theta)$,

and in fact, there is a standard choice of this isomorphism once a prime element π of R is fixed. To write it down, take any $\delta \in \Gamma(U_0, \Theta)$ and let x_n be a local section of the structure sheaf of U_n. Then $x_n + \pi^n(\delta \cdot x_0)$ is another local section[1], and the collection of ring automorphisms $x_n \to x_n + \pi^n(\delta x_0)$ determines an element ε of $\mathrm{Aut}\,(U_n/U_{n-1})$. This mapping $\delta \to \varepsilon$ determines the standard isomorphism (5.1).

Now take a smooth R_n-scheme U_n extending U_{n-1}, and consider the question of infinitesimal extensions of $T_{n-1} \cap U_{n-1}$ on U_n. In doing this, we assume that U_{n-1} is so small that $T \cap U_0$ is defined by a single equation in U_0 and that U_n is also affine. Then by (R3), $T_{n-1} \cap U_{n-1}$ is also defined by a single equation $f_{n-1} = 0$ in U_{n-1}. Moreover, if f_n is any extension of f_{n-1} on U_n, the closed subscheme of U_n defined by $f_n = 0$ is R_n-flat and extends $T_{n-1} \cap U_{n-1}$. Conversely, any R_n-flat closed subschemes of U_n extending $T_{n-1} \cap U_{n-1}$ is obtained in this manner in view of (R3), (R1). Let f_n and $f_n + \pi^n z_0$ be two extensions of f_{n-1}, and let $T_n^\circ(U_n), T_n(U_n)$ be the corresponding closed subschemes of U_n. Let $\varepsilon \in \mathrm{Aut}\,(U_n/U_{n-1})$ correspond with $\delta \in \Gamma(U_0, \Theta)$ via (5.1). Then, as can be verified directly, the following conditions are equivalent:

(a) $T_n(U_n) = T_n^\circ(U_n)^\varepsilon$,

(b) $z_0 - \delta f_0 \in (f_0)$.

From this equivalence, we obtain the following two facts. First, ε leaves $T_n(U_n)$ invariant if and only if $\delta f_0 \in (f_0)$, i.e., $\delta \in \Gamma(U_0, E)$. This fact will be expressed briefly as

(5.2) $\mathrm{Aut}\,((U_n, T_n(U_n))/U_{n-1}) \simeq \Gamma(U_0, E)$ (induced from (5.1)) .

Secondly, $T_n^\circ(U_n)$ and $T_n(U_n)$ are equivalent (i.e., (a) holds with some $\varepsilon \in \mathrm{Aut}\,(U_n/U_{n-1})$) *if and only if* z_0 is contained in the ideal of $\Gamma(U_0, \mathcal{O}_{C\times C'})$ generated by f_0 and δf_0 where δ runs over all elements of $\Gamma(U_0, \Theta)$. But this is the ideal defining the singularities of T in U_0; i.e., the ideal corresponding to the closed subscheme $U_0 \cap \Pi \cap \Pi'$ of U_0. Therefore, if U_{n-1} is so small that U_0 contains at most one point of $\Pi \cap \Pi'$, then the number of equivalence classes of $T_n(U_n)$ is given by

$$\begin{array}{ll} 1 & \cdots \text{ when } U_0 \cap \Pi \cap \Pi' = \phi\ , \\ q^{\deg P} & \cdots \text{ when } U_0 \cap \Pi \cap \Pi' = \{P\}\ , \end{array}$$

1) Recall our conventions "$\pi^{n-i}a_i \in A_n$".

and in the latter case, the class of $T_n(U_n)$ is determined by $z_0(P)$, the value of z_0 at P. Since U_n itself is unique, this gives the number of extensions $(U_n, T_n(U_n))$ of $(U_{n-1}, T_{n-1} \cap U_{n-1})$ counted up to infinitesimal isomorphisms.

Each germ of (infinitesimal) isomorphism classes of $(U_n, T_n(U_n))$ at P will be called a *local class at* P. A mapping $P \to l_P$, which assigns to each $P \in \Pi \cap \Pi'$ a local class l_P at P, will be called a *local condition* (on $(C_{n-1}, C'_{n-1}; T_{n-1})$). There are q^{N_2} distinct local conditions, where

$$N_2 = \sum_{P \in \Pi \cap \Pi'} \deg P = \sum_{\substack{Q \in C \\ \deg Q \leq 2}} \deg Q \ .$$

We say that $(C_n, C'_n; T_n)$ *satisfies* the local condition $l = (l_P)$, when $(C_n \times C'_n; T_n)$ belongs to the class l_P at each $P \in \Pi \cap \Pi'$. Finally, when $\Pi \cap \Pi' = \phi$, we understand that there is one and only one local condition l on $(C_{n-1}, C'_{n-1}; T_{n-1})$.

6. Now we assign, in addition to $(C_{n-1}, C'_{n-1}; T_{n-1})$, a local condition $l = (l_P)$ on $(C_{n-1}, C'_{n-1}; T_{n-1})$ (see § 5). We shall formulate in cohomological terms the problem of finding all triples $(C_n, C'_n; T_n)$ extending $(C_{n-1}, C'_{n-1}; T_{n-1})$ and satisfying l.

First, since C_{n-1}, C'_{n-1} are smooth extensions of a curve C, there exist smooth R_n-schemes $C_n^*, C_n^{*\prime}$ that extend C_{n-1}, C'_{n-1} respectively (cf. [2]; indeed, this obstruction belongs to $H^2(C, \Theta_C) = 0$). We shall fix C_n^* and $C_n^{*\prime}$ for an auxiliary purpose. Let $C_{n-1} \times C'_{n-1} = \bigcup_\lambda U_{n-1}^\lambda$ be an affine open cover. Let U_n^λ be the open subscheme of $C_n^* \times C_n^{*\prime}$ having the same base space as U_{n-1}^λ. We may assume that our affine open cover is so fine that each U_n^λ is also affine and that $T_{n-1} \cap U_{n-1}^\lambda$ is defined by a single equation $f_{n-1}^\lambda = 0$. Take any such extension f_n^λ of f_{n-1}^λ on U_n^λ that $(U_n^\lambda, T_n^\lambda)$ belongs to the assigned local class, where T_n^λ is the closed subscheme of U_n^λ defined by $f_n^\lambda = 0$. Take any (λ, μ), and put $U_n^{\lambda\mu} = U_n^\lambda \cap U_n^\mu$. Then since $(U_n^{\lambda\mu}, T_n^\lambda \cap U_n^{\lambda\mu})$ and $(U_n^{\lambda\mu}, T_n^\mu \cap U_n^{\lambda\mu})$ belong to the same local class, there is an infinitesimal automorphism $\varepsilon^{\lambda\mu}$ of $U_n^{\lambda\mu}$ which transforms $T_n^\lambda \cap U_n^{\lambda\mu}$ to $T_n^\mu \cap U_n^{\lambda\mu}$. Let $\theta^{\lambda\mu}$ be the element of $\Gamma(U_0^{\lambda\mu}; \Theta)$ corresponding to $\varepsilon^{\lambda\mu}$, and put $\beta^{\lambda\mu\nu} = \theta^{\lambda\mu} + \theta^{\mu\nu} + \theta^{\nu\lambda} \in \Gamma(U_0^{\lambda\mu\nu}, E)$, where $U_n^{\lambda\mu\nu} = U_n^\lambda \cap U_n^\mu \cap U_n^\nu$ (see (5.2)). Then $(\beta^{\lambda\mu\nu})$ is a 2-cocycle of E. Let $\beta \in H^2(E)$ be its cohomology class. Then β does not depend on the choice of C_n^* and $C_n^{*\prime}$, nor on the choice of $\{U_{n-1}^\lambda\}, f_{n-1}^\lambda, f_n^\lambda$ and $\varepsilon^{\lambda\mu}$. It depends only on $(C_{n-1}, C'_{n-1}; T_{n-1})$ and l. Moreover, the image of β in $H^2(\Theta)$ vanishes, as $(\beta^{\lambda\mu\nu})$ is a 2-coboundary of Θ. Thus for each local condition l on a fixed triple $(C_{n-1}, C'_{n-1}; T_{n-1})$, we have defined an element $\beta = \beta(l) \in \boldsymbol{Obs} = \operatorname{Ker} \psi$.

It is clear that the existence of $(C_n, C'_n; T_n)$ satisfying l would imply $\beta = 0$.

Conversely, if $\beta = 0$, then we can replace $\theta^{\lambda\mu}$ by $\theta^{\lambda\mu} - e^{\lambda\mu}$, with some $e^{\lambda\mu} \in \Gamma(U_0^{\lambda\mu}, E)$ for each (λ, μ), to make $\theta^{\lambda\mu}$ a 1-cocycle, so that we can re-patch $(U_n^\lambda, T_n^\lambda)$ together to construct a pair (S_n, T_n), where S_n is a smooth R_n-scheme that extends $C_{n-1} \times C'_{n-1}$ and T_n is an R_n-flat closed subscheme of S_n extending T_{n-1}, satisfying l. But since the set of all infinitesimal isomorphism classes of smooth extensions of $C_{n-1} \times C'_{n-1}$ (resp. C_{n-1}, C'_{n-1}) over R_n forms a principal homogeneous space of $H^1(\Theta)$ (resp. $H^1(\Theta_C), H^1(\Theta_{C'})$) in the natural way (cf. [2] Exp. III, Theorem 6.3), and since we already examined that $H^1(\Theta) \simeq H^1(\Theta_C) \oplus H^1(\Theta_{C'})$ (canonically) (§ 4), S_n can be decomposed uniquely as $S_n = C_n \times C'_n$, where C_n, C'_n are smooth R_n-schemes extending C_{n-1}, C'_{n-1}. Therefore, the existence of $(C_n, C'_n; T_n)$ is equivalent with the vanishing of β. (That C_n, C'_n are *proper* over R_n follows automatically; in fact, $C_{n-1} \to \operatorname{Spec} R_n$ is proper, being the composite of the two proper morphisms $C_{n-1} \to \operatorname{Spec} R_{n-1}$ and $\operatorname{Spec} R_{n-1} \to \operatorname{Spec} R_n$, but since $C_{n-1} \to C_n$ is surjective (in fact, topologically bijective), $C_n \to \operatorname{Spec} R_n$ must also be proper; [1] II, 5.4.3).

Finally, since the set of all solutions $(C_n, C'_n; T_n)$ of Problem A_n satisfying l forms a principal homogeneous space of $H^1(E)$ in the natural manner, we obtain by Proposition 1 and its Corollary (§ 4) the following

Theorem 1. *The solutions $(C_n, C'_n; T_n)$ of Problem A_n satisfying a given local condition l on $(C_{n-1}, C'_{n-1}; T_{n-1})$ is at most unique, and the obstruction to its existence is an element $\beta(l)$ of $\boldsymbol{Obs} = \operatorname{Ker}(H^2(E) \xrightarrow{\psi} H^2(\Theta))$ which is a $4(q-1)(g-1)$ dimensional $\boldsymbol{F}_q$-module.*

7. To study the group theoretic structure of the mapping $l \to \beta(l)$, consider the sheaves N_T, N_T^0 and N_T/N_T^0 on T, where N_T is the normal sheaf of T and N_T^0 is the *image* of the canonical homomorphism $\Theta \to N_T$. Since this homomorphism is surjective outside the singular points of T, N_T/N_T^0 is with support in $\Pi \cap \Pi'$. From the two short exact sequences

$$0 \longrightarrow N_T^0 \longrightarrow N_T \longrightarrow N_T/N_T^0 \longrightarrow 0 \ , \tag{7.1}$$

$$0 \longrightarrow E \longrightarrow \Theta \longrightarrow N_T^0 \longrightarrow 0 \ , \tag{7.2}$$

we obtain a natural homomorphism

$$\beta_0 \colon H^0(N_T/N_T^0) \longrightarrow \boldsymbol{Obs} \ , \tag{7.3}$$

as the composite of the three homomorphisms, $H^0(N_T/N_T^0) \to H^1(N_T^0)$ (from (7.1)), $H^1(N_T^0) \to H^1(N_T^0)/H^1(\Theta)$ (the canonical homomorphism) and $H^1(N_T^0)/H^1(\Theta) \simeq \boldsymbol{Obs}$ (from (7.2)).

Fix $(C_{n-1}, C'_{n-1}; T_{n-1})$, and let $\mathscr{L}$ be the set of all local conditions $l = (l_P)$ on $(C_{n-1}, C'_{n-1}; T_{n-1})$. Then $H^0(N_T/N_T^0)$ acts on $\mathscr{L}$ in a simply transitive way as follows. Take any $P \in \Pi \cap \Pi'$, and a small affine neighborhood U_{n-1} of P on $C_{n-1} \times C'_{n-1}$. Since U_0 is affine, $\Gamma(U_0, N_T/N_T^0) = \Gamma(U_0, N_T)/\Gamma(U_0, N_T^0)$. Since N_T is the normal sheaf, there are isomorphisms $i_{f_0}: \Gamma(U_0, N_T) \simeq \Gamma(U_0, \mathcal{O}_T)$ defined with respect to each choice of local equation $f_0 = 0$ for T, whose dependence on f_0 being given by $i_{f_0'} = (f_0'/f_0) \cdot i_{f_0}$. Moreover i_{f_0} induces $\Gamma(U_0, N_T/N_T^0) \simeq \kappa_P$, where κ_P is the residue field of P. Now take any $\alpha_P \in \Gamma(U_0, N_T/N_T^0)$. Let U_n be a smooth extension of U_{n-1} over R_n and $f_n = 0$ be a closed subscheme of U_n representing the local class l_P. Then the local class represented by the closed subscheme $f_n - \pi^n i_{f_0}(\alpha_P) = 0$ on U_n depends only on α_P and l_P, which will be denoted by $l_P + \alpha_P$. Then $l_P \to l_P + \alpha_P$ gives a simply transitive action of $\Gamma(U_0, N_T/N_T^0)$ on the set $\mathscr{L}_P$ of all local classes l_P at P. Extending this to the direct sum over all $P \in \Pi \cap \Pi'$, we obtain a simply transitive action $l \to l + \alpha$ of $\alpha \in H^0(N_T/N_T^0)$ on $\mathscr{L}$. Now the following compatibility can be checked by a straightforward calculation.

Proposition 2. $\beta(l + \alpha) = \beta(l) + \beta_0(\alpha)$.

Let V be the kernel of β_0. It can be identified with the inverse image of $H^1(\Theta)$ by the above homomorphism $H^0(N_T/N_T^0) \to H^1(N_T^0)$.

Corollary 1. *The set of all $l \in \mathscr{L}$ such that $\beta(l) = 0$ is either empty or forms a single V-orbit in $\mathscr{L}$. In particular, the number of solution of Problem A_n for each given $(C_{n-1}, C'_{n-1}; T_{n-1})$ is either zero or $q^{\dim V}$.*

Corollary 2. *If Problem A_1 has a unique solution, then the solution of Problem A is at most unique.*

Associated differentials and a rescue sheaf F

8. The following sheaf F on $C \times C'$ will play an important role in our problem. Let x, y, K, K' be as in § 4. Then F is the subsheaf of Θ determined by the following condition; *a local section $\delta = a(\partial/\partial x) + b(\partial/\partial y)$ of Θ is a local section of F if and only if the restrictions $a_{\Pi'}, b_\Pi$ are q-th powers in the function fields of Π', Π, respectively.* In view of the equalities $K \cdot \Pi' = qK_{\Pi'}$ and $K' \cdot \Pi = qK_\Pi$, we note the following. If $\delta = a(\partial/\partial x) + b(\partial/\partial y)$ is a local section of Θ, so that a, b are local sections of $\mathcal{O}(-K), \mathcal{O}(-K')$, respectively, then $a_{\Pi'}$, b_Π are local sections of $\mathcal{O}_{\Pi'}(-qK_{\Pi'}), \mathcal{O}_\Pi(-qK_\Pi)$, respectively. Therefore, when δ belongs to a local section of F, $a_{\Pi'}$ and b_Π are q-th powers *in the ring of local sections of $\mathcal{O}_{\Pi'}(-K_{\Pi'}), \mathcal{O}_\Pi(-K_\Pi)$, respectively.* So, we may express concisely as

$$F = F_1 \oplus F_2 = \mathscr{F}_1^K \frac{\partial}{\partial x} + \mathscr{F}_2^{K'} \frac{\partial}{\partial y}, \tag{8.1}$$

where $\mathscr{F}_1^K$ (resp. $\mathscr{F}_2^{K'}$) is the inverse image of $\mathcal{O}_{\Pi'}(-K_{\Pi'})^q$ (resp. $\mathcal{O}_\Pi(-K_\Pi)^q$) in the restriction homomorphism $\mathcal{O}(-K) \to \mathcal{O}_{\Pi'}(-qK_{\Pi'})$ (resp. $\mathcal{O}(-K') \to \mathcal{O}_\Pi(-qK_\Pi)$)[1]. This definition of F is independent of the choice of x; in fact, F can also be defined as the subsheaf of Θ whose stalk at $P = (Q, Q')$ ($Q \in C$, $Q' \in C'$) is the module of all such derivations δ of $O_{C \times C', P}$ that, for any $\tilde{x} \in O_{C,Q}$ (resp. $\tilde{y} \in O_{C',Q'}$), the restriction of $\delta(p_1^* \tilde{x})$ to Π' (resp. $\delta(p_2^* \tilde{y})$ to Π) is a q-th power element of $O_{\Pi', P}$ (resp. $O_{\Pi, P}$), whenever $P \in \Pi'$ (resp. $P \in \Pi$).

It is clear that $E \subset F \subset \Theta$. Although F is not an $\mathcal{O}_{C \times C'}$-Submodule of Θ, it is a coherent $\mathcal{O}_{C \times C'}^q$-Module. Therefore, F can be *regarded* as a coherent $\mathcal{O}_{C \times C'}$-Module through the q-th power homomorphism $\mathcal{O}_{C \times C'} \to \mathcal{O}_{C \times C'}^q$. Therefore, the cohomologies of F coincides with the Čech cohomologies. We shall rely heavily on the following

Proposition 3. *The homomorphisms $H^1(F) \to H^1(\Theta)$ and $H^2(E) \to H^2(F)$ induced from the sheaf inclusions $E \subset F \subset \Theta$ are bijective.*

Proof. Let Θ_C^* denote the subsheaf of Θ_1 determined by the condition: a local section $\delta = a(\partial/\partial x)$ of Θ_1 is a local section of Θ_C^* if and only if a is a pull-back of a function on C. Then $\Theta_C^* \subset F_1 \subset \Theta_1$, as the restrictions to Π' of the pull-backs of functions on C are q-th powers. Therefore, the isomorphism $H^1(\Theta_C) \simeq H^1(\Theta_1)$ (4.3) factors through $H^1(F_1)$. Therefore, $H^1(F_1) \to H^1(\Theta_1)$ is surjective. By symmetry, $H^1(F) \to H^1(\Theta)$ is *surjective*. In particular, $\dim H^1(F) \geq 6(g-1)$.

Now look at the exact sequence $0 \to E_1 \to F_1 \to F_1/E_1 \to 0$. By the restriction to Π', we obtain $F_1/E_1 \simeq \mathcal{O}_{\Pi'}(-K_{\Pi'})^q \simeq \mathcal{O}_{\Pi'}(-K_{\Pi'})$. Therefore, $\dim H^1(F_1/E_1) = 3(g-1)$; hence $\dim H^1(F/E) = 6(g-1)$. Since F/E has one-dimensional support, we have $H^2(F/E) = 0$. Now look at the cohomology exact sequence

$$\begin{aligned} 0 = H^1(E) \longrightarrow H^1(F) \xrightarrow{\mu} H^1(F/E) \\ \longrightarrow H^2(E) \longrightarrow H^2(F) \longrightarrow H^2(F/E) = 0 . \end{aligned} \tag{8.2}$$

Since μ is injective and $\dim H^1(F) \geq 6(g-1) = \dim H^1(F/E)$, μ must be

1) The q-th power of a sheaf means the image of the q-th power endomorphism of this sheaf.

bijective and $\dim H^1(F) = 6(g-1)$. Now our conclusions follow immediately from the surjectivity of $H^1(F) \to H^1(\Theta)$ and the exact sequence (8.2). q.e.d.

Corollary 1. (i) *The sheaf exact sequence* $0 \to F \to \Theta \to \Theta/F \to 0$ *induces an exact sequence* $0 \to H^1(\Theta/F) \to H^2(F) \to H^2(\Theta) \to 0$.

(ii) $\dim H^i(F) = 0,\ 6(g-1),\ (6g+4q-4)(g-1)$ *for* $i = 0, 1, 2$;
$\dim H^i(\Theta/F) = 0,\ 4(q-1)(g-1)$ *for* $i = 0, 1$;

respectively.

With the aid of F, we can reformulate our problem of finding all $(C_n, C_n'; T_n)$ starting from a given triple $(C_{n-1}, C_{n-1}'; T_{n-1})$. For this purpose, *fix* any smooth R_n-schemes $C_n^*, C_n^{*\prime}$ that extend C_{n-1}, C_{n-1}', respectively. *A family* $\{T_n^\lambda\}_{\lambda \in \Lambda}$ *of local extensions of* T_{n-1} *on* $C_n^* \times C_n^{*\prime}$ is defined by an affine open cover $\bigcup_{\lambda \in \Lambda} U_n^\lambda$ of $C_n^* \times C_n^{*\prime}$ and, for each λ, an R_n-flat closed subscheme T_n^λ of U_n^λ that extends $T_{n-1} \cap U_{n-1}^\lambda$. Such a family $\{T_n^\lambda\}$ will be called *F-intimate* if T_n^λ and T_n^μ are *congruent* mod F for all $\lambda, \mu \in \Lambda$; i.e., $T_n^\lambda \cap U_n^{\lambda\mu}$ and $T_n^\mu \cap U_n^{\lambda\mu}$ are congruent by an infinitesimal automorphism of $U_n^{\lambda\mu}$ corresponding to a section of F on $U_0^{\lambda\mu}$. Since $E \subset F \subset \Theta$, this condition is weaker than the coincidence of T_n^λ with T_n^μ on $U_n^{\lambda\mu}$, but stronger than the coincidence of the local class of $(U_n^\lambda, T_n^\lambda)$ with that of (U_n^μ, T_n^μ) at each point of $U_0^{\lambda\mu} \cap \Pi \cap \Pi'$. Two F-intimate families $\{T_n^\lambda\}_{\lambda \in \Lambda}$ and $\{T_n^{\lambda'}\}_{\lambda' \in \Lambda'}$ are called *equivalent* if T_n^λ and $T_n^{\lambda'}$ are congruent mod F. Since $H^0(\Theta/F) = 0$, they are equivalent if and only if they are just congruent mod Θ (i.e., the local classes of $(U_n^\lambda, T_n^\lambda)$ and $(U_n^{\lambda'}, T_n^{\lambda'})$ coincide at each point of $\Pi \cap \Pi'$). (Use the affine cover $C_n^* \times C_n^{*\prime} = \bigcup_{\lambda,\lambda'} (U_n^\lambda \cap U_n^{\lambda'})$ to check this.) Therefore, non-equivalent F-intimate families determine distinct local conditions.

Corollary 2. *Let* $(C_{n-1}, C_{n-1}'; T_{n-1})$ *and* $C_n^*, C_n^{*\prime}$ *be fixed as above, and let* l *be a local condition on* $(C_{n-1}, C_{n-1}'; T_{n-1})$. *Then a solution* $(C_n, C_n'; T_n)$ *of Problem* A_n *satisfying* l *exists if and only if there exists an F-intimate family* $\{T_n^\lambda\}_{\lambda \in \Lambda}$ *of local extensions of* T_{n-1} *on* $C_n^* \times C_n^{*\prime}$ *belonging to* l. *In this manner, the solutions of Problem* A_n *are in one-to-one correspondence with the equivalence classes of F-intimate families* $\{T_n^\lambda\}_{\lambda \in \Lambda}$ *of local extensions of* T_{n-1} *on a fixed surface* $C_n^* \times C_n^{*\prime}$.

Proof. Suppose that an intimate family $\{T_n^\lambda\}$ belonging to l exists. Then, with the notation of § 6, $\theta^{\lambda\mu}$ belongs to $\Gamma(U_0^{\lambda\mu}, F)$, so that $(\beta^{\lambda\mu\nu})$ is a 2-coboundary in F. But since the canonical homomorphism $H^2(E) \to H^2(F)$ is bijective by Proposition 3, $\beta(l)$ must vanish. Conversely, if $\beta(l) = 0$ in § 6, there is some $e^{\lambda\mu} \in \Gamma(U_0^{\lambda\mu}, E)$ for each (λ, μ) such that $\theta^{\lambda\mu} - e^{\lambda\mu}$ is a 1-cocycle of Θ. But since the canonical homomorphism $H^1(F) \to H^1(\Theta)$ is bijective by Proposition 3, we have

$$\theta^{\lambda\mu} - e^{\lambda\mu} = f^{\lambda\mu} + (\theta^\lambda - \theta^\mu)$$

with $f^{\lambda\mu} \in \Gamma(U_0^{\lambda\mu}, F)$, $\theta^\lambda \in \Gamma(U_0^\lambda, \Theta)$. Therefore, replacing T_n^λ by its translation by θ^λ, we obtain an F-intimate family belonging to l. The rest of our assertion follows immediately from Theorem 1 (a). q.e.d.

Remark. When $\beta(l) = 0$, the curves C_n and C_n' in the "real solution" $(C_n, C_n'; T_n)$ have nothing to do with the auxiliary curves $C_n^*, C_n^{*\prime}$. Their difference is represented by the element of $H^1(\Theta)$ corresponding to the above 1-cocycle $\theta^{\lambda\mu} - e^{\lambda\mu}$.

Finally, call F° the sheaf on $C \times C'$ defined by just replacing "q-th power" by "p-th power" in the definition of F. For F°, Proposition 3 will be replaced by

Proposition 3°. *The canonical homomorphism* $H^1(F^\circ) \to H^1(\Theta)$ *is bijective. The canonical homomorphism* $H^2(E) \to H^2(F^\circ)$ *is surjective and its kernel is of dimension* $4(p^{f-1}-1)(g-1)$ *over* $\boldsymbol{F}_q$, *where* $q = p^f$.

This will be used only as a remark.

9. In § 9, it is assumed that $n \geq 1$. Let C_n be a smooth R_n-scheme that extends C and denote by $\mathfrak{R}_n$ the local ring at the generic point of C_n. Then, as an R_n-algebra, $\mathfrak{R}_n$ is determined uniquely by C and n. In fact, if U_0 is any affine open set of C, the smooth R_n-scheme U_n that extends U_0 is unique up to R_n-isomorphisms and $\mathfrak{R}_n$ is the inductive limit of the rings of sections of open sets of U_n. Clearly, $\mathfrak{R}_n$ is a local ring which is a flat R_n-algebra such that $\mathfrak{R}_n/\pi = \mathfrak{R}_0$ is the function field of C. The finite étale extensions of $\mathfrak{R}_n$ are in a categorical equivalence with the finite separable extensions of the residue field $\mathfrak{R}_0$ (e.g., apply [1] IV 18.3.4); let $\tilde{\mathfrak{R}}_n$ denote the union (inductive limit) of all such extensions of $\mathfrak{R}_n$. Then $\tilde{\mathfrak{R}}_0 = \tilde{\mathfrak{R}}_n/\pi$ is the separable closure of $\mathfrak{R}_0$.

The derivations of $\mathfrak{R}_n$ over R_n form a free $\mathfrak{R}_n$-module of rank one. If x_n is any element of $\mathfrak{R}_n$ such that x_0 is not a p-th power in $\mathfrak{R}_0$, a derivation D of $\mathfrak{R}_n$ over R_n is determined by $D(x_n)$ which can take any value in $\mathfrak{R}_n$. The dual $\mathfrak{R}_n$-module is the module of *differentials* (or 1-forms) of $\mathfrak{R}_n$. It is generated by dx_n for such x_n. A generator of the module of differentials will be called

a *unitary differential*. As for $\tilde{\mathfrak{K}}_n$, the situation is completely parallel, and the same kind of terminology will be used.

An R_n-endomorphism σ_n of $\mathfrak{K}_n$ (resp. $\tilde{\mathfrak{K}}_n$) into itself will be called a *Frobenius mapping* of $\mathfrak{K}_n$ (resp. $\tilde{\mathfrak{K}}_n$) if the induced endomorphism σ_0 (resp. $\tilde{\sigma}_0$) of $\mathfrak{K}_0$ (resp. $\tilde{\mathfrak{K}}_0$) is the q-th power endomorphism $x_0 \to x_0^q$. The Frobenius mappings of $\mathfrak{K}_n$ (or of $\tilde{\mathfrak{K}}_n$) are injective and *not* surjective. It is easy to see, by a standard argument, that every Frobenius mapping of $\mathfrak{K}_n$ extends *uniquely* to that of $\tilde{\mathfrak{K}}_n$. By the uniqueness, this extended Frobenius mapping commutes with each element of the Galois group of $\tilde{\mathfrak{K}}_n$ over $\mathfrak{K}_n$. If σ_n is any Frobenius mapping of $\tilde{\mathfrak{K}}_n$, then the only σ_n-invariant elements of $\tilde{\mathfrak{K}}_n$ are the elements of R_n. (In fact, if $x_n^{\sigma_n} = x_n$, then $x_0 \in \boldsymbol{F}_q$, so that $x_n = r_n + \pi y$ with $r_n \in R_n$, $y \in \tilde{\mathfrak{K}}_n$, and y is again σ_n-invariant; repeat this argument $n+1$ times.)

A numerical invariant $\nu = \nu(\sigma_n)$ is defined for each Frobenius mapping $\sigma = \sigma_n$ of $\tilde{\mathfrak{K}}_n$, as follows. Take any *unitary* differential ξ of $\tilde{\mathfrak{K}}_n$. Then $\xi^\sigma = A\xi$ with some $A \in \tilde{\mathfrak{K}}_n$. If $A = 0$, put $\nu = \infty$. If $A \neq 0$, ν is defined as the greatest exponent for which A is divisible by π^ν. Since σ maps the group of units of $\tilde{\mathfrak{K}}_n$ into itself, ν is independent of the choice of ξ. One may choose $\xi = dx_n$ $(x_0 \notin \tilde{\mathfrak{K}}_0^p)$; then $x_n^\sigma = x_n^q + \pi r$ $(r \in \tilde{\mathfrak{K}}_n)$; hence $dx_n^\sigma = (qx_n^{q-1} + \pi(dr/dx_n))dx_n$. Therefore, A is divisible by π, which implies that ν is always positive. Therefore, either $1 \leq \nu \leq n$, or $\nu = \infty$. When $R = \boldsymbol{Z}_p$, we have $dx_n^\sigma = p(x_n^{p-1} + u\cdot(dr/dx_n))dx_n$ with $u \in R_n^\times$. Since $x_0^{p-1}dx_0$ is not an exact differential of C, $x_n^{p-1} + u(dr/dx_n)$ cannot be divisible by p. Therefore, we have $\nu = 1$ in the case $R = \boldsymbol{Z}_p$. (More generally, we have $\nu \leq \mathrm{ord}_\pi q$ *if* $\mathrm{ord}_\pi q \leq n$. But this will not be used; the proof is exactly the same as that of Proposition 1 of [4].) Finally, if σ_n is a Frobenius mapping of $\mathfrak{K}_n$ and $\tilde{\sigma}_n$ is its unique extension to $\tilde{\mathfrak{K}}_n$ as a Frobenius mapping, we define $\nu(\sigma_n)$ by $\nu(\sigma_n) = \nu(\tilde{\sigma}_n)$.

Theorem 2[1]. *Let σ_n be a Frobenius mapping of $\tilde{\mathfrak{K}}_n$ with $\nu(\sigma_n) = \nu < \infty$, and choose any $c \in R_n$ with $cR_n = \pi^\nu R_n$ (as a normalizing constant). Then* (i) *there exists a unitary differential ω_n of $\tilde{\mathfrak{K}}_n$ satisfying*

$$\omega_n^{\sigma_n} = c\omega_n \ ; \tag{9.1}$$

(ii) *the differential $\omega_{n-\nu} = \omega_n \pmod{\pi^{n+1-\nu}}$ of $\tilde{\mathfrak{K}}_{n-\nu} = \tilde{\mathfrak{K}}_n/\pi^{n+1-\nu}$ is determined uniquely up to $R_{n-\nu}^\times$-multiples*; (iii) *when σ_n is the extension of a Frobenius mapping of $\mathfrak{K}_n$, $\omega_{n-\nu}$ is invariant, up to multiplications of elements of $R_{n-\nu}^\times$, by the Galois group of $\tilde{\mathfrak{K}}_{n-\nu}/\mathfrak{K}_{n-\nu}$.*

1) A parallel result for $\mathfrak{K}_\infty = \varprojlim \mathfrak{K}_n$ was given in my previous mimeographed note "Non-abelian invariant differentials (1971)".

Proof. To begin with, note that each side of (9.1) depends only on $\omega_{n-\nu}$. Take any element $x_n \in \tilde{\mathfrak{K}}_n$ such that $x_0 \notin \tilde{\mathfrak{K}}_0^p$, and put $dx_n^{\sigma_n} = c\cdot U_{n-\nu}dx_n (U_{n-\nu} \in \tilde{\mathfrak{K}}_{n-\nu}^\times)$. Put $\omega_{n-\nu} = w_{n-\nu}dx_{n-\nu}$. Then (9.1) is equivalent to the equation

$$w_{n-\nu}^{\sigma_{n-\nu}-1} = U_{n-\nu}^{-1} \ , \tag{9.2}$$

for $w_{n-\nu}$ in $\tilde{\mathfrak{K}}_{n-\nu}^\times$, where $\sigma_{n-\nu}$ is the Frobenius mapping of $\tilde{\mathfrak{K}}_{n-\nu}$ induced from σ_n. From now on, we shall omit most of the subscripts, and consider the above equation $w^{\sigma-1} = U^{-1}$ in $\tilde{\mathfrak{K}}_{n-\nu}^\times$. Since $\tilde{\mathfrak{K}}_0$ is separably closed, we can solve in $\tilde{\mathfrak{K}}_0$ the Kummer equation for the exponent $q-1$, and also the Artin-Schreier equations. First, since U_0 has a $(q-1)$-th root in $\tilde{\mathfrak{K}}_0$, we can find $u \in \tilde{\mathfrak{K}}_{n-\nu}^\times$ such that $U^{-1} \equiv u^{\sigma-1} \bmod \pi$. Put $\alpha = u^{1-\sigma}\cdot U^{-1}$ $(\equiv 1 \pmod{\pi})$, and $w' = w/u$. Then the equation is transformed to $(w')^{\sigma-1} = \alpha$. We shall construct a sequence $\{y_i\}_{i=0}^n$ in $\tilde{\mathfrak{K}}_{n-\nu}^\times$ such that $y_{i+1} \equiv y_i \pmod{\pi^{i+1}}$ and $y_i^{\sigma-1} \equiv \alpha \pmod{\pi^{i+1}}$. Then $w' = y_n$ would give a solution of the above equation. Put $y_0 = 1$, and suppose that $y_0, \cdots, y_i$ have been constructed. Put $y_i^{\sigma-1} = \alpha + \pi^{i+1}A^{(i)}$ and $y_{i+1} = y_i(1 + \pi^{i+1}B^{(i)})$. Then

$$y_{i+1}^{\sigma-1} \equiv (\alpha + \pi^{i+1}A^{(i)})(1 + \pi^{i+1}(B^{(i)q} - B^{(i)})) \qquad \bmod \pi^{i+2} \ ; \tag{9.3}$$

therefore, y_{i+1} is obtained by solving the Artin-Schreier equation

$$B^{(i)q} - B^{(i)} \equiv -A^{(i)} \qquad (\bmod \pi)$$

in $\tilde{\mathfrak{K}}_0$. This settles (i). Since we know that the only $\sigma_{n-\nu}$-invariant elements of $\tilde{\mathfrak{K}}_{n-\nu}$ are elements of $R_{n-\nu}$, (ii) is obvious. Also, (iii) follows immediately from the uniqueness of $\omega_{n-\nu}$. q.e.d.

We shall call $\omega_{n-\nu}$ *the differential associated with* σ_n (or *with* τ_n, when σ_n is the extension of a Frobenius mapping τ_n of $\mathfrak{K}_n$). It depends on the normalizing constant c, but if we change c by c', $\omega_{n-\nu}$ is simply multiplied by an element d which is a solution of the equation $d^{\sigma_{n-\nu}-1} = c'/c$ in an étale extension of $R_{n-\nu}$. To avoid unnecessary complexifications of descriptions, we make it a rule to choose $c = \pi^\nu$, when no reference is made about the normalizing constant.

The next theorem will *not* be used in this paper but it will be presented as a remark, without proof.

Theorem 3. *Let $R = \boldsymbol{Z}_p$ and σ_n be a Frobenius mapping of $\tilde{\mathfrak{K}}_n$. Then there exists an element $t_n \in \tilde{\mathfrak{K}}_n$ such that $t_0 \notin \tilde{\mathfrak{K}}_0^p$ and that*

$$t_n^{\sigma_n} = t_n^p \ . \tag{9.4}$$

Moreover, if t'_n is another element of $\tilde{\mathfrak{R}}_n$ with $t'_0 \notin \tilde{\mathfrak{R}}_0^p$, then $t'^{\sigma_n}_n = t'^p_n$ holds if and only if $t'_n = t_n^r \cdot u^{p^n}$ with some $r \in \boldsymbol{Z}$, $r \not\equiv 0 \pmod p$ and $u \in \tilde{\mathfrak{R}}_n^\times$. The differential

$$\frac{dt_n}{t_n} \pmod{p^n},$$

which is determined up to $R_{n-1}^\times$-multiples, is the differential ω_{n-1} associated with σ_n.

10. We continue the notation of § 9. The following lemma will be used later.

Lemma 2. *Let σ_n and σ'_n be two Frobenius mappings of $\tilde{\mathfrak{R}}_n$ which coincide* mod π^n. *Put $\nu = \nu(\sigma_n)$, $\nu' = \nu(\sigma'_n)$, let x_n be any element of $\tilde{\mathfrak{R}}_n$ such that $x_0 \notin \tilde{\mathfrak{R}}_0^p$, and put $x_n^{\sigma'_n} - x_n^{\sigma_n} = \pi^n z_0$ ($z_0 \in \tilde{\mathfrak{R}}_0$). Then the following conditions* (i) ~ (iii) *are equivalent*;

(i) *either $\nu = \nu' = \infty$; or $\nu = \nu' < \infty$ and σ_n, σ'_n have the same associated differentials*;

(ii) $dx_n^{\sigma'_n} = dx_n^{\sigma_n}$;

(iii) $z_0 \in \tilde{\mathfrak{R}}_0^p$.

Proof. Obviously, (ii) is equivalent with (iii). As we have seen in § 9, the differential $\omega_{n-\nu}$ associated with σ_n is determined by the three equations;

$$dx_n^{\sigma_n} = cU_{n-\nu}dx_n ,$$
$$U_{n-\nu}^{-1} = w_{n-1}^{\sigma_{n-\nu}-1} ,$$
$$\omega_{n-\nu} = w_{n-\nu}dx_{n-\nu} .$$

Since $\sigma_{n-1} = \sigma'_{n-1}$ by assumption, (i) is equivalent with (ii). q.e.d.

We shall now look at the Frobenius mappings and their differential invariants associated with our problem. Fix two smooth R_n-schemes C_n, C'_n that extend C, C', and let $\mathfrak{R}_n, \mathfrak{R}'_n$ be the local rings at the generic points of C_n, C'_n, respectively. Then since $C = C'$, their function fields $\mathfrak{R}_0 = \mathfrak{R}_n/\pi$ and $\mathfrak{R}'_0 = \mathfrak{R}'_n/\pi$ can be identified with each other. It is clear from the argument at the beginning of § 8 that there is an R_n-isomorphism $\iota_n : \mathfrak{R}_n \xrightarrow{\sim} \mathfrak{R}'_n$ inducing the identity mod π.

Suppose that $U_n \subset C_n \times C'_n$ is an open set, and $T_n(U_n)$ is an R_n-flat closed subscheme of U_n extending $T \cap U_0$. For each such *local extension* $T_n(U_n)$ of T, we can define (generally two) Frobenius mappings σ_n and σ'_n of $\mathfrak{R}_n$, where σ_n (resp. σ'_n) is defined whenever $\Pi \cap U_0 \neq \phi$ (resp. $\Pi' \cap U_0 \neq \phi$). To define them, suppose that $\Pi \cap U_0 \neq \phi$, and let $O_{T_n(U_n),\Pi}$ be the local ring of $T_n(U_n)$ at the generic point of $\Pi \cap U_0$. Then $\boldsymbol{p}_1^* : \mathfrak{R}_n \to O_{T_n(U_n),\Pi}$ is *bijective* (this follows immediately by combining the facts that $\boldsymbol{p}_1^*$ induces a bijection between their residue fields and that $\mathfrak{R}_n$ and $O_{T_n(U_n),\Pi}$ are R_n-flat local rings with the maximal ideal (π)). Therefore, $\boldsymbol{p}_1^{*-1} \circ \boldsymbol{p}_2^*$ defines a homomorphism $\sigma_n : \mathfrak{R}'_n \to \mathfrak{R}_n$. Similarly, if $\Pi' \cap U_0 \neq \phi$, $\sigma'_n : \mathfrak{R}_n \to \mathfrak{R}'_n$ is defined by using Π' instead of Π.

By means of the given identification $\iota_n : \mathfrak{R}_n \xrightarrow{\sim} \mathfrak{R}'_n$, we shall regard σ_n, σ'_n as endomorphisms of $\mathfrak{R}_n$. Then they are obviously the Frobenius mappings of $\mathfrak{R}_n$. The invariant ν associated with σ_n (resp. σ'_n) will be denoted by $\nu(T_n(U_n))$ (resp. $\nu'(T_n(U_n))$), and when it is finite, the differential associated with σ_n (resp. σ'_n) will be denoted by $\omega(T_n(U_n))$ (resp. $\omega'(T_n(U_n))$).

When we have two local extensions $T_n(U_n)$ and $T_n^*(V_n)$ of T_{n-1} and we say that *their invariants $\nu, \nu', \omega, \omega'$ are the same*, we mean that each of the four invariants *which is defined for both $T_n(U_n)$ and $T_n^*(V_n)$* has the same value for these two extensions. It is clear that $T_n(U_n)$ and its restriction to an open subset of U_n have the same invariants $\nu, \nu', \omega, \omega'$.

Remark. The nature of dependence of these four invariants of $T_n(U_n)$ on the choice of an isomorphism ι_n is not clear. But for our present purpose, it suffices to note that they depend only on $\iota_{n-1} = \iota_n \pmod{\pi^n}$. This verification is trivial; hence omitted.

Now for the connections between the associated differentials and the sheaf F° defined at the end of § 8!

Proposition 4. *Let U_n be an affine open set of $C_n \times C'_n$, and $T_n^\circ(U_n)$, $T_n(U_n)$ be two R_n-flat closed subschemes of U_n which coincide* mod π^n *and which extend $T \cap U_0$. Then the following two conditions* (i), (ii) *are equivalent*;

(i) *$T_n^\circ(U_n)$ and $T_n(U_n)$ have the same invariants $\nu, \nu', \omega, \omega'$*;

(ii) *$T_n^\circ(U_n)$ and $T_n(U_n)$ are congruent* mod F°; *i.e., they are transformed to each other by an infinitesimal automorphism of U_n corresponding to a section of F° on U_0.*

Proof. We can assume that U_n is a sufficiently small affine neighborhood of some point $P = (Q, Q') \in T$. Since $T_n^\circ(U_n)$ and $T_n(U_n)$ coincide mod π^n, we may also assume that they are defined by the local equations $f_n = 0$ and $f_n + \pi^n z_0 = 0$, respectively. Let x_P, y_P be as in § 4. Then we may assume that $f_0 = (y_P - x_P^q)(x_P - y_P^q)$. Let δ be a local section of Θ on U_0 and express it as $\delta = a(\partial/\partial x_P) + b(\partial/\partial y_P)$, by using x_P and y_P. Recall (§ 8) that δ is a section of F° if and only if $a_{\Pi'}, b_\Pi$ are p-th power elements, and that $T(U_n) = T_n^\circ(U_n)^\varepsilon$ holds if and only if $z_0 - \delta f_0 \in (f_0)$, where ε is the infinitesimal auto-

morphism of U_n corresponding to δ (§ 5). Since $\delta f_0 = (y_P - x_P^q)a + (x_P - y_P^q)b$, we obtain the following equivalence; "$T_n(U_n) \equiv T_n^\circ(U_n) \pmod{F^\circ}$ holds if and only if $(x_P - x_P^{q^2})^{-1}(z_0)_\Pi$, $(y_P - y_P^{q^2})^{-1}(z_0)_{\Pi'}$ are p-th power elements in the function fields of Π, Π', respectively (and are finite at P)." Here, the last condition of finiteness at P can be dropped, since $(x_P - x_P^{q^2})^{-1}(z_0)_\Pi$ and $(y_P - y_P^{q^2})^{-1}(z_0)_{\Pi'}$ have at most simple poles at P, so that they must be finite at P if they are p-th power elements.

On the other hand, let σ_n° (resp, σ_n) be the mappings $\mathfrak{R}_n' \to \mathfrak{R}_n$ defined by the Π-component of $T_n^\circ(U_n)$ (resp. $T_n(U_n)$), and $\sigma_n^{\circ\prime}$ (resp. σ_n') be the mappings $\mathfrak{R}_n \to \mathfrak{R}_n'$ defined by the Π'-component of $T_n^\circ(U_n)$ (resp. $T_n(U_n)$). Let x_n be any extension of x_P on C_n, and put $y_n = \iota_n(x_n)$. Then we obtain easily, by localizations $O_{T_n(U_n),P} \to O_{T_n(U_n),\Pi}, O_{T_n(U_n),\Pi'}$, the following relations

$$y_n^{\sigma_n^\circ} - y_n^{\sigma_n} = \pi^n (x_P - x_P^{q^2})^{-1}(z_0)_\Pi ,$$
$$x_n^{\sigma_n^{\circ\prime}} - x_n^{\sigma_n'} = \pi^n (y_P - y_P^{q^2})^{-1}(z_0)_{\Pi'} ,$$

where we regard $(z_0)_\Pi$ (resp. $(z_0)_{\Pi'}$) as a function on C (resp. C') *via* $\boldsymbol{p}_1 : \Pi \simeq C$ (resp. $\boldsymbol{p}_2 : \Pi' \simeq C'$). Therefore, our assertion is reduced to Lemma 2. q.e.d.

11. Now we came to a certain theoretic conclusion. Fix $(C_{n-1}, C_{n-1}'; T_{n-1})$ and also an R_{n-1}-isomorphism $\iota_{n-1} : \mathfrak{R}_{n-1} \simeq \mathfrak{R}_{n-1}'$ between the local rings at the generic points of C_{n-1}, C_{n-1}' inducing the identity mod π.

First, fix also C_n^* and $C_n^{*\prime}$ as in § 8. Let $\{T_n^\lambda\}_{\lambda \in \Lambda}$ be an F-intimate family of local extensions of T_{n-1} on $C_n^* \times C_n^{*\prime}$. Then since the members of $\{T_n^\lambda\}_{\lambda\in\Lambda}$ are mutually congruent mod F, they are *a priori* congruent mod F°. Therefore, by Proposition 4, the invariants $\nu, \nu', \omega, \omega'$ of T_n^λ are independent of λ. Here, $\nu, \nu', \omega, \omega'$ are those defined with respect to ι_{n-1} (see Remark, § 10). Thus, to each equivalence class of F-intimate family $\{T_n^\lambda\}_{\lambda\in\Lambda}$, we can associate a quadruple $(\nu, \nu'; \omega, \omega')$ of its invariants. When $q = p$, so that $F = F^\circ$, Proposition 4 tells us that this association is one-to-one. We also observe that the condition for a quadruple $(\nu, \nu'; \omega, \omega')$ to correspond with some $\{T_n^\lambda\}_{\lambda\in\Lambda}$, is completely of a *local* nature; i.e., it is (necessary and) sufficient that each point $P \in C_n^* \times C_n^{*\prime}$ has an affine neighborhood U_n^P (on $C_n^* \times C_n^{*\prime}$) and an R_n-flat closed subscheme T_n^P on U_n^P that extends $T_{n-1} \cap U_{n-1}^P$ and having $\nu, \nu', \omega, \omega'$ as its invariants. Indeed, then, $\{T_n^P\}$ is an F-intimate family (by $q = p$ and by Proposition 4). Therefore, combining with Corollary 2 of Proposition 3 (§ 9), we obtain a one-to-one correspondence

$$(C_n, C_n'; T_n) \longrightarrow (\nu, \nu'; \omega, \omega') \tag{11.1}$$

between the set of all solutions $(C_n, C_n'; T_n)$ of Problem A_n and that of all quadruples $(\nu, \nu'; \omega, \omega')$ satisfying the above local conditions. Here, $(C_n, C_n'; T_n)$ are counted up to equivalence, and the differentials ω, ω' are counted up to multiplications of elements of $R_{n-\nu}^\times, R_{n-\nu'}^\times$, respectively. We observe easily that this correspondence (11.1) is independent of the choice of C_n^* or $C_n^{*\prime}$. In particular, we observe that the map (11.1) associates to each $(C_n, C_n'; T_n)$ the invariant $(\nu, \nu'; \omega, \omega')$ of T_n on $C_n \times C_n'$. So we arrive at the following definition and theorem.

Definition. Let $(\nu, \nu'; \omega, \omega')$ be a quadruple, where each of ν, ν' is either a positive integer $\leq n$ or ∞, and ω (resp. ω') is a unitary differential of $\tilde{\mathfrak{R}}_{n-\nu}$ (resp. $\tilde{\mathfrak{R}}_{n-\nu'}$) which appears in the quadruple only when ν (resp. ν') is finite. Let P be any point of T. Then $(\nu, \nu'; \omega, \omega')$ is called *of type* T_n^P, if the following condition is satisfied;

($\boldsymbol{B}_n$) P has an affine open neighborhood U_n^P on $C_n^* \times C_n^{*\prime}$, on which we can find an R_n-flat closed subscheme T_n^P that extends $T_{n-1} \cap U_{n-1}^P$ and that has the given invariants ν (when $P \in \Pi$), ν' (when $P \in \Pi'$), ω (when $P \in \Pi$ and $\nu < \infty$), and ω' (when $P \in \Pi'$ and $\nu' < \infty$).

Since this condition $\boldsymbol{B}_n$ is local, it does not depend on the choice of C_n^* or $C_n^{*\prime}$.

Theorem 4. *Let $q = p$. Fix $(C_{n-1}, C_{n-1}'; T_{n-1})$ and ι_{n-1}, as at the beginning of* § 11. *Then there is a canonical bijection between the set of all solutions $(C_n, C_n'; T_n)$ of Problem A_n and that of all quadruples $(\nu, \nu'; \omega, \omega')$ which are of type T_n^P at every $P \in T$. Here, $(C_n, C_n'; T_n)$ are counted up to equivalence and ω, ω' are up to multiplications of elements of $R_{n-\nu}^\times, R_{n-\nu'}^\times$, respectively.*

Remark. When $R = \boldsymbol{Z}_p$, condition $\boldsymbol{B}_n$ implies $\nu = \nu' = 1$, as we have shown in § 9. So, in this case, the quadruples $(\nu, \nu'; \omega, \omega')$ can be replaced by the pairs (ω, ω'). When $q \neq p$, our argument fails, in view of Proposition 3° (§ 8).

Extensions of $\Pi + \Pi'$ on R/π^2 .

12. Now let $q = p$. We shall consider Problem A_1 which is to find all triples $(C_1, C_1'; T_1)$ of proper smooth R_1-schemes C_1, C_1' extending C and an R_1-flat closed subscheme T_1 of $C_1 \times C_1'$ extending T. Since $R_0 = \boldsymbol{F}_p$, there are two cases for R_1; (Case 1) $R_1 = \boldsymbol{Z}/p^2$, which is the case where $R = \boldsymbol{Z}_p$; (Case 2) $R_1 = \boldsymbol{F}_p[\varepsilon]$ with $\varepsilon^2 = 0$, which is the case where R is either a fully ramified extension of $\boldsymbol{Z}_p$ or the ring of formal power series over $\boldsymbol{F}_p$. In Case

2, there is one *trivial solution* of Problem A_1, which is the solution obtained by the trivial base-change $\otimes_{F_p} F_p[\varepsilon]$ of $(C, C'; T)$.

To state our result, let Ω_1 (resp. Ω_2) be the set of all rational differentials $\omega^{\cdot}$ of degree $p-1$ on C satisfying the following two conditions (a) and (b), where Φ is the divisor of C defined by the formal sum of all closed points Q of C with $\deg Q \leq 2$;

(a) $\omega^{\cdot} \prec 2\Phi$;

(b) $\gamma(\omega) = \omega$ (resp. $\gamma(\omega) = 0$) ,

where ω is a differential of degree 1 on a cyclic covering of C such that $\omega^{\cdot} = \omega^{\otimes(p-1)}$, and γ is the Cartier operator.

In other words, fix any rational function x on C which is not a p-th power in the function field of C, and write

$$\omega^{\cdot} = (dx)^{\otimes p}/\zeta ,$$

where ζ is a differential of degree 1 on C. Then, in terms of ζ, the above two conditions (a), (b) are interpreted as

(a)′ $\zeta \succ p\cdot(dx) - 2\Phi$,

(b)′ $\gamma(\zeta) = dx$ (resp. $\gamma(\zeta) = 0$) .

By (b)′, ζ is of the form $\zeta = x^{p-1}dx + dr$ (resp. $\zeta = dr$), where r is a rational function on C. *The zeros of $\omega^{\cdot}$ must be of order* 2. In fact, in considering the order of $\omega^{\cdot}$ at $Q \in C$, we may choose x as a local uniformization at Q; then $\omega^{\cdot}$ has a zero at Q if and only if dr has a pole at Q, and in this case $\mathrm{ord}_Q\, \omega^{\cdot} = -\mathrm{ord}_Q\,(dr)$; therefore, the order of zeros of $\omega^{\cdot}$ cannot be 1; hence it must be 2 by (a). A similar argument shows that, for the elements $\omega^{\cdot} \in \Omega_1$ the poles of $\omega^{\cdot}$ must be of order $\geq -(p-1)$.

Let $i = 1$ or 2, and $\omega^{\cdot}, \omega^{\cdot\prime} \in \Omega_i$. We say that $\omega^{\cdot}$ and $\omega^{\cdot\prime}$ are the *F_p-conjugates* of each other, if the following conditions (c), (d) are satisfied;

(c) the zeros of $\omega^{\cdot}$ coincide with the zeros of $\omega^{\cdot\prime}$;

(d) at each zero Q, let x_Q be a local uniformization and expand $\omega^{\cdot}, \omega^{\cdot\prime}$ as

$$\begin{aligned} \omega^{\cdot} &= cx_Q^2(1 + a_1x_Q + \cdots)(dx_Q)^{\otimes(p-1)} , \\ \omega^{\cdot\prime} &= c'x_Q^2(1 + a_1'x_Q + \cdots)(dx_Q)^{\otimes(p-1)} ; \end{aligned} \tag{12.1}$$

then c and c' are conjugate over F_p. (As $\deg Q \leq 2$ by (a), the coefficients in (12.1) belong to F_{p^2}.)

For each $\omega^{\cdot} \in \Omega_i$, there is at most one $\omega^{\cdot\prime} \in \Omega_i$ which is the F_p-conjugate of $\omega^{\cdot}$. In fact, if $\omega^{\cdot\prime} = (dx)^{\otimes p}/\zeta'$ and $\omega^{\cdot\prime\prime} = (dx)^{\otimes p}/\zeta''$ are both the F_p-conjugates of $\omega^{\cdot}$, then $\zeta' - \zeta'' \succ p(dx) - \Phi$ by (a)′ and (d), but since $\gamma(\zeta' - \zeta'') = 0$, this implies that $\zeta' - \zeta'' \succ p(dx)$; hence $\zeta' = \zeta''$. By definition, the mutually F_p-conjugate differentials $\omega^{\cdot}, \omega^{\cdot\prime}$ have the same numerators in their divisors, but their denominators are generally different (see Example 1 § 15). Also, there are some examples of a differential of Ω_i which is *not* the F_p-conjugate of any differential of Ω_i (see Examples 2, 3, 4; § 15).

Theorem 5. (i) *The set of all solutions $(C_1, C_1'; T_1)$ of Problem A_1 in Case* 1 (resp. *the set of all non-trivial solutions $(C_1, C_1'; T_1)$ of Problem A_1 in Case* 2) *is in a canonical one-to-one correspondence with the set of all ordered pairs $(\omega^{\cdot}, \omega^{\cdot\prime})$ of mutually F_p-conjugate elements of Ω_1* (resp. Ω_2).

(ii) *This one-to-one correspondence is determined by the following description of the local class of $(C_1 \times C_1'; T_1)$ at each $P = (Q, Q') \in \Pi \cap \Pi'$ in terms of $(\omega^{\cdot}, \omega^{\cdot\prime})$. Let x_Q be a local uniformization at Q on C, $y_{Q'}$ be the corresponding function on C', x_1, y_1 be any extensions of $x_Q, y_{Q'}$ on C_1, C_1', and let*

$$(y_1 - x_1^p)(x_1 - y_1^p) + \pi z_0 = 0 \tag{12.2}$$

be the local equation for T_1 at P, where $\pi = p$ (resp. $\pi = \varepsilon$) in Case 1 (resp. *Case* 2). *Then*

$$\begin{cases} z_0(P) = 0 & \text{if } \mathrm{ord}_Q\, \omega^{\cdot} \leq 0 , \\ z_0(P) = c^{-1} & \text{if } \mathrm{ord}_Q\, \omega^{\cdot} = 2 , \end{cases} \tag{12.3}$$

where c is the constant defined in (12.1).

(iii) *When $(C_1, C_1'; T_1)$ corresponds with $(\omega^{\cdot}, \omega^{\cdot\prime})$, its transpose $(C_1', C_1, {}^tT_1)$ corresponds with $(\omega^{\cdot\prime}, \omega^{\cdot})$.*

13. Now we shall prove Theorem 5 by using Theorem 4. We first restrict ourselves to Case 1. Then, with the notation of Theorem 4, we always have $\nu = \nu' = 1$ (see § 9); therefore, $(C_1, C_1'; T_1)$ are in a canonical one-to-one correspondence with the pairs (ω, ω') of unitary differentials of $\tilde{\mathfrak{R}}_0$ (the separable closure of the function field $\mathfrak{R}_0$ of C) satisfying Condition B_1 of § 11 for all $P \in T$. Since ω, ω' are differentials associated with some Frobenius mappings of $\mathfrak{R}_1$, they are invariant up to $F_p^{\times}$-multiples by the Galois automorphisms of $\tilde{\mathfrak{R}}_0/\mathfrak{R}_0$ (Theorem 2, § 9). Therefore, if we take $\omega^{\cdot} = \omega^{\otimes(p-1)}$ and $\omega^{\cdot\prime} = \omega'^{\otimes(p-1)}$, then they are *rational* differentials of degree $p-1$ on C. (At the same time, the indeterminacy of ω, ω' by a scalar factor of $F_p^{\times}$ disappears for $\omega^{\cdot}, \omega^{\cdot\prime}$.)

Our task is to interpret the local Condition B_1 in terms of $\omega^{\cdot}, \omega^{\cdot\prime}$ in a *simpler* way.

For this purpose, let, $C_1^*, C_1^{*\prime}$ be as in § 11 and let $\mathfrak{R}_1, \mathfrak{R}_1'$ be the local rings at their generic points respectively. Choose an R_1-isomorphism $\iota_1 : \mathfrak{R}_1 \simeq \mathfrak{R}_1'$ inducing the identity mod p. Let P be a closed point of $T = \Pi + \Pi'$ with the projections Q, Q' on C, C', respectively. Let x_0 be a local uniformization on C at Q, and y_0 be the corresponding local uniformization on C' at Q'. Let x_1 (resp. y_1) be any extensions of x_0 (resp. y_0) on C_1^* (resp. $C_1^{*\prime}$) such that $\iota_1(x_1) = y_1$.

In general, let σ_1 be any Frobenius mapping of $\mathfrak{R}_1$ and put $x_1^{\sigma_1} = x_1^p + pr_0$ ($r_0 \in \mathfrak{R}_0$). Let $\omega(\sigma_1)$ be the differential associated with σ_1 (with normalizing constant p), and put $\omega(\sigma_1) = w_0 dx_0$ with $w_0 \in \bar{\mathfrak{R}}_0$. Then w_0 is determined by the equation

$$w_0^{p-1} = U_0^{-1}, \qquad \text{with } dx_1^{\sigma_1} = pU_0 dx_1 \quad \text{(see § 9)}.$$

Since $U_0 = x_0^{p-1} + dr_0/dx_0$, we obtain $w_0^{p-1} = (x_0^{p-1} + dr_0/dx_0)^{-1}$; hence

$$\omega(\sigma_1)^{\otimes(p-1)} = \left(x_0^{p-1} + \frac{dr_0}{dx_0}\right)^{-1} (dx_0)^{\otimes(p-1)}. \tag{13.1}$$

The Condition B_1 at $P \in \Pi$, $P \notin \Pi'$. An extension of Π on $C_1^* \times C_1^{*\prime}$ near P is defined by a local equation

$$y_1 = x_1^p + pz_0,$$

with some function z_0 on $C \times C'$ which is regular at P. The corresponding Frobenius mapping of $\mathfrak{R}_1$ is given by $x_1^{\sigma_1} = x_1^p + pr_0$ with $r_0 = (z_0)_\Pi$, the restriction of z_0 on Π considered as a function on C via $\boldsymbol{p}_1 : \Pi \simeq C$. Since any function r_0 on C regular at Q can be expressed as $(z_0)_\Pi$ with some z_0, the Condition B_1 for $\omega^\cdot$ at P is that

(i_P) $\omega^\cdot$ is of the form $(x_0^{p-1} + dr_0/dx_0)^{-1}(dx_0)^{\otimes(p-1)}$

and

(ii_P) r_0 can be *chosen* to be regular at Q.

But since $\gamma(x_0^{p-1}dx_0) = dx_0$, ($i_P$) is equivalent with the condition (b)′ (§ 12) (for $x = x_0$) and hence also with (b). This being assumed, (ii_P) is just equivalent with $\mathrm{ord}_Q \omega^\cdot \leq 0$. Therefore, the Condition B_1 at $P \in \Pi$, $P \notin \Pi'$ consists of

Condition (b) (§ 12) and $\mathrm{ord}_Q \omega^\cdot \leq 0$.

The Condition B_1 at $P \in \Pi'$, $P \notin \Pi$. This consists of

Condition (b) (§ 12) and $\mathrm{ord}_Q \omega^{\cdot\prime} \leq 0$.

The Condition B_1 at $P \in \Pi \cap \Pi'$. An extension of $\Pi + \Pi'$ on $C_1^* \times C_1^{*\prime}$ near P is defined by an equation

$$(y_1 - x_1^p)(x_1 - y_1^p) + pz_0 = 0$$

with some function z_0 on $C \times C'$ which is regular at P. The two corresponding Frobenius mappings defined from the Π-component and the Π'-component are given respectively by

$$x_1^{\sigma_1} = x_1^p + pr_0, \qquad \text{with } r_0 = (x_0^{p^2} - x_0)^{-1}(z_0)_\Pi,$$

and

$$x_1^{\sigma_1'} = x_1^p + pr_0', \qquad \text{with } r_0' = (x_0^{p^2} - x_0)^{-1}({}^t z_0)_\Pi,$$

where ${}^t z_0$ is the transpose of z_0, and $(z_0)_\Pi$, $({}^t z_0)_\Pi$ are considered as functions on C via $\boldsymbol{p}_1 : \Pi \simeq C$. Therefore, the Condition B_1 at P is equivalent with the existence of z_0, regular at P, such that

$$\omega^\cdot = \left(x_0^{p-1} + \frac{dr_0}{dx_0}\right)^{-1}(dx_0)^{\otimes(p-1)}, \qquad r_0 = (x_0^{p^2} - x_0)^{-1}(z_0)_\Pi,$$

and

$$\omega^{\cdot\prime} = \left(x_0^{p-1} + \frac{dr_0'}{dx_0}\right)^{-1}(dx_0)^{\otimes(p-1)}, \qquad r_0' = (x_0^{p^2} - x_0)^{-1}({}^t z_0)_\Pi.$$

There are two cases here. The existence of z_0 with $z_0(P) = 0$ is equivalent with

Condition (b) for $\omega^\cdot$, $\omega^{\cdot\prime}$; and $\mathrm{ord}_Q \omega^\cdot \leq 0$, $\mathrm{ord}_Q \omega^{\cdot\prime} \leq 0$.

While the existence of z_0 with $z_0(P) \neq 0$ is equivalent with

Condition (b) for $\omega^\cdot$, $\omega^{\cdot\prime}$; $\mathrm{ord}_Q \omega^\cdot = \mathrm{ord}_Q \omega^{\cdot\prime} = 2$; and $c' = c^p$;

where $\omega^\cdot = cx_0^2(1 + \cdots)(dx_0)^{\otimes(p-1)}$ and $\omega^{\cdot\prime} = c'x_0^2(1 + \cdots)(dx_0)^{\otimes(p-1)}$ at Q. Note also that $z_0(P) = c^{-1}$ in this case. As we have seen in § 12, (b) implies that $\omega^\cdot$ cannot have simple zeros. Therefore, we conclude that Condition B_1 is equivalent with "(a) and (b) for $\omega^\cdot$, $\omega^{\cdot\prime}$, and (c) and (d) for $(\omega^\cdot, \omega^{\cdot\prime})$". This settles the proof of (i), and also (ii), for Case 1.

Now consider Case 2, where $R_1 = \boldsymbol{F}_p[\varepsilon]$. Look at the local equation (12.2) for T_1 at $P \in \Pi \cap \Pi'$. The local class at P is determined by $z_0(P)$. By Theorem 1, $(C_1, C_1'; T_1)$ must be the *trivial solution* if $z_0(P) = 0$ for all $P \in \Pi \cap \Pi'$. Therefore, $z_0(P) \neq 0$ for at least one $P \in \Pi \cap \Pi'$ for a non-trivial solution. We shall show that *if* $(C_1, C_1'; T_1)$ *is a non-trivial solution, then* $\nu = \nu' = 1$. Let σ_1 (resp. σ_1') be the Frobenius mappings defined by the Π-component (resp. Π'-

component) of T_1. Then $x_1'^1 = x_1^p + \pi r_0$ (resp. $x_1'^i = x_1^p + \pi r_0'$) with

$$r_0 = (x_0^{p^2} - x_0)^{-1}(z_0)_{\Pi}\ , \qquad r_0' = (x_0^{p^2} - x_0)^{-1}({}^t z_0)_{\Pi}\ .$$

Take P where $z_0(P) \neq 0$. Then r_0, r_0' have poles of order -1 at Q. In particular, r_0, r_0' are *not* p-th powers in the function field of C. Therefore, $\nu = \nu' = 1$. The rest is exactly the same, except that one has to replace $x_0^{p-1} + dr_0/dx_0$ by dr_0/dx_0 in the formula for the associated differentials. (Indeed, this time, $dx_1'^1/dx_1 = px_0^{p-1} + \pi(dr_0/dx_0) = \pi(dr_0/dx_0)$.)

Finally, (iii) follows immediately from (ii), because,by Theorem 1, $(C_1, C_1'; T_1)$ is uniquely determined by the local classes at $P \in \Pi \cap \Pi'$.

This completes the proof of Theorem 5.

14. Here, we shall give some scattered remarks.

Put $N_2 = \deg \Phi$, the number of $\boldsymbol{F}_{p^2}$-rational points of C. Then the condition (a) (§ 12) tells us that Ω_1, Ω_2 are empty unless

$$N_2 \geq (p-1)(g-1)\ . \tag{14.1}$$

So, (14.1) is a necessary condition for the existence of solutions (Case 1) (resp. non-trivial solutions (Case 2)) of Problem A_1.

Let V be, as in § 7, the kernel of $\beta_0 : H^0(N_T/N_T^0) \to \boldsymbol{Obs}$. Recall Corollary 1 of Proposition 2 (§ 7). In Case 1, the set of all solutions of Problem A_1 is either empty or forms a principal homogeneous space of V, and in Case 2 the set of all solutions can be identified with V if we take the trivial solution as the origin. (In particular, the number of solutions for $R_1 = \boldsymbol{Z}/p^2$ is equal to that for $R_1 = \boldsymbol{F}_p[\varepsilon]$ as long as the former is non-zero). The scalar multiplication of $a \in \boldsymbol{F}_p^{\times}$ in the space of solutions in Case 2 corresponds to $(\omega', \omega'') \to (a^{-1}\omega', a^{-1}\omega'')$ and also to the automorphism of $\boldsymbol{F}_p[\varepsilon]$ induced by $\varepsilon \to a\varepsilon$.

Finally, one word about the connection between Corollary 1 of Proposition 2 (§ 7) and Theorem 5. The set of all local conditions l satisfying $\beta(l) = 0$ can be calculated by means of Theorem 5 (ii) using the differentials on C, and on the other hand it forms a single V-orbit (unless empty). In re-verifying this connection *directly* (i.e., without passing through the extensions $(C_1, C_1'; T_1)$), one meets the following equality which is a simple example of the Serre duality (for $\mathcal{O}_C^p$-Modules on C);

$$\begin{aligned} &N_2 - 2(p-1)(g-1) \\ &\quad = \dim W_{ex}(2\Phi - pK_C) - \dim W_{ex}(pK_C - \Phi)\ . \end{aligned} \tag{14.2}$$

Here, $W_{ex}(D)$ (for a divisor D on C) will denote the $\boldsymbol{F}_p$-module of all *exact* differentials ξ satisfying $\xi \succ -D$. This formula can also be used for evaluating the dimension of V. For example, if $N_2 > 2(p+1)(g-1)$, then $\dim W_{ex}(pK_C - \Phi) = \dim W(pK_C - \Phi) = 0$. Therefore, the space of ζ satisfying (a)′ and (b)′ (for Ω_2) has dimension $N_2 - 2(p-1)(g-1)$. Therefore, $\dim V \leq N_2 - 2(p-1)(g-1)$. On the other hand, since V is the kernel of $H^0(N_T/N_T^0) \to \boldsymbol{Obs}$, $\dim V \geq N_2 - 4(p-1)(g-1)$. Therefore,

$$N_2 - 4(p-1)(g-1) \leq \dim V \leq N_2 - 2(p-1)(g-1) \tag{14.3}$$

holds when $N_2 > 2(p+1)(g-1)$.

15. *Example 1.* Let C be defined by the equation

$$y^2 + x^3 y = x$$

over $\boldsymbol{F}_2$. Then $g = 2$, $N_2 = 5$. This is a hyperelliptic curve whose ramification in the double covering $C \to \boldsymbol{P}^1$ defined by $(x, y) \to x$ is concentrated to a wild ramification at $x = 0$. The points of degree 1 are P_1, Q_1, R_1 defined by $(x, y) = (\infty, 0)$, (∞, ∞), $(0, 0)$, respectively, and the point of degree 2 is S_2 defined by $x = 1$. The space of differentials $\zeta \succ p(dx) - 2\Phi = 10R_1 - 6P_1 - 6Q_1 - 2S_2$ is spanned by $(x+1)^{-2}x^i dx$ $(2 \leq i \leq 6)$ and $(x+1)^{-2}x^j y dx$ $(2 \leq j \leq 3)$. The kernel of γ in this space is spanned by $(x+1)^{-2}x^i dx$ $(i = 2, 4, 6)$. Since γ maps $x^3(1+y)(1+x)^{-2}dx$ to dx, we obtain

$$\Omega_1 = \left\{ \frac{(x+1)^2 dx}{x^3(1+y) + ax^2 + bx^4 + cx^6}\ ;\ a, b, c \in \boldsymbol{F}_2 \right\}\ ,$$

$$\Omega_2 = \left\{ \frac{(x+1)^2 dx}{ax^2 + bx^4 + cx^6}\ ;\ a, b, c \in \boldsymbol{F}_2,\ (a, b, c) \neq (0, 0, 0) \right\}\ .$$

Name each $\omega' \in \Omega_1$ as $\omega' = \omega'(a, b, c)$. Then $\omega'(a, b, c)$ is $\boldsymbol{F}_2$-conjugate with $\omega'(a, b+1, c)$, and the numerators of their divisors for $(a, c) = (0, 0)$, $(1, 0), (0, 1), (1, 1)$ are given respectively by $2(Q_1 + S_2)$, $2(Q_1 + R_1 + S_2)$, $2(P_1 + S_2)$, $2(P_1 + R_1 + S_2)$, respectively. For example,

$$(\omega(0, 0, 0)) = 2(Q_1 + S_2) - (P_1 + D_3)\ ,$$

and

$$(\omega(0, 1, 0)) = 2(Q_1 + S_2) - D_4\ ;$$

where D_3 is the point of degree 3 defined by $y = 1$, and D_4 is the point of degree 4 defined by $x^5 = 1$, $x \neq 1$, $y = x + 1$. These differentials are mutually $\boldsymbol{F}_2$-conjugate, as the values of $\omega(0, 0, 0)/(x+1)^2 dx$ and $\omega(0, 1, 0)/(x+1)^2 dx$ at each geometric point in S_2 are conjugate over $\boldsymbol{F}_2$.

Accordingly, there are eight triples $(C_1, C_1'; T_1)$ over $\boldsymbol{Z}/4$, of which none

is symmetric. As for Ω_2, we see that each $\omega^{\cdot} \in \Omega_2$ is F_2-conjugate with itself. (For example, $(a, b, c) = (1, 1, 0)$ gives $\omega^{\cdot} = x^{-2}dx$ whose divisor is $2R_1$.) Accordingly, there are (one trivial and) seven non-trivial triples $(C_1, C_1'; T_1)$ over $\boldsymbol{F}_2[\varepsilon]$, all of which are symmetric.

Example 2. Let C be the non-singular quartic

$$y^4 + (x^3 + x^2 + 1)y + (x^4 + x + 1) = 0$$

over $\boldsymbol{F}_2$. Then $g = 3$ and $N_2 = 2$. In fact, there is one point P_2 of degree 2 defined by $(x, y) = (\rho, \rho^2)$ with $\rho^2 + \rho + 1 = 0$, and this is the unique point with degree ≤ 2. Therefore, $\Phi = P_2$. Since $(p - 1)(g - 1) = N_2$ in this case, the condition $\omega^{\cdot} \prec 2\Phi$ implies $(\omega^{\cdot}) = 2\Phi = 2P_2$. Therefore,

$$\omega^{\cdot} = \frac{y + x + 1}{x^3 + x^2 + 1}dx \ .$$

Since $\gamma(\omega^{\cdot}) = 0$, Ω_1 is empty and $\Omega_2 = (\omega^{\cdot})$. Accordingly, there is no triples $(C_1, C_1'; T_1)$ over $\boldsymbol{Z}/4$. The remaining question is whether $\omega^{\cdot} \in \Omega_2$ is the $\boldsymbol{F}_2$-conjugate of itself, or equivalently, whether the value of $\omega^{\cdot}/t^2dt$ at P_2 belongs to the prime field $\boldsymbol{F}_2$, where t is a local uniformization at P_2. Take $t = x^2 + x + 1$, and put $z = y + x + 1$. Then $z^4 + (x^3 + x^2 + 1)z = t^2$. Therefore, the value of $\omega^{\cdot}/t^2dt = t^{-2}(x^3 + x^2 + 1)^{-1}z$ at $(x, y) = (\rho, \rho^2)$ is equal to ρ^2. Therefore, $\Omega^{\cdot}$ does not yield a pair $(\omega^{\cdot}, \omega^{\cdot\prime})$. Therefore, there are also no non-trivial triples $(C_1, C_1'; T_1)$ over $\boldsymbol{F}_2[\varepsilon]$.

Another similar example is:

Example 3. Let C be the non-singular quartic

$$y^4 + (x + 1)y^3 + xy^2 + (x + 1)^3y + x^2 = 0$$

over $\boldsymbol{F}_2$. Then $N_2 = 4$, and the points of degree ≤ 2 are P_1, Q_1, R_2, defined by $(x, y) = (1, 0), (0, 0), (1, \rho)$ with $\rho^2 + \rho + 1 = 0$, respectively. We obtain

$$\Omega_1 = \left\{ \frac{ydx}{(x + 1)(x + y + 1)^2}, \frac{ydx}{(x + y + 1)^3} \right\} ,$$

$$\Omega_2 = \left\{ \frac{dx}{(x + y + 1)^2} \right\} .$$

In the course of finding the mutually $\boldsymbol{F}_2$-conjugate pairs, only the self-conjugate differential

$$\omega^{\cdot} = \frac{ydx}{(x + 1)(x + y + 1)^2}$$

in Ω_1 remains. (Its divisor is $2(P_1 + Q_1)$.) Therefore, there is exactly one triple $(C_1, C_1'; T_1)$ over $\boldsymbol{Z}/4$ (which naturally is symmetric), and no non-trivial ones over $\boldsymbol{F}_2[\varepsilon]$.

Example 4. Let C be defined by

$$y^5 = x^3 - x + 1$$

over $\boldsymbol{F}_3$. Then $g = 4$ and $N_2 = 10$. Although $N_2 > (p - 1)(g - 1) = 6$, there are no solutions of Problem A_1 except the trivial one in Case 2. In fact, Ω_1 is empty; while as for Ω_2, it consists of two differentials

$$\pm y^{-1}(y^3 + y^2 + 1)^2(dy)^{\otimes 2} ,$$

but it yields *no* pairs $(\omega^{\cdot}, \omega^{\cdot\prime})$.

Example 5. Let C be defined by

$$y^2 = 1 + x^6$$

over $\boldsymbol{F}_5$. Then $g = 2$ and $N_2 = 46$. In this case, $N_2 - (p - 1)(g - 1)$ is so big that the calculations are too tedious to be carried through. But by the formula (14.3), we obtain an evaluation of $d = \dim V$, as

$$30 \leq d \leq 38 \ .$$

On the other hand, put

$$\omega^{\cdot} = \frac{2x^2(dx)^{\otimes 4}}{y^4} \ .$$

Then $\omega^{\cdot}$ satisfies (a), (b) for Ω_1, and $\omega^{\cdot}$ is the $\boldsymbol{F}_5$-conjugate of itself. Therefore, there is at least one symmetric solution $(C_1, C_1'; T_1)$ over $\boldsymbol{Z}/25$ corresponding to $(\omega^{\cdot}, \omega^{\cdot})$. Therefore, there are 5^d solutions over $\boldsymbol{Z}/25$ and also the same number of solutions (including the trivial one) over $\boldsymbol{F}_5[\varepsilon]$. The above particular solution comes from a Shimura-Morita's congruence relation for a quaternionic modular group (cf. our previous work [5] for details). So, we know "from the other side" that it can be further extended to a solution $(\mathscr{C}, \mathscr{C}'; \mathscr{T})$ of Problem A for $R = \boldsymbol{Z}_5$.

16. *Remark.* We have assumed throughout the paper that C is geometrically irreducible. We can replace this by a weaker assumption of irreducibility over $\boldsymbol{F}_q$, with only minor modifications. In fact, the only necessary changes arise from the fact that, if $\boldsymbol{F}_{q^m}$ is the field of constant functions on C, $C \times_{\boldsymbol{F}_q} C$ decomposes into m connected components (corresponding to the decomposition

of $F_{q^m} \otimes_{F_q} F_{q^m}$). If $m > 2$, then Π and Π' lie on the different components; so the only important case besides the case of $m = 1$ is that of $m = 2$. In this case, replace $C \times_{F_q} C$ by *the component containing Π and Π'*, consider the cohomology groups on *this* component, and consider their dimensions *over* F_{q^2} (instead of over F_q). Then, the dimension formulae for these groups do not change if we take g to be the genus of C over F_{q^2}. All other results of this paper remain valid under this generalization without modifications.

References

[1] Grothendieck, A., Eléments de géométrie algébrique I–IV, Publ. IHES. Le Bois-Marie, 1960–'67.
[2] Grothendieck, A., Revêtements étales et groupe fondamental (SGA 1), Lecture Notes in Math. **224**, Springer, Berlin, 1971.
[3] Horikawa, E., On deformations of holomorphic maps, I, J. Math. Soc. Japan **25** (1973), 372–396, II, J. Math. Soc. Japan **26** (1974), 647–667, III, Math. Ann. **222** (1976), 275–282.
[4] Ihara, Y., On the differentials associated to congruence relations and the Schwarzian equations defining uniformizations, J. Fac. Sci. Univ. Tokyo IA, **21** (1974), 309–332.
[5] Ihara, Y., Some fundamental groups in the arithmetic of algebraic curves over finite fields, Proc. Nat. Acad. Sci. USA **72** (1975), 3281–3284.
[6] Serre, J-P., Géométrie algébrique, Proc. Intern. Congress Math., 1962, 190–196 Inst. Mittag-Leffler, Djursholm, 1963.
[7] Shimura, G., On the zeta functions of the algebraic curves uniformized by certain automorphic functions, J. Math. Soc. Japan **13** (1961), 275-331.
[8] Shimura, G., On canonical models of arithmetic quotients of bounded symmetric domains, I, Ann. Math. **91** (1970), 144–222.

Department of Mathematics
Faculty of Science
University of Tokyo
Hongo, Tokyo 113
Japan

ALGEBRAIC NUMBER THEORY, Papers contributed for the International Symposium, Kyoto 1976: S. Iyanaga (Ed.): Japan Society for the Promotion of Science, Tokyo, 1977

Some Remarks on Hecke Characters

KENKICHI IWASAWA

In the present paper, we shall make some simple remarks on Hecke characters of type (A_0) for a special type of finite algebraic number fields. For imaginary abelian extensions over the rational field, examples of such characters are provided by Jacobi sums and these will also be discussed briefly.[1)]

§ 1. Let j denote the automorphism of the complex field C mapping each α in C to its complex-conjugate $\bar{\alpha}$. An algebraic number field k, i.e., an algebraic extension of the rational field Q contained in C, will be called a j-field if k is invariant under j and $\sigma j = j\sigma$ for every isomorphism σ of k into C. One sees immediately that k is a j-field if and only if k is either a totally real field or a totally imaginary quadratic extension of a totally real subfield.

In the following, we shall consider Hecke characters of type (A_0) for a field k which is an imaginary j-field and is also a finite Galois extension over Q. Let $G = \mathrm{Gal}(k/Q)$. The restriction of j on k, which will simply be denoted again by j, is an element of order 2 in the center of G. Let I denote the idele group of k. Then $I = I_0 \times I_\infty$ where I_0 and I_∞ are the finite part and the infinite part of I respectively. The multiplicative group $k^\times$ of the field k is naturally imbedded in I as a discrete subgroup of the locally compact abelian group I. Hence each α in $k^\times$ can be uniquely written in the form $\alpha = \alpha_0\alpha_\infty$ with $\alpha_0 \in I_0$, $\alpha_\infty \in I_\infty$. Now, a Hecke character of k (for ideles) is, by definition, a continuous homomorphism $\chi: I \to C^\times$ such that $\chi(k^\times) = 1$; it is called a Hecke character of type (A_0) if there exists an element ω in the group ring $R = Z[G]$ of G over the ring of rational integers Z with the property that

$$\chi(\alpha_\infty) = \alpha^{-\omega}$$

1) For Hecke characters of type (A_0) in general and for Jacobi sums in particular, see Weil [2a], [2b], [2c].

for every α in $k^\times$. Such ω is uniquely determined for χ by the above equality and is denoted by ω_χ. The set H of all Hecke characters of type (A_0) on k forms a multiplicative abelian group in the obvious manner and the map $\chi \mapsto \omega_\chi$ defines a homomorphism

$$\varphi : H \longrightarrow R$$

from the multiplicative group H into the additive group of the group ring $R = \boldsymbol{Z}[G]$. One sees easily that the kernel of φ is the torsion subgroup T of H which is, by class field theory, dual to the Galois group of the maximal abelian extension over k. Let A denote the image of φ in R so that

$$H/T \xrightarrow{\sim} A .$$

Lemma 1. *Let*

$$\theta = \sum_{\sigma \in G} \sigma .$$

Then A consists of all elements ω in R such that

$$(1 + j)\omega = a\theta$$

for some integer a. In particular, A is a two-sided ideal of R containing $(1 - j)R$.

Proof. Let $\|\xi\|$ denote the norm of an idele ξ in I defined in the usual manner. It is well known that $\xi \mapsto \|\xi\|$ defines a surjective homomorphism of I onto the multiplicative group of real numbers, that $k^\times$ is contained in the kernel I_1 of the homomorphism, and that $I_1/k^\times$ is a compact group. It then follows that for each Hecke character χ, there exists a real number r such that $|\chi(\xi)| = \|\xi\|^r$ for every idele ξ. The lemma follows from this and from the definition of Hecke characters of type (A_0).

Let $[G : 1] = [k : \boldsymbol{Q}] = 2n$ and let

$$G = \{\sigma_1, \cdots, \sigma_n, j\sigma_1, \cdots, j\sigma_n\} , \qquad \theta' = \sum_{i=1}^{n} \sigma_i .$$

Then $(1 + j)\theta' = \theta$ and it follows immediately from the above lemma that

$$A = (1 - j)R \oplus \boldsymbol{Z}\theta' .$$

Hence A is a free abelian group of rank $n + 1$. Note also that A is generated over $\boldsymbol{Z}$ by the sums $\theta' = \sum_{i=1}^{n} \sigma_i$ when $\{\sigma_1, \cdots, \sigma_n\}$ ranges over all subsets of G such that $G = \{\sigma_1, \cdots, \sigma_n, j\sigma_1, \cdots, j\sigma_n\}$.

Now, for each integral ideal $\mathfrak{m}$ of k, let $\mathfrak{I}_\mathfrak{m}$ denote the multiplicative group of all ideals of k which are prime to $\mathfrak{m}$. Let χ be a Hecke character of k. Then it follows from the continuity of χ that for a suitable integral ideal $\mathfrak{m}$, χ induces a homomorphism

$$\tilde{\chi} : \mathfrak{I}_\mathfrak{m} \longrightarrow \boldsymbol{C}^\times$$

with the property that

$$\tilde{\chi}((\alpha)) = \chi(\alpha_0) = \chi(\alpha_\infty)^{-1}$$

for every α in $k^\times$ satisfying $\alpha \equiv 1 \bmod^\times \mathfrak{m}$. Furthermore, if χ is of type (A_0), the sets $\chi(I_0)$ and $\tilde{\chi}(\mathfrak{I}_\mathfrak{m})$ generate over k the same field k_χ:

$$k_\chi = k(\chi(I_0)) = k(\tilde{\chi}(\mathfrak{I}_\mathfrak{m})) .$$

Let $\omega = \omega_\chi$ and $(1 + j)\omega = a\theta$, $a \in \boldsymbol{Z}$, as stated in Lemma 1.

Lemma 2. *k_χ is a j-field, finite over k, and for each ideal $\mathfrak{a}$ in $\mathfrak{I}_\mathfrak{m}$,*

$$\tilde{\chi}(\mathfrak{a})^{1+j} = N(\mathfrak{a})^a , \qquad \mathfrak{a}^a = (\tilde{\chi}(\mathfrak{a}))$$

where $N(\mathfrak{a})$ denotes the norm of $\mathfrak{a}$ over $\boldsymbol{Q}$ and $(\tilde{\chi}(\mathfrak{a}))$ is the principal ideal of k_χ generated by $\tilde{\chi}(\mathfrak{a})$.

Proof. If $\alpha \equiv 1 \bmod^\times \mathfrak{m}$, then $\tilde{\chi}((\alpha)) = \chi(\alpha_\infty)^{-1} = \alpha^a$. The two equalities of the lemma follow from this and from the fact that the ray class group mod $\mathfrak{m}$ is a finite group. Let $\xi = \tilde{\chi}(\mathfrak{a})$ for an ideal $\mathfrak{a}$ in $\mathfrak{I}_\mathfrak{m}$ and let $\mathfrak{a}^h = (\alpha)$, $h \geqslant 1$, $\alpha \in k^\times$, $\alpha \equiv 1 \bmod^\times \mathfrak{m}$. Then $\xi^h = \tilde{\chi}((\alpha)) = \alpha^a$ belongs to k while $\xi^{1+j} = N(\mathfrak{a})^a$ is a rational number. Hence $k(\xi)$ is a finite extension of k, invariant under the complex-conjugation. Let σ be any isomorphism of $k(\xi)$ into $\boldsymbol{C}$. Since k is a j-field, $\sigma j = j\sigma$ on k. In particular, $(\xi^h)^{\sigma(1+j)} = (\xi^h)^{(1+j)\sigma}$, namely, $(\xi^{1+j})^{h\sigma} = (\xi^\sigma)^{h(1+j)}$. Since $(\xi^{1+j})^\sigma = N(\mathfrak{a})^{a\sigma} > 0$ and $(\xi^\sigma)^{1+j} > 0$, it follows that $(\xi^{1+j})^\sigma = (\xi^\sigma)^{1+j}$ so that $\sigma j = j\sigma$ on $k(\xi)$. Therefore $k(\tilde{\chi}(\mathfrak{a})) = k(\xi)$ is a j-field, finite over k. As the ray class group mod $\mathfrak{m}$ is finite, k_χ is the composite of a finite number of j-fields such as $k(\xi)$. Hence k_χ is again a j-field, finite over k.

By a similar argument, one can prove the following result which may be of some interest for itself: For each j-field k, finite over $\boldsymbol{Q}$, there exists a j-field F, finite over k, such that every ideal of k becomes a principal ideal in F.

§ 2. Let F be an algebraic number field containing k and let A_F denote

the set of all ω in A such that for every ideal $\mathfrak{a}$ of k, $\mathfrak{a}^\omega$ becomes a principal ideal in F. On the other hand, let B_F be the set of all $\omega_\chi = \varphi(\chi)$ for Hecke characters χ of type (A_0) with the property that $k_\chi \subseteq F$. Then A_F and B_F are additive subgroups of A and by Lemma 2

$$B_F \subseteq A_F \subseteq A .$$

From now on, we shall assume that F is a j-field containing k; since k is imaginary, F also is an imaginary j-field. Let E, E_r, and E_+ denote the group of all units in F, the subgroup of all real units in E, and the subgroup of all totally positive real units in E_r, respectively. Clearly $E_r^2 \subseteq E^{1+j} \subseteq E_+ \subseteq E_r \subseteq E$. Let W be the group of all roots of unity contained in F. Since F is a j-field, the index $[E: WE_r]$ is either 1 or 2, and so is the index $[E^{1+j}: E_r^2]$. Let

$$\bar{E}_F = \bar{E} = E_+/E^{1+j} .$$

Obviously $\bar{E}$ is an abelian group with exponent (at most) 2.

Now, let ω be an element of A_F and let $\mathfrak{a}$ be any ideal of k. By the definition of A_F, $\mathfrak{a}^\omega$ is a principal ideal in F so that

$$\mathfrak{a}^\omega = (\mu)$$

with an element μ in $F^\times$. Since $A_F \subseteq A$, it follows from Lemma 1 that

$$(1 + j)\omega = a\theta$$

with an integer a. Hence

$$N(\mathfrak{a})^a = \mathfrak{a}^{a\theta} = (\mu^{1+j})$$

and we see that

$$\varepsilon = N(\mathfrak{a})^{-a}\mu^{1+j}$$

is a unit of F and, indeed, a totally positive real unit in E_+. If μ is replaced by $\mu\eta$ with η in E, then ε is replaced by $\varepsilon\eta^{1+j}$. Therefore the coset of ε mod E^{1+j} is uniquely determined by ω and $\mathfrak{a}$ so that it may be denoted by $[\omega, \mathfrak{a}]$:

$$[\omega, \mathfrak{a}] = N(\mathfrak{a})^{-a}\mu^{1+j} \bmod E^{1+j} .$$

It is clear that $[\omega, \mathfrak{a}]$ defines a pairing of A_F and the ideal group of k into $\bar{E}$. Furthermore, if $\mathfrak{a} = (\alpha)$, $\alpha \in k^\times$, then $\mathfrak{a}^\omega = (\mu)$ with $\mu = \alpha^\omega$ so that $\varepsilon = N(\mathfrak{a})^{-a}\mu^{1+j}$

$= 1$. Hence $[\omega, \mathfrak{a}]$ depends only upon the ideal class of $\mathfrak{a}$ and it also defines a pairing of A_F and the ideal class group C_k of k into $\bar{E} = \bar{E}_F$:

$$A_F \times C_k \longrightarrow \bar{E}_F .$$

Theorem. *B_F is the annihilator of C_k in A_F in the above pairing so that there is a monomorphism*

$$A_F/B_F \longrightarrow \mathrm{Hom}\,(C_k, \bar{E}_F) .$$

Proof. In the above, F is not necessarily a finite extension over k. However, the proof for the general case can be easily reduced to that of the special case where F is a finite extension of k. Therefore we shall assume in the following that F is finite over k and, hence, also finite over $\boldsymbol{Q}$.

It is clear from Lemma 2 that B_F is contained in the annihilator of C_k in A_F. To prove the converse, let ω be any element of A_F which annihilates C_k in the above pairing. Let w denote the order of the finite group W consisting of all roots of unity in F. We fix a prime ideal $\mathfrak{p}$ of k, prime to w, and denote the norm of $\mathfrak{p}$ over $\boldsymbol{Q}$ by q: $q = N(\mathfrak{p})$. The residue class field of $\mathfrak{p}$ then contains a subgroup canonically isomorphic to W so that $q - 1$ is divisible by w. Let $\mathfrak{a}$ be any ideal of the ideal group $\mathfrak{I}_q$ in k and let $\mathfrak{a}^\omega = (\mu)$, $\mu \in F^\times$, as stated above. Since $[\omega, \mathfrak{a}] = 1$ by the assumption on ω, $\varepsilon = N(\mathfrak{a})^{-a}\mu^{1+j}$ is contained in E^{1+j}: $\varepsilon = \eta^{1+j}$, $\eta \in E$. Hence, replacing μ by $\mu\eta$, we may assume that $N(\mathfrak{a})^a = \mu^{1+j}$. As $\mathfrak{a}$ belongs to $\mathfrak{I}_q$, μ is prime to $\mathfrak{p}$, and there exists a root of unity ζ in W satisfying $\mu^{(q-1)/w} \equiv \zeta \bmod^\times \mathfrak{p}$. Let

$$\omega' = \frac{q-1}{w}\omega , \qquad \nu = \mu^{(q-1)/w}\zeta^{-1} .$$

Then

$$\mathfrak{a}^{\omega'} = (\nu) , \quad N(\mathfrak{a})^{((q-1)/w)a} = \nu^{1+j} , \quad \nu \equiv 1 \bmod^\times \mathfrak{p} .$$

We shall next show that for each $\mathfrak{a}$ in $\mathfrak{I}_q$, there exists only one ν in $F^\times$ satisfying the above conditions. Indeed, let ν' be another element in $F^\times$ satisfying the same conditions and let $\nu' = \nu\eta$. Then η is a unit of F such that $\eta^{1+j} = 1$, $\eta \equiv 1 \bmod^\times \mathfrak{p}$. Since $[E: WE_r] = 1$ or 2, let $\eta^2 = \zeta'\eta_0$ with $\zeta' \in W$, $\eta_0 \in E_r$. From $\eta^{2(1+j)} = 1$, we then see that $\eta_0^2 = 1$, $\eta_0 = \pm 1$ so that $\eta = \pm\zeta'$ belongs to W. It then follows from $\eta \equiv 1 \bmod^\times \mathfrak{p}$ that $\eta = 1$, $\nu' = \nu$.

Now, since ν is unique for $\mathfrak{a}$, the map $\mathfrak{a} \mapsto \nu$ defines a homomorphism

$$\rho: \mathfrak{I}_q \longrightarrow C^\times .$$

If α is an element of $k^\times$ satisfying $\alpha \equiv 1 \bmod^\times \mathfrak{q}$, then $\nu = \alpha^{\omega'}$ obviously satisfies the above conditions for the principal ideal $\mathfrak{a} = (\alpha)$. Hence

$$\rho((\alpha)) = \alpha^{\omega'}$$

for such an ideal (α). By [2a], we then know that there exists a Hecke character χ on k which induces the homomorphism ρ on $\mathfrak{J}_q$: $\tilde{\chi} = \rho$. We also see immediately that χ is of type (A_0) and $\omega' = \omega_\chi = \varphi(\chi)$. Since $\tilde{\chi}(\mathfrak{J}_q) = \rho(\mathfrak{J}_q) \subseteq F^\times$, $\omega' = ((q-1)/w)\omega$ is contained in B_F.

In the above, we have fixed a prime ideal $\mathfrak{p}$ of F, prime to w. However, it is easy to see by class field theory that when $\mathfrak{p}$ ranges over all prime ideals of k, prime to w, then the g.c.d. of $N(\mathfrak{p}) - 1$ is w. Therefore it follows from the above that ω itself is contained in B_F, and this completes the proof of the theorem.

§ 3. We shall next make some remarks on the results mentioned above.

Let F be an arbitrary j-field containing k. Since A_F is a subgroup of A which is a free abelian group of rank $n+1$ and since $\bar{E}^2 = 1$, it follows from the theorem that A_F/B_F is a finite abelian group of type $(2, \cdots, 2)$ with rank at most equal to $n+1$. In particular,

$$2A_F \subseteq B_F \subseteq A_F .$$

Note also that if $\bar{E} = 1$, i.e., if $E_+ = E^{1+J}$, then $A_F = B_F$.

Let $F = k$. In this case, A_k is the subgroup of all ω in A such that $C_k^\omega = 1$, namely, the subgroup of all "relations" on the R-module C_k contained in A. The theorem then states that up to a finite factor group of exponent 2, all such relations are provided by Hecke characters χ of type (A_0) on k with the property $k_\chi = k$, i.e., $\chi(I_0) \subseteq k$.

Let L denote the field generated over k by $\chi(I_0)$ for all Hecke characters χ of type (A_0) on k and let K be the subfield of L generated by $\chi(I_0)$ for all χ in the torsion subgroup T of H:

$$k \subseteq K \subseteq L .$$

As one sees immediately, K is the field generated over k by all roots of unity in C. By the definition, L is the composite of the fields k_χ for all χ in H. Hence, by Lemma 2, L is a j-field. It is also easy to show that L is a Galois extension of the rational field $\boldsymbol{Q}$. Furthermore, since $H/T \simeq A$ and A is a finitely generated abelian group, it follows from the proof of Lemma 2

that L/K is a finite abelian extension. It seems that the extension L/K, which is thus canonically associated with the field k, has some significance for the arithmetic of the ground field k. Here we note only the following simple fact. Let ω be any element of $A = \varphi(H)$ and let $\omega = \omega_\chi$ with χ in H. For any σ in $\mathrm{Gal}(L/K)$, define

$$\chi^{\sigma-1}: I \longrightarrow C^\times$$

by $\chi^{\sigma-1}(\xi) = \chi(\xi)^{\sigma-1}$ for $\xi \in I$. Then $\chi^{\sigma-1}$ is a Hecke character in the torsion subgroup T of H and it depends only upon ω and σ. The map $(\omega, \sigma) \mapsto \chi^{\sigma-1}$ then defines a pairing of A and $\mathrm{Gal}(L/K)$ into T and this induces a non-degenerate pairing

$$A/B_K \times \mathrm{Gal}(L/K) \longrightarrow T .$$

Therefore there exist monomorphisms

$$A/B_K \longrightarrow \mathrm{Hom}(\mathrm{Gal}(L/K), T) , \qquad \mathrm{Gal}(L/K) \longrightarrow \mathrm{Hom}(A/B_K, T) .$$

§ 4. Important examples of Hecke characters χ of type (A_0) with $k_\chi = k$ are provided by Jacobi sums when k is an abelian extension over the rational field.[2] We add here some further remarks on such Hecke characters in connection with what has been discussed above.

For each integer $m \geqslant 1$, let K_m denote the cyclotomic field of m-th roots of unity and let $G_m = \mathrm{Gal}(K_m/\boldsymbol{Q})$ and $R_m = \boldsymbol{Z}[G_m]$. For any real number α, let $\langle \alpha \rangle = \alpha - [\alpha]$ where $[\alpha]$ denotes the largest integer $\leqslant \alpha$. and for any integer t, prime to m, let σ_t denote the automorphism of K_m which maps every m-th root of unity in K_m to its t-th power. We then define

$$\theta_m(a) = \sum_{\substack{t \bmod m \\ (t,m)=1}} \left\langle -\frac{at}{m} \right\rangle \sigma_t^{-1}$$

for any integer a. $\theta_m(a)$ is an element of $\boldsymbol{Q}[G_m]$ such that $m\theta_m(a) \in R_m$, and it depends only upon the residue class of $a \bmod m$. Let $r = (r_1, \cdots, r_s)$ be any finite sequence of elements r_i in $\boldsymbol{Q}/\boldsymbol{Z}$ such that $mr = 0$ and let $r_i = a_i/m \pmod{\boldsymbol{Z}}$ with $a_i \in \boldsymbol{Z}$, $1 \leqslant i \leqslant s$. For such a sequence r, we put

$$\gamma(m, r) = \sum_{i=1}^{s} \theta_m(a_i) .$$

Again $\gamma(m, r)$ is an element of $\boldsymbol{Q}[G_m]$ such that $m\gamma(m, r) \in R_m$. In [2c], a

2) See [2b], [2c].

"modified" Gauss sum $J_m(r, \mathfrak{A})$ is defined for each sequence $r = (r_1, \cdots, r_s)$ with $mr = 0$ and for each ideal $\mathfrak{A}$ of K_m, prime to m. It is an algebraic number of which the m-th power is contained in K_m, and

$$(J_m(r, \mathfrak{A})^m) = \mathfrak{A}^{m r(m,r)}$$

for the principal ideal $(J_m(r, \mathfrak{A})^m)$ in K_m.

In general, let $\boldsymbol{Q} \subseteq k' \subseteq k$ and let both $k/\boldsymbol{Q}$ and $k'/\boldsymbol{Q}$ be finite Galois extensions. Let $G = \mathrm{Gal}(k/\boldsymbol{Q})$, $G' = \mathrm{Gal}(k'/\boldsymbol{Q})$ and $R = \boldsymbol{Z}[G]$, $R' = \boldsymbol{Z}[G']$. Then the canonical homomorphism $f_{k/k'}: G \to G'$ induces a ring homomorphism $R \to R'$ and this will be denoted again by $f_{k/k'}$. There also exists an additive homomorphism $f_{k'/k}: R' \to R$ which maps each σ' in G' to the sum of all σ in G such that $f_{k/k'}(\sigma) = \sigma'$. $f_{k/k'}$ and $f_{k'/k}$ can be extended to homomorphisms $\boldsymbol{Q}[G] \to \boldsymbol{Q}[G']$ and $\boldsymbol{Q}[G'] \to \boldsymbol{Q}[G]$ respectively in the obvious manner. When one or both of k and k' are cyclotomic fields, e.g., $k = K_m$, we shall write simply $f_{m/k'}$ and $f_{k'/m}$ for $f_{k/k'}$ and $f_{k'/k}$ respectively.

Now, let k be an arbitrary finite abelian extension over the rational field $\boldsymbol{Q}$ and let m be any positive integer. Let k' be any subfield of $k \cap K_m$ and let $r = (r_1, \cdots, r_s)$ be a sequence such that $mr = 0$ and such that $f_{m/k'}(\gamma(m, r))$ is contained in the group ring $R' = \boldsymbol{Z}[G']$ of $G' = \mathrm{Gal}(k'/\boldsymbol{Q})$[3]. Then $J_m(r, N_{k/k'}(\mathfrak{a}))$ is contained in k (in fact, in k') for any ideal $\mathfrak{a}$ of k, prime to m. Such an element of k is called a (generalized) Jacobi sum for the field k because in the special case where $k = K_m = k'$, it coincides with a classical Jacobi sum for K_m studied in [2b]. Let a be any integer. The main theorem in [2c] states that there is a Hecke character χ of type (A_0) on k which induces the homomorphism $\tilde{\chi}: \mathfrak{S}_{2m} \longrightarrow \boldsymbol{C}^\times$ defined by

$$\tilde{\chi}(\mathfrak{a}) = J_m(r, N_{k/k'}(\mathfrak{a}))N_{k/\boldsymbol{Q}}(\mathfrak{a})^a .$$

From now on, let us assume that k is an imaginary abelian extension over $\boldsymbol{Q}$. We then see that $k_\chi = k$ for the Hecke character χ mentioned above and that $\omega_\chi = \varphi(\chi)$ in $R = \boldsymbol{Z}[G]$ is given by

$$\delta_k(m, k', r, a) = f_{k'/k}(f_{m/k'}(\gamma(m, r)) + a\theta$$

where θ denotes as before the sum of all elements in $G = \mathrm{Gal}(k/\boldsymbol{Q})$. With k fixed, let S denote the submodule of R generated over $\boldsymbol{Z}$ by such $\delta_k(m, k', r, a)$ for all possible choices of $m, k', r,$ and a (i.e., $m, a \in \boldsymbol{Z}$, $m \geqslant 1$, $k' \subseteq k \cap K_m$,

3) One checks easily that this condition on r is equivalent to the condition $d|r|=0$ in the lemma on p. 6 of [2c].

$mr = 0$, and $f_{m/k'}(\gamma(m, r)) \in R' = \boldsymbol{Z}[G']$ where $G' = \mathrm{Gal}(k'/\boldsymbol{Q})$). Then S is an ideal of R contained in B_k:

$$S \subseteq B_k \subseteq A_k \subseteq A \subseteq R .$$

The elements in S may be called Stickelberger operators for k because in the special case where $k = K_m$, they appear in the classical theorem of Stickelberger. Using the fact that Dirichlet's L-functions $L(s; \psi)$ do not vanish at $s = 1$, we can show that

$$[A : S] < +\infty .$$

Now the question arises: What are the indices

$$[A : S], \quad [A_k : S] = [A_k : B_k][B_k : S] .$$

In the simplest case, namely, in the case where k is an imaginary quadratic field, one can compute $[A : A_k]$ and $[A : S]$ without much difficulty and find that $[A : A_k]$ is the exponent of the ideal class group C_k of k while $[A : S]$ is the order of C_k, namely, the class number of k. Hence, in general, A_k/S is not a 2-group like A_k/B_k. On the other hand, one can also prove that if k is the cyclotomic field of m-th roots of unity, $k = K_m$, and if m is divisible by at most two distinct prime numbers, then $[A : S]$ is equal to the first factor of the class number of k[4]. Although the number of known examples is limited, this seems to suggest that the same equality might hold for any imaginary abelian extension k over $\boldsymbol{Q}$ or at least for all cyclotomic fields K_m[5]. The proof of such a conjecture, if true, may require some intrinsic characterization of the elements of S among the relations on C_k given by the elements of A_k or B_k, and such a characterization in turn may enable us to define Stickelberger operators for an arbitrary Galois j-field k which is not necessarily abelian over $\boldsymbol{Q}$.

Bibliography

[1] Iwasawa, K., A class number formula for cyclotomic fields, Ann. Math. **76** (1962), 171–179.

[2] Weil, A., (a) On a certain type of characters of the idele-class group, Proc. Int. Symp. Alg. Number Theory, Tokyo-Nikko, 1955, 1–7; (b) Jacobi sums as "Grössencharak-

4) See [1] for the case where m is a power of an odd prime.

5) *Added in proof.* Indeed, such an equality for K_m has since been proved by W. M. Sinnott with an additional factor which is a power of 2.

tere", Trans. Amer. Math. Soc. **73** (1952), 487–495; (c) Sommes de Jacobi et caracteres de Hecke, Nachrich. der Akad. Göttingen 1974, 1–14.

Department of Mathematics
Princeton University
Princeton, N.J. 08540
U.S.A.

ALGEBRAIC NUMBER THEORY, Papers contributed for the International Symposium, Kyoto 1976; S. Iyanaga (Ed.): Japan Society for the Promotion of Science, Tokyo, 1977

Congruences between Cusp Forms and Linear Representations of the Galois Group

MASAO KOIKE

Let $f(z)$ be a cusp form of type $(1, \varepsilon)$ on $\Gamma_0(N)$ which is a common eigenfunction of all the Hecke operators. For such $f(z)$, Deligne and Serre [1] proved that there exists a linear representation

$$\rho : G \longrightarrow GL_2(C) \qquad \text{where } G = \mathrm{Gal}(\bar{Q}/Q) ,$$

such that the Artin L-function for ρ is equal to the L-function associated to $f(z)$. Here, we shall show that, for almost every prime l, the subfield of $\bar{Q}$ corresponding to the kernel of ρ is realized as a field generated by the coordinates of certain points of finite order of an abelian variety attached to a certain cusp form of type $(2, \varepsilon\psi)$ on $\Gamma_0(Nl)$, where ψ is a character of $(Z/lZ)^\times$ of order $l-1$. (See Theorem 2.3)

We next apply the above result to the theory of Shimura [5] to obtain further theorems in § 4.

The proof is based on an idea of Shimura which is very useful for proving congruences between cusp forms. The author wishes to express his hearty thanks to Prof. G. Shimura for suggesting these problems.

For proofs of theorems in this note, see [3] which is to appear.

Notations

K: number field.
$\mathfrak{o}_K$: the maximal integer ring of K.
$\mathfrak{p}_\infty$: a real archimedean prime of K.
$(x/\mathfrak{p}_\infty) = 1$ or -1 according as x is positive or negative at $\mathfrak{p}_\infty$ for $x \in K$.
For a formal product $\mathfrak{f}$ of an integral ideal $\mathfrak{f}_0$ and archimedean primes of K, $I(\mathfrak{f})$ will denote the group of all fractional ideals in K prime to $\mathfrak{f}_0$.
$\chi(a) = (N/a)$: the Legendre symbol for $a \in Z, (a, N) = 1$.

$S_*(N, \varepsilon)$: the vector space of all cusp forms of type (κ, ε) on $\Gamma_0(N)$.

§ 1. Preliminaries

Here we explain an idea which is very useful to prove congruences between cusp forms of different weights and of different levels. The idea consists of the following two parts.

1.1. Eisenstein series of weight 1.

Let l be an odd prime. We fix a prime divisor $\tilde{l}$ lying above l in the algebraic closure $\bar{\boldsymbol{Q}}$ in $\boldsymbol{C}$ of $\boldsymbol{Q}$. Let ψ be the Dirichlet character defined mod l satisfying

$$\psi(a)a \equiv 1 \pmod{\tilde{l}} \qquad \text{for all } a \in \boldsymbol{Z},\ (a, l) = 1 .$$

For any Dirichlet character χ defined mod l, let

$$E_{1,\chi}(z) = 1 + \frac{2}{L(0,\chi)} \sum_{\substack{m>0 \\ m_1>0}} \chi(m) e^{2\pi i m m_1 z} ,$$

where $L(s, \chi)$ is the Dirichlet's L-function for the character χ. Then $E_{1,\chi}(z)$ is the Eisenstein series of type $(1, \chi)$ on $\Gamma_0(l)$.

Since $L(0,\chi) = -\dfrac{\sum_{1 \le a \le l-1} \chi(a)a}{l}$, we have

$$\left| \frac{2}{L(0,\chi)} \right| = \begin{cases} l^{-1} & \text{if } \chi = \psi , \\ \geq 1 & \text{otherwise} , \end{cases}$$

where we denote by $|x|$, for $x \in \bar{\boldsymbol{Q}}$, the absolute value on $\tilde{l}$-adic completion of $\bar{\boldsymbol{Q}}$ normalized so that $|l| = l^{-1}$.

Especially for the character ψ, we have the following congruence:

$$E_{1,\psi}(z) \equiv 1 \pmod{\tilde{l}} .$$

We should remark that the Eisenstein series $E_{l-1}(z)$ of weight $l-1$ on $SL_2(\boldsymbol{Z})$ satisfies the same congruence:

$$E_{l-1}(z) = 1 - \frac{2(l-1)}{B_{l-1}} \sum_{\substack{m>0 \\ m_1>0}} m^{l-2} e^{2\pi i m m_1 z} ,$$

$$E_{l-1}(z) \equiv 1 \pmod{l} \qquad \text{if } l \geq 5 ,$$

where B_{l-1} is the $l-1$-th Bernoulli number. $E_{p-1}(z)$ was used by Serre in [4] to develop the theory of p-adic modular forms and was also used by Deligne and Serre to prove a theorem about which we shall make a certain remark in the next section. Our idea, which is due to Shimura, is to use $E_{1,\psi}(z)$ instead of $E_{l-1}(z)$.

1.2. Lemma of Deligne and Serre. We quote a lemma from [1].

Lemma 1.1 (Deligne and Serre). *Let $f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z}$ be a cusp form of type (κ, ε) on $\Gamma_0(N)$ such that a_n are $\tilde{l}$-adic integers for all $n \geq 1$. Suppose a_n satisfy the following congruences for every prime p*

$$a_n a_p \equiv a_{np} + \varepsilon(p) p^{\kappa-1} a_{n/p} \pmod{\tilde{l}} \qquad \text{if } p \nmid N ,$$
$$a_n a_p \equiv a_{np} \pmod{\tilde{l}} \qquad \text{if } p \mid N .$$

Then, there exists a cusp form $g(z) = \sum_{n=1}^{\infty} b_n e^{2\pi i n z}$ of the same type (κ, ε) as $f(z)$ on $\Gamma_0(N)$ such that

(1.1) *$g(z)$ is a common eigenfunction of all the Hecke operators.*

(1.2) $a_n \equiv b_n \pmod{\tilde{l}}$ *for all* $n \geq 1$.

§ 2. Remark on a theorem of Deligne and Serre

2.1. First we recall a theorem of Deligne and Serre.

Theorem 2.1 (Deligne and Serre [1]). *Let $N \geq 1$ be an integer and let ε be a Dirichlet character defined* mod N *such that $\varepsilon(-1) = -1$. Let*

$$f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z} , \qquad a_1 = 1 ,$$

be a cusp form of type $(1, \varepsilon)$ on $\Gamma_0(N)$ which is a common eigenfunction of Hecke operators $T(p)$ for all primes $p \nmid N$ with eigenvalues a_p. Then there exists a linear representation

$$\rho : G \longrightarrow GL_2(\boldsymbol{C}) \qquad \text{where } G = \mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q}) ,$$

such that ρ is unramified outside of N and satisfies

$$\mathrm{Tr}(F_{\rho,p}) = a_p , \quad \det(F_{\rho,p}) = \varepsilon(p) \qquad \text{for all primes } p \nmid N ,$$

where $F_{\rho,p}$ is the image by ρ of the Frobenius element related to p.

The representation ρ associated with $f(z)$ by Theorem 2.1 is irreducible and the image of ρ is finite. We denote by K_f the subfield of $\bar{\boldsymbol{Q}}$ corresponding to the kernel of ρ. Then K_f is a finite Galois extension over $\boldsymbol{Q}$. We shall show that K_f can be realized as a field generated by the coordinates of certain points of finite order of an abelian variety attached to a certain cusp form of type $(2, \varepsilon\psi)$ on $\Gamma_0(Nl)$.

Before that, we recall a theorem of Shimura. Let $N \geq 1$ be an integer and let χ be a Dirichlet character defined mod N such that $\chi(-1) = 1$. Let

$$h(z) = \sum_{n=1}^{\infty} c_n e^{2\pi i n z}, \qquad c_1 = 1,$$

be a cusp form of type $(2, \chi)$ on $\Gamma_0(N)$ which is a common eigenfunction of all the Hecke operators. We denote by M the subfield of $\boldsymbol{C}$ generated over $\boldsymbol{Q}$ by the Fourier coefficients c_n for all n. Then we have

Theorem 2.2 (Shimura [5]). *There exists a couple (A, θ) with the following properties:*

(2.1) *A is an abelian subvariety, of dimension $[M: \boldsymbol{Q}]$, of the Jacobian variety of the modular function field with respect to $\Gamma_1(N)$.*

(2.2) *θ is an isomorphism of M into* End $(A) \otimes \boldsymbol{Q}$.

(2.3) *A and the elements of $\theta(M) \cap$* End (A) *are rational over $\boldsymbol{Q}$.*

(2.4) *For every prime p, $\theta(c_p)$ coincides with the homomorphism of A naturally induced from the Hecke operator $T(p)$ or $U(p)$.*

Changing (A, θ) by an isogeny over $\boldsymbol{Q}$, if necessary, we may assume

(2.5) $$\theta(\mathfrak{o}_M) \subset \text{End}\, A\ .$$

2.2. We fix a cusp form $f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z}$, $a_1 = 1$, of type $(1, \varepsilon)$ on $\Gamma_0(N)$ which is a common eigenfunction of all the Hecke operators. Let N' be the least common multiple of N and l. If l does not divide N, $f(z)$ is replaced by $f(z) - \alpha f(lz)$ where α is a solution of the equation $X^2 - a_l X + \varepsilon(l) = 0$. Put $g(z) = f(z) \cdot E_{1,\psi}(z) = \sum_{n=1}^{\infty} b_n e^{2\pi i n z}$. Then $g(z)$ is an element of $S_2(N', \varepsilon\psi)$ and it is obvious that b_n satisfy the conditions in Lemma 1.1. Therefore, there exists an element $h(z) = \sum_{n=1}^{\infty} c_n e^{2\pi i n z}$, $c_1 = 1$, of $S_2(N', \varepsilon\psi)$ such that (1) $h(z)$ is a common eigenfunction of all the Hecke operators and (2) $c_n \equiv b_n \pmod{\tilde{\mathfrak{l}}}$ for all $n \geq 1$.

Now we assume that l is greater than 3 and is prime to the order of Gal $(K_f/\boldsymbol{Q})$. Let (A, θ) be a couple associated with $h(z)$ by means of Theorem 2.1. We denote by $\mathfrak{l}$ the prime ideal of M which is lying below $\tilde{\mathfrak{l}}$. Put

$A[\mathfrak{l}] = \{t \in A \mid \theta(\mathfrak{l})t = 0\}$,

$L_{\mathfrak{l}}$ = the subfield of $\boldsymbol{C}$ generated by the coordinates of all points of $A[\mathfrak{l}]$.

Then we have

Theorem 2.3. *$L_{\mathfrak{l}}$ coincides with K_f.*

§ 3. Congruences between cusp forms

First we briefly recall Shimura's theory from [5]. Let N be a positive integer and χ be an arbitrary real-valued character of $(\boldsymbol{Z}/N\boldsymbol{Z})^{\times}$ such that $\chi(-1) = 1$. We denote by k the real quadratic field corresponding to χ and by ε the non-trivial automorphism of k. We fix a cusp form $h(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z}$ of $S_2(N, \chi)$. We assume that $h(z)$ belongs to the essential part and that $h(z)$ is a common eigenfunction of all the Hecke operators. We normalize h so that $a_1 = 1$. We denote by K the subfield of $\boldsymbol{C}$ generated over $\boldsymbol{Q}$ by the coefficients a_n for all n and by F the maximal real subfield of K. Let $\mathfrak{b}$ be the odd part of the ideal of $\mathfrak{o}_K$ generated by $\{x \in \mathfrak{o}_K \mid x^{\rho} = -x\}$ (ρ being the complex conjugation) and put $N_{K/F}(\mathfrak{b}) = \mathfrak{c}$. Then the following is a fundamental theorem in [5].

Theorem 3.1 (Shimura). *Let $\mathfrak{l}$ be a prime factor of $\mathfrak{c}$ in F. Then, there exist $(\mathfrak{o}_F/\mathfrak{l})^{\times}$-valued characters $r_{\mathfrak{l}}$ and $s_{\mathfrak{l}}$ of an ideal group of k satisfying the following properties:*

(3.1) *Let $\mathfrak{f}[r_{\mathfrak{l}}]$ be the conductor of $r_{\mathfrak{l}}$. Then $\mathfrak{f}[r_{\mathfrak{l}}]^{\rho} = \mathfrak{f}[s_{\mathfrak{l}}]$ and every finite prime factor of $\mathfrak{f}[r_{\mathfrak{l}}]$ divides $N_{k/\boldsymbol{Q}}(\mathfrak{l})N$.*

(3.2) *$r_{\mathfrak{l}}(\mathfrak{a}) = s_{\mathfrak{l}}(\mathfrak{a}^{\rho})$ for every $\mathfrak{a} \in I(\mathfrak{f}[r_{\mathfrak{l}}])$.*

(3.3) *$r_{\mathfrak{l}}(m\mathfrak{o}_k) = s_{\mathfrak{l}}(m\mathfrak{o}_k) = \left(\frac{m}{\mathfrak{p}_{\infty}}\right) \cdot (m \bmod \mathfrak{l})$ for every $m \in \boldsymbol{Z}$ prime to $\mathfrak{f}[r_{\mathfrak{l}}]$ where $\mathfrak{p}_{\infty}$ is the archimedean prime of $\boldsymbol{Q}$.*

(3.4) *$r_{\mathfrak{l}}(\mathfrak{a}) \cdot s_{\mathfrak{l}}(\mathfrak{a}) = \mathrm{N}_{k/\boldsymbol{Q}}(\mathfrak{a}) \bmod \mathfrak{l}$ for every $\mathfrak{a} \in I(\mathfrak{f}[r_{\mathfrak{l}}]) \cap I(\mathfrak{f}[s_{\mathfrak{l}}])$.*

(3.5) *If p is a rational prime that is prime to $\mathrm{N}_{k/\boldsymbol{Q}}(\mathfrak{l})N$, and that decomposes into two distinct prime ideals $\mathfrak{p}$ and $\mathfrak{p}^{\rho}$ in k, then*

$$r_{\mathfrak{l}}(\mathfrak{p}) + s_{\mathfrak{l}}(\mathfrak{p}^{\rho}) = a_p \bmod \mathfrak{l}\ .$$

The properties of these characters $r_{\mathfrak{l}}$ and $s_{\mathfrak{l}}$ are connected with the reciprocity law of a certain abelian extension of k which can be generated by the coordinates of certain points of finite order on an abelian variety associated with $h(z)$. From Theorem 3.1, it follows a formal congruence between partial sum of $h(z)$ and a formal power series $\tilde{h}_{r_{\mathfrak{l}}}(z)$ defined by

$$\tilde{h}_{r_{\mathfrak{l}}}(z) = \sum_{\mathfrak{a}} r_{\mathfrak{l}}(\mathfrak{a}) e^{2\pi i N_{k/\boldsymbol{Q}}(\mathfrak{a}) z}\ ,$$

where the sum is extended over all integral ideals prime to $\mathfrak{f}[r_\mathfrak{l}]$. Moreover Shimura conjectured that the congruence holds between entire sums. $\tilde{h}_{r_\mathfrak{l}}(z)$ is actually reduction mod $\tilde{\mathfrak{l}}$ of a cusp form of weight 1 which is the Mellin transform of a L-function of k with a certain class character.

Our purpose is to prove directly, not by way of abelian varieties, congruences between cusp forms of weight $\kappa, \kappa \geq 2$ and cusp forms of weight 1 which are the Mellin transforms of L-functions of real quadratic fields with certain class characters. Our result is as follows:

Let $k = \boldsymbol{Q}(\sqrt{N})$ be a real quadratic field and let N be the discriminant of k. Let $l \geq 5$ be a prime which decomposes into two distinct prime ideals in k. We fix a prime factor $\mathfrak{l}_1$ of l in k such that $\mathfrak{l}_1$ is lying below $\tilde{\mathfrak{l}}$. Let $\mathfrak{p}_\infty$ be an archimedean prime of k and let $\mathfrak{m}$ be an integral ideal of k such that $\mathfrak{m}$ is prime to l. Put $m = \mathrm{N}_{k/\boldsymbol{Q}}\mathfrak{m}$. Let λ be a $\boldsymbol{C}^\times$-valued character of the ideal group of k whose conductor is $\mathfrak{p}_\infty \cdot \mathfrak{m} \cdot \mathfrak{l}_1$. With such a λ, we associate a function $f_\lambda(z)$ by

$$f_\lambda(z) = \sum_{\mathfrak{a}} \lambda(\mathfrak{a}) e^{2\pi i N_{k/\boldsymbol{Q}}(\mathfrak{a})} ,$$

where $\mathfrak{a}$ runs over all integral ideals of k prime to $\mathfrak{m}\mathfrak{l}_1$. $f_\lambda(z)$ is proved to be a cusp form of type $(1, \chi)$ on $\Gamma_0(lmN)$ with $\chi(a) = (N/a)\lambda(a\mathfrak{o}_k)$ for $a \in \boldsymbol{Z}$, $(a, lmN) = 1$, where (N/a) is the Legendre symbol. Moreover, on account of that the corresponding L-function has an Euler product, $f_\lambda(z)$ is a common eigenfunction of all the Hecke operators. χ is decomposed into the product of χ_1 and χ_2 which are characters of $(\boldsymbol{Z}/l\boldsymbol{Z})^\times$ and of $(\boldsymbol{Z}/mN\boldsymbol{Z})^\times$ respectively. Since ψ is a generator of the character group of $(\boldsymbol{Z}/l\boldsymbol{Z})^\times$, there exists a positive integer κ such that $\chi_1 = \psi^{-\kappa}$. Then our result is the following:

Theorem 3.2. *The notations being as above, there exists a cusp form $h(z)$ of type $(\kappa + 1, \chi_2)$ on $\Gamma_0(mN)$ such that*

(3.6) *$h(z)$ is a common eigenfunction of all the Hecke operators.*

(3.7) $$h(z) \equiv f_\lambda(z) \pmod{\tilde{\mathfrak{l}}} .$$

§ 4. Real quadratic fields and Hecke operators

Here we apply our result in § 3 to Shimura's theory [5] for proving some conjectures and we deal with only the case of square-free level N with the character $(N/\ )$.

Let $k = \boldsymbol{Q}(\sqrt{N})$ with a positive square-free integer $N \equiv 1 \pmod 4$. Let u be the fundamental unit of k. *Suppose* $\mathrm{N}_{k/\boldsymbol{Q}}u = -1$. Let $l \geq 5$ be a rational prime which divides $\mathrm{N}_{k/\boldsymbol{Q}}(u-1)$. Then l decomposes into two prime ideals $\mathfrak{l}_1$ and $\mathfrak{l}_1'$ in k. Moreover $u - 1$ is divisible by only one of the two prime factors of l in k. Hence we may assume that $u \equiv 1 \pmod{\mathfrak{l}_1}$ and $\mathfrak{l}_1$ is lying below $\tilde{\mathfrak{l}}$. Let $\mathfrak{p}_\infty$ be an archimedean prime of k such that $(u/\mathfrak{p}_\infty) = 1$. Then, there exists an ideal character λ of k with conductor $\mathfrak{p}_\infty \cdot \mathfrak{l}_1$ satisfying

$$\lambda(\alpha\mathfrak{o}_k) = \left(\frac{\alpha}{\mathfrak{p}_\infty}\right) \cdot \psi^{-1} \circ \iota(\alpha \bmod \mathfrak{l}_1)$$

for every α in k prime to $\mathfrak{l}_1$. Here $\iota : (\mathfrak{o}_k/\mathfrak{l}_1)^\times \to (\boldsymbol{Z}/l\boldsymbol{Z})^\times$ is the natural isomorphism such that $\iota(a \bmod \mathfrak{l}_1) = a \bmod l$ for every $a \in \boldsymbol{Z}$, $(a, l) = 1$.

We fix such a λ. Then the associated function $f_\lambda(z)$ is a cusp form of type $(1, (N/\ )\psi^{-1})$ on $\Gamma_0(lN)$ which is a common eigenfunction of all the Hecke operators. Applying Theorem 3.2 to $f_\lambda(z)$, we obtain the following

Proposition 4.1. *There exists a cusp form $h(z)$ of type $(2, (N/\ ))$ on $\Gamma_0(N)$ such that*

(4.1) *$h(z)$ is a common eigenfunction of all the Hecke operators.*

(4.2) $$h(z) \equiv f_\lambda(z) \pmod{\tilde{\mathfrak{l}}} .$$

We fix such a $h(z)$ obtained in the above proposition and, to $h(z)$, we apply Shimura's theory a part of which is explained in § 3, namely we consider $(A, \theta), K, F, \mathfrak{c}, r_\mathfrak{l}$, etc. for the fixed $h(z)$. Let $\mathfrak{b}^*$ be the ideal of K generated by the Fourier coefficients c_n of $h(z)$ for all n such that $(N/n) = -1$. We suppose that $\mathfrak{b}$ and $\mathfrak{b}^*$ consist of the same prime factors except 2 and 3. This is not yet proved. As a corollary, we immediately obtain

Corollary 4.2. *l is a prime factor of $N(\mathfrak{c})$.*

Hence the prime ideal $\mathfrak{l}$ of F which is lying below $\tilde{\mathfrak{l}}$ is a prime factor of $\mathfrak{c}$, let $\mathfrak{b}_\mathfrak{l}$ be a prime ideal of K such that $\mathfrak{b}_\mathfrak{l}^2 = \mathfrak{l} \cdot \mathfrak{o}_K$. Then we have

Corollary 4.3. $L_{\mathfrak{b}_\mathfrak{l}} = K_{f_\lambda}$.

The relation between λ and $r_\mathfrak{l}$ is as follows. We denote by $\mathscr{F}$ the residue field of $\bar{\boldsymbol{Q}}$ with respect to $\tilde{\mathfrak{l}}$. Then $\mathfrak{o}_F/\mathfrak{l}$ is canonically imbedded into $\mathscr{F}$. For any $\mathfrak{a} \in I(\mathfrak{l}_1)$, we define $\tilde{\lambda}(\mathfrak{a})$ by $\tilde{\lambda}(\mathfrak{a}) = \lambda(\mathfrak{a}) \bmod \tilde{\mathfrak{l}}$. It is obvious that the conductor of $\tilde{\lambda}$ is equal to $\mathfrak{p}_\infty \cdot \mathfrak{l}_1$.

Corollary 4.4. *Either $r_\mathfrak{l}$ or $s_\mathfrak{l}$ coincides with $\tilde{\lambda}$. Especially the conductor $\mathfrak{f}[r_\mathfrak{l}]$ of $r_\mathfrak{l}$ is equal to $\mathfrak{p}_\infty \cdot \mathfrak{l}_1$ and the following congruence holds:*

$$h(z) \equiv \tilde{f}_{r_l} \pmod{\tilde{l}} .$$

Now we go back to the general theory and explain another conjecture of Shimura. Assume N is a prime. Accordingly $\chi(a) = (N/a)$ and $N \equiv 1 \pmod 4$, so that $k = Q(\sqrt{N})$. Let u be the fundamental unit of k. In [5], Shimura conjectured that

(4.3) $\mathrm{N}_{F/Q}(\mathfrak{c})$ *and* $\mathrm{Tr}_{k/Q}u$ *consist of the same prime factors, if we disregard* 2 *and* 3.

We can give a partial answer for his conjecture as a direct consequence of Proposition 4.1.

Proposition 4.5. *Let N be a square-free integer such that $N \equiv 1 \pmod 4$ and let u be the fundamental unit of $k = Q(\sqrt{N})$. Assume $\mathrm{N}_{k/Q}u = -1$. Let $l \geq 5$ be any prime which divides $\mathrm{Tr}_{k/Q}u$. Then there exists a cusp form $h(z)$ of type $(2, (N/\ ))$ on $\Gamma_0(N)$ which is a common eigenfunction of all the Hecke operators such that l divides $\mathrm{N}_{F/Q}(\mathfrak{c})$ for $h(z)$.*

References

[1] Deligne, P. and Serre, J.-P., Formes modulaires de poids 1, Ann. scient. Ec. Norm. Sup. 4e série, **7**, 1974, 507–530.

[2] Hecke, E., Theorie der Eisensteinschen Reihen höhere Stufe und ihre Anwendung auf Funktionentheorie und Arithmetik, Math. Werke, 461–468, Vandenhoeck & Ruprecht, Göttingen, 1958.

[3] Koike, M., Congurences between cusp forms and linear representations of the Galois group, to appear.

[4] Serre, J.-P., Formes modulaires et fonctions zêta p-adiques, Modular functions of one variable III, 191–268, Proc. Intern. Summer School, Univ. Antwerp, RUCA, 1972, Lecture Notes in Math., **350** (1973), Springer, Berlin.

[5] Shimura, G., Class fields over real quadratic fields and Hecke operators, Ann. of Math., **95** (1972), 130–190.

Department of Mathematics
Faculty of Science
Nagoya University
Chikusa-ku, Nagoya 464
Japan

ALGEBRAIC NUMBER THEORY, Papers contributed for the International Symposium, Kyoto 1976; S. Iyanaga (Ed.): Japan Society for the Promotion of Science, Tokyo, 1977

On a Generalized Weil Type Representation

TOMIO KUBOTA*

This paper contains a complete exposition on the unitary representation announced in [1].

For three particular types of elements σ of $G = SL(2, C)$, define unitary operators $r(\sigma)$ of $L^2(C)$ with respect to the euclidean measure $dV(z)$ of C by

$$(1) \qquad (r(\sigma)\Phi)(t) = \begin{cases} |a|\,\Phi(at) & \sigma = \begin{pmatrix} a & \\ & a^{-1} \end{pmatrix}, \\ \Phi(t)e(\frac{1}{2}bt^2) & \text{for} \quad \sigma = \begin{pmatrix} 1 & b \\ & 1 \end{pmatrix}, \\ |c|^{-1}\hat{\Phi}(-c^{-1}t) & \sigma = \begin{pmatrix} & -c^{-1} \\ c & \end{pmatrix}, \end{cases}$$

$(\Phi \in L^2(C))$, where

$$e(t) = \exp(\pi\sqrt{-1}(t + \bar{t})) ,$$

and $\hat{\Phi}$ is the Fourier transform of Φ defined by

$$\hat{\Phi}(w) = \int_C \Phi(z)e(zw)\, dV(z) ;$$

then $\sigma \to r(\sigma)$ extends multiplicatively to a unitary representation of G, which is a special case of the representation constructed in [4], and, as the second formula of (1) shows, is "quadratic". The aim of the present paper is to construct a similar unitary representation "of degree n" for an arbitrary natural number $n \geqq 2$, which is fixed once for all.

Throughout this paper, the function $k(z)$ given in Theorem 1 of [2], and the integral transformation $\Phi \to \Phi^*$ defined by (7) of [2] using $k(z)$ will be assumed to be known, and every integral of the form $\int_C$ resp. $\int_0^\infty$, which is

* This research is supported by NSF Grant GP-43950 (SK-CUCB).

not absolutely convergent, should be understood in the sense of $\lim_{Y\to\infty}\int_{|z|<Y}$ resp. $\lim_{Y\to\infty}\int_C^Y$.

Proposition 1. *If $z, w \in C$ are not zero, then*

$$\int_C e(t^n z)k(tw)\,|t|^{2n-4}\,dV(t) = |z|^{-2(n-1)/n}e\left(w^n\frac{-1}{z}\right).$$

Proof. It is enough to prove the case of $z = -\frac{1}{z} = \sqrt{-1}$.

In view of

$$(2)\qquad e(t^n\sqrt{-1}) = \sum_{m=-\infty}^{\infty} J_{-m}(2\pi r^n)\exp(\sqrt{-1}mn\theta)\,, \qquad (t = r\exp(\sqrt{-1}\theta))\,,$$

and Proposition 1 of [2], we have

$$\int_C e(t^n)k(tw)\,|t|^{2n-4}\,dV(t) = \sum_{m=-\infty}^{\infty} c_{mn}(r')\exp(\sqrt{-1}mn\theta')\,,$$

$(w = r'\exp(\sqrt{-1}\theta'))$, with

$$c_{mn}(r') = 2\pi\int_0^\infty J_m(2\pi r^n)a_{mn}(rr')r^{2n-3}\,dr\,.$$

To show the existence of this integral, we first change the variable from r to $r^{1/n}$, and then, using the asymptotic formula

$$J_\nu(z) = \sqrt{\frac{2}{\pi z}}\left\{\cos\left(z - \frac{2\nu+1}{4}\pi\right) + O(|z|^{-1})\right\},$$

$(|z|\to\infty)$, and the corollary to Theorem 1 of [2], reduce the problem to the existence of the integral of the form $\int_1^\infty e(x)e(x^\alpha)x^{-\beta}dx$, $(0<\alpha<1,\ 0<\beta)$, that can be verified by means of partial integration and by the fact that $e(x)$ remains bounded after repeated integration.

We introduce here a parameter ρ, put

$$(3)\qquad c_{mn}(r',\rho) = 2\pi\int_0^\infty J_m(2\pi r^n)a_{mn}(rr')r^{\rho+2n-3}\,dr$$

for $m \geqq 0$, and compute $M(c_{mn}(r',\rho), s)$ first formally, where M stands for the Mellin transformation defined by

$$M(\psi, s) = \int_0^\infty \psi(r)r^s\frac{dr}{r}$$

for a function $\psi(r)$ of $r \geqq 0$. Since

$$M(J_m(2\pi r^n), s) = \frac{1}{n}(2\pi)^{-s/n}\frac{2^{(s/n)-1}\Gamma(s/2n + m/2)}{\Gamma(1 - s/2n + m/2)}\,,$$

$(0 < \operatorname{Re} s < n/2)$, we get

$$\begin{aligned} &M(c_{mn}(r',\rho), s)\\ &\quad= 2\pi\int_0^\infty\int_0^\infty J_m(2\pi r^n)a_{mn}(rr')r^{\rho+2n-3}\,dr\,r'^s\frac{dr'}{r'}\\ &\quad= 2\pi\int_0^\infty\int_0^\infty J_m(2\pi r^n)a_{mn}(r')r^{\rho+2n-3}\left(\frac{r'}{r}\right)^s dr\frac{dr'}{r'}\\ &\quad= 2\pi\int_0^\infty J_m(2\pi r^n)r^{\rho+2n-2-s}\frac{dr}{r}\int_0^\infty a_{mn}(r')r'^s\frac{dr'}{r'}\,, \end{aligned}$$

which is equal to

$$(4)\qquad \begin{aligned} &2\pi\cdot\frac{1}{n}(2\pi)^{-(\rho+2n-2-s)/n}\\ &\quad\times\frac{2^{(\rho+2n-2-s)/n-1}\Gamma((\rho+2n-2-s)/2n + m/2)}{\Gamma(1-(\rho+2n-2-s)/2n + m/2)}M(a_{mn}, s)\,. \end{aligned}$$

Now, the last two integrals exist in the region determined, for instance, by $0 < \operatorname{Re} s < \varepsilon$ and $-2n + 3 - \varepsilon < \operatorname{Re}\rho < -2n + 3$ with small $\varepsilon > 0$. Consequently, $M(c_{mn}(r',\rho), s)$ is well-defined in the same region, and $c_{mn}(r',\rho)$ is the inverse Mellin transform of $M(c_{mn}(r',\rho), s)$, whenever $-2n + 3 - \varepsilon < \operatorname{Re}\rho < -2n + 3$. Since, however, the integral (3) exists for $-2n + 3 - \varepsilon < \operatorname{Re}\rho < \varepsilon$, and is holomorphic with respect to ρ, the analytic continuation to $\rho = 0$ of (3) should coincide with that of the inverse Mellin transform of (4). At $\rho = 0$, (4) reduces to

$$2\pi M(J_m(2\pi r^n), 2n - 2 - s)M(a_{mn}, s)\,,$$

and, by Proposition 1 of [2], reduces furthermore to

$$\begin{aligned} &\frac{2\pi}{n}(2\pi)^{-(2n-2-s)/n}2^{(2n-2-s)/n-1}\frac{(-1)^m}{2\pi}\pi^{-2(s-(n-1))/n}\frac{\Gamma(s/2n + m/2)}{\Gamma((2n-s)/2n + m/2)}\\ &\quad= (-1)^m M(J_m(2\pi r^n), s) = M(J_{-m}(2\pi r^n), s)\,, \end{aligned}$$

because of $M_0(a_{mn}, s) = M(a_{mn}, s)$. This shows

(5) $$c_{mn}(r') = c_{mn}(r', 0) = J_{-m}(2\pi r'^n) ,$$

i.e.,

$$J_{-m}(r') = 2\pi \int_0^\infty J_m(2\pi r^n) a_{mn}(rr') r^{2n-3}\, dr .$$

Since this formula remains true after m is replaced by $-m$, (5) holds for $m < 0$, too. (q.e.d.)

Here we introduce the upper half space; it is the space H of all $u = (z, v)$, $(z \in \boldsymbol{C},\ v > 0)$. If we put $\tilde{t} = \begin{pmatrix} t & \\ & \bar{t} \end{pmatrix}$, $(t \in \boldsymbol{C})$, and identify $u = (z, v) \in H$ with the matrix $\begin{pmatrix} z & -v \\ v & \bar{z} \end{pmatrix}$, then $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G = SL(2, \boldsymbol{C})$ operates on H by the fractional linear transformation $\sigma u = (\tilde{a}u + \tilde{b})(\tilde{c}u + \tilde{d})^{-1}$. Since $K = SU(2)$ is the isotropy group of $(0, 1) \in H$, H is a realization of the homogenous space G/K. There is a G-invariant Riemannian structure $v^{-2}(dx^2 + dy^2 + dv^2)$, $(x = \operatorname{Re} z,\ y = \operatorname{Im} z)$, on H, and corresponding invariant measure and Laplacian are given by $du = v^{-3}\, dx\, dy\, dv$ and by

$$D = v^2\left(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} + \frac{\partial^2}{\partial v^2}\right) - v\frac{\partial}{\partial v} ,$$

respectively. Furthermore, if $g(u)$ is a function on H, and $s, \lambda \in \boldsymbol{C}$, then

(6) $$Dv^s g = \lambda v^s g$$

is equivalent to

(7) $$v^2\left(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} + \frac{\partial^2}{\partial v^2}\right)g + (2s - 1)v\frac{\partial}{\partial v}g = (\lambda - s(s - 2))g .$$

An element of $SU(2)$ is of the form $\begin{pmatrix} \alpha & -\beta \\ \bar{\beta} & \bar{\alpha} \end{pmatrix}$, $(|\alpha|^2 + |\beta|^2 = 1)$, and is decomposed as

(8) $$\begin{pmatrix} \alpha & -\beta \\ \bar{\beta} & \bar{\alpha} \end{pmatrix} = \begin{bmatrix} \exp\left(\sqrt{-1}\frac{\phi}{2}\right) & \\ & \exp\left(-\sqrt{-1}\frac{\phi}{2}\right) \end{bmatrix} \times \begin{pmatrix} |\alpha| & -|\beta| \\ |\beta| & |\alpha| \end{pmatrix} \begin{bmatrix} \exp\left(\sqrt{-1}\frac{\eta}{2}\right) & \\ & \exp\left(-\sqrt{-1}\frac{\eta}{2}\right) \end{bmatrix} ,$$

$(-\pi \leqq \phi < \pi,\ -2\pi \leqq \eta < 2\pi)$, with $\frac{1}{2}(\phi + \eta) = \arg\alpha$, $\frac{1}{2}(\phi - \eta) = \arg\beta$. Moreover, we have

(9) $$\begin{pmatrix} |\alpha| & -|\beta| \\ |\beta| & |\alpha| \end{pmatrix} = \begin{bmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix} , \qquad (0 \leqq \theta \leqq \pi) .$$

Thus, $SU(2)$ is equipped with the coordinate system (ϕ, θ, η), and, considering the operation of an element of $SU(2)$ on the tangent vector $\partial/\partial v$ at $(0, 1) \in H$, one sees at once that $\sin\theta\, d\phi\, d\theta\, d\eta$ is the Haar measure of $SU(2)$.

Next, we fix a $u_0 = (z_0, v_0) \in H$, and take $u_0' = (z_0, v_0')$ with $v_0'/v_0 = R$, so that $d(u_0, u_0') = \log R$, if $d(u, u')$ stands for the Riemannian distance between two points u, u' of H. If $\sigma_0 = \begin{pmatrix} a_0 & b_0 \\ & a_0^{-1} \end{pmatrix}$ is a fixed element of $SL(2, \boldsymbol{C})$ such that $\sigma_0 u_0 = (0, 1)$, then every u with $d(u_0, u) = R$ is of the form $u = \sigma_0^{-1}\sigma\sigma_0 u_0$, where $\sigma \in SU(1)$ and is expressed as in (8) and (9). Therefore, a coordinate system (θ, ϕ) is provided on the sphere determined by $d(u_0, u) = R$. Denote by $dA(R)$ the measure induced on the sphere by the Riemannian metric on H; then the invariance of the Riemannian structure implies that $dA(R)$ is proportional to the Haar measure of $SU(2)$, i.e., there is a constant $C_0 > 0$ such that

(10) $$dA(R) = C_0 (\log R)^2 \sin\theta\, d\theta\, d\phi .$$

Let $v(u) = v$ for $u = (z, v) \in H$; then, in the above notation, $\lim_{R\to\infty} v(\sigma_0^{-1}\sigma\sigma_0 u_0') = \infty$ or 0 according to $\theta = 0$ or $\theta \neq 0$. But, more precisely, we have

Proposition 2. *If $\theta \neq 0$, then $Rv(\sigma_0^{-1}\sigma\sigma_0 u_0')$ is monotonically increasing, and tends to $v_0(\sin\theta/2)^{-2}$ as $R \to \infty$.*

Proof. Put $\sigma_0^{-1}\sigma\sigma_0 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$; then a computation shows

$$v(\sigma_0^{-1}\sigma\sigma_0 u_0') = \frac{v_0'}{|cz_0 + d|^2 + |c|^2 v_0'^2} = \frac{1}{v_0'}\,\frac{1}{v_0'^{-2}|cz_0 + d|^2 + |c|^2} .$$

Since $v_0' = Rv_0$, $Rv(\sigma_0^{-1}\sigma\sigma_0 u_0')$ is monotonically increasing as $R \to \infty$. On the other hand, (8) and (9) imply $|c| = |a_0|^2 \sin\theta/2$. Hence $\lim_{R\to\infty} Rv(\sigma_0^{-1}\sigma\sigma_0 u_0') = v_0^{-1}|a_0|^{-4}(\sin\theta/2)^{-2} = v_0(\sin\theta/2)^{-2}$, $(\theta \neq 0)$. (q.e.d.)

If a function $g(u)$ on H satisfies $Dg = \lambda g$, $(\lambda \in C)$, then the theory of [3] shows that there exists a constant $\Lambda_\lambda(R)$ depending only on λ and R such that

$$\int_{d(u_0,u)=\log R} g(u)dA(R) = \Lambda_\lambda(R)g(u_0) ,$$

and, to determine $\Lambda_\lambda(R)$, it is enough to put $g(u) = v(u)^s$, $(s \in C)$, and determine $\Lambda_s(R)$ by

$$\int_{d(u_0,u)=\log R} v(u)^s dA(R) = \Lambda_s(R)v(u_0)^s . \tag{11}$$

Proposition 3. *If* $0 \leqq \operatorname{Re} s < 1$, *then* $\lim_{R\to\infty} (\log R)^{-2}R^s\Lambda_s(R)$ *exists, and is positive, whenever* $0 \leqq s < 1$.

Proof. It follows from (11) that

$$(\log R)^{-2}R^s\Lambda_s(R) = \int_{d(u_0,u)=\log R} (\log R)^{-2}R^s v(u)^s dA(R) ,$$

and the right hand side of this formula is, according to (10), equal to

$$C_0 \int_{-\pi}^{\pi}\int_0^{\pi} R^s v(\sigma_0^{-1}\sigma\sigma_0 u_0')^s \sin\theta \, d\theta \, d\phi .$$

Since $|R^s v(\sigma_0^{-1}\sigma\sigma_0 u_0')^s|$ is, by Proposition 2, monotonically increasing and tends to $v_0^S (\sin\theta/2)^{-2S}$, $(S = \operatorname{Re} s)$, and since

$$v_0^S C_0 \int_{-\pi}^{\pi}\int_0^{\pi} \left(\sin\frac{\theta}{2}\right)^{-2S} \sin\theta \, d\theta \, d\phi < \infty ,$$

we have

$$\lim_{R\to\infty} (\log R)^{-2}R^s\Lambda_s(R) = v_0^s C_0 \int_{-\pi}^{\pi}\int_0^{\pi} \left(\sin\frac{\theta}{2}\right)^{-2s} \sin\theta \, d\theta \, d\phi .$$

This shows at the same time that the limit is positive for $0 \leqq s < 1$. (q.e.d.)

Theorem 1. *Let* g *be a function on* H *satisfying the following three conditions*: i) g *is a solution of* (6), *i.e., of* (7), *with* $\lambda = s(s-1)$, $(0 \leqq s < 1)$. ii) g *is bounded on* H. iii) $\lim_{v\to 0} g(u) = 0$ *for almost every* $z \in C$, $(u = (z, v))$. *Then,* $g = 0$.

Proof. Consider an arbitrary point $u_0 = (z_0, v_0) \in H$. Then, in the same notation as in Proposition 2,

$$\int_{d(u_0,u)=\log R} v(u)^s g(u)dA(R) = \Lambda_s(R)v(u_0)^s g(u_0)$$

and (10) imply

$$(\log R)^{-2}R^s\Lambda_s(R)v(u_0)^s g(u_0) = C_0 \int_{-\pi}^{\pi}\int_0^{\pi} R^s v(\sigma_0^{-1}\sigma\sigma_0 u_0')^s g(\sigma_0^{-1}\sigma\sigma_0 u_0') \sin\theta \, d\theta d\phi . \tag{12}$$

By Proposition 2, $|R^s v(\sigma_0^{-1}\sigma\sigma_0 u_0')^s|$ is bounded by the product of a constant and $\left(\sin\frac{\theta}{2}\right)^{-2S}$, $(S = \operatorname{Re} s)$, and $\int_0^{\pi}\left(\sin\frac{\theta}{2}\right)^{1-2S} < \infty$. Therefore, by the assumptions ii) and iii), the right hand side of (12) tends to 0 as $R \to \infty$, so that

$$\lim_{R\to\infty} (\log R)^{-2}R^s\Lambda_s(R)v(u_0)^s g(u_0) = 0 .$$

Hence, it follows from Proposition 3 that $g(u_0) = 0$. (q.e.d.)

For $u = (z, v) \in H$, we introduce new notations $u^* = \omega u$, $\left(\omega = \begin{pmatrix} & -1 \\ 1 & \end{pmatrix}\right)$, $|u| = \sqrt{|z|^2 + v^2}$, and $tu = (tz, |t|v)$, $(t \in C)$. If $f(u)$ is a function on H, then

$$|u|^{2(n-1)/n} \int_C f(t^n u)k(tw)|t|^{2n-4} dV(t)$$

depends only on $w^n u^*$. Accordingly,

$$\int_C f(t^n u)k(tw)|t|^{2n-4} dV(t) = |u|^{-2(n-1)/n} f^*(w^n u^*)$$

defines a linear transformation $f \to f^*$, and Theorem 3 of [2] implies $f^{**} = f$.

We now propose to construct a function F on H which satisfies $F^* = F$ and has many other good properties; main tools to do this are Proposition 1 and Theorem 1.

Theorem 2. *The function* $F(u) = v^{1/n}K_{1/n}(2\pi v)e(z)$, $(u = (z, v) \in H)$, *satisfies* $F^* = F$, *and is a solution of* (6), *i.e. of* (7), *with* $s = (n-1)/n$ *and* $\lambda = s(s-2) = -(1 - n^{-2})$.

Proof. Since $\psi(v) = vK_{1/n}(2\pi v)$ is a solution of

$$\frac{d^2\psi}{dv^2} - \frac{1}{v}\frac{d\psi}{dv} - \left(4\pi^2 + \frac{\lambda}{v}\right)\psi = 0 ,$$

$F_1(u) = v^{(n-1)/n}F(u)$ is an eigenfunction of D belonging to λ.

Put next $u^* = (z^*, v^*)$; then $v/v^* = |u|^2$ gives rise to

$$(13)\qquad v^{(n-1)/n}\int_C F(t^n u)k(tw)|t|^{2n-4}\,dV(t) = v^{*(n-1)/n}F^*(w^n u^*)\ .$$

The left hand side of this formula can be written as

$$\int_C |t|^{1-n}(|t|^n v)^{(n-1)/n}F(t^n u)|t|^{2n-4}\,dV(t)\ ,$$

and D is an invariant operator. Hence, the right hand side of the same formula is, and consequently $F_1^*(u) = v^{(n-1)/n}F^*(u)$ is an eigenfunction of D belonging to λ.

Thus $g(u) = F(u) - F^*(u)$ satisfies the condition i) of Theorem 1. To show the condition ii), i.e., the boundedness of $g(u)$, we write $F^*(u)$ as

$$F^*(u) = |u|^{-2(n-1)/n}\int_C F(t^n u^*)k(t)|t|^{2n-4}\,dV(t)\ ,$$

and assume first that $v/|z|$ is bounded from above. In this case, the boundedness of $g(u)$ follows from

$$F^*(u) = \left(\sqrt{1+\frac{v^2}{|z|^2}}\,\frac{|z|}{|z|^2+v^2}\right)^{2(n-1)/n} \cdot \int_C \left(\frac{|t|^n v}{|z|^2+v^2}\right)^{1/n} K_{1/n}\left(2\pi\frac{|t|^n v}{|z|^2+v^2}\right)e\left(t^n\frac{-\bar z}{|z|^2+v^2}\right)k(t)|t|^{2n-4}\,dV(t)\ ,$$

from Proposition 1, and from the following Abel type estimation of an integral: if $\alpha(x)$ is a function defined on a real interval $[a, b]$ such that $|A(x)| \leqq M$, $\left(A(x) = \int_a^x \alpha(x)\,dx,\ x \in [a, b]\right)$, and if $\varepsilon(x)$ is real valued, differentiable and monotone on the same interval, then

$$\int_a^b \alpha(x)\varepsilon(x)\,dx = A(x)\varepsilon(x)\Big|_a^b - \int_a^b A(x)\varepsilon'(x)\,dx$$

entails

$$(14)\qquad \left|\int_a^b \alpha(x)\varepsilon(x)\,dx\right| \leqq 2M(|\varepsilon(a)| + |\varepsilon(b)|)\ .$$

In our case, $\varepsilon(x) = xK_{1/n}(2\pi(v/(|z|^2+v^2))x^n)$, $(x > 0)$. Since this function is monotonically decreasing, we may use (14) with $a = 0$ and $b = \infty$, $(\varepsilon(b) = 0)$. To prove the boundedness of $g(u)$ when $v/|z|$ is bounded from below by a positive constant, it is enough to note that

$$|F^*(u)| \leqq |u|^{-2(n-1)/n}\int_C (|t|^n v^*)^{1/n}K_{1/n}(2\pi|t|^n v^*)|t|^{2n-4}\,dV(t)$$

$$= \sqrt{1+\frac{|z|^2}{v^2}}^{\,2(n-1)/n}\int_C |t|K_{1/n}(2\pi|t|^n)\cdot|t|^{2n-4}\,dV(t)\ .$$

The condition iii) of Theorem 1 is again a consequence of Proposition 1. Hence, from Theorem 1 follows $g(u) = 0$, i.e., $F = F^*$. (q.e.d.)

When $n = 2$, $F(u)$ reduces to $\frac{1}{2}e^{-2\pi v}e(z)$.

For three special types of elements $\sigma \in G = SL(2, \boldsymbol{C})$, we define unitary operators $r_n(\sigma)$ of the Hilbert space $\mathfrak{H}_n$ in the sense of [2] as follows:

$$(15)\qquad (r_n(\sigma)\Phi)(t) = \begin{cases} |a|^{2(n-1)/n}\,\Phi(a^{2/n}t) & \sigma = \begin{pmatrix} a & \\ & a^{-1}\end{pmatrix}, \\ \Phi(t)e(bt^n) & \text{for}\quad \sigma = \begin{pmatrix} 1 & b \\ & 1\end{pmatrix}, \\ |c|^{-2(n-1)/n}\,\Phi^*(c^{-2/n}t) & \sigma = \begin{pmatrix} & -c^{-1} \\ c & \end{pmatrix}, \end{cases}$$

$(\Phi \in \mathfrak{H}_n)$. The fact that $r_n(\sigma)$ is unitary follows from Theorem 3 of [2]. If $n = 2$, then (15) coincides with (1) up to a trivial deviation. Another remarkable fact here is that, in all the three formulas of (15), $\Phi \in \mathscr{S}_n$ in the sense of [2] implies $r_n(\sigma)\Phi \in \mathscr{S}_n$. In fact, the case of the first formula is evident, and for the second formula, $\Phi \in \mathscr{S}_n$ follows from the definition of $\mathscr{S}_n$, from (2), and from the power series expansion of J_m. The case of the third formula is nothing else than Proposition 3 of [2].

Using the function $F(u)$ of Theorem 2, we put

$$\Phi_u(t) = F(t^n u) = (|t|^n v)^{1/n}K_{1/n}(2\pi|t|^n v)e(t^n z)\ ,$$

$(u = (z, v) \in H)$, and

$$(16)\qquad \Psi_u(t) = v^{(n-1)/n}\Phi_u(t)\ .$$

By the formula for the Mellin transform of $K_{1/n}$, we see that

$$\Phi_{(0,1)}(t) = |t|K_{1/n}(2\pi|t|^n) \in \mathscr{S}_n\ ,$$

and therefore $\Phi_u(t) \in \mathscr{S}_n$ for any $u \in H$.

Proposition 4. *For each of three types of σ in* (15), *we have $r_n(\sigma)\Phi_u = \Phi_{\sigma u}$.*

Proof. It is easy to verify $r_n(\sigma)\Phi_u = \Phi_{u\sigma}$ by direct computations for the first two types of σ in (15). For the third type of σ, the required formula follows from Theorem 2. (q.e.d.)

Proposition 5. *The Hilbert space $\mathfrak{H}_n$ is generated by all the Φ_u, or equivalently by all the Ψ_u, $(u \in H)$.*

Proof. Let $g(t)$ be a function in $\mathfrak{H}_n$ such that

$$\int_C g(t)\Phi_u(t)\,|t|^{2n-4}\,dV(t) = 0$$

for all u; then, we have

$$\int_C g_1(t)\Phi_{1,u}(t)\,dV(t)$$
$$= \frac{1}{n}\int_C |t|^{-(n-1)/n}\, g_1(t^{1/n})\cdot|t|^{-(n-1)/n}\,\Phi_{1,u}(t^{1/n})\,dV(t) = 0$$

with

$$g_1(t) = g(t)\,|t|^{n-2}\,, \qquad \Phi_{1,u}(t) = \Phi_u(t)\,|t|^{n-2}\,.$$

Furthermore, it follows from

$$\int_C \|t|^{-(n-1)/n}\, g_1(t^{1/n})|^2\,dV(t) = n\int_C |g_1(t)|^2\,dV(t)$$

that $|t|^{-(n-1)/n}\, g_1(t^{1/n}) = |t|^{-1/n}\, g(t^{1/n}) \in L^2(\boldsymbol{C})$. On the other hand, $|t|^{-(n-1)/n}\,\Phi_{1,u}(t^{1/n})$ $= |t|^{-1/n}\,\Phi_u(t^{1/n}) = v^{1/n}K_{1/n}(2\pi\,|t|\,v)e(tz)$ belongs to $L^2(\boldsymbol{C})$, and $K_{1/n}(2\pi\,|t|\,v) \neq 0$ for any $t \in \boldsymbol{C}$. Therefore, if $\hat{\psi}(z)$ is the Fourier transform of an arbitrary Schwartz function ψ on $\boldsymbol{C}$, then

$$0 = \int_C\int_C |t|^{-1/n}\, g(t^{1/n})\cdot|t|^{-1/n}\,\Phi_u(t^{1/n})\,dt\hat{\psi}(z)dz$$
$$= \int_C |t|^{-1/n}\, g(t^{1/n})v^{1/n}K_{1/n}(2\pi\,|t|\,v)\psi(-t)\,dV(t)\,.$$

Hence $g(t) = 0$ almost everywhere. (q.e.d.)

An arbitrary element $\sigma \in G = SL(2, \boldsymbol{C})$ is expressed by a product $\sigma_1\sigma_2\sigma_3$ of at most three elements which are of the form as considered in (1). If we put $r_n(\sigma) = r_n(\sigma_1)r_n(\sigma_2)r_n(\sigma_3)$ for $\sigma = \sigma_1\sigma_2\sigma_3$, then the above two propositions imply

Theorem 3. *The operator $r_n(\sigma)$ is well-defined, and $\sigma \to r_n(\sigma)$ is a unitary representation of $G = SL(2, \boldsymbol{C})$ on $\mathfrak{H}_n$.*

A zonal spherical function $\omega_\lambda(u)$ on H belonging to the eigenvalue $\lambda \in \boldsymbol{C}$ is defined by the following conditions: i) $\omega_\lambda(\sigma u) = \omega_\lambda(u)$ for any $\sigma \in K = SU(2)$; ii) $D\omega_\lambda = \lambda\omega_\lambda$; iii) $\omega_\lambda((0, 1)) = 1$. For every $\lambda \in \boldsymbol{C}$, there exists one and only one zonal spherical function.

Theorem 4. *The representation given by Theorem 3 is irreducible.*

Proof. Let Ψ_u be as in (16), and let dk be the Haar measure of $K = SU(2)$ such that the total measure of the group is 1. Then, there exists a function $h(t)$ of the complex variable t such that

$$\int_K r_n(k)\Psi_u(t)dk = h(t)\omega_\lambda(u)\,, \tag{17}$$

$(\lambda = -(1 - n^{-2}))$. In fact, Theorem 2 and Proposition 4 imply that the left hand side of this formula is equal to ω_λ up to a constant factor.

Define a projection P of $\mathfrak{H}_n$ by

$$P = \int_K r_n(k)dk\,,$$

and let $\mathfrak{H}'$ be the subspace of $\mathfrak{H}_n$ consisting of all functions $\Phi \in \mathfrak{H}_n$ such that $P\cdot r_n(\sigma)\Phi = 0$ for all $\sigma \in G$. Then, the orthogonal complement $\mathfrak{H}''$ of $\mathfrak{H}'$ in $\mathfrak{H}_n$ is not zero, because it follows from Proposition 4 and (17) with $u = (0, 1)$ that

$$h(t) = P\Psi_{(0,1)}(t) = \Psi_{(0,1)}(t) = |t|\,K_{1/n}(2\pi\,|t|^n)\,, \tag{18}$$

and this function ($\in \mathfrak{H}_n$) does not belong to $\mathfrak{H}'$. Let now $\Phi \neq 0$ be an arbitrary function in $\mathfrak{H}''$. Then, there exists a $\sigma \in G$ such that $P\cdot r_n(\sigma)\Phi \neq 0$. From Proposition 5 and (17), it follows that $P\cdot r_n(\sigma)\Phi$ is of the form $ch(t)$, $(c \neq 0)$. Therefore, by (18), $\mathfrak{H}''$ contains $\Psi_{(0,1)}$. On the other hand, we have by definition $r_n(\sigma)\mathfrak{H}'' \subset \mathfrak{H}''$ for all $\sigma \in G$, and hence $\mathfrak{H}''$ contains all Ψ_u, $(u \in H)$. This shows that $\mathfrak{H}'' = \mathfrak{H}_n$, and at the same time that the representation $\sigma \to r_n(\sigma)$ on $\mathfrak{H}'' = \mathfrak{H}_n$ is irreducible. (q.e.d.)

Let $\sigma \to T_\sigma$ be an irreducible unitary representation of class 1 of $G = SL(2, \boldsymbol{C})$, where T_σ means a unitary operator of a Hilbert space $\mathfrak{H}$. Then, as the general theory shows, an element $f_0 \in \mathfrak{H}$ satisfying $\|f_0\| = 1$ and $T_\sigma f_0 = f_0$ for all $\sigma \in K = SU(2)$ is uniquely determined up to a constant factor, and $(f_0, T_\sigma f_0) = \omega(\sigma) = \omega_\lambda(u)$, $(u = \sigma(0, 1) \in H)$, turns out to be a zonal spherical function. Moreover, λ determines the equivalence class of the irreducible representation, and if we express λ as $\lambda = s(s - 2)$, $(s \in \boldsymbol{C})$, then all equivalence classes of irreducible representations of G are in one to one correspondence with s satisfying either i) $\mathrm{Re}\, s = 1$, $\mathrm{Im}\, s \geqq 0$, (principal series), or ii) $1 < s \leqq 2$ (supplementary series).

Theorem 5. *The irreducible representation $\sigma \to r_n(\sigma)$ belongs to the supplementary series, and the value of the parameter s corresponding to the representation is $(n + 1)/n$.*

Proof. For the representation $\sigma \to r_n(\sigma)$ in Theorem 3, we may take $\Psi_{(0,1)}(t) = h(t)$ as f_0 (up to a constant factor), so that we have

$$c'\omega_\lambda(u) = (h(t), r_n(\sigma)h(t)) = (h(t), \Psi_u(t)) ,$$

$(c' > 0)$, and

$$Dc'\omega_\lambda(u) = -\left(1 - \frac{1}{n^2}\right)(h(t), \Psi_u(t)) = -\left(1 - \frac{1}{n^2}\right)c'\omega_\lambda(u)$$

by Theorem 2 and Proposition 4. Hence, $\lambda = -(1 - n^{-2})$, and $s = (n + 1)/n$.

References

[1] Kubota, T., A generalized Weil type representation, Technical Report TR 73-7, University of Maryland, 1973.

[2] ——On a generalized Fourier transformation, to appear in J. Fac. Sci. Univ. Tokyo, Sec. I.A., **24** (1977), 1–10.

[3] Selberg, A., Harmonic analysis and discontinuous groups in weakly symmetric Riemannian spaces with applications to Dirichlet series, Journ. Indian Math. Soc., **20** (1956), 47–87.

[4] Weil, A., Sur certain groupes d'opérateurs unitaires, Acta Math., **111** (1964), 143–211.

Department of Mathematics
Faculty of Science
Nagoya University
Chikusa-ku, Nagoya 464
Japan

ALGEBRAIC NUMBER THEORY, Papers contributed for the International Symposium, Kyoto 1976; S. Iyanaga (Ed.): Japan Society for the Promotion of Science, Tokyo, 1977

Family of Families of Abelian Varieties

MICHIO KUGA* AND SHIN-ICHIRO IHARA

§ 1. Introduction and thanks

This note is a supplement to Ichiro Satake's work on symplectic representations [3] in 1967.

Moduli-space of elliptic curves is described in terms of the upper half plane and $SL_2(Z)$. This is the first example of the happy marriages of algebraic geometries and semi-simple Lie group theories. As further examples we know that theorems of moduli of polarized abelian varieties (with additional structures), and that of K–3 surfaces are also describable in terms of symmetric domains. A big(?) problem arises naturally; i.e.: find more examples of algebraic varieties, of which moduli-spaces are quotients $\Gamma'\backslash X'$ of symmetric domains X'.

The purpose of this note is to show that the above work of Satake is actually giving some answer to this problem.

Let $V \xrightarrow{\pi} U$ be a family of abelian varieties, constructed as in [2], over a local hermitian symmetric space $U = \Gamma\backslash X = \Gamma\backslash G/K$, where G is a connected semi-simple Lie group with finite center, K is a maximal compact subgroup, $X = G/K$ is a symmetric domain, and Γ is a discrete subgroup such that $\Gamma\backslash X$ is smooth and compact. Then V and U are projective algebraic varieties, of which projective embeddings are given by "standard" Hodge metrics on them. The Hodge metric, as well as the corresponding polarization i.e. the ample divisor or the line bundle of V, is denoted by P. In this lecture we shall investigate the space U' of all "algebraic deformations" of the polarized variety (V, P), and we shall show that under the assumptions $(H), (+)$, and (I), described in § 2, with some additional assumptions on the rank of the irreducible components of X, the "moduli-space" U' of (V, P) is again a quotient $U' = \Gamma'\backslash X'$ of a symmetric domain X'.

* Supported by N.S.F.

A lecture on this topic is given at the Takagi's 100 th-birthday-conference by the first named author. But he found after that, a new result of T. Sunada [4] simplifies greatly the last part of our work, and that the essential part of our story stands on the calculations of cohomologies, which is same as ones in an still unpublished old collaboration of two authors. So he believes that this note should be published as collaboration.

Authors hope that, by further study of Sunada's results, they could remove some of our unpleasant restrictions $(+), (I)$, and/or rank conditions. And this note is only a mid-investigation report without detailed proof.

Authors thank to Professors Satake and Sunada for obvious reasons, to Professors Matsushima, Murakami, Nagano, Hotta, Kazdan, Serre, Tate, Gromov, Leahy and Sah for various reasons.

§ 2. Symplectic representations of SATAKE type

Let G be a connected semi-simple algebraic group defined over Q such that a homogeneous space $X = G/(\text{max. compact})$ is a hermitian symmetric domain with a G-invariant complex structure. The action of G on X is denoted by $\iota: G \to \mathrm{Aut}(X)$. The triple (G, X, ι) is called a C-structure.

Let F be an even dimensional vector space over Q, and B be an alternating non-degenerate bi-linear form on F. Put $N = 2m = \dim F$, and let $Sp(F, B) = \{g \in GL(F) \mid B(gx, gy) = B(x, y), {}^\forall x, {}^\forall y \in F\}$ be the symplectic group of (F, B) which is also denoted by G°. Put $X^\circ = \{J \in GL(F_R) \mid J^2 = -1, B(x, Jy) = \text{a positive definite symmetric bilinear form in } x, y \in F_R\}$, where F_R denotes $F \otimes R$. We write $B(x, Jy)$ as $S_J(x, y)$. $Sp(F, B)$ acts on X° by $g(J) = g \circ J \circ g^{-1}$. The action is sometimes denoted by $\iota^\circ: G \to \mathrm{Aut}(X)$, but usually it is abbreviated as $\iota^\circ(g) = g$. The action ι° is transitive, and the isotropy subgroup $K_J^\circ = Sp(F, B) \cap O(S_J)$ at a point $J \in X$ is a maximal compact subgroup of G°, where $O(S_J)$ is the orthogonal group of the quadratic form S_J. The center of K_J° is the one-parameter subgroup $\exp(-Jt)$ which is a circle; the orientations $t \to \exp(-Jt)$ of the circles for all $J \in X^\circ$ determine the G°-invariant complex analytic structure on X°. The C-structure $\{G^\circ, X^\circ, \iota^\circ\}$ is called the S-structure. Obviously, $G^\circ \cong Sp(m, R)$, and $X^\circ = \mathfrak{H}^m = \{Z = {}^tZ \in M(m, C) \mid \mathrm{Im}(Z) > 0\}$, the Siegel's upper-half-space. If $F = R^{2m}$, and $B = \begin{pmatrix} 0 & I_m \\ -I_m & 0 \end{pmatrix}$, an isomorphism of $\mathfrak{H}^m$ with X° is given by $Z \leftrightarrow J = \begin{pmatrix} -I & Z \\ -I & \bar{Z} \end{pmatrix}^{-1} \begin{pmatrix} iI & 0 \\ 0 & -iI \end{pmatrix} \begin{pmatrix} -I & Z \\ -I & \bar{Z} \end{pmatrix}$.

Let (G, X, ι) be a C-structure. A symplectic representation of G is a homorphism defined over Q of G into a symplectic group $Sp(F, B)$ of some (F, B). A symplectic representation ρ of G into $Sp(F, B)$ is said to have the property (H) with respect to the given C-structure (G, X, ι), if there is a holomorphic map τ of X into X°, satisfying the compatibility condition: $\rho(g)[\tau(x)] = \tau[g(x)]$ for all $x \in X$, $g \in G$. Such a map τ is called an Eichler map for ρ. The set of all Eichler maps τ for ρ is denoted by $X' = X'_\rho = X'(\rho, \iota, \iota_0)$.

Denote by $\mathfrak{g}_R$ the Lie algebra of G_R; let $\mathfrak{g}_1, \cdots, \mathfrak{g}_\nu$ be non-compact simple components of $\mathfrak{g}_R$, $\mathfrak{g}_{\nu+1}, \cdots, \mathfrak{g}_\mu$ compact simple components. Put $\mathfrak{g}_{nc} = \mathfrak{g}_1 + \cdots + \mathfrak{g}_\nu$ and $\mathfrak{g}_c = \mathfrak{g}_{\nu+1} + \cdots + \mathfrak{g}_\mu$, then $\mathfrak{g}_R = \mathfrak{g}_{nc} \oplus \mathfrak{g}_c$. The projection operators of $\mathfrak{g}_R$ to $\mathfrak{g}_{n,c}$ or to $\mathfrak{g}_c$ are denoted by proj_{nc} or proj_c respectively. A symplectic representation ρ of G is said to have the property $(+)$, if there are two subspaces W_1, W_2 of $F_C = F \otimes C$, with $F_C = W_1 \oplus W_2$, and two representations $d\rho_{nc}: \mathfrak{g}_{nc} \to \mathrm{End}(W_1)$, $d\rho_c: \mathfrak{g}_c \to \mathrm{End}(W_2)$ of the Lie subalgebras such that $d\rho = (d\rho_{nc} \circ \mathrm{proj}_{nc}) \oplus (d\rho_c \circ \mathrm{proj}_c)$, where $d\rho$ is the representation of the Lie algebra $\mathfrak{g}_R$ corresponding to ρ.

Finally, we say that ρ has the property (I), if $d\rho$ is injective and none of irreducible components of $d\rho$ is trivial.

For any C-structure (G, X, ι), Satake determined all possible (F, B) and $\rho: G \to Sp(F, B)$, which satisfy $(H), (+)$, and (I). Such representations ρ will be called hereafter symplectic representations of Satake-type. Moreover, for each ρ of Satake-type, Satake determined the set X'_ρ of all Eichler maps for ρ [3]. Following facts on ρ of Satake-type and on X'_ρ are given in [3] implicitly.

Denote by G' the centralizer of $\rho(G)$ in G°. G' operates on X'_ρ by $g'(\tau) = g' \circ \tau$ $(g' \in G', \tau \in X'_\rho)$. The action is transitive and X'_ρ is the symmetric space of the semi-simple group G'. The action is denoted by $\iota': G \to \mathrm{Aut}(X')$. The complex structure of X'_ρ is given uniquely in such a way that the map $(x, \tau) \mapsto \tau(x)$ of $X \times X'_\rho$ to X° is holomorphic. The triple (G', X'_ρ, ι') is a C-structure, and the natural inclusion $\rho': G' \to G^\circ$ is a symplectic representation of the Satake-type. Finally, for any $x \in X$, the map $\tau \mapsto \tau(x)$ of X'_ρ to X° is an Eichler map of X'_ρ.

§ 3. Algebraic deformations

Let V be a compact complex manifold, and let $L \to V$ be a linebundle of which coordinate-transformations are denoted by $\{g_{\alpha\beta}\}$. The cohomology class of 1-cocycle $\{g_{\alpha\beta}\}$ is also denoted by $L \in H^1(V, \mathcal{O}^\times)$, where $\mathcal{O}^\times$ is the invertible sheaf of V.

The tangent space of the space of all deformations of V is majorated by

$H^1(V, T(V))$, where $T(V)$ is the sheaf of germs of holomorphic vector fields on V. We simply call $H^1(V, T(V))$ the space of (infinitesimal) deformations.

We define a subspace $H^1(V, T(V))^L$ of $H^1(V, T(V))$ as follows. Take a 1-cocycle $\{\theta_{\alpha\beta}\}$ of $H^1(V, T(V))$, where $\theta_{\alpha,\beta}$ is a holomorphic vector field on the intersection $U_\alpha \cap U_\beta$ of two coordinate neighborhoods U_α and U_β. For each triple (α, β, γ) with $U_\alpha \cap U_\beta \cap U_\gamma \neq \phi$, define a holomorphic function $f_{\alpha,\beta,\gamma}$ on $U_\alpha \cap U_\beta \cap U_\gamma$ by $f_{\alpha,\beta,\gamma} = \theta_{\alpha,\beta}(d \log g_{\beta,\gamma}) = (\theta_{\alpha,\beta}, g_{\beta,\gamma}^{-1} dg_{\beta,\gamma})$, where $(\ ,\ )$ is the coupling of vector fields and differential 1-forms. Then the system $\{f_{\alpha,\beta,\gamma}\}$ is a 2-cocycle in $H^2(V, \mathcal{O})$, where $\mathcal{O}$ is the sheaf of germs of holomorphic functions on V. This process $\{\theta_{\alpha,\beta}\} \to \{f_{\alpha,\beta,\gamma}\}$ induces a linear map of $H^1(V, T(V))$ to $H^2(V, \mathcal{O})$, which we denote by $F(L): H^1(V, T(V)) \to H^2(V, \mathcal{O})$. The kernel of $F(L)$ is denoted by $H^1(V, T(V))^L$. If $W \xrightarrow{p} M$ is a holomorphic family of algebraic varieties $V_t = p^{-1}(t)$, $(t \in M)$, such that all V_t are in a same projective space $P^N(C)$. The line bundle on V defined by a hyper-plane is denoted by L. Then the Kodaira-Spencer map $\kappa_t: T_t(M) \to H^1(V_t, T(V_t))$, at any point $t \in M$, has its image $\kappa_t(T_t(M))$ in $H(V_t, T(V_t))^L$.

The mapping $F(L)$ depends only on the chern class $C = C(L) \in H^2(V, Z)$ of L. So we denote $F(L)$ by $F(C)$, and $H^1(V, T(V))^L$ by $H^1(V, T(V))^C$. Note that if $m_1 C_1 = m_2 C_2$ $(m_i \neq 0)$, then $H^1(V, T(V))^{C_1} = H^1(V, T(V))^{C_2}$. If $A = C^N/L$ is an abelian variety, the Chern class of the ample line bundle L is given by an alternating R-bilinear form B on C^N, with properties: $B(L, L) \subset Z$, $B(x, iy) = B(y, ix)$, $B(x, ix) > 0$ for $x \neq 0$. Such B is also called a polarization of A. We also denote $F(L)$ by $F(B)$, $H^1(A, T(A))^L$ by $H^1(A, T(A))^B$. Sometimes a polarization is defined as the ray $(B) = \{\lambda B: \lambda \in Q,\ \lambda > 0\}$, still $H^1(A, T(A))^B$ is well defined.

§ 4. Standard family of polarized abelian varieties

For each $J \in X^\circ$, the linear space F_R equipped with the complex (linear) structure J is a complex linear space (F_R, J), which will be denoted by E_J.

On the product $X^\circ \times F_R$, there is a unique complex analytic structure $\mathfrak{F}$, with respect to which following conditions (E1, E2, E3) are satisfied:

(E1) the projection map of $X^\circ \times F_R$ onto X° is holomorphic,

(E2) the injection maps: $u \mapsto J \times u$ of E_J into $X^\circ \times F_R$ are holomorphic for all $J \in X^\circ$,

(E3) $X^\circ \times F_R \to X^\circ$ is a complex vector bundle over X°.

We denote the vector bundle, or the complex manifold $(X^\circ \times F_R, \mathfrak{F})$ by E_{X°. For details see [2].

Take a lattice L in the Q-linear space F. Then for any $J \in X^\circ$, the complex torus $A_J = E_J/L$ is an abelian variety with the polarization B. L also acts on E_{X° as translations: $T_d: J \times u \mapsto J \times (u + d)$, $(d \in L)$. The actions T_d are biholomorphic. The quotient $L\ E_{X^\circ}$ is denoted by A_{X°, which is a fibred space over X° with the natural projection $\pi: A_{X^\circ} \to X^\circ$ whose fibres $\pi^{-1}(J)$ are abelian varieties A_J polarized by B.

Since $A_{X^\circ} = \bigcup_{J \in X^\circ} A_J$ is a family of deformations of a fibre A_J, we have the Kodaira-Spencer map $\kappa_J: \tau_J(X^\circ) \to H^1(A_J, T(A_J))$, where $T_J(X^\circ)$ is the holomorphic tangent space of X° at J. This κ_J is injective, but not surjective if $m > 1$. However, it is known that κ_J is surjective onto the subspace $H^1(A_J, T(A_J))^B$:

$$\kappa_J(T_J(X^\circ)) = H(A_J, T(A_J))^B \ . \tag{4–1}$$

Let $\mathcal{O}_J$ be the sheaf of germs of holomorphic functions on A_J. Then, we have

$$T(A_J) \cong E_J \ , \tag{4–2}$$

$$H^1(A_J, T(A_J)) \cong H^1(A_J, \mathcal{O}_J) \otimes E_J \ . \tag{4–3}$$

On the other hand, we know that $H^1(A_J, \mathcal{O}_J) \cong$ "the universal cover of the Picard variety $\hat{A}_J$" $\cong E_J$ (by means of the polarization B). So, we have

$$H^1(A_J, \mathcal{O}_J) \cong E_J \ , \tag{4–4}$$

$$H^1(A_J, T(A_J)) \cong E_J \otimes E_J \ . \tag{4–5}$$

Moreover we can show

$$H^r(A_J, \mathcal{O}_J) \cong \bigwedge^r (E_J) \ , \tag{4–6}$$

$$H^r(A_J, T(A_J)) = \bigwedge^r (E_J) \otimes E_J \ , \tag{4–7}$$

where $\bigwedge^r$ is the r-th exterior power of the vector space. These isomorphisms (4–3, 4, 5, 6, 7) depend on the polarization B.

The map $F(B): H^1(A_J, T(A_J)) \mapsto H^2(A_J, \mathcal{O}_J)$, defined in § 3, is translated into the projection map $\bigwedge^2: x \otimes y \mapsto x \wedge y$ of $E_J \otimes E_J \mapsto \bigwedge^2 (E_J)$, via isomorphisms (4–5), (4–6); i.e. we have the following diagram:

$$\begin{array}{ccc} H^1(A_J, T(A_J)) & \xrightarrow{F(B)} & H^2(A_J, \mathcal{O}_J) \\ \| & & \| \\ E_J \otimes E_J & \xrightarrow{\wedge^2} & \bigwedge^2 (E_J) \ . \end{array}$$

Therefore the kernel of $F(B)$ is isomorphic to the symmetric square $S^2(E_J)$ of E_J:

$$H^1(A_J, T(A_J))^B \cong S^2(E_J) \ . \tag{4–9}$$

Combining (4–9) with (4–1), we have the isomorphism:

$$\kappa_J : T_J(X^0) \cong S^2(E_J) \cong H^1(A_J, T(A_J))^B \ . \tag{4–10}$$

These formulas of isomorphisms (4–1), $\cdots$, (4–10), are also true in the sheave level. The projection $A_{X^\circ} \to X^\circ$ induces a map $\pi_* : T_\xi(A_{X^\circ}) \to T_x(X^\circ)$ $(x = \pi(\xi))$. A tangent vector of A_{X° is called vertical if it belongs to the kernel of π_*. The vector-sub-bundle of all the vertical tangent vectors of $T(A_{X^\circ})$ is denoted by $T^V(A_{X^\circ})$. The quotient bundle $(T/T^V)(X^\circ)$ is denoted by $T^H(A_{X^\circ})$, and called horizontal vector bundle. Let $\boldsymbol{T}(A_{X^\circ})$, $\boldsymbol{T}^V(A_{X^\circ})$, $\boldsymbol{T}^H(A_{X^\circ})$ be sheaves over A_{X° of germs of holomorphic sections of $T^V(A_{X^\circ})$, $T^H(A_{X^\circ})$ respectively. Let $\boldsymbol{E}(X^\circ)$ be the sheaf over X° of germs of holomorphic sections of $E_{X^\circ} = E(X^\circ)$; $\mathcal{O}(A_{X^\circ})$, $\mathcal{O}(X^\circ)$ the sheaves of holomorphic functions over A_{X°, X° respectively. Then, there are sheaf-isomorphisms over X°:

$$R^1\pi_*(\mathcal{O}(A_{X^\circ})) \cong \boldsymbol{E}(X^\circ) \ , \tag{4–11}$$

$$R^1\pi_*(\boldsymbol{T}^V(A_{X^\circ})) \cong (\boldsymbol{E} \otimes \boldsymbol{E})(X^\circ) \ , \tag{4–12}$$

$$R^2\pi_*(\mathcal{O}(A_{X^\circ})) \cong \bigwedge^2(\boldsymbol{E})(X^\circ) \ . \tag{4–13}$$

Also the sheaf-homomorphism $\boldsymbol{F}(\boldsymbol{B})$ of $R^1\pi_*(\boldsymbol{T}^V A_{X^\circ}))$ to $R^2\pi_*(\mathcal{O}(A_{X^\circ}))$ defined by the same cup-product map

$$\begin{aligned} F(B)_W : H^1(\pi^{-1}(W), T^V) &\longrightarrow H^2(\pi^{-1}(W), \mathcal{O}) \ , \\ \{\theta_{\alpha,\beta}\} &\longmapsto \{f_{\alpha,\beta,\tau}\} \ , \end{aligned}$$

where $f_{\alpha,\beta,\tau} = (\theta_{\alpha,\beta}, d\log g_{\beta,\tau})$, for open sets W in X°, is translated to the obvious sheaf-homomorphism $\bigwedge : \boldsymbol{E} \otimes \boldsymbol{E} \to \bigwedge^2(\boldsymbol{E})$ via the above isomorphisms (4–12, 13): i.e. the diagram

$$\begin{array}{ccc} R^1\pi_*(\boldsymbol{T}^V(A_{X^\circ})) & \xrightarrow{F(B)} & R^2\pi_*(\mathcal{O}(A_{X^\circ})) \\ \| & & \| \\ (\boldsymbol{E} \otimes \boldsymbol{E})(X^\circ) & \xrightarrow{\wedge} & \bigwedge^2(\boldsymbol{E})(X^\circ) \end{array} \tag{4–14}$$

is commutative. So, denoting the kernel of $\boldsymbol{F}(\boldsymbol{B})$ by $R^1\pi_*(\boldsymbol{T}^V(A_{X^\circ}))^B$, we have

$$R^1\pi_*(\boldsymbol{T}(A_{X^\circ}))^B = \boldsymbol{S}^2(\boldsymbol{E})(X^\circ) \ . \tag{4–15}$$

Define $Sp(L, B)$ by $Sp(L, B) = \{\gamma \in Sp(F, B) ; \gamma L = L\}$. Take a subgroup Γ° of $Sp(L, B)$ of finite index which has not a torsion element. Then $U^\circ = \Gamma^\circ \backslash X^\circ$ is a smooth manifold, which may be considered as a Zariski-open set of a projective algebraic variety.

There exists a unique holomorphic vector bundle $E^\circ \to U^\circ$, such that $E(X^\circ) \to X^\circ$ is the pull back by $X^\circ \to U^\circ$. Also, we can define the family of abelian varieties $V^\circ \to U^\circ$ over U°, as the unique one, whose pull-back is $A_{X^\circ} \to X^\circ$. Since sheaves are local objects, all formulas (4–11, $\cdots$ 15) are also true for corresponding sheaves on U°: i.e. employing obvious notations, we have

$$R^1\pi_*(\mathcal{O}(V^\circ)) = \boldsymbol{E}^\circ \ , \tag{4–16}$$

$$R^1\pi_*(\boldsymbol{T}^V(V^\circ)) = \boldsymbol{E}^\circ \otimes \boldsymbol{E}^\circ \ , \tag{4–17}$$

$$R^2\pi_*(\mathcal{O}(V^\circ)) = \bigwedge^2(\boldsymbol{E}^\circ) \ , \tag{4–18}$$

$$R^1\pi_*(\boldsymbol{T}^V(V^\circ)) = \boldsymbol{S}^2(\boldsymbol{E}^\circ) \ , \tag{4–19}$$

and

$$\begin{array}{ccccccc} 0 & \longrightarrow & R^1\pi_*(\boldsymbol{T}^V(V^\circ))^B & \longrightarrow & R^1\pi_*(\boldsymbol{T}^V(V^\circ)) & \xrightarrow{F(B)} & R^2\pi_*(\mathcal{O}(V^\circ)) \\ & & \| & & \| & & \| \\ 0 & \longrightarrow & \boldsymbol{S}^2(\boldsymbol{E}^\circ) & \longrightarrow & \boldsymbol{E}^\circ \otimes \boldsymbol{E}^\circ & \xrightarrow{\wedge} & \bigwedge^2(\boldsymbol{E}^\circ) \end{array} \tag{4–20}$$

§ 5. Family of families of abelian varieties

Let (G, X, ι) be a C-structure, $\rho : G \to G^\circ = Sp(F, B)$ a symplectic representation of Satake-type, and let $X^\circ, \iota^\circ, L, \Gamma^\circ, U^\circ, X', G'$ be same as in § 2, § 4.

Take an arithmetic discrete subgroup Γ in G, such that $\rho(\Gamma) \subset \Gamma^\circ$. We assume that Γ has no torsion element, and that $U = \Gamma \backslash X$ is compact.

For each $\tau \in X'$, the Eichler map $\tau : X \to X^\circ$ induces a holomorphic map $\tau : U \to U^\circ$, which we again denote by the same letter τ. The pull-back of the vector bundle $E^\circ \to X^\circ$ by τ is denoted by $E_\tau \xrightarrow{\pi_\tau} U$; the pull-back of the family $V^\circ \to U^\circ$ is denoted by $E_\tau \xrightarrow{\pi_\tau} U$, which is a family over U of polarized abelian varieties polarized by B. Usually we abriviate the word "polarized", and call them simply a "family of abelian varieties". Such families of abelian varieties as $V_\tau \xrightarrow{\pi_\tau} U$ obtained by that way are called "group theoretic type".

A standard polarization of the algebraic variety V_τ is described in [2]. It is given there by the Hodge-metric $ds^2 = ds_0^2 + S_{\tau(x)}(d\xi, d\eta)$, where ds_0^2 is the Hodge metric on U given by the Bergmann-metric of X, and $S_J(d\xi, d\eta)$ $(J = \tau(x))$ is the definite symmetric form $B(X, JY)$ on the vertical tangent space $T^V(V_\tau) = F_R$. This polarization of V_τ is denoted by P, or by P_B.

As same as in § 4, there are isomorphisms of sheaves over U, i.e. employing the obvious notations, we have

$$R^1\pi_*(\mathcal{O}(V_\tau)) \cong E_\tau\ , \tag{5-1}$$

$$\begin{array}{ccccc} R^1\pi_*(T^V(V_\tau))^B & \longrightarrow & R^1\pi_*(T^V(V_\tau)) & \xrightarrow{F(B)} & R^2\pi_*(\mathcal{O}(V_\tau)) \\ \| & & \| & & \| \\ S^2(E_\tau) & \longrightarrow & E_\tau \otimes E_\tau & \xrightarrow{\wedge} & \wedge^2(E_\tau)\ . \end{array} \tag{5-2}$$

Since for each $\tau \in X'$, there is a (group theoretical) family $V_\tau \xrightarrow{\pi_\tau} U$ of abelian varieties, we have a family $\{V_\tau \xrightarrow{\pi_\tau} U\}_{\tau \in X'}$ of families $V_\tau \xrightarrow{\pi_\tau} U$ of abelian varieties, parametrized by $\tau \in X'$.

Take a subgroup Γ' of $G' \cap Sp(L, B)$ of finite index. We assume that Γ' has no torsion element. For two points $\tau_1, \tau_2 \in X'$, families $V_{\tau_1} \xrightarrow{\pi_{\tau_1}} U$, $V_{\tau_2} \xrightarrow{\pi_{\tau_2}} U$ are isomorphic (as families of polarized abelian varieties), if $\tau_2 = \gamma'\tau_1$ with some $\gamma' \in \Gamma'$. Therefore, actually the quotient manifold $U' = \Gamma' \backslash X'$ does parametrize a family of families of polarized abelian varieties: $\{V_\tau \xrightarrow{\pi_\tau} U\}_{\tau \in U'}$.

Satake showed in [3] implicitly, that if $\tau_1, \tau_2 \in X'$ and τ_1 and τ_2 are very close but $\tau_1 \neq \tau_2$, then $V_{\tau_1} \xrightarrow{\pi_{\tau_1}} U$ is not isomorphic to $V_{\tau_2} \xrightarrow{\pi_{\tau_2}} U$. We call this fact as Satake's effectiveness.

We shall investigate hereafter the deformations of V_τ as a (bare) manifold, not as a family of abelian varietis. So, we consider $\{V_\tau\}_{\tau \in U'}$ or $\{V_\tau\}_{\tau \in X'}$ as a family of varieties V_τ, and consider the Kodaira-Spencer map

$$\kappa = \kappa_\tau : T_\tau(U') = T_\tau(X') \longrightarrow H^1(V_\tau, T(V_\tau))\ .$$

Since every fibre V_τ is polarized uniformly by P, we have

$$\kappa : T_\tau(U') = T_\tau(X') \longrightarrow H^1(V_\tau, T(V_\tau))^P\ . \tag{5-3}$$

Combining the Satake's effectiveness with the Adler's lemma described below, we can prove easily

Proposition 5.4. *κ_τ is injective.*

Lemma 5.5 (Allan Adler). *Let $V_1 \xrightarrow{\pi_1} U$, $V_2 \xrightarrow{\pi_2} U$ are two group theoretical families of abelian varieties over $U = \Gamma \backslash X$. Suppose that V_1 is isomorphic with V_2 as complex manifolds, and let $\psi : V_1 \to V_2$ be an isomorphism. Then there is an automorphism φ of U, such that $\varphi \circ \pi_1 = \pi_2 \circ \psi$.* [1].

(A corollary to the Adler's lemma). *Let $V \to U$ be a group theoretical family of abelian varieties, P the standard polarization of V. Then, the automorphism group of (V, P) is finite.*

§ 6. Calculation of cohomologies

In this and the next sections, we calculate $H^1(V_\tau, T(V_\tau))$ and $H^1(V_\tau, T(V_\tau))^P$. Here τ is an arbitrally fixed point of X', and remains fixed through these sections. So we abriviate suffices τ, and write as $V \xrightarrow{\pi} U$ for $V_\tau \xrightarrow{\pi_\tau} U$.

The fibre-structure $V \xrightarrow{\pi} U$ provides a spectral sequence $\{E_r^{p,q}, d\}$ with

$$E_2^{p,q} = H^p(U, R^q\pi_*(T(V)))\ , \tag{6.1}$$

and

$$\sum_{p+q=r} E_\infty^{p,q} \cong H^r(V, T(V))\ . \tag{6.2}$$

In particular, we have

$$\begin{aligned} \dim H^1(V, T(V)) &\leqq \dim E_2^{1,0} + \dim E_2^{0,1} \\ &= \dim H^1(U, R^0\pi_*(T(V)) + \dim H^0(U, R^1\pi_*(T(V)))\ . \end{aligned} \tag{6.3}$$

More precisely, reading the exact sequence of Hochschild,

$$0 \longrightarrow E_2^{1,0} \longrightarrow H^1(V, T(V)) \longrightarrow E_2^{0,1} \longrightarrow E_2^{2,0} \longrightarrow \cdots\ ,$$

we have

Proposition 6.4. *If $E_2^{1,0} = H^1(U, R^0\pi_*(T(V))) = 0$, then*

$$0 \longrightarrow H^1(V, T(V)) \xrightarrow{\mu} E_2^{0,1} = H^0(U, R^1\pi_*(T(V)))\ . \tag{6.4}$$

The injection is denoted by μ.

Proposition 6.5. *If $E_2^{1,0} = 0$ and $E_2^{2,0} = H^2(U, R^0\pi_*(T(V))) = 0$, then*

$$\mu : H^1(V, T(V)) \cong H^0(U, R^1\pi_*(T(V)))\ . \tag{6.5}$$

Now, we have

Lemma 6.6. $R^0\pi_*(T(V)) = E$.

Proof. omitted.

By the definitions of vertical and horizontal vectors, we have

$$0 \longrightarrow T^V(V) \longrightarrow T(V) \longrightarrow T^H(V) \longrightarrow 0 ,$$

and $T^H(V) =$ "the pull-back of $T(U)$ by $V \xrightarrow{\pi} U$" $= \pi^*T(U)$, where $T(U)$ is the holomorphic tangent bundle of U. Taking sections, we have

$$0 \longrightarrow \boldsymbol{T}^V(V) \longrightarrow \boldsymbol{T}(V) \longrightarrow \pi^*(\boldsymbol{T}(\boldsymbol{U})) \longrightarrow 0 .$$

Consequently, we have the long exact sequence

$$\begin{aligned} 0 &\longrightarrow A^0 \longrightarrow B^0 \longrightarrow C^0 \\ &\longrightarrow A^1 \longrightarrow B^1 \longrightarrow C^1 \\ &\longrightarrow A^2 \longrightarrow B^2 \longrightarrow C^2 \longrightarrow \cdots , \end{aligned} \tag{6.7}$$

where

$$A^i = R^i\pi_*(T^V(V)) , \quad B^i = R^i\pi_*(T(V)) , \quad C^i = R^i\pi_*(T^H(V)) . \tag{6.8}$$

Lemma 6.9. $A^i = R^i\pi_*(T^V(V)) \cong \bigwedge^i(E) \otimes E$,
$C^i = R^i\pi_*(T^H(V)) \cong \bigwedge^i(E) \otimes T(U)$.

Proof. Omitted. We need harmonic forms.

Corollary 6.10. $A^0 \cong E$, $C^0 \cong T(U)$, $A^1 \cong E \otimes E$, $C^1 \cong E \otimes T(U)$, $B^0 \cong E$.

Denote by $\bar{A}^i$ the image of A^i in B^i, $\bar{B}^i$ the image of B^i in C^i, and $\bar{C}^i$ the image of C^i in A^{i+1}. Then, we have

$$\bar{A}^0 \cong A^0 , \tag{6.11}$$

and

$$0 \longrightarrow \bar{A}^i \longrightarrow B^i \longrightarrow \bar{B}^i \longrightarrow 0 , \tag{6.12; a-i}$$

$$0 \longrightarrow \bar{B}^i \longrightarrow C^i \longrightarrow \bar{C}^i \longrightarrow 0 . \tag{6.13; b-i}$$

$$0 \longrightarrow \bar{C}^i \longrightarrow A^{i+1} \longrightarrow \bar{A}^{i+1} \longrightarrow 0 . \tag{6.14; c-i}$$

Since $A^0 \cong E$, $B^0 \cong E$, (6–12; a-0) becomes $0 \to E \to E \to \bar{B}^0 \to 0$, or

$$\bar{B}^0 = 0 . \tag{6–15; a-0}$$

Hence,

$$\bar{C}^0 \cong C^0 \cong T(U) , \quad \text{and} \tag{6–16; b-0}$$

$$0 \longrightarrow \boldsymbol{T}(\boldsymbol{U}) \longrightarrow A^1 \longrightarrow \bar{A}^1 \longrightarrow 0 . \tag{6–17; c-0}$$

The long exact sequence of (6–17; c-0) is

$$\begin{aligned} 0 &\longrightarrow H^0(T(U)) \longrightarrow H^0(A^1) \longrightarrow H^0(\bar{A}^1) \longrightarrow H^1(T(U)) \\ &\longrightarrow H^1(A^1) \longrightarrow \cdots , \end{aligned} \tag{6–18; Lc-0}$$

where $H^i(*)$ is the abriviation of $H(U, *)$.

So, we have

Lemma 6.19. *If* $H^0(U, T(U)) = 0$, $H^1(U, T(U)) = 0$, *then*

$$H^0(U, A^1) \cong H^0(U, \bar{A}^1) .$$

The long exact sequences of (6–12; a-1) and of (6–13; b-1) are

$$0 \longrightarrow H^0(\bar{A}^1) \longrightarrow H^0(B^1) \longrightarrow H^0(\bar{B}^1) \longrightarrow H^1(\bar{A}^1) \longrightarrow \cdots , \tag{6–20; La-1}$$

$$0 \longrightarrow H^0(\bar{B}^1) \longrightarrow H^0(C^1) \longrightarrow H^0(\bar{C}^1) \longrightarrow \cdots . \tag{6–21; Lb-1}$$

From these we have

Lemma 6.22. *If* $H^0(C^1) = H^0(U, E \otimes T(U)) = 0$, *then*

$$H^0(\bar{B}^1) = 0 , \quad \textit{and}$$
$$H^0(\bar{A}^1) \cong H^0(B^1) = H^0(U, R^1\pi_*T(V)) .$$

Combining Lemmas 6–19, 6–22 and Corollary 6–10, we have

Lemma 6.23. *If* $H^0(T(U)) = 0$, $H^1(T(U)) = 0$, *and* $H^0(E \otimes T(U)) = 0$, *then*

$$H^0(U, R^1\pi_*(T(V))) = H^0(U, E \otimes E) .$$

Combine this with Propositions 6–4, 6–5, then we have

Theorem 6.24. (1) *If* $H^0(U, T(U)) = 0$, $H^1(U, T(U)) = 0$, $H^1(U, E) = 0$ *and* $H^0(U, E \otimes T(U)) = 0$, *then*

$$0 \longrightarrow H^1(V, T(V)) \xrightarrow{\mu_B} H^0(U, E \otimes E) .$$

(2) *If moreover* $H^2(U, E) = 0$, *then*

$$\mu_B : H^1(V, T(V)) \cong H^0(U, E \otimes E) .$$

The injection μ_B is suffixed by B here, since the isomorphism depends on the polarization B.

The injection μ_B can be expressed in terms of harmonic forms. And from that expression, we have

Theorem 6.25. (1) *If* $H^0(U, T(U)) = 0$, $H^1(U, T(U)) = 0$, $H^1(U, E) = 0$, *and* $H^0(U, E \otimes T(U)) = 0$, *then*

$$0 \longrightarrow H^1(V, T(V))^P \longrightarrow H^0(U, S^2(E)) .$$

(2) *If moreover,* $H^2(U, E) = 0$, *then*

$$\mu_B : H^1(V, T(V))^P \cong H^0(U, S^2(E)) .$$

As for the conditions $H^0(T) = 0$, $H^1(T) = 0$, $H^1(E) = 0$, $H^0(E \otimes T) = 0$, and $H^2(E) = 0$ in Theorems 6–24, 25, we see that: $H^0(U, T(U)) = 0$ is always true, since $\mathrm{Aut}(U)$ is a finite group; $H^1(U, T(U)) = 0$ means U is rigid, and this is true if X has no component of complex dimension one; $H^1(U, E) = 0$ if X has no component of rank one; $H^2(U, E) = 0$ if X has no component of rank $\leqq 2$ by a result due to R. Hotta; $H^0(U, E \otimes T(U)) = 0$ is true if no component of X is of rank one. The last statement is proved according to the Matsushima-Murakami theory, if we note that $H^0(U, E \otimes T) \subset H^0(U, \rho \otimes Ad) = H^0(G, \rho \otimes Ad)$ and that the representation $\rho \otimes Ad$ of G does not contain a trivial component by checking case by case following to Satake's list of symplectic representations.

§ 7. Completeness of the algebraic deformation

In this section, we assume that the semi-simple algebraic group G defined over $\boldsymbol{Q}$ is connected, and that no $\boldsymbol{Q}$-simple component of G is compact; i.e. that any compact ideal of $\mathfrak{g}_{\boldsymbol{R}}$ can not be defined over $\boldsymbol{Q}$. This assumption will be called the assumption (A).

By pulling back the isomorphism $S^2(E^\circ) \cong T(U^\circ)$ of the vector bundle over U°, by $\tau : U \to U^\circ$, and by taking sections, we have the isomorphism

$$S^2(E_\tau) \cong \tau^*(T(U^\circ)) \tag{7.1}$$

of sheaves over U, and the isomorphism

$$H^0(U, S^2(E)) \cong H^0(U, \tau^*(T(U^\circ)) . \tag{7.2}$$

Sunada [4] investigated the space of sections $H^0(U, \tau^*T(U^\circ))$, and proved that all the sections are obtained in the following way. Take an element Y of the Lie algebra $\mathfrak{g}^\circ = sp(F, B)$. Since G° operates on X° holomorphically, Y defines a holomorphic vector field $Y : J \to Y(J)$ on X°, which is also denoted by the same letter Y. Pull back the vector field Y by $\tau : X \to X^\circ$, and obtain a section $\tau^*Y \in H^0(X^\circ, \tau^*T(X^\circ))$. If τ^*Y is Γ-invariant, namely if

$$Y(\tau(\gamma x)) = \gamma_* Y(\tau(x)) \tag{7.3}$$

for all $x \in X$ and for all $\gamma \in \Gamma$, then τ^*Y induces a section in $H^0(U, \tau^*T(U^\circ))$. The section is denoted by Y_U. Sunada proved that all sections in $H^0(U, \tau^*T(U^\circ))$ can be obtained in this way [4].

In our circumstances, the condition (7.3) implies $Y \in \mathfrak{g}' =$ the Lie algebra of G'. A proof of this, which we omit here, is purely group theoretic, and depends on the assumption (A).

Denote by $\mathfrak{k}'_\tau$ the Lie algebra of the isotopy subgroup K'_τ of G' at a point $\tau \in X'$, and let $\mathfrak{g}'_{\boldsymbol{R}} = \mathfrak{k}'_\tau + \mathfrak{p}'_\tau$ be the Cartan decomposition. $\mathfrak{p}'_\tau$ has the complex linear structure, and $\mathfrak{p}'_\tau \cong T_\tau(X')$. Obviously, $Y_U = 0$ for all $Y \in \mathfrak{k}'_\tau$. Therefore, the above result of Sunada is now described as

$$\begin{array}{ccc} \mathfrak{p}'_\tau & \longrightarrow H^0(U, \tau^*T(U^0)) \longrightarrow 0 . \\ \omega & \omega \\ Y & \longrightarrow Y_U \end{array} \tag{7.4}$$

Combining results in this and previous sections, we have the following inequalities under the assumtion (A) and the assumptions in the Theorem 6–25(1):

$$\begin{aligned} \dim \mathfrak{p}'_\tau &\geqq \dim H^0(U, \tau^*T(U^\circ)) && \text{(by 7–4)} \\ &\geqq \dim H(V, T(V))^P && \text{(by 6–25(1))} \\ &\geqq \dim T_\tau(X') && \text{(by 5–4)} \\ &= \dim \mathfrak{p}'_\tau . \end{aligned}$$

Hence, all the equalities should hold. Thus we have

Theorem 7.5. *If* $(G, X, \iota) \xrightarrow{\rho} (G^\circ, X^\circ, \iota^\circ)$ *is of Satake type, and* G *satisfies the assumption* (A), *and if*

$$H^1(U, T(U)) = 0 , \quad H^1(U, E) = 0 , \quad \text{and} \quad H^0(U, E \otimes T(U)) = 0 ,$$

then

$$\kappa : T(U') \cong H^1(V_\tau, T(V_\tau))^P .$$

Namely, our family $\{V_\tau\}_{\tau \in U'}$ *or* $\{V_\tau\}_{\tau \in X'}$ *are locally effective and complete as a family of deformations of polarized variety* (V_τ, P).

Corollary 7.6. *Under the assumptions in Theorem 7–5, a deformation of a total space* V *of a group-theoretical family* $V \xrightarrow{\pi} U$ *of abelian varieties* $\{\pi^{-1}(x)\}$ *is again fibred by a group theoretical family of abelian varieties.*

Corollary 7.7. *Under the assumptions that* ρ *is of Satake type and that*

G satisfies (A), if we further assume that every irreducible component of X is of rank greater than one, then the conclusions of Theorem 7.5 and of Corollary 7.6 are true.

Theorem 7.8. *If $\rho: G \to Sp(F, B)$ is of Satake-type with respect to (G, X, ι), and if the assumptions in Theorem 7.5 (or in Corollary 7.7) are true, then there exists an algebraic number field $K \subset C$ of finite degree $[K: Q] < \infty$, such that for any $\sigma \in Aut(C/K)$, $\tau \in X'$ and model of V_τ, U, π_τ, $V_\tau^\sigma \xrightarrow{\pi_\tau^\sigma} U^\sigma$ is again a group theoretical family of abelian varieties, isomorphic o one of the members of the family of families $\{V_\tau \xrightarrow{\pi_\tau} U\}_{\tau \in U'}$ of abelian varieties.*

References

[1] Adler, A., Thesis, State University of New York as Stony Brook, N. Y., 1974.
[2] Kuga, M., Fiber varieties over a symmetric space whose fibers are abelian varieties, **I, II.**, Lecture Notes, Univ. of Chicago, Chicago, 1963–64.
[3] Satake, I., Symplectic representations of algebraic groups satisfying a certain analytic condition, Acta Math., **117** (1967), 215–279.
[4] Sunada, T., Maximal family of certain holomorphic mappings, I, to appear.

Michio Kuga
Department of Mathematics
SUNY at Stony Brook
Stony Brook, New York 11790
U.S.A.

Shin-ichiro Ihara
Department of Mathematics
College of General Education
University of Tokyo
Komaba. Tokyo 153
Japan

ALGEBRAIC NUMBER THEORY, Papers contributed for the International Symposium, Kyoto 1976; S. Iyanaga (Ed.): Japan Society for the Promotion of Science, Tokyo, 1977

Examples of p-adic Arithmetic Functions

YASUO MORITA

This paper is a summary (and a reformulation) of my recent result (cf. Y. Morita [8] and [9]).

In recent years, the problem of constructing p-adic analogues of arithmetic functions has been attracting interest of many mathematicians (cf. Kubota-Leopoldt [7], Iwasawa [4], etc.). The main purpose of this paper is to make some contribution to this interesting problem.

In § 1, we shall construct a p-adic analogue of the Hurwitz-Lerch L-function $L(s; a, b, \chi)$ by applying the method of Kubota-Leopoldt [7]. In § 2, using the result of § 1, we shall construct a p-adic analogue of the Γ-function $\Gamma(z)$. In § 3, remarks and references will be given.

§ 1. L-functions of Hurwitz-Lerch

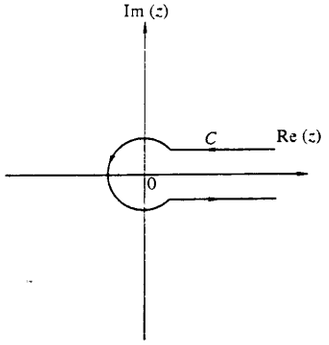
1.1. Let χ be a primitive Dirichlet character with conductor f, χ^0 the trivial character. Let a, b, s be complex numbers such that $-1 < a < \infty$, $|b| \leqq 1$, $\mathrm{Re}\,(s) > 1$. We define the Hurwitz-Lerch L-function for the character χ by

$$L(s; a, b, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n) b^n}{(a + n)^s} .$$

Then, by the standard arguments, we obtain

$$L(s; a, b, \chi) = -\frac{\Gamma(1-s)}{2\pi i} \int_C \sum_{n=1}^{f} \frac{\chi(n) b^n e^{-(a+n)z}}{1 - b^f e^{-fz}} (-z)^{s-1} dz ,$$

where $\Gamma(1-s)$ is the Γ-function, $|\arg(-z)| \leqq \pi$ and C denotes a path which encircles the positive real axis in the positive direction and separates all other singularities of the integrand from the positive real axis. Hence $L(s; a, b, \chi)$



can be extended to a meromorphic function on the entire s-plane with a possible simple pole at $s = 1$. In particular, $L(1-m; a, b, \chi)$ $(m = 1, 2, 3, \cdots)$ are well-defined.

Let

$$\sum_{n=1}^{f} \frac{\chi(n)b^n e^{-(a+n)z}}{1-b^f e^{-fz}} = \begin{cases} \sum_{m=0}^{\infty} \frac{\psi_{m,\chi}(a,b)}{m!}(-z)^m & \text{if } b^f \neq 1 \\ \psi_{-1,\chi}(a,b)(-z)^{-1} + \sum_{m=0}^{\infty} \frac{\psi_{m,\chi}(a,b)}{m!}(-z)^m & \text{if } b^f = 1 . \end{cases}$$

Then the coefficients $\psi_{m,\chi}(a, b)$ belong to $\boldsymbol{Q}(\chi)(b)[a]$ (resp. $\boldsymbol{Q}(\chi, b)[a]$) if $b^f \neq 1$ (resp. $b^f = 1$), here $\boldsymbol{Q}(\chi)$ (resp. $\boldsymbol{Q}(\chi, b)$) denotes the field that is generated over the rational number field $\boldsymbol{Q}$ by the values of χ (resp. by b and the values of χ). Furthermore, by the standard arguments, we obtain

Proposition 1. *Let m be a positive integer. Then*

$$L(1-m; a, b, \chi) = \psi_{m-1,\chi}(a, b) .$$

1.2. Let p be a prime number, $\boldsymbol{Q}_p$ the field of p-adic numbers, $\boldsymbol{C}_p$ the completion of an algebraic closure of $\boldsymbol{Q}_p$. Let $|\ |$ be the valuation of $\boldsymbol{C}_p$ such that $|p| = p^{-1}$. Put $q = 4$ if $p = 2$, and $q = p$ otherwise. Let $\omega(x)$ be the Dirichlet character with conductor q such that $\omega(x) \equiv x \bmod q$ (cf. e.g. Kubota-Leopoldt [7]). For any p-adic unit $x \in \boldsymbol{Z}_p^{\times}$, let $x = \omega(x)\langle x \rangle$.

Let a, b be elements of $\boldsymbol{C}_p$ such that $|a| \leqq |q|$ and $|b-1| < |p|^{1/(p-1)}$. Hereafter we assume $b = 1$ if χ is an integral power of ω. Put

$$\varphi_m(u; a, b) = \int_{-a}^{u} b^u (u+a)^m du$$

$$\left(\text{i.e. } b^{-a} \sum_{k=0}^{\infty} \frac{(\log b)^k}{k!} \frac{(u+a)^{m+k+1}}{m+k+1}\right)$$

for any non-negative integer m. Then we can prove (cf. Y. Morita [9], § 2)

Proposition 2. *In $\boldsymbol{C}_p$,*

$$\psi_{m,\chi}(a, b) = -\lim_{\alpha \to \infty} \frac{1}{fp^{\alpha}} \sum_{n=1}^{fp^{\alpha}} \chi(n)\varphi_m(n; a, b) .$$

1.3. Let $L^*(-m; a, b, \chi)$ be the value of $\sum_{\substack{1 \leqq n < \infty \\ (n,p)=1}} \chi(n)b^n/(a+n)^s$ at a non-positive integer $s = -m$. Since $L^*(-m; a, b, \chi) = \psi_{m,\chi}(a, b) - \chi(p)p^m \psi_{m,\chi}(a/p, b^p)$, $L^*(-m; a, b, \chi)$ belongs to $\boldsymbol{Q}(\chi)(b)[a]$ or $\boldsymbol{Q}(\chi, b)[a]$. Hence we may substitute in a and b elements of $\boldsymbol{C}_p$. Then the following theorem can be obtained from Proposition 2 (cf. Y. Morita [9], § 3).

Theorem 1. *Let the notation and assumptions be as before. Then there exists a function $L_p(s; a, b, \chi)$ with the following properties:*

(i) *$L_p(s; a, b, \chi)$ is given in $\boldsymbol{C}_p$ by*

$$L_p(s; a, b, \chi) = \delta_{\chi,b}(1-p^{-1})(s-1)^{-1} + \sum_{0 \leqq i,j,k < \infty} c_{i,j,k} a^i (\log b)^j (s-1)^k ,$$

where $c_{i,j,k} \in \boldsymbol{Q}_p(\chi)$, $\sum_{0 \leqq i,j,k < \infty} c_{i,j,k} a^i (\log b)^j (s-1)^k$ converges for $|a| \leqq |q|$, $|\log b| < |p^{1/(p-1)}|$ and $|s-1| < |q^{-1}p^{1/(p-1)}|$, $\delta_{\chi,b} = 1$ if $\chi = \chi^0$ and $b = 1$, and $\delta_{\chi,b} = 0$ otherwise.

(ii) *For any positive integer m (and for $|a| \leqq |q|$, $|b-1| < |p^{1/(p-1)}|$),*

$$L_p(1-m; a, b, \chi) = L^*(1-m; a, b, \chi\omega^{-m}) .$$

§ 2. Γ-function

Let $\Gamma(z)$ be the Γ-function. Then it is well-known that $\Gamma(z)$ satisfies the following (differential) equations over $\boldsymbol{C}$:

$(\sharp\, 1)$ $\left(\frac{d}{dz}\right)^2 \log \Gamma(z+1) = \sum_{n=1}^{\infty} \frac{1}{(n+z)^2}$;

$(\sharp\, 2)$ $\left[\frac{d}{dz} \log \Gamma(z+1)\right]_{z=0} = -\gamma$ (γ: the Euler constant);

$(\sharp\, 3)$ $[\log \Gamma(z+1)]_{z=0} = 0$.

Since $\sum_{n=1}^{\infty} 1/(n+z)^2 = L(2; z, 1, \chi^0)$ and since γ is the constant term of the Laurent expansion of $L(s; 0, 1, \chi^0)$ at $s = 1$, we define the p-adic analogues of the above equations by the following:

$(\sharp\, 1)_p$ $\left(\frac{d}{dz}\right)^2 \log \Gamma_p(z+1) = L_p(2; z, 1, \omega^{-1})$;

$(\sharp 2)_p$ $\left[\frac{d}{dz}\log\Gamma_p(z+1)\right]_{z=0} = -\gamma_p$,

where γ_p is the constant term of the Laurent expansion of $L_p(s;0,1,\chi^0)$ at $s=1$;

$(\sharp 3)_p$ $[\log\Gamma_p(z+1)]_{z=0} = 0$.

For $|z| \leqq |q|$, these equations are well-defined, and the solution is given in $\boldsymbol{C}_p$ by

$$\log\Gamma_p(z+1) = \lim_{a\to\infty}\frac{1}{p^a}\sum_{\substack{1\leqq n\leqq p^a\\(n,p)=1}}\omega(n)\langle n+z\rangle(\log\langle n+z\rangle - 1)$$
$$- \lim_{a\to\infty}\frac{1}{p^a}\sum_{\substack{1\leqq n\leqq p^a\\(n,p)=1}}\omega(n)\langle n\rangle(\log\langle n\rangle - 1)\,,$$

where $\langle n+z\rangle = \omega(n)^{-1}(n+z)$. We study this function and obtain the following theorem (for a proof see Y. Morita [8] and [9]).

Theorem 2. *There exists a function* $\log\Gamma_p(z+1)$ *with the following properties*:

(i) $\log\Gamma_p(z+1)$ *is given in* $\boldsymbol{C}_p$ *by*

$$\log\Gamma_p(z+1) = \sum_{n=0}^{\infty} a_n z^n \qquad (a_n \in \boldsymbol{Q}_p)$$

and $\sum_{n=0}^{\infty} a_n z^n$ *converges for* $|z| < 1$.(*)

(ii) $\log\Gamma_p(z+1)$ *satisfies* $(\sharp 1)_p$, $(\sharp 2)_p$ *and* $(\sharp 3)_p$ *for* $|z| \leqq |q|$.

(iii) *For any positive integer* z *that is divisible by* q,

$$\log\Gamma_p(z+1) = \sum_{\substack{1\leqq n\leqq z\\(n,p)=1}}\log\langle n\rangle\,.$$

(iv) $(d/dz)^2\log\Gamma_p(z+1)$ *can be extended to an analytic function on* $(\boldsymbol{C}_p \cup \{\infty\})\backslash\boldsymbol{Z}_p^{\times}$ *(in the terminology of Krasner* [5]*). For* $|z| > 1$, *this analytic function is given by*

$$\left(\frac{d}{dz}\right)^2\log\Gamma_p(z+1) = (1-p^{-1})\frac{1}{z}$$
$$+ \sum_{m=1}^{\infty}(-1)^m(-m)(1-p^{m-1})\zeta(1-m)\frac{1}{z^{m+1}}\,,$$

where $\zeta(s)$ *denotes the Riemann zeta function.*

(*) We obtained in [8]

$$\log\Gamma_p(z+1) = -\gamma_p z + \sum_{m\geqq 2} L_p(m;\omega^{1-m})\frac{(-z)^m}{m}.$$

(v) $(d/dz)\log\Gamma_p(z+1)$ *can not be continued outside* $\{z \in \boldsymbol{C}_p \mid |z| < 1\}$ *as an analytic function of Krasner. Hence* $\log\Gamma_p(z+1)$ *has also no analytic continuation outside* $\{z \in \boldsymbol{C}_p \mid |z| < 1\}$.(**)

§ 3. Remarks

(A) P. Cassou-Noguès and K. Hatada studied p-adic analogues of zeta functions of the form

$$\sum_{0\leqq n_i<\infty}(a + a_1 n_1 + \cdots + a_m n_m)^{-s}$$

(cf. Cassou-Noguès [2] and Hatada [3]). Furthermore, put

$$\zeta(A,x,s) = \sum_{0\leqq m_1,\cdots,m_i<\infty}\prod_{l=1}^{n}\left\{\sum_{i=1}^{i} a_{il}(x_i+m_i)\right\}^{-s}$$

(cf. Shintani [10]). Then Hatada constructed a p-adic analogue of $(\partial/\partial x_1)\cdots(\partial/\partial x_t)\zeta(A,x,s)$. But, for $n \geqq 2$, the problem of constructing a p-adic analogue of $\zeta(A,x,s)$ seems difficult.

(B) K. Shiratani studied p-adic analogues of partial zeta functions

$$\zeta(s;a,f) = \sum_{n\equiv a \bmod f}\frac{1}{n^s}$$

(cf. Shiratani [12]).

(C) Let $\chi = \chi_1\chi_2\chi_3$ be the decomposition such that the conductor of χ_1 is prime to p, χ_2 is an integral power of ω, and χ_3 depends only on $\langle\ \rangle$. Let f_0 be the conductor of $\chi_1\chi_3$, ζ a primitive f_0-th root of unity. Then, by applying the method of Amice-Fresnel [1], we can prove (cf. Y. Morita [9], § 4) that there exists an analytic function (cf. Krasner [6]) on

$$\bigcup_{1\leqq|\xi|<|q^{-1}p^{1/(p-1)}|}\left\{(s,a,b)\in(\boldsymbol{C}_p)^3 \;\middle|\; \begin{array}{l}|s| < |q^{-1}p^{1/(p-1)}\xi^{-1}|,\ |a| \leqq |q\xi|\,,\\ |b-\zeta^{\nu}| > |p^{1/(p-1)}\xi^{-1}|^{1/q}\ (1\leqq\nu\leqq f_0,\ (\nu,p)=1)\end{array}\right\}$$

that satisfies

$$L_p(1-m;a,b,\chi) = L^*(1-m;a,b,\chi\omega^{-m})$$

for any positive integer m.

(D) K. Shiratani studied the number γ_p and named it the p-adic Euler constant (cf. [11]).

(**) Though this assertion (v) is not proved in [8], it can be easily proved by showing that the coefficients of the Taylor expansion of $(d/dz)\log\Gamma_p(z+1)$ at $z=0$ are not bounded (cf. Krasner [5], p. 126).

(E) J. Diamond constructed a p-adic analogue of $\log \Gamma(z+1)$. His result is slightly different from ours (cf. [14]).

References

[1] Amice, Y. et Fresnel, J., Fonctions zèta p-adiques des corps de nombres abéliens réele, Acta Arith., 20 (1972), 353–384.

[2] Cassou-Noguès, P., Analogues p-adiques de certaines fonctions arithmétiques, Publ. Math. Bordeaux, Année, 1974–75, 1–43.

[3] Hatada, K., P-adic analytic functions and Dirichlet series (in Japanese), Master thesis (1976), University of Tokyo.

[4] Iwasawa, K., Lecture on p-adic L-functions, Annals of Math. Studies, **74**, Princeton U.P. Princeton, 1972.

[5] Krasner, M., Prolongement analytique uniforme et multiforme dans les corps valués complets, Colloque Int. C.N.R.S., **143**, Paris, 1964.

[6] ——, Rapport sur le prolongement analytique dans les corps valués complets par la methode des elements analytiques quasi-connexes, Bull. Soc. Math. France, Mémoire, **39–40** (1974), 131–254.

[7] Kubota, T. and Leopoldt, H. W., Eine p-adische Theorie der Zetawerte, I, J. reine angew. Math., **214/215** (1964), 328–339.

[8] Morita, Y., A p-adic analogue of the Γ-function, J. Fac. Sci. Univ. Tokyo, Sec. IA, **22** (1975), 255–266.

[9] ——, On the Hurwitz-Lerch L-functions, to appear in J. Fac. Sci. Univ. Tokyo, Sec. I.A.

[10] Shintani, T., On evaluation of zeta functions of totally real algebraic number fields at non positive integral places, J. Fac. Sci. Univ. Tokyo, Sec. I.A, 23 (1976), 393–417.

[11] Shiratani, K., Kummer's congruence for generalized Bernoulli numbers and its application, Mem. Fac. Sci. Kyushu Univ., **26** (1972), 119–138.

[12] ——, On a kind of p-adic zeta function, Algebraic Number Theory, Kyoto, (1976), 213–217.

[13] Whittaker, E. T. and Watson, G. N., A course of modern analysis, Cambridge U. P., London, 1902.

[14] Diamond, J., The p-adic log gamma function and p-adic Euler constants, to appear.

Department of Mathematics
Faculty of Science
Hokkaido University
Sapporo 060
Japan

ALGEBRAIC NUMBER THEORY, Papers contributed for the International Symposium, Kyoto 1976: S. Iyanaga (Ed.): Japan Society for the Promotion of Science, Tokyo, 1977

The Representation of Galois Group Attached to Certain Finite Group Schemes, and its Application to Shimura's Theory

MASAMI OHTA

In [2], Oort and Tate gave classification theorems of group schemes of prime order over certain base schemes. Especially, they classified group schemes of prime order over a normal subring of a finite algebraic number field in terms of characters of the idele class group. Raynaud [3] then gave a classification theorem of group schemes of type $(p, \cdots, p)$ satisfying certain conditions. In this paper, we first study the properties of the Galois modules associated with such group schemes over the integer ring of a local field (of characteristic zero), or over a normal subring of a finite algebraic number field. We next apply our result to the theory of Shimura [5].

§1. Let p be a fixed prime number, and r be a fixed positive integer. We put $q = p^r$, and denote by $\boldsymbol{F}_q$ the finite field with q elements. Let $\mathfrak{o}$ be an integral domain of characteristic zero, with its quotient field k. Our object is a commutative group scheme G, finite, flat and locally free of rank q over $\mathfrak{o}$, on which $\boldsymbol{F}_q$ acts unitarily as its $\mathfrak{o}$-endmorphisms (i.e. G is a "schéma en $\boldsymbol{F}_q$-vectoriels" of rank q over $\mathfrak{o}$, in the terminology of [3]). We denote by $\bar{k}$ the algebraic closure of k, and by $\mathrm{Gal}(\bar{k}/k)$ the Galois group of $\bar{k}$ over k. Then $\mathrm{Gal}(\bar{k}/k)$ acts on the one-dimensional $\boldsymbol{F}_q$-vector space $G(\bar{k})$ $\boldsymbol{F}_q$-linearly, and hence we obtain a representation ρ_G of the Galois group;

$$\rho_G : \mathrm{Gal}(\bar{k}/k) \longrightarrow \mathrm{Aut}_{\boldsymbol{F}_q}(G(\bar{k})) \cong \boldsymbol{F}_q^{\times} .$$

Since this representation is abelian, ρ_G factors through the maximal abelian quotient of $\mathrm{Gal}(\bar{k}/k)$. The purpose of this section is to study this representation in terms of class field theory.

We first assume that k is a finite extension of the p-adic number field $\boldsymbol{Q}_p$,

and that $\mathfrak{o}$ is the integer ring of k. Then for a given G as above, we obtain a representation φ_G of $k^\times$, corresponding to ρ_G by the local class field theory;

$$\varphi_G : k^\times \longrightarrow \mathrm{Aut}_{F_q}(G(\bar{k})) \cong F_q^\times .$$

We denote by $\mathfrak{p}$ (resp. κ) the maximal ideal of $\mathfrak{o}$ (resp. the residue field of $\mathfrak{o}$), and assume that κ has p^n elements. We denote by $\mathrm{ord}_\mathfrak{p}(\ )$ the normalized additive valuation of k.

Proposition 1. *Let the notation be as above, and fix an embedding of F_q into the algebraic closure of κ. Let m be the G.C.D. of n and r, and F_{p^m} be the unique subfield of F_q and κ with p^m elements. Then we have:*

$$\varphi_G(u) = N_{\kappa/F_{p^m}}(\tilde{u})^{-c} \qquad \text{for all } u \in \mathfrak{o}^\times ,$$

where $N_{\kappa/F_{p^m}}$ is the norm from κ to F_{p^m}, $\tilde{u}$ is the residue class mod $\mathfrak{p}$ *of u, and c is an integer satisfying the following condition:*

$$c\frac{q-1}{p^m-1} = \sum_{i=0}^{r-1} c_i p^i \quad \text{with } 0 \leqslant c_i \leqslant e = \mathrm{ord}_\mathfrak{p}(p) , \quad \text{and } c_i \in \boldsymbol{Z} .$$

Proof. First assume that n is divisible by r. In this case, $\mathfrak{o}$ contains all the $(q-1)$-th roots of unity in $\bar{k}$. We fix a character $\chi : F_q^\times \to \mathfrak{o}^\times$ such that the resulting homomorphism $\bar{\chi} : F_q^\times \to \kappa^\times$ is extendable to a field homomorphism. We regard F_q as a subfield of κ by means of $\bar{\chi}$. Then by [3] Corollary 1.5.1, G is $\mathfrak{o}$-isomorphic to $\mathrm{Spec}\,(\mathfrak{o}[X_1, \cdots, X_r]/\mathfrak{a})$, where $\mathfrak{a}$ is the ideal of $\mathfrak{o}[X_1, \cdots, X_r]$ generated by $X_i^p - \delta_i X_{i+1}$ $(i \in \boldsymbol{Z}/r\boldsymbol{Z}, \delta_i \in \mathfrak{o}$, and $\mathrm{ord}_\mathfrak{p}(\delta_i) \leqslant e$ for all $i)$. Here, $F_q^\times$ acts on the bialgebra by: $[\lambda]X_i = \chi(\lambda)^{p^i} X_i$ for all $\lambda \in F_q^\times$ and i. The extension of k corresponding to ρ_G is the splitting field of the equation: $X_i^q - a_i X_i = 0$ with $a_i = \delta_i^{p^{r-1}} \delta_{i+1}^{p^{r-2}} \cdots \delta_{i+r-1}$. By the explicit formula of the tame norm residue symbol, we conclude that

$$\varphi_G(t) = N_{\kappa/F_q}((-1)^{v(a_0)v(t)} a_0^{v(t)} t^{-v(a_0)} \bmod \mathfrak{p}) ,$$

for all $t \in k^\times$, where $v(\ ) = \mathrm{ord}_\mathfrak{p}(\ )$. This proves our assertion in this case.

In the general case, put $N = nr/m$, and denote by K the unramified extension of k corresponding to the residue extension F_{p^N}/F_{p^n}. Let $\mathfrak{O}$, $\mathfrak{P}$, and κ' be the integer ring of K, the maximal ideal of $\mathfrak{O}$, and the residue field of $\mathfrak{O}$, respectively. Then $G \otimes \mathfrak{O}$ over $\mathfrak{O}$ satisfies the above condition. Let χ and a_0 be as above for $G \otimes \mathfrak{O}$ over $\mathfrak{O}$, and regard F_q as a subfield of κ' by means of $\bar{\chi}$. Take $u \in \mathfrak{o}^\times$. Then there exists an element $t \in \mathfrak{O}^\times$ such that $N_{K/k}(t) = u$. By the compatibility of the canonical homomorphism: $\mathrm{Gal}\,(K_{ab}/K) \to \mathrm{Gal}\,(k_{ab}/k)$ (L_{ab} being the maximal abelian extension of L), the norm homomorphism $N_{K/k} : K^\times \to k^\times$, and the reciprocity homomorphisms for K and k, we have $\varphi_G(u) = \varphi_{G\otimes\mathfrak{O}}(t)$. Hence by the first step of the proof, we have $\varphi_G(u) = N_{\kappa'/F_q}(\tilde{t})^{-v(a_0)}$, where $v(\ ) = \mathrm{ord}_\mathfrak{P}(\ )$. Since the image of $\mathfrak{o}^\times$ by φ_G is contained in F_{p^m}, $v(a_0)$ must be divisible by $(q-1)/(p^m-1)$. Write $c = v(a_0)(p^m-1)/(q-1)$. Since K is unramified over k, we have:

$$\varphi_G(u) = N_{\kappa'/F_{p^m}}(\tilde{t})^{-c} = N_{\kappa/F_{p^m}}(\tilde{u})^{-c} .$$

Since $\mathrm{ord}_\mathfrak{P}(p) = \mathrm{ord}_\mathfrak{p}(p)$, we have the conclusion. Q.E.D.

Remark. By the proof, we have $c_i = \mathrm{ord}_\mathfrak{P}(\delta_{r-1-i})$, where δ_i's are elements of $\mathfrak{O}$ corresponding to $G \otimes \mathfrak{O}$ as in the first part of the proof. The (ordered) set $\{\mathrm{ord}_\mathfrak{P}(\delta_0), \cdots, \mathrm{ord}_\mathfrak{P}(\delta_{r-1})\}$ depends on the embedding of F_q into the algebraic closure of κ. By a change of an embedding, this set is changed by a cyclic permutation.

Next, we assume that k is a finite extension of the rational number field $\boldsymbol{Q}$, and that $\mathfrak{o}$ is a normal subring of k whose quotient field is k. For a given G over $\mathfrak{o}$ as in the beginning of this section, we obtain a representation φ_G of the idele class group C_k of k, corresponding to ρ_G by the global class field theory;

$$\varphi_G : C_k \longrightarrow \mathrm{Aut}_{F_q}(G(\bar{k})) \cong F_q^\times .$$

For a finite prime $\mathfrak{p}$ of k, we denote by $k_\mathfrak{p}$, $\mathfrak{o}_\mathfrak{p}$, and $\kappa(\mathfrak{p})$, the $\mathfrak{p}$-completion of k, the integer ring of $k_\mathfrak{p}$, and the residue field of $\mathfrak{o}_\mathfrak{p}$, respectively. For such a $\mathfrak{p}$, we denote by $\varphi_\mathfrak{p}$ the composite of φ_G and the canonical homomorphism: $k_\mathfrak{p}^\times \to C_k$. As a global reformulation of Proposition 1, we obtain the following theorem (the first assertion is proved in [2] Lemma 5).

Theorem 1. *Let the notation be as above. For a finite prime $\mathfrak{p}$ of k which corresponds to a closed point of* Spec $(\mathfrak{o})$, *we have;*

(1) $\varphi_\mathfrak{p}(\mathfrak{o}_\mathfrak{p}^\times) = \{1\}$ *if $\mathfrak{p}$ does not divide p.*

(2) *If $\mathfrak{p}$ divides p,*

$$\varphi_\mathfrak{p}(u) = N_{\kappa(\mathfrak{p})/F_{p^m}}(\tilde{u})^{-c_\mathfrak{p}} \qquad \text{for all } u \in \mathfrak{o}_\mathfrak{p}^\times ,$$

where m is the G.C.D. of $n = \mathrm{ord}_p(\#\kappa(\mathfrak{p}))$ and r, $\tilde{u}$ is the residue class mod $\mathfrak{p}$ *of u, and we are fixing an embedding of F_q into the algebraic closure of $\kappa(\mathfrak{p})$. $c_\mathfrak{p}$ is an integer which satisfies the following condition:*

$$c_\mathfrak{p}\frac{q-1}{p^m-1} = \sum_{i=0}^{r-1} c_i p^i \quad \text{with } 0 \leqslant c_i \leqslant e_\mathfrak{p} = \mathrm{ord}_\mathfrak{p}(p) \quad \text{and } c_i \in \boldsymbol{Z} .$$

Remark. If $r = 1$, this is contained in Theorem 3 of Oort, Tate [2]. There, they moreover established the one-to-one correspondence between the isomorphism classes of G's over $\mathfrak{o}$ and the system $(\varphi_G, \{c_\mathfrak{p}\}_{\mathfrak{p}|p})$'s satisfying (1) and (2).

Example. Let G be as above over the integer ring $\mathfrak{o}_k$ of k. Assume that $p\mathfrak{o}_k = \mathfrak{p}$ is a prime ideal, and that $m = (n, r) = 1$ for $\mathfrak{p}$. Then we see that $c_\mathfrak{p} = 0$ or 1 in the above notation. Hence either G or its Cartier dual is étale over $\mathfrak{o}_k$ (cf. the remark after Proposition 1 and [3] 1.5.3). If moreover the class number of k in the narrow sense is prime to $q - 1$, G must be isomorphic to either the constant scheme $(\boldsymbol{Z}/p\boldsymbol{Z})^r_{\mathfrak{o}_k}$ or its Cartier dual $(\boldsymbol{\mu}_p)^r_{\mathfrak{o}_k}$ (the product of r copies).

§2. We first recall the notation of Shimura [5]. Let N be a positive integer, and let ψ be a non-trivial quadratic character defined mod N such that $\psi(-1) = 1$. Take a cusp form $f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z}$ of weight 2 which is Neben-type of level N and with the character ψ. We assume that f belongs to the essential part, and that f is a common eigen function of all the Hecke operators. We normalize f so that $a_1 = 1$. Let K be the field generated over $\boldsymbol{Q}$ by all a_n's. K is a CM-field, and we denote by F the maximal real subfield of K. Let $\mathfrak{o}_K$ and $\mathfrak{o}_F$ be the integer rings of K and F, respectively.

There corresponds to f an abelian variety A defined over $\boldsymbol{Q}$, together with an injective homomorphism of K into $\mathrm{End}(A) \otimes \boldsymbol{Q}$. A is a factor of the jacobian variety of the modular curve associated to $\Gamma_1(N)$. By changing A with a $\boldsymbol{Q}$-isogeny, if necessary, we assume that $\mathfrak{o}_K$ acts on A as $\boldsymbol{Q}$-endomorphisms. Let k be the real quadratic field corresponding to ψ. Then $\begin{bmatrix} 0 & -1 \\ N & 0 \end{bmatrix}$ defines an automorphism η of A defined over k such that $\eta^\varepsilon = -\eta$ (ε being the generator of $\mathrm{Gal}(k/\boldsymbol{Q})$). Put $B = (1 + \eta)A$ and $B^\iota = (1 - \eta)A$. Then $\mathfrak{o}_F$ acts on B and B^ι as k-endomorphisms.

Now let $\mathfrak{b}$ be the odd part of the ideal of $\mathfrak{o}_K$ generated by $\{x \in \mathfrak{o}_K \mid x^\rho = -x\}$ (ρ being the complex conjugation), and put $N_{K/F}(\mathfrak{b}) = \mathfrak{c}$. We hereafter assume that $\mathfrak{b} \neq \mathfrak{o}_K$. Take a prime factor $\mathfrak{b}_\mathfrak{l}$ of $\mathfrak{b}$, and put $\mathfrak{l} = N_{K/F}(\mathfrak{b}_\mathfrak{l})$. Let p be the rational prime divisible by $\mathfrak{l}$, and assume that $N_{F/\boldsymbol{Q}}(\mathfrak{l}) = p^r = q$. We denote by $\mathfrak{x}_\mathfrak{l}$ the finite subgroup scheme of $\mathfrak{b}_\mathfrak{l}$-section points of A, and define the finite subgroup scheme $\mathfrak{y}_\mathfrak{l}$ (resp. $\mathfrak{z}_\mathfrak{l}$) of B (resp. B^ι) by: $\mathfrak{y}_\mathfrak{l}(\bar{k}) = B(\bar{k}) \cap \mathfrak{x}_\mathfrak{l}(\bar{k})$ (resp. $\mathfrak{z}_\mathfrak{l}(\bar{k}) = B^\iota(\bar{k}) \cap \mathfrak{x}_\mathfrak{l}(\bar{k})$). $\mathfrak{y}_\mathfrak{l}(\bar{k})$ and $\mathfrak{z}_\mathfrak{l}(\bar{k})$ are isomorphic to $\mathfrak{o}_F/\mathfrak{l}$ as $\mathfrak{o}_F$-modules. There is a natural representation of $\mathrm{Gal}(\bar{k}/k)$ on $\mathrm{Aut}_{\mathfrak{o}_F}(\mathfrak{y}_\mathfrak{l}(\bar{k})) \cong \boldsymbol{F}_q^\times$ (resp. $\mathrm{Aut}_{\mathfrak{o}_F}(\mathfrak{z}_\mathfrak{l}(\bar{k})) \cong \boldsymbol{F}_q^\times$). Shimura raised several questions and conjectures concerning this representation (see especially [5] p. 148).

In the following, we impose the following

Assumption (A). N is square free, and ψ is a primitive character defined mod N.

Under the assumption (A), there is an abelian scheme $\mathscr{B}$ (resp. $\mathscr{B}^\iota$) over the integer ring $\mathfrak{o}_k$ of k, whose general fibre is isomorphic to B (resp. B^ι) (Deligne, Rapoport [1] V.3.7). Identifying B (resp. B^ι) with $\mathscr{B} \otimes k$ (resp. $\mathscr{B}^\iota \otimes k$), we denote by $\bar{\mathfrak{y}}_\mathfrak{l}$ (resp. $\bar{\mathfrak{z}}_\mathfrak{l}$) the schemetic closure of $\mathfrak{y}_\mathfrak{l}$ (resp. $\mathfrak{z}_\mathfrak{l}$) in $\mathscr{B}$ (resp. $\mathscr{B}^\iota$). This is a commutative group scheme, finite, flat and of rank q over $\mathfrak{o}_k$, and this group scheme is naturally equipped with the structure of a "schéma on $\mathfrak{o}_F/\mathfrak{l}$-vectoriels". Therefore our Theorem 1 of § 1 applies with $G = \bar{\mathfrak{y}}_\mathfrak{l}$ or $\bar{\mathfrak{z}}_\mathfrak{l}$, and $\mathfrak{o} = \mathfrak{o}_k$. In the following, we denote by G one of $\bar{\mathfrak{y}}_\mathfrak{l}$ and $\bar{\mathfrak{z}}_\mathfrak{l}$, and use the notation of § 1 for this G. For the determination of $c_\mathfrak{p}$ with $\mathfrak{p}$ dividing p, the key point is the formula (iii) of [5] Theorem 2.3;

Lemma 1 (Shimura [5]). *Let m be a positive integer which is prime to p. Denote by $a(m)$ the idele of k, whose components at the finite primes dividing p are 1, and whose other components are all equal to m. Then under the above notation, we have*

$$\varphi_G(a(m)) = (m \bmod \mathfrak{l}) .$$

Now there are three cases to consider:

(I) $p\mathfrak{o}_k = \mathfrak{p}\mathfrak{p}'$ with two distinct prime ideals $\mathfrak{p}$ and $\mathfrak{p}'$.
(II) $p\mathfrak{o}_k = \mathfrak{p}$ is prime.
(III) $p\mathfrak{o}_k = \mathfrak{p}^2$.

Lemma 2. *In the above three cases, the possibilities of $c_\mathfrak{p}$'s for G are as follows.*

Case (I) $(c_\mathfrak{p}, c_{\mathfrak{p}'}) = (1, 0)$ or $(0, 1)$.
Case (II) *r must be even, and in this case, $c_\mathfrak{p} = 1$ or p.*
Case (III) $c_\mathfrak{p} = 1$.

Proof. Our Theorem 1 of § 1 shows that there are following possibilities in each case:

Case (I) $0 \leqq c_\mathfrak{p},\ c_{\mathfrak{p}'} \leqq 1$, and $\varphi_G(a(m)) = (m \bmod p)^{c_\mathfrak{p} + c_{\mathfrak{p}'}}$.
Case (II) When r is odd, $c_\mathfrak{p} = 0$ or 1, and $\varphi_G(a(m)) = (m \bmod p)^{2c_\mathfrak{p}}$. When r is even, $0 \leqq c_\mathfrak{p} \leqq p + 1$, and $\varphi_G(a(m)) = (m \bmod p)^{c_\mathfrak{p}}$.

Case (III) $0 \leqslant c_{\mathfrak{p}} \leqslant 2$, and $\varphi_G(a(m)) = (m \bmod p)^{e_{\mathfrak{p}}}$.

Here, m is a positive integer which is prime to p. This and Lemma 1 gives the desired conclusion. Q.E.D.

We denote by u_0 the fundamental unit of k. If $N_{k/\boldsymbol{Q}}(u_0) = 1$, we take u_0 to be totally positive.

Theorem 2. *Under the assumption* (A) *and the above notation, we have*;

(i) $N_{k/\boldsymbol{Q}}(u_0 - 1) \equiv 0 \bmod p$, *and*

(1) *If* $N_{k/\boldsymbol{Q}}(u_0) = -1$, *then* $\psi(p) = 1$, *i.e. p decomposes into two distinct prime factors in k.*

(2) *If* $N_{k/\boldsymbol{Q}}(u_0) = 1$, *and r is odd, then* $\psi(p) \neq -1$, *i.e. p does not remain prime in k.*

(ii) *In the case* (1) *of* (i), *the conductor of the class field corresponding to* ρ_G *is* $\mathfrak{p}\mathfrak{p}_\infty$, *where* $\mathfrak{p}$ *is a prime factor of* $p\mathfrak{o}_k$, *and* $\mathfrak{p}_\infty$ *is a real prime of k which satisfies the condition that* u_0 *is positive or negative at* $\mathfrak{p}_\infty$ *according as* $u_0 \equiv 1$ or $-1 \bmod \mathfrak{p}$.

Proof. Let U_+ be the subgroup of "totally positive units" of the idele group of k, i.e. $U_+ = \boldsymbol{R}_+ \times \boldsymbol{R}_+ \times \prod_{\mathfrak{q}:\text{ finite}} \mathfrak{o}_{\mathfrak{q}}^\times$. Then $U_+ \cap k^\times = E_+$ is the group of totally positive units in k. Since φ_G is the character of the idele class group of k, φ_G must be trivial on E_+. But the restriction of φ_G to U_+ is determined by the local character $\varphi_{\mathfrak{p}}$'s with $\mathfrak{p}$ dividing p. There are two cases;

(1) $N_{k/\boldsymbol{Q}}(u_0) = -1$, and hence E_+ is generated by u_0^2.

(2) $N_{k/\boldsymbol{Q}}(u_0) = 1$, and hence E_+ is generated by u_0.

Denoting by (α) the principal idele whose components are $\alpha \in k^\times$, we have by Lemma 2 and Theorem 1:

Case (I) (1) $\varphi_G((u_0^2)) = (u_0^2 \bmod \mathfrak{p})^{-1} = 1$ if $c_{\mathfrak{p}} = 1$, and $\varphi_G((u_0^2)) = (u_0^2 \bmod \mathfrak{p}')^{-1} = 1$ if $c_{\mathfrak{p}'} = 1$.

(2) $\varphi_G((u_0)) = (u_0 \bmod \mathfrak{p})^{-1} = 1$ if $c_{\mathfrak{p}} = 1$, and $\varphi_G((u_0)) = (u_0 \bmod \mathfrak{p}')^{-1} = 1$ if $c_{\mathfrak{p}'} = 1$.

Case (II) (1) $\varphi_G((u_0^2)) = (u_0^2 \bmod \mathfrak{p})^{-1}$ or $(u_0^2 \bmod \mathfrak{p})^{-p}$ and this is equal to 1.

(2) $\varphi_G((u_0)) = (u_0 \bmod \mathfrak{p})^{-1}$ or $(u_0 \bmod \mathfrak{p})^{-p}$ and this is equal to 1.

Case (III) (1) $\varphi_G((u_0^2)) = (u_0^2 \bmod \mathfrak{p})^{-1} = 1$.

(2) $\varphi_G((u_0)) = (u_0 \bmod \mathfrak{p})^{-1} = 1$.

Noting that $u_0^2 - 1 = N_{k/\boldsymbol{Q}}(u_0 - 1)/u_0^4$ when $N_{k/\boldsymbol{Q}}(u_0) = -1$, we have $N_{k/\boldsymbol{Q}}(u_0 - 1) \equiv 0 \bmod p$ in any cases. This together with Proposition A. II. 1 of [5] concludes the proof of (i).

The assertion about the finite part of the conductor in (ii) is clear from Lemma 2. The proof of the assertion about the real prime is contained in the proof of Proposition 3.2 of [5] (and follows easily from the equality $\varphi_G((u_0)) = \varphi_G((-u_0)) = 1$). Q.E.D.

Corollary 1. *Let the situation be as above, and assume that* $N_{k/\boldsymbol{Q}}(u_0) = -1$. *Assume that* $c_{\mathfrak{p}} = 0$ *and* $c_{\mathfrak{p}'} = 1$ *for G, and let* $b(\mathfrak{p})$ *be the idele of k, whose* $\mathfrak{p}$*-component is a prime element of* $\mathfrak{p}$, *and whose other components are all equal to* 1. *Then,*

$$\varphi_G(b(\mathfrak{p})) = (a_p \bmod \mathfrak{l}) ,$$

and especially a_p *is prime to* $\mathfrak{l}$.

Proof. By the above assumption, $G \otimes \mathfrak{o}_k/\mathfrak{p}$ is étale. By the congruence relation (cf. [5] (1.11)), a_p acts on the reduction mod $\mathfrak{p}$ of $A \otimes k$ as $\pi_p + \pi_p^*$, where π_p is the Frobenius endomorphism of degree p, and π_p^* is the dual of π_p. Q.E.D.

Remark. (i) In Shimura [5] p. 148 (I), it was conjectured that $N_{F/\boldsymbol{Q}}(\mathfrak{c})$ and $N_{k/\boldsymbol{Q}}(u_0 - 1)$ have the same prime factors except 2 and 3, provided that N is prime (see also the examples in [5] § 7).

(ii) The above assertion (ii) was conjectured in [5] (3.1) (when N is prime).

(iii) For the assertion of Corollary 1, cf. [5] Theorem 2.8.

We next add the following

Assumption (*B*). The class number of k in the narrow sense is prime to $q - 1$.

Since $q - 1$ is even, we see that (A) + (B) is equivalent to the following

Assumption (*C*). N is a prime number which is congruent to 1 mod 4, and the class number of $k = \boldsymbol{Q}(\sqrt{N})$ is prime to $q - 1$.

The second assertion of the following corollary is due to H. Yoshida.

Corollary 2. *Under the assumption* (C), *we have*;

(1) *The class field over k corresponding to* ρ_G *is the unique class field of degree* $p - 1$ *with the conductor* $\mathfrak{p}\mathfrak{p}_\infty$, *where* $\mathfrak{p}$ *and* $\mathfrak{p}_\infty$ *are as in* (ii) *of Theorem 2.*

(2) *Let R be the subring of* $\mathfrak{o}_K$ *generated over* $\boldsymbol{Z}$ *by all* a_n*'s such that*

n is prime to N. Then $R/R \cap \mathfrak{b}_t$ *is isomorphic to* F_p (cf. [5] p. 148 (IV)).

Proof. Since $N_{k/Q}(u_0) = -1$, the conductor of the corresponding class field is as asserted as above by Theorem 2 (ii). But the class number of the ray class mod $\mathfrak{p}\mathfrak{p}_\infty$ is equal to $h(N)(p-1)$, where $h(N)$ is the class number of $k = Q(\sqrt{N})$, hence we obtain the first assertion. We also see that the image of φ_G is contained in the prime subfield of $\mathfrak{o}_F/\mathfrak{l}$. The second assertion follows from this, Corollary 1, and [5] Theorem 2.3 (v). Q.E.D.

Remark. (i) In the above discussions, we assumed (A) in order to ensure the following

Assumption (*A'*). A has everywhere good reduction over k.

If (A') is assumed, our argument also applies to the abstract situation of Shimura [5] § 9. In fact, under the notation and assumptions (9.1)–(9.6) and (9.8) there, we have the same conclusions as above, if we replace (A) by (A'), and (C) by (A') + (B).

(ii) Similar results had been obtained by H. Yoshida under the assumption $r = 1$ (unpublished).

References

[1] Deligne, P. and Rapoport, M., Les schémas de modules de courbes elliptiques, in Modular Functions of One Variable II, 143–316, Proc. Int. Summer School, Univ. of Antwerp, RUCA, 1972, Lecture Notes in Math., Springer, **349** (1973), Berlin.

[2] Oort, F. and Tate, J., Group schemes of prime order, Ann. scient. Éc. Norm. Sup., 4e série, **3** (1970), 1–21.

[3] Raynaud, M., Schémas en groupes de type $(p,..,p)$, Bull. Soc. math. France, **102** (1974), 241–280.

[4] Shimura, G., Introduction to the arithmetic theory of automorphic functions, Publ. Math. Soc. Japan 11, Iwanami Shoten Publ. and Princeton U.P., 1971.

[5] ——, Class fields over real quadratic fields and Hecke operators, Ann. of Math.,**95** (1972), 130–190.

Department of Mathematics
Faculty of Science
Kyoto University
Kitashirakawa, Kyoto 606
Japan

ALGEBRAIC NUMBER THEORY, Papers contributed for the International Symposium, Kyoto 1976; S. Iyanaga (Ed.): Japan Society for the Promotion of Science, Tokyo, 1977

A Note on Spherical Quadratic Maps over Z

TAKASHI ONO

Since the results presented at the time of the Symposium under the title of "Hopf maps and quadratic forms over Z" will appear elsewhere, I will report a relevant (but independent) result obtained after the Symposium.

Let R^n be the euclidean space of dimension $n \geqq 1$ with the standard inner product $(x, y) = \sum x_i y_i$ and the norm $|x| = (x, x)^{1/2}$. The unit sphere S^{n-1} consists of all $x \in R^n$ with $|x| = 1$. A map $f: R^n \to R^m$ will be called *quadratic* if there exist m quadratic forms $f_1, \cdots, f_m$ on R^n such that $f(x) = (f_1(x), \cdots, f_m(x))$ for all $x \in R^n$. A map $f: R^n \to R^m$ will be called *spherical* if we have $f(S^{n-1}) \subset S^{m-1}$. We shall denote by $S_{n,m}(R)$ the set of all quadratic and spherical maps from R^n to R^m.

Maps in $S_{n,m}(R)$ can be constructed by the method of Hopf: Let $R^n = X \perp Y$, $R^m = R\varepsilon \perp V$, $\varepsilon \in S^{m-1}$, be any orthogonal decompositions of spaces into subspaces and let B be a bilinear map $X \times Y \to V$ such that $|B(x, y)| = |x||y|$, $x \in X$, $y \in Y$. Then the Hopf map $h: R^n \to R^m$ defined by

$$h(x + y) = (|x|^2 - |y|^2)\varepsilon + 2B(x, y)$$

belongs to $S_{n,m}(R)$. We shall denote by $H_{n,m}(R)$ the subset of $S_{n,m}(R)$ consisting of all Hopf maps. R. Wood has proved that every f in $S_{n,m}(R)$ is homotopic to a Hopf map h, where f and h being considered as maps from S^{n-1} to S^{m-1}. (See, R. Wood, Polynomial maps from spheres to spheres, Inventiones math. 5, 163–168 (1968), Theorem 3.)

The purpose of this paper is to prove a theorem which is a kind of Z-version of the theorem of Wood.

So, we begin with the introduction of the subset $S_{n,m}(Z)$ of $S_{n,m}(R)$. For a quadratic map $f: R^n \to R^m$, write its k-th component as

$$f_k(x) = \sum_{i,j=1}^{n} x_i x_j s_{ij}^k$$

with the symmetric matrix $s^k = (s^k_{ij}) \in \boldsymbol{R}^{\frac{1}{2}n(n+1)}$. We say that f is *integral* if $s^k \in \boldsymbol{Z}^{\frac{1}{2}n(n+1)}$ for all $k, 1 \leqq k \leqq m$. We denote by $S_{n,m}(\boldsymbol{Z})$ the subset of all integral maps in $S_{n,m}(\boldsymbol{R})$. We also put $H_{n,m}(\boldsymbol{Z}) = H_{n,m}(\boldsymbol{R}) \cap S_{n,m}(\boldsymbol{Z})$, the integral Hopf maps. What we want to prove is the following

Theorem. $S_{n,m}(\boldsymbol{Z}) = H_{n,m}(\boldsymbol{Z})$.

We first need some preliminary discussions over $\boldsymbol{R}$. Notation being as above, for a fixed pair i, j, put $s_{ij} = (s^k_{ij}) \in \boldsymbol{R}^m$. We have then

$$f(x) = \sum_{i,j=1}^{n} x_i x_j s_{ij}$$

with the symmetric "matrix" $s = (s_{ij}) \in (\boldsymbol{R}^m)^{\frac{1}{2}n(n+1)} = \boldsymbol{R}^{\frac{1}{2}mn(n+1)}$. From now on, we shall identify f with s in this way. Since the sphericality condition $f(S^{n-1}) \subset S^{m-1}$ is equivalent to the polynomial identity $|f(x)|^2 = |x|^4$, i.e. to the identity

$$\sum_{i,j,k,l} x_i x_j x_k x_l (s_{ij}, s_{kl}) = \sum_{i,j} x_i^2 x_j^2$$

one verifies easily that f belongs to $S_{n,m}(\boldsymbol{R})$ if and only if the following conditions (i)—(v) are satisfied by s:

(i) $|s_{\alpha\alpha}|^2 = 1$,

(ii) $(s_{\alpha\alpha}, s_{\alpha\beta}) = 0$,

(iii) $(s_{\alpha\alpha}, s_{\beta\beta}) + 2|s_{\alpha\beta}|^2 = 1$,

(iv) $(s_{\alpha\alpha}, s_{\beta\gamma}) + 2(s_{\alpha\beta}, s_{\alpha\gamma}) = 0$,

(v) $(s_{\alpha\beta}, s_{\gamma\delta}) + (s_{\alpha\gamma}, s_{\beta\delta}) + (s_{\alpha\delta}, s_{\beta\gamma}) = 0$,

where indices $\alpha, \beta, \gamma, \delta, 1 \leqq \alpha, \beta, \gamma, \delta \leqq n$, are all distinct. It is easy to see that, in the set of conditions (i)–(v), one can replace (iii) by the following

(iii)′ $$|s_{\alpha\alpha} - s_{\beta\beta}| = 2|s_{\alpha\beta}| .$$

From this it follows that $|s_{ij}| \leqq 1$ for all i, j and the set $S_{n,m}(\boldsymbol{R})$ becomes a compact algebraic subset of $\boldsymbol{R}^{\frac{1}{2}mn(n+1)}$. Note that the set $S_{n,m}(\boldsymbol{Z})$ is finite as being a discrete subset of $S_{n,m}(\boldsymbol{R})$.

Proof of Theorem. We only have to prove that $S_{n,m}(\boldsymbol{Z}) \subset H_{n,m}(\boldsymbol{Z})$. Take an $f \in S_{n,m}(\boldsymbol{Z})$ and let $s = (s_{ij})$ be the corresponding element in $\boldsymbol{Z}^{\frac{1}{2}mn(n+1)}$. Since $|s_{ij}| \leqq 1$ and $|s_{ij}|^2 \in \boldsymbol{Z}$, it follows from (iii)′ that $|s_{ij}|^2 = 1$ whenever $s_{ii} \neq s_{jj}$. In this case, however, we see from (iii) that $(s_{ii} + s_{jj}, s_{ii} + s_{jj}) = 2 + 2(s_{ii}, s_{jj}) = 2 + 2(-1) = 0$, and hence $s_{jj} = -s_{ii}$. In other words, we have $s_{\alpha\alpha} = \pm s_{11}$ for all $\alpha, 1 \leqq \alpha \leqq n$. Call P, Q the subset of $\{1, 2, \cdots, n\}$ defined by $P = \{\alpha, s_{\alpha\alpha} = s_{11}\}$, $Q = \{\beta, s_{\beta\beta} = -s_{11}\}$, respectively. To see that f is a Hopf map,

let $e_i = (0, \cdots, 1, \cdots, 0)$, 1 being at the i-th position, $1 \leqq i \leqq n$, and put

$$X = \sum_{\alpha \in P} \boldsymbol{R}e_\alpha , \qquad Y = \sum_{\beta \in Q} \boldsymbol{R}e_\beta .$$

Since $s_{ij} = 0$ whenever $s_{ii} \neq s_{jj}$, we have

$$\begin{aligned} f(x) &= \sum_{i,j} x_i x_j s_{ij} = \sum_i x_i^2 s_{ii} + \sum_{i \neq j} x_i x_j s_{ij} \\ &= \Big(\sum_{\alpha \in P} x_\alpha^2 - \sum_{\beta \in Q} x_\beta^2\Big) s_{11} + 2 \sum_{\alpha \in P, \beta \in Q} x_\alpha x_\beta s_{\alpha\beta} . \end{aligned}$$

Now, since we have $(s_{\alpha\beta}, s_{11}) = (s_{\alpha\beta}, s_{\alpha\alpha}) = (s_{\alpha\beta}, -s_{\beta\beta}) = 0$ by (ii), we see that $\sum_{\alpha \in P, \beta \in Q} \boldsymbol{R}s_{\alpha\beta} \subset (\boldsymbol{R}s_{11})^\perp = V$. Hence, if we call B the bilinear map $X \times Y \to V$ defined by

$$B(x, y) = \sum_{\alpha \in P, \beta \in Q} x_\alpha y_\beta s_{\alpha\beta}$$

for $x = \sum_{\alpha \in P} x_\alpha e_\alpha \in X$, $y = \sum_{\beta \in Q} y_\beta e_\beta \in Y$, and if, finally, we put $\varepsilon = s_{11} \in S^{m-1} \cap \boldsymbol{Z}^m$, then we see that $f(x + y) = (|x|^2 - |y|^2)\varepsilon + 2B(x, y)$, i.e. f is a Hopf map, q.e.d.[1]

Remark. The orthogonal groups $O_n(\boldsymbol{R})$, $O_m(\boldsymbol{R})$ act on the space $S_{n,m}(\boldsymbol{R})$ by the rule:

$$(\tau f \sigma)(x) = \tau(f(\sigma x)) , \qquad \sigma \in O_n(\boldsymbol{R}),\ \tau \in O_m(\boldsymbol{R}) .$$

The subgroups $O_n(\boldsymbol{Z})$, $O_m(\boldsymbol{Z})$ of integral matrices act then on the finite set $S_{n,m}(\boldsymbol{Z})$. Hence the quotient $O_m(\boldsymbol{Z}) \backslash S_{n,m}(\boldsymbol{Z}) / O_n(\boldsymbol{Z})$ is essential. From now on we shall use the equivalence of maps f (and corresponding matrices s) in this sense. For each $s \in S_{n,m}(\boldsymbol{Z})$, associate the subsets P, Q of the set $\{1, 2, \cdots, n\}$ as in the proof of theorem. Let p, q be the cardinalities of P, Q, respectively. We have $p \geqq 1$ since $1 \in P$. Replacing s by its suitable equivalent, we may assume that

$$s_{11} = \varepsilon = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \in \boldsymbol{R}^m$$

and that $P = \{1, 2, \cdots, p\}$, $Q = \{p + 1, \cdots, n\}$ $(p + q = n)$. If $q = 0$, s is diagonal:

1) The condition $|B(x, y)| = |x|\,|y|$ follows from the sphericality of f: $(|x|^2 + |y|^2)^2 = |x + y|^4 = |f(x + y)|^2 = (|x|^2 - |y|^2)^2 + 4|B(x, y)|^2$.

$$s = \begin{pmatrix} \varepsilon & & \\ & \varepsilon & \\ & & \ddots \\ & & & \varepsilon \end{pmatrix}$$

and the corresponding f is trivial: $f(x) = |x|^2 \varepsilon$. If $q \geqq 1$, then the symmetric matrix s takes the following form:

$$(\sharp\sharp) \qquad s = \left(\begin{array}{cccc} \varepsilon & & s_{1,p+1}, \cdots, & s_{1,n} \\ & \ddots & & \\ & \varepsilon & s_{p,p+1}, \cdots, & s_{p,n} \\ \hline & & -\varepsilon & \\ * & & & \ddots \\ & & & -\varepsilon \end{array}\right)$$

Since $s_{\alpha\alpha} = \pm s_{11}$, the conditions (ii) and (iv) imply that each row (resp. column) of the $p \times q$-matrix $(s_{\alpha\beta})$ in $(\sharp\sharp)$ forms an orthonormal q (resp. p)-frame in $\boldsymbol{R}^r = (\boldsymbol{R}\varepsilon)^{\perp}$, $r = m - 1$. Hence, when there exists a non-trivial s, one must have $p, q \leqq r$, or, equivalenly, $n - m + 1 \leqq p \leqq m - 1$.

Example. Let us apply the above Remark to the case where $n = 4$, $m = 3$. Let f be a non-trivial map in $S_{4,3}(\boldsymbol{Z})$. Hence, we must have $1 \leqq p, q \leqq 3 - 1 = 2$. Since $p + q = 4$, this is possible only when $p = 2\,(= q = r)$. As above, we can assume that s takes the form:

$$s = \begin{pmatrix} \varepsilon & 0 & s_{13} & s_{14} \\ 0 & \varepsilon & s_{23} & s_{24} \\ & * & -\varepsilon & 0 \\ & & 0 & -\varepsilon \end{pmatrix}, \qquad \varepsilon = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix},$$

where all $s_{\alpha\beta} \in S^2 \cap \boldsymbol{Z}^3$ with $(s_{13}, s_{14}) = (s_{13}, s_{23}) = (s_{23}, s_{24}) = (s_{14}, s_{24}) = 0$ and $(s_{13}, s_{24}) + (s_{14}, s_{23}) = 0$ (by (v)). Replacing s by its equivalent if necessary, we may take

$$s_{13} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \quad s_{14} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \quad s_{23} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \quad s_{24} = \begin{pmatrix} 0 \\ -1 \\ 0 \end{pmatrix}.$$

Then, we have

$$f(x) = \sum_{i,j=1}^{4} x_i x_j s_{ij} = \begin{pmatrix} x_1^2 + x_2^2 - x_3^2 - x_4^2 \\ 2(x_1 x_3 - x_2 x_4) \\ 2(x_1 x_4 + x_2 x_3) \end{pmatrix},$$

which shows that the classical Hopf fibration: $S^3 \to S^2$ is essentially the unique non-trivial map in $S_{4,3}(\boldsymbol{Z})$.

Problem. Let ν be a natural number. Denote by $S^{\nu}_{n,m}(\boldsymbol{R})$ the set of all quadratic maps $f: \boldsymbol{R}^n \to \boldsymbol{R}^m$ such that $|f(x)|^2 = \nu |x|^4$. Thus our original situation is the special case $\nu = 1$. The symmetric matrix s corresponding to $f \in S^{\nu}_{n,m}(\boldsymbol{R})$ is described by the conditions (i)–(v) where 1 in (i), (iii) is replaced by ν. Hence $S^{\nu}_{n,m}(\boldsymbol{R})$ is again a compact algebraic subset of $\boldsymbol{R}^{\frac{1}{2}mn(n+1)}$ and the integral part $S^{\nu}_{n,m}(\boldsymbol{Z})$ becomes a finite set. Call $a_{n,m}(\nu)$ its cardinality. When $n = 1$, all conditions (ii)–(v) are vacuous and so the number $a_{1,m}(\nu)$ is nothing else than the number of representations of ν as the sum of m squares. What can one say about the general sequence $a_{n,m}(\nu)$?

Department of Mathematics
The Johns Hopkins University
Baltimore, Maryland 21218
U.S.A.

ALGEBRAIC NUMBER THEORY, Papers contributed for the International Symposium, Kyoto 1976; S. Iyanaga (Ed.): Japan Society for the Promotion of Science, Tokyo, 1977

Q-forms of Symmetric Domains and Jordan Triple Systems

ICHIRO SATAKE

It is known (Koecher [7b]) that there exists a one-to-one correspondence between symmetric domains and positive definite hermitian JTS's (= Jordan triple systems). This correspondence is actually an equivalence of two categories, and to give a "cusp" (i.e., a point in the Šilov boundary) of a symmetric domain $\mathscr{D}$ amounts to giving a principal idempotent in the corresponding JTS. Combining this with the theory of Korányi-Wolf ([8], [12d]) and a more recent development on Siegel domains ([5], [4], [14], [12e, f, g], [2]), we can establish a more precise form of the equivalences between the related categories (Theorem 1). As an application, we will give a determination of $\boldsymbol{Q}$-forms of (the Lie algebra of) a symmetric domain $\mathscr{D}$ with a $\boldsymbol{Q}$-rational cusp in terms of the corresponding JTS and Jordan algebra representation.

1. We first review some known results on symmetric domains and JTS's. (The main references will be [12h] and [9b].)

We consider a symmetric domain $\mathscr{D}$ along with an "origin" $o \in \mathscr{D}$ and a cusp $o_\infty \in \partial\mathscr{D}$. As is well-known, $\mathfrak{g} = \mathrm{Lie}(\mathrm{Hol}(\mathscr{D}))$ is a real semi-simple Lie algebra of hermitian type and the stabilizer $\mathfrak{k}$ (resp. $\mathfrak{b}$) of o (resp. o_∞) in $\mathfrak{g}$ is a maximal compact (resp. maximal parabolic) subalgebra of $\mathfrak{g}$. Let $\mathfrak{g} = \mathfrak{k} + \mathfrak{p}$ be the Cartan decomposition at o and θ the corresponding Cartan involution of $\mathfrak{g}$. Then there exists a unique element Z in the center of $\mathfrak{k}$ such that $J = \mathrm{ad}_{\mathfrak{p}} Z$ $(= \mathrm{ad}\, Z|\mathfrak{p})$ is a complex structure on $\mathfrak{p}$ compatible with that on $\mathscr{D}$. On the other hand, there exists a unique element X in $\mathfrak{p}$ such that $\mathfrak{b}$ is the direct sum of the eigenspaces of $\mathrm{ad}\, X$ for eigenvalues $0, 1, 2$, which we call $\mathfrak{g}_0, V, U$, respectively. (V may reduce to $\{0\}$.) We then have $o_\infty = \lim_{\lambda\to\infty} (\exp \lambda X)o$. It is known ([8], [11], [12d]) that one has a unique decomposition

$$Z = Z_0 + \tfrac{1}{2}(e + \theta e)\,, \tag{1}$$

where $e \in U$, Z_0 is in the center of $\mathfrak{g}_0$ and one has

$$(2) \qquad [e, \theta e] = -X\ , \qquad \mathrm{ad}_U Z_0 = 0\ , \qquad \mathrm{ad}_V Z_0 = \tfrac{1}{2}I\ ,$$

where I is a complex structure on V (uniquely determined by X alone, *cf.* Lemma 2 below). Thus to give a pair (o, o_∞) amounts to giving a pair (Z, X) satisfying the above conditions, or equivalently, a (maximal) homomorphism κ of $\mathfrak{sl}(2, \boldsymbol{R})$ into $\mathfrak{g}$ (satisfying the condition (H_1)) determined by

$$\kappa\colon \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \longrightarrow e\ , \quad \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \longrightarrow -\theta e\ , \quad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \longrightarrow X\ .$$

Now let $\mathfrak{g}_C$ be the complexification of $\mathfrak{g}$ and let V_+ be that i-eigenspace of I in V_C. Then the (complex) subspace $\tilde{V} = U_C \oplus V_+$ of $\mathfrak{g}_C$ with the triple product

$$(3) \qquad \{x, y, z\} = -\tfrac{1}{2}[[x, \theta\bar{y}], z]$$

becomes a *positive definite hermitian JTS*. By definition, this means that $\{x, y, z\}$ is $\boldsymbol{C}$-linear in x, z, $\boldsymbol{C}$-antilinear in y, and satisfies the following conditions (JT1–3).

(JT1) $$\{x, y, z\} = \{z, y, x\}\ ;$$

(JT2) $$\{x_1, y_1, \{x, y, z\}\} = \{\{x_1, y_1, x\}, y, z\} - \{x, \{y_1, x_1, y\}, z\} + \{x, y, \{x_1, y_1, z\}\}$$

for all $x, y, z, x_1, y_1 \in \tilde{V}$. Following Koecher, we denote by $x \square y$ the C-linear transformation $z \mapsto \{x, y, z\}$ and define the "trace form" by $\tau(x, y) = \mathrm{tr}\,(x \square y)$. Then

(JT3) $\tau(x, y)$ is a positive definite hermitian form on $\tilde{V}$.

We note that the i-eigenspace $\mathfrak{p}_+$ of $\mathrm{ad}\,Z$ in $\mathfrak{p}_C$ with the same triple product as (3) is also a positive definite hermitian JTS, isomorphic to $\tilde{V}$, and an isomorphism $\mathfrak{p}_+ \to \tilde{V}$ is given by the "generalized Cayley transformation" ([8], [12d]).

From (2) we see that e is a "principal idempotent", i.e., one has $\{e, e, e\} = e$ and $e \square e$ is non-singular. The corresponding "Peirce decomposition" is $\tilde{V} = U_C \oplus V_+$, U_C and V_+ being the eigenspaces of $e \square e$ for eigenvalues 1 and $\frac{1}{2}$. With the product defined by

$$uu' = \{u, u', e\} = \{u, e, u'\}\ ,$$

U becomes a formally real Jordan algebra with unity e. If we denote by G_0 the (real) analytic subgroup of $\mathrm{Ad}(\mathfrak{g}_C)$ (the adjoint group of $\mathfrak{g}_C$) corresponding

to $\mathfrak{g}_0$, then the G_0-orbit Ω of e is a self-dual homogeneous open convex cone in U (with respect to the inner product $\tau | U \times U$), and one has

$$\Omega = \text{Interior } \{u^2 \mid u \in U\}$$

([2], [7a]). We put $R(u) = u \square e | V_+$ for $u \in U_C$ and

$$(4) \qquad H(v, v') = \{v, v', e\} = \frac{i}{2}[v, \bar{v}']$$

for $v, v' \in V_+$. Then $H\colon V_+ \times V_+ \to U_C$ is an (Ω-positive) hermitian map satisfying the relation

$$(5) \qquad \tau(H(v, v'), u) = \tau(v, R(u)v')\ .$$

Putting further $f = \frac{1}{2}\tau | V_+ \times V_+$, we denote by $\mathscr{H}(V_+, f)$ the Jordan algebra of hermitian transformations of V_+ with respect to the hermitian inner product f. Then it can be shown ([12e, f], [3]) that $2R$ is a (unital) Jordan algebra homomorphism of (U, e) into $\mathscr{H}(V_+, f)$ satisfying the condition

$$(6) \qquad R(H(v, v'))R(u)v = R(H(v, R(u)v'))v$$

for all $u \in U, v, v' \in V_+$. We note that, through the generalized Cayley transformation mentioned above, the symmetric domain $\mathscr{D}$ is analytically equivalent to a "Siegel domain"

$$\mathscr{D}(U, V_+, H, \Omega) = \{(u, v) \in U_C \times V_+ \mid \mathrm{Im}\, u - H(v, v) \in \Omega\}$$

(which depends only on X and not on Z), and the conditions mentioned above (i.e., the self-duality of Ω and the existence of the linear representation $2R$ satisfying (6)) are precisely the necessary and sufficient conditions for this Siegel domain to be symmetric. In particular, if $2R$ is trivial, i.e., $V_+ = \{0\}$, then $\mathscr{D}$ is equivalent to a symmetric tube domain $U + i\Omega$.

We shall now show that the Jordan algebra representation $2R\colon (U, e) \to \mathscr{H}(V_+, f)$ determines completely the structures of the JTS $\tilde{V}$ and the Lie algebra $\mathfrak{g}$. First, the Jordan triple product $\{\ \}$ can be expressed as follows:

$$(7) \qquad \begin{aligned} \{u, u', u''\} &= (u\bar{u}')u'' + u(\bar{u}'u'') - \bar{u}'(uu'')\ , \\ \{u, u', v\} &= 2R(u)R(\bar{u}')v\ , \\ \{v, v', u\} &= 2H(v, R(\bar{u})v')\ , \\ \{v, v', v''\} &= 2R(H(v, v'))v'' + 2R(H(v'', v'))v \end{aligned}$$

for all $u, u', u'' \in U_C$ and $v, v', v'' \in V_+$. The product of the form $\{u, v, u'\}$ or $\{v, u, v'\}$ vanishes identically. From (7) one obtains

$$\tau(u, u') = \mathrm{tr}_{U_C} T(u\bar{u}') + 2\,\mathrm{tr}_{V_+} R(u)R(\bar{u}') \tag{8}$$

for $u, u' \in U_C$, where we put $T(u) = u \square e \,|\, U_C$. Hence the hermitian inner product $\tau \,|\, U_C \times U_C$ is uniquely determined by the data: (U, e), $2R$, and f. Therefore, in view of (5), so is H. Thus the hermitian JTS $\tilde{V}$ (with the Peirce decomposition $U_C \oplus V_+$) is completely determined by these data. Next, identifying the underlying vector space of $\mathfrak{g}_C$ with $\tilde{V} \oplus (\tilde{V} \square \tilde{V}) \oplus \theta\bar{\tilde{V}}$ in a natural manner, we see that the Lie algebra structure of $\mathfrak{g}_C$ (with the Cartan involution $x \mapsto \theta\bar{x}$) is easily described by (3). The complex conjugation of $\mathfrak{g}_C$ with respect to $\mathfrak{g}$ is given by

$$\begin{cases} \bar{u} = \{e, u, e\} & \text{for } u \in U_C\,, \\ \bar{v} = 2i\, e \square v & \text{for } v \in V_+\,. \end{cases} \tag{9}$$

Thus the real form $\mathfrak{g}$ (with the gradation $U + V + \mathfrak{g}_0 + \theta V + \theta U$ and the Cartan involution θ) is also determined.

Conversely, starting from any formally real Jordan algebra (U, e) and any linear representation $2R: (U, e) \to \mathscr{H}(V_+, f)$ satisfying (6) and using the above formulas as definitions, one can construct a positive definite hermitian JTS $\tilde{V}$ with a principal idempotent e and then a semi-simple Lie algebra of hermitian type $\mathfrak{g}$ (with Z and X). Moreover these constructions are all functorial. In this way, we obtain the following

Theorem 1. *The categories of the following objects with morphisms defined in a suitable manner are equivalent to one another*:

(a) $(\mathscr{D}, o, o_\infty)$ (*symmetric domains with origins and cusps*),

(b) $(\mathfrak{g}, Z, X)$ (*semi-simple Lie algebras of hermitian type with maximal homomorphisms from* $\mathfrak{sl}(2, \boldsymbol{R})$ *satisfying* (H_1)),

(c) $(U_C \oplus V_+, e)$ (*positive definite hermitian JTS's with principal idempotents*),

(d) $(U, e) \xrightarrow{2R} \mathscr{H}(V_+, f)$ (*formally real Jordan algebras with linear representations satisfying* (6)).

For a more precise statement and a proof, see [12h]. The linear representations of formally real Jordan algebras (satisfying (6)) are completely determined in [14] and [12c, f].

2. We give some lemmas relevant to our considerations.

Lemma 1. *When Z is given in the form* (1), *the corresponding Cartan involution θ is given by*

$$\theta = \begin{cases} 1 + \mathrm{ad}\, e \cdot \mathrm{ad}\, \theta e & \text{on } \mathfrak{g}_0 \\ \mathrm{ad}\, \theta e \cdot I & \text{on } V \\ \frac{1}{2}(\mathrm{ad}\, e)^2 & \text{on } U\,. \end{cases} \tag{10}$$

This formula can be derived by a straightforward computation of $\theta = \exp(\pi\, \mathrm{ad}\, Z) = \exp(\pi\, \mathrm{ad}\, Z_0) \cdot \exp((\pi/2)(e + \theta e))$. *Cf.* also [5], [11], [12e].

Lemma 2. *Let Z' be another element in $\mathfrak{g}$ satisfying the same condition as Z with respect to X. Then Z' can be written in the form*

$$Z' = Z_0 + \tfrac{1}{2}(a + \theta a^{-1})\,, \tag{11}$$

where $a \in \Omega$ and a^{-1} is the "inverse" of a in the Jordan algebra (U, e) (i.e., the unique element in U such that $\{a, a^{-1}, a\} = a$).

Proof. Since $\mathrm{Ad}\, \mathfrak{g}$ (= the identity connected component of $\mathrm{Aut}\, \mathfrak{g}$) is transitive on the set of all possible pairs (Z, X) satisfying the conditions mentioned in **1**, there exists $g_1 \in \mathrm{Ad}\, \mathfrak{g}$ such that $g_1 Z = Z'$ and $g_1 X = X$. Put $G_0' = \{g \in \mathrm{Aut}\, \mathfrak{g} \,|\, gX = X\}$. Then, since G_0' is an algebraic subgroup of $\mathrm{Aut}\, \mathfrak{g}$ with Lie algebra $\mathfrak{g}_0$ and is stable under θ, it admits a global Cartan decomposition induced by θ. Hence one has $g_1 = \exp x_1 \cdot k_1$ with $x_1 \in \mathfrak{p}_0$, $k_1 \in K$, where $\mathfrak{p}_0 = \mathfrak{p} \cap \mathfrak{g}_0$ and K is the analytic subgroup of $\mathrm{Ad}\, \mathfrak{g}$ corresponding to $\mathfrak{k}$. Therefore, from (1), one has

$$\begin{aligned} Z' &= (\exp x_1)Z = (\exp x_1)(Z_0 + \tfrac{1}{2}(e + \theta e)) \\ &= Z_0 + \tfrac{1}{2}((\exp x_1)e + \theta(\exp(-x_1))e)\,. \end{aligned}$$

In general, we put

$$P(x)y = \{x, \bar{y}, x\} = \tfrac{1}{2}(\mathrm{ad}\, x)^2 \theta y$$

for $x, y \in U_C$. Then it is clear that

$$P((\exp x_1)x) = (\exp x_1)P(x)(\exp x_1) \qquad \text{on } U_C\,.$$

In particular, putting $x = e$ and $a = (\exp x_1)e$, one has $P(a) = (\exp x_1)^2$ on U_C. Therefore $P(a)$ is non-singular, and one has $a^{-1} = P(a)^{-1}a = \exp(-x_1)e$, q.e.d.

Lemma 2 shows that for a fixed X the set of all possible Z is parametrized by $\Omega = G_0 e$. We write Z_a for Z' given by (11) and θ_a for the corresponding Cartan involution. Then, comparing (1) and (11), one has

$$\theta_a a = \theta a^{-1}\,. \tag{12}$$

We denote by $\{\ \}_a$ the corresponding Jordan triple product, i.e.,

$$\{x, y, z\}_a = -\tfrac{1}{2}[[x, \theta_a \bar{y}], z] \qquad (x, y, z \in \tilde{V}) \ . \tag{13}$$

Lemma 3. *One has*

$$\{x, y, z\}_a = \{x, P(a^{-1})u + 2R(a^{-1})v, z\} \ , \tag{14}$$

where $y = u + v$ *and* $u \in U_C$, $v \in V_+$.

Proof. It is enough to prove that

$$\theta\theta_a(u + v) = P(a^{-1})u + 2R(a^{-1})v \ .$$

For $u \in U_C$, one obtains by (10), (12), (JT2) and (7)

$$\begin{aligned}
\theta\theta_a u &= \tfrac{1}{4}[e, [e, [\theta a^{-1}, [\theta a^{-1}, u]]]] \\
&= \tfrac{1}{4}[e, [[e, \theta a^{-1}], [\theta a^{-1}, u]] + [\theta a^{-1}, [e, [\theta a^{-1}, u]]]] \\
&= [e, -[e \,\square\, a^{-1}, u \,\square\, a^{-1}] - \{u, a^{-1}, e\} \,\square\, a^{-1}] \\
&= [e, -\{e, a^{-1}, u\} \,\square\, a^{-1} + u \,\square\, \{a^{-1}, e, a^{-1}\} - (ua^{-1}) \,\square\, a^{-1}] \\
&= 2a^{-1}(a^{-1}u) - a^{-2}u = P(a^{-1})u \ .
\end{aligned}$$

Similarly, for $v \in V_+$, one has

$$\theta\theta_a v = -[e, [\theta a^{-1}, v]] = 2\{v, a^{-1}, e\} = 2R(a^{-1})v \ , \qquad \text{q.e.d.}$$

We denote the Jordan product in U, the representation $2R$, and the hermitian form f relative to the triple product $\{\ \}_a$ by $u \underset{a}{\cdot} u'$, $2R_a$, and f_a, respectively. Then by (14) and (7) one has

$$\begin{cases} u \underset{a}{\cdot} u' = \{u, a^{-1}, u'\} \ , \\ R_a(u)v = 2R(u)R(a^{-1})v \ , \\ f_a(v, v') = f(v, 2R(a^{-1})v') \ . \end{cases} \tag{15}$$

We say that the hermitian Jordan triple product $\{\ \}_a$ (and $\underset{a}{\cdot}$, $2R_a$, f_a) are obtained from $\{\ \}$ (and $\cdot$, $2R$, f) by a "mutation" by a^{-1} (*cf.* [2], [7a]).

3. Let F be a subfield of $\boldsymbol{R}$. An "F-form" of $\mathfrak{g}$ is a Lie algebra $\mathfrak{g}_F$ over F such that $\mathfrak{g} = \mathfrak{g}_F \otimes_F \boldsymbol{R}$. When an F-form is given, we put $W_F = W \cap \mathfrak{g}_F$ for any subspace W of $\mathfrak{g}$; W is called "defined over F" if one has $W = W_F \otimes_F \boldsymbol{R}$. An origin o (resp. cusp o_∞) is called "F-rational" if the corresponding $\mathfrak{k}$ (resp. $\mathfrak{b}$) is defined over F, or equivalently, if θ is F-rational (i.e., θ leaves $\mathfrak{g}_F$ stable). By an *F-structure* on an object $(\mathscr{D}, o, o_\infty)$ in the category (a) we mean an F-form $\mathfrak{g}_F$ of $\mathfrak{g}$ such that o and o_∞ are F-rational. For brevity, an object endowed with an F-structure will be called an *F-object*. We note that for an F-object

the corresponding X is always F-rational (i.e., $X \in \mathfrak{g}_F$). In fact, since $\mathfrak{b}$ is defined over F, so are $U + V$ and U. ($U + V$ is the unipotent radical of $\mathfrak{b}$, and U is the center of $U + V$.) Moreover, since θ is F-rational, $\mathfrak{g}_0 = \mathfrak{b} \cap \theta\mathfrak{b}$ is defined over F. Hence V, which is the intersection with $\mathfrak{b}$ of the orthogonal complement of $U + \mathfrak{g}_0 + \theta U$ with respect to the Killing form, is also defined over F. Thus the gradation

$$\mathfrak{g} = U + V + \mathfrak{g}_0 + \theta V + \theta U$$

is defined over F. Therefore, X is F-rational, since X is the unique element in $\mathfrak{g}$ such that the eigenspace decomposition of $\mathfrak{g}$ with respect to $\operatorname{ad} X$ for eigenvalues $2, 1, 0, -1, -2$ coincides with this gradation.

Now we want to determine all $\boldsymbol{Q}$-objects in the category (a). Clearly it is sufficient to determine "$\boldsymbol{Q}$-simple" $\boldsymbol{Q}$-objects, i.e., those for which $\mathfrak{g}_{\boldsymbol{Q}}$ is $\boldsymbol{Q}$-simple. Let $\mathfrak{g}^{(i)}$ $(1 \leqslant i \leqslant d)$ be the simple factors of $\mathfrak{g}$ and let $\pi_i : \mathfrak{g} \to \mathfrak{g}^{(i)}$ be the canonical projection. Then, as is well-known, a $\boldsymbol{Q}$-form $\mathfrak{g}_{\boldsymbol{Q}}$ of $\mathfrak{g}$ is $\boldsymbol{Q}$-simple if and only if there exists a (uniquely determined) totally real number field F of degree d such that $\mathfrak{g}^{(1)}$ is defined over F and that π_1 induces an isomorphism $\mathfrak{g}_{\boldsymbol{Q}} \cong \mathfrak{g}_F^{(1)}$ (as Lie algebra over $\boldsymbol{Q}$). (This situation is expressed as $\mathfrak{g} = R_{F/\boldsymbol{Q}}(\mathfrak{g}^{(1)})$ in Weil's notation.) If we denote by $\{\sigma_1, \cdots, \sigma_d\}$ ($\sigma_1 = \mathrm{id}$) the set of injections of F into $\boldsymbol{R}$ arranged in a suitable order, then we have $\mathfrak{g}^{(i)} = (\mathfrak{g}_F^{(1)})^{\sigma_i} \otimes_{F^{\sigma_i}} \boldsymbol{R}$ $(1 \leqslant i \leqslant d)$, i.e., $\mathfrak{g}^{(i)}$ has an F^{σ_i}-form $\mathfrak{g}_{F^{\sigma_i}}^{(i)} = (\mathfrak{g}_F^{(1)})^{\sigma_i}$. If we write $X = \sum_{i=1}^d X^{(i)}$ with $X^{(i)} \in \mathfrak{g}^{(i)}$, then X is $\boldsymbol{Q}$-rational if and only if $X^{(1)}$ is F-rational and $X^{(i)} = X^{(1)\sigma_i}$ for $1 \leqslant i \leqslant d$. A similar statement is also true for the Cartan involution θ. Thus the determination of $\boldsymbol{Q}$-simple $\boldsymbol{Q}$-objects is equivalent to determining systems of (absolutely) simple F^{σ_i}-objects $(1 \leqslant i \leqslant d)$ which are mutually conjugate.

Now suppose there is given a $\boldsymbol{Q}$-simple $\boldsymbol{Q}$-form $\mathfrak{g}_{\boldsymbol{Q}}$ of $\mathfrak{g}$ for which there exists a $\boldsymbol{Q}$-rational cusp o_∞. (Hence the totally real number field F and the F-form $\mathfrak{g}_F^{(1)}$ of $\mathfrak{g}^{(1)}$ are determined.) We will show that there exists also a $\boldsymbol{Q}$-rational origin. First, it is known ([12a]) that the element X corresponding to o_∞ can be chosen to be $\boldsymbol{Q}$- rational. (This amounts to choosing a $\boldsymbol{Q}$-rational $\mathfrak{g}_0$ in a $\boldsymbol{Q}$-rational $\mathfrak{b}$.) Moreover, any $\boldsymbol{Q}$-rational X can be expressed in the form

$$X = \sum_{i=1}^{d} \sum_{j=1}^{r_0} X_j^{(1)\sigma_i} \ ,$$

where $\{X_1^{(1)}, \cdots, X_{r_0}^{(1)}\}$ ($r_0 = F$-rank $\mathfrak{g}_F^{(1)}$) is a "canonical basis" for the Lie algebra of a maximal F-split torus in $\operatorname{Ad} \mathfrak{g}_C^{(1)}$. Hence, from the conjugacy of maximal F-split tori, we see that the F-rational element $X^{(1)} = \sum_{j=1}^{r_0} X_j^{(1)}$ is uniquely deter-

mined up to F-rational inner automorphism of $\mathfrak{g}_C^{(1)}$, or what amounts to the same thing, the Q-rational element X is uniquely determined up to Q-rational inner automorphism of $\mathfrak{g}_C$. Therefore, in what follows, we may (hence shall) fix a Q-rational X once and for all. (From the above expression of X, it also follows that the R-rank of each factor $\mathfrak{g}^{(i)}$, which may depend on i, is a positive multiple of r_0. In particular, none of $\mathfrak{g}^{(i)}$ is compact.)

Let θ be a Cartan involution of $\mathfrak{g}$ such that $\theta X = -X$ and write

$$\theta = \sum_{i=1}^{d} \theta^{(i)}, \qquad Z = \sum_{i=1}^{d} Z^{(i)},$$

where $\theta^{(i)}$ is a Cartan involution of $\mathfrak{g}^{(i)}$ and $Z^{(i)} = \pi_i(Z)$ is the corresponding element in $\mathfrak{g}^{(i)}$. Similarly, we put $\mathfrak{k}^{(i)} = \pi_i(\mathfrak{k})$, $\mathfrak{p}^{(i)} = \pi_i(\mathfrak{p})$; then $\mathfrak{g}^{(i)} = \mathfrak{k}^{(i)} + \mathfrak{p}^{(i)}$ is the Cartan decomposition corresponding to $\theta^{(i)}$. In this notation, we obtain

Lemma 4. *Under the above assumptions, a Cartan involution θ is Q-rational, if and only if there exists a totally positive element α in F such that $\sqrt{\alpha}Z^{(1)}$ is F-rational and one has*

$$\sqrt{\alpha^{\sigma_i}}Z^{(i)} = (\sqrt{\alpha}Z^{(1)})^{\sigma_i} \tag{16}$$

for all $1 \leq i \leq d$. The totally imaginary quadratic extension $F' = F(\sqrt{-\alpha})$ is then uniquely determined by θ.

Proof. Suppose θ is Q-rational. Then $\theta^{(1)}$ is F-rational, and so $\mathfrak{k}^{(1)}$ and $\mathfrak{p}^{(1)}$ ($\neq \{0\}$) are defined over F. Since the restriction of the adjoint representation of $\mathfrak{k}^{(1)}$ on $\mathfrak{p}^{(1)}$ is irreducible and the center of $\mathrm{ad}_{\mathfrak{p}^{(1)}}\mathfrak{k}^{(1)}$ contains $J^{(1)} = \mathrm{ad}_{\mathfrak{p}^{(1)}} Z^{(1)}$, the commuter algebra of $\mathrm{ad}_{\mathfrak{p}_F^{(1)}}\mathfrak{k}_F^{(1)}$ in $\mathrm{End}\,\mathfrak{p}_F^{(1)}$ is a field F-isomorphic to an imaginary quadratice xtension F' of F (in C). If we write $F' = F(\sqrt{-\alpha})$ with ap ositive element α in F, uniquely determined modulo $(F^\times)^2$, then $\sqrt{\alpha}J^{(1)}$ and hence $\sqrt{\alpha}Z^{(1)}$ is F-rational; moreover $\alpha \pmod{(F^\times)^2}$ is uniquely characterized by this property. Transforming everything by the conjugation σ_i, we obtain the corresponding statement for the factor $\mathfrak{g}^{(i)}$. Hence α is totally positive, F' is totally imaginary, and one has the relation (16). Conversely, if there exists a totally positive element α in F satisfying the conditions mentioned in the Lemma, then clearly $\mathfrak{k}^{(1)}$ is defined over F and one has $\mathfrak{k}^{(i)} = \mathfrak{k}^{(1)\sigma_i}$ for all i. Hence θ is Q-rational. If there exists another totally positive element α' in F satisfying the same condition, then by the above-mentioned uniqueness, one has $\alpha' \sim \alpha$, i.e., $\alpha' = \alpha\beta^2$ for some $\beta \in F^\times$, and hence $F(\sqrt{-\alpha'}) = F(\sqrt{-\alpha})$, q.e.d.

Remark. In the case, where $V \neq \{0\}$, let $\mathfrak{g}_0^{(i)} = \pi_i(\mathfrak{g}_0)$, $V^{(i)} = \pi_i(V)$, $Z_0^{(i)} = \pi_i(Z_0)$. Then the representation $\mathrm{ad}_{V^{(i)}}\mathfrak{g}_0^{(i)}$ is irreducible and contains $I^{(i)} = 2\,\mathrm{ad}_{V^{(i)}} Z_0^{(i)}$ in its center. Hence, by the same reason as above, we see that there exists a uniquely determined totally imaginary quadratic extension $F_0' = F(\sqrt{-\alpha_0})$ such that the commuter algebra of $\mathrm{ad}_{V^{(1)}}\mathfrak{g}_{0F'}^{(1)}$ in $\mathrm{End}\,V_F^{(1)}$ is F-isomorphic to F_0', or equivalently, $\sqrt{\alpha_0}I^{(1)}$ (or $\sqrt{\alpha_0}Z_0^{(1)}$) is F-rational. (Then the relation $\sqrt{\alpha_0^{\sigma_i}}Z_0^{(i)} = (\sqrt{\alpha_0}Z_0^{(1)})^{\sigma_i}$ follows automatically.) By (1), if $\sqrt{\alpha}Z^{(1)}$ is F-rational, so is $\sqrt{\alpha}Z_0^{(1)}$. Hence one has $\alpha \sim \alpha_0$ and $F' = F_0'$. Thus, in this case, the field F' is uniquely determined by the Q-form $\mathfrak{g}_Q$ alone, independently of the choice of θ.

To find a Q-rational origin, we may proceed as follows. If $V = \{0\}$, let α be an arbitrary totally positive element in F; if $V \neq \{0\}$, we let $\alpha \sim \alpha_0$ in the notation of the above Remark. Take a Q-rational element $e' \in \Omega$ and set

$$e = \sum_{i=1}^{d} e^{(i)}, \qquad e^{(i)} = \sqrt{\alpha^{\sigma_i - 1}}\pi_i(e').$$

Then the origin o corresponding to e (i.e., $o = (\sqrt{-1}\,e, 0)$ in the Siegel domain expression of $\mathfrak{D}$) is Q-rational. In fact, let θ be the Cartan involution corresponding to e. Then, since $(\mathrm{ad}\,e)^2$ is Q-rational, Lemma 1 assures that $\theta|U$ is Q-rational; in particular, $\theta e' = \sum \sqrt{\alpha^{\sigma_i}}\theta^{(i)}e^{(i)}$ is Q-rational. Therefore, by Lemma 1 (or Lemma 4), we see that θ is Q-rational. Conversely, by Lemma 4, all Q-rational θ, and hence all Q-rational origin o, is obtained in this way. Note that $e^{(1)} \in \Omega^{(1)} = \pi_1(\Omega)$ corresponding to a Q-rational origin is characterized by the following two properties:

(i) $\sqrt{\alpha}e^{(1)}$ is F-rational;

(ii) $(\sqrt{\alpha}e^{(1)})^{\sigma_i}$ is in $\Omega^{(i)} = \pi_i(\Omega)$ for all $1 \leq i \leq d$.

Now, suppose α and $e^{(1)}$ are chosen as above. Then, (in the case $V \neq \{0\}$), since $\sqrt{\alpha}I^{(1)}$ is F-rational, $V_+^{(1)}$ ($= \pi_1(V_+)$) is defined over F'. Since $\theta^{(1)}$ is F-rational, the Jordan triple product $\{\ \}$ on $\tilde{V}^{(1)} = U_C^{(1)} \oplus V_+^{(1)}$ ($= \pi_1(\tilde{V})$) is defined over F'. Therefore, $\tilde{V}_{F'}^{(1)} = U_{F'}^{(1)} \oplus V_{+F'}^{(1)}$ with the induced triple product is a positive definite hermitian JTS over F'. Transforming everything by (an extension of) σ_i, we obtain positive definite hermitian JTS's $V_{F'^{\sigma_i}}^{(i)}$ over $F'^{\sigma_i} = F^{\sigma_i}(\sqrt{-\alpha^{\sigma_i}})$. In this sense, we call $\tilde{V}_{F'}^{(1)}$ a "totally positive" hermitian JTS. In a similar sense, $f^{(1)} = f|V_+^{(1)} \times V_-^{(1)}$ gives an F'-valued totally positive hermitian form on $V_{+F'}^{(1)}$, and $\mathscr{H}(V_{+F'}^{(1)}, f^{(1)})$ is a totally formally real Jordan algebra over F.

To define a Jordan algebra structure on $U_F^{(1)}$, we consider a mutation of $\tilde{V}^{(1)}$ by $e'^{(1)} = \sqrt{\alpha}\,e^{(1)}$

$$\{x, y, z\}_{e'^{(1)}} = \{x, \alpha^{-1}u + \sqrt{\alpha}^{-1}v, z\}, \tag{17}$$

where $y = u + v$ with $u \in U_C^{(1)}$, $v \in V_-^{(1)}$. Then the corresponding Jordan product and representation

$$(18)\qquad \begin{aligned} u_{e'^{(1)}}u' &= \sqrt{\alpha}^{-1}u\cdot u' = \{u', \sqrt{\alpha}^{-1}e^{(1)}, u'\}\ , \\ 2R^{(1)}_{e'^{(1)}}(u) &= 2\sqrt{\alpha}^{-1}R^{(1)}(u) = (2u \square \sqrt{\alpha}^{-1}e^{(1)})\,|\,V_+^{(1)} \qquad (u, u' \in U^{(1)}) \end{aligned}$$

are defined over F and F', respectively. Thus $(U_F^{(1)}, \sqrt{\alpha}e^{(1)})$ is a totally formally real (central simple) Jordan algebra over F and

$$2\sqrt{\alpha}^{-1}R^{(1)}: (U_F^{(1)}, \sqrt{\alpha}e^{(1)}) \longrightarrow \mathscr{H}(V^{(1)}_{+F'}, f^{(1)})$$

is an F-linear representation of it satisfying the condition (6). If we replace $e^{(1)}$ by another $a^{(1)} \in \Omega^{(1)}$ satisfying the conditions (i), (ii) for a totally positive element α' in F ($\alpha' \sim \alpha$ if $V \neq \{0\}$), then the triple product $\{\ \}$ (and the data $_{e'^{(1)}}$, $R^{(1)}_{e'^{(1)}}$, $f^{(1)}$) are transformed by a "totally positive F-mutation", that is, a mutation by an F-rational element $(\alpha/\sqrt{\alpha'})a^{(1)-1}$ satisfying the condition (ii) (i.e., $(\sqrt{\alpha'}a^{(1)-1})^{\sigma_i} \in \Omega^{(i)}$ for all i).

Conversely, starting from any totally imaginary quadratic extension $F' = F(\sqrt{-\alpha})$ of a totally real number field F, a totally formally real (central simple) Jordan algebra $(U_F^{(1)}, \sqrt{\alpha}e^{(1)})$ over F, and an F-linear representation $2\sqrt{\alpha}^{-1}R^{(1)}$ of it satisfying (6), we can construct by the process explained in 1 a (simple) totally positive hermitian JTS $(\tilde{V}_{F'}^{(1)}, \{\ \})$ over F' and then a (simple) Lie algebra of hermitian type $\mathfrak{g}_F^{(1)}$ over F with an F-rational origin and cusp. In this way, we obtain a system of mutually conjugate (simple) F^{σ_i}-objects, which gives rise to a ($\boldsymbol{Q}$-simple) $\boldsymbol{Q}$-object.

It is possible to give a theorem analogous to Theorem 1, concerning $\boldsymbol{Q}$-objects. However, for our purpose, the following partial result will be sufficient. First, the notion of "F-isomorphism" of F-objects in the category (a) is defined in a natural manner. In particular, when, as above, the $\boldsymbol{Q}$-form $\mathfrak{g}_{\boldsymbol{Q}}$ and the $\boldsymbol{Q}$-rational element X are fixed, the $\boldsymbol{Q}$-objects corresponding to $e^{(1)}$ and $a^{(1)} \in \Omega^{(1)}$ satisfying the conditions (i), (ii) are $\boldsymbol{Q}$-isomorphic, if and only if there exists g_1 in $G'^{(1)}_{0F}$ (the group of F-rational elements in $G'^{(1)}_0 = \{g \in \operatorname{Aut}\mathfrak{g}_C^{(1)} \mid gX^{(1)} = X^{(1)}\}$) such that $\sqrt{\alpha'}a^{(1)} = g_1\sqrt{\alpha}e^{(1)}$. On the other hand, an "F-equivalence" of two (non-trivial) Jordan algebra representations over F

$$2\sqrt{\alpha}^{-1}R^{(1)}: (U_F^{(1)}, \sqrt{\alpha}e^{(1)}) \longrightarrow \mathscr{H}(V^{(1)}_{+F'}, f^{(1)})\ ,$$

and

$$2\sqrt{\alpha'}^{-1}R^{(1)}_{a^{(1)}}: (U_F^{(1)}, \sqrt{\alpha'}a^{(1)}) \longrightarrow \mathscr{H}(V^{(1)}_{+F'}, f^{(1)}_{a^{(1)}})$$

are defined to be a pair (φ, ψ) formed of a Jordan algebra isomorphism

$\varphi: (U_F^{(1)}, \sqrt{\alpha}e^{(1)}) \to (U_F^{(1)}, \sqrt{\alpha'}a^{(1)})$ over F and $\psi \in GL(V^{(1)}_{+F'})$ such that

$$(19)\qquad \begin{aligned} \psi\cdot\sqrt{\alpha}^{-1}R^{(1)}(u)\cdot\psi^{-1} &= \sqrt{\alpha'}^{-1}R^{(1)}_{a^{(1)}}(\varphi(u)) \qquad \text{for } u \in U_F\ , \\ f^{(1)}(v, v') &= f^{(1)}_{a^{(1)}}(\psi(v), \psi(v')) \qquad \text{for } v, v' \in V^{(1)}_{+F'}\ . \end{aligned}$$

(For trivial representations, an F-equivalence is simply a Jordan algebra isomorphism φ.) It is clear that, if $g_1 \in G'^{(1)}_{0F}$ and $g_1(\sqrt{\alpha}e^{(1)}) = \sqrt{\alpha'}a^{(1)}$, then the pair of $\varphi = g_1|U_F^{(1)}$ and $\psi = g_1|V^{(1)}_{+F'}$ is an F-equivalence of the corresponding representations. Conversely, it can be shown by a standard augument in JTS ([12h]) that any F-equivalence of two Jordan algebra representations over F can uniquely be extended to an F-isomorphism of the corresponding F-objects in the category (a).

Summing up, we obtain the following

Theorem 2. *Let F be a totally real number field. Then $\boldsymbol{Q}$-isomorphism classes of $\boldsymbol{Q}$-simple $\boldsymbol{Q}$-objects belonging to F (i.e., objects in the category* (a) *endowed with $\boldsymbol{Q}$-simple $\boldsymbol{Q}$-forms $\mathfrak{g}_{\boldsymbol{Q}}$ such that o and o_∞ are $\boldsymbol{Q}$-rational, $\mathfrak{g}^{(1)}$ is defined over F and $\mathfrak{g}_{\boldsymbol{Q}} \cong \mathfrak{g}_F^{(1)}$) are in a one-to-one correspondence with F-equivalence classes of Jordan algebra representations*

$$2\sqrt{\alpha}^{-1}R^{(1)}: (U_F^{(1)}, \sqrt{\alpha}e^{(1)}) \longrightarrow \mathscr{H}(V^{(1)}_{+F'}, f^{(1)})$$

satisfying the condition (6), *where $F' = F(\sqrt{-\alpha})$ is a totally imaginary quadratic extension of F, $(U_F^{(1)}, \sqrt{\alpha}e^{(1)})$ is a totally formally real central simple Jordan algebra over F, and $f^{(1)}$ is a totally positive hermitian form on $V^{(1)}_{+F'}$. In particular, without specifying the $\boldsymbol{Q}$-rational origins, the $\boldsymbol{Q}$-isomorphism classes of $\boldsymbol{Q}$-simple Lie algebras $\mathfrak{g}_{\boldsymbol{Q}}$ over $\boldsymbol{Q}$ with $\boldsymbol{Q}$-rational cusps correspond in a one-to-one way to the equivalence classes of the Jordan algebras $(U_F^{(1)}, \sqrt{\alpha}e^{(1)})$ and their representations $2\sqrt{\alpha}^{-1}R^{(1)}$ with respect to totally positive F-mutation.*

4. In the tube domain case ($V = \{0\}$), it follows from Theorem 2 that the determination of $\boldsymbol{Q}$-simple $\boldsymbol{Q}$-objects (resp. $\boldsymbol{Q}$-simple $\boldsymbol{Q}$-forms $\mathfrak{g}_{\boldsymbol{Q}}$) up to $\boldsymbol{Q}$-isomorphism is reduced to that of totally formally real F-forms of the formally real simple Jordan algebras $U^{(1)}$ up to F-isomorphism (resp. totally positive F-mutation). (For classification of F-forms of Jordan algebras, see [2], [13]. Cf. also [12], [15].)

As an example of non-tube-domain case, we consider the case of an exceptional symmetric domain $\mathscr{D}$ where $\mathfrak{g}^{(1)}$ is of type E_6. In this case, the data $(U^{(1)}, e^{(1)})$, $2R^{(1)}$, etc. are given as follows. Let $U^{(1)}$ be an 8-dimensional real vector space endowed with a symmetric bilinear form S of singnature $(1, 7)$ and

let $e^{(1)} \in U^{(1)}$ be such that $S(e^{(1)}, e^{(1)}) > 0$. Then the Jordan product in $U^{(1)}$ is given by

$$uu' = S(e^{(1)}, e^{(1)})^{-1}(S(u, e^{(1)})u' + S(u', e^{(1)})u - S(u, u')e^{(1)}) . \tag{20}$$

Let C be the Clifford algebra of $(U^{(1)}, S)$, and C^+ the even part of C. Then one has

$$C \cong \mathcal{M}_{16}(\boldsymbol{R}) \quad \text{and} \quad C^+ \cong \mathcal{M}_8(\boldsymbol{C}) .$$

We identify C^+ with $\mathcal{M}_8(\boldsymbol{C})$ by the second isomorphism in such a way that one has $e^{-1}x^\iota e = {}^t\bar{x}$ for all $x \in C^+$, where ι is the canonical anti-involution of C^+. (This is equivalent to saying that the standard Cartan involution $x \mapsto -{}^t\bar{x}$ of $C^+ = \mathcal{M}_8(\boldsymbol{C})$ induces the Cartan involution of $\mathfrak{so}(U^{(1)}, S) \subset C^+$ corresponding to the orthogonal decomposition $U^{(1)} = (\boldsymbol{R}e^{(1)}) \oplus (\boldsymbol{R}e^{(1)})^\perp$.) The representation $2R^{(1)}$ satisfying (6) is then given by the "spin representation"

$$U^{(1)} \ni u \longmapsto S(e^{(1)}, e^{(1)})^{-1}ue^{(1)} \in \mathcal{H}_8(\boldsymbol{C}) . \tag{21}$$

Note that the "conjugate" representation $2\bar{R}^{(1)} : u \mapsto S(e^{(1)}, e^{(1)})^{-1}e^{(1)}u$ is $\boldsymbol{R}$-equivalent to $2R^{(1)}$ by

$$\varphi : u \longmapsto -\hat{u} = -u + \frac{2S(u, e^{(1)})}{S(e^{(1)}, e^{(1)})}e^{(1)}$$

and $\psi = \mathrm{id}$. (These representations correspond to the two mutually conjugate spin representations of $\mathfrak{so}(U^{(1)}, S)$.)

The data determining a $\boldsymbol{Q}$-simple $\boldsymbol{Q}$-object are given as follows. Let F be a totally real number field. Let $U_F^{(1)}$ be an F-form of $U^{(1)}$ (as vector space) and take an F-rational S such that all conjugates S^{σ_i} $(1 \leq i \leq d)$ are of signature $(1, 7)$. Then we have F-forms C_F and C_F^+ of C and C^+. Put $\alpha = -\det(S)$ (for any fixed basis). Then α is totally positive, and the center of C_F^+ may be identified with $F' = F(\sqrt{-\alpha})$. Since the representation $2\sqrt{\alpha}^{-1}R^{(1)}$ should be obtained on F'^8, one must have $C_F^+ \cong \mathcal{M}_8(F')$. Hence one has

$$C_F \otimes_F F' \sim (C_F^+/F') \sim 1 .$$

($\sim$ means the equivalence in the sense of Brauer.) The same is also true for all conjugates $(C_F)^{\sigma_i}$ $(1 \leq i \leq d)$. Therefore, by the theory of simple algebras over algebraic number fields, C_F is equivalent to a quaternion algebra over F of the form $(-\alpha, \beta)$ with a totally positive $\beta \in F$. It follows that S is equivalent to a symmetric bilinear form corresponding to

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus \mathrm{diag}(-\beta, -\beta, -\beta, -\alpha\beta, -\alpha\beta, -\alpha\beta) , \tag{22}$$

since these two forms have the same invariants. Finally, we take $e^{(1)}$ in such a way that $e'^{(1)} = \sqrt{\alpha}e^{(1)}$ is F-rational. Then we obtain an F-linear Jordan algebra representation

$$2\sqrt{\alpha}^{-1}R^{(1)} : (U_F^{(1)}, \sqrt{\alpha}e^{(1)}) \longrightarrow \mathcal{H}_8(F') .$$

Thus, in particular, the $\boldsymbol{Q}$-form of $\mathfrak{g}$ with a $\boldsymbol{Q}$-rational cusp is completely determined by the symmetric bilinear form S satisfying the above conditions, or equivalently, by the pair of totally positive elements α, β in F.

Finally, we remark that our method can also be applied to the determination of certain $\boldsymbol{Q}$-forms of real semi-simple Lie algebras corresponding to (non-compact) symmetric "R-spaces" introduced by Kobayashi and Nagano ([6], [9a]). Beyond formal analogy, there seems to be a direct connection between the $\boldsymbol{Q}$-forms of symmetric domains and symmetric R-spaces.

References

[1] Baily, W. and Borel, A., Compactification of arithmetic quotients of bounded symmetric domains, Ann. of Math. **84** (1966), 442–528.

[2] Braun, H. and Koecher, M., Jordan-Algebren, Springer, Berlin-Heidelberg-New York, 1966.

[3] Dorfmeister, J., Infinitesimal automorphisms of homogeneous Siegel domains, to appear.

[4] Kaup, W., Einige Bemerkungen über polynomiale Vektorfelder, Jordanalgebren und die Automorphismen von Siegelschen Gebieten, Math. Ann. **204** (1973), 131–144.

[5] Kaup, W., Matsushima, Y. and Ochiai, T., On the automorphisms and equivalences of generalized Siegel domains, Amer. J. Math. **92** (1970), 475–497.

[6] Kobayashi, S. and Nagano, T., On filtered Lie algebras and geometric structures, I, J. Math. Mech. **13** (1964), 875–908; II, ibid. **14** (1965), 513–521; III, ibid **14** (1965), 679–706.

[7] Koecher, M., (a) Jordan algebras and their applications, Lecture Notes, Univ. of Minnesota, Minneapolis, 1962.
(b) An elementary approach to bounded symmetric domains, Lecture Notes, Rice Univ., Houston, 1969.

[8] Korányi, A. and Wolf, J., Realization of hermitian symmetric spaces as generalized half-planes, Ann. of Math. **81** (1965), 265–288.

[9] Loos, O., (a) Jordan triple systems, R-spaces, and bounded symmetric domains, Bull. Amer. Math. Soc. **77** (1971), 558–561.
(b) Bounded symmetric domains and Jordan triple systems, I, to appear.

[10] Meyberg, K., Jordan-Tripelsysteme und die Koecher-Konstruktion von Lie-Algebren, Math. Z. **115** (1970), 58–78.

[11] Nakajima, K., On realization of Siegel domains of the second kind as those of the third kind, J. Math., Kyoto Univ. **16** (1976), 143–166.

[12] Satake, I., (a) A note on holomorphic imbeddings and compactification of symmetric domains, Amer. J. Math. **90** (1968), 231–247.

(b) Classification theory of semi-simple algebraic groups, Marcel Dekker, New York, 1971.
(c) Linear imbeddings of self-dual homogeneous cones, Nagoya Math. J. **46** (1972), 121–145.
(d) Realization of symmetric domains as Siegel domains of the third kind, Lecture Notes, Univ. of California, Berkeley, 1972.[1)]
(e) Infinitesimal automorphisms of symmetric domains, preprint, 1974.[1)]
(f) On classification of quasi-symmetric Siegel domains, Nagoya Math. J. **62** (1976), 1–12.
(g) On symmetric and quasi-symmetric Siegel domains, Several Complex Variables, Proc. of Symposia in pure Math. **30**, AMS, 1977, 309–315.
(h) See footnote below.

[13] Springer, T., Jordan algebras and algebraic groups, Ergebn. Math. **75**, Springer, New York-Heidelberg-Berlin, 1973.
[14] Takeuchi, M., On symmetric Siegel domains, Nagoya Math. J. **59** (1975), 9–44.
[15] Tits, J., Classification of algebraic semisimple groups, Algebraic groups an discontinuous subgroups, Proc. of Symposia in Pure Math. **10**, AMS, 1966, 33–62.
[16] Wolf, J. and Korányi, A., Generalized Cayley transformations of bounded symmetric domains, Amer. J. Math. 87 (1965), 899–939.

Department of Mathematics
University of California
Berkeley, California 94720
U.S.A.

1) The contents of [12d, e] will be incorporated in a book to be published from Iwanami and Princeton Univ. Press, which we refer to as [12h].

ALGEBRAIC NUMBER THEORY, Papers contributed for the International Symposium, Kyoto 1976; S. Iyanaga (Ed.): Japan Society for the Promotion of Science, Tokyo, 1977

Représentations *l*-adiques

JEAN-PIERRE SERRE

La notion de *système rationnel de représentations l-adiques* a été introduite par Taniyama [37], il y a près de vingt ans. Cette notion joue le rôle de la *cohomologie rationnelle* pour les variétés algébriques; elle est d'une grande utilité dans l'étude arithmétique de ces variétés. Malheureusement, on sait peu de chose sur les systèmes rationnels de représentations *l*-adiques, en dehors du cas abélien ([27], [37], [40]): les *problèmes* sont plus nombreux que les *théorèmes*! Ce sont ces problèmes, et ces théorèmes, que je me propose de discuter.

§ 1. Notations et définitions

Dans tout ce qui suit (§ 7 excepté), on note K un corps de nombres algébriques[1)], $\bar{K}$ une clôture algébrique de K, et G_K le groupe de Galois de $\bar{K}$ sur K. Soit $\sum_K$ l'ensemble des places ultramétriques de K; si $v \in \sum_K$, on note k_v le corps résiduel correspondant, p_v sa caractéristique, et Nv le nombre de ses éléments.

Soit l un nombre premier. Une *représentation l-adique* de G_K est un homomorphisme continu

$$\rho_l : G_K \longrightarrow \mathrm{Aut}\,(V_l)\ ,$$

où V_l est un $\boldsymbol{Q}_l$-espace vectoriel de dimension finie.

Un *système de représentations l-adiques de* G_K est la donnée, pour tout l, d'une représentation l-adique ρ_l. Un tel système est dit *rationnel* s'il jouit de la propriété suivante (cf. [27], [37]):

Il existe une partie finie S de $\sum_K$ telle que, si $v \in \sum_K - S$, et si $l \neq p_v$, alors ρ_l est non ramifiée en v et le polynôme caractéristique de l'élément de

1) On pourrait se borner à supposer que K est une *extension de type fini de* $\boldsymbol{Q}$, non nécessairement algébrique; cela ne changerait rien aux résultats et conjectures des §§ 2 et 3.

Frobenius $\rho_l(\mathrm{Frob}_v)$ *est à coefficients dans* $\boldsymbol{Q}$, *et ne dépend pas de* l.

Cette condition de compatibilité entraîne que, si l'on connaît ρ_l pour *un* l, on connaît, sinon tous les ρ_l, du moins tous leurs semi-simplifiés ([27], I–10).

Les seuls exemples connus[2] de systèmes rationnels proviennent, de près ou de loin, de la *cohomologie l-adique*, cf. § 2. On serait par exemple fort surpris de trouver des systèmes rationnels (ρ_l) tels que les valeurs absolues des valeurs propres des $\rho_l(\mathrm{Frob}_v)$ ne soient pas des puissances entières de $Nv^{1/2}$!

§ 2. Systèmes fournis par la cohomologie

Soient X une variété projective lisse sur K, et $\overline{X}$ la $\overline{K}$-variété déduite de X par extension du corps de base à $\overline{K}$. Soit m un entier $\geqslant 1$. Posons $V_l = H^m(\overline{X}; \boldsymbol{Q}_l)$, m-ième groupe de cohomologie l-adique de $\overline{X}$, au sens de [1]; c'est un $\boldsymbol{Q}_l$-espace vectoriel de dimension finie. Le groupe G_K opère par transport de structure sur V_l; on en déduit une représentation l-adique

$$\rho_l : G_K \longrightarrow \mathrm{Aut}\,(V_l)\ .$$

Soit S une partie finie de $\sum_K$ assez grande pour que X ait "bonne réduction en dehors de S", i.e. provienne d'un schéma projectif et lisse X_S sur l'anneau des S-entiers de K. Si $v \in \sum_K - S$, notons X_v la fibre en v du schéma X_S; c'est une variété projective et lisse sur k_v, appelée parfois la *réduction de* X *modulo* v; notons $\overline{X}_v$ la variété déduite de X_v par extension du corps de base à une clôture algébrique de k_v. Les théorèmes de changement de base pour la topologie étale [1] montrent que, si $l \neq p_v$, on peut identifier V_l à $H^m(\overline{X}_v; \boldsymbol{Q}_l)$, que ρ_l est non ramifiée en v, et que $\rho_l(\mathrm{Frob}_v)$ s'identifie à l'inverse du "Frobenius géométrique" de $H^m(\overline{X}_v; \boldsymbol{Q}_l)$. D'après Deligne [8], ceci entraîne:

2.1. *Si* $v \notin S$, *le polynôme caractéristique de* $\rho_l(\mathrm{Frob}_v)$, $l \neq p_v$, *est à coefficients dans* $\boldsymbol{Q}$ *et indépendant de* l; *de plus les inverses de ses racines sont des entiers algébriques dont toutes les valeurs absolues (archimédiennes) sont égales à* $Nv^{m/2}$.

En particulier, le système (ρ_l) est *rationnel*.

(Lorsque $m = 1$, V_l est le dual du *module de Tate* de la variété d'Albanese de X; on retrouve le cas considéré initialement par Taniyama [37].)

Soit $G_l = \rho_l(G_K)$ l'image de ρ_l; c'est un sous-groupe de Lie du groupe de Lie l-adique $\mathrm{Aut}\,(V_l)$, cf. [26]; son algèbre de Lie $\mathfrak{g}_l$ est une sous-algèbre de $\mathrm{End}\,(V_l)$. On sait très peu de choses sur les $\mathfrak{g}_l$; on ignore même si leur

2) A part, peut-être, ceux construits par Shimura [32], [33].

dimension est indépendante de l (cf. § 3). Voici quelques résultats élémentaires:

2.2. *Supposons que les* $\rho_l(\mathrm{Frob}_v)$, *pour* $v \notin S$, $p_v \neq l$, *soient semi-simples. Alors* $\mathfrak{g}_l$ *est scindable* (Bourbaki, LIE VII, § 5) *et ses sous-algèbres de Cartan sont commutatives et formées d'éléments semi-simples.*

Cela résulte de Bourbaki, *loc. cit.*, p. 62, exerc. 16, compte tenu de ce que les logarithmes[3] des $\rho_l(\mathrm{Frob}_v)$ sont denses dans $\mathfrak{g}_l$ d'après le théorème de Čebotarev.

L'hypothèse faite sur les $\rho_l(\mathrm{Frob}_v)$ est vraie pour $m = 1$, en vertu des résultats de Weil sur les variétés abéliennes; on espère qu'elle est vraie pour tout m (cela résulterait des "conjectures standard" de Grothendieck, cf. [11], 4.6).

2.3 (Deligne). *L'enveloppe algébrique* $\mathfrak{g}_l^{\mathrm{alg}}$ *de* $\mathfrak{g}_l$ *contient les homothéties.* (On conjecture que $\mathfrak{g}_l^{\mathrm{alg}} = \mathfrak{g}_l$, cf. § 3.)

Soit en effet $v \in \sum_K - S$ tel que $p_v \neq l$. L'algèbre de Lie $\mathfrak{g}_l$ contient l'élément $F_v = \log \rho_l(\mathrm{Frob}_v)$; si $\lambda_1, \cdots, \lambda_n$ sont les valeurs propres de F_v, il résulte de 2.1 que toute relation linéaire

$$\sum a_i \lambda_i = 0\ , \qquad \text{avec } a_i \in \boldsymbol{Z}\ ,$$

entraîne $\sum a_i = 0$; or on sait que cette propriété équivaut à dire que l'enveloppe algébrique de F_v contient les homothéties. D'où 2.3.

2.4. *On a* $H^i(\mathfrak{g}_l; V_l) = 0$ *pour tout* i. (Le même résultat vaut pour les espaces tensoriels $T^r V_l \otimes T^s V_l^*$, avec $r \neq s$.)

Cela résulte de 2.1 combiné avec le critère de nullité de cohomologie donné dans [26], II (cf. Bourbaki, LIE VII. 56, exerc. 6). Deligne m'a fait observer que cela peut aussi se déduire de 2.3, et du fait que $\mathfrak{g}_l^{\mathrm{alg}}$ opère trivialement sur $H^i(\mathfrak{g}_l; V_l)$.

Le cas $m = 1$, $i = 1$, $s = 1$, $r = 0$ de 2.4 a la conséquence suivante: si A est une variété abélienne sur K, *tout sous-groupe d'indice fini de* $A(K)$ *est un groupe de congruence* [26].

§ 3. Relations avec les groupes de Hodge: conjectures

Les notations étant celles du § 2, choisissons un plongement de $\overline{K}$ dans C, et soit X_C la variété complexe déduite de $\overline{X}$ par le changement de base $\overline{K} \to C$. Notons $V_{\boldsymbol{Q}}$ (resp. V_C) le m-ième groupe de cohomologie de X_C à coefficients dans $\boldsymbol{Q}$ (resp. dans C). On a

3) Il s'agit de logarithmes *l-adiques*, cf. Bourbaki, LIE III, §7, n°6.

$V_C = C \otimes V_Q$ et $V_l = Q_l \otimes V_Q$ pour tout l (cf. [1]).

La théorie de Hodge définit une bigraduation de V_C:

$$V_C = \coprod_{p+q=m} V_C^{p,q} .$$

Soit $T = C^* \times C^*$; faisons opérer T sur V_C par:

$$(u, v).h = u^p v^q h \qquad \text{si } h \in V_C^{p,q} .$$

On obtient ainsi un homomorphisme de groupes algébriques

$$\varphi : T \longrightarrow GL(V_C) .$$

Le *groupe de Hodge* $\mathrm{Hdg} = \mathrm{Hdg}_{m,X}$ peut être défini comme le plus petit Q-sous-groupe algébrique de $GL(V_Q)$ qui, après extension des scalaires à C, contienne le tore $\varphi(T)$; il est engendré par les $\varphi^\sigma(T)$, où σ parcourt le groupe des Q-automorphismes de C. Ce groupe a été introduit par Mumford-Tate [16], et étudié par Saavedra dans sa thèse [24] (voir aussi [7], [17]). C'est un groupe réductif connexe; son algèbre de Lie $\mathfrak{h}_Q$ est une sous-algèbre de $\mathrm{End}(V_Q)$; par construction, elle contient les homothéties. On conjecture (cf. [16]):

C.3.1. *L'algèbre de Lie $\mathfrak{g}_l$ du groupe de Galois $G_l = \mathrm{Im}(\rho_l)$ est égale à $\mathfrak{h}_l = Q_l \otimes \mathfrak{h}_Q$.*

(Cela entraînerait en particulier que $\mathfrak{g}_l$ est algébrique, réductive dans $\mathrm{End}(V_l)$, et que sa dimension est indépendante de l.)

L'assertion C.3.1 est équivalente à:

C.3.2. *Les groupes G_l et $\mathrm{Hdg}(Q_l)$ sont commensurables* (i.e. leur intersection est ouverte dans chacun d'eux).

On peut formuler une conjecture plus précise:

C.3.3. *Il existe un Q-sous-groupe algébrique H de $GL(V_Q)$, de composante neutre* Hdg, *tel que*:

a) *On a $\rho_l(G_K) \subset H(Q_l)$ pour tout l.*

b) *Si Γ désigne le groupe fini* H/Hdg, *l'homomorphisme*

$$G_K \longrightarrow H(Q_l) \longrightarrow \Gamma .$$

est surjectif, et indépendant de l.

c) *Si $v \in \sum_K - S$, et $l \neq p_v$, l'image F_v de $\rho_l(\mathrm{Frob}_v)$ dans la variété Cl_H des classes de conjugaison*[4] *de H est rationnelle sur Q, et ne dépend pas de l.*

4) La variété Cl_H est, par définition, le spectre de la sous-algèbre de l'algèbre affine de H formée des *fonctions centrales*.

d) *Pour tout l, $\rho_l(G_K)$ est ouvert dans $H(Q_l)$.*

On notera que, si un tel groupe H existe, il est unique, puisque c'est l'adhérence de $\rho_l(G_K)$ pour la topologie de Zariski.

Exemple. $m = 1$, X est une courbe elliptique à multiplications complexes par un corps quadratique imaginaire F non contenu dans K. Le groupe Hdg est le sous-groupe de Cartan de GL_2 défini par F, et H est le normalisateur de Hdg; le groupe Γ a deux éléments, et l'homomorphisme $G_K \longrightarrow \Gamma$ de b) est celui défini par l'extension quadratique $K.F$ de K.

La conjecture C.3.3 entraîne:

C.3.4. *Il existe une extension finie K' de K telle que, pour tout l, $\rho_l(G_{K'})$ soit un sous-groupe ouvert de* $\mathrm{Hdg}(Q_l)$.

En effet, il suffit de choisir K' tel que $G_{K'}$ soit contenu dans le noyau de l'homomorphisme $G_K \longrightarrow \Gamma$ de C.3.3. b).

Les conjectures ci-dessus sont étroitement liées à celles de Hodge et Tate sur les *classes de cohomologie algébriques* (cf. [38], ainsi que [24], p. 402–405):

3.5. *Si la conjecture de Tate est vraie pour tous les $X \times \cdots \times X$, on a $\mathfrak{g}_l^{\mathrm{alg}} \supset \mathfrak{h}_l$ pour tout l.*

3.6. *Si la conjecture de Hodge est vraie pour tous les $X \times \cdots \times X$, il existe un Q-sous-groupe algébrique H de $GL(V_Q)$, de composante neutre* Hdg, *tel que les propriétés* a) *et* b) *de* C.3.3 *soient satisfaites. En particulier, on a $\mathfrak{g}_l \subset \mathfrak{h}_l$ pour tout l.*

Variation avec l

Supposons C.3.4 vraie, et remplaçons K par K', de sorte que $G_l \subset \mathrm{Hdg}(Q_l)$ pour tout l. Choisissons une base de V_Q, ce qui donne un sens à $\mathrm{Hdg}(Z_l)$. Pour presque tout l, on a $G_l \subset \mathrm{Hdg}(Z_l)$, et, comme $\mathrm{Hdg}(Z_l)$ est compact, l'indice de G_l dans ce groupe est *fini*. On peut se demander si cet indice est égal à 1 pour presque tout l. Des exemples simples montrent qu'il n'en est rien (même pour $m = 1$, cf. 4.2.1, 4.2.2). Toutefois, il me paraît raisonnable de conjecturer:

C.3.7. a) *L'indice de G_l dans $\mathrm{Hdg}(Z_l)$ est borné.*

b) *Pour presque tout l, G_l contient les commutateurs de $\mathrm{Hdg}(Z_l)$, ainsi que les puissances m-ièmes des homothéties.*

On peut aussi exprimer les choses en termes *adéliques*: soit $A^f = Q \otimes \hat{Z}$ l'anneau des adèles finis de Q. La famille des ρ_l définit un homomorphisme

continu ρ de G_K dans le groupe $\mathrm{Hdg}(A^f)$, produit "restreint" des $\mathrm{Hdg}(\boldsymbol{Q}_l)$, et l'on aimerait savoir si $\rho(G_K)$ est *ouvert* dans $\mathrm{Hdg}(A^f)$, ce qui entraînerait que $G_l = \mathrm{Hdg}(\boldsymbol{Z}_l)$ pour presque tout l. On peut espérer que seule la présence d'isogénies[5] s'oppose à cette propriété. D'où la conjecture :

C.3.8. *Supposons qu'il n'existe aucune $\boldsymbol{Q}$-isogénie $H' \to \mathrm{Hdg}$, de degré >1, avec H' connexe, telle que $\varphi : T \to \mathrm{Hdg}(\boldsymbol{C})$ se relève en $\varphi' : T \to H'(\boldsymbol{C})$. Alors $\rho(G_K)$ est ouvert dans $\mathrm{Hdg}(A^f)$.*

(L'hypothèse faite sur Hdg revient à dire que $\pi_1(\mathrm{Hdg}(\boldsymbol{C}))$ est engendré par les $\varphi^\sigma(\pi_1(T))$, pour $\sigma \in \mathrm{Aut}(\boldsymbol{C})$.)

§ 4. Relations avec les groupes de Hodge : résultats

Le cas le plus étudié est celui où $m = 1$, X étant une variété abélienne. On a alors :

4.1. (Piatetckii-Šapiro [21], Deligne, Borovoi [4]). *Il existe une extension finie K' de K telle que, pour tout l, on ait $\rho_l(G_{K'}) \subset \mathrm{Hdg}(\boldsymbol{Q}_l)$; en particulier, on a $\mathfrak{g}_l \subset \mathfrak{h}_l$.*

En comparant à 3.6, on voit que l'on obtient essentiellement le même résultat que si la conjecture de Hodge était vraie pour les variétés abéliennes (ce que l'on ignore) ; autrement dit, sur une telle variété, toute classe de cohomologie rationnelle de type (p, p) se comporte, du point de vue galoisien, comme si elle était algébrique.

Il est remarquable que la démonstration de 4.1 utilise le cas particulier des variétés abéliennes à multiplications complexes :

4.2 (Shimura-Taniyama [34], Weil [40]). *Si X est de type (CM), la conjecture* C.3.3 *est vraie ; en particulier, on a $\mathfrak{g}_l = \mathfrak{h}_l$.*

Le groupe Hdg est alors un *tore*, ce qui permet d'expliciter les homomorphismes

$$\rho_l : G_K \longrightarrow \mathrm{Hdg}(\boldsymbol{Q}_l) \ , \qquad \text{cf. [34], [40], et [27], II, 2.8.}$$

Signalons que, même dans ce cas, il n'est pas toujours vrai que $\rho(G_K)$ soit *ouvert* dans le groupe adélique $\mathrm{Hdg}(A^f)$. Voici deux contre-exemples :

4.2.1. X est la jacobienne de la courbe $y^2 = 1 - x^{23}$.

4.2.2. X est le produit de quatre courbes elliptiques à multiplications complexes par $\boldsymbol{Q}(\sqrt{-d_i})$, $i = 1, 2, 3, 4$, les d_i étant choisis tels que $d_1 d_2 d_3 d_4$ soit un carré et qu'aucun des $d_i d_j$ $(i \neq j)$ n'en soit un.

(Dans 4.2.1, l'homomorphisme $\rho : G_K \to \mathrm{Hdg}(A^f)$ se factorise par une isogénie de degré 3 de Hdg, et dans 4.2.2, il se factorise par une isogénie de degré 2.)

5) On sait que, si $H' \to H$ est une isogénie de degré >1, l'image de $H'(A^f)$ dans $H(A^f)$ n'est pas ouverte; il faut donc éviter que ρ ne se factorise par une telle isogénie.

4.3 (cf. [27], [31]). *Si X est une courbe elliptique sans multiplications complexes, on a $\mathrm{Hdg} = \boldsymbol{GL}(V_{\boldsymbol{Q}})$, et $\rho(G_K)$ est ouvert dans $\mathrm{Hdg}(A^f) \simeq \boldsymbol{GL}_2(A^f)$; en particulier, on a $\mathfrak{g}_l = \mathfrak{h}_l$ pour tout l.*

Le fait que Hdg soit de rang semi-simple 1 entraîne que, si les groupes de Galois G_l étaient "trop petits", ils seraient "presque" abéliens, et donc justiciables de [27], Chap. II et III ; à partir de là, on peut en déduire de diverses façons que la courbe X a des multiplications complexes, contrairement à l'hypothèse faite.

4.4 (*"fausses courbes elliptiques"*, cf. Ohta [18], Jacobson [10]). On suppose que $\dim X = 2$, et que $\mathrm{End}(X)$ est *un ordre d'un corps de quaternions D*. On a alors les mêmes résultats que dans 4.3, à cela près que Hdg est, non plus $\boldsymbol{GL}_2$, mais le groupe multiplicatif de D.

4.5. On suppose que X est *un produit $E_1 \times \cdots \times E_n$ de courbes elliptiques* sans multiplications complexes, deux à deux non isogènes (sur $\bar{K}$), et dont les invariants modulaires ne sont pas des entiers algébriques. Le groupe Hdg est alors le sous-groupe de $\boldsymbol{GL}_2 \times \cdots \times \boldsymbol{GL}_2$ formé des $(s_1, \cdots, s_n)$ tels que $\det(s_1) = \cdots = \det(s_n)$, et $\rho(G_K)$ est ouvert dans $\mathrm{Hdg}(A^f)$.

Le cas $n = 2$ est traité dans [31] ; le cas général se ramène au cas $n = 2$ grâce à un lemme de Ribet [23].

On trouvera également dans Ribet [22] une forme "tordue" de 4.5 : le cas d'une variété abélienne de dimension d ayant pour anneau d'endomorphismes un ordre d'un corps de nombres totalement réel de degré d.

En dehors de ces cas, tous relatifs aux variétés abéliennes, il n'y a guère à signaler que celui des *variétés de Fermat*

$$X_0^n + \cdots + X_r^n = 0 \ ,$$

où le groupe Hdg est un tore, et où l'on peut décrire les (ρ_l) comme dans 4.2 (Weil [41], [42], Deligne).

On aimerait avoir d'autres exemples.

§ 5. Représentations l-adiques, séries de Dirichlet et formes modulaires

Soit (ρ_l) un système de représentations l-adiques du type considéré aux

§§ 2,3. Rappelons (cf. [30]) la définition de la *série de Dirichlet* $L_\rho(s)$ attachée à ce système ; on a :

$$L_\rho(s) = \prod_{v \in \Sigma_K} 1/P_v(Nv^{-s}) ,$$

où P_v est un certain polynôme, à coefficients entiers, de terme constant 1 :

si $v \notin S$, on a $P_v(T) = \det(1 - T\rho_l(\mathrm{Frob}_v)^{-1})$ pour tout $l \neq p_v$,

si $v \in S$, on définit $P_v(T)$ par une recette que l'on trouvera dans [30] (elle fait intervenir certaines conjectures sur la restriction de ρ_l au groupe de décomposition de v, pour $l \neq p_v$).

Je renvoie également à [30] pour la définition du *conducteur* $\mathfrak{f}_\rho$ et du *facteur gamma* $\Gamma_\rho(s)$ du système (ρ_l) ; le conducteur ne dépend que des propriétés locales (conjecturales) des ρ_l aux places de S ; le facteur gamma ne dépend que de la décomposition de Hodge de $H^m(X_C ; C)$ et de l'action des "Frobenius réels" attachés aux places réelles de K. Si D_K désigne le discriminant de K, et $n(\rho)$ le degré de ρ (i.e. le m-ième nombre de Betti de $\bar{X}$), on pose :

$$A_\rho = N(\mathfrak{f}_\rho) \cdot |D_K|^{n(\rho)} \quad \text{et} \quad \Lambda_\rho(s) = A_\rho^{s/2} \Gamma_\rho(s) L_\rho(s) .$$

Par construction, $L_\rho(s)$ et $\Lambda_\rho(s)$ sont holomorphes pour $R(s) > 1 + m/2$. La conjecture principale de [30] est :

C.5.1. *La fonction $\Lambda_\rho(s)$ se prolonge analytiquement en une fonction holomorphe dans tout le plan complexe, à la seule exception* (si m est pair) *des points $s = m/2$ et $s = 1 + m/2$, où elle est méromorphe. Elle satisfait à l'équation fonctionnelle*

$$\Lambda_\rho(m + 1 - s) = \pm \Lambda_\rho(s) .$$

C.5.2. Supposons m pair, et soit r_K le rang du groupe des classes de cohomologie de $\bar{X}$ représentables par des cycles algébriques de codimension $m/2$ rationnels sur K. D'après Tate [38], la fonction $\Lambda_\rho(s)$ devrait avoir un *pôle d'ordre* r_K aux points $s = m/2$ et $s = 1 + m/2$.

C.5.3. On trouvera dans Deligne [6] une généralisation de C.5.1 aux fonctions L de "motifs", ainsi qu'une formule exprimant la constante de l'équation fonctionnelle comme produit de constantes locales, à la Langlands.

C.5.4 (*Valeurs* des $\Lambda_\rho(s)$ en certains entiers). Soit $n \in \boldsymbol{Z}$ tel que $\Gamma_\rho(s)$ et $\Gamma_\rho(m + 1 - s)$ soient holomorphes en $s = n$.[6] Il devrait être possible d'écrire $\Lambda_\rho(n)$ comme produit d'une "période" par un nombre rationnel ayant des propriétés d'interpolation p-adique analogues à celles des nombres de Bernoulli et de Hurwitz (ce qui permettrait de définir des fonctions L *p-adiques*). Bien entendu, cet énoncé n'a de sens que si l'on précise ce que l'on entend par "période", ce que je suis incapable de faire ; toutefois, il existe tellement d'exemples[7] où c'est possible que je ne doute pas qu'il y ait là un phénomène général.

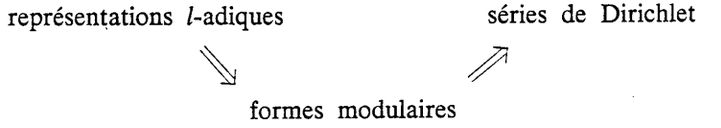
C.5.5. La non-annulation de $L_\rho(s)$ sur la droite

$$R(s) = 1 + m/2$$

est également une question intéressante. On peut espérer en tirer une généralisation de la conjecture de Sato-Tate [38], i.e. (avec les notations de C.3.3) la distribution des classes F_v dans la variété réelle $Cl_H(\boldsymbol{R})$, cf. [27], Chap. I, App.

Lien avec les formes modulaires

La correspondance entre représentations l-adiques et séries de Dirichlet discutée ci-dessus devrait pouvoir se "factoriser" en :



Autrement dit :

C.5.6. Tout système rationnel de représentations l-adiques (ou, plus généralement, tout "motif") devrait définir une forme modulaire sur un groupe réductif G convenable[8] ;

C.5.7. Toute forme modulaire doit définir une série de Dirichlet ayant un prolongement analytique et une équation fonctionnelle analogues à C.5.1.

Dans le cas particulier du système associé à une courbe elliptique définie

6) Cette condition m'a été signalée par Deligne.

7) dus à Euler, Hurwitz, Katz, Kubota, Leopoldt, Manin, Mazur, Rankin, Shimura, Siegel, Swinnerton-Dyer, Zagier . . . et j'en oublie.

8) Lorsque C. 3.3 est vérifiée, on choisit un sous-groupe réductif connexe L de $GL(V_{\boldsymbol{Q}})$ contenant le groupe H, et l'on prend pour G un groupe réductif déployé dont le dual (au sens de Langlands) est égal à L/C ; la forme modulaire correspond au système des classes $F_v \in Cl_L$, comme expliqué dans [14].

sur Q, la conjecture C.5.6 n'est autre que la classique "conjecture de Weil" (cf. [43], ainsi que Taniyama [36]). Elle entre dans le cadre général de la "philosophie de Langlands", cf. [3], [14].

La conjecture C.5.7 est discutée dans Langlands [14] sous une forme plus précise: Langlands part d'une forme modulaire sur G, et d'une représentation linéaire du groupe dual, et leur associe une série de Dirichlet analogue à $\Lambda_\rho(s)$; dans certains cas (dont la liste augmente régulièrement...) on peut prouver que cette série a les propriétés voulues (cf. Borel [3]).

Signalons également que l'on peut (parfois) "inverser" C.5.6 et C.5.7, et passer des séries de Dirichlet aux formes modulaires (Hecke, Weil [42], Jacquet-Langlands, Piateckii-Šapiro, ...) et des formes modulaires aux représentations l-adiques (Deligne [5]).

(Pour plus de détails sur les questions évoquées dans ce § , le lecteur aura intérêt à se reporter au texte de Deligne "*Non-abelian class field theory*" paru dans "Problems of Present Day Mathematics", Proc. Symp. Pure Math. XXVIII, A.M.S., 1976, p. 41–44.)

§ 6. Problèmes relatifs aux courbes elliptiques

Conjecture de Weil

C.6.1 (Taniyama [36], Weil [43]). *Toute courbe elliptique sur Q, de conducteur N, est quotient de la courbe modulaire $X_0(N)$.*

Cette conjecture est corroborée par d'abondants résultats numériques, cf. [35]. Par contre, on ne sait pas grand-chose (ni numériquement, ni conjecturalement) lorsque le corps de base est distinct de Q.

Isogénies

La conjecture suivante est un cas particulier de celle de Tate sur les classes de cohomologie algébriques [38]:

C.6.2. *Deux courbes elliptiques sur K dont les systèmes de représentations l-adiques sont isomorphes sont isogènes.*

Ce n'est démontré que lorsque l'invariant j de l'une des deux courbes n'est pas un entier algébrique (cf. 4.5 ainsi que [27], IV–14). Le cas général résulterait de l'assertion suivante:

C.6.3. *Si S est une partie finie de $\sum_K$, il n'existe qu'un nombre fini* (à isomorphisme près) *de courbes de genre 2 sur K dont les jacobiennes aient bonne réduction en dehors de S.*

Voir là-dessus Paršin [19], [20].

Effectivité

Soit X une courbe elliptique sur K, sans multiplications complexes, et soit $\rho = (\rho_l)$ le système de représentations l-adiques défini par les modules de Tate de X. On peut identifier ρ à un homomorphisme de G_K dans $\boldsymbol{GL}_2(\hat{\boldsymbol{Z}}) = \prod \boldsymbol{GL}_2(\boldsymbol{Z}_l)$, et ρ_l à la l-ième composante de ρ. D'après 4.3, $\rho(G_K)$ est un sous-groupe *ouvert* de $\boldsymbol{GL}_2(\hat{\boldsymbol{Z}})$.

6.4. *Peut-on déterminer $\rho(G_K)$ de façon effective?*

Cela équivaut à:

6.4′. *Peut-on déterminer effectivement un entier $n_{K,X} \geqslant 1$ tel que $\rho(G_K)$ contienne tous les éléments de $\boldsymbol{GL}_2(\hat{\boldsymbol{Z}})$ qui sont congrus à* 1 mod. $n_{K,X}$?

En particulier:

6.4.1. *Peut-on déterminer effectivement les courbes elliptiques qui sont K-isogènes à X?*

6.4.2. *Peut-on déterminer effectivement un entier $m_{K,X}$ tel que $\rho_l(G_K) = \boldsymbol{GL}_2(\boldsymbol{Z}_l)$ pour tout $l > m_{K,X}$?*

Ces problèmes semblent abordables, maintenant que l'on dispose d'une forme effective du théorème de densité de Čebotarev [12].

Uniformité

La question suivante paraît plus hasardeuse:

6.5. *Peut-on choisir l'entier $m_{K,X}$ de* 6.4.2 *indépendamment de X*[9]?

(Par exemple, pour $K = Q$, peut-on prendre $m_{K,X}$ égal à 37 quelle que soit la courbe X?)

La question peut se reformuler en termes de *points rationnels sur des courbes modulaires*. Soient en effet B, N_+ et N_- les sous-groupes de $\boldsymbol{GL}_2(\boldsymbol{F}_l)$ définis ainsi:

$B = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$ = sous-groupe de Borel,

$N_+ = \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix} \cup \begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix}$ = normalisateur de sous-groupe de Cartan déployé,

N_- = normalisateur de sous-groupe de Cartan non déployé.

9) On pourrait se poser la même question pour l'entier $n_{K,X}$ de 6.4′, mais il est facile de voir que la réponse serait "non".

A ces groupes correspondent des courbes modulaires $X_B(l), X_{N+}(l)$, et $X_{N-}(l)$ qui sont définies sur $\boldsymbol{Q}$, cf. [9], chap. IV; les deux premières ne sont autres que les classiques $X_0(l)$ et $X_0^*(l^2)$. La question 6.5 est équivalente[10] à:

6.6. *Existe-t-il un entier n_K tel que, pour tout $l > n_K$, aucune des courbes $X_B(l), X_{N+}(l)$ et $X_{N-}(l)$ n'ait de point rationnel sur K* (à part les "pointes")?

Le seul cas sur lequel on ait des résultats est celui de la courbe $X_B(l) = X_0(l)$, pour $K = \boldsymbol{Q}$ (cf. Mazur [15]).

Répartition des éléments de Frobenius

Supposons, pour simplifier, que $K = \boldsymbol{Q}$, et que la courbe elliptique X considérée n'ait pas de multiplications complexes. Soit S l'ensemble des p en lesquels X a mauvaise réduction. Si $p \notin S$, soit a_p la trace de l'endomorphisme de Frobenius de la réduction de X modulo p; on a

$$\operatorname{Tr} \rho_l(\mathrm{Frob}_p) = a_p \quad \text{et} \quad \det \rho_l(\mathrm{Frob}_p) = p \qquad \text{si } l \neq p\ .$$

Soit $H(U, V)$ un polynôme non nul, en deux variables, sur un corps de caractéristique zéro, et soit P_H l'ensemble des $p \notin S$ tels que $H(a_p, p) = 0$. On déduit facilement de 4.3 (cf. [27], p. IV–13, exerc. 1) que:

6.7. *L'ensemble P_H est de densité* 0.

Autrement dit, si $P_H(x)$ désigne le nombre des $p \leqslant x$ qui appartiennent à P_H, on a

6.7′. $$P_H(x) = o(x/\log x) \qquad \textit{pour } x \to \infty\ .$$

De combien peut-on améliorer cette estimation? Est-il vrai, par exemple, que:

C.6.8. $$P_H(x) = O(x^{1/2}/\log x) \qquad \textit{pour } x \to \infty\ ?$$

Si l'on admet l'hypothèse de Riemann généralisée, on peut montrer, en utilisant [12], que $P_H(x) = O(x^\alpha)$ pour $\alpha = 7/8$, et même pour $\alpha = 5/6$ si $H(U, V)$ est isobare (pour U de poids 1 et V de poids 2).

Le cas où $H(U, V) = U + n$, avec $n \in \boldsymbol{Z}$, est étudié en détail, du point de vue numérique et heuristique, dans Lang-Trotter [13]; il semble que, dans ce cas, on ait

C.6.9. $$P_H(x) \sim C_n x^{1/2}/\log x \qquad \textit{pour } x \to \infty\ ,$$

10) Cela résulte de la classification des sous-groupes de $PGL_2(F_l)$, compte tenu de ce que les groupes "exceptionnels" A_4, S_4 et A_5 ne peuvent pas intervenir lorsque l est assez grand.

pourvu bien sûr qu'il n'existe aucune relation de congruence sur les a_p impliquant que $a_p \div n \neq 0$ pour presque tout p; on trouvera dans [13] la valeur (conjecturale) de la constante C_n. Les cas $n = 0$ et $n = -1$ sont spécialement intéressants.

§ 7. Le cas local: modules de Hodge-Tate

Pour étudier une représentation l-adique, il est précieux de connaître l'action du groupe d'inertie en une place v telle que $p_v = l$. Après changement du corps de base (et remplacement de l par p), cela amène à la situation suivante:

Le corps K est un corps complet pour une valuation discrète v à corps résiduel k algébriquement clos; on suppose k de caractéristique p, et K de caractéristique 0. On note $\overline{K}$ une clôture algébrique de K, et G_K le groupe de Galois de $\overline{K}$ sur K. On s'intéresse à une représentation continue

$$\rho : G_K \longrightarrow \mathrm{Aut}\,(V)\ ,$$

où V est un $\boldsymbol{Q}_p$-espace vectoriel de dimension finie (par exemple $V = H^m(\overline{X}; \boldsymbol{Q}_p)$, où X est une variété projective lisse sur K, cf. § 2).

Soient C le complété de $\overline{K}$, et $V_C = C \otimes V$. Le groupe G_K opère sur V_C par $s \cdot (c \otimes v) = s(c) \otimes \rho(s)v$. On dit que V est un *module de Hodge-Tate* (cf. [25], [28], [39]) s'il existe une base e_i de V_C et des entiers n_i tels que

$$s(e_i) = \chi(s)^{n_i} e_i \qquad \text{pour tout } s \in G_K\ ,$$

où $\chi : G_K \to \boldsymbol{Z}_p^*$ est le caractère qui donne l'action de G_K sur les racines p^m-ièmes de l'unité. Tate [39] a conjecturé:

C.7.1. *Les modules galoisiens $H^m(\overline{X}; \boldsymbol{Q}_p)$ sont des modules de Hodge-Tate.*

C'est vrai pour $m = 1$, d'après Tate [39], complété par Raynaud. Pour $m = 2$, il y a des résultats partiels dus à Artin-Mazur [2]. Le cas général devrait résulter d'une meilleure compréhension des relations entre "cohomologie cristalline" et "cohomologie étale"[11].

Soit V un module de Hodge-Tate. Par définition, V_C possède une graduation analogue à celle de Hodge dans le cas complexe. On en déduit, comme au § 3, un *groupe de Hodge* Hdg_V, qui est un $\boldsymbol{Q}_p$-sous-groupe algébrique connexe de $\boldsymbol{GL}(V)$, non nécessairement réductif. Soit d'autre part H_V le plus

11) C'est de ce côté que devrait également sortir une démonstration des conjectures sur les caractères du groupe d'inertie modérée faites dans [31], p. 278.

petit sous-groupe algébrique de $GL(V)$ contenant $\rho(G_K)$. D'après un théorème de Sen [25], on a:

7.2. a) *Le groupe $\rho(G_K)$ est un sous-groupe ouvert de $H_V(Q_p)$.*
b) *La composante neutre de H_V est égale à* Hdg_V.

En particulier:

7.3. *L'algèbre de Lie de $\rho(G_K)$ est égale à celle de* Hdg_V; *c'est une algèbre de Lie algébrique.*

(La situation est donc plus favorable que dans le cas global.)

Soit HT la $\otimes$-catégorie (au sens de [24]) des modules de Hodge-Tate sur K. Lorsque V parcourt HT, les H_V (resp. les Hdg_V) forment un système projectif. Soit H (resp. Hdg) la limite projective de ce système; c'est un groupe pro-algébrique affine sur Q_p; la $\otimes$-catégorie des représentations linéaires de H est équivalente à HT. On a sur H et Hdg les renseignements suivants (cf. [29]):

7.4. *La composante neutre de H est* Hdg; *le quotient* H/Hdg *s'identifie à G_K* (considéré comme groupe pro-algébrique "constant", de dimension 0).

7.5. *Le groupe* Hdg *ne change pas lorsque l'on remplace K par une extension finie.*

7.6. *Soit* Hdg^{ab} *le quotient de* Hdg *par son groupe des commutateurs. Le groupe* Hdg^{ab} *ne dépend que de p* (mais pas de K): *c'est la limite projective des tores $R_{E/Q_p}(G_m)$, où E parcourt l'ensemble des extensions finies de Q_p.*

(Les assertions 7.4 et 7.5 sont des conséquences immédiates de 7.2; quant à 7.6, c'est une traduction de résultats de Tate, cf. [27], Chap. III, App.)

On sait par contre très peu de choses sur le plus grand quotient *semi-simple* de Hdg. On ne sait même pas quels sont les types de groupes simples qui peuvent intervenir: $A_n, B_n, \cdots, E_8$?

Ici encore, on manque fâcheusement d'exemples.

Bibliographie

[1] Artin, M., Grothendieck, A. et Verdier, J.-L., Théorie des Topos et Cohomologie étale des schémas (SGA 4), Lecture Notes in Math. **269**, **270**, **305**, Springer-Verlag, 1972.

[2] Artin, M. et Mazur, B., Formal groups arising from algebraic varieties, Ann. Sci. E.N.S., à paraître.
[3] Borel, A., Formes automorphes et séries de Dirichlet (d'après R. P. Langlands), Sém. Bourbaki 1974/75, exposé 466, Lecture Notes in Math. **514**, 183–222, Springer-Verlag, 1976.
[4] Borovoi, M. V., Sur l'action du groupe de Galois sur les classes de cohomologie rationnelles de type (p, p) des variétés abéliennes (en russe), Mat. Sbornik, **94** (1974), 649–652.
[5] Deligne, P., Formes modulaires et représentations l-adiques, Sém. Bourbaki 1968/69, exposé 355, Lecture Notes in Math. **179**, 139–186, Springer-Verlag, 1971.
[6] ——, Les constantes des équations fonctionnelles, Sém. Delange-Pisot-Poitou 1969/70, exposé 19 bis. (Voir aussi Lecture Notes in Math. **349**, 501–597, Springer-Verlag, 1973.)
[7] ——, La conjecture de Weil pour les surfaces K3, Inv. Math., **15** (1972), 206–226.
[8] ——, La conjecture de Weil I, Publ. Math. I.H.E.S., **43** (1974), 273–307.
[9] Deligne, P. et Rapoport, M., Les schémas de modules de courbes elliptiques (Proc. Int. Summer School Univ. of Antwerp, RUCA, 1972), Lecture Notes in Math. **349**, 143–316, Springer-Verlag, 1973.
[10] Jacobson, M. I., Variétés abéliennes de dimension deux ayant pour algèbre d'endomorphismes une algèbre de quaternions indéfinie (en russe), Usp. Mat. Nauk, **29** (1974), 185–186.
[11] Kleiman, S., Algebraic cycles and the Weil conjectures, Dix exposés sur la théorie des schémas, 359–386, Masson, Paris et North-Holland, Amsterdam, 1968.
[12] Lagarias, J. C. et Odlyzko, A. M., Effective versions of the Chebotarev density theorem, Proc. Durham Conf., 409–464. Academic Press, 1977.
[13] Lang, S. et Trotter, H., Frobenius Distributions in GL_2-Extensions, Lecture Notes in Math. **504**, Springer-Verlag, 1976.
[14] Langlands, R. P., Euler Products, Yale Univ. Press, 1967.
[15] Mazur, B., Modular curves and the Eisenstein ideal, Publ. Math. I.H.E.S., **47** (1977).
[16] Mumford, D., Families of abelian varieties, Proc. Symp. Pure Math., A.M.S., IX, 1966, 347–351.
[17] ——, A note on Shimura's paper "Discontinuous Groups and Abelian Varieties", Math. Ann., **81** (1969), 345–351.
[18] Ohta, M., On l-adic representations of Galois groups obtained from certain two-dimensional abelian varieties, J. Fac. Sci. Univ. Tokyo, Sec. I.A. **21** (1974), 299–308.
[19] Paršin, A. N., Modèles minimaux des courbes de genre 2, et homomorphismes de variétés abéliennes définies sur un corps de caractéristique finie (en russe), Izv. Akad. Nauk URSS, **36** (1972),67–109 (= Math. USSR Izv. **6** (1972), 65–108).
[20] ——, Correspondances modulaires, hauteurs et isogénies de variétés abéliennes (en russe), Trud. Inst. Math. Steklov, **82** (1973), 211–236 (= Proc. Steklov Inst. of Math., **132** (1973), 223–270).
[21] Piateckii-Šapiro, I. I., Relations entre les conjectures de Hodge et de Tate pour les variétés abéliennes (en russe), Mat. Sbornik, **87** (1971), 610–620 (= Math. USSR Sb. **14** (1971), 615–625).
[22] Ribet, K., Galois action on division points of abelian varieties with many real multiplications, Amer. J. Math., **98** (1976), 751–804.
[23] ——, On l-adic representations attached to modular forms, Inv. Math., **28** (1975), 245–275.

[24] Saavedra Rivano, N., Catégories Tannakiennes, Lecture Notes in Math., **265**, Springer-Verlag, 1972.
[25] Sen, S., Lie algebras of Galois groups arising from Hodge-Tate modules, Ann. of Math., **97** (1973), 160–170.
[26] Serre, J.-P., Sur les groupes de congruence des variétés abéliennes, Izv. Akad. Nauk URSS, **28** (1964), 3–20; II, *ibid.*, **35** (1971), 731–737.
[27] ——, Abelian l-adic representations and elliptic curves, Benjamin, New York, 1968.
[28] ——, Sur les groupes de Galois attachés aux groupes p-divisibles, Proc. Conf. on Local Fields, Driebergen, 1966, Springer-Verlag, 1968, 118–131.
[29] ——Résumé des cours de 1967–1968, Annuaire du Collège de France (1968–1969), 47–50.
[30] ——, Facteurs locaux des fonctions zèta des variétés algébriques (définitions et conjectures), Sém. Delange-Pisot-Poitou 1969/70, exposé 19.
[31] ——, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Inv. Math., **15** (1972), 259–331.
[32] Shimura, G., Local representations of Galois groups, Ann. of Math., **89** (1969), 99–124.
[33] ——, On canonical models of arithmetic quotients of bounded symmetric domains, Ann. of Math., **91** (1970), 144–222.
[34] Shimura, G. et Taniyama, Y., Complex multiplication of abelian varieties, Publ. Math. Soc. Japan, **6**, Tokyo, 1961.
[35] Swinnerton-Dyer, H. P. F. et Birch, B. J., Elliptic curves and modular functions, Lecture Notes in Math., **476**, 2–32, Springer-Verlag, 1975.
[36] Taniyama, Y., Problem 12, *in* "Some Unsolved Problems in Mathematics", Tokyo-Nikko, 1955, 8.[12)]
[37] ——, L-functions of number fields and zeta functions of abelian varieties, J. Math. Soc. Japan, **9** (1957), 330–366 (= *Oeuvres*, 99–130).
[38] Tate, J., Algebraic Cycles and Poles of Zeta Functions, Arithmetical Algebraic Geometry, Harper and Row, New York, 1965, 93–110.
[39] ——, p-divisible groups, Proc. Conf. on Local Fields, Driebergen, 1966, Springer-Verlag 1968, 158–183.
[40] Weil, A., On a certain type of characters of the idèle-class group of an algebraic number field, Proc. Int. Symp. Tokyo-Nikko, 1955, 1–7.
[41] ——, Numbers of solutions of equations in finite fields, Bull. Amer. Math. Soc., **55** (1949), 497–508.

12) Comme ce texte n'a été publié qu'en japonais (dans les *Oeuvres* de Taniyama), je le reproduis pour la commodité du lecteur:

"12. Let C be an elliptic curve defined over an algebraic number field k, and $L_C(s)$ denote the L-function of C over k. Namely

$$\zeta_C(s)=\zeta_k(s)\zeta_k(s-1)/L_C(s)$$

is the zeta function of C over k. If a conjecture of Hasse is true for $\zeta_C(s)$, then the Fourier series obtained from $L_C(s)$ by the inverse Mellin-transformation must be an automorphic form of dimension -2, of some special type (cf. Hecke). If so, it is very plausible that this form is an elliptic differential of the field of that automorphic functions. The problem is to ask if it is possible to prove Hasse's conjecture for C, by going back this considerations, and by finding a suitable automorphic form from which $L_C(s)$ may be obtained. (Y. Taniyama)"

[42] ——, Jacobi sums as "Grössencharaktere", Trans. Amer. Math. Soc., **73** (1952), 487–495.
[43] ——, Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen, Math. Ann., **168** (1967), 149–156.

Collège de France
11, place Marcelin Berthelot
75231 Paris Cedex 05
France

ALGEBRAIC NUMBER THEORY, Papers contributed for the International Symposium, Kyoto 1976; S. Iyanaga (Ed.): Japan Society for the Promotion of Science, Tokyo, 1977

Unitary Groups and Theta Functions

GORO SHIMURA

Our first theme is the theta functions which occur as the Fourier coefficients of automorphic forms. This will eventually lead to the second one: the special values of various zeta functions, especially those associated with cusp forms. The point of contact of these two themes is a certain Eisenstein series, of which the Fourier coefficients are "arithmetic theta functions", and which, evaluated at some points, gives special values of a certain zeta function.

First we define, with a fixed imaginary quadratic field K, a unitary group U by

$$U = \{X \in SL_m(K) \mid {}^t\bar{X}RX = R\} ,$$

$$R = \begin{pmatrix} 0 & 0 & 1_q \\ 0 & S & 0 \\ -1_q & 0 & 0 \end{pmatrix} , \qquad -{}^t\bar{S} = S \in GL_n(K) ,$$

where $m = n + 2q$ with positive integers n and q. We assume that $-iS$ is positive definite. The group acts naturally on the space $\mathfrak{Z}$ consisting of all elements (z, w) of $M_q(\boldsymbol{C}) \times M_{n,q}(\boldsymbol{C})$ such that $i({}^t\bar{z} - z + {}^t\bar{w}Sw)$ is positive definite, where $M_{n,q}(F)$, for any field F, denotes the set of all $n \times q$ matrices with coefficients in F, and $M_n(F) = M_{n,n}(F)$ as usual. If $(z, w) \in \mathfrak{Z}$ and

$$\alpha = \begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{pmatrix} \in U ,$$

then the image of (z, w) under α is defined by

$$\alpha(z, w) = ((a_1z + b_1w + c_1)(a_3z + b_3w + c_3)^{-1} ,$$
$$(a_2z + b_2w + c_2)(a_3z + b_3w + c_3)^{-1}) .$$

Put $j(\alpha ; z, w) = \det(a_3z + b_3w + c_3)$. Then the jacobian of α is $j(\alpha ; z, w)^{-m}$.

For any congruence subgroup Γ of U and a positive integer k, we understand, by an *automorphic form on* $\mathfrak{H}$ *of weight* k *with respect to* Γ, a holomorphic function f on $\mathfrak{H}$ satisfying

$$(1) \qquad f(\gamma(z,w)) = f(z,w)j(\gamma;z,w)^k \qquad \text{for all } \gamma \in \Gamma .$$

Such a function f has an expansion

$$(2) \qquad f(z,w) = \sum_{0 \leqslant r \in B} g_r(w)e(\mathrm{tr}(rz)) ,$$

with holomorphic functions g_r on $M_{n,q}(\boldsymbol{C})$, where $e(x) = e^{2\pi ix}$, and B is a lattice in the vector space

$$\{x \in M_q(K) \mid {}^t\bar{x} = x\} ;$$

we write $0 \leqslant r$ to indicate that r is non-negative. Moreover, each g_r satisfies

$$(3) \qquad g_r(w + l) = e\Big(\frac{1}{2i}H_r\Big(l, w + \frac{1}{2}l\Big)\Big)g_r(w) \qquad \text{for all } l \in L ,$$

where L is a lattice in $M_{n,q}(K)$ depending only on Γ, and H_r is the hermitian form defined by

$$H_r(u,v) = -2i \cdot \mathrm{tr}\,(r \cdot {}^t\bar{u}Sv) \qquad ((u,v) \in M_{n,q}(\boldsymbol{C}) \times M_{n,q}(\boldsymbol{C})) .$$

Thus the "Fourier coefficients" of f are theta functions on $M_{n,q}(\boldsymbol{C})$ with respect to L. Now, in the theory of elliptic modular functions, the modular forms that are important from the number-theoretical viewpoint are those with cyclotomic (or more generally algebraic) Fourier coefficients. This leads us to the following natural question:

Can one define the notion of "arithmetic theta functions" in such a way that the forms f with arithmetic Fourier coefficients behave like elliptic modular forms with cyclotomic Fourier coefficients?

We shall actually show that the answer is affirmative. To define "arithmetic theta functions" in a more general setting, let V be a finite dimensional complex vector space, L a lattice in V, and $H(u,v)$ a non-negative hermitian form on V. We put $E(u,v) = \mathrm{Im}\,(H(u,v))$, and assume that $E(L,L) \subset \boldsymbol{Z}$, i.e., H is a Riemann form. Further let ψ be a map of L into the group of all roots of unity such that

$$\psi(l + l') = \psi(l)\psi(l')e(E(l,l')/2) .$$

Then we consider a "reduced theta function" of type (H, ψ, L) in the sense of Weil [8], which is a holomorphic function $g(u)$ on V satisfying

$$g(u + l) = \psi(l)e\Big(\frac{1}{2i}H\Big(l, u + \frac{1}{2}l\Big)\Big)g(u) \qquad \text{for all } l \in L .$$

Let $T(H, \psi, L)$ denote the set of all such g. For each $g \in T(H, \psi, L)$, put

$$g_*(u) = e\Big(\frac{i}{4}H(u,u)\Big)g(u) .$$

Then g_* is not holomorphic unless $g = 0$, but it satisfies

$$g_*(u + l) = \psi(l)e(E(l,u)/2)g_*(u) \qquad \text{for all } l \in L \text{ and } u \in V .$$

Therefore the restriction of g_* to $\boldsymbol{Q}L$ can be extended to a function on $\boldsymbol{Q}L \otimes_{\boldsymbol{Q}} \boldsymbol{A}$, where $\boldsymbol{A}$ denotes the ring of adeles. It should be noted that g_* is not a function on V/M for any lattice M commensurable with L.

Now suppose that V/L is an abelian variety and $\mathrm{End}\,(V/L) \otimes \boldsymbol{Q}$ is isomorphic to $M_h(F)$ with a CM-field F, where $h = 2 \cdot \dim\,(V)/[F: \boldsymbol{Q}]$. Then we obtain a CM-type (F, Φ) such that h times Φ is the representation of F on V. Let (F', Φ') be the reflex of (F, Φ), and let $T_a(H, \psi, L)$ be the set of all g in $T(H, \psi, L)$ such that $g_*(u) \in F'_{ab}$ for all $u \in \boldsymbol{Q}L$, where F'_{ab} denotes the maximal abelian extension of F'. (It is also meaningful and even advantageous to consider all g such that $g_*(u)$ is algebraic for all $u \in \boldsymbol{Q}L$.) We call the elements of $T_a(H, \psi, L)$ *arithmetic theta functions*. It can be shown that $T(H, \psi, L)$ can be spanned by $T_a(H, \psi, L)$ over $\boldsymbol{C}$. Let $F'^{\times}_{\boldsymbol{A}}$ and $F^{\times}_{\boldsymbol{A}}$ denote the idele groups of F' and F, respectively. We can define a map η of $F'^{\times}_{\boldsymbol{A}}$ into $F^{\times}_{\boldsymbol{A}}$ by $\eta(x) = \det(\Phi'(x))$.

Theorem 1. *Every element x of $F'^{\times}_{\boldsymbol{A}}$ defines a $\boldsymbol{Q}$-linear map $g \mapsto g^x$ of $T_a(H, \psi, L)$ onto $T_a(N(x)H, \psi', \eta(x)^{-1}L)$ satisfying $g_*(u)^x = (g^x)_*(\eta(x)^{-1}u)$ for all $u \in \boldsymbol{Q}L$, where $\psi'(l) = \psi(\eta(x)l)^x$, and $N(x)$ is the norm of the ideal associated with x.*

Here c^x for $c \in F'_{ab}$ denotes the image of c under the element of $\mathrm{Gal}\,(F'_{ab}/F')$ corresponding to x; one should also note that every element of $F^{\times}_{\boldsymbol{A}}$ acts on $\boldsymbol{Q}L \otimes_{\boldsymbol{Q}} \boldsymbol{A}$, and therefore $(g^x)_*(\eta(x)^{-1}u)$ and $\psi(\eta(x)l)$ are meaningful. We can actually generalize the theorem to the case of an abelian variety which is isogenous to the product of several varieties of the above type with different F's. The details will be given in [5].

Let us now come back to the function f of (2) and its Fourier coefficients g_r satisfying (3). Putting $V = M_{n,q}(\boldsymbol{C})$, we observe that $\mathrm{End}\,(V/L) \otimes \boldsymbol{Q}$ is isomorphic to $M_{nq}(K)$, so that the above definitions and results are applicable.

In this case, we have $F = F' = K$ and η is the identity map. Let $\mathcal{M}_k(\Gamma)$ denote the vector space of all f satisfying (1). We call an element f of $\mathcal{M}_k(\Gamma)$ *arithmetic* if $g_\tau \in T_a(H_\tau, 1, L)$ for all r. Let $\mathcal{M}_k^a(\Gamma)$ denote the set of all such f, and $\mathcal{M}_k^a$ the union of $\mathcal{M}_k^a(\Gamma)$ for all congruence subgroups Γ. Further let $\mathfrak{R}$ denote the field of all arithmetic automorphic functions with respect to the algebraic group

$$G = \{X \in GL_m(K) \mid {}^t\bar{X}RX = \nu(X)R \qquad \text{with } \nu(X) \in \boldsymbol{Q}\}$$

in the framework of canonical models as considered in [1], [2]. Then we have

Theorem 2. *The field $K_{ab}\mathfrak{R}$ consists of all the quotients f/g with automorphic forms f and g of the same weight belonging to $\bigcup_{k=1}^{\infty} \mathcal{M}_k^a$.*

We can also prove some theorems concerning the explicit action of a certain subgroup of the adelization of G on $\mathfrak{R}$ and on $\mathcal{M}_k^a$, similar to those in [3], [4].

Let us now consider Eisenstein series in the present setting. Suppose $q = 1$; let Λ be a lattice in $M_{1,m}(K)$, and let μ be an element of $M_{1,m}(K)$. Put

$$X = X(\Lambda, \mu) = \{\lambda \in M_{1,m}(K) \mid \lambda R^{-1} \cdot {}^t\bar{\lambda} = 0\ ,\ 0 \neq \lambda \equiv \mu \bmod \Lambda\}\ .$$

Then we define an Eisenstein series $E_{X,k}$ by

$$E_{X,k}(z, w) = \sum_{(a,b,c) \in X} (az + bw + c)^{-k} \qquad ((z, w) \in \mathfrak{Z})\ ,$$

where $a, c \in K$, and $b \in M_{1,n}(K)$. If $k > 2n + 2$, this is convergent and defines an element of $\mathcal{M}_k(\Gamma)$, where

$$\Gamma = \{\gamma \in U \mid \Lambda\gamma = \Lambda\ ,\ \mu\gamma \equiv \mu \bmod \Lambda\}\ .$$

Our main result about $E_{X,k}$ is

Theorem 3. *Let h be an elliptic modular form of weight k with rational Fourier coefficients at $i\infty$, and τ an element of K with positive imaginary part such that $h(\tau) \neq 0$. Then $\pi^{-k}h(\tau)^{-1}E_{X,k}$ is arithmetic.*

This fact implies some interesting results about the special values of a new type of zeta function of the form

$$\zeta(s; P, d, \mathfrak{a}, k) = \sum x^k |x|^{-2s}\ .$$

Here s is a complex variable, P is the composite of K with a totally real algebraic number field P_0 of degree m, and d is a negative element of P_0 whose all other conjugates are positive; the sum is extended over all x belonging to a lattice $\mathfrak{a}$ in P such that $\mathrm{Tr}_{P_0/\boldsymbol{Q}}(dx\bar{x}) = 0$. The series is convergent for sufficiently large $\mathrm{Re}(s)$, and can be continued to a meromorphic function on the whole s-plane. One interesting feature of this function is that $|x|^2$ is not necessarily a rational integer. Similar zeta functions can be defined with a direct sum of fields in place of P.

We finally mention a result on the special values of the zeta function

$$D(s, f, \varphi) = \sum_{n=1}^{\infty} \varphi(n) a_n n^{-s}\ ,$$

where φ is a primitive Dirichlet character, and f is a cusp form which has an expansion $f(z) = \sum_{n=1}^{\infty} a_n e(nz)$ and satisfies

$$f(\beta(z)) = \chi(d)(cz + d)^k f(z)$$

for all $\beta = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\boldsymbol{Z})$ such that $c \equiv 0 \pmod N$ with a positive integer N; χ is a Dirichlet character modulo N. Suppose that $a_1 = 1$, and f is an eigenfunction of all Hecke operators of level N; suppose further that f is "primitive" in the sense that it cannot be obtained from the forms of lower level. Define the Gauss sum $\mathfrak{g}(\varphi)$ by

$$\mathfrak{g}(\varphi) = \sum_{n=1}^{c} \varphi(n) e(n/c)\ ,$$

where c is the conductor of φ. Then we obtain

Theorem 4. *Let φ and φ' be primitive Dirichlet characters, and f a primitive cusp form as above. Further let m and m' be two positive integers less than k such that $(\varphi\varphi')(-1) = (-1)^{m-m'}$ and $D(m', f, \varphi') \neq 0$. Then*

$$(2\pi i)^{m'-m} \cdot \frac{\mathfrak{g}(\varphi')D(m, f, \varphi)}{\mathfrak{g}(\varphi)D(m', f, \varphi')}$$

is an algebraic number belonging to the field generated over $\boldsymbol{Q}$ by $a_n, \varphi(n)$, and $\varphi'(n)$ for all n.

There is also a complementary result which concerns the case where $(\varphi\varphi')(-1) = (-1)^{m-m'-1}$. For details, the reader is referred to [6], [7].

The proof of Theorem 4 relies on a certain result concerning the special values of a zeta function

$$D(s, f, g) = \sum_{n=1}^{\infty} a_n b_n n^{-s}\ ,$$

which is defined with another modular form $g(z) = \sum_{n=0}^{\infty} b_n e(nz)$. The pull-back of $E_{\chi,k}$ to the upper half plane evaluated at a point belonging to K is a constant times $D(k-1, f, g)$, where f is the Mellin transform of an L-function of K with a Grössen-character and g is a product of two theta series. Although this phenomenon is not so important, nor needed for the proof of the above theorem, it shows at least how these values are intricately connected with each other.

One final remark may be added: the whole theory of arithmetic automorphic forms with respect to a unitary group can be generalized to the case where the basic field K is a totally imaginary quadratic extension of a totally real algebraic number field; also Theorem 4 can be generalized to the zeta functions associated with Hilbert modular forms.

References

[1] Miyake, K., Models of certain automorphic function fields, Acta Math. **126** (1971), 245–307.
[2] Shimura, G., On canonical models of arithmetic quotients of bounded symmetric domains, I, II, Ann. of Math. **91** (1970), 144–222; **92** (1970), 528–549.
[3] ——, On some arithmetic properties of modular forms of one and several variables, Ann. of Math. **102** (1975), 491–515.
[4] ——, On the Fourier coefficients of modular forms of several variables, Göttingen Nachr. Akad. Wiss. 1975, 261–268.
[5] ——, Theta functions with complex multiplication, Duke Math. J. **43** (1976), 673–696.
[6] ——, The special values of the zeta functions associated with cusp forms, Comm. Pure and Appl. Math. **29** (1976), 783–804.
[7] ——, On the periods of modular forms, to appear in Math. Ann.
[8] Weil, A., Introduction à l'étude des variétés kählériennes, Hermann, Paris, 1958.

Department of Mathematics
Princeton University
Princeton, New Jersey 08540
U.S.A.

ALGEBRAIC NUMBER THEORY, Papers contributed for the International Symposium, Kyoto 1976; S. Iyanaga (Ed.): Japan Society for the Promotion of Science. Tokyo. 1977

On Values at $s = 1$ of Certain L Functions of Totally Real Algebraic Number Fields[1)]

TAKURO SHINTANI

Introduction

0.1. Let F be a *totally real* algebraic number field of degree n and let χ be a character of the group of narrow ideal classes modulo $\mathfrak{f}$ of F. Denote by $L_F(s, \chi)$ the Hecke L-function of F associated with the character χ. *Assuming that χ is primitive and the gamma factor in the functional equation for $L_F(s, \chi)$ is $\Gamma(s/2)\Gamma((s+1)/2)^{n-1}$*, we derive a formula for $L_F(1, \chi)$. The formula represents $L_F(1, \chi)$ as a finite linear combination of logarithms of special values of *multiple gamma functions* which were introduced and studied by E. W. Barnes in [2]. In particular, when χ corresponds to a quadratic extension of F in which only one of n real primes of F splits, the formula is a generalization of the Dirichlet class number formula for real quadratic fields. When F is real quadratic, the formula was obtained in our previous paper [5].

In his Nice Congress talk [6], H. M. Stark conjectured that, under our assumptions, $L_F(1, \chi)$ would be a linear form with elementary coefficients in logarithms of units of certain abelian extension of F. In view of the conjecture, our result may be of some interest.

0.2. The present paper consists of three sections. In § 1, we summarize basic definitions and properties of multiple gamma functions. In § 2, we evaluate the derivative at $s = 0$, of the following Dirichlet series:

$$(0.1) \qquad \sum_{z_1, \cdots, z_r = 0}^{\infty} \prod_{j=1}^{n} \{L_j^*(z_1 + x_1, \cdots, z_r + x_r)^{-s}\} ,$$

where $L_1^*, L_2^*, \cdots, L_n^*$ are linear forms with positive coefficients and $x = (x_1,$

1) The result presented at the time of the conference has appeared in [4]. In the present article, a relevant result obtained after the Symposium is exposed.

$\cdots, x_r) \neq 0$ is an r-tuple of non-negative real numbers. In § 3., our formula for $L_F(1, \chi)$ is derived. Under our assumption, $L_F(1, \chi)$ is equal to, up to an elementary factor, $\left[\left(\frac{d}{ds}\right)L_F(s, \chi)\right]_{s=0}$. On the other hand, it is shown in [4] (see also Zagier [7]) that $L_F(s, \chi)$ is a finite linear combination of Dirichlet series of type (0.1).
Thus, the result of § 2 yields our formula for $L_F(1, \chi)$.

Notation. As usual, we denote by $\boldsymbol{Z}$, $\boldsymbol{Q}$, $\boldsymbol{R}$ and $\boldsymbol{C}$ the ring of integers, the field of rational numbers, the field of real numbers and the field of complex numbers. Further, $\boldsymbol{Z}_+$ denotes the set of non-negative integers. The set of positive rational (resp. real) numbers is denoted by $\boldsymbol{Q}_+$ (resp. $\boldsymbol{R}_+$).
We denote by $\Gamma(s)$ the gamma function, by $B_m(x)$ the m-th. Bernoulli polynomial and by γ the Euler constant.

§ 1. We recall definitions and basic properties of *multiple gamma functions* introduced and studied by Barnes in [2].

For an r-tuple $\omega = (\omega_1, \omega_2, \cdots, \omega_r)$ of positive numbers and for a positive number a, we denote by $\zeta_r(s, \omega, a)$ the multiple Riemann zeta function given by $\zeta_r(s, \omega, a) = \sum_{\Omega} (a + \Omega)^{-s}$, where the summation with respect to Ω is over all the *non-negative* integral linear combinations $\Omega = m_1\omega_1 + m_2\omega_2 + \cdots + m_r\omega_r$ $(m_1, \cdots, m_r \in \boldsymbol{Z}_+)$ of $\omega_1, \omega_2, \cdots, \omega_r$. It is known that the Dirichlet series $\zeta_r(s, \omega, a)$ is absolutely convergent if $\operatorname{Re} s > r$ and is continued analytically to a meromorphic function in the whole complex plane which is entire except for simple poles at $s = 1, 2, \cdots, r$.

Put

$$-\log \rho_r(\omega) = \lim_{a \to +0} \left[\frac{\partial}{\partial s}\zeta_r(s, \omega, a)\right]_{s=0} + \log a\,.$$

Further, set

$$\left[\frac{\partial}{\partial s}\zeta_r(s, \omega, a)\right]_{s=0} = \log\left\{\frac{\Gamma_r(a, \omega)}{\rho_r(\omega)}\right\}.$$

It is proved that, as a function of a, $\Gamma_r(a, \omega)^{-1}$ is extended to an entire function of order r of a.

Put

$$-\gamma_{rq}(\omega) = \lim_{a \to +0}\left\{(-1)^{q-1}\frac{(q-1)!}{a^q} + \frac{\partial^q}{\partial a^q}\log \Gamma_r(a, \omega)\right\}$$

for $q = 1, 2, \cdots, r$. Then it is known that $\Gamma_r(a, \omega)^{-1}$ has the following canonical product expression:

$$\Gamma_r(a, \omega)^{-1} = \exp\left(a\gamma_{r1} + \frac{a^2}{2!}\gamma_{r2} + \cdots + \frac{a^r}{r!}\gamma_{rr}\right) \times a \prod{}' \left(1 + \frac{a}{\Omega}\right)\exp\left\{-\frac{a}{\Omega} + \frac{a^2}{2\Omega^2} + \cdots + \frac{(-1)^r a^r}{r\Omega^r}\right\}, \tag{1}$$

where the product is over all the non-negative integral linear combinations $\Omega = m_1\omega_1 + m_2\omega_2 + \cdots + m_r\omega_r \neq 0$ $(m_1, \cdots, m_r \in \boldsymbol{Z}_+)$ of $\omega_1, \omega_2, \cdots, \omega_r$.

For an integer i $(1 \leqslant i \leqslant r)$, we denote by $\check{\omega}(i)$ the $(r-1)$-tuple of positive numbers given by $\check{\omega}(i) = (\omega_1, \cdots, \omega_{i-1}, \omega_{i+1}, \cdots, \omega_r)$. Then the multiple gamma function $\Gamma_r(a, \omega)$ satisfies the following difference equations:

$$\Gamma_r(a + \omega_i, \omega) = \rho_{r-1}(\check{\omega}(i))\Gamma_{r-1}(a, \check{\omega}(i))^{-1}\Gamma_r(a, \omega) \qquad (i = 1, 2, \cdots, r)\,. \tag{2}$$

For a positive number ε, denote by $I(\varepsilon, +\infty)$ the integral path in the complex plane consisting of the line segment $(+\infty, \varepsilon)$, the counterclockwise circle of radius ε around the origin and the line segment $(\varepsilon, +\infty)$.
If $0 < \varepsilon < 2\pi/\omega_i$ for $i = 1, 2, \cdots, r$, then we have the following integral representation for $\log\{\Gamma_r/\rho_r\}$,

$$\log\left\{\frac{\Gamma_r(a, \omega)}{\rho_r(\omega)}\right\} = \frac{1}{2\pi\sqrt{-1}}\int_{I(\varepsilon, +\infty)} \frac{\exp(-at)}{\prod_{i=1}^{r}\{1 - \exp(-\omega_i t)\}}\frac{\log t}{t}dt + (\gamma - \pi\sqrt{-1})\zeta_r(0, \omega, a)\,, \tag{3}$$

where $\log t$ is understood to be real valued on the upper line segment $(+\infty, \varepsilon)$ on $I(\varepsilon, +\infty)$.

Remark. For $r = 1$,

$$\frac{\Gamma_1(a, \omega)}{\rho_1(\omega)} = \frac{1}{\sqrt{2\pi}}\Gamma\left(\frac{a}{\omega}\right)\exp\left\{\left(\frac{a}{\omega} - \frac{1}{2}\right)\log(\omega)\right\}.$$

For $r = 2$, $\Gamma_2(a, \omega)$ is the double gamma function studied in [1] (see also § 1 of [5]).

§ 2. Let $A = (a_{ij})$ $(1 \leqslant i \leqslant r,\ 1 \leqslant j \leqslant n)$ be an $r \times n$ matrix with *positive* entries and let $x = (x_1, x_2, \cdots, x_r)$ be an r-tuple of non-negative numbers. We assume that $x \neq 0$. Set

$$\zeta(s, A, x) = \sum_{z}\prod_{j=1}^{n}\left\{\sum_{i=1}^{r} a_{ij}(z_i + x_i)\right\}^{-s}, \tag{4}$$

where the summation with respect to z is over all the r-tuples $z = (z_1, \cdots, z_r)$

of non-negative integers. The Dirichlet series $\zeta(s, A, x)$ is absolutely convergent if $\mathrm{Re}\, s > r/n$ and has an analytic continuation to a meromorphic function in the whole complex plane. For each j $(1 \leqq j \leqq n)$, set $\omega^{(j)} = (a_{1j}, a_{2j}, \cdots, a_{rj})$ and $z(x)^{(j)} = \sum_{k=1}^{r} a_{kj}x_k$. If $n = 1$, it is easy to see that $\zeta(s, A, x) = \zeta_r(s, \omega^{(1)}, z(x)^{(1)})$. Furthermore, for each r-tuple $l = (l_1, \cdots, l_r)$ of non-negative integers, set

$$C_l(A) = \sum_{(j,k)} \int_0^1 \left\{ \prod_{i=1}^{r} (a_{ij} + a_{ik}u)^{l_i - 1} - \prod_{i=1}^{r} a_{ij}^{l_i - 1} \right\} \frac{du}{u} , \tag{5}$$

where the summation with respect to (j, k) is over all pairs (j, k) of positive integers which satisfy the conditions $1 \leqq j,\ k \leqq n$ and $j \neq k$.

Proposition 1 (cf. Proposition 1′ of [4] and Proposition 3 of [5]). *The notation being as above,*

$$\left[\frac{d}{ds}\zeta(s, A, x)\right]_{s=0} = \log\left\{\prod_{j=1}^{n} \frac{\Gamma_r(z(x)^{(j)}, \omega^{(j)})}{\rho_r(\omega^{(j)})}\right\} + \frac{(-1)^r}{n} \sum_{l} C_l(A) \prod_{i=1}^{r} \left\{\frac{B_{l_i}(x_i)}{l_i!}\right\} ,$$

where the summation with respect to l is over all the r-tuples of non-negative integers which satisfy the equality $l_1 + l_2 + \cdots + l_r = r$.

Proof (cf. the proof of Proposition 3 of [5]). Set

$$g(t) = g(t_1, \cdots, t_n) = \prod_{i=1}^{r} \frac{\exp\{(1 - x_i)L_i(t)\}}{\exp\{L_i(t)\} - 1} ,$$

where $L_i(t) = a_{i1}t_1 + a_{i2}t_2 + \cdots + a_{in}t_n$ $(1 \leqq i \leqq r)$. Then we have the following integral representation for $\zeta(s, A, x)$ $(\mathrm{Re}\, s > r/n)$.

$$\Gamma(s)^n \zeta(s, A, x) = \int_0^\infty dt_1 \cdots \int_0^\infty dt_n\, g(t)(t_1 \cdots t_n)^{s-1} . \tag{6}$$

For $j = 1, 2, \cdots, n$, put

$$D_j = \{(t_1, t_2, \cdots, t_n) \in \boldsymbol{R}_+^n ;\ t_1, t_2, \cdots, t_{j-1}, t_{j+1}, \cdots, t_n \leqq t_j\} .$$

For a positive number $\varepsilon < 1$, let $I(\varepsilon, +\infty)$ be the integral path introduced at the end of § 1 and let $I(\varepsilon, 1)$ be the integral path consisting of the line segment $[1, \varepsilon]$, the counterclockwise circle of radius ε around the origin and the line segment $[\varepsilon, 1]$. *If ε is sufficiently small,* we have

$$\begin{aligned} &\int_{D_j} g(t)(t_1 \cdots t_n)^{s-1} dt_1 \cdots dt_n \\ &= \{\exp(2n\pi\sqrt{-1}s) - 1\}^{-1} \{\exp(2\pi\sqrt{-1}s) - 1\}^{1-n} \\ &\quad \times \int_{I(\varepsilon, +\infty)} t^{ns-1} dt \int_{I(\varepsilon,1)^{n-1}} g_j(t, u)(u_1u_2 \cdots u_{n-1})^{s-1} du_1 \cdots du_{n-1} , \end{aligned} \tag{7}$$

where we put $g_j(t, u) = g(tu_1, \cdots, tu_{j-1}, t, tu_j, \cdots, tu_{n-1})$ $(j = 1, 2, \cdots, n)$.

It follows from (6) and (7) that

$$\zeta(0, A, x) = \frac{1}{2\pi\sqrt{-1}n} \sum_{j=1}^{n} \int_{I(\varepsilon, +\infty)} g_j(t, 0) \frac{dt}{t} . \tag{8}$$

Furthermore,

$$\begin{aligned} &\left[\frac{d}{ds}\zeta(s, A, x)\right]_{s=0} \\ &= \{\gamma n - (2n - 1)\pi\sqrt{-1}\}\zeta(0, A, x) \\ &\quad + \frac{1}{2\pi\sqrt{-1}} \sum_{j=1}^{n} \int_{I(\varepsilon, +\infty)} \prod_{i=1}^{r} \left\{\frac{\exp(1 - x_i)a_{ij}t}{\exp(a_{ij}t) - 1}\right\} \frac{\log t}{t} dt \\ &\quad + \frac{1}{(2\pi\sqrt{-1})^2} \frac{1}{n} \sum_{j=1}^{n} \sum_{k \neq j} \int_{I(\varepsilon, -\infty)} \frac{1}{t} \int_{I(\varepsilon,1)} g_{jk}(t, u) \frac{\log u}{u} du dt \end{aligned}$$

where we put

$$g_{jk}(t, u) = \prod_{i=1}^{r} \frac{\exp\{(1 - x_i)t(a_{ij} + a_{ik}u)\}}{\exp\{(a_{ij} + a_{ik}u)t\} - 1} \qquad (1 \leqq j,\ k \leqq n,\ j \neq k) .$$

It is easy to see that

$$\begin{aligned} &\frac{1}{2\pi\sqrt{-1}} \int_{I(\varepsilon,1)} g_{jk}(t, u) \frac{\log u}{u} du \\ &\quad = \pi\sqrt{-1} g_{jk}(t, 0) + \frac{1}{2\pi\sqrt{-1}} \int_{I(\varepsilon,1)} \{g_{jk}(t, u) - g_{jk}(t, 0)\} \frac{\log u}{u} du . \end{aligned}$$

Since $g_{jk}(t, 0) = g_j(t, 0)$, it follows from (8) that

$$\frac{1}{2\pi\sqrt{-1}n} \sum_{j=1}^{n} \sum_{k \neq j} \int_{I(\varepsilon, +\infty)} g_{jk}(t, 0) \frac{dt}{t} = (n - 1)\zeta(0, A, x) .$$

Moreover

$$\begin{aligned} &\frac{1}{(2\pi\sqrt{-1})^2} \int_{I(\varepsilon, +\infty)} \frac{dt}{t} \int_{I(\varepsilon,1)} \{g_{jk}(t, u) - g_{jk}(t, 0)\} \frac{\log u}{u} du \\ &\quad = \frac{1}{2\pi\sqrt{-1}} \sum_{l} \prod_{i=1}^{r} \left\{\frac{B_{l_i}(1 - x_i)}{l_i!}\right\} \\ &\qquad \times \int_{I(\varepsilon,1)} \left\{\prod_{i=1}^{r} (a_{ij} + a_{ik}u)^{l_i - l} - \prod_{i=1}^{r} a_{ij}^{l_i - 1}\right\} \frac{\log u}{u} du \\ &\quad = \sum_{l} \prod_{i=1}^{r} \left\{\frac{B_{l_i}(x_i)}{l_i!}(-1)^{l_i}\right\} \\ &\qquad \times \int_0^1 \left[\prod_{i=1}^{r} (a_{ij} + a_{ik}u)^{l_i - 1} - \prod_{i=1}^{r} (a_{ij}^{l_i - 1})\right] \frac{du}{u} \end{aligned}$$

where the summation with respect to l is over all the r-tuples $l = (l_1, l_2, \cdots, l_r)$ of non-negative integers which satisfy $l_1 + \cdots + l_r = r$.
On the other hand, it follows from (3) that

$$\frac{1}{2\pi\sqrt{-1}} \sum_{j=1}^{n} \int_{I(\varepsilon,+\infty)} \prod_{i=1}^{r} \left[\frac{\exp\{(1-x_i)ta_{ij}\}}{\exp(ta_{ij}) - 1} \right] \frac{\log t}{t} dt$$
$$= \log \left\{ \prod_{j=1}^{n} \frac{\Gamma_r(\sum_{i=1}^{r} x_i a_{ij}, (a_{1j}, \cdots, a_{rj}))}{\rho_r(a_{1j}, \cdots, a_{rj})} \right\}$$
$$+ (\pi\sqrt{-1} - \gamma) \sum_{j=1}^{n} \zeta_r\left(0, (a_{1j}, \cdots, a_{rj}), \sum_{i=1}^{r} x_i a_{ij}\right) .$$

The equality (8) implies that

$$\sum_{j=1}^{n} \zeta_r\left(0, (a_{1j}, \cdots, a_{rj}), \sum_{i=1}^{r} x_i a_{ij}\right) = n\zeta(0, A, x) .$$

Thus, we obtain the proposition.

Remark. For each r-tuples of non-negative integers $l = (l_1, \cdots, l_r)$, $C_l(A)$ is expressed as an elementary function of $a_{11}, a_{12}, \cdots, a_{rn}$. *Assume that,* $l_1 + \cdots + l_r = r$ and set

$$T_1 = \{i;\ 1 \leqslant i \leqslant r,\ l_i > 1\} \quad \text{and} \quad T_2 = \{i;\ 1 \leqslant i \leqslant r;\ l_i = 0\} .$$

For simplicity assume that for any

$$p, q \in T_2\ (p \neq q),\ \prod_{1 \leqslant j < k \leqslant n} (a_{pj}a_{qk} - a_{pk}a_{qj}) \neq 0 .$$

Then

$$C_l(A) = \sum_{p \in T_2} \sum_{1 \leqslant j < k \leqslant n} \frac{\prod_{i \in T_1} (a_{ij}a_{pk} - a_{ik}a_{pj})^{l_i - 1}}{a_{pj}a_{pk} \prod_{p \neq q \in T_2} (a_{qj}a_{pk} - a_{qk}a_{pj})} \log\left(\frac{a_{pj}}{a_{pk}}\right) .$$

§ 3. 1. Let F be a *totally real* algebraic number field of degree n. Let $x \mapsto x^{(i)}$ $(i = 1, 2, \cdots, n;\ x \in F)$ be n different embeddings of x into the real number field $\boldsymbol{R}$. *Embed F into $\boldsymbol{R}^n$ via the mapping*: $x \mapsto (x^{(1)}, x^{(2)}, \cdots, x^{(n)})$. By componentwise multiplication, the group $F - \{0\}$ operates on $\boldsymbol{R}^n$. Denote by E_+ and by $\mathfrak{o}(F)$ the group of totally positive units of F and the ring of integers of F, respectively. For linearly independent vectors $v_1, v_2, \cdots, v_r$ of $\boldsymbol{R}^n$ $(1 \leqslant r \leqslant n)$, denote by $C(v_1, v_2, \cdots, v_r)$ the *open simplicial cone* of dimension r *with the generators* $v_1, v_2, \cdots, v_r$. More precisely,

$$C(v_1, v_2, \cdots, v_r) = \left\{ \sum_{i=1}^{r} c_i v_i ;\ c_1, \cdots, c_r > 0 \right\} .$$

Set $\mathfrak{o}(F)_+ = \boldsymbol{R}^n_+ \cap \mathfrak{o}(F)$.

It is known (see Proposition 4 of [4]) that there exists a *finite system* of open simplicial cones $\{C_j;\ j \in J\}$ (J is a *finite* set of indices) *with generators all in* $\mathfrak{o}(F)_+$ such that

$$\boldsymbol{R}^n_+ = \bigcup_{u \in E_+} \bigcup_{j \in J} uC_j \qquad \text{(disjoint union)} , \tag{9}$$

where $C_j = C_j(v_{j1}, v_{j2}, \cdots, v_{jr(j)})$ $(v_{j1}, v_{j2} \cdots, v_{jr(j)} \in \mathfrak{o}(F)_+)$.

We choose and fix such a system of open simplicial cones together with their generators in $\mathfrak{o}(F)_+$ *once and for all.*

Let $\mathfrak{f}$ be an integral ideal of F and let χ be a character of the group of *narrow* ideal classes modulo $\mathfrak{f}$ of F. Denote by $L_F(s, \chi)$ the Hecke L-function of F associated with the character χ:

$$L_F(s, \chi) = \sum_{\mathfrak{g}} \chi(\mathfrak{g}) N(\mathfrak{g})^{-s} \qquad (\mathrm{Re}\, s > 1) ,$$

where the summation with respect to $\mathfrak{g}$ is over all the integral ideals of F.

Choose a complete set of representatives $\mathfrak{a}_1, \mathfrak{a}_2, \cdots, \mathfrak{a}_{h_0}$ *of the group of narrow ideal classes of F so that* $\mathfrak{a}_1, \mathfrak{a}_2, \cdots, \mathfrak{a}_{h_0}$ *are all integral ideals of F.*

For each $j \in J$ (J is the set of indices for our system of open simplicial cones) and for each $\mathfrak{a}_i$ $(1 \leqslant i \leqslant h_0)$, set

$$R(C_j, (\mathfrak{a}_i\mathfrak{f})^{-1})$$
$$= \left\{ x \in \boldsymbol{R}^{r(j)};\ 0 < x_1, \cdots, x_{r(j)} \leqslant 1,\ \sum_{k=1}^{r(j)} x_k v_{jk} \in (\mathfrak{a}_i\mathfrak{f})^{-1} \right\} \tag{10}$$
$$(r(j) \text{ is the dimension of } C_j) .$$

Since $v_{j1}, \cdots, v_{jr(j)}$ are all in $\mathfrak{o}(F)$ and are linearly independent over $\boldsymbol{R}$, it is easy to see that $R(C_j, (\mathfrak{a}_i\mathfrak{f})^{-1})$ is a finite subset of $\boldsymbol{Q}^{r(j)}$.

For each $x \in R(C_j, (\mathfrak{a}_i\mathfrak{f})^{-1})$, set

$$z(x) = \sum_{k=1}^{r(j)} x_k v_{jk} . \tag{11}$$

Furthermore, for each $j \in J$, denote by A_j the $r(j) \times n$ matrix whose (k, l)-entry is $v_{jk}^{(l)}$ $(1 \leqslant k \leqslant r(j),\ 1 \leqslant l \leqslant n)$:

$$A_j = \begin{pmatrix} v_{j1}^{(1)} & \cdots & v_{j1}^{(n)} \\ v_{jr(j)}^{(1)} & \cdots & v_{jr(j)}^{(n)} \end{pmatrix} . \tag{12}$$

Lemma 2. *The notation being as above,*

$$L_F(s,\chi)=\sum_{i=1}^{h_0}N(\mathfrak{a}_i\mathfrak{f})^{-s}\sum_{j\in J}\sum_{x}\chi(\mathfrak{a}_i\mathfrak{f}z(x))\zeta(s,A_j,x)$$

where the summation with respect to x is over $R(C_j,(\mathfrak{a}_i\mathfrak{f})^{-1})$.

Proof. It follows from the definition of $L_F(s,\chi)$ that

$$L_F(s,\chi)=\sum_{i=1}^{h_0}\sum_{\mu}\chi(\mathfrak{a}_i\mathfrak{f}(\mu))N(\mathfrak{a}_i\mathfrak{f}(\mu))^{-s},$$

where the summation with respect to μ is over all totally positive numbers in $(\mathfrak{a}_i\mathfrak{f})^{-1}$ which are not associated with each other under the action of the group E_+. In view of (9), we have

$$\sum_{\mu}\chi(\mathfrak{a}_i\mathfrak{f}(\mu))N(\mu)^{-s}=\sum_{j\in J}\sum_{\mu\in(\mathfrak{a}_i\mathfrak{f})^{-1}\cap C_j}\chi(\mathfrak{a}_i\mathfrak{f}(\mu))N(\mu)^{-s}.$$

Since both $\mathfrak{a}_i$ and $\mathfrak{f}$ are integral and the generators $v_{j1},\cdots,v_{jr(j)}$ are all in $\mathfrak{o}(F)_+$, each $\mu\in(\mathfrak{a}_i\mathfrak{f})^{-1}\cap C_j$ is uniquely written in the form

$$\mu=\sum_{k=1}^{r(j)}(x_k+z_k)v_{jk}, \tag{13}$$

where

$$x=(x_1,\cdots,x_{r(j)})\in R(C_j,(\mathfrak{a}_i\mathfrak{f})^{-1})$$

and

$$z=(z_1,\cdots,z_{r(j)})\in Z_+^{r(j)}.$$

On the other hand, for each $x\in R(C_j,(\mathfrak{a}_i\mathfrak{f})^{-1})$ and each $z\in Z_+^{r(j)}$, (13) gives an element of $(\mathfrak{a}_i\mathfrak{f})^{-1}\cap C_j$. Since χ is a character modulo $\mathfrak{f}$,

$$\begin{aligned}\chi(\mathfrak{a}_i\mathfrak{f}(\mu))&=\chi\Big(\mathfrak{a}_i\mathfrak{f}\Big(\sum_{k=1}^{r(j)}x_kv_{jk}\Big)\Big)\\&=\chi(\mathfrak{a}_i\mathfrak{f}(z(x)).\end{aligned}$$

Thus

$$\begin{aligned}&\sum_{\mu\in(\mathfrak{a}_i\mathfrak{f})^{-1}\cap C_j}\chi(\mathfrak{a}_i\mathfrak{f}(\mu))N(\mu)^{-s}\\&\quad=\sum_{x}\chi(\mathfrak{a}_i\mathfrak{f}(z(x)))\sum_{z}\prod_{m=1}^{n}\Big\{\sum_{k=1}^{r(j)}(x_k+z_k)v_{jk}^{(m)}\Big\}^{-s}\end{aligned}$$

where the summation with respect to z is over $Z_+^{r(j)}$ and the summation with respect to x is over $R(C_j,(\mathfrak{a}_i\mathfrak{f})^{-1})$. The Lemma now follows from (4).

Since χ is a character of the group of narrow ideal classes modulo $\mathfrak{f}$ of

F, there exists a subset S of the set of indices $\{1,2,3,\cdots,n\}$ and a character χ_0 of the group of invertible residue classes modulo $\mathfrak{f}$ such that

$$\chi((x))=\chi_0(x)\prod_{i\in S}(\operatorname{sgn}x^{(i)}) \tag{14}$$

for any integral principal ideal (x) of F.

Let $n_1=|S|$ be the cardinality of the set S and put

$$\xi(s,\chi)=\sqrt{\frac{dN(\mathfrak{f})^s}{\pi^n}}L_F(s,\chi)\Gamma\Big(\frac{s}{2}\Big)^{n-n_1}\Gamma\Big(\frac{s+1}{2}\Big)^{n_1},$$

where d is the discriminant of F. It is known (see [3]) that if χ is primitive, $\xi(s,\chi)$ satisfies the following functional equation:

$$\xi(1-s,\chi)=w(\chi)\xi(s,\chi^{-1}), \tag{15}$$

where $w(\chi)$ is a complex number of modulus 1 which depends only upon χ. For each $j\in J$, set

$$\omega_j^{(i)}=(v_{j1}^{(i)},v_{j2}^{(i)},\cdots,v_{jr(j)}^{(i)})\in\boldsymbol{R}_+^{r(j)}\qquad(i=1,2,,\cdots,n). \tag{16}$$

Furthermore, for each $x\in R(C_j,(\mathfrak{a}_i\mathfrak{f})^{-1})$, put

$$z(x)^{(m)}=\sum_{k=1}^{r(j)}x_kv_{jk}^{(m)}\in\boldsymbol{R}_+ \tag{17}$$

and

$$\chi_i(z(x))=\chi(\mathfrak{a}_i\mathfrak{f}(z(x)). \tag{18}$$

Theorem 1 (cf. Theorem 1 of [5] and Theorem 3 of [4]). *Let χ be a non-principal primitive character of the group of narrow ideal classes modulo $\mathfrak{f}$ of F of the form* (14) *with $n_1=|S|=n-1$. Then*

$$\begin{aligned}&w(\chi)^{-1}\frac{\sqrt{dN(\mathfrak{f})}}{2\pi^{n-1}}L_F(1,\chi)\\&=\sum_{i=1}^{h_0}\sum_{j\in J}\sum_{x}\chi_i(z(x))^{-1}\log\Big\{\prod_{m=1}^{n}\frac{\Gamma_{r(j)}(z(x)^{(m)},\omega_j^{(m)})}{\rho_{r(j)}(\omega_j^{(m)})}\Big\}\\&\quad+\frac{1}{n}\sum_{i=1}^{h_0}\sum_{j\in J}(-1)^{r(j)}\sum_{x}\chi_i(z(x))^{-1}\sum_{l}C_l(A_j)\Big\{\prod_{k=1}^{r(j)}\frac{B_{l_k}(x_k)}{l_k!}\Big\}\end{aligned} \tag{19}$$

where the summation with respect to x is over $R(C_j,(\mathfrak{a}_i\mathfrak{f})^{-1})$ and the summation with respect to l is over all the $r(j)$-tuples of non-negative integers $l=(l_1,l_2,\cdots,l_{r(j)})$ such that $l_1+l_2+\cdots+l_{r(j)}=r(j)$ (for notations see (9), (15), (18), (11), (10), (3), (16), (17), (12) *and* (5)).

Proof. Since χ is non-principal and primitive and is of the form (14) with $n_1 = |S| = n - 1$, $L_F(s, \chi)$ is an entire function of s and $L_F(1, \chi) \neq 0$. Hence, the functional equation (15) implies that $s = 0$ is a simple zero of $L_F(s, \chi)$. Let λ be an arbitrary character of the group of narrow ideal classes of F. Then it is easy to see that $\chi\lambda$ is also a primitive character of the group of narrow ideal classes modulo $\mathfrak{f}$ of F and that $L_F(0, \chi\lambda) = 0$. It follows from Lemma 2 that

$$\sum_{i=1}^{h_0} \lambda(\mathfrak{a}_i\mathfrak{f}) \sum_{j \in J} \sum_{x} \chi(\mathfrak{a}_i\mathfrak{f}(z(x)))\zeta(0, A_j, x) = 0 ,$$

where the summation with respect to x is over the finite set $R(C_j, (\mathfrak{a}_i\mathfrak{f})^{-1})$.

Since the above equality holds for any λ, we have

$$\sum_{j \in J} \sum_{x \in R(C_j, (\mathfrak{a}_i\mathfrak{f})^{-1})} \chi(\mathfrak{a}_i\mathfrak{f}(z(x)))\zeta(0, A_j, x) = 0 \qquad (i = 1, 2, \cdots, h_0) . \tag{20}$$

The functional equation (15) implies that

$$\frac{\sqrt{dN(\mathfrak{f})}}{2\pi^{n-1}} L_F(1, \chi) = w(\chi)\left[\frac{d}{ds} L_F(s, \chi^{-1})\right]_{s=0} .$$

The Theorem now follows easily from Proposition 1, Lemma 2 and the equality (20).

Remark 1. Take an open simplicial cone C_j $(j \in J)$ of dimension n. Let $R'(C_j, (\mathfrak{a}_i\mathfrak{f})^{-1})$ be the subset of $R(C_j, (\mathfrak{a}_i\mathfrak{f})^{-1})$ given as follows:

$$R'(C_j, (\mathfrak{a}_i\mathfrak{f})^{-1}) = \left\{x \in \boldsymbol{R}^n ; 0 < x_1, \cdots, x_n < 1, \sum_{k=1}^{n} x_k v_{jk} \in (\mathfrak{a}_i\mathfrak{f})^{-1}\right\}$$

(cf. (10)).

Then if $x = (x_1, \cdots, x_n) \in R'(C_j, (\mathfrak{a}_i\mathfrak{f})^{-1})$, $1 - x = (1 - x_1, 1 - x_2, \cdots, 1 - x_n) \in R'(C_j, (\mathfrak{a}_i\mathfrak{f})^{-1})$, since $v_{j1}, \cdots, v_{jn} \in \mathfrak{o}(F)$.

Furthermore, since $n_1 = |S| = n - 1$ in (14),

$$\chi(\mathfrak{a}_i\mathfrak{f}(x)) = (-1)^{n-1}\chi(\mathfrak{a}_i\mathfrak{f}(1 - x)) .$$

Hence, it follows from the equality $B_l(1 - x) = (-1)^l B_l(x)$ that

$$\sum_{x \in R'(C_j, (\mathfrak{a}_i\mathfrak{f})^{-1})} \chi_i(z(x))C_l(A_j) \prod_{k=1}^{n} \left\{\frac{B_{l_k}(x_k)}{l_k!}\right\} = 0$$

for any n-tuple $l = (l_1, \cdots, l_n)$ such that $l_1 + \cdots + l_n = n = r(j)$.

Remark 2. If $n = 1$, $F = \boldsymbol{Q}$, $h_0 = 1$ and χ is a primitive character modulo f $(f > 1)$ such that $\chi(-1) = 1$. We may put $\mathfrak{a}_1 = (1)$, $j = \{1\}$, $C_1 = C(1)$. Then $R(C_1, (\mathfrak{a}_i\mathfrak{f})^{-1}) = \{x/f ; x = 1, 2, \cdots, f\}$. Furthermore

$$w(\chi) = \frac{1}{\sqrt{f}} \sum_{x=1}^{f} \chi(x) \exp\left(\frac{2\pi i}{f} x\right) .$$

Hence, the formula (19) reduces to the following:

$$\begin{aligned} w(\chi)^{-1}\frac{\sqrt{f}}{2} L_F(1, \chi) &= \sum_{x=1}^{f-1} \chi(x)^{-1} \log\left\{\Gamma\left(\frac{x}{f}\right)\Big/\sqrt{2\pi}\right\} \\ &= \frac{1}{2}\sum_{x=1}^{f-1} \chi(x)^{-1} \log\left\{\pi/\sin\left(\frac{x\pi}{f}\right)\right\} = -\frac{1}{2}\sum_{x=1}^{f-1} \chi(x)^{-1} \log \sin\left(\frac{x\pi}{f}\right) . \end{aligned}$$

Thus, when $F = \boldsymbol{Q}$, the formula (19) coincides with the well-known formula for the values of Dirichlet L functions at $s = 1$.

2. Let K be a quadratic extension of F. *We assume that only one of n real primes of F splits in K.* Denote by $\mathfrak{d}$ the relative discriminant of K with respect to F and let χ be the character of the group of narrow ideal classes modulo $\mathfrak{d}$ of F which corresponds to the quadratic extension K in class field theory. Then χ is primitive and is of the form (14) with $n_1 = |S| = n - 1$. Denote by $\zeta_K(s)$ (resp. $\zeta_F(s)$) the Dedekind zeta function of K (resp. F). Then we have

$$\zeta_K(s) = \zeta_F(s)L_F(s, \chi) . \tag{21}$$

Further, $w(\chi) = 1$ in (15).

Denote by R_K (resp. R_F) the regulator of K (resp. F) and denote by h_K (resp. h_F) the class number of K (resp. F). Evaluating the residues at $s = 1$ of both sides of (21), we have

$$\frac{2^{n+1}R_K h_K \pi^{n-1}}{2\sqrt{d^2N(\mathfrak{d})}} = \frac{2^n R_F h_F}{2\sqrt{d}} L_F(1, \chi) .$$

Let $E(K)$ (resp. $E(F)$) be the group of units of K (resp. F). *Denote by m the cardinality of the toroidal part of the abelian group* $E(K)/E(F)$. *Take a unit* ε *of* K *so that the subgroup of* $E(K)$ *generated by* ε *and* $E(F)$ *has index m in* $E(K)$. Denote by ε^σ the conjugate of ε with respect to F. There exists an embedding of K into $\boldsymbol{R}$ such that $|\varepsilon/\varepsilon^\sigma| > 1$. We identify K with a subfield of $\boldsymbol{R}$ via this embedding. Then it is easy to see that $mR_K = 2^{n-2}R_F \log|\varepsilon/\varepsilon^\sigma|$. Thus,

$$2^{n-2}h_K \log|\varepsilon/\varepsilon^\sigma| = mh_F\frac{\sqrt{dN(\mathfrak{d})}}{2\pi^{n-1}}L_F(1,\chi)\,.$$

Combining this equality with Theorem 1, we obtain the following:

Corollary to Theorem 1. *The notation being as above,*

$$\begin{aligned}|\varepsilon/\varepsilon^\sigma|^{(2^{n-2}h_K)} &= \prod_{i=1}^{h_0}\prod_{j\in J}\prod_{x}\prod_{k=1}^{n}\left[\frac{\Gamma_{r(j)}(z(x)^{(k)},\omega_j^{(k)})}{\rho_{r(j)}(\omega_j^{(k)})}\right]^{\{mh_F\chi_i(z(x))\}} \\ &\times \prod_{i=1}^{h_0}\prod_{j\in J}\prod_{x}\prod_{l}\exp\left[(-1)^{r(j)}\frac{C_i(A_j)}{n}\prod_{k=1}^{r(j)}\left\{\frac{B_{l_k}(x_k)}{l_k!}\right\}\right]^{\{mh_F\chi_i(z(x))\}}\end{aligned} \tag{22}$$

where the product with respect to x is over $R(C_j,(\mathfrak{a}_i\mathfrak{d})^{-1})$ and the product with respect to l is over all the $r(j)$-tuples $l=(l_1,\cdots,l_{r(j)})$ of non-negative integers such that $l_1+l_2+\cdots+l_{r(j)}=r(j)$.

Remark 3. When $F=\boldsymbol{Q}$, formula (22) coincides with the Dirichlet class number formula for real quadratic fields.

References

[1] Barnes, E. W., The theory of the double gamma function, Philos. Trans. Roy. Soc. London (A) **196** (1901), 265–387.

[2] ——, On the theory of the multiple gamma function, Trans. Cambridge Philos. Soc. **19** (1904), 374–425.

[3] Hecke, E., Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen, zweite Mitteilung, Math. Z. **6** (1920), 11–51 (Werke, 249–289).

[4] Shintani, T., On evaluation of zeta functions of totally real algebraic number fields at non-positive integers, J. Fac. Sci. Univ. Tokyo Sec. IA. **23** (1976), 393–417.

[5] ——, On a Kronecker limit formula for real quadratic fields, to appear, J. Fac. Sci. Univ. Tokyo Sec. IA.

[6] Stark, H. M., Class-number problems in quadratic fields, Actes Congrès, intern. math. Tom 1 (1970), pp. 511–518, Gauthier-Villars, Paris.

[7] Zagier, D., A Kronecker limit formula for real quadratic fields, Math. Ann. **231** (1975), 153–184.

Department of Mathematics
Faculty of Science
University of Tokyo
Bunkyo-ku, Tokyo 113
Japan

ALGEBRAIC NUMBER THEORY, Papers contributed for the International Symposium, Kyoto 1976; S. Iyanaga (Ed.): Japan Society for the Promotion of Science, Tokyo, 1977

On a Kind of p-adic Zeta Functions

KATSUMI SHIRATANI

1. Introduction

It is our purpose to construct explicitly a special class of p-adic functions attached to the partial zeta functions in the rationals Q.

Let Z denote the ring of rational integers, Z_p the ring of rational p-adic integers, and Q_p the rational p-adic number field. As usual we set $q=p$ for $p>2$ and $q=4$ for $p=2$.

Let $\zeta(z,a,f)$ be the partial zeta function of a modulo f, where f means a given natural number and a denotes an integer prime to f. Then, following Siegel [10] we know that for each positive integer $m\in Z$

$$\zeta(1-m,a,f) = -f^{m-1}\frac{1}{m}P^m\left(\frac{a}{f}\right)$$

holds with the m-th Bernoulli function $P^m(y)$ except for the case $f=1$, $m=1$. In this case we have $\zeta(0)=-1/2$. The number $\zeta(1-m,a,f)$ for $m>2$ is the constant term of the Fourier expansion at infinity of a certain modular form, which is a linear combination of the primitive Eisenstein series of weight m and level f.

2. Some p-adic integrals

A function $u: Z_p\to\Omega_p$, the complete algebraic closure of Q_p, is said to be uniformly differentiable if there exists a continuous function $\phi_u: Z_p\times Z_p\to\Omega_p$ such that $\phi_u(x,x')=u(x)-u(x')/x-x'$ holds for any $x\neq x'$ in Z_p. Then we see easily that the integral

$$I_0(u)=\lim_{\rho\to\infty}\frac{1}{p^\rho}\sum_{x=0}^{p^\rho-1}u(x)$$

exists. Take $u(x)=(x+a/f)^m$; then we have $I_0(u)=B^m(a/f)$ for the m-th Bernoulli polynomial $B^m(y)$.

In the case $p \nmid f$, by the integral $I_0(u)$ with $u(x) = \omega^{-m}(x + a/f)(x + a/f)^m$ we define similar numbers $B^m_{\omega^{-m}}(a/f)$ in Q_p, where $\omega(x)$ denotes the canonical function defined on Z_p, namely $\omega(x) = \lim_{\rho\to\infty} x^{p^\rho}$ for $x \in Z_p - pZ_p$, $\omega(x) = 0$ for $x \in pZ_p$ $(p > 2)$ and $\omega(x) = \pm 1$, $\omega(x) \equiv x \pmod 4$ for $x \in Z_2 - 2Z_2$, $\omega(x) = 0$ for $x \in 2Z_2$ $(p = 2)$.

We regard the characters ω^{-m} with $m \equiv 0 \pmod{p-1}$ to $p > 2$ and ω^{-m} with $m \equiv 0 \pmod 2$ to $p = 2$ as the primitive principal character χ^0 respectively.

We also remark that the number $B^m_{\omega^{-m}}(a/f)$ for $p \mid a$ is an expression in Q_p of the value of a generalized Bernoulli polynomial belonging to the character ω^{-m}.

We further set $P^m_{\omega^{-m}}(a/f) = B^m_{\omega^{-m}}(a_0/f)$ for $a \in Z$ prime to f, where $a_0 = a - f[a/f]$ denotes the least non-negative residue of a module f. Hence we have $P^m_{\omega^{-m}}(a/f) = P^m(a/f)$ if $\omega^{-m} = \chi^0$.

As for the function ω we have the decomposition $x = \omega(x)\langle x\rangle$ to any unit x in Z_p with a principal unit $\langle x\rangle \equiv 1 \pmod q$.

3. A sequence of numbers

Now we take any integer $c \in Z$ as a parameter such that $(c, pf) = 1$, $c > 1$. Then we define a sequence of numbers $V(m, c, a, f)$ in Q_p as follows:

$$V(m,c,a,f) = \begin{cases} f^{m-1}\omega^{-m}(ac)\dfrac{1}{m}P^m\left(\dfrac{ac}{f}\right) - \langle c\rangle^m f^{m-1}\omega^{-m}(a)\dfrac{1}{m}P^m\left(\dfrac{a}{f}\right) \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{for } p \mid f\,, \\ f^{m-1}\omega^{-m}(f)\dfrac{1}{m}P^m_{\omega^{-m}}\left(\dfrac{ac}{f}\right) - (fp)^{m-1}\omega^{-m}(fp)\dfrac{1}{m}P^m_{\omega^{-m}}\left(\dfrac{(ac)_1}{f}\right) \\ -\langle c\rangle^m f^{m-1}\omega^{-m}(f)\dfrac{1}{m}P^m_{\omega^{-m}}\left(\dfrac{a}{f}\right) + \langle c\rangle^m (fp)^{m-1}\omega^{-m}(fp)\dfrac{1}{m}P^m_{\omega^{-m}}\left(\dfrac{a_1}{f}\right) \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{for } p \nmid f\,, \end{cases}$$

where a_1, $(ac)_1$ mean two integers satisfying $a \equiv pa_1 \pmod f$, $ac \equiv p(ac)_1 \pmod f$.

Let us determine an integer $r_\rho(x) \in Z$ for each integer $x = 0, 1, \cdots, p^\rho - 1$ by requiring $0 \leqq cx + p^\rho r_\rho(x) \leqq p^\rho - 1$.

Then, we see

$$V(m,c,a,f) = \frac{1}{f}\frac{1}{m}\lim_{\rho\to\infty}\frac{1}{p^\rho}\sum_{\substack{x=0\\ fx+(ac)_0\not\equiv 0 \pmod p}}^{p^\rho-1}\langle fx + (ac)_0\rangle^m - \langle c\rangle^m\frac{1}{f}\frac{1}{m}\lim_{\rho\to\infty}\frac{1}{p^\rho}\sum_{\substack{x=0\\ fx+a_0\not\equiv 0 \pmod p}}^{p^\rho-1}\langle fx + a_0\rangle^m\,.$$

When we take the integer a such as $a \geqq f$, we can transform $V(m, c, a, f)$ in the following form:

$$V(m,c,a,f) = \lim_{\rho\to\infty}\sum_{x=0}^{p^\rho-1}{}^* \omega^{-1}(fcx + ac)\langle fcx + ac\rangle^{m-1}r_\rho(x) - \sum_{x=-[ac/f]}^{-1}{}^* \omega^{-1}(fx + ac)\langle fx + ac\rangle^{m-1} + \langle c\rangle^m \sum_{x=-[a/f]}^{-1}{}^* \omega^{-1}(fx + a)\langle fx + a\rangle^{m-1}\,,$$

where $*$ means to take sums over all integers x satisfying $fcx + ac \not\equiv 0$, $fx + ac \not\equiv 0$, $fx + a \not\equiv 0 \pmod p$ in the given ranges respectively.

Because the number $V(m, c, a, f)$ is determined modulo f it follows from this that $\delta^k V(m, c, a, f) \equiv 0 \pmod{q^k}$ holds with a usual linear difference operator δ defined by $\delta\alpha_m = \alpha_{m+1} - \alpha_m$ on any sequence $\{\alpha_m\}$.

4. Partial zeta functions

By making use of the sequence $V(m, c, a, f)$ with a parameter $c \equiv 1 \pmod{pf}$ we can obtain a continuous function on Z_p

$$F(s,c,a,f) = -\sum_{k=0}^{\infty}\binom{-s}{k}\delta^k V(1,c,a,f)\,.$$

Let us now define a p-adic partial zeta function $\zeta_p(s, a, f)$ by

$$\zeta_p(s,a,f) = \frac{F(s,c,a,f)}{1 - \langle c\rangle^{1-s}} \qquad \text{for } s \in Z_p \ (s \neq 1)\,.$$

Denoting by e the order of the character ω we have the following

Theorem 1. *There exists a continuous function $\zeta_p(s, a, f)$ on Z_p $(s \neq 1)$, such that for each positive integer $m \equiv 0 \pmod e$*

$$\zeta_p(1-m,a,f) = \begin{cases}\zeta(1-m,a,f) & \text{if } p \mid f\,,\\ \zeta(1-m,a,f) - p^{m-1}\zeta(1-m,a_1,f) & \text{if } p \nmid f\end{cases}$$

holds. Moreover this function can be explicitly obtained from dividing $F(s, c, a, f)$ by $1 - \langle c\rangle^{1-s}$ as above.

Next, from the definitions of the generalized Bernoulli numbers B^m_χ and the p-adic L-functions $L_p(s, \chi)$ [3], [4] we obtain

Theorem 2. *Let χ be a primitive Dirichlet character with conductor f_χ. It holds then that for $s \in 1 + eZ_p$ $(s \neq 1)$, hence for all $s \in Z_p$ $(s \neq 1)$ in the case $p > 2$*

$$L_p(s,\chi) = \sum_{a \bmod f_\chi} \chi(a)\zeta_p(s,a,f_\chi) .$$

Conversely, we have for any natural number f

$$\zeta_p(s,a,f) = \frac{1}{\varphi(f)} \sum_{\chi \bmod f} \left\{ \chi^{-1}(a) L_p(s,\chi) \prod_{l \mid f,\,(l,pf_\chi)=1} (1 - \chi(l) l^{-s}) \right\} .$$

Herein φ means Euler's function, χ runs through all the Dirichlet characters defined modulo f and they are interpreted as primitive, and l runs over all prime factors of f prime to pf_χ.

5. Calculation of the residue

Finally we compute the residue of $\zeta_p(s,a,f)$ at $s=1$ from Theorem 1 by using the theory of Γ-transforms [3], [5], [8], which can be also directly seen from Theorem 2 if we assume the known results on p-adic L-functions.

Let ζ_r denote a primitive r-th root of unity and Δ be another linear difference operator acting on the numbers $n^\rho (n = 0, 1, 2, \cdots)$.

Then we find that

$$\frac{1}{f} \sum_{d=1}^{f} \zeta_f^{-ad} \sum_{\mu=1}^{c-1} \sum_{k=1}^{\infty} \frac{1}{k} \frac{\Delta^k 0^m}{(\zeta_f^{-d}\zeta_c^{-\mu} - 1)^k} = -(c^m - 1) f^{m-1} \frac{1}{m} P^m\left(\frac{a}{f}\right) .$$

By the way, let $g(t) = \sum b_j t^j$ be any polynomial, whose coefficients are elements in a finite extension K of Q_p. For any integer $n \in Z$ we set $\partial^n g(t) = \sum_{j \geq 1} b_j j^n$. Then we obtain a formula

$$\lim_{\rho \to \infty} \Delta^k 0^{p^\rho (p-1)+n} = \partial_*^n (t-1)^k ,$$

where we put $\partial_*^n (t-1)^k = -\frac{1}{p} \sum_{\nu=0}^{p-1} \partial^n \{(\zeta_p^\nu t - 1)^k - (t-1)^k\}$.

This operator ∂_*^n can be extended to an operator on a p-adic Banach algebra over K consisting of some formal power series in $K[[t-1]]$ under a certain norm. It is useful for a calculation of the values of $L_p(s,\chi)$ and $\zeta_p(s,a,f)$ at each rational integer point [9].

From the above formulas we conclude, in particular, with use of the p-adic logarithms

$$\begin{aligned} F(1,c,a,f) &= \lim_{\rho \to \infty} F(1 - p^\rho(p-1), c, a, f) \\ &= \lim_{\rho \to \infty} (c^{p^\rho(p-1)} - 1) f^{p^\rho(p-1)-1} \frac{1}{p^\rho (p-1)} P^{p^\rho(p-1)}\left(\frac{a}{f}\right) \\ &= -\frac{1}{f} \frac{1}{p} \sum_{d=1}^{f} \zeta_f^{-ad} \sum_{\mu=1}^{c-1} \log_p \left\{ \frac{(1 - \zeta_f^{pd} \zeta_c^{p\mu})}{(1 - \zeta_f^d \zeta_c^\mu)^p} \right\} \end{aligned}$$

$$= \begin{cases} \frac{1}{f} \log_p c & \text{for } p \mid f , \\ \frac{1}{f}\left(1 - \frac{1}{p}\right) \log_p c & \text{for } p \nmid f . \end{cases}$$

This gives us the following

Theorem 3. *The function $\zeta_p(s,a,f)$ has a pole of order 1 at $s=1$, and indeed we have*

$$\lim_{s \to 1} (s-1)\zeta_p(s,a,f) = \begin{cases} \frac{1}{f} & \text{for } p \mid f , \\ \frac{1}{f}\left(1 - \frac{1}{p}\right) & \text{for } p \nmid f . \end{cases}$$

We can analogously discuss p-adic class zeta functions for real quadratic number fields by starting again from a formula of Siegel [1], [2], [6], [7].

References

[1] Cassou-Noguès, P., Prolongement analytique et valeurs aux entiers négatifs de certaines séries arithmétiques relatives a des formes quadratiques, Sém. de Théorie des Nombres, Univ. Bordeaux, **4** (1975–1976), 1–34.

[2] Coates, J. and Sinnott, W., On p-adic L-functions over real quadratic fields, Inv. Math., **25** (1974), 253–279.

[3] Iwasawa, K., Lectures on p-adic L-functions, Ann. Math. Stud., **74**, Princeton U.P., Princeton, 1972.

[4] Kubota, T. und Leopoldt, H. W., Eine p-adische Theorie der Zetawerte. I, J. reine angew. Math., **214/215** (1964), 328–339.

[5] Leopoldt, H. W., Eine p-adische Theorie der Zetawerte. II, J. reine angew. Math., **274/275** (1975), 224–239.

[6] Morita, Y., On Hurwitz-Lerch L-functions, J. Fac. Sci. Univ. Tokyo, Ser. IA, to appear.

[7] Serre, J.-P., Formes modulaires et fonctions zêta p-adiques, Lecture Notes in Math., **350**, Springer, Berlin, 1973, 191–268.

[8] Shiratani, K., On certain values of p-adic L-functions, Mem. Fac. Sci. Kyushu Univ., **28** (1974), 59–82.

[9] ——, On a formula for p-adic L-function, J. Fac. Sci. Univ. Tokyo, Ser. IA. to appear.

[10] Siegel. C. L., Über die Fourierschen Koeffizienten von Modulformen, Göttinger Nachr., **3** (1970), 15–56.

Department of Mathematics
Faculty of Science
Kyushu University
Hakozaki, Fukuoka 812
Japan

ALGEBRAIC NUMBER THEORY, Papers contributed for the International Symposium, Kyoto 1976; S. Iyanaga (Ed.): Japan Society for the Promotion of Science, Tokyo, 1977

Representation Theory and the Notion of the Discriminant

TSUNEO TAMAGAWA*

The representation theory of reductive algebraic groups over arbitrary fields has been developed extensively by I. Satake [2] and J. Tits [3]. Applying the theory to the representation of outer-twisted groups of type A_{2r-1} corresponding to the center vertex of the Dynkin diagram, one can define an invariant attached to an involutorial algebra A of the second kind of even degree over its center. If the algebra A splits over its center, the involution is defined by a hermitian form and the invariant is essentially the discriminant of the form. Pushing the analogy further, we would like to prove a few theorems on the invariant. The definition of the invariant is based on the representation theory of unitary groups, and one can expect there would be a more algebraic approach to the theory.

Throughout this note, unless specified otherwise, fields are subfields of a fixed algebraically closed field L and vector spaces are finite dimensional over the common ground field L. Let G be a group and V a vector space. A representation ρ of G on V is a homomorphism of G into the general linear group $GL(V)$ of V. A representation ρ of G on V is uniquely extended to a homomorphism $\tilde{\rho}$ of the group ring $L[G] = \coprod_{s\in G} Ls$ into the algebra $E(V)$ of all linear transformations of V. We denote the kernel of $\tilde{\rho}$ by $I[\rho]$. If ρ is simple, $\tilde{\rho}$ is surjective and the equivalency class of ρ is uniquely determined by $I[\rho]$.

Let ρ be a simple representation. An element $\sum c(s)s$ of $L[G]$ belongs to $I[\rho]$ if and only if $\sum c(s)\chi_\rho(st) = 0$ for all $t \in G$ where $\chi_\rho(s)$ is the character $\chi_\rho(s) = \operatorname{tr} \rho(s)$ of the representation ρ. Hence the equivalency class of ρ is determined uniquely by its character χ_ρ. Let $X(\rho)$ denote the set $\{\chi_\rho(s) : s \in G\}$. We say ρ is defined over a field F if $F \supset X(\rho)$. If ρ is defined over F, then

* Research partially supported by NSF research grant MPS71-03469.

$I[\rho]_F = I[\rho] \cap F[G]$ contains a linear base of $I[\rho]$ over F and the factor algebra $A[\rho]_F = F[G]/I[\rho]_F$ is central simple over F of degree $n = \dim V$. We denote by $b[\rho]_F$ the Brauer class of $A[\rho]_F$ and by $\rho[s]$ the image of $s \in G$ in $A[\rho]_F$. We denote by B_F the Brauer group over F. If an algebra A is central simple over F, we denote by $b(A)$ the Brauer class of A. If K is an extension of F, we denote by $\mathrm{Rest}_{F\to K}$ the restriction morphism of B_F into B_K. Namely, $\mathrm{Rest}_{F\to K}b(A)$ is the Brauer class of the algebra $K \otimes_F A$ over K. We state the following lemmas without proof.

Lemma 1. *Let G be a group, ρ a simple representation defined over a field F and H a subgroup of G. Suppose that the restriction ρ_H of ρ to H is semi-simple and there exists a simple constituent η of multiplicity 1 of ρ_H defined over F. Then we have*

$$b[\rho]_F = b[\eta]_F .$$

Lemma 2. *Let ρ be a simple representation of a group G on a vector space V defined over a field F. Let p be an integer $1 \leq p \leq n$ and $\rho^{(p)}$ denote the representation of G on $V^{(p)} = V \wedge \cdots \wedge V$ defined by*

$$\rho^{(p)}(s)(x_1 \wedge \cdots \wedge x_p) = \rho(s)x_1 \wedge \cdots \wedge \rho(s)x_p ,$$

$x_1, x_2, \cdots, x_p \in V$. If $\rho^{(p)}$ is simple, $\rho^{(p)}$ is defined over F and we have

$$b[\rho^{(p)}]_F = b[\rho]_F^p .$$

Let A be a central simple algebra of degree n over a field Z and V a minimal left ideal of $A_L = L \otimes_Z A$. For $\alpha \in A$, let $f(t, \alpha) = t^n - S_1(\alpha)t^{n-1} + \cdots + (-1)^n S_n(\alpha)$ denote the characteristic polynomial of the linear transformation $\lambda(\alpha)$, $x \to \alpha x$ of V. $f(t, \alpha)$ is a polynomial in $Z[t]$ and $N\alpha = S_n(\alpha)$ is called the norm of α. The other terms $S_1(\alpha), S_2(\alpha), \cdots$ are traces of linear transformations $\lambda(\alpha), \lambda^{(2)}(\alpha), \cdots$ of $V, V^{(2)}, \cdots$ defined by

$$\lambda^{(p)}(\alpha)(x_1 \wedge \cdots \wedge x_p) = \alpha x_1 \wedge \cdots \wedge \alpha x_p$$

respectively. Let $GL(A)$ denote the group of all invertible elements of A. For each p, S_p is the character of the simple representation $\rho^{(p)}$ of $GL(A)$ on $V^{(p)}$ which is the restriction of $\lambda^{(p)}$ to $GL(A)$.

Proposition 1. *If d is a divisor of n, then the Schur index of $b(A)^d$ is a divisor of n/d.*

Proof. It suffices to prove our assertion in the case where d is a prime number p. The degree of $\rho^{(p)}$ is equal to $\binom{n}{p}$ and by Lemma 2, the Schur index of $b(A)^p$ is a divisor of the greatest common divisor of n and $n!/p!(n-p)!$ which is equal to n/p.

Henceforth we assume that $n = 2r$ is even. For $\alpha \in GL(A)$, we have $N\alpha^{-1}t^n f(t^{-1}, \alpha) = f(t, \alpha^{-1})$ and

$$S_p(\alpha) = N\alpha S_{n-p}(\alpha^{-1}) . \tag{1}$$

For each p, put $A^{(p)} = A[\rho^{(p)}]_Z$ and $\alpha^{(p)} = \rho^{(p)}[\alpha]$, $\alpha \in GL(A)$.

Proposition 2. *There exists an involution of the first kind $\mu \to \mu^*$ of $A^{(r)}$ such that*

$$(\alpha^{(r)})^* = N\alpha(\alpha^{(r)})^{-1} , \qquad \alpha \in GL(A) .$$

Proof. Put $G = GL(A)$. We define an involution $*$ of $Z[G]$ by

$$(\sum c(\alpha)\alpha)^* = \sum c(\alpha)N\alpha \cdot \alpha^{-1} .$$

We have, by (1),

$$\sum c(\alpha)\alpha \in I[\rho^{(r)}]_Z \longleftrightarrow \sum c(\alpha)S_r(\alpha\beta) = 0 \quad \text{for all } \beta \in G$$
$$\longleftrightarrow \sum N\alpha c(\alpha)S_r(\alpha^{-1}\beta) = 0 \quad \text{for all } \beta \in G \longleftrightarrow (\sum c(\alpha)\alpha)^* \in I[\rho^{(r)}]_Z ,$$

and $I[\rho^{(r)}]_Z^* = I[\rho^{(r)}]_Z$. Therefore the involution $*$ of $Z[G]$ induces an involution of $A^{(r)} = Z[G]/I[\rho^{(r)}]_Z$ with the required property.

Assume that Z is a separable quadratic extension of a field F and algebra A admits an involution J of the second kind. Let σ denote the conjugation of Z over F. For every $\alpha \in A$ we have

$$S_p(\alpha^J) = S_p(\alpha)^\sigma . \tag{2}$$

The following proposition will be proved in the same manner as the proof of Prop. 2.

Proposition 3. *There exists an involution $J(p)$ of the second kind $\mu \to \mu^{J(p)}$ of $A^{(p)}$ such that*

$$(\alpha^{(p)})^{J(p)} = (\alpha^J)^{(p)} .$$

For every $\alpha \in GL(A)$ we have

$$(\alpha^{(r)*})^{J(r)} = N\alpha^\sigma\{(\alpha^J)^{-1}\}^{(r)} = (\alpha^{(r)J(r)})^* ,$$

hence involutions $*$ and $J(r)$ of $A^{(r)}$ commute to each other. Therefore the

set A_0 of all $\mu \in A^{(\tau)}$ with $\mu^* = \mu^{J^{(\tau)}}$ is a central simple algebra over F and we have

$$A^{(\tau)} = ZA_0 \cong Z \underset{F}{\otimes} A_0 .$$

The involution $\mu \to \mu^*$ induces an involution of the first kind of A_0.

Definition. The Brauer class of A_0 will be called the *discriminant* of the involutorial algebra (A, J) and denoted by $\delta(A, J)$.

Let $SU(A, J)$ denote the gooup of all $s \in GL(A)$ with $ss^J = 1$ and $Ns = 1$. By restricting $\rho^{(1)}, \rho^{(2)}, \cdots$ to $SU(A, J)$ we have representations $\zeta^{(1)}, \zeta^{(2)}, \cdots$ of $SU(A, J)$. They are all simple because $SU(A, J)$ is a Zariski-dense subgroup of the special linear group $SL(A)$ of A. By (1) and (2) we have

$$S_p(s) = S_{n-p}(s^{-1}) = S_{n-p}(s)^\sigma , \qquad s \in SU(A, J) .$$

Therefore $\zeta = \zeta^{(\tau)}$ is defined over F and the algebra $A[\zeta]_F$ is identified with the algebra of all F-linear combinations of $s^{(\tau)}$, $s \in SU(A, J)$ in $A^{(\tau)}$. Since $s^{(\tau)*} = s^{(\tau)-1} = (s^J)^{(\tau)}$ we have $A_0 = A[\zeta]_F$. We have proved the following:

Theorem 1. *The representation $\zeta = \zeta^{(\tau)}$ of $SU(A, J)$ is defined over F and $b[\zeta]_F$ is equal to $\delta(A, J)$. The discriminant $\delta(A, J)$ has the following properties:*

1. $\delta(A, J)^2 = 1$
2. $\mathrm{Rest}_{F \to Z}\, \delta(A, J) = b(A)^\tau$.

Let $d \neq 0$ be an element of F. By $(d, Z/F)$ we denote the quaternion algebra $Z + Zu$ defined by

$$u^2 = d , \quad uc = c^\sigma u , \quad c \in Z .$$

Theorem 2. *Let γ be an element of $GL(A)$ such that $\gamma^J = \gamma$ and J' denotes the involution of A defined by $\alpha^{J'} = \gamma \alpha^J \gamma^{-1}$. Then we have*

3. $\delta(A, J') = \delta(A, J) b((N\gamma, Z/F))$.

Proof. First we assume that $A^{(\tau)}$ splits over Z. Let W be a minimal left ideal of $A^{(\tau)}$. By Prop. 2 there exists a non-degenerate bilinear form B on $W \times W$ such that

$$B(\alpha^{(\tau)} u, v) = N\alpha B(u, \alpha^{(\tau)-1} v) . \tag{3}$$

The form B is uniquely determined up to scalar multiplications. By Prop. 3 there exists a non-degenerate hermitian form $H(u, v)$ on $W \times W$ such that $H(cu, v) = c^\sigma H(u, v)$, $c \in Z$ and

$$H(\alpha^{(\tau)} u, v) = H(u, \alpha^{J^{(\tau)}} v) . \tag{4}$$

There exists a σ-semi-linear transformation λ of W such that

$$B(u, v) = H(\lambda u, v) \tag{5}$$

for all $(u, v) \in W \times W$. For every $\mu \in A_0$ we have $\mu^* = \mu^{J^{(\tau)}}$ and

$$B(\mu u, v) = H(\lambda \mu u, v) = H(\lambda u, \mu^* v) = B(u, \mu^* v) = H(\mu \lambda u, v) .$$

Hence we have $\lambda \mu = \mu \lambda$ and λ^2 commutes with all $\mu \in A_0$. Since $ZA_0 = A^{(\tau)}$ we have $\lambda^2 u = du$ with a fixed $d \in F^* = F - \{0\}$. The F-algebra C generated by λ and scalar multiplications $u \to cu$, $c \in Z$, is isomorphic to $(d, Z/F)$ and the centralizer of A_0 in the algebra $E_F(W)$ of all F-linear transformations of W. Hence we have

$$b(A_0) = \delta(A, J) = b((d, Z/F)) . \tag{6}$$

The involution $J'(r)$ corresponding to J' is obviously given by

$$\mu^{J'^{(\tau)}} = \gamma^{(\tau)} \mu^{J^{(\tau)}} \gamma^{(\tau)-1} .$$

Put $\Gamma = \gamma^{(\tau)}$. The form $H(u, v)$ is replaced by $H(\Gamma^{-1}u, v)$ and λ is replaced by $\lambda' = \Gamma\lambda$. On the other hand, by (3) and (4) we have

$$B(\Gamma u, v) = N\gamma B(u, \Gamma^{-1} v) = N\gamma H(\lambda u, \Gamma^{-1} v) = N\gamma H(\Gamma^{-1}\lambda u, v)$$

and $\lambda(\Gamma u) = N\gamma \Gamma^{-1} \lambda u$. Therefore we have $(\lambda')^2 u = N\gamma \lambda^2 u = dN\gamma u$. Replacing d by $dN\gamma$ in (6), we have

$$\delta(A, J') = b((d, Z/F)) b((N\gamma, Z/F)) = \delta(A, J) b((N\gamma, Z/F)) .$$

Suppose that $A^{(\tau)}$ does not split over Z. By Prop. 1, the Schur index of $A^{(\tau)}$ is equal to 2. Let W be a minimal left ideal of $A^{(\tau)}$ and Q denote the algebra of all $A^{(\tau)}$-homomorphisms of W. Q is a quaternion algebra over Z admitting an involution of the second kind over F. By Albert's theorem (Albert [1], Chap. X, Th. 21), there exists a F-subalgebra Q_0 of Q such that $Q = ZQ_0 \cong Z \otimes Q_0$. Let K be a maximal separable subfield of Q_0 (which is not a subfield of L). Since Q does not split over Z, K and Z are not isomorphic over F, and $K_1 = ZK \cong Z \otimes_F K$ is a Galois extension of degree 4 over F. The Galois group of K_1/F is generated by σ regarded as the conjugation over K and the conjugation τ of K_1 over Z. We now regard W as a

vector space over K_1. There exists a non-degenerate bilinear form B on $W \times W$ satisfying (3) and a non-degenerate hermitian form H satisfying (4). There exists an element $\kappa \in Q_0$ such that $\kappa^2 = a \in F^*$ and $c\kappa = \kappa c^\tau$ for all $c \in K_1$. Since B and H are determined uniquely up to scalar multiplications, we have

$$B(\kappa u, \kappa v) = cB(u, v)^\tau \qquad c \in K_1 ,$$
$$H(\kappa u, \kappa v) = c'H(u, v)^\tau \qquad c' \in K .$$

We have $cc^\tau = c'c'^\tau = a^2$. Choosing $b \in K_1$ and $b' \in K$ so that $b^{\tau-1} = c/a$ and $b'^{\tau-1} = c'/a$, we have $bB(\kappa u, \kappa v) = a(bB(u, v))^\tau$ and $b'H(\kappa u, \kappa v) = a(b'H(u, v))^\tau$. Therefore we may assume that $c = c' = a$. Let λ be the σ-semi-linear transformation satisfying (5). We have

$$B(\kappa u, v) = H(\lambda\kappa u, v) = B(u, \kappa v)^\tau$$
$$= H(\lambda u, \kappa v) = H(\kappa\lambda u, v)$$

and $\lambda\kappa = \kappa\lambda$. We now have $\lambda^2 = d$ with $d = d^\tau \in F^*$. The F-algebra C generated by λ, κ and scalar multiplications $x \to cx$, $c \in K_1$ is isomorphic to $(d, Z/F) \otimes (a, K/F)$ and is the centralizer of A_0 in the algebra $E_F(W)$ of all F-linear transformations of W. Therefore we have

$$b(A_0) = \delta(A, J) = b((d, Z/F))b((a, K/F)) .$$

If we replace the involution J by J', then as in the first case, d is replaced by $dN\gamma$ and we have

$$\delta(A, J') = b((dN\gamma, Z/F))b((a, K/F)) = b((N\gamma, Z/F))\delta(A, J) .$$

For an element $\alpha \in A$, the rank of α is defined by

$$\operatorname{rank} \alpha = n^{-1} \dim_Z A\alpha .$$

Theorem 3. *Suppose that there exists an idempotent $\varepsilon \neq 0, 1$ of even rank $2r_1$ such that $\varepsilon^J = \varepsilon$. Put $A_1 = \varepsilon A\varepsilon$ and $A_2 = (1 - \varepsilon)A(1 - \varepsilon)$. The involution J induces an involution J_1 on A_1 and J_2 and A_2 respectively. Then we have*

$$4. \quad \delta(A, J) = \delta(A_1, J_1)\delta(A_2, J_2) .$$

Proof. A_1 is a central simple algebra over Z $(=Z\varepsilon)$ of degree $n_1 = 2r_1$ and A_2 is a central simple algebra over Z $(=Z(1 - \varepsilon))$ of degree $n_2 = 2r_2 = 2(r - r_1)$. Let $\rho_i^{(1)}, \rho_i^{(2)}, \cdots$ denote the fundamental representations of $GL(A_i)$, $i = 1, 2$, and H denote the group of all $\alpha \in GL(A)$ with $\varepsilon\alpha = \alpha\varepsilon$. H is a subgroup of $GL(A)$ and naturally isomorphic to $GL(A_1) \times GL(A_2)$. The restriction of $\rho^{(p)}$ to H is equivalent to the direct sum

$$\sum_{q+t=p} \rho_1^{(q)} \otimes \rho_2^{(t)} .$$

Let ζ_1 and ζ_2 denote the restrictions of $\rho_1^{(r_1)}$, $\rho_2^{(r_2)}$ to $SU(A_1, J_1)$ and $SU(A_2, J_2)$ respectively. Then the restriction of ζ to $SU(A_1, J_1) \times SU(A_2, J_2)$ is equivalent to

$$\zeta_1 \otimes \zeta_2 + \sum \zeta_1^{(q)} \otimes \zeta_2^{(t)}$$

Now $\zeta_1 \otimes \zeta_2$ is simple and defined over F. By Lemma 1 we have

$$\delta(A, J) = b[\zeta_1 \otimes \zeta_2]_F = \delta(A_1, J_1)\delta(A_2, J_2) .$$

Theorem 4. *Suppose that there exists an idempotent ε of A such that $\varepsilon + \varepsilon^J = 1$. Then we have*

$$\delta(A, J) = 1 .$$

Proof. Let H denote the group of all $s \in SU(A, J)$ such that $s\varepsilon = \varepsilon s$. Put $A' = \varepsilon A\varepsilon$. A' is a central simple algebra of degree r over Z $(=Z\varepsilon)$. Let $N'\alpha'$ denote the reduced norm of $\alpha' \in A'$. Then H is the group of all $\alpha' + (\alpha'^J)^{-1}$, $\alpha' \in GL(A')$ such that $N'\alpha' = a \in F$. Put $\xi(s) = N'\alpha'$, $s \in H$. The restriction of ζ to H is semi-simple and has two constituents of degree 1, ξ and ξ^{-1}. By Lemma 1 we have $b[\zeta]_F = 1$.

Theorem 5. *Let V be a vector space of dimension $n = 2r$ over Z and $h(x, y)$ a non-degenerate hermitian form on $V \times V$ such that $h(cx, y) = c^\sigma h(x, y)$. Let J denote the involution of $A = E(V)$ defined by*

$$h(\alpha x, y) = h(x, \alpha^J y) .$$

Then we have

$$\delta(A, J) = b((d, Z/F))$$
$$d = (-1)^r \det (h(x_i, x_j))$$

where $x_1, \cdots, x_n$ are a base of V over Z.

Proof. We may assume that $x_1, \cdots, x_n$ are an orthogonal base with respect to h. By Theorem 3, it suffices to treat the case where $n = 2$. In this case, the algebra A_0 is isomorphic to $(-a_1a_2, Z/F)$ and our assertion follows immediately.

So far we have treated only the case where the center Z of A is a field. To describe the behavior of $\delta(A,J)$ by the basic field extensions, we consider somewhat degenerate cases.

Let (A,J) be a normal simple involutorial algebra of the second kind over a field F and Z denote the center of A. Z is a commutative semi-simple algebra over F of rank 2 and J induces a non-trivial automorphism of Z over F. If Z is a field we have studied the case. If Z is not a field, Z is the sum of two ideals $F\varepsilon + F\varepsilon'$, $\varepsilon + \varepsilon' = 1$, $\varepsilon\varepsilon' = 0$, and A is the sum $A\varepsilon + A\varepsilon'$ of ideals $A_1 = A\varepsilon$ and $A_2 = A\varepsilon'$. Both A_1 and A_2 are normal simple over F and the involution J induces an anti-isomorphism of A_1 onto A_2. The special unitary group $SU(A,J)$ is the group of all $s_1 + s_1^J$, $s_1 \in SL(A_1)$. Therefore if the degree $n = 2r$ of A_1 over F (which will be called the degree of A over Z) is even, it is reasonable to assign $b(A_1)^r$ as the value of $\delta(A,J)$. Now we have the following:

Theorem 6. *Let (A,J) be a normal simple involutorial algebra over F of the second kind. Suppose that the degree n of A over the center is even, $n = 2r$. If K is an extension of F and J_K is the canonical extension of J to $A_K = A \otimes_F K$, we have*

$$\delta(A_K, J_K) = \mathrm{Rest}_{F\to K}\, \delta(A,J) .$$

Proof. Put $G = SU(A,J)$ and $G_K = SU(A_K, J_K)$. Denote by ζ_K the representation $\zeta_K^{(r)}$ of G_K. Obviously we have $I[\zeta_K]_K \cap F[G] \supseteq I[\zeta]_F$ and the morphism $A[\zeta]_F \to A[\zeta_K]_K$ is injective. Comparing the degrees of ζ and ζ_K we have $A[\zeta_K]_K \cong K \otimes_F A[\zeta]_F$ and

$$\mathrm{Rest}_{F\to K}\, b[\zeta]_F = b[\zeta_K]_K .$$

Let F be an algebraic number field, Z a quadratic extension of F and A a central simple algebra over Z of degree $n = 2r$. Assume that A admits an involution J of the second kind over F. By Theorem 6, we have $\mathrm{Rest}_{F\to F_\mathfrak{p}}\, \delta(A,J) = \delta(A_\mathfrak{p}, J_\mathfrak{p})$ for all prime $\mathfrak{p}$ where $F_\mathfrak{p}$ is the completion of F at $\mathfrak{p}$ and $A_\mathfrak{p}$ is the algebra $F_\mathfrak{p} \otimes_F A$. If $Z_\mathfrak{p} = Z \otimes_F F_\mathfrak{p}$ is a field, namely there is only one prime of Z over $\mathfrak{p}$, then $A_\mathfrak{p}$ splits over $Z_\mathfrak{p}$ and we have $\delta(A_\mathfrak{p}, J_\mathfrak{p}) = b((d_\mathfrak{p}, Z_\mathfrak{p}/F_\mathfrak{p}))$ where $d_\mathfrak{p}$ is the "discriminant" of the hermitian form $h_\mathfrak{p}$ defined by $J_\mathfrak{p}$. The Hasse invariant of $\delta(A_\mathfrak{p}, J_\mathfrak{p})$ is 0 or $1/2$ according as $d_\mathfrak{p}$ is a norm of an element of $Z_\mathfrak{p}$ or not. If $Z_\mathfrak{p}$ splits into the sum of two fields $\cong F_\mathfrak{p}$, $\mathfrak{p}$ splits into two primes $\mathfrak{P}_1$ and $\mathfrak{P}_2$ of Z and the sum of invariants $\mathrm{Inv}\,(A_{\mathfrak{P}_1}) + \mathrm{Inv}\,(A_{\mathfrak{P}_2})$ is $\equiv 0 \bmod 1$. We have

$$\mathrm{Inv}\,(\delta(A_\mathfrak{p}, J_\mathfrak{p})) \equiv r\,\mathrm{Inv}\,(A_{\mathfrak{P}_1}) \equiv r\,\mathrm{Inv}\,(A_{\mathfrak{P}_2}) \bmod 1 .$$

$\delta(A,J)$ is uniquely determined by giving $\mathrm{Inv}\,(\delta(A_\mathfrak{p}, J_\mathfrak{p}))$ for all $\mathfrak{p}$ and we have the relation

$$\sum_\mathfrak{p} \mathrm{Inv}\,(\delta(A_\mathfrak{p}, J_\mathfrak{p})) \equiv 0 \bmod 1 .$$

References

[1] Albert, A. A., Structures of Algebras, AMS Colloq. Pub., **24**, Providence, 1939.
[2] Satake, I., Symplectic representations of algebraic groups satisfying a certain analytic condition, Acta Math., **117**, (1967), 215–279.
[3] Tits, J., Représentations linéares irréductibles d'un groupe réductif sur un corps quelconque, J. reine angew. Math., **247** (1971), 196–220.

Department of Mathematics
Yale University
New Haven, Connecticut 06520
U.S.A.

Added in proof. Professor Tits kindly informed the author that Theorem 5 has been proved in the following paper:

Slodowy, P., Unitäre Darstellungen halbeinfacher algebraischer Gruppen über Divisionsalgebren mit Involution, Diplomarbeit, Bonn, 1973.

ALGEBRAIC NUMBER THEORY, Papers contributed for the International Symposium, Kyoto 1976; S. Iyanaga (Ed.): Japan Society for the Promotion of Science, Tokyo, 1977

Selberg Trace Formula for Picard Groups

YOSHIO TANIGAWA

A Picard group in the title means a discrete subgroup of $SL(2, C)$ that operates discontinuously on the 3-dimensional upper half space. Historically E. Picard was the first who considered such a group. Recently T. Kubota considers an automorphic function with respect to a Picard group in his theory of power residue symbols. In this paper, we shall write down the trace formula in Selberg's original form with respect to $\Gamma = SL(2, \boldsymbol{Z}[i])$.

This paper contains an introductory part of a research of the author, in which he proposes to develop, to certain extent, a theory on the vector valued, real analytic automorphic functions related to $SL(2, C)$.

Shortly after the author had completed the manuscript, a new translation of Venkov [7] was published, which is more extensive than the present paper.

Nevertheless, it still seems to make some sense officially to announce and to publish the results in the present paper for, between [7] and this paper, there are a few differences in displacement of contents as well as in details of proofs, although they might be inessential. For instance, [7] is based upon the theory of resolvent as described in Faddeev [1], while the present paper derives every theorem by direct computations of Eisenstein series. More recently, Dr. de la Torre in Princeton has worked on this topic in her private note, too [6].

The auther wishes to express his thanks to Prof. Kubota for his helpful advices.

§ 1. Three dimensional upper half space

The *three dimensional upper half space* H is a space consisting of all elements $u = (z, v)$ where z is a complex number and v is a positive real number. The group $G = SL(2, C)$ operates on this space by a linear fractional transformation:

$$G \ni \sigma = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}:$$

$$(z, v) \longrightarrow \left(\frac{(\alpha z + \beta)(\bar{\gamma}\bar{z} + \bar{\delta}) + \alpha\bar{\gamma}v^2}{|\gamma z + \delta|^2 + |\gamma|^2 v^2}, \frac{v}{|\gamma z + \delta|^2 + |\gamma|^2 v^2} \right).$$

This action is transitive and the isotropy group of $u_0 = (0, 1)$ is the maximal compact subgroup $K = SU(2)$ of G, so we can canonically identify the space H with the homogeneous space G/K.

We shall use the following notations in the sequel,

$$n(z) = \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix} \quad z \in \boldsymbol{C}, \quad a(v) = \begin{pmatrix} v^{1/2} & 0 \\ 0 & v^{-1/2} \end{pmatrix} \quad v > 0.$$

$\dot{g}$ = the image of $g \in G$ under the projection $G \to H$.

It is well known that the space H is of rank 1 and has a G-invariant metric $ds^2 = v^{-2}(dx^2 + dy^2 + dv^2)$ and a G-invariant volume element $d\mu(u) = d\dot{g} = v^{-3}dxdydv$ ($x = \mathrm{Re}\,(z)$, $y = \mathrm{Im}\,(z)$). The Laplace-Beltrami operator on this space is

$$D = v^2\left(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} + \frac{\partial^2}{\partial v^2} \right) - v\frac{\partial}{\partial v}.$$

§ 2. The Selberg transformation

We shall normalize the Haar measure dg on G by

$$\int_G f(g)dg = \int_H f(n(z)a(v))\frac{dxdydv}{v^3} \qquad \text{for all } f \in L^1(G/K)$$

where $z = x + iy$.

Let $\mathscr{H}_0$ be the space of continuous functions on G with compact support such that

$$\varphi(kgk') = \varphi(g) \qquad \text{for all } g \in G \text{ and all } k, k' \in K.$$

The function defined by $k(g, g') = \varphi(g'^{-1}g)$, for $\varphi \in \mathscr{H}_0$ is a point-pair invariant so derives an invariant integral operator L_φ, i.e.

$$(L_\varphi f)(g) = \int_G f(g')k(g, g')dg'$$

Theorem 1 (Selberg). *Suppose that the function f on G/K is an eigenfunction of D with an eigenvalue λ. Then f is an eigenfunction of an arbitrary invariant integral operator L_φ. Moreover, its eigenvalue is determined only by L_φ and λ.*

This eigenvalue is denoted by $h(\lambda)$ and the map $\varphi(g) \to h(\lambda)$ is called the *Selberg transformation*.

Before stating the next proposition, we will make two conventions. Every element φ of $\mathscr{H}_0$ is in fact a function of $t = \|g\|^2 = |\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2$ where $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in G$, so we will often write as $\varphi(g) = \psi(t)$. Secondly, we introduce the new variable r by $\lambda = -1 - r^2$, and write $h(r)$ instead of $h(\lambda)$.

Proposition 2. *Let φ be an element of $\mathscr{H}_0$, and let $\psi(t) = \varphi(g)$ as above. Then the Selberg transformation can be computed as follows. Set*

$$Q(w) = \pi\int_w^\infty \psi(t)dt$$

and $g(u) = Q(w)$ where $w = e^u + e^{-u}$. Then,

$$h(r) = \int_{-\infty}^{\infty} g(u)e^{iru}du.$$

Conversely,

$$g(u) = \frac{1}{2\pi}\int_{-\infty}^{\infty} h(r)e^{-iru}dr = Q(w)$$

and

$$\psi(t) = -\frac{1}{\pi}Q'(t).$$

For the proof, we refer to [3].

Let $\mathcal{O}$ be the ring of integers of $\boldsymbol{Q}(i)$. The group $\Gamma = SL(2, \mathcal{O})$ is a discrete subgroup of G and operates discontinuously on the space H. The *fundamental domain* for it is given, as a standard form, by

$$\mathscr{D} = \{(z, v) \mid z = x + iy,\ 0 \leqq x + y,\ x \leqq \tfrac{1}{2},\ y \leqq \tfrac{1}{2},\ x^2 + y^2 + v^2 \geqq 1\}.$$

Let $L^2(\Gamma\backslash G)$ be the space of measurable functions on G such that

(i) $f(\gamma g) = f(g)$ for all $\gamma \in \Gamma$,

(ii) $\int_{\Gamma\backslash G} |f(g)|^2\, dg < +\infty$.

Let $L_0^2(\Gamma\backslash G)$ be the subspace of $L^2(\Gamma\backslash G)$ satisfying the additional condition

(iii) $\int_{-1/2}^{1/2}\int_{-1/2}^{1/2} f(n(z)g)dxdy = 0$ for all $g \in G$.

The operator L_φ derived from $\varphi \in \mathscr{H}_0$ is, on $L^2(\Gamma\backslash G)$, an integral operator with the kernel function $K(g, g') = \sum_{\gamma\in\Gamma} \varphi(g'^{-1}\gamma g)$. The *Eisenstein series* with respect to Γ is defined by

$$E(g, s) = \sum_{\sigma\in\Gamma_0\backslash\Gamma} v(\sigma g)^s ,$$

where s is a complex number, $v = v(g)$ is the v-part in the Iwasawa decomposition $g = n(z)a(v)k$ $(k \in K)$, and $\Gamma_0 = \left\{\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} \in \Gamma \mid \gamma = 0\right\}$. This series converges absolutely in $Re(s) > 2$ and defines a holomorphic function. It can be continued to all complex plane as a meromorphic function and satisfies a functional equation:

$$\Phi(s)E(g, 2 - s) = E(g, s) ,$$

where $\Phi(s) = \pi/(s - 1)\cdot Z(s - 1)/Z(s)$, and $Z(s)$ is the Dedekind zeta function of $\boldsymbol{Q}(i)$. Put

$$H(g, g') = \frac{1}{\pi}\int_{-\infty}^{\infty} h(r)E(g, s)\overline{E(g', s)}dr ,$$

where $s = 1 + ir$.

From Selberg's theory we know that L_φ operates completely continuously on $L_0^2(\Gamma\backslash G)$ and has only discrete spectra with finite multiplicities. The continuous spectrum of L_φ on $L^2(\Gamma\backslash G)$ is expressed by $H(g, g')$, that is, the operator L_φ^* on $L^2(\Gamma\backslash G)$ with the kernel function $K^* = K - H$ is completely continuous and has all discrete spectra of L_φ. Suppose that L_φ^* is of trace class. Then the following trace formula holds:

$$\sum h(r_j) = \int_{\Gamma\backslash G} (K(g, g) - H(g, g))dg ,$$

where the sum in the left hand side ranges over all $r_j > 0$ such that the differential equation $Df = -(1 + r_j^2)f$ has a non-trivial solution in $L^2(\mathscr{D})$.

§ 3. Decomposition of $\Gamma = SL(2, \mathbb{C})$ into conjugacy classes

We denote by the symbol $\{\gamma\}_\Gamma$ the *conjugacy class* of $\gamma \in \Gamma$ in Γ, and denote Γ_γ the *centralizer* of γ in Γ. If $\gamma \in G$ has Jordan form $\begin{pmatrix}\lambda & 0\\ 0 & \lambda^{-1}\end{pmatrix}$ with $\lambda > 0$, then γ is said to have the norm $N\{\gamma\} = \lambda^2$.

Every element of $\Gamma = SL(2, \mathbb{C})$ is conjugate to one of the following elements:

$\pm$ the *unit matrix*;

parabolic element $\left(\text{conjugate to } \pm\begin{pmatrix}1 & z\\ 0 & 1\end{pmatrix} \text{ in } G \text{ where } z \in \boldsymbol{C},\ z \neq 0\right)$;

elliptic element $\left(\text{conjugate to } \pm\begin{pmatrix}\varepsilon & 0\\ 0 & \varepsilon^{-1}\end{pmatrix} \text{ in } G \text{ where } |\varepsilon| = 1,\ \varepsilon \neq \pm 1\right)$;

hyperbolic element $\left(\text{conjugate to } \pm\begin{pmatrix}v & 0\\ 0 & v^{-1}\end{pmatrix} \text{ in } G \text{ where } v > 1\right)$,

loxodromic element $\left(\text{conjugate to } \pm\begin{pmatrix}v\varepsilon & 0\\ 0 & v^{-1}\varepsilon^{-1}\end{pmatrix} \text{ in } G,\ \text{where } v > 1,\ |\varepsilon| = 1,\ \varepsilon \neq \pm 1\right)$.

(i) *Parabolic elements.*

Let Γ_0, Γ_1 be the subgroups of Γ defined by

$$\Gamma_0 = \left\{\begin{pmatrix}\alpha & \beta\\ 0 & \delta\end{pmatrix} \middle| \alpha\delta = 1,\ \alpha, \beta, \delta \in \mathscr{O}\right\}$$

$$\Gamma_1 = \left\{\pm\begin{pmatrix}1 & \beta\\ 0 & 1\end{pmatrix} \middle| \beta \in \mathscr{O}\right\} .$$

Then, Γ_1 is the group consisting of all parabolic elements which leave the cusp ∞ fixed. Every parabolic element of Γ is conjugate to some element of Γ_1, so that it is sufficient to decompose the group Γ_1 into its conjugacy classes. The result is as follows. The full set of representatives of conjugacy classes is given by

$$\left\{\pm\begin{pmatrix}1 & \beta\\ 0 & 1\end{pmatrix}\right\} ,$$

where β runs over the following set:

$$\{\beta \in \mathscr{O} \mid \mathrm{Im}\,\beta > 0\} \cup \{\beta \in \mathscr{O} \mid \mathrm{Im}\,\beta = 0,\ \mathrm{Re}\,\beta > 0\} .$$

For every $\gamma \in \Gamma_1$, its centralizer is just the group Γ_1.

(ii) *Elliptic elements.*

The elliptic element of Γ has an order equal to 4, 3 or 6.

There are four conjugacy classes of elliptic elements of order 4, and they are represented by

$$\sigma_\lambda = \begin{pmatrix}i & \lambda\\ 0 & -i\end{pmatrix} \qquad \lambda = 0,\ 1,\ -i,\ 1 - i .$$

Their centralizers are

$$\Gamma_{\sigma_\lambda} = \{\pm 1, \pm\sigma_i\} ,$$

for all λ.

On the other hand, there are two conjugacy classes of elliptic elements of order 3. The representatives of them are

$$a = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \qquad b = \begin{pmatrix} 0 & -i \\ -i & -1 \end{pmatrix}$$

and Γ_a is generated by $\begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 2+i & -2i \\ 2i & 2-i \end{pmatrix}$, and Γ_b is generated by $\begin{pmatrix} 1 & -i \\ -i & 0 \end{pmatrix}$ and $\begin{pmatrix} 2+i & 2 \\ 2 & 2-i \end{pmatrix}$. The case of elliptic elements of order 6 is similar. The representatives are given by $-a$, $-b$, and $\Gamma_{-a} = \Gamma_a$, $\Gamma_{-b} = \Gamma_b$.

(iii) *Hyperbolic or loxodromic elements.*

It is difficult for the author to determine the full set of representatives of conjugacy classes of them. Hereafter, we assume that the full set of representatives of primitive elements $\{\gamma_\alpha\}_{\alpha\in A}$ is given (an element is said to be primitive if it is not a power of any other element of Γ). Every hyperbolic or loxodromic element γ can be written as $\gamma = \gamma_0^k$ with some primitive element γ_0 and some integer k.

§ 4. Trace formula

In § 2, we defined an integral operator L_φ^* on $L^2(\Gamma\backslash G)$. We assume that it is of trace class. Then the trace formula holds.

$$\begin{aligned} \sum h(r_j) &= \int_{\Gamma\backslash G} (K(g,g) - H(g,g))dg \\ &= \int_{\Gamma\backslash G} \Big(\sum_{\{\gamma\}_\Gamma} \sum_{\sigma\in\{\gamma\}_\Gamma} \varphi(g^{-1}\sigma g) - H(g,g) \Big) dg . \end{aligned}$$

The conjugacy class of elliptic elements of order 4 and that of parabolic elements have the continuous spectrum. So we shall compute

$$C(\{\gamma\}_\Gamma) = \int_{\Gamma\backslash G} \sum_{\sigma\in\{\gamma\}_\Gamma} \varphi(g^{-1}\sigma g)dg$$

for the class of $\pm$unit, elliptic elements of order 3 or 6, and hyperbolic or loxodromic elements. And to exclude the continuous spectrum we shall compute

$$\lim_{V\to\infty} \Big\{ \frac{1}{2} \int_{\mathcal{D}_V} \Big(\begin{matrix} \text{elliptic element} \\ \text{of order 4} \end{matrix} \Big) + \frac{1}{2} \int_{\mathcal{D}_V} (\text{parabolic element}) \Big)$$

$$- \frac{1}{2} \int_{\mathcal{D}_V} H(\dot{g}, \dot{g})d\dot{g} \Big\} ,$$

where $\mathcal{D}_V = \{(z, v) \in \mathcal{D} \mid v \leqq V\}$.

Proposition 3. *Let Γ be a discrete subgroup of G of finite type and let $\mathcal{D}$ be its fundamental domain in H. Let φ be an element of $\mathcal{H}_0$. Then the contribution from $\pm$unit is given by*

$$c(1_2) + c(-1_2) = \frac{m(\mathcal{D})}{4\pi^2} \int_{-\infty}^{\infty} r^2 h(r)dr$$

where $m(\mathcal{D})$ is the volume of $\mathcal{D}$ and h is the Selberg transformation associated with φ.

Proposition 4. *Let Γ be a discrete subgroup of G of finite type and let $\mathcal{D}$ be its fundamental domain in H. Let φ be an element of $\mathcal{H}_0$. If γ is an elliptic elements of Γ with the Jordan canonical form $\begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{pmatrix}$ such that Γ_γ is generated by two elements. Then one of them is of infinite order which we denote by γ_1. Let $(\Gamma_\gamma)'$ be a free part of Γ_γ. Then*

$$c(\{\gamma\}_\Gamma) = \frac{\log |N\{\gamma_1\}|}{4\pi\, |\varepsilon - \bar{\varepsilon}|^2\, [\Gamma_\gamma : (\Gamma_\gamma)']} \int_{-\infty}^{\infty} h(r)dr ,$$

where $[\ :\ ]$ means the index as a transformation group.

Proposition 5. *Let Γ be a discrete subgroup of G of finite type with fundamental domain $\mathcal{D}$. Let φ be an element of $\mathcal{H}_0$. Let γ_0 be a primitive hyperbolic or loxodromic element, and let $\gamma = \gamma_0^k$ for some integer k. Then*

$$c(\{\gamma\}_\Gamma) = \frac{\log |N\{\gamma_0\}|\, g(k \log |N\{\gamma_0\}|)}{2\, |N\{\gamma_0\}^{k/2} - N\{\gamma_0\}^{-k/2}|^2\, [\Gamma_{\gamma_0} : (\Gamma_{\gamma_0})']} ,$$

where $(\Gamma_{\gamma_0})'$ is a free part of Γ_{γ_0}, $[\ :\ ]$ denotes the index as a transformation group, and g is the inverse Fourier transform of h (Proposition 2).

The proofs of these three propositions are similar to the case of a Fuchsian group of the first kind. So we omit their proofs.

Now we take $SL(2, \mathcal{O})$ for Γ where $\mathcal{O}$ is the ring of integers of $\boldsymbol{Q}(i)$. Assume that $\{\gamma_\alpha\}_{\alpha\in A}$ is a full set of representatives of conjugacy classes of primitive hyperbolic or loxodromic elements. Then the terms of elements described in the above propositions are

$$\frac{Z(2)}{2\pi^4}\int_{-\infty}^{\infty} r^2h(r)dr + \frac{2\log(2+\sqrt{3})}{9\pi}\int_{-\infty}^{\infty} h(r)dr + \frac{1}{2}\sum_{\alpha\in A}\sum_{k=1}^{\infty}\frac{\log|N\{\gamma_\alpha\}|\, g(k\log|N\{\gamma_\alpha\}|)}{|N\{\gamma_\alpha\}^{k/2}-N\{\gamma_\alpha\}^{-k/2}|^2[\Gamma_{\gamma_\alpha}:(\Gamma_{\gamma_\alpha})']}$$

Note that $m(\mathscr{D})$ is equal to $2\cdot\pi^{-2}Z(2)$ in our case.

To exclude the continuous spectrum, we divide the fundamental domain $\mathscr{Z} = \Gamma\backslash H$ as $\mathscr{D}_V \cup \mathscr{D}'_V$, where $\mathscr{D}_V = \{(z,v)\in\mathscr{D}\mid v\leqq V\}$, $\mathscr{D}'_V = \mathscr{D} - \mathscr{D}_V$, and compute the asymptotic behavior of the integral $\int_{\mathscr{D}_V}$ as $V\to\infty$.

For the elliptic elements of order 4, we must compute the following integral:

$$\begin{aligned} I_\lambda &= \int_{\mathscr{D}_V}\sum_{\sigma\in\Gamma_{\sigma\lambda}\backslash\Gamma}\varphi(\dot g^{-1}\sigma^{-1}\sigma_\lambda\sigma\dot g)d\dot g \\ &= \frac{1}{2}\int_{\mathscr{D}_V}\sum_{\sigma\in\Gamma}\varphi(\dot g^{-1}\sigma^{-1}\sigma_\lambda\sigma\dot g)d\dot g = \frac{1}{2}\int_{\bigcup_{\sigma\in\Gamma}\sigma\mathscr{D}_V}\varphi(\dot g^{-1}\sigma_\lambda\dot g)d\dot g \\ &= \frac{1}{2}\int_D\varphi(\dot g^{-1}\sigma_\lambda\dot g)d\dot g\ , \end{aligned}$$

where $D = \left[\bigcup_{\sigma\in\Gamma}\sigma\mathscr{D} - \bigcup_{\sigma\in\Gamma_0}\sigma\mathscr{D}'_V\right] - \bigcup_{\substack{\sigma\in\Gamma\\ \sigma\notin\Gamma_0}}\sigma\mathscr{D}'_V$.

From the compactly supportedness of φ we get the following

Lemma 6. *For a sufficiently large V we have*

$$\int_{\bigcup\sigma\mathscr{D}'_V}\varphi(\dot g^{-1}\sigma_\lambda\dot g)d\dot g = 0\ ,$$

where $\sigma = \begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ runs over all elements of Γ such that $\sigma\notin\Gamma_0$, $\alpha/\gamma\neq\lambda i/2$.

So, it is sufficient to integrate on the following domain:

$$\tilde{\mathscr{D}}_\lambda = \bigcup_{\sigma\in\Gamma}\sigma\mathscr{D} - \bigcup{}^{*}_{\sigma}\sigma\mathscr{D}'_V - \bigcup{}^{**}_{\sigma}\sigma\mathscr{D}'_V$$

the union $\bigcup^*$ is over all $\sigma\in\Gamma_0$, and $\bigcup^{**}$ is over all $\sigma = \begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}\in\Gamma$ such that $\sigma\notin\Gamma_0$ and $\alpha/\gamma = \lambda i/2$.

More explicitly,

$$\tilde{\mathscr{D}}_0 = \left\{(z,v)\in H\mid v\leqq V,\ |z|^2 + \left(v-\frac{1}{2V}\right)^2\geqq\left(\frac{1}{2V}\right)^2\right\}$$

and

$$\tilde{\mathscr{D}}_\lambda = \left\{(z,v)\in H\mid v\leqq V,\ \left|z-\frac{\lambda i}{2}\right|^2 + \left(v-\frac{|\lambda|^2}{8V}\right)^2\geqq\left(\frac{|\lambda|^2}{8V}\right)^2\right\}$$

for $\lambda\neq 0$.

If we put $\varphi(g) = \psi(t)$ for $t = \|g\|^2$ then

$$\begin{aligned} I_0 &= \pi\int_0^{1/V}\int_{\sqrt{(v/V)(1-Vv)}}^{\infty}\psi\left(2+4\frac{r^2}{v^2}\right)rdr\frac{dv}{v^3} \\ &\quad + \pi\int_{1/V}^{V}\int_0^{\infty}\psi\left(2+4\frac{r^2}{v^2}\right)rdr\frac{dv}{v^3} + o(1) \\ &= \frac{1}{8}\int_0^{1/V}Q\left(2\frac{2-Vv}{Vv}\right)\frac{dv}{v} + \frac{\pi}{8}\int_{1/V}^{V}\int_2^{\infty}\psi(t)dt\frac{dv}{v} + o(1)\ . \end{aligned}$$

In order to express these integrals in terms of $h(r)$ and $g(u)$ we shall change the variables by

$$w = 2\frac{2-Vv}{Vv} = e^u + e^{-u}\ .$$

Then the first integral reduces to

$$\begin{aligned} \int_2^{\infty}\frac{Q(w)}{w+2}dw &= \int_0^{\infty}\frac{e^{u/2}-e^{-u/2}}{e^{u/2}+e^{-u/2}}g(u)du \\ &= \frac{1}{2\pi}\int_0^{\infty}\int_{-\infty}^{\infty}h(r)e^{-iru}\frac{e^{u/2}-e^{-u/2}}{e^{u/2}+e^{-u/2}}drdu\ . \end{aligned}$$

We note the following equation

$$\begin{aligned} e^{-iru}\frac{e^{u/2}-e^{-u/2}}{e^{u/2}+e^{-u/2}} &= e^{-iru} - 2\left(\frac{e^{-2u}}{2u} - \frac{e^{-2u(1+ir/2)}}{1-e^{-2u}}\right) \\ &\quad + 2\left(\frac{e^{-2u}}{2u} - \frac{e^{-2u(1/2+ir/2)}}{1-e^{-2u}}\right) \end{aligned}$$

and the formula

$$\int_0^{\infty}\left(\frac{e^{-u}}{u} - \frac{e^{-u(1+ir)}}{1-e^{-u}}\right)du = \frac{\Gamma'(1+ir)}{\Gamma(1+ir)}\ .$$

If we put $\Psi(s) = (\Gamma'(s))/(\Gamma(s))$ for simplicity, the above integral is equal to

$$\frac{1}{2}h(0) - \frac{1}{2\pi}\int_{-\infty}^{\infty}h(r)\left(\Psi\left(1+\frac{ir}{2}\right) - \Psi\left(\frac{1}{2}+\frac{ir}{2}\right)\right)dr\ .$$

On the other hand, the second integral is equal to

$$\frac{2}{\pi}g(0)\log V\ .$$

Therefore

$$I_0=\frac{1}{16}\Big\{h(0)-\frac{1}{\pi}\int_{-\infty}^{\infty}h(r)\Big(\Psi\Big(1+\frac{ir}{2}\Big)-\Psi\Big(\frac{1}{2}+\frac{ir}{2}\Big)\Big)dr\Big\}$$
$$+\frac{1}{4}g(0)\log V+o(1)\ .$$

For other $\lambda(=1,\ -i,\ 1-i)$, we get similarly

$$I_\lambda=\pi\int_0^{|\lambda|^2/4V}\int_{\sqrt{(|\lambda|^2/4V)v-v^2}}^{\infty}\psi\Big(2+4\frac{r^2}{v^2}\Big)rdr\frac{dv}{v^3}$$
$$+\pi\int_{|\lambda|^2/4V}^{\infty}\int_0^{\infty}\psi\Big(2+4\frac{r^2}{v^2}\Big)rdr\frac{dv}{v^3}+o(1)\ .$$

After some calculations, I_λ is equal to

$$\frac{1}{16}\Big\{h(0)-\frac{1}{\pi}\int_{-\infty}^{\infty}h(r)\Big(\Psi\Big(1+\frac{ir}{2}\Big)-\Psi\Big(\frac{1}{2}+\frac{ir}{2}\Big)\Big)dr\Big\}$$
$$+\frac{1}{4}g(0)\Big(\log V-\log\frac{|\lambda|}{2}\Big)+o(1)\ .$$

Now we get,

Proposition 6. *Contributions from the elliptic elements of order* 4 *is given by*

$$\frac{1}{2}\sum_{\{\sigma_\lambda\}_\Gamma}\int_{\mathfrak{F}}\sum_{\sigma\in\Gamma_{\sigma_\lambda}\backslash\Gamma}\varphi(\dot g^{-1}\sigma^{-1}\sigma_\lambda\sigma\dot g)d\dot g$$
$$=\frac{1}{2}g(0)\log V+\frac{5}{16}g(0)\log 2$$
$$+\frac{1}{8}\Big\{h(0)-\frac{1}{\pi}\int_{-\infty}^{\infty}h(r)\Big(\Psi\Big(1+\frac{ir}{2}\Big)-\Psi\Big(\frac{1}{2}+\frac{ir}{2}\Big)\Big)dr\Big\}+o(1)\ ,$$

where $V\to\infty$.

Next we shall consider the parabolic elements.

We must compute the asymptotic behavior of the following integral:

$$\sum_{\{\gamma\}_\Gamma}\int_{\mathfrak{F}}\sum_{\sigma\in\Gamma_1\backslash\Gamma}\varphi(\dot g^{-1}\sigma^{-1}\gamma\sigma\dot g)d\dot g\ .$$

This reduces to

$$\sum_{\substack{\beta\in\sigma\\ \beta\neq 0}}\frac{1}{2\pi|\beta|^2}Q\Big(2+\frac{|\beta|^2}{V^2}\Big)-\sum_{\substack{\beta\in\sigma\\ \beta\neq 0}}\int_E\psi\Big(2+\frac{|\beta|^2}{v^2}\Big)\frac{dxdydv}{v^3}\qquad(\beta=x+iy)\ .$$

where $E=\cup\,\sigma\mathfrak{D}'_V$.

$$\sigma\in\Gamma_1\backslash\Gamma$$
$$\sigma\neq\Gamma_1\begin{pmatrix}1&0\\0&1\end{pmatrix},\Gamma_1\begin{pmatrix}i&0\\0&-i\end{pmatrix}$$

But the second integral is $o(1)$ when $V\to\infty$, so we have only to consider the first sum. For that purpose, we shall put

$$S=\sum_{\substack{\beta\in\sigma\\ \beta\neq 0}}\frac{1}{|\beta|^2}Q\Big(2+\frac{|\beta|^2}{V^2}\Big)$$

and

$$A(x)=\sum_{\substack{m,n\in Z\\ n^2+m^2\leqq x}}1=\pi x+P(x)\qquad(x>0)\ .$$

Then we have

$$S=\int_{1-}^{\infty}\frac{1}{x}Q\Big(2+\frac{x}{V^2}\Big)dA(x)=\pi\int_1^{\infty}\frac{1}{x}Q\Big(2+\frac{x}{V^2}\Big)dx$$
$$+\int_{1-}^{\infty}\frac{1}{x}Q\Big(2+\frac{x}{V^2}\Big)dP(x)$$

Changing the variable in the first integral and integrating by parts in the second integral, we get

$$S=\pi\int_{2+1/V^2}^{\infty}\frac{Q(w)}{w-2}dw-Q\Big(2+\frac{1}{V^2}\Big)P(1-)$$
$$+\int_{1-}^{\infty}P(x)Q\Big(2+\frac{x}{V^2}\Big)\frac{dx}{x^2}$$
$$-\frac{1}{V^2}\int_{2+1/V^2}^{\infty}\frac{P(V^2(w-2))}{w-2}dQ(w)\ .$$

In order to express the first integral in terms of h and g, we introduce a new variable u by

$$w=e^u+e^{-u}\ .$$

Let u_1 be a real number such that $2+1/V^2=e^{u_1}+e^{-u_1}$. Then

$$\int_{2+1/V^2}^{\infty}\frac{Q(w)}{w-2}dw=\int_{u_1}^{\infty}\frac{e^{u/2}+e^{-u/2}}{e^{u/2}-e^{-u/2}}g(u)du$$
$$=\frac{1}{2\pi}\int_{u_1}^{\infty}\int_{-\infty}^{\infty}h(r)e^{-iru}\frac{1+e^{-u}}{1-e^{-u}}drdu$$

$$= \frac{1}{2\pi}\int_{u_1}^{\infty}\int_{-\infty}^{\infty} h(r)\left(e^{-iru} + 2\frac{e^{-u}}{u} - 2\left(\frac{e^{-u}}{u} - \frac{e^{-u(1+ir)}}{1-e^{-u}}\right)\right)drdu$$

$$= \int_{u_1}^{\infty} g(u)du + 2g(0)\int_{u_1}^{\infty}\frac{e^{-u}}{u}du$$

$$- \frac{1}{\pi}\int_{-\infty}^{\infty}\int_{u_1}^{\infty} h(r)\left(\frac{e^{-u}}{u} - \frac{e^{-u(1+ir)}}{1-e^{-u}}\right)dudr\ .$$

With the formula of exponential integral

$$-\int_x^{\infty}\frac{e^{-u}}{u}du = \log x + C - x + \frac{x^2}{2\cdot 2!} - \cdots + \frac{(-x)^r}{rr!} + \cdots$$

where C is an *Euler constant* and with $V \sim 1/u_1$ as $V \to \infty$, we have

$$\int_{2+1/V^2}^{\infty}\frac{Q(w)}{w-2}dw = \frac{1}{2}h(0) + 2g(0)(\log V - C)$$

$$- \frac{1}{\pi}\int_{-\infty}^{\infty} h(r)\Psi(1+ir)dr + o(1)$$

where $\Psi(s) = (\Gamma'(s))/(\Gamma(s))$ as before. From the lattice point theorem we know $P(x) = 0(x^{1/2})$. Then the last three terms is equal to

$$g(0)C_{Q(i)} + o(1)$$

where $C_{Q(i)}$ is a *generalized Euler constant* attached to $Q(i)$, i.e. $C_{Q(i)} = \lim_{N\to\infty}\left(\sum_{\substack{x=n^2+m^2\le N\\ m,n\in Z\\ (m,n)\neq(0,0)}}\frac{1}{x} - \pi\log N\right)$. Therefore, we obtain

Proposition 7. *Contributions from the parabolic elements is given by*

$$\frac{1}{2}g(0)\log V + \frac{1}{8}h(0) - \frac{1}{2}g(0)C + \frac{1}{4\pi}g(0)C_{Q(i)}$$

$$- \frac{1}{4\pi}\int_{-\infty}^{\infty} h(r)\Psi(1+ir)dr + o(1)\ .$$

Finally we shall consider the Eisenstein series. We must compute the integral

$$\frac{1}{2}\int_{\mathfrak{F}_V} H(\dot g, \dot g)d\dot g$$

where $H(g, g') = \frac{1}{\pi}\int_{-\infty}^{\infty} h(r)E(g, s)\overline{E(g', s)}dr \qquad (s = 1 + ir)$.

Proposition 8. *The part of continuous spectrum is*

$$\frac{1}{2}\int_{\mathfrak{F}_V} H(\dot g, \dot g)d\dot g = g(0)\log V$$

$$- \frac{1}{4\pi}\int_{-\infty}^{\infty} h(r)\frac{\Phi'(1+ir)}{\Phi(1+ir)}dr + \frac{1}{4}h(0)\Phi(1) + o(1)$$

where $\Phi(s)$ is defined by $(\pi/(s-1))\cdot(Z(s-1)/Z(s))$ with the Dedekind zeta function $Z(s)$ of $Q(i)$.

(Sketch of the proof)

If we set $\mathfrak{F} = \mathfrak{D} \cup \begin{pmatrix} i & 0\\ 0 & -i\end{pmatrix}\mathfrak{D}$, $\mathfrak{F}_V = \mathfrak{D}_V \cup \begin{pmatrix} i & 0\\ 0 & -i\end{pmatrix}\mathfrak{D}_V$, $\mathfrak{F}'_V = \mathfrak{F} - \mathfrak{F}_V$, the above integral is

$$\int_{\mathfrak{F}_V}\int_{-\infty}^{\infty} h(r)E(\dot g, s)\overline{E(\dot g, s)}drd\dot g = \frac{1}{2}\int_{\mathfrak{F}_V}\int_{-\infty}^{\infty} h(r)E(\dot g, s)\overline{E(\dot g, s)}drd\dot g\ .$$

Define $E^V(\dot g, s)$ by

$$E^V(\dot g, s) = \begin{cases} E(\dot g, s) & \text{if } \dot g \in \mathfrak{F}_V\ ,\\ E(\dot g, s) - (v^s + \Phi(s)v^{2-s}) & \text{if } \dot g \in \mathfrak{F}'_V\ .\end{cases}$$

Then we have

$$\left|\int_{\mathfrak{F}_V}\int_{-\infty}^{\infty} h(r)\,|E(\dot g, s)|^2\,drd\dot g - \int_{\mathfrak{F}}\int_{-\infty}^{\infty} h(r)\,|E^V(\dot g, s)|^2\,drd\dot g\right| = o(1)$$

as $V \to \infty$. On the other hand,

$$\int_{\mathfrak{F}}\int_{-\infty}^{\infty} h(r)\,|E^V(\dot g, s)|^2\,drdu$$

$$= 4\pi g(0)\log V - \int_{-\infty}^{\infty} h(r)\frac{\Phi'(1+ir)}{\Phi(1+ir)}dr$$

$$+ \int_{-\infty}^{\log V}\int_{-\infty}^{\infty} h(r)\Phi(s)e^{-2ir(\log v)}drd(\log v)$$

$$- \int_V^{\infty}\int_{-\infty}^{\infty} h(r)\overline{\Phi(s)}v^{-1+2ir}drdv$$

$$= 4\pi g(0)\log V - \int_{-\infty}^{\infty} h(r)\frac{\Phi'(1+ir)}{\Phi(1+ir)}dr + \pi h(0)\Phi(1) + o(1)$$

as $V \to \infty$, hence the proposition follows.

Theorem 9. *Let $\mathcal{O}$ be the ring of integers of $Q(i)$ and let $\Gamma = SL(2, \mathcal{O})$ be a special linear subgroup of G with entries in $\mathcal{O}$. Then the trace formula for Γ is*

$$\sum h(r_j) = \frac{Z(2)}{2\pi^4}\int_{-\infty}^{\infty} r^2 h(r)dr + \frac{2\log(2+\sqrt{3})}{9\pi}\int_{-\infty}^{\infty} h(r)dr$$
$$+\frac{1}{2}\sum_{\alpha\in A}\sum_{k=1}^{\infty}\frac{\log|N\{\gamma_\alpha\}|\, g(k\log|N\{\gamma_\alpha\}|)}{|N\{\gamma_\alpha\}^{k/2} - N\{\gamma_\alpha\}^{-k/2}|^2\,[\Gamma_{\gamma_\alpha}:(\Gamma_{\gamma_\alpha})']}$$
$$+\frac{1}{4}h(0) + \frac{5}{16}g(0)\log 2 - \frac{1}{2}g(0)C + \frac{1}{4\pi}g(0)C_{Q(i)}$$
$$-\frac{1}{4}h(0)\Phi(1) - \frac{1}{8\pi}\int_{-\infty}^{\infty} h(r)\Big(\Psi\Big(1+\frac{ir}{2}\Big)$$
$$-\Psi\Big(\frac{1}{2}+\frac{ir}{2}\Big) + 2\Psi(1+ir)\Big)dr + \frac{1}{4\pi}\int_{-\infty}^{\infty} h(r)\frac{\Phi'(1+ir)}{\Phi(1+ir)}dr\,.$$

References

[1] Faddeev, L., Expansion in eigenfunctions of the Laplace operator on the fundamental domain of a discrete group on the Lobacevskii plane, Transactions Moscow Math. Soc. A.M.S. Trudy **17** (1967), 357–386.

[2] Godement, R., The decomposition of $L^2(G/\Gamma)$ for $\Gamma = SL(2, Z)$, Proc. Symp. Pure Math. A.M.S. **9** (1966), 211–224.

[3] Kubota, T., Topics around a discrete subgroup of Picard type. Proceedings of the Symposium on the arithemetic of discontinuous groups. Kanazawa-Yamashiro, 1965 **8** (1966), 9–20. (Japanese)

[4] —, Elementary Theory of Eisenstein Series, Kodansha Ltd. Tokyo, 1973.

[5] Selberg, A., Harmonic analysis and discontinuous groups in weakly symmetric Riemannian spaces with applications to Dirichlet series. J. Indian Math. Soc. **20** (1956), 47–87.

[6] de la Torre, P., Selberg's trace formula for 3-dimensional hyperbolic space (private note to Professor Kubota).

[7] Venkov, A. B., Expansion in automorphic eigenfunctions of the Laplace-Beltrami operator in classical symmetric spaces of rank one, and the Selberg trace formula, Proc. Steklov Inst. Math. **125** (1973), 1–48.

[8] Weil, A., Dirichlet series and automorphic forms, Lecture Notes in Math. **189**, Springer, Berlin, 1971.

Department of Mathematics
Faculty of Science
Nagoya University
Chikusa-ku, Nagoya 464
Japan

ALGEBRAIC NUMBER THEORY, Papers contributed for the International Symposium, Kyoto 1976; S. Iyanaga (Ed.): Japan Society for the Promotion of Science, Tokyo, 1977

On the Torsion in K_2 of Fields*

J. TATE

§ 1. Introduction

Let F be a field and F^* its multiplicative group. Let R_F denote the subgroup of $F^* \otimes F^*$ generated by the elements $a \otimes b$ with $a + b = 1$. Theorems of Steinberg and Matsumoto give a canonical isomorphism

$$(F^* \otimes F^*)/R_F \xrightarrow{\sim} K_2F$$

(see [5], for example). The image of $a \otimes b$ in K_2F is denoted by $\{a, b\}$. We have $\{a, -a\} = 1$ and $\{a, b\}\{b, a\} = 1$. That's about all the algebraic K-theory we use in this paper except for the existence of a "K_2-norm" which we now recall.

Suppose E is an extension field of F. The inclusion $F \subset E$ induces a homomorphism $K_2F \to K_2E$ such that $\{a, b\}_F \mapsto \{a, b\}_E$, for a and b in F^*, where the subscripts F and E are added to make clear in which K_2 group the symbol $\{a, b\}$ is to be interpreted. If the degree of E over F is finite, then there is a "natural" K_2-norm homomorphism $N_{E/F}: K_2E \to K_2F$ such that

$$N_{E/F}\{a, b\}_E = \{a, N_{E/F}b\}_F$$

for $a \in F^*$ and $b \in E^*$ (see [5, § 14]). When neither a nor b is in F the image of $\{a, b\}_E$ under the norm map is not easy to describe in terms of the symbols $\{\ ,\ \}_F$, although there do seem to be complicated algorithms for such computations hidden in [1, Ch. I, § 5].

Now let m be an integer ≥ 1 and suppose F contains a primitive m-th root of unity, z. Then there is a complex

$$(1.1)\qquad F^* \xrightarrow{m} F^* \xrightarrow{g} K_2F \xrightarrow{m} K_2F \xrightarrow{h} \mathrm{Br}\,F \xrightarrow{m} \mathrm{Br}\,F\,,$$

* Work partially supported by NSF.

where $\mathrm{Br}\,F$ denotes the Brauer group of F, the maps labelled by m are the endomorphisms $x \mapsto x^m$ of the abelian group in question, and the homomorphisms g and h are given by $g(a) = \{z, a\}$ and $h(\{a, b\}) = \langle a, b\rangle$, where $\langle a, b\rangle$ is the class of the "cyclic" algebra $A_{a,b}$ of degree m^2 over F defined by

$$A_{a,b} = F[\alpha, \beta]\ , \quad \alpha^m = a, \beta^m = b\ , \quad \text{and } \alpha\beta = z\beta\alpha\ .$$

The complex (1.1) has a tendency to be acyclic; I know of no field F for which any one of the three "homology" groups

$$\mathrm{Br}_m F/\mathrm{Im}\, h\ , \quad \mathrm{Ker}\, h/(K_2F)^m\ , \quad (K_2F)_m/\mathrm{Im}\, g$$

is known to be non-zero (we write X_m for the kernel of $m: X \to X$). These three groups *are* zero if F is a global or local field, or a field of cohomological dimension 1. For the first group this is classical; for example, if $m = 2$, the vanishing of $\mathrm{Br}_m F/\mathrm{Im}\, h$ is equivalent to every element of order 2 in the Brauer group being a product of classes of quaternion algebras. The second group, $\mathrm{Ker}\, h/(K_2F)^m$ is discussed in [9], where some criteria for it to vanish are derived. In this paper we study the third group $(K_2F)_m/\mathrm{Im}\, g$ by a method proposed originally by Birch [2] in case $m = 2$, which was seen by Bass to be generalizable to arbitrary m by using the K_2-norm. This method is described in § 2. Bass' generalization of Birch's idea raises a curious algebraic problem (cf. (2.6) below) which we have been unable to solve.

In § 3 these ideas are applied to fields F of cohomological dimension 1 (meaning roughly that $\mathrm{Br}\,F = 0$). For such fields all difficulties vanish and the method gives immediately $(K_2F)_m = \mathrm{Im}\, g$. This is true in particular if F is a function field in one variable over an algebraically closed field. In that case I would conjecture that the fourth "homology group", $\mathrm{Ker}\, g/(F^*)^m$, of our sequence (1.1) is also trivial, and there is a brief discussion of this problem at the end of § 3.

In § 4 we use the method of Birch and Bass to prove a relative result, to the effect that for a subfield $F_0 \subset F$ such that $F_0^*/(F_0^*)^m$ maps isomorphically to $F^*/(F^*)^m$, the map $(K_2F_0)_m \to (K_2F)_m$ is surjective.

In § 5 we prove $(K_2F)_m = \mathrm{Im}\, g$ for local fields by using the result of § 4 to reduce that question to the corresponding statement for global fields which is known to be true. We also discuss in detail (Theorem (5.5)) the relationships among some conjectures of Lichtenbaum's and mine on the torsion in K_2 of local fields. Finally, we are able to prove all these conjectures in the special case that $\boldsymbol{Q}_l \subset F \subset \boldsymbol{Q}_l(a)$, where $\boldsymbol{Q}_l$ is the field of l-adic numbers, and a is an

l-power root of unity. Thus for such an F there is a canonical splitting of K_2F into the direct sum of its torsion subgroup $(K_2F)_{\mathrm{tors}}$ and its maximal divisible subgroup $(K_2F)_d$, which is *uniquely* divisible; and if F_0 is the algebraic closure of $\boldsymbol{Q}$ in F we have canonical isomorphisms

$$K_2F_0 \xrightarrow{\sim} (K_2F)_{\mathrm{tors}} \xrightarrow{\sim} \mu_F$$

where μ_F is the group of all roots of 1 in F, the map to μ_F being given by the norm residue symbol.

The results of § 4 and § 5 were not known to me at the time of the conference in Kyoto. My talk there was more in the nature of a report on unsolved problems. It was only in preparing this written version that I found at least the partial answers given here.

§ 2. Extracting roots of symbols

Let F be a field containing a primitive m-th root of unity, z, for some integer $m \geq 1$. Let $X \subset K_2F$ be the group of elements of the form $\{z, a\}$ with $a \in F^*$. Since $z^m = 1$ we have $X \subset (K_2F)_m$; we want to find conditions under which these two groups are equal, i.e., under which every element of order dividing m in K_2F is of the form $\{z, a\}$.

The equality $X = (K_2F)_m$ is equivalent to the existence of a homomorphism $f: (K_2F)^m \to K_2F/X$ such that $f(u^m) = uX$ for all $u \in K_2F$, and such a homomorphism, if it exists, is unique. In [2], Birch proposed a method for constructing such an f in case $m = 2$. Bass remarked that by using the K_2-norm, a corresponding approach could be devised for arbitrary m. The idea is the following. For $a, b \in F^*$ it is well known ([5], Theorem 15.12, or [9], Proposition 4.3) that the following statements are equivalent

(i) $\{a, b\} \in (K_2F)^m$

(ii) There exists a finite extension field E of F and elements α and $\beta \in E$ such that $\alpha^m = a$ and $N_{E/F}\beta = b$.

The idea of Birch is that the proof of (ii) $\Rightarrow$ (i) yields more than just $\{a, b\} \in (K_2F)^m$; it furnishes an "m-th root" of $\{a, b\}$, namely $N_{E/F}\{\alpha, \beta\}$, which is *uniquely determined modulo* X.

(2.1) **Lemma.** *For E, α, and β as in condition* (ii), *the class of $N_{E/F}\{\alpha, \beta\}$ modulo X depends only on the pair a, b.*

Clearly it suffices to consider fields E contained in a fixed algebraic closure of F. Then α is determined by a up to a power of z, so that changing α

changes $N_{E/F}\{\alpha, \beta\}$ by a power of $N_{E/F}\{z, \beta\} = \{z, N_{E/F}\beta\} = \{z, b\} \in X$. Let $E_1 = F(\alpha)$, and $\beta_1 = N_{E/E_1}\beta$. By the transitivity of the K_2-norm we have

$$N_{E/F}\{\alpha, \beta\} = N_{E_1/F}N_{E/E_1}\{\alpha, \beta\} = N_{E_1/F}\{\alpha, \beta_1\} ,$$

and since $N_{E_1/F}\beta_1 = b$, we can assume from now on that $E = E_1 = F(\alpha)$. We must show then that for fixed α the class of $N_{E/F}\{\alpha, \beta\}$ modulo X depends only on $N_{E/F}\beta$, or what is the same, that $N_{E/F}\{\alpha, \beta\} \in X$ if $N_{E/F}\beta = 1$. Suppose $N_{E/F}\beta = 1$, and let σ be a generator of the cyclic group $\mathrm{Gal}\,(E/F)$. Then by Hilbert's Theorem 90 we have $\beta = \gamma^\sigma/\gamma$ for some element $\gamma \in E^*$, and since

$$N_{E/F}\{\alpha, \gamma^\sigma\} = N_{E/F}(\{\alpha, \gamma^\sigma\}^{\sigma^{-1}}) = N_{E/F}\{\alpha^{\sigma^{-1}}, \gamma\} ,$$

we have $N_{E/F}\{\alpha, \beta\} = N_{E/F}\{\alpha^{\sigma^{-1}}/\alpha, \gamma\}$. This is in X, because $\alpha^{\sigma^{-1}}/\alpha$ is a power of z.

Let P be the set of all pairs $a \times b \in F^* \times F^*$ satisfying the equivalent conditions (i) and (ii) above. In view of (2.1) we can define a map $f: P \to K_2F/X$ by

$$f(a, b) = N_{E/F}\{\alpha, \beta\}X , \tag{2.2}$$

where E, α, and β are related to a and b as in condition (ii).

(2.3) *Example* (Birch [2]). Suppose $m = 2$. Then P is the set of all $a \times b \in F^* \times F^*$ such that the equation $ax^2 + by^2 = 1$ has a solution in non-zero elements $x, y \in F^*$, and for any such x, y we have

$$f(a, b) = \{y, a\}\{b, x\}\{y, x\}^2 , \qquad \mathrm{mod}\ X . \tag{2.4}$$

Indeed let α be a square root of a. If $\alpha \notin F$, then to compute $f(a, b)$ we can take $E = F(\alpha)$, $\beta = y^{-1}(1 + x\alpha)$, and have

$$\begin{aligned} f(a, b) &= N_{E/F}\left\{\alpha, \frac{1 + x\alpha}{y}\right\} = N_{E/F}\left(\frac{\{-x\alpha,\ 1 + x\alpha\}}{\{\alpha, y\}\{-x, 1 + x\alpha\}}\right) \\ &= \frac{1}{\{-a, y\}\{-x, 1 - x^2a\}} = \{y, -a\}\{by^2, -x\} \\ &\equiv \{y, a\}\{by^2, x\} \bmod X . \end{aligned}$$

We leave to the reader the verification of (2.4) in case $\alpha \in F$, i.e., $a \in (F^*)^2$.

(2.5) **Proposition.** *The map f has the following properties:*

(2.5.1) *For all $a \times b \in P$ we have*

$$\{a, b\} = (f(a, b))^m$$

in the sense that $\{a, b\} = \theta^m$ if $f(a, b) = \theta X$.

(2.5.2) *For $a \in F^*$, $a \neq 1$, we have*

$$f(a, 1 - a) = 1 , \quad \text{and} \quad f(a, -a) = 1 .$$

(2.5.3) *For $a \times b$ and $a \times b'$ in P we have*

$$f(a, bb') = f(a, b)f(a, b') .$$

(2.5.4) *Suppose $a \times b$ and $a' \times b$ are in P. If b is a norm from $F(a^{1/m}, (a')^{1/m})$, then*

$$f(aa', b) = f(a, b)f(a', b) .$$

In particular, this rule holds if either a or a' is in $(F^*)^m$.

(2.5.5) *For all $a \times b \in F^* \times F^*$ we have*

$$f(a^m, b) = \{a, b\}X = f(a, b^m) .$$

Proof of (2.5.1): With notation as in (2.2) we have

$$\begin{aligned} (f(a, b))^m &= (N_{E/F}\{\alpha, \beta\})^m = N_{E/F}\{\alpha^m, \beta\} \\ &= N_{E/F}\{a, \beta\} = \{a, N_{E/F}\beta\} = \{a, b\} . \end{aligned}$$

Proof of (2.5.2): Let $E = F(\alpha)$, where α is an m-th root of a in some extension field of F. Then E/F is a cyclic extension whose degree $n = [E: F]$ divides m; say $m = rn$. Then

$$1 - a = \prod_{i=0}^{m-1}(1 - z^i\alpha) = \prod_{j=0}^{r-1}\prod_{k=0}^{n-1}(1 - z^{j+rk}\alpha) = \prod_{j=0}^{r-1}N_{E/F}(1 - z^j\alpha) .$$

Hence

$$f(a, 1 - a) = \prod_{j=0}^{r-1}N_{E/F}\{\alpha, 1 - z^j\alpha\} ,$$

and this is in X because $\{z^j\alpha, 1 - z^j\alpha\} = 1$ and $N_{E/F}\{z^j, \beta\} \in X$ for all $\beta \in E$. The case of $f(a, -a)$ is handled similarly, replacing $1 - z^i\alpha$ by $-z^i\alpha$ in the above.

Proof of (2.5.3): Let α be an m-th root of a, let $E = F(\alpha)$, and let β and β' be elements of E such that $N_{E/F}\beta = b$ and $N_{E/F}\beta' = b'$. Then $N_{E/F}\beta\beta' = bb'$, so

$$f(a, bb') = N_{E/F}\{\alpha, \beta\beta'\} = N_{E/F}\{\alpha, \beta\}N_{E/F}\{\alpha, \beta'\} = f(a, b)f(a, b') .$$

Proof of (2.5.4): Let $E = F(\alpha, \alpha')$, where $\alpha^m = a$ and $(\alpha')^m = a'$. If $b =$

$N_{E/F}\beta$ for some $\beta \in E$, then

$$f(aa', b) = N_{E/F}\{\alpha\alpha', \beta\} = N_{E/F}\{\alpha, \beta\}\{\alpha', \beta\} = f(a, b)f(a', b) .$$

Proof of (2.5.5): To compute $f(a^m, b)$ we can take $E = F$, $\beta = b$, and find $\{a, b\}$ as the result immediately. For $f(a, b^m)$, let E, α, r, and n be related to a as in the proof of (2.3.2) above. Then

$$\begin{aligned} f(a, b^m) &= N_{E/F}\{\alpha, b^r\} = N_{E/F}\{\alpha^r, b\} \\ &= \{N_{E/F}\alpha^r, b\} = \{z^j\alpha^{rn}, b\} \end{aligned}$$

for some j. Since $\alpha^{rn} = \alpha^m = a$, this is congruent modulo X to $\{a, b\}$.

(2.6) *Remark.* It looks like an interesting algebraic problem to prove that the rule $f(aa', b) = f(a, b)f(a', b)$ holds in general without any hypothesis. If this were so, then f would be bimultiplicative on its domain P. Since $f(a, -a) = 1$ is known, bimultiplicativity would imply skew-symmetry, i.e., $f(a, b)f(b, a) = 1$. Conversely, since f is multiplicative on the right, skew-symmetry would imply bimultiplicativity. Skew-symmetry would follow in turn from the rule $f(a, b) = f(-ab, b)$ for $a \times b \in P$, for that would imply $f(a, b)f(b, a) = f(-ab, b)f(-ab, a) = f(-ab, ab) = 1$. These things are at least true in many cases. If $m = 2$, then f is skew-symmetric by (2.4), hence bimultiplicative. Also f is bimultiplicative whenever $X = (K_2F)_m$, because in that case $f(a, b)$ is *characterized* by the fact that $(f(a, b))^m = \{a, b\}$. Hence bimultiplicativity holds if F is an algebraic number field or an algebraic function field in one variable over a finite field (cf. [9]).

The map f is functorial in the following sense

(2.7) **Lemma.** *Let F' be a field containing F. Then the following diagram is commutative*

$$\begin{array}{ccc} P & \longrightarrow & P' \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f'} \\ K_2F/X & \longrightarrow & K_2F'/X' \end{array}$$

where P', X', and f' have the same meaning for F' as P, X, and f do for F, and where the horizontal arrows are induced by the inclusion of F in F'.

Let $a \times b \in P$ and let α be an m-th root of a in some field containing F'. Let $E = F(\alpha)$ and $E' = F'(\alpha)$. Let $F_1 = E \cap F'$. Let $\beta \in E$ be such that $N_{E/F}\beta = b$. Let

$$K_2F \xrightarrow{i} K_2F_1 \xrightarrow{j} K_2F'$$

be the maps induced by the inclusions $F \subset F_1 \subset F'$. Then

$$\begin{aligned} iN_{E/F}\{\alpha, \beta\} &= iN_{F_1/F}(N_{E/F_1}\{\alpha, \beta\}) = \prod_{\sigma \in \mathrm{Gal}\,(F_1/F)} (N_{E/F_1}\{\alpha, \beta\})^\sigma \\ &= \prod_{\sigma \in R} N_{E/F_1}\{\alpha^\sigma, \beta^\sigma\} , \end{aligned}$$

if R is some chosen set of representatives for the cosets of $\mathrm{Gal}\,(E/F_1)$ in $\mathrm{Gal}\,(E/F)$. Since α^σ/α is a power of z for each $\sigma \in R$ we have

$$iN_{E/F}\{\alpha, \beta\} \equiv \prod_{\sigma \in R} N_{E/F_1}\{\alpha, \beta^\sigma\} = N_{E/F_1}\{\alpha, \beta'\} \mod \{z, F_1^*\} ,$$

where $\beta' = \prod_{\sigma \in R} \beta^\sigma$. Since $E \otimes_{F_1} F' \to E'$ is an isomorphism we have then

$$jiN_{E/F}\{\alpha, \beta\} \equiv jN_{E/F_1}\{\alpha, \beta'\} = N_{E'/F'}\{\alpha, \beta'\} .$$

On the other hand,

$$\begin{aligned} N_{E'/F'}\beta' = N_{E/F_1}\beta' &= N_{E/F_1}\Big(\prod_{\sigma \in R} \beta^\sigma\Big) \\ &= \prod_{\sigma \in R} (N_{E/F_1}\beta)^\sigma = N_{E/F}\beta = b . \end{aligned}$$

Hence $f'(a, b) = N_{E'/F'}\{\alpha', \beta'\}X' = jiN_{E/F}\{\alpha, \beta\}X = jif(a, b)$ as was to be shown.

§ 3. Fields of cohomological dimension 1

The method of Birch works beautifully when F satisfies the following condition:

(3.1) $\mathrm{Br}_m F' = 1$ *for each finite extension F' of F.*

This condition is satisfied by fields of dimension 1 in the sense of [7, Ch. II, § 3] and C_1-fields, in particular, function fields in one variable over algebraically closed fields (Theorem of Tsen), fields complete with respect to a discrete valuation with algebraically closed residue field (Lang), and finite fields.

(3.2) **Theorem.** *Suppose our field F with the primitive m-th root of unity, z, satisfies condition* (3.1). *Then K_2F is divisible by m, and an element $x \in K_2F$ such that $x^m = 1$ is of the form $x = \{z, a\}$ for some $a \in F^*$.*

Condition (3.1) implies, via the theory of "cyclic algebras", that $P = F^* \times F^*$. Thus $f(a, b)$ is defined for every pair $a \times b \in F^* \times F^*$, and each generator $\{a, b\}$ of K_2F is an m-th power, so K_2F is divisible by m. Condition (3.1) also implies that for each finite extension F' of F and each element $a' \in F'$, the norm

map $N_{E/F'}: E^* \to (F')^*$ is surjective, for $E = F'((a')^{1/m})$. By the transitivity of of the norm, it follows that for any two elements $a, a' \in F^*$, the map $N_{E/F}$ is surjective for $E = F(a^{1/m}, (a')^{1/m})$. Hence $f(a, b)$ is multiplicative in a, by (2.5.4). It is multiplicative in b by (2.5.3) and satisfies $f(a, 1-a) = 1$ by (2.5.2). Being defined on all of $F^* \times F^*$ it is therefore a "symbol", and there is a homomorphism $f_0: K_2F \to K_2F/X$ such that $f_0(\{a, b\}) = f(a, b)$ for all $a, b \in F^*$. We have $f_0(x^m) = xX$, by (2.5.5) for $x = \{a, b\}$, and hence for all $x \in K_2F$. If $x^m = 1$ it follows that $x \in X$, i.e., x is of the form $\{z, a\}$ as was to be shown.

Suppose F is a function field in one variable over an algebraically closed constant field k. The map

$$F^*/(F^*)^m \longrightarrow (K_2F)_m \tag{3.3}$$

induced by $x \to \{z, x\}$ is surjective, as we have just seen. *Is it bijective*? When k is the algebraic closure of a finite field the answer is "yes", as can be seen by viewing F as a limit of function fields over finite fields and applying results of [9]. In any case, the existence of "tame symbols" at the places of F shows that if x is in the kernel of (3.3), then the divisor of x is divisible by m. It follows that the kernel of (3.3) is isomorphic to a subgroup of the group of divisor classes of order m on F, so is contained in a product of $2g$ cyclic groups of order m, if g is the genus of F. For example, if $m = 2$ and F is the function field of an elliptic curve of the form $y^2 = (x - e_1)(x - e_2)(x - e_3)$, then the injectivity of (3.3) is equivalent to the statement that $\{-1, x - e_i\} \neq 1$ in K_2F, for each $i = 1, 2, 3$. I don't know whether this is true, even in the "classical" case $k = C$.

§ 4. A condition for $(K_2F_0)_m \to (K_2F)_m$ to be surjective

Suppose F_0 is a subfield of F containing the primitive m-th root of unity z and such that

$$F^* = F_0^*(F^*)^m \quad \textit{and} \quad F_0^* \cap (F^*)^m = (F_0^*)^m\ , \tag{4.1}$$

in other words such that the natural map $F_0^*/(F_0^*)^m \to F^*/(F^*)^m$ is bijective. Let X_0, P_0, and f_0 have the same meaning for F_0 as X, P, and f do for F. The condition

$$P_0 = P \cap (F_0^* \times F_0^*) \tag{4.2}$$

is implied by

(4.3) *If $a \in F_0^*$ and α is an m-th root of a in an extension field of F, then* $F(\alpha)^* = F_0(\alpha)^*(F(\alpha)^*)^m$.

Indeed, suppose $a, b \in F_0^*$ and $a \times b \in P$. With α as in (4.3) there is a $\beta \in F(\alpha)$ such that $b = N_{F(\alpha)/F}\beta$. We must show that b is a norm from $F_0(\alpha)$. By (4.3) we have $\beta = \beta_0\gamma^m$ with $\beta_0 \in F_0(\alpha)$. By (4.1) and Kummer theory, the degrees $[F_0(\alpha): F_0]$ and $[F(\alpha): F]$ are the same, so $N_{F_0(\alpha)/F_0}\beta_0 = N_{F(\alpha)/F}\beta_0$. Hence

$$b = N_{F(\alpha)/F}(\beta_0\gamma^m) = (N_{F_0(\alpha)/F_0}\beta_0)c^m\ , \qquad \text{where } c = N_{F(\alpha)/F}\gamma\ .$$

Since $c^m \in F_0$ we have $c \in F_0$ by (4.1). Hence b is a norm from $F_0(\alpha)$ as we wanted to show.

(4.4) **Theorem.** *Suppose F_0 is a subfield of F containing the primitive m-th root of unity z, and satisfying conditions* (4.1) *and* (4.2). *Then the natural map $(K_2F_0)_m \to (K_2F)_m$ is surjective.*

Let U be an abelian group like the unit circle which is divisible and has elements of all orders. To prove the theorem it is enough by duality to show that any homomorphism $s: K_2F \to U$ which kills the image of $(K_2F_0)_m$ in K_2F also kills $(K_2F)_m$. Let s be such a homomorphism and let $s_0: K_2F_0 \to U$ be the homomorphism obtained by composing s with the natural map $K_2F_0 \to K_2F$. Then s_0 kills $(K_2F_0)_m$ and consequently, since U is divisible, there exists a homomorphism $t_0: K_2F_0 \to U$ such that $s_0 = t_0^m$.

For convenience we will write simply $s(a, b)$ instead of $s(\{a, b\})$ for $a, b \in F^*$, and similarly with s_0 and t_0, when $a, b \in F_0^*$. We want to construct a homomorphism $t: K_2F \to U$ such that $s = t^m$. To do this we try to define a "symbol" $t: F^* \times F^* \to U$ as follows. For $a, b \in F^*$, let, by (4.1),

$$a = a_0x^m \qquad b = b_0y^m \tag{4.5}$$

with $a_0, b_0 \in F_0^*$, and put

$$\begin{aligned} t(a, b) &= t_0(a_0, b_0)s(a_0, y)s(x, b) \\ &= t_0(a_0, b_0)s(a_0, y)s(x, b_0)s(x, y)^m \\ &= t_0(a_0, b_0)s(x, b_0)s(a, y)\ . \end{aligned} \tag{4.6}$$

To check that this $t(a, b)$ is independent of the choice of a_0, x and b_0, y in (4.5), note that, for example, a different choice of b_0 and y would be of the form

$$b_0' = b_0v_0^m \quad \text{and} \quad y' = yv_0^{-1}$$

with $v_0 \in F_0$ because of (4.1). The new value of $t(a, b)$ is then

$$t_0(a_0, b_0 v_0^m)s(a_0, y v_0^{-1})s(x, b)$$
$$= t_0(a_0, b_0)t_0(a_0, v_0)^m s_0(a_0, v_0)^{-1}s(a_0, y)s(x, b)$$

and this is the same as the old, since $s_0 = t_0^m$. Similarly, $t(a, b)$ is independent of the decomposition $a = a_0 x^m$. Thus t is well-defined. It is obviously bi-multiplicative. The key fact is

(4.7) **Lemma.** *Suppose* $a \times b \in P$. *Then* $t(a, b) = s(f(a, b))$. (Here $f: P \to K_2F/X$ is the map defined in § 2; note that $s(f(a, b))$ is well-defined, i.e., $s(X) = 1$, because by (4.1) any element of X is of the form $\{a_0, z\}$ with $a_0 \in F_0^*$, so X is in the image of $(K_2F_0)_m$.)

Suppose (4.7) is proved. Taking $b = 1 - a$ we find, by (2.5.2), that $t(a, 1 - a) = 1$, for any $a \in F^*$. Hence t is a "symbol" and induces a homomorphism $t: K_2F \to U$ such that $t(\{a, b\}) = t(a, b)$. We have $t^m = s$ because, using $t_0^m = s_0$, we find

$$t(a, b)^m = s_0(a_0, b_0)s(a_0, y^m)s(x^m, b_0)s(x, y)^m$$
$$= s(a_0 x^m, b_0 y^m) = s(a, b) .$$

Hence s kills $(K_2F)_m$ as was to be shown. The theorem will be proved, once we give the

Proof of (4.7): Expressing a and b as in (4.5) we have

$$a \times b \in P \Longrightarrow a_0 \times b_0 \in P \Longrightarrow a_0 \times b_0 \in P_0 ,$$

by (4.2). Using (2.5.1) for f_0 we can therefore write

$$t_0(a_0, b_0) = t_0(\{a_0, b_0\}) = t_0(f_0(a_0, b_0)^m) = s_0(f_0(a_0, b_0)) .$$

Similarly, using (2.5.5) for f,

$$s(a_0, y) = s(f(a_0, y^m)) , \quad \text{and} \quad s(x, b) = s(f(x^m, b)) .$$

Thus by (4.6)

$$t(a, b) = s_0(f_0(a_0, b_0))s(f(a_0, y^m))s(f(x^m, b)) .$$

By the functorality of f (2.7), we have $s_0 \cdot f_0 = s \cdot f$ on P_0, so

$$t(a, b) = s(f(a_0, b_0)f(a_0, y^m)f(x_m, b))$$
$$= s(f(a_0, b)f(x^m, b)) \qquad \text{by (2.5.3)}$$
$$= s(f(a, b)) \qquad \text{by (2.4.5)} ,$$

which applies because $x^m \in F^{*m}$.

§ 5. Local fields

Let F_{00} be a global field, i.e., a finite extension of the field of rational numbers, or of the field of rational functions in one variable over a finite field. From now on we suppose that F is the completion of F_{00} at a place v, and that F_0 is the algebraic closure of F_{00} in F. We still suppose z is a root of 1 in F, hence in F_0 too, of order $m \geq 1$.

(5.1) **Proposition.** a) *The natural map* $(K_2F_0)_m \to (K_2F)_m$ *is surjective.*

b) *Let* l *be any prime number. Then* $(K_2F_0)_l \to (K_2F)_l$ *is surjective, whether or not* F *contains the* l*-th roots of* 1.

To prove (a), via (4.4), we will show that the pair F_0 and F satisfy conditions (4.1) and (4.2). The condition $(F^*)^m \cap F_0^* = (F_0^*)^m$ holds because F_0 is algebraically closed in F. On the other hand, we have $F^* = F_0^*(F^*)^m$ because F_0^* is dense in F^* and $(F^*)^m$ is open in F^*. (This last is obvious if F is the real or complex field; in the non-archimedean case "Newton's method" furnishes a root x of $x^m = a$ for a such that $v(a - 1) > 2v(m)$.) Condition (4.2) is implied by (4.3), and (4.3) is satisfied because if α is an m-th root of $a \in F_0$, then $F_0(\alpha)$ is dense in $F(\alpha)$, so that $F(\alpha)^* = F_0(\alpha)^*(F(\alpha)^*)^m$.

We now prove (b). If l is equal to the characteristic of F then there is nothing to prove, because $(K_2F)_l = 0$. This is a consequence of the fact that $[F: F^l] = l$. The map $x \mapsto x^l$ is an isomorphism of $F^{1/l}$ onto F; hence the map

$$\{x, y\} \mapsto \{x^l, y^l\} = N_{F^{l-1}/F}\{x^l, y\} = N_{F^{l-1}/F}\{x, y\}^l$$

gives an isomorphism $K_2F^{l-1} \xrightarrow{\sim} K_2F$. It follows immediately from this that the K_2-norm is surjective for the extension F^{l-1}/F, and that K_2F is uniquely divisible by l.

Suppose l is different from the characteristic of F. Let $F_0' = F_0(w)$, and $F' = F_0'F = F(w)$, where w is a primitive l-th root of unity. It is easy to see that F_0' is algebraically closed in F' and that F'/F and F_0'/F_0 are Galois with the "same" Galois group, G, which is of order prime to l. Part (a) of the Proposition, applied to the field F' with $m = l$, shows that $(K_2F_0')_l \to (K_2F')_l$ is surjective. It follows that

$$(K_2F_0)_l = (K_2F_0')_l^G \longrightarrow (K_2F')_l^G = (K_2F)_l$$

is surjective because the functor $A \mapsto A^G$ is exact on the category of G-modules killed by l. The fact that $(K_2F)_l = (K_2F')_l^G$, and similarly for F_0, can be

proved by a simple argument using the K_2-norm as, for example, in the proof of Lemma 3.3 in [9].

(5.2) **Theorem.** *Locally compact non-discrete fields E have the following property: If E contains a root of unity z of order $m \geq 1$, then every element $x \in K_2E$ such that $x^m = 1$ is of the form $x = \{z, a\}$ with $a \in E^*$.*

Global fields have this property. This is Theorem 6.1 of [9] when $m = l$ is prime, and the case of general m follows by induction on m. (If l is a prime dividing m and $x^m = 1$ we can assume inductively that $x^l = \{z^l, b\}$. Then $(x\{z, b\}^{-1})^l = 1$, so, by the prime case, we have $x\{z, b\}^{-1} = \{z^{m/l}, c\} = \{z, c^{m/l}\}$, and finally $x = \{z, bc^{m/l}\}$.) The property in question carries over to direct limits, because K_2 commutes with direct limits. Hence the field F_0 of Proposition (5.1) has the property, for F_0 is a union of global fields. The property carries over to F by part (a) of the Proposition; and any locally compact non-discrete field is isomorphic to such an F.

(5.3) *Remark.* When F is non-archimedean and m is prime to the residue characteristic of F, Theorem (5.2) is due to J. E. Carroll [3]. Carroll's proof is local, whereas ours is global.

We want now to investigate the whole torsion subgroup $(K_2F)_{\text{tors}}$ of K_2F, and its relation to K_2F_0. (Recall that K_2F_0 is a torsion group, by Garland's theorem in the number field case, and by [1, Ch. II, § 2] in the function field case.) If F is the complex field $\boldsymbol{C}$, then both groups vanish, for it is well known (and follows easily from (3.2)) that the K_2 of an algebraically closed field is uniquely divisible.

Suppose now the place v is not complex, i.e., F is not isomorphic to the complex field $\boldsymbol{C}$. Then F contains only a finite number of roots of 1. Let m be the number of roots of unity in F and let $\mu_m = (F^*)_{\text{tors}}$ be the group they form. Consider the diagram

(5.4)
$$\begin{array}{ccc} K_2F_0 & \xrightarrow{\beta_0} & \\ {\scriptstyle\alpha}\downarrow & & \mu_m = (F^*)_{\text{tors}} \\ (K_2F)_{\text{tors}} & \xrightarrow{\beta} & \end{array}$$

where α is induced by the inclusion $F_0 \subset F$ and where β and $\beta_0 = \beta\alpha$ are the homomorphisms given by the m-th power local norm residue symbol

$$\beta_0, \beta\colon \{a, b\} \longrightarrow (a, b)_m .$$

The maps β_0 and β are surjective because the norm residue pairing is non-degenerate, and the natural map $\mu_m \to F_0^*/(F_0^*)^m \approx F^*/(F^*)^m$ is injective. As we shall see below, α is surjective as well. Hence the statement "*β_0 is bijective*" is equivalent to the conjunction of the two statements "*α is bijective*" and "*β is bijective*". The first of these three statements has been conjectured by Lichtenbaum. The second is mentioned in problem 10, p. 19 of [4]. The third is an old hope of mine [9]. I would certainly guess that the maps α, β, and β_0 are isomorphisms in all cases. The theorem below summarizes what I can prove at present in that direction. The real case is easy, and the results on the parts prime to the residue characteristic in the non-archimedean case are essentially due to Carroll [3].

(5.5) **Theorem.** 1) *The three maps α, β, and β_0 in diagram* (5.4) *are surjective in all cases.*

2) *They are bijective in the function field case* (char $F \neq 0$) *and in case F is the real field.*

3) *Suppose F is a finite extension of $\boldsymbol{Q}_l$ for some prime l. If $F \subset \boldsymbol{Q}_l(a)$, where a is an l-power root of unity, then the maps α, β, and β_0 are bijective. In any case, the kernel of each of the three maps is isomorphic to $(\boldsymbol{Q}_l/\boldsymbol{Z}_l)^r$ for some integer r, and* Ker β_0 *is isomorphic to the direct sum of* Ker α *and* Ker β. *As F increases, the* "corank" *r increases or stays the same, for each of the three kernels.*

We first treat the case $F = \boldsymbol{R}$, the real field. If x and y are two real numbers and $x + y = 1$, then one of the two is >0 and is therefore an n-th power for every integer $n > 0$. It follows that the subgroup of $\boldsymbol{R}^* \otimes \boldsymbol{R}^*$ generated by the elements $x \otimes y$ with $x + y = 1$ is divisible, and is therefore a direct summand. Hence the quotient, $K_2\boldsymbol{R}$ can be viewed as a subgroup of

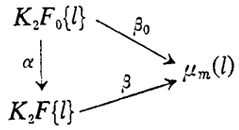
$$\begin{aligned} \boldsymbol{R}^* \otimes \boldsymbol{R}^* &\approx ((\boldsymbol{Z}/2\boldsymbol{Z}) \oplus \boldsymbol{R}) \otimes ((\boldsymbol{Z}/2\boldsymbol{Z}) \oplus \boldsymbol{R}) \\ &\approx (\boldsymbol{Z}/2\boldsymbol{Z}) \oplus (\boldsymbol{R} \otimes \boldsymbol{R}) . \end{aligned}$$

Since $\boldsymbol{R} \otimes \boldsymbol{R}$ is torsion-free it follows that the torsion subgroup of $K_2\boldsymbol{R}$ is of order 1 or 2. Since $\beta(\{-1, -1\}) = (-1, -1)_2 = -1$, the order is 2, and β is an isomorphism. If we replace $\boldsymbol{R}$ by the field $\boldsymbol{R}_0$ of real algebraic numbers, the same argument goes through, word for word, showing β_0 is an isomorphism. Hence α is an isomorphism.

From now on we assume F is non-archimedean. Let l be a prime number and, if C is an abelian group, let $C\{l\}$ denote the l-primary part of C, i.e., the subgroup of elements of l-power order. It obviously suffices for us to

discuss separately, for each l, the maps induced by α, β, and β_0 on the l-primary parts of the groups involved, as in the diagram

(5.4l)



and we hope it will create no confusion to denote these induced maps by the same symbols as the original maps, rather than by something like $\alpha\{l\}$, etc.

We begin with the case in which l is not equal to the characteristic of the residue field, and will show in that case that the maps β_0 and β are bijective, hence α also. As remarked above before the statement of the theorem, β_0 and β are bijective. To show they are injective, it is enough to show that $\operatorname{Ker}\beta_0$ and $\operatorname{Ker}\beta$ contain no elements of order l. The same argument works for β_0 as for β; it is due to Carroll [3]. We give it here, for β, for the convenience of the reader.

Assume first that F contains the l-th roots of unity. Then $l \mid m$, and if z is a generator of μ_m, then $z_1 = z^{m/l}$ is a primitive l-root of 1. By (5.1), any element of order l in K_2F is of the form $\{z_1, x\}$. Suppose such an element is in $\operatorname{Ker}\beta$. Then $1 = \beta(\{z_1, x\}) = (z_1, x)_m = (z, x)_l$, where $(\ ,\ )_l$ denotes the l-power norm-residue symbol. Since any unit in F is a power of z times a 1-unit, and since 1-units are l-th powers, it follows that $(u, x)_l = 1$ for all units u. Hence x is a unit modulo l-th powers, and so is a power of z modulo l-th powers. This implies that $\{z_1, x\} = 1$, as we wanted to show, because $\{z_1, z\} = 1$. Indeed we have $\{z_1, z\} = \{z, z\}^{m/l} = \{z, -1\}^{m/l}$, so this is killed by l and by 2, and is therefore 1 if l is odd. It is also 1 if $l = 2$ and 4 divides m, because $\{z, -1\}^2 = 1$. If $l = 2$ and 4 does not divide m then our element is $\{z^{m/l}, -1\} = \{-1, -1\}$. In the function field case it is 1, because K_2 of finite fields is $\{1\}$. In the number field case we must show $\{-1, -1\} = 1$ in $K_2\boldsymbol{Q}_l$ for l odd, and we can assume $l \equiv 3 \pmod 4$. An argument of A. Waterman for this runs as follows. Solve the congruence $x^2 + y^2 \equiv -1 \pmod l$, taking x to be an $l-1$ root of 1 in $\boldsymbol{Z}_l$. By Hensel's lemma, there is a $y \in \boldsymbol{Z}_l$ such that $x^2 + y^2 = -1$. Then $1 = \{-x^2, -y^2\} = \{-1, -1\}\{x^2, y^2\}$, and since x^2 is a root of unity of odd order we conclude that $\{-1, -1\}$ is of odd order, so is 1.

Now suppose l is equal to the residue characteristic. If $\operatorname{char} F = l$, we have $[F: F^l] = l = [F_0: F_0^l]$ and it follows, as explained in the proof of (5.1)(b)

that the groups in diagram (5.4l) are 0, and there is nothing to prove. This completes the proof of part 2) of the Theorem.

From now on we assume F is a finite extension of $\boldsymbol{Q}_l$. We first show that $\operatorname{Ker}\beta$ and $\operatorname{Ker}\beta_0$ are divisible. In case of β, this is an immediate consequence of a theorem of C. Moore ([6], see also the appendix of Milnor's book [5]). The methods of Moore and Milnor can presumably be adapted to the case of β_0. One can also deduce the divisibility directly from the connection between K_2 and Galois cohomology, as follows. Consider the map

$$h: K_2F_0\{l\} \longrightarrow H^2(F_0, \boldsymbol{Z}_l(2))$$

introduced in [9, Th. 3.1]. The hypothesis "h_1 *injective*" of the corollary of Theorem 3.4 of [9] is satisfied for the field F_0 because F_0 is a union of global fields, and the map h_1 is injective for global fields by Theorem 5.1 of [9]. Therefore, by the above-mentioned corollary, $\operatorname{Ker} h$ is the maximal divisible subgroup of $K_2F_0\{l\}$, and $K_2F_0\{l\}$ is the direct sum of $\operatorname{Ker} h$ and a subgroup mapped isomorphically by h onto $H^2(F_0, \boldsymbol{Z}_l(2))\{l\}$. Now in fact the map h is just another version of our map β_0, via a canonical isomorphism $\theta: H^2(F_0, \boldsymbol{Z}_l(2)) \approx \mu_m\{l\}$. We will construct such an isomorphism θ below, but we leave to the reader to check that $\theta \circ h = \beta_0$ (at least up to sign), for all we really need here is that $\operatorname{Ker}\beta_0 = \operatorname{Ker} h$, and this equality follows from the existence of θ. Namely, $\operatorname{Ker} h$ is killed by β_0 because it is divisible, and since β_0 and h are surjective, the existence of θ shows that their images have the same order, and hence their kernels are equal.

To construct θ, note first that $E_0 \mapsto E_0 \otimes_{F_0} F$ is an equivalence of the category of finite separable extensions of F_0 with the category of finite separable extensions of F. Therefore $H^2(F_0, \boldsymbol{Z}_l(2)) \approx H^2(F, \boldsymbol{Z}_l(2))$. By [9, Cor. of Prop. 2.2] we have an isomorphism

$$H^2(F, \boldsymbol{Z}_l(2)) \xrightarrow{\sim} \varprojlim_n H^2(F, \boldsymbol{Z}/l^n\boldsymbol{Z})(2))$$

because $H^1(F, \boldsymbol{Z}/l^n\boldsymbol{Z}(2))$ is finite for each n (indeed $H^i(F, M)$ is finite for all i and all finite M). By local duality, [7, Ch. II, § 5.1, Th. 2], this group is dual to

$$\varinjlim_n H^0(F, (\boldsymbol{Z}/l^n\boldsymbol{Z})(-1)) = H^0(F, (\boldsymbol{Q}_l/\boldsymbol{Z}_l)(-1)) .$$

Since there is only a finite number of roots of unity in F, this last is dual to $H^0(F, (\boldsymbol{Q}_l/\boldsymbol{Z}_l)(1)) = \mu_m\{l\}$, and we get θ by double duality.

This concludes our proof that β and β_0 are surjective with divisible kernels. Next we show that α has the same property. Consider the exact commutative diagram

$$(5.6)\qquad \begin{array}{ccccccccc} 0 & \longrightarrow & \operatorname{Ker}\beta_0 & \longrightarrow & K_2F_0\{l\} & \xrightarrow{\beta_0} & \mu_m\{l\} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle\alpha_1} & & \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\alpha_2} & & \\ 0 & \longrightarrow & \operatorname{Ker}\beta & \longrightarrow & K_2F\{l\} & \xrightarrow{\beta} & \mu_m\{l\} & \longrightarrow & 0\ . \end{array}$$

Since α_2 is injective, it follows from (5.1)(b) that α_1 maps $(\operatorname{Ker}\beta_0)_l$ *onto* $(\operatorname{Ker}\beta)_l$. From the fact that $\operatorname{Ker}\beta_0$ is divisible and $\operatorname{Ker}\beta$ is an l-primary torsion group, it follows easily that α_1 is surjective and its kernel divisible by l, hence divisible. (One way to see this is to apply the snake lemma to the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & (\operatorname{Ker}\beta_0)_l & \longrightarrow & \operatorname{Ker}\beta_0 & \xrightarrow{l} & \operatorname{Ker}\beta_0 & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle\alpha_1} & & \downarrow{\scriptstyle\alpha_1} & & \\ 0 & \longrightarrow & (\operatorname{Ker}\beta)_l & \longrightarrow & \operatorname{Ker}\beta & \xrightarrow{l} & \operatorname{Ker}\beta & \longrightarrow & 0\ .) \end{array}$$

Now applying the snake lemma to (5.6) we find, since α_2 is bijective, that $\operatorname{Ker}\alpha = \operatorname{Ker}\alpha_1$, so is divisible, and $\operatorname{Coker}\alpha = \operatorname{Coker}\alpha_1$, so is zero, as we wished to show. Now parts 1) and 2) of the Theorem are proven.

Since all three maps in (5.4l) are surjective, their kernels form an exact sequence $0 \to \operatorname{Ker}\alpha \to \operatorname{Ker}\beta_0 \to \operatorname{Ker}\beta \to 0$, and since $\operatorname{Ker}\alpha$ is divisible, this sequence splits. Since $\operatorname{Ker}\beta$ and $\operatorname{Ker}\beta_0$ are divisible the exact sequences in (5.6) split and we have isomorphisms

$$(5.7)\qquad K_2F_0\{l\} \approx \operatorname{Ker}\beta_0 \oplus \mu_m\{l\}$$

and

$$(5.8)\qquad K_2F\{l\} \approx \operatorname{Ker}\beta \oplus \mu_m\{l\}\ .$$

Suppose F contains a primitive l-th root of unity z_1. Let A (resp. A_0) be the group of all $x \in F^*$ (resp. F_0^*) such that $\{z_1, x\} = 1$ in K_2F (resp. K_2F_0). By Theorem (5.2) the map $x \mapsto \{z_1, x\}$ induces an isomorphism

$$F^*/A \xrightarrow{\sim} (K_2F)_l$$

and similarly (cf. the proof of Theorem (5.2)) we have an isomorphism

$$F_0^*/A_0 \xrightarrow{\sim} (K_2F_0)_l\ .$$

Let r and r_0 be the integers defined by $(F^*\colon A) = l^r$ and $(F_0^*\colon A_0) = l^{r_0}$. Then

$(K_2F)_l$ has order l^r and $(K_2F_0)_l$ is of order l^{r_0}. By (5.7) and (5.8) we conclude that $(\operatorname{Ker}\beta)_l$ is of order l^{r-1} and $(\operatorname{Ker}\beta_0)_l$ of order l^{r_0-1}. Since $\operatorname{Ker}\beta$ and $\operatorname{Ker}\beta_0$ are l-divisible l-primary torsion groups it follows from this that they are isomorphic to $(\boldsymbol{Q}_l/\boldsymbol{Z}_l)^{r-1}$ and $(\boldsymbol{Q}_l/\boldsymbol{Z}_l)^{r_0-1}$, respectively.

Suppose F' is an extension of F of finite degree, n. Then the kernel of the natural map $K_2F \to K_2F'$ is killed by n. Hence its intersection with $\operatorname{Ker}\beta$ is finite, and it follows that the image of $\operatorname{Ker}\beta$ in K_2F' has the same "corank", $r-1$, as $\operatorname{Ker}\beta$. Thus the corank of $\operatorname{Ker}\beta$ cannot decrease when we enlarge F. A similar argument shows that the same holds for $\operatorname{Ker}\beta_0$ and $\operatorname{Ker}\alpha$.

We have now proved everything in the theorem except the first sentence of part 3). For that we use

(5.9) **Lemma.** *Let E be a field, n an integer ≥ 2, and $a, x \in E^*$ such that $x^{n+1} - x^n - x + 1 - a = 0$. Then $\{x, a\}^n = 1$ in K_2E, and if a is a j-th root of unity, then $\{x, a\}^d = 1$, where d is the* g.c.d. *on n and j.*

The given relation between x and a can be written $a = (1-x)(1-x^n)$. Hence

$$\{x, a\}^n = \{x, 1-x\}^n\{x, 1-x^n\}^n = \{x^n, 1-x^n\} = 1$$

as claimed. If $a^j = 1$ then also $\{x, a\}^j = 1$, so $\{x, a\}^d = 1$.

Let us suppose now that $F = \boldsymbol{Q}_l(a)$, where a is a primitive l^ν root of unity for some $\nu \geq 1$. Let v be the valuation of F, normalized so that $v(F^*) = \boldsymbol{Z}$. Then $v(1-a) = 1 > 0$, and consideration of the Newton polygon of the polynomial $X^{n+1} - X^n - X + 1 - a$ shows that it has a unique root $x = x_n$ such that $v(x) = v(1-a) = 1$. Because it is unique this root is in F, hence in F_0. Let $u_n = x/(1-a)$. Then

$$\frac{x^{n+1} - x^n}{1-a} - u_n + 1 = 0$$

and consequently

$$v(u_n - 1) = (n-1)v(1-a) = n-1\ .$$

This shows that the l^ν elements u_n, for $2 \leq n \leq l^\nu + 1$ generate the group U of units in F_0, modulo U^l, for if U_i denotes the group of units $\equiv 1 \bmod (1-a)^i$ then u_n generates U_{n-1} modulo U_n for each $n \geq 2$, and we have $U_1^l \supset U_{l^\nu+1}$, as is well known (cf., e.g., [5, Lemma A.4]). We define, specially, $u_1 = 1 - a$. Then the $l^\nu + 1$ elements u_n, for $1 \leq n \leq l^\nu + 1$ generate F_0^* modulo $(F_0^*)^l$.

On the other hand, putting $z_1 = a^{l^{\nu-1}}$, a primitive l-th root of unity, we have

$$\{z_1, u_1\} = \{a, 1 - a\}^{l^{\nu-1}} = 1 ,$$

and for $n \geq 2$

$$\{z_1, u_n\} = \{a^{l^{\nu-1}}, u_n\} = \left\{a, \frac{x_n}{1-a}\right\}^{l^{\nu-1}} = \{a, x_n\}^{l^{\nu-1}} .$$

By the lemma we conclude that for $n \geq 1$ we have $\{z_1, u_n\} = 1$, if $l^\nu \nmid n$. Hence, for $1 \leq n \leq l^\nu + 1$ we have $\{z_1, u_n\} = 1$ except possibly for $n = l^\nu$. Since the $l^\nu + 1$ elements u_n, $1 \leq n \leq l^\nu + 1$, generate F_0^* modulo l-th powers, it follows that $(K_2F_0)_l$ is generated by the single element $\{z_1, u_{l^\nu}\}$, because every element of $(K_2F_0)_l$ is of the form $\{z_1, x\}$, as one sees on passing to the limit with Theorem 6.1 of [9]. Moreover

$$\beta_0(\{z_1, u_n\}) = (z_1, u_n)_m = (z, u_m)_l ,$$

if z is a primitive $m = (l-1)l^\nu$ root of 1 such that $z^{l-1} = a$. Since $z \notin (F^*)^l$, and the l-th power norm residue symbol is non-degenerate, the map $x \mapsto (z, x_l)$ is not identically 1. Therefore there is some $n \leq l^\nu + 1$ such that $(z, u_n)_l \neq 1$. The only possibility is $n = l^\nu$. Hence $\beta_0(\{z_1, u_{l^\nu}\}) \neq 1$, and it follows that $(K_2F_0)_l$ is cyclic of order l, generated by $\{z_1, u_{l^\nu}\}$, and that β_0 is injective.

Exactly the same argument, with F_0 replaced by F throughout, shows that β is injective. The only difference is that we must appeal to (5.2) to know that every element of $(K_2F)_l$ is of the form $\{z_1, x\}$. Thus $\operatorname{Ker}\beta_0$ and $\operatorname{Ker}\beta$ are 0 when $F = \boldsymbol{Q}_l(a)$, where a is a primitive l^ν root of unity. If we have only $\boldsymbol{Q}_l \subset F \subset \boldsymbol{Q}_l(a)$ the same conclusion holds, because, as we have seen, $\operatorname{Ker}\beta_0$ and $\operatorname{Ker}\beta$ can not decrease in size when we enlarge F.

References

[1] Bass, H. and Tate, J., The Milnor ring of a global field, in Algebraic K-Theory II, Lecture Notes in Math., **342**, Springer, Berlin, 1973.

[2] Birch, B. J., K_2 of global fields, Proc. Symp. Pure Math., **20**, AMS, Providence, R.I., 1970.

[3] Carroll, J. E., On the torsion in K_2 of local fields, in Algebraic K-Theory II, Lecture Notes in Math., **342**, Springer, Berlin, 1973.

[4] Dennis, R. K. and Stein, M. R., The functor K_2: A survey of computations and problems, in Algebraic K-Theory II. Lecture Notes in Math., **342**, Springer, Berlin, 1973.

[5] Milnor, J., Introduction to Algebraic K-Theory, Annals of Math. Studies, **72**, Princeton U.P., Princeton, 1971.

[6] Moore, C., Group extensions of p-adic and adelic linear groups, Publ. Math. I.H.E.S., 35, 5–74, I.H.E.S., Le Bois, 1969.

[7] Serre, J.-P., Cohomologie Galoisienne, Lecture Notes in Math., **5**, 4th Ed., Springer, Berlin, 1973.

[8] Tate, J., Symbols in Arithmetic, Actes Congrès Intern. Math. 1970, Tome, **1**, 201–211, Gauthier Villars, Paris, 1971.

[9] Tate, J., Relations between K_2 and Galois cohomology, Invent. Math., **36** (1976), 257–274.

Department of Mathematics
Harvard University
Cambridge, Massachusetts 02138
U.S.A.

ALGEBRAIC NUMBER THEORY, Papers contributed for the International Symposium, Kyoto 1976; S. Iyanaga (Ed.): Japan Society for the Promotion of Science, Tokyo, 1977

Isomorphisms of Galois Groups of Algebraic Number Fields

KÔJI UCHIDA

Let Q be the field of the rational numbers. Let Ω be a normal algebraic extension of Q such that Ω has no abelian extension. Let G be the Galois group of Ω over Q. Neukirch [3, 4] has shown that every open normal subgroup of G is a characteristic subgroup, and has proposed a problem whether every automorphism of G is inner. This problem is solved affirmatively, i.e., we prove

Theorem 1. *Let G_1 and G_2 be open subgroups of G, and let $\sigma: G_1 \to G_2$ be a topological isomorphism. Then σ can be extended to an inner automorphism of G.*

Neukirch has stated his theorems in the case Ω is the algebraic closure or the solvable closure of Q. The author proved Theorem 1 in these cases. Theorem 1 of the above form is due to Iwasawa who noticed that Neukirch's theorems are valid for every Ω as above. Ikeda also proved Neukirch's problem independently.

Let N be any open normal subgroup of G contained in G_1 and G_2. We put $H = G/N$, $H_1 = G_1/N$ and $H_2 = G_2/N$. Neukirch has shown $\sigma(N) = N$. Hence σ induces an isomorphism $\sigma_N: H_1 \to H_2$. We only need to show that σ_N can be extended to an inner automorphism of H for every N.

Lemma 1. *Let h be any element of H_1. Then cyclic subgroups generated by h and $\sigma_N(h)$ are conjugate in H. Especially there exists an integer r which is prime to the order of h such that $\sigma_N(h)$ is conjugate to h^r in H.*

Lemma 2. *Let n be the order of H, and let p be any prime number such that $p \equiv 1 \pmod{n}$. Let F_p be a finite field with p elements, and let $A = F_pH$ be the group ring of H. Then there exists an open normal subgroup M of G contained in N such that N/M is isomorphic to A as an H-module.*

Lemma 1 comes from Neukirch's theorems, and Lemma 2 is the easiest case of the embedding problem. We take M as in Lemma 2. Then σ induces an

isomorphism σ_M which is an extension of σ_N, i.e., $\pi\sigma_M(x) = \sigma_N\pi(x)$ for every $x \in G_1/M$, where π is a natural projection of G/M to H. An additive group A is considered as a subgroup of G/M. As A is contained in G_1/M, $\sigma_M(\alpha)$ is defined for any $\alpha \in A$. Identity element of H is written as 1. Let h be any element of H_1. If we consider h as an element of A. it holds

$$\sigma_M(h) = \sigma_M(h \cdot 1) = \sigma_N(h)\sigma_M(1) ,$$

because the operation of h onto A is induced from an inner automorphism by an element of G_1/M. Let $B = F_pH_1$ be a subring of A. For any element $\alpha = \Sigma a_h h \in B$, $a_h \in F_p$, $h \in H_1$, we put

$$\sigma_N(\alpha) = \Sigma a_h \sigma_N(h) .$$

Then it holds

$$\sigma_M(\alpha) = \sigma_N(\alpha)\sigma_M(1)$$

for any $\alpha \in B$. Let ε be an idempotent of B. A left ideal $A\varepsilon$ is a normal subgroup of G/M which is invariant by σ_M as Neukirch's theorems show. Hence it holds

$$\sigma_M(\varepsilon) = \sigma_N(\varepsilon)\sigma_M(1) = \beta\varepsilon$$

for some $\beta \in A$. As $1 - \varepsilon$ is also an idempotent of B,

$$\sigma_M(1) = \sigma_M(\varepsilon) + \sigma_M(1 - \varepsilon) = \beta\varepsilon + \gamma(1 - \varepsilon)$$

for some $\gamma \in A$. By multiplying ε from the right, it holds

$$\sigma_M(\varepsilon) = \sigma_N(\varepsilon)\sigma_M(1) = \beta\varepsilon = \sigma_M(1)\varepsilon .$$

Lemma 1 shows that $\sigma_M(1)$ is conjugate to $r \cdot 1$ in G/M for some $r \in F_p^*$. All the conjugates of 1 are just the set H considered as a subset of A. Hence $\sigma_M(1) = rh_0$ for some $h_0 \in H$, and then

$$\sigma_N(\varepsilon)h_0 = h_0\varepsilon .$$

for every idempotent ε of B. Let h be any element of H_1 and let m be its order. As $p \equiv 1 \pmod{m}$, F_p contains a primitive m-th root μ of unity. Then

$$\varepsilon_i = m^{-1}(1 + \mu^i h + \cdots + \mu^{(m-1)i}h^{m-1})$$

are idempotents of B for $i = 0, 1, \cdots, m - 1$. Then above relations for these ε_i show that

$$\sigma_N(h)h_0 = h_0h ,$$

i.e.,

$$\sigma_N(h) = h_0hh_0^{-1}$$

for every $h \in H_1$. This shows that σ_N can be extended to an inner automorphism of H by h_0.

Corollary 1 (Neukirch's problem). *Every automorphism of G is inner.*

Corollary 2. *Let K_1 and K_2 be subfields of Ω of finite degrees. Let $G_1 = G(\Omega/K_1)$ and $G_2 = G(\Omega/K_2)$. If G_1 and G_2 are isomorphic, K_1 and K_2 are conjugate.*

Corollary 3. *Let K be a subfield of Ω of finite degree and let $G_K = G(\Omega/K)$. Then*

$$\text{Aut } G_K/\text{Inn } G_K \simeq \text{Aut } K .$$

Corollaries 1 and 2 are easy from our theorem. Corollary 3 was pointed out by Neukirch. In the above, Aut G_K and Inn G_K are the group of the topological automorphisms of G_K and the normal subgroup of the inner automorphisms, respectively. Aut K is the automorphism group of the field K, which is $G(K/Q)$ if K is normal over Q. Theorem 1 shows that every automorphism of G_K is extended to an inner automorphism of G. Then this corollary holds if the centralizer of G_K is trivial. The method of the proof of Proposition 1 in [1] is valid also in this case, and it shows the centralizer is trivial.

In Theorem 1 we assume two subgroups are open. But this assumption can be weakened.

Theorem 2. *Let G_1 be an open subgroup of G and let G_2 be a closed subgroup of G. If G_1 and G_2 are isomorphic as topological groups, G_2 must be open.*

Replacing by a suitable subgroup if necessary, we may assume that G_1 is a normal subgroup of G. Let K_1 and K_2 be fixed subfields of G_1 and G_2, respectively. We first show that $K_1 \subset K_2$. We fix an isomorphism $\sigma: G_1 \to G_2$. As K_1K_2 is a Galois extension of K_2 of finite degree, corresponding subgroup H_2 of G_2 is open and normal. Then $H_1 = \sigma^{-1}(H_2)$ is an open normal subgroup of G_1. We must show that $H_1 = G_1$.

Let p be a prime number. Let v be a valuation of Ω which is an extension of the p-adic valuation. Let D_1 be the decomposition subgroup of v in G_1. Neukirch theory shows that $D_2 = \sigma(D_1)$ is a decomposition subgroup of a valuation w of Ω in G_2. As w is also above p, completions $K_{1,v}$ and $K_{2,w}$ are extensions

of Q_p. They have the same ramification index and the same residue class field. Now let v be unramified in the extension K_1/Q. As v and w are conjugate, $K_{1,w}$ is also an unramified extension of Q_p of degree $[K_{1,v}: Q_p]$. As $K_{2,w}$ is an unramified extension of the same degree, it holds $(K_1K_2)_w = K_{2,w}$. This shows $D_2 \subset H_2$, and then $D_1 \subset H_1$. Then it must be $H_1 = G_1$ because any unramified prime of K_1 splits completely in the extension corresponding to G_1/H_1.

Now let L_1 be an algebraic extension of K_1 of finite degree, which is normal over Q. Let F_1 be a corresponding subgroup of G_1. Let $F_2 = \sigma(F_1)$ and let L_2 be the fixed field of F_2. As F_1 and F_2 are isomorphic, above argument shows $L_1 \subset L_2$. Then $M_2 = L_1K_2$ is a normal subextension of L_2/K_2. There exists a normal subextension M_1 of L_1/K_1 corresponding to M_2 through the isomorphism σ. Let ν and w be as above. Then

$$[L_{1,v}: Q_p] = [L_{2,w}: Q_p] \geqq [M_{2,w}: Q_p]$$

holds. As M_2 contains L_1 and as w and v are conjugate on L_1,

$$[M_{2,w}: Q_p] \geqq [L_{1,v}: Q_p]$$

holds. Then it holds

$$[L_{2,w}: Q_p] = [M_{2,w}: Q_p] ,$$

i.e., $L_{2,w} = M_{2,w}$. This shows $L_{1,v} = M_{1,v}$, i.e., a prime of M_1 corresponding to v splits completely in L_1. As v is arbitrary, it must be $L_1 = M_1$. Then $L_2 = M_2$ and

$$[L_1: K_1] = [L_2: K_2] = [L_1K_2: K_2]$$

for any L_1. This holds only when $K_1 = K_2$. This shows $G_2 = G_1$ is open.

References

[1] Komatsu, K., A remark of a Neukirch's conjecture, Proc. Japan Acad., **50** (1974), 253–255.

[2] ——, The Galois group of the algebraic closure of an algebraic number field, Kōdai Math. Sem. Rep., **26** (1974), 44–52.

[3] Neukirch, J., Kennzeichnung der p-adischen und der endlichen algebraischen Zahlkörper, Inv. Math., **6** (1969), 296–314.

[4] ——, Kennzeichnung der endlich-algebraischen Zahlkörper durch die Galoisgruppe der maximal auflösbaren Erweiterungen, J. für Math., **238** (1969), 135–147.

[5] Uchida, K., Isomorphisms of Galois groups, to appear in J. Math. Soc. Japan vol. 28 (1976).

Mathematical Institute
Tôhoku University
Sendai 980
Japan

ALGEBRAIC NUMBER THEORY, Papers contributed for the International Symposium, Kyoto 1976; S. Iyanaga (Ed.): Japan Society for the Promotion of Science, Tokyo, 1977

Remarks on Hecke's Lemma and its Use

ANDRÉ WEIL

1. Leibniz' discovery, early in his career, of his famous series for π was not only, in the eyes of his contemporaries, one of his most striking achievements (on which Huyghens, who had hitherto regarded him as a talented young amateur, immediately congratulated him as one likely to preserve his name for posterity); it also paved the way for the no less sensational summation by Euler, some fifty years later, of the series we now denote by $\zeta(2n)$. In retrospect, we see that these were the first examples of relations between periods of abelian integrals (in this case, the one which defines π) and special values of Dirichlet series, or (more generally) of automorphic forms. As a further typical instance of such a relation, I will merely quote here Jacobi's famous formula

$$\sqrt{\frac{2K}{\pi}} = \vartheta_3(0)$$

expressing the period

$$2K = 2\int_0^1 \frac{dx}{\sqrt{(1-x^2)(1-k^2x^2)}}$$

of the "standard" elliptic integral of the first kind as a modular *form* with respect to the "transcendental" module τ (the ratio of the periods), while the "algebraic" module k^2 is expressed as a modular *function* of τ (the quotient of two "Thetanullwerte"). Incidentally, that formula does not seem to have been generalized yet to theta-functions of more than three variables (cf. [7]).

Although a number of the best mathematicians of the last and of the present century have studied various aspects of this subject, it may fairly be said that only its surface has been scratched so far; nor will the present paper (which should be regarded as a "report on work in progress") attempt to do more. My purpose is merely to point out the usefulness of Hecke's classical lemma in

dealing with some of the problems raised by the evaluation of the periods of certain abelian integrals.

Broadly speaking, Hecke's lemma establishes the relation between automorphic forms and Dirichlet series satisfying functional equations of the classical type. Hecke introduced it in connection with the full modular group $GL_2(Z)$ and some of its subgroups of small index; it is no less useful, however, in the study of the discrete subgroups of $GL_2(k)$, where k is any algebraic number-field (cf. e.g. [6]). Even the formulation I gave for it in connection with the latter problem ([6], p. 132) is not quite general enough, however, for some of its most interesting applications; my first step will be to formulate it with the proper degree of generality.

Hecke's Lemma. *Let φ, φ' be two continuous functions on $\boldsymbol{R}_+^\times$, such that both $\varphi(\nu)$ and $\varphi'(\nu^{-1})$ are $O(e^{-A\nu})$, with some $A > 0$, for $\nu \to +\infty$, and $O(\nu^{-B})$, with some $B \geqq 0$, for $\nu \to 0$. Put*

$$f(s) = \int_0^{+\infty} \varphi(\nu)\nu^{s-1}d\nu\ , \qquad f'(s) = \int_0^{+\infty} \varphi'(\nu)\nu^{s-1}d\nu\ ;$$

then these integrals are absolutely convergent and define holomorphic functions f, f' in the half-planes $Re(s) > B$ and $Re(s) < -B$, respectively. Let now $R(s)$ be a rational function of s, vanishing at $s = \infty$, and assume that, for some $\sigma > B$ and some $\sigma' < -B$, $t \to f(\sigma + it)$ and $t \to f'(\sigma' + it)$ are $O(|t|^{-2})$. Then the following two assertions are equivalent:

(i) *$f(s) - R(s)$ and $f'(s) - R(s)$ can be continued to one and the same entire function in the s-plane, bounded in every strip $\sigma_1 \leqq Re(s) \leqq \sigma_2$;*

(ii) *for all $\nu > 0$, we have*

$$\varphi(\nu) - \varphi'(\nu) = \sum \text{Res}\,(R(s)\nu^{-s})\ ,$$

where Res *means the residue, and the sum is extended to all the poles of $R(s)$.*

The lemma, as formulated in [6], p. 132, is the special case $R = 0$; the proof remains of course exactly the same.[1)]

2. Some of Hecke's early applications of his lemma concerned groups which were not commensurable with the modular group; and it is perhaps worthwhile to emphasize here that its scope is actually wider than is generally realized. Take for instance any fuchsian group G in the upper half-plane, and

1) A rather broad generalization will be found in S. Bochner, Ann. of Math. 53 (1951), pp. 332–363. I am indebted to J.-P. Serre for this reference.

assume that it has at least one cusp; then it has infinitely many, including all the transforms of that cusp under G. Normalize the group by assuming that $i\infty$ is one such cusp, i.e. that G contains a substitution $t \to t + p$, with $p > 0$. Let ρ be another cusp of G; put $t' = (\rho - t)^{-1}$, and call G' the transform of G by $t \to t'$; then $i\infty$ is a cusp of G', and G' contains a substitution $t' \to t' + q$ with $q > 0$.

Let $A(t)$ be an automorphic form of degree $-k$ for G, holomorphic everywhere including the cusps; then $A(t)$ has at $i\infty$ a power-series expansion in $\exp(2\pi it/p)$; call a_0 its constant term, and put

$$F(\tau) = A(p\tau + \rho) - a_0\ .$$

This has a power-series expansion:

$$F(\tau) = \sum_1^\infty a_n e^{2\pi i n\tau}\ ,$$

absolutely convergent in the upper half-plane. Similarly, put:

$$B(t') = t'^{-k}A\left(\rho - \frac{1}{t'}\right)\ ;$$

this is an automorphic form for G'; call b_0 the constant term of its expansion at $i\infty$; then we can write

$$G(\tau) = B(q\tau) - b_0 = \sum_1^\infty b_n e^{2\pi i n\tau}\ ,$$

and we have

$$F(\tau) + a_0 = (-p\tau)^{-k}\left[G\left(\frac{-1}{pq\tau}\right) + b_0\right]\ .$$

Now put, for $\nu > 0$:

$$\varphi(\nu) = F(i\nu)\ , \qquad \varphi'(\nu) = (-ip\nu)^{-k}G(i/pq\nu)\ ,$$
$$R(s) = -a_0 s^{-1} + b_0(-ip)^{-k}(s-k)^{-1}\ ,$$

and apply Hecke's lemma. We find:

$$f(s) = (2\pi)^{-s}\Gamma(s)\sum_1^\infty a_n n^{-s}\ ,$$
$$f'(s) = i^k p^{-s}q^{k-s}(2\pi)^{s-k}\Gamma(k-s)\sum_1^\infty b_n n^{s-k}\ ,$$

and we conclude from the lemma that f, f' can be continued to one and the same meromorphic function with the same poles and the same residues as $R(s)$.

In this manner, we have associated Dirichlet series with functional equations to every pair of cusps and every automorphic form for G. Whether such series have an arithmetical significance, when G is not commensurable with the modular group, will remain an open question for the moment; for such a group G, of course, the theory of the Hecke operators cannot be applied.

3. For $k = 2$, the automorphic form $A(t)$ defines an invariant differential $A(t)dt$ of the second kind for G, and a differential of the first kind if it is a cusp form (i.e. if $a_0 = 0$, and $b_0 = 0$ for every cusp $\rho \neq i\infty$); to simplify notations, we will consider only this latter case. Put

$$I(t) = \int_{i\infty}^{t} A(t)dt \ .$$

In the formulas of no. 2, put $k = 2$, $a_0 = 0$, $b_0 = 0$, $R(s) = 0$. In the functional equation $f(s) = f'(s)$, substitute $s + 1$ for s, and divide both sides by $s/2\pi$. We find a functional equation $F(s) = F'(s)$, where F, F' are respectively defined, in suitable half-planes $Re(s) > B$ and $Re(s) < -B$, by the series

$$F(s) = (2\pi)^{-s}\Gamma(s) \sum_1^\infty \frac{a_n}{n} n^{-s} \ ,$$

$$F'(s) = p^{-s-1}q^{1-s}(2\pi)^s\Gamma(-s) \sum_1^\infty \frac{b_n}{n} n^s \ .$$

These can be written as

$$F(s) = \int_0^{+\infty} \Phi(v)v^{s-1}dv \ , \qquad F'(s) = \int_0^{+\infty} \Phi'(v)v^{s-1}dv \ ,$$

where we have put

$$\Phi(v) = \sum_1^\infty \frac{a_n}{n} e^{-2\pi nv} = \frac{2\pi i}{p} I(ipv + \rho) \ ,$$

$$\Phi'(v) = \frac{2\pi i}{p}[I(ipv + \rho) - I(\rho)] \ .$$

We apply Hecke's lemma, where we have to take into account the fact that we have divided the functional equation by $s/2\pi$, so that F, F' have a simple pole at $s = 0$, with the residue $2\pi \cdot f(1)$. This gives:

$$\Phi - \Phi' = -\frac{2\pi i}{p} I(\rho) = 2\pi \cdot f(1) = \left(\sum_1^\infty a_n n^{-s}\right)_{s=1} \ .$$

In particular, if γ is any element of G, we can take $\rho = \gamma(i\infty)$, and $I(\rho)$ is then the period of $A(t)dt$ belonging to the cycle defined by γ.

4. The principles of the above proofs can also be applied to more general problems; actually, they were suggested by the proof given by Goldstein and de la Torre [3] for the transformation formula of $\log \eta(\tau)$ under general modular substitutions, which may now, in retrospect, be regarded as an application of the above method to the differential $A(\tau)d\tau = d \log \eta(\tau)$, combined with the knowledge of the functional equation for "Hurwitz' zeta-function". In their case, of course, the presence of double poles in the functions denoted above by $F(s), F'(s)$ requires greater care in the evaluation of the residues; but the basic idea in their proof is the same as described above.

Another interesting case is the one where the group is Hecke's group $\Gamma_0(N)$, and the invariant differential $A(t)dt$ is the Mellin transform of the zeta-function of an elliptic curve E of conductor N, with complex multiplication, defined over $\boldsymbol{Q}$. Let k be the imaginary quadratic field generated by the complex multipliers for E; let $\bar{\omega}$ be one of the periods of a differential of the first kind on E, defined over $\boldsymbol{Q}$. Well-known conjectures had led to expect that the periods of $A(t)dt$ are of the form $\bar{\omega}a$, with $a \in k$, and this has been verified by Shimura [5b] by using Hecke operators; closely related results had already been obtained by Hecke [4] by a method depending on the direct calculation of the periods. Here we merely wish to point out that the method explained above, combined with Damerell's theorem [1], leads immediately to the conclusion that the periods of $A(t)dt$ are all of the form $\bar{\omega}a$, where a is an algebraic number. It may be surmised that the conclusion $a \in k$ could be derived from Shimura's work on the same subject [5c]; but I must leave this question open for the time being.

5. The method explained in no. 3 applies equally well to the periods of Eichler's integrals (see [2] and [5a]). Here it will be convenient to normalize the group G of no. 2 so that the two cusps to be considered are at $i\infty$ and at 0, and that G contains the substitution $\tau \to \tau + 1$. Let A be a holomorphic form of degree $-k$, where k is an integer $\geqq 2$; as before, call a_0 the constant term in its expansion at $i\infty$, q the period of the form $A(-1/\tau)\tau^{-k}$, and b_0 the constant term in its expansion. We write again:

$$F(\tau) = A(\tau) - a_0 = \sum_1^\infty a_n e^{2\pi i n\tau} \ ,$$

$$G(\tau) = (q\tau)^{-k}A\left(-\frac{1}{q\tau}\right) - b_0 = \sum_1^\infty b_n e^{2\pi i n\tau} \ ;$$

and now, changing our earlier notations, we will write

$$\varphi(s) = \sum_1^\infty a_n n^{-s}\,, \qquad \Phi(s) = (2\pi)^{-s}\Gamma(s)\varphi(s)\,,$$

$$\psi(s) = \sum_1^\infty b_n n^{-s}\,, \qquad \Psi(s) = (2\pi)^{-s}\Gamma(s)\psi(s)\,.$$

We apply Hecke's lemma exactly in the manner explained in no. 2, and conclude that Φ, Ψ satisfy the functional equation

$$\Phi(s) = i^k q^{k-s}\Psi(k-s)\,,$$

where both sides have simple poles at $s = 0$ and $s = k$, with residues respectively equal to $-a_0$ and to $i^k b_0$. In view of the definition of Φ and Ψ this gives $\varphi(0) = -a_0$, $\psi(0) = -b_0$.

Now we replace s by $s + k - 1$ in this functional equation, and then divide it by $(s+1)\cdots(s+k-2)$; the new functional equation can be written as

$$\Phi_1(s) = i^{2-k}q^{1-s}\Psi_1(2-k-s)$$

where we have put

$$\varphi_1(s) = \varphi(s+k-1) = \sum_1^\infty (a_n n^{1-k})n^{-s}\,, \qquad \Phi_1(s) = (2\pi)^{-s}\Gamma(s)\varphi_1(s)\,,$$

$$\psi_1(s) = \psi(s+k-1) = \sum_1^\infty (b_n n^{1-k})n^{-s}\,, \qquad \Psi_1(s) = (2\pi)^{-s}\Gamma(s)\psi_1(s)\,.$$

Moreover, in this new functional equation, both sides have simple poles at $s = 1, 0, -1, \cdots, 1-k$, with residues given in an obvious manner in terms of the values of φ_1 (or of ψ_1) at these points, i.e. in terms of $\varphi(0), \varphi(1), \cdots, \varphi(k-1)$, and of b_0.

On the other hand, put

$$F_1(\tau) = \sum_1^\infty a_n n^{1-k}e^{2\pi i n\tau}\,, \qquad G_1(\tau) = \sum_1^\infty b_n n^{1-k}e^{2\pi i n\tau}\,.$$

Then we have

$$F(\tau) = (2\pi i)^{1-k}\frac{d^{k-1}F_1}{d\tau^{k-1}}\,, \qquad F_1(\tau) = \frac{(2\pi i)^{k-1}}{(k-2)!}\int_{i\infty}^{\tau} F(t)(\tau - t)^{k-2}dt\,,$$

and similar formulas for $G_1(\tau)$; F_1, G_1 are essentially no other than the "Eichler integrals" for the automorphic form $A(\tau)$ and its transform under $\tau \to -1/q\tau$. Then Hecke's lemma, applied to the functional equation between Φ_1 and Ψ_1, gives:

$$F_1(\tau) + a_0\frac{(2\pi i\tau)^{k-1}}{(k-1)!} - (-1)^k q^{k-1}\tau^{k-2}\left[G_1\left(\frac{-1}{q\tau}\right) + b_0\frac{(-2\pi i/q\tau)^{k-1}}{(k-1)!}\right]$$

$$= \sum_{\nu=0}^{k-2}\frac{1}{\nu!}\varphi(k-\nu-1)(2\pi i\tau)^\nu\,.$$

When the two cusps of G under consideration are the transforms of one another under an automorphism $\gamma \in G$, then (as in the special case discussed above in no. 3) the polynomial in the right-hand side gives the corresponding period of the Eichler integral $F_1(\tau)$. A typical case of this formula (the one corresponding to the modular form $\Delta(\tau)$ of degree $k = -12$) had already been described by Shimura [5a].

6. In conclusion, it seems appropriate to mention one important motivation for the calculations described above.

There is, by now, a fair amount of well-documented conjectures on the zeta-functions of elliptic curves over $\boldsymbol{Q}$; moreover, most of them (with the notable exception of the Birch-Swinnerton-Dyer conjecture) have been verified for curves with complex multiplication. On the other hand, we are still unable even to guess what the corresponding facts may look like for elliptic curves over an algebraic number-field k.

The known facts suggest at any rate that the zeta-function of such a curve is the Mellin transform of a modular form for the group $GL_2(k)$. More precisely, let k have r archimedean real places and s imaginary places, its degree being $r + 2s$; the Riemannian symmetric space for $GL_2(k \otimes \boldsymbol{R})$ is the product of r copies of the Poincaré upper half-plane and of s copies of hyperbolic 3-space; it has a natural complex structure if $s = 0$, but not otherwise. Then (cf. [6, p. 144]), in view of the available evidence, one many surmise that the zeta-function is the Mellin transform of a harmonic differential form of degree $r + s$, invariant under a suitable congruence subgroup of $GL_2(k)$, and of its dual (or "star") which is of degree $r + 2s$; if $s = 0$, it amounts to the same to consider, instead of this form, the corresponding holomorphic form of degree r. As we have seen above, the more precise conjectures which can be made (and partly verified) in the case $k = \boldsymbol{Q}$ depend upon the calculation of the periods of these differentials, which can be carried out at any rate when the curve has complex multiplications. Thus one has some right to expect that a calculation of the periods of the differentials in question for a curve with complex multiplication, over a field $k \neq \boldsymbol{Q}$, might lead to more precise conjectures concerning the general case. I have little doubt that Hecke's lemma would prove its usefulness even there.

References

[1] Damerell, R. M., L-functions of elliptic curves with complex multiplication (I), Acta Arith. **17** (1970), 287–301.

[2] Eichler, M., Eine Verallgemeinerung der Abelschen Integrale, Math. Zeit. **67** (1957), 267–298.

[3] Goldstein, L. and de la Torre, P., On the transformation of $\log \eta(\tau)$, Duke Math. J. **41** (1974), 291–297.

[4] Hecke, E., Bestimmung der Perioden gewisser Integrale durch die Theorie der Klassenkörper, Math. Zeit. **28** (1928), 708–727 (=Math. Werke 505–524).

[5] Shimura, G., (a) Sur les intégrales attachées aux formes automorphes, J. Math. Soc. Jap. **11** (1959), 291–311; (b) On elliptic curves with complex multiplication . . ., Nagoya Math. J. **43** (1971), 199–208; (c) On some arithmetical properties of modular forms of one and several variables, Ann. of Math. **102** (1975), 491–515.

[6] Weil, A., Dirichlet series and automorphic forms, Lecture Notes in Math. **189**, Springer, Berlin, 1971.

[7] ——, Sur les périodes des intégrales abéliennes, Comm. Pure and Appl. Math. **29** (1976), 813–819.

The Institute for Advanced Study
Princeton, New Jersey 08540
U.S.A.

ALGEBRAIC NUMBER THEORY, Papers contributed for the International Symposium, Kyoto 1976; S. Iyanaga (Ed.): Japan Society for the Promotion of Science, Tokyo, 1977

Dirichlet Series with Periodic Coefficients

YOSHIHIKO YAMAMOTO

0. Introduction

Let p be an odd prime and (a/p) denote the Legendre symbol mod p. We define S_r^N (N, r positive integers, $1 \leq r \leq N$) by

$$S_r^N = \sum_{(r-1)\frac{p}{N} < a < r\frac{p}{N}} \left(\frac{a}{p}\right).$$

Clearly $S_1^1 = 0$ and $S_r^N = (-1/p)S_{N-r+1}^N$, so we have $S_1^2 = 0$ for $p \equiv 1 \pmod 4$. Dirichlet showed $S_1^2 = (2 - (2/p))h(-p)$ for $p \equiv 3 \pmod 4$, where $h(-p)$ is the class number of the imaginary quadratic field $\boldsymbol{Q}(\sqrt{-p})$.

According to Karpinski [6], the sum S_r^N for certain small values were first studied by Gauss and Dedekind [3]. Their results were extended by Karpinski, Lerch, Holden, Yamamoto, Berndt and Johnson-Mitchell [1, 2, 4, 6, 7, 8]. These results give equalities between linear combinations of S_r^N's and $h(-p)$'s.

We give here more general treatment of character sums as special values of periodic Dirichlet series, which contains formulas for

$$\sum \left(\frac{a}{p}\right) \log \left|\sin \pi\left(\frac{a}{p} - \frac{r}{N}\right)\right|$$

(cf. Lerch [7]) as well as the results mentioned above.

1. Periodic sequences $P(N)$

Let $c = \{c(n)\}_{n=1}^{\infty}$ be a sequence of complex numbers of period $N \geqq 1$; $c(n) = c(n + N)$. We often identify the sequence with the function defined on the natural numbers N taking values in the complex numbers $\boldsymbol{C}$. The set of all sequences of period N makes a complex vector space $C(N)$ by the natural isomorphism $C(N) \ni c \mapsto (c(1), \cdots, c(N)) \in \boldsymbol{C}^N$. Define $\xi_a \in C(N)$ by

$$\xi_a(n) = e^{2\pi i an/N} = \zeta^{an} \qquad (\zeta = e^{2\pi i/N}) \ ;$$

then clearly $\xi_0, \cdots, \xi_{N-1}$ is a basis of $C(N)$. We define an inner product

$$(c_1, c_2) = \sum_{a \bmod N} c_1(a)\overline{c_2(a)}$$

of c_1 and c_2 in $C(N)$. Then the basis above mentioned is an orthogonal basis of $C(N)$. Let $\psi(n)$ be a Dirichlet character mod u (not necessarily primitive), then $\psi \in C(ku)$ for $k = 1, 2, \cdots$. For a positive integer t we define $\psi^{(t)} \in C(tu)$ by

$$\psi^{(t)}(n) = \begin{cases} \psi(n/t) & \text{if } t|n \ , \\ 0 & \text{otherwise} \ . \end{cases}$$

Put

$$X(N) = \{\psi^{(t)} \mid \psi \text{ is a Dirichlet character mod } u, \ tu = N\} \ .$$

It is easy to see the following

Proposition 1.1. *$X(N)$ gives an orthogonal basis of $C(N)$.*

2. Periodic Dirichlet series

Let

$$D(s, c) = \sum_{n=1}^{\infty} c(n)n^{-s}$$

be the Dirichlet series with periodic coefficients $c(n) \in C(N)$. It follows from the periodicity of $c(n)$ that $D(s, c)$ is absolutely convergent for $\operatorname{Re} s > 1$ and defines an analytic function $D(s, c)$, regular at $\operatorname{Re} s > 1$. Moreover, if $\sum_{a=1}^{N} c(n) = 0$, $D(s, c)$ is convergent uniformly for $\operatorname{Re} s > \sigma_0$ ($\sigma_0 > 0$), so $D(s, c)$ is regular at $\operatorname{Re} s > 0$. The set $P(N) = \{D(s, c) \mid c \in C(N)\}$ of all periodic Dirichlet series of period N makes a complex vector space of dimension N, canonically isomorphic to $C(N)$. It is clear that $D(s, \xi_a)$ ($0 \leqq a \leqq N - 1$) gives a basis of the vector space $P(N)$. On the other hand, it follows from Proposition 1.1 that $D(s, \psi)$ ($\psi \in X(N)$) gives another basis of $P(N)$. Take $\psi^{(t)} \in X(N)$, where ψ is a Dirichlet character mod u and $N = tu$. Let ψ_0 be the primitive character mod u_0 defined by ψ. Then, for $\operatorname{Re} s > 1$,

$$\begin{aligned} (2.1) \qquad D(s, \psi^{(t)}) &= \sum_{n=1}^{\infty} \psi^{(t)}(n)n^{-s} = \sum_{n=1}^{\infty} \psi(n)(tn)^{-s} \\ &= t^{-s} \sum_{n=1}^{\infty} \psi(n)n^{-s} = t^{-s}L(s, \psi) \\ &= t^{-s}\Big(\prod_{p} (1 - \psi_0(p)p^{-s})\Big)L(s, \psi_0) \ , \end{aligned}$$

where $L(s, \psi)$ and $L(s, \psi_0)$ are the Dirichlet L-functions for the Dirichlet characters ψ and ψ_0 respectively and the p in the product runs through all primes p dividing u but not dividing u_0.

3. Function $F(s, z)$

We define a Dirichlet series $F(s, z)$ with a complex parameter z by

$$F(s, z) = \sum_{n=1}^{\infty} e^{2\pi i n z} n^{-s} \ .$$

The series $F(s, z)$ is absolutely convergent for $s \in C$ if $\operatorname{Im} z > 0$ and for $\operatorname{Re} s > 1$ if $z = x \in R$, the real number. We can, in the usual manner, express $F(s, z)$ as a contour integral, which shows that $F(s, z)$ is continued analytically to the whole s-plane, univalent and meromorphic with only possible pole of order one at $s = 1$, and the pole arises only when $z \in Z$, the rational integers. Furthermore, if we fix $s \in C$, we have a one-valued holomorphic function $F(s, z)$ defined on the z-plane slit at negative imaginary axis and its translations by integers, i.e. on $C_1 = C - \{n + iy \mid n \in Z \text{ and } y \leqq 0\}$. Clearly $F(s, a/N) = D(s, \xi_a)$ ($0 \leqq a \leqq N - 1$) and $F(s, 0) = \zeta(s)$, the Riemann zeta-function.

Proposition 3.1. *Any periodic Dirichlet series $D(s, c) \in P(N)$ is a linear combination of $F(s, a/N)$ ($0 \leqq a \leqq N - 1$). Hence, $D(s, c)$ is continued analytically to the whole s-plane.*

When z is in the upper half plane, we have

$$\frac{\partial}{\partial z} F(s, z) = 2\pi i F(s - 1, z) \ , \qquad F(0, z) = \frac{e^{2\pi i z}}{1 - e^{2\pi i z}}$$

and

$$F(1, z) = -\log (1 - e^{2\pi i z}) \ .$$

Hence

$$F(-k, z) = (2\pi i)^{-k} \frac{d^k}{dz^k} \frac{e^{2\pi i z}}{1 - e^{2\pi i z}} \qquad (k \geqq 1)$$

and

$$F(k, z) = 2\pi i \int_0^z F(k - 1, w)dw + \zeta(k) \qquad (k \geqq 2) \ ,$$

where the integral is taken over the line joining 0 and z. Making $z \to x + i0$ ($x \in R$) in the upper half plane, we get

Proposition 3.2. (i) *For* $x \in R - Z$,

$$F(0, x) = \frac{e^{2\pi i x}}{1 - e^{2\pi i x}} = \frac{1}{1 - e^{2\pi i x}} - 1$$

and

$$F(-k, x) = \sum_{r=1}^{k} S(k, r) \frac{e^{2\pi i r x}}{(1 - e^{2\pi i x})^{r+1}} \qquad (k \geqq 1) ,$$

where

$$S(k, r) = \sum_{m=1}^{r} (-1)^{r-m} \binom{r}{m} m^k .$$

(ii) *For* $0 < x < 1$,

$$F(k, x) = \frac{(2\pi i)^{k-1}}{k!} [A_k(x) - \pi i B_k(x)] \qquad (k \geqq 1) ,$$

where

$$A_1(x) = -\log 2 \, |\sin \pi x| ,$$

$$A_k(x) = k \int_0^x A_{k-1}(t) dt + \begin{cases} \dfrac{(-1)^{(k-1)/2} k!}{(2\pi)^{k-1}} \zeta(k) & \text{if } k \text{ is odd} , \\ 0 & \text{if } k \text{ is even} , \end{cases}$$

$$B_1(x) = x - 1/2$$

and $B_k(x)$ *is the k-th Bernoulli polynomial defined by*

$$\frac{te^{xt}}{e^t - 1} = \sum_{k=0}^{\infty} B_k(x) \frac{t^k}{k!} .$$

On the other hand, for $0 < x < 1$ and $k \geqq 1$,

$$F(k, x) = \sum_{n=1}^{\infty} (\cos 2\pi n x + i \sin 2\pi n x) n^{-k}$$
$$= \sum_{n=1}^{\infty} \frac{\cos 2\pi n x}{n^k} + i \sum_{n=1}^{\infty} \frac{\sin 2\pi n x}{n^k} .$$

Hence we get the Fourier series of A_k and B_k,

$$A_k(x) = \begin{cases} (-1)^{(k-1)/2} \dfrac{k!}{(2\pi)^{k-1}} \displaystyle\sum_{n=1}^{\infty} \frac{\cos 2\pi n x}{n^k} & (k = \text{odd}) , \\ (-1)^{k/2-1} \dfrac{k!}{(2\pi)^{k-1}} \displaystyle\sum_{n=1}^{\infty} \frac{\sin 2\pi n x}{n^k} & (k = \text{even}) , \end{cases}$$

$$B_k(x) = \begin{cases} (-1)^{(k+1)/2} \dfrac{2k!}{(2\pi)^k} \displaystyle\sum_{n=1}^{\infty} \frac{\sin 2\pi n x}{n^k} & (k = \text{odd}) , \\ (-1)^{k/2-1} \dfrac{2k!}{(2\pi)^k} \displaystyle\sum_{n=1}^{\infty} \frac{\cos 2\pi n x}{n^k} & (k = \text{even}) , \end{cases}$$

Then it is easily seen that

$$\begin{cases} A_k(1 - x) = (-1)^{k-1} A_k(x) \\ B_k(1 - x) = (-1)^k B_k(x) \end{cases} \tag{3.1}$$

and the Fourier series of A_k is, up to constant multiple, the conjugate Fourier series of B_k.

4. Singular values of $L(s, \chi)$

Let χ be a primitive Dirichlet character modulo $N > 1$. We can write χ as linear combination of ξ_a $(0 \leqq a \leqq N - 1)$;

$$\chi = \frac{1}{G(\bar{\chi})} \sum_{a=1}^{N-1} \bar{\chi}(a) \xi_a ,$$

where $G(\bar{\chi}) = \sum_{a=0}^{N-1} \bar{\chi}(a) \xi_a(1)$, the normalized Gaussian sum for $\bar{\chi}$. If $\operatorname{Re} s > 1$,

$$\begin{aligned} L(s, \chi) &= \sum_{n=1}^{\infty} \bar{\chi}(n) n^{-s} \\ &= G(\bar{\chi})^{-1} \sum_{a=0}^{N-1} \bar{\chi}(a) \sum_{n=1}^{\infty} \xi_a(n) n^{-s} \\ &= G(\bar{\chi})^{-1} \sum_{a=0}^{N-1} \bar{\chi}(a) F\left(s, \frac{a}{N}\right) . \end{aligned} \tag{4.1}$$

By analytic continuation, (4.1) holds for every $s \in C$. From Proposition 3.2 and (3.1) follows

Proposition 4.1. *For every* $s \in C$,

$$L(s, \chi) = G(\bar{\chi})^{-1} \sum_{a=0}^{N-1} \bar{\chi}(a) F\left(s, \frac{a}{N}\right) .$$

In particular, for $k = 1, 2, \cdots$,

$$L(k, \chi) = \begin{cases} \dfrac{(2\pi i)^{k-1}}{k! \, G(\bar{\chi})} \displaystyle\sum_{a=0}^{N-1} \bar{\chi}(a) A_k\left(\frac{a}{N}\right) & \text{if } \chi(-1) = (-1)^{k-1} , \\ -\dfrac{(2\pi i)^k}{2k! \, G(\bar{\chi})} \displaystyle\sum_{a=0}^{N-1} \bar{\chi}(a) B_k\left(\frac{a}{N}\right) & \text{if } \chi(-1) = (-1)^k . \end{cases}$$

In case $\chi = 1$, the principal character, consider the sum

$$\sum_{a=0}^{N-1} F\left(k, \frac{a}{N}\right) = N \sum_{a=0}^{N-1} (Nn)^{-k} = N^{1-k}\zeta(k) ,$$

and we have

Proposition 4.2. *For any positive integer $N > 1$,*

$$\frac{1 - N^{k-1}}{N^{k-1}}\zeta(k) = \begin{cases} \dfrac{(2\pi i)^{k-1}}{k!} \displaystyle\sum_{a=1}^{N-1} A_k\left(\frac{a}{N}\right) & \text{for } k = 3, 5, \cdots , \\ -\dfrac{(2\pi i)^k}{2 \cdot k!} \displaystyle\sum_{a=1}^{N-1} B_k\left(\frac{a}{N}\right) & \text{for } k = 2, 4, \cdots . \end{cases}$$

5. Character sums S_α and T_α

We fix an integer $k \geqq 0$ and a rational number $\alpha = t/u$ $(t, u \in \boldsymbol{Z}, 0 < t \leqq u)$ in the following. Let $f(x)$ be a periodic function on $\boldsymbol{R}$ with period 1, satisfying

$$f(x) = \begin{cases} x^k & (0 < x \leqq \alpha) , \\ 0 & (\alpha < x \leqq 1) \end{cases} \tag{5.1}$$

and the Fourier series of $f(x)$ be

$$f(x) \sim \sum_{n=-\infty}^{\infty} \hat{f}_n e^{2\pi i n x} ,$$

where

$$\begin{aligned} \hat{f}_0 &= \frac{\alpha^{k+1}}{k+1} \qquad \text{and for } n \neq 0 \\ \hat{f}_n &= -\sum_{r=1}^{k} \frac{k!\,\alpha^{k-r+1}}{(2\pi i)^r (k-r+1)!} \frac{e^{-2\pi i n \alpha}}{n^r} + \frac{k!}{(2\pi i)^{k+1}} \frac{1 - e^{-2\pi i n \alpha}}{n^{k+1}} . \end{aligned} \tag{5.2}$$

The Fourier series converges to $\frac{1}{2}(f(x+0) + f(x-0))$ at every $0 \leqq x < 1$.

Now we take a primitive Dirichlet character $\chi \bmod N > 1$ and put

$$S_\alpha = \frac{1}{N^k} \sum_{0 \leqq a \leqq \alpha N}{}' \chi(a) a^k ,$$

where the prime in the summation indicates that, if a takes the extreme values 0 or $\alpha N\,(= (t/u)N)$, the corresponding summand is to be halved. From (5.1) and (5.2)

$$S_\alpha = \sum_{0 \leqq a \leqq \alpha N}{}' \chi(a)\left(\frac{a}{N}\right)^k = \sum_{a=0}^{N-1} \chi(a) \sum_{n=-\infty}^{\infty} \hat{f}_n e^{2\pi i n a/N}$$

$$\begin{aligned} &= \sum_{n=-\infty}^{\infty} \hat{f}_n \sum_{a=0}^{N-1} \chi(a)\zeta^{na} = G(\chi) \sum_{n=-\infty}^{\infty} \bar{\chi}(n)\hat{f}_n \\ &= \frac{\alpha^{k+1}\chi(0)G(\chi)}{k+1} + k!\,G(\chi) \sum_{r=1}^{k} \frac{\alpha^{k-r+1}}{(2\pi i)^r (k-r+1)!} \sum_{n=1}^{\infty} \frac{b_r(n)\bar{\chi}(n)}{n^r} \\ &\quad + \frac{k!\,G(\chi)}{(2\pi i)^{k+1}} \sum_{n=1}^{\infty} \frac{b_{k+1}(n)\bar{\chi}(n)}{n^{k+1}} , \end{aligned} \tag{5.3}$$

where

$$\begin{aligned} b_r(n) &= (-1)^{r+1}\chi(-1)\eta^{nt} - \eta^{-nt} \qquad (1 \leqq r \leqq k) , \\ b_{k+1}(n) &= (-1)^{k+1}\chi(-1)(1 - \eta^{nt}) + (1 - \eta^{-nt}) \end{aligned}$$

and $\eta = e^{2\pi i/u}$. We see easily

$$b_r(-n) = (-1)^r \chi(-1) b_r(n) \qquad (1 \leqq r \leqq k+1) ,$$

that is, b_r has the parity $\varepsilon(b_r) = (-1)^r\chi(-1)$. Since $b \in C(u)$ $(1 \leqq r \leqq k+1)$, by Proposition 1.1, b_r is a linear combination of $\psi \in X(u)$, the parity of which is the same as b_r;

$$b_r = \sum_{\substack{\psi \in X(u) \\ \varepsilon(\psi) = \varepsilon(b_r)}} b_{r,\psi}\psi . \tag{5.4}$$

Hence

$$\sum_{n=1}^{\infty} \frac{b_r(n)\bar{\chi}(n)}{n^r} = \sum_{\psi} b_{r,\psi} \sum_{n=1}^{\infty} \frac{\psi(n)\bar{\chi}(n)}{n^r} = \sum_{\psi} b_{r,\psi} D(r, \psi\bar{\chi}) .$$

It is easily seen that $\chi(v) \cdot \psi\bar{\chi} = (\psi_1\bar{\chi})^{(v)} \in X(uN)$ if ψ is of the form $\psi = \psi_1^{(v)}$, where ψ_1 is a Dirichlet character mod u/v. The parity $\varepsilon(\psi\bar{\chi}) = \varepsilon(\psi)\varepsilon(\bar{\chi}) = \varepsilon(b_r)\varepsilon(\bar{\chi}) = (-1)^r$. Combining (5.3) and (5.4), we finally get the following

Theorem 5.1. *$N^k G(\chi)^{-1} S_\alpha$ is a linear combination of $D(r, \psi\bar{\chi})$ $(1 \leqq r \leqq k+1$, $\psi \in X(u)$, $\varepsilon(\psi) = (-1)^r\chi(-1))$. The coefficients depend only upon ψ, r and the parity of χ.*

For the other expressions of the sum S_α, see Berndt [2] and Kanemitsu-Shiratani [5].

Example 5.1. Case $k = 0$:

$$\begin{aligned} S_\alpha &= \sum_{0 \leqq a \leqq \alpha N}{}' \chi(a) = \frac{G(\chi)}{2\pi i} \sum_{n=1}^{\infty} \frac{b_1(n)\bar{\chi}(n)}{n} , \\ b_1(n) &= -\chi(-1)(1 - \eta^{nt}) + (1 - \eta^{-nt}) \\ &= \begin{cases} \eta^{nt} - \eta^{-nt} & \text{if } \chi(-1) = 1 , \\ 2 - \eta^{nt} - \eta^{-nt} & \text{if } \chi(-1) = -1 , \end{cases} \end{aligned}$$

where $\alpha = t/u$ and $\eta = e^{2\pi i/u}$.

$\alpha = \frac{1}{2}$:

$$b_1 = \begin{cases} 0 & \text{if } \chi(-1) = 1 , \\ 4[1_2] & \text{if } \chi(-1) = -1 , \end{cases}$$

where $[1_2]$ denotes the principal character mod 2.

$$S_{1/2} = 0 , \qquad \text{if } \chi(-1) = 1$$

and

$$S_{1/2} = \frac{G(\chi)}{2\pi i} \cdot 4 \cdot \sum_{n=1}^{\infty} \frac{[1_2](n)\bar{\chi}(n)}{n} = \frac{2G(\chi)}{\pi i} \sum_{n=1}^{\infty} \frac{\bar{\chi}(2n+1)}{2n+1}$$
$$= \frac{G(\chi)}{\pi i}(2 - \bar{\chi}(2))L(1, \bar{\chi}) , \qquad \text{if } \chi(-1) = -1 .$$

When $\chi(n) = (d/n)$, where d is a discriminant number of a certain quadratic number field, then $N = |d|$ and $S_{1/2} = S_1^3$ by the notation of § 0, and

$$S_{1/2} = \begin{cases} 0 & \text{if } d > 0 , \\ \left(2 - \left(\frac{d}{2}\right)\right)\frac{2}{w(d)}h(d) & \text{if } d < 0 , \end{cases}$$

since $G(\chi) = \sqrt{d}$ and $L(1, \chi) = 2\pi h(d)/w(d)\sqrt{|d|}$ $(d < 0)$, where $w(d)$ is the number of roots of unity contained in $Q(\sqrt{d})$.

$\alpha = \frac{1}{3}$:

$$b_1 = \begin{cases} i\sqrt{3}\,[3] & \text{if } \chi(-1) = 1 , \\ 3[1_3] & \text{if } \chi(-1) = -1 , \end{cases}$$

where $[3]$ denotes the unique primitive character mod 3, $[3](n) = (n/3)$, and $[1_3]$ is the principal character mod 3.

$$S_{1/3} = \frac{\sqrt{3}\,G(\chi)}{2\pi}L(1, [3]\bar{\chi}) \qquad \text{if } \chi(-1) = 1$$

and

$$S_{1/3} = \frac{G(\chi)}{2\pi i}(3 - \bar{\chi}(3))L(1, \bar{\chi}) \qquad \text{if } \chi(-1) = -1 .$$

When $\chi(n) = (d/n)$, $S_{1/3} = S_1^3$, and

$$S_{1/3} = \begin{cases} \frac{1}{2}h(-3d) & \text{if } d > 0 \text{ and } 3 \nmid d , \\ \frac{1}{w(d')}\left(3 - \left(\frac{d'}{3}\right)\right)h(d') & \text{if } d = -3d' > 0 , \\ \frac{1}{w(d)}\left(3 - \left(\frac{d}{3}\right)\right)h(d) & \text{if } d < 0 . \end{cases}$$

$\alpha = \frac{1}{5}$:

$$b_1 = \begin{cases} -\frac{1}{2}\bar{g}[5] + \frac{1}{2}g[5]^3 & \text{if } \chi(-1) = 1 , \\ \frac{5}{2}[1_5] - \frac{\sqrt{5}}{2}[5]^2 & \text{if } \chi(-1) = -1 , \end{cases}$$

where $[5]$ is the primitive character mod 5 satisfying $[5]\,(2) = i$ and

$$g = G([5]) = -\sqrt{\frac{5 - \sqrt{5}}{2}} + i\sqrt{\frac{5 + \sqrt{5}}{2}} .$$

$$S_{1/5} = -\frac{G(\chi)}{4\pi i}[\bar{g}L(1, [5]\bar{\chi}) - gL(1, [5]^3\bar{\chi})] \qquad \text{if } \chi(-1) = 1$$

and

$$S_{1/5} = \frac{G(\chi)}{4\pi i}(5 - \bar{\chi}(5))L(1, \bar{\chi}) - \frac{\sqrt{5}\,G(\chi)}{4\pi i}L(1, [5]^2\bar{\chi}) \quad \text{if } \chi(-1) = -1 .$$

When $\chi(n) = (d/n)$, $S_{1/5} = S_1^5$ and

$$S_{1/5} = \begin{cases} -\frac{\sqrt{d}}{2\pi}\operatorname{Im}\left(\bar{g}L\left(1, [5]\left(\frac{d}{-}\right)\right)\right) & \text{if } d > 0 \text{ and } 5 \nmid d , \\ \frac{\sqrt{d}}{2\pi}\operatorname{Im}\left(gL\left(1, [5]\left(\frac{d'}{-}\right)\right)\right) & \text{if } d = 5d' > 0 , \\ \frac{1}{2w(d)}\left(5 - \left(\frac{d}{5}\right)\right)h(d) - \frac{1}{4}h(5d) & \text{if } d < 0 \text{ and } 5 \nmid d , \\ \frac{5}{4}h(d) - \frac{1}{2w(d')}\left(5 - \left(\frac{d'}{5}\right)\right)h(d') & \text{if } d = 5d' < 0 . \end{cases} \tag{5.5}$$

In the same way, we have, for $\alpha = 2/5$ and $\chi(n) = (d/n)$,

$$(5.6)\quad S_{2/5}=\begin{cases}-\dfrac{\sqrt{d}}{2\pi}\operatorname{Re}\left(gL\left(1,[5]\left(\dfrac{d}{-}\right)\right)\right) & \text{if } d>0 \text{ and } 5\nmid d,\\ -\dfrac{\sqrt{d}}{2\pi}\operatorname{Re}\left(gL\left(1,[5]\left(\dfrac{d'}{-}\right)\right)\right) & \text{if } d=5d'>0,\\ \dfrac{1}{2w(d)}\left(5-\left(\dfrac{d}{5}\right)\right)h(d)+\dfrac{1}{4}h(5d) & \text{if } d<0 \text{ and } 5\nmid d,\\ \dfrac{5}{4}h(d)+\dfrac{1}{2w(d')}\left(5-\left(\dfrac{d'}{5}\right)\right)h(d') & \text{if } d=5d'<0.\end{cases}$$

Combining (5.5) and (5.6),

$$L\left(1,[5]\left(\frac{d}{-}\right)\right)=\frac{2\pi}{\bar{g}\sqrt{d}}(S_{2/5}+iS_{1/5}) \qquad \text{if } d>0 \text{ and } 5\nmid d,$$

and

$$h(5d)=2(S_{2/5}-S_{1/5})=2S_2^5 \qquad \text{if } d<0 \text{ and } 5\nmid d.$$

Example 5.2. Case $k=1$:

$$\begin{aligned}S_\alpha&=\frac{1}{N}\sum_{0\leqq a\leqq aN}{}'\chi(a)a\\&=\frac{\alpha G(\chi)}{2\pi i}\sum_{n=1}^{\infty}\frac{b_1(n)\bar{\chi}(n)}{n}+\frac{G(\chi)}{(2\pi i)^2}\sum_{n=1}^{\infty}\frac{b_2(n)\bar{\chi}(n)}{n^2}.\end{aligned}$$

$$b_1(n)=\chi(-1)\eta^{nt}-\eta^{-nt}.$$

$$b_2(n)=\chi(-1)(1-\eta^{nt})+(1-\eta^{-nt}).$$

$\alpha=\frac{1}{2}$:

If $\chi(-1)=1$, $\begin{cases}b_1=0,\\ b_2=4[1_2].\end{cases}$

$$S_{1/2}=-\frac{G(\chi)}{4\pi^2}(4-\bar{\chi}(2))L(2,\bar{\chi}).$$

If $\chi(-1)=-1$, $\begin{cases}b_1=-2[1]^2+2[1_2],\\ b_2=0.\end{cases}$

$$\begin{aligned}S_{1/2}&=-\frac{G(\chi)}{4\pi i}[\bar{\chi}(2)L(1,\bar{\chi})-(2-\bar{\chi}(2))L(1,\bar{\chi})]\\&=\frac{G(\chi)}{2\pi i}(1-\bar{\chi}(2))L(1,\bar{\chi}).\end{aligned}$$

$\alpha=\frac{1}{3}$:

If $\chi(-1)=1$, $\begin{cases}b_1=i\sqrt{3}\,[3],\\ b_2=-3[1_3].\end{cases}$

$$S_{1/3}=\frac{G(\chi)}{2\sqrt{3}\,\pi}L(1,[3]\bar{\chi})-\frac{G(\chi)}{12\pi^2}(9-\bar{\chi}(3))L(2,\bar{\chi}).$$

If $\chi(-1)=-1$, $\begin{cases}b_1=-2[1]^{(3)}+[1_3],\\ b_2=i\sqrt{3}\,[3].\end{cases}$

$$S_{1/3}=\frac{G(\chi)}{6\pi i}(1-\bar{\chi}(3))L(1,\bar{\chi})-\frac{i\sqrt{3}\,G(\chi)}{4\pi^2}L(2,[3]\bar{\chi}).$$

The conjugate function $\tilde{f}$ of f defined at the beginning of this section is given by the singular integral

$$\tilde{f}(x)=PV\int_0^1 f(x-y)\cot\pi y\,dy.$$

The Fourier series of $\tilde{f}$,

$$(5.7)\qquad \tilde{f}(x)\sim -i\sum_{n=-\infty}^{\infty}\operatorname{sgn}(n)\hat{f}_n e^{2\pi i n x},$$

converges to $\tilde{f}(x)$ at every $x\neq 0,\alpha$. We define another character sum

$$T_\alpha=\sum_{a=0}^{N-1}\chi(a)\tilde{f}\left(\frac{a}{N}\right)$$

for a primitive Dirichlet character $\chi \bmod N$, where we assume $N\nmid u$ and the sum is taken over $(a,N)=1$. Then, from (5.2) and (5.7),

$$\begin{aligned}(5.8)\qquad T_\alpha&=\sum_{a=0}^{N-1}\chi(a)(-i)\sum_{n=-\infty}^{\infty}\operatorname{sgn}(n)\hat{f}_n\zeta^{nt}\\&=-i\sum_{n=-\infty}^{\infty}\operatorname{sgn}(n)\hat{f}_n\sum_{a=0}^{N-1}\chi(a)\zeta^{nt}=-iG(\chi)\sum_{n=-\infty}^{\infty}\operatorname{sgn}(n)\bar{\chi}(n)\hat{f}_n\\&=(-i)k!\,G(\chi)\sum_{r=1}^{k}\frac{\alpha^{k-r+1}}{(2\pi i)^r(k-r+1)!}\sum_{n=1}^{\infty}\frac{\tilde{b}_r(n)\bar{\chi}(n)}{n^r}\\&\quad-\frac{i\cdot k!\,G(\chi)}{(2\pi i)^{k+1}}\sum_{n=1}^{\infty}\frac{\tilde{b}_{k+1}(n)\bar{\chi}(n)}{n^{k+1}},\end{aligned}$$

where

$$\tilde{b}_r(n)=(-1)^r\chi(-1)\eta^{nt}-\eta^{-nt} \qquad (1\leqq r\leqq k),$$

$$\tilde{b}_{k+1}(n)=(-1)^k\chi(-1)(1-\eta^{nt})+(1-\eta^{-nt}).$$

Clearly,

$$\tilde{b}_r(-n) = (-1)^{r-1}\chi(-1)\tilde{b}_r(n) \qquad (1 \leqq r \leqq k+1) .$$

We have, corresponding to (5.4),

$$\tilde{b}_r = \sum_{\substack{\psi \in X(u) \\ \varepsilon(\psi) = \varepsilon(\tilde{b}_r)}} \tilde{b}_{r,\psi}\psi .$$

Hence we get

Theorem 5.2. *$G(\chi)^{-1}T_a$ is a linear combination of $D(r, \psi\bar{\chi})$ $(1 \leqq r \leqq k+1$, $\psi \in X(u)$, $\varepsilon(\psi) = (-1)^{r-1}\chi(-1))$, whose coefficients depend only upon ψ, r and the parity of χ.*

All the results on S_a in Example 5.1 and 5.2 can be transfered to T_a canonically.

Example 5.3. Case $k = 0$:

$$\begin{aligned}\tilde{f}(x) &= PV\int_0^a \cot \pi(x-y)dy \\ &= -\frac{1}{\pi}\left(\log 2\,|\sin \pi(x-\alpha)| - \log 2\,|\sin \pi x|\right) \\ &= \frac{1}{\pi}[A_1(x-\alpha) - A_1(x)] .\end{aligned}$$

Therefore,

$$\begin{aligned}T_a &= \frac{1}{\pi}\sum_{a=1}^{N-1}\chi(a)\left[A_1\left(\frac{a}{N}-\alpha\right) - A_1\left(\frac{a}{N}\right)\right] \\ &= \frac{1}{\pi}\sum_{a=1}^{N-1}\chi(a)\log\left|\frac{\sin \pi(a/N)}{\sin \pi(a/N-\alpha)}\right| .\end{aligned}$$

On the other hand, from (5.8),

$$T_a = -\frac{G(\chi)}{2\pi}\sum_{n=1}^{\infty}\frac{\tilde{b}_1(n)\bar{\chi}(n)}{n} ,$$

where

$$\tilde{b}_1(n) = \chi(-1)(1-\eta^{nt}) + (1-\eta^{-nt}) .$$

From Proposition 4.1 we see that

$$\sum_{a=1}^{N-1}\chi(a)A_1\left(\frac{a}{N}\right) = \begin{cases} G(\chi)L(1,\bar{\chi}) & \text{if } \chi(-1) = 1 , \\ 0 & \text{if } \chi(-1) = -1 . \end{cases}$$

Put

$$T_a^* = \sum_{a=1}^{N-1}\chi(a)A_1\left(\frac{a}{N}-\alpha\right) = -\sum_{a=1}^{N-1}\chi(a)\log\left|\sin \pi\left(\frac{a}{N}-\alpha\right)\right| ;$$

then

$$T_a^* = \pi T_a + \begin{cases} G(\chi)L(1,\bar{\chi}) & \text{if } \chi(-1) = 1 , \\ 0 & \text{if } \chi(-1) = -1 . \end{cases}$$

$\alpha = \frac{1}{2}$:

$$b_1 = \begin{cases} 4[1_2] & \text{if } \chi(-1) = 1 , \\ 0 & \text{if } \chi(-1) = -1 . \end{cases}$$

$$T_{1/2} = -\frac{G(\chi)}{\pi}(2 - \bar{\chi}(2))L(1,\bar{\chi}) \qquad \text{if } \chi(-1) = 1$$

and

$$T_{1/2} = 0 \qquad \text{if } \chi(-1) = -1 .$$

When $\chi(n) = (d/n)$,

$$T_{1/2} = \begin{cases} -\frac{2}{\pi}\left(2 - \left(\frac{d}{2}\right)\right)h(d)R(d) & \text{if } d > 0 , \\ 0 & \text{if } d < 0 , \end{cases}$$

where $R(d) = \log \varepsilon_d$ and $\varepsilon_d > 1$ is the fundamental unit of $Q(\sqrt{d})$.

$\alpha = \frac{1}{3}$:

$$\tilde{b}_1 = \begin{cases} 3[1_3] & \text{if } \chi(-1) = 1 , \\ i\sqrt{3}\,[3] & \text{if } \chi(-1) = -1 . \end{cases}$$

$$T_{1/3} = -\frac{G(\chi)}{2\pi}(3 - \bar{\chi}(3))L(1,\bar{\chi}) \qquad \text{if } \chi(-1) = 1 ,$$

and

$$T_{1/3} = -\frac{i\sqrt{3}\,G(\chi)}{2\pi}L(1,[3]\bar{\chi}) \qquad \text{if } \chi(-1) = -1 .$$

When $\chi(n) = (d/n)$,

$$T_{1/3} = \begin{cases} -\frac{1}{\pi}\left(3 - \left(\frac{d}{3}\right)\right)h(d)R(d) & \text{if } d > 0 , \\ \frac{1}{\pi}h(-3d)R(-3d) & \text{if } d < 0 \text{ and } 3 \nmid d , \\ \frac{1}{\pi}\left(3 - \left(\frac{d'}{3}\right)\right)h(d')R(d') & \text{if } d = -3d' < 0 . \end{cases}$$

$\alpha = \frac{1}{5}$:

$$\tilde{b}_1 = \begin{cases} \frac{5}{2}[1_5] - \frac{\sqrt{5}}{2}[5]^2 & \text{if } \chi(-1) = 1\ , \\ -\frac{1}{2}\bar{g}[5] + \frac{1}{2}g[5]^3 & \text{if } \chi(-1) = -1\ . \end{cases}$$

$$T_{1/5} = -\frac{G(\chi)}{4\pi}(5 - \bar{\chi}(5))L(1, \bar{\chi}) + \frac{\sqrt{5}\,G(\chi)}{4\pi}L(1, [5]^2\bar{\chi}) \quad \text{if } \chi(-1) = 1\ .$$

$$T_{1/5} = \frac{G(\chi)}{4\pi}[\bar{g}L(1, [5]\bar{\chi}) - gL(1, [5]^3\bar{\chi})] \quad \text{if } \chi(-1) = -1\ .$$

When $\chi(n) = (d/n)$,

$$(5.9)\quad T_{1/5} = \begin{cases} -\frac{1}{2\pi}\left(5 - \left(\frac{d}{5}\right)\right)h(d)R(d) + \frac{1}{2\pi}h(5d)R(5d) & \text{if } d > 0 \text{ and } 5 \nmid d\ , \\ -\frac{5}{2\pi}h(d)R(d) + \frac{1}{2\pi}\left(5 - \left(\frac{d'}{5}\right)\right)h(d')R(d') & \text{if } d = 5d' > 0\ , \\ -\frac{\sqrt{|d|}}{2\pi}\operatorname{Im}\left(\bar{g}L\left(1, [5]\left(\frac{d}{-}\right)\right)\right) & \text{if } d < 0 \text{ and } 5 \nmid d\ , \\ \frac{\sqrt{|d|}}{2\pi}\operatorname{Im}\left(gL\left(1, [5]\left(\frac{d'}{-}\right)\right)\right) & \text{if } d = 5d' < 0\ . \end{cases}$$

In the same way, we have, for $\alpha = 2/5$ and $\chi(n) = (d/n)$,

$$(5.10)\quad T_{1/5} = \begin{cases} -\frac{1}{2\pi}\left(5 - \left(\frac{d}{5}\right)\right)h(d)R(d) - \frac{1}{2\pi}h(5d)R(5d) & \text{if } d > 0 \text{ and } 5 \nmid d\ , \\ -\frac{5}{2\pi}h(d)R(d) - \frac{1}{2\pi}\left(5 - \left(\frac{d'}{5}\right)\right)h(d')R(d') & \text{if } d = 5d' > 0\ , \\ -\frac{\sqrt{|d|}}{2\pi}\operatorname{Re}\left(\bar{g}L\left(1, [5]\left(\frac{d}{-}\right)\right)\right) & \text{if } d < 0 \text{ and } 5 \nmid d\ , \\ -\frac{\sqrt{|d|}}{2\pi}\operatorname{Re}\left(gL\left(1, [5]\left(\frac{d'}{-}\right)\right)\right) & \text{if } d = 5d' < 0\ . \end{cases}$$

Combining (5.9) and (5.10),

$$h(5d)R(5d) = -\pi(T_{2/5} - T_{1/5}) = \sum_{a=1}^{d-1}\left(\frac{d}{a}\right)\log\left|\frac{\sin\pi(a/d - 2/5)}{\sin\pi(a/d - 1/5)}\right| \quad \text{if } d > 0 \text{ and } 5 \nmid d\ .$$

$$L\left(1, [5]\left(\frac{d}{-}\right)\right) = -\frac{2\pi}{g\sqrt{|d|}}(T_{2/5} + iT_{1/5}) \quad \text{if } d < 0 \text{ and } 5 \nmid d\ .$$

References

[1] Berndt, B. C., Character analogues of the Poisson and Euler-Maclaurin summation formulas with applications, J. Number Theory **7** (1975), 413–445.

[2] ——, Periodic Bernoulli Numbers, summation formulas and applications, Theory and applications of special functions, Academic Press, New York, 1975.

[3] Gauss, C. F., Carl Friedrich Gauss Werke, **II** Königliche Gesellschaft Wiss., Göttingen, 1863.

[4] Johnson, W. and Mitchel, K. J., Symmetries for sums of the Legendre symbol (to appear).

[5] Kanemitsu, S. and Shiratani, K., An application of the Bernoulli functions to character sums, Mem. Faculty of Science Kyushu Univ., Ser A. **30** (1976), 65–73.

[6] Karpinski, L., Uber die Verteilung der quadratischen Reste, J. reine angew. Math. **127** (1904), 1–19.

[7] Lerch, M., Essais sur le calcul de nombre des classes de formes quadratiques binaires aux coefficients entiers, Acta Math. **29** (1905), 333–424, **30** (1906), 203–293.

[8] Yamamoto, Y., On Sato's conjecture (in Japanese), Master's thesis (Osaka Univ.) (unpublished).

Department of Mathematics
Faculty of Science
Osaka University
Toyonaka, Osaka 560
Japan

ALGEBRAIC NUMBER THEORY, Papers contributed for the International Symposium, Kyoto 1976; S. Iyanaga (Ed.): Japan Society for the Promotion of Science, Tokyo, 1977

On Extraordinary Representations of GL_2

HIROYUKI YOSHIDA

Introduction

Let k be a non-archimedean local field. In § 12 of Jacquet-Langlands [7], it is shown that there is a certain correspondence from continuous 2-dimensional representations of the Weil group W_k to irreducible admissible representations of $GL_2(k)$, under the assumption of the Artin conjecture about the holomorphy of "Artin-Hecke" L-functions. We need a precise statement of this conjectural correspondence. Let σ be a continuous representation of W_k in $GL_2(\boldsymbol{C})$. Then $\det\sigma$ defines a quasicharacter ω of $k^\times$ because every continuous one dimensional representation of W_k factors through the transfer map $W_k \to k^\times$. For an irreducible admissible representation π of $GL_2(k)$, let ω_π denote the quasicharacter of $k^\times$ which is defined by the restriction of π to the center of $GL_2(k)$. Let ψ be a non-trivial additive character of k.

Conjecture. *There exists an irreducible admissible representation $\pi = \pi(\sigma)$ of $GL_2(k)$ which satisfies that* (i) $\det\sigma = \omega_\pi$, (ii) $L(s, \sigma\otimes\chi) = L(s, \pi\otimes\chi)$, (iii) $\varepsilon(s, \sigma\otimes\chi, \psi) = \varepsilon(s, \pi\otimes\chi, \psi)$ *for every quasicharacter χ of $k^\times$, where $\varepsilon(s, \sigma\otimes\chi, \psi)$ denotes the "Artin root number" and $L(s, \sigma\otimes\chi)$ the L-function of the representation $\sigma\otimes\chi$ of W_k, which are defined in* [3], [8]. *$L(s, \pi\otimes\chi)$ and $\varepsilon(s, \pi\otimes\chi, \psi)$ are defined in* [7].

We should recall that this conjecture can be regarded as a non-abelian analogue of local class field theory and remains unsolved only when the residual characteristic of k is 2 (cf. [2], [15]). Because the problem is local, a purely local approach may be worth attempting. In § 1, we shall prove that the existence of the representation $\pi(\sigma)$ is equivalent to certain relations satisfied by the Artin root numbers (Theorem 1). Let Z be the center of $GL_2(k)$ and $\mathfrak{O}$ the maximal compact subring of k. Let τ be a "strongly cuspidal" representation (cf. § 2) of $GL_2(\mathfrak{O})\cdot Z$. By a theorem of Casselman [1], we know that

Ind $(\tau, GL_2(\mathfrak{O})\cdot Z \to GL_2(k)) \cong \pi$ or $\pi \oplus \pi\otimes\nu_0$ where π is an irreducible admissible absolutely cuspidal representation of $GL_2(k)$ and ν_0 is the unramified character of order 2 of $k^\times$. We can compute the local functional equation of $\pi\otimes\chi$ from τ for any quasicharacter χ of $k^\times$ (Theorem 2). By considering the restriction of $\pi(\sigma)$ to $GL_2(\mathfrak{O})$, we get such τ and another conjectural correspondence $\sigma \to \tau(\sigma)$. As an application of Theorem 1 and 2, we can see that there is an algorithm to check the conjecture when σ is given.

§ 3 and § 4 are entirely based on the recent work of Langlands [9]. In § 3, we shall show that $\pi(\sigma)$ exists if the module of k is an odd power of 2 and σ is of "tetrahedral type" (Theorem 3). Our proof depends on the consideration of the behavior of an irreducible admissible representation of $GL_2(k)$ under the automorphism group of C. Let K/k be a finite Galois extension of algebraic number fields and σ a 2-dimensional representation of $\mathrm{Gal}(K/k)$ of "tetrahedral type". In § 4, we discuss some problem about the existence of the automorphic representation $\pi(\sigma)$ of $GL_2(k_A)$.

Notations and terminologies.

For a non-archimedean local field k, $\mathfrak{O}_k$ (sometimes we drop the suffix k) denotes the maximal compact subring of k. If ρ (resp. π) is a finite dimensional continuous (resp. irreducible admissible) representation of the Weil group W_k (resp. $GL_2(k)$), $f(\rho)$ (resp. $f(\pi)$) denotes the conductor of ρ (resp. π). We denote the quasicharacter $\det\rho$ of $k^\times$ by ω_ρ. For an algebraic number field F, F_A and $F_A^\times$ denote the adele ring and the idele group of F respectively. If an object π is defined globally with respect to F and v is a place of F, π_v denotes the local object obtained naturally from π. Let σ be a representation of a group G in $GL_2(C)$ and ϕ the natural map $GL_2(C) \to PGL_2(C)$. We call σ "of tetrahedral type" if $\phi\circ\sigma(G)$ is isomorphic to A_4. For others, we follow the notations and terminologies of Jacquet-Langlands [7], Langlands [9] and Weil [14].

§ 1. $\pi(\sigma)$ and the Artin root numbers

We may assume that σ is irreducible. (If σ is reducible, the existence of the special representations causes a little trouble. The conjecture is true, however, after a little modification). The irreducibility implies that $\pi(\sigma)$ is absolutely cuspidal, because we have $L(s, \sigma\otimes\chi) = 1$ for every quasicharacter χ of $k^\times$ (cf. [6], I. 47). Let π be an irreducible admissible absolutely cuspidal representation of $GL_2(k)$, $w = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in GL_2(k)$, $\mathscr{S}(k^\times)$ the vector space of all the

Schwarz-Bruhat functions on $k^\times$ and χ a quasicharacter of $k^\times$. We use the same letter π for the Kirrilov realization of π, which is the representation equivalent to π realized on $\mathscr{S}(k^\times)$ and satisfies that $\left(\pi\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}\xi\right)(x) = \psi(bx)\xi(ax)$ for $\forall\xi \in \mathscr{S}(k^\times)$, $x \in k^\times$. Then the local functional equation of $\pi\otimes\chi$ takes the following form;

$$(1)\qquad \int_{k^\times} (\pi(w)\xi)(x)\omega_\pi^{-1}(x)\chi^{-1}(x)|x|^{1/2-s}d^\times x = \varepsilon(s, \pi\otimes\chi, \psi)\int_{k^\times}\hat{\xi}(x)\chi(x)|x|^{s-1/2}d^\times x \qquad \text{for } \forall\xi \in \mathscr{S}(k^\times)\ ,$$

where $|x|$ denotes the absolute value of $x \in k^\times$ and $d^\times x$ denotes a Haar measure on $k^\times$. Hence, by the Fourier inversion formula, the action of w is given by

$$(2)\qquad (\pi(w)\xi)(x) = \int_{\hat{k}^\times}\left\{\varepsilon(\pi\otimes\chi\omega_\pi^{-1}, \psi)\int_{k^\times}\xi(x)\chi\omega_\pi^{-1}(x)d^\times x\right\}\chi(x)d^\times\chi\ ,$$

where $\hat{k}^\times$ denotes the Pontrjagin dual of $k^\times$, $d^\times\chi$ the dual measure of $d^\times x$ and we put $\varepsilon(\pi\otimes\chi\omega_\pi^{-1}, \psi) = \varepsilon(1/2, \pi\otimes\chi\omega_\pi^{-1}, \psi)$. Let us define the action of $B = \left\{g = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \middle| g \in GL_2(k)\right\}$ by

$$(3)\qquad \left(\pi\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\xi\right)(x) = \omega(d)\psi(bd^{-1}x)\xi(ad^{-1}x)\ , \qquad \omega = \det\sigma$$

and the action of w by

$$(4)\qquad (\pi(w)\xi)(x) = \int_{\hat{k}^\times}\left\{\varepsilon(\sigma\otimes\chi\omega^{-1}, \psi)\int_{k^\times}\xi(x)\chi\omega^{-1}(x)d^\times x\right\}\chi(x)d^\times\chi\ ,$$

where $\varepsilon(\sigma\otimes\chi\omega^{-1}, \psi) = \varepsilon(1/2, \sigma\otimes\chi\omega^{-1}, \psi)$. Then it is clear that the conjecture is reduced to the following question; "*Does this action define an irreducible admissible representation of* $GL_2(k)$?" To prove that π is a homomorphism, it is enough to show that π preserves all the relations among the generators of $GL_2(k)$. We note the Bruhat decomposition

$$(5)\qquad GL_2(k) = B \cup BwB \qquad \text{(disjoint union)}\ .$$

It is obvious that π defines a homomorphism $B \to \mathrm{Aut}(\mathscr{S}(k^\times))$ by (3). The relations between the elements of B and w are reduced into three types.

(i) $w^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, (ii) $w\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} = \begin{pmatrix} \beta & 0 \\ 0 & \alpha \end{pmatrix}w$,

(iii) $w\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}w = \begin{pmatrix} -\alpha^{-1} & 1 \\ 0 & -\alpha \end{pmatrix}w\begin{pmatrix} 1 & -\alpha^{-1} \\ 0 & 1 \end{pmatrix}$.

Let λ be a character of $k^\times$ and q the module of k. Define an element $\xi_\lambda^{(n)}$ $(n \in \boldsymbol{Z})$ of $\mathscr{S}(k^\times)$ by

$$(6) \qquad \xi_\lambda^{(n)}(x) = \begin{cases} \lambda(x) & \text{if } |x| = q^n \\ 0 & \text{otherwise .} \end{cases}$$

Any element of $\mathscr{S}(k^\times)$ can be written as a finite linear combination of $\xi_\lambda^{(n)}$. Therefore it is enough to verify the relations (i), (ii), (iii) only for $\xi_\lambda^{(n)}$. We normalize $d^\times x$ so that the volume of $\mathfrak{O}^\times$ is 1 and ψ so that $\mathfrak{O}$ is the largest ideal of k on which ψ is trivial. It is easy to see the following properties of ε-function.

$$(7) \qquad \varepsilon(s, \sigma \otimes \lambda^{-1}, \psi) = \varepsilon(\sigma \otimes \lambda^{-1}, \psi) \cdot q^{-f(s-1/2)} \qquad \text{with } f = f(\sigma \otimes \lambda^{-1}) .$$

$$(8) \qquad \begin{cases} f(\sigma \otimes \lambda^{-1}) = f(\sigma \otimes \lambda\omega^{-1}) \\ \varepsilon(\sigma \otimes \lambda^{-1}, \psi)\varepsilon(\sigma \otimes \lambda\omega^{-1}, \psi) = \omega(-1) . \end{cases}$$

From (4), (7), we obtain

$$(9) \qquad \pi(w)\xi_\lambda^{(n)} = \varepsilon(\sigma \otimes \lambda^{-1}, \psi)\xi_{\omega\lambda^{-1}}^{(f-n)} ,$$

and we can verify the relations (i) and (ii) from (8), (9). It is enough to verify (iii) for $\xi_\lambda^{(0)}$, because if we take the inner automorphism by $\begin{pmatrix} 1 & 0 \\ 0 & \mu \end{pmatrix}$, $\mu \in k^\times$, the relation (iii) for α is transformed to that for $\mu\alpha$. Let ϖ be a prime element of k. We may assume that $\alpha = \varpi^\delta$ with $\delta \in \boldsymbol{Z}$ and $\lambda(\varpi) = 1$. For a character η of $k^\times$ and $a \in \boldsymbol{Z}$, put

$$(10) \qquad \Delta_a(\eta, \psi) = \int_{\mathfrak{O}^\times} \psi(\varpi^{-a}u)\eta(u)d^\times u .$$

We have the Fourier expansion

$$(11) \qquad \psi(\varpi^N x) = \sum_\eta \Delta_{n-N}(\eta^{-1}, \psi)\eta(x) \qquad \text{for } x \in k^\times,\ |x| = q^n,\ N \in \boldsymbol{Z} ,$$

where η extends over all the characters of $k^\times$ such that $\eta(\varpi) = 1$.

Lemma 1. *Let σ be as above and η a quasicharacter of $k^\times$. If $f(\sigma) \geq 2f(\eta)$, we have $f(\sigma \otimes \eta) \leqq f(\sigma)$. If $f(\sigma) < 2f(\eta)$, we have $f(\sigma \otimes \eta) = 2f(\eta)$.*

We can prove this lemma using Lemma 3 of Weil [15]. We consider the equation

$$(E) \qquad \pi(w)\pi\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}\pi(w)\ \xi_\lambda^{(0)} = \pi\begin{pmatrix} -\alpha^{-1} & 1 \\ 0 & -\alpha \end{pmatrix}\pi(w)\pi\begin{pmatrix} 1 & -\alpha^{-1} \\ 0 & 1 \end{pmatrix}\xi_\lambda^{(0)}$$

with $\alpha = \varpi^\delta$. Put $f = f(\sigma \otimes \lambda^{-1})$ and assume that $\omega(\varpi) = 1$. Using (11) and Lemma 1, we can see the followings.

If $0 < \delta < f$, (E) is equivalent to

$$(A) \qquad \begin{aligned} &\chi(-1)\varepsilon(\sigma \otimes \lambda^{-1}, \psi)\varepsilon(\sigma \otimes \chi\lambda\omega^{-1}, \psi)\Delta_{f-\delta}(\chi, \psi) \\ &\quad = \sum_j \varepsilon(\sigma \otimes \eta_j\lambda^{-1}, \psi)\Delta_\delta(\eta_j, \psi)\Delta_{f-\delta}(\eta_j\omega\lambda^{-2}\chi^{-1}, \psi) , \end{aligned}$$

where χ is any character of $k^\times$ such that $\Delta_{f-\delta}(\chi, \psi) \neq 0$, $\chi(\varpi) = 1$, $f_j = f(\sigma \otimes \eta_j\lambda^{-1})$ and η_j extends over all the characters of $k^\times$ such that $f(\sigma \otimes \chi\lambda\omega^{-1}) - f = f_j - 2\delta$, $\eta_j(\varpi) = 1$.

If $\delta \leqq 0$ or $f \leqq \delta$, (E) is equivalent to

$$(B) \qquad \varepsilon(\sigma \otimes \lambda^{-1}\eta, \psi) = \varepsilon(\omega\lambda^{-2}\eta, \psi)\varepsilon(\eta, \psi)$$

for any quasicharacter η such that $f(\eta) = \delta$ (resp. $f - \delta$) if $f \leqq \delta$ (resp. $\delta \leqq 0$). Now we can state our first theorem.

Theorem 1. *The conjecture for σ is equivalent to the relations* (A) *and* (B) *satisfied by the ε-function.*

Proof. It is enough to prove that π is irreducible and admissible under the assumption of (A) and (B). That π is admissible is equivalent to (i) For any $\xi \in \mathscr{S}(k^\times)$, the stabilizer Γ_ξ of ξ is open. (ii) For a positive integer N, put $\Gamma(N) = \left\{ g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| g \in GL_2(\mathfrak{O}) \text{ and } a - 1 \equiv d - 1 \equiv b \equiv c \equiv 0 \bmod \varpi^N \right\}$. The vectors fixed by $\Gamma(N)$ make a finite dimensional vector space. To prove (i), we may assume that $\xi = \xi_\lambda^{(0)}$. We have $\pi\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\xi_\lambda^{(0)} = \xi_\lambda^{(0)}$ if $a - 1 \equiv d - 1 \equiv 0 \bmod \varpi^u$ with $u = \max.(f(\lambda), f(\omega))$ and $b \in \mathfrak{O}$. Also we can see that $\pi\begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}\xi_\lambda^{(0)} = \xi_\lambda^{(0)}$ if $c \in \varpi^f\mathfrak{O}$ with $f = f(\sigma \otimes \lambda^{-1})$. Therefore Γ_ξ contains $\Gamma(N)$, where $N = \max.(u, f)$. Hence (i) is proved. Let us assume that $\xi = \sum_{i=1}^n a_i\xi_{\lambda_i}^{(n_i)}$ is fixed by $\Gamma(N)$. We may assume that $\lambda_i(\varpi) = 1$ $(\forall i)$ and $(\lambda_i, n_i) \neq (\lambda_j, n_j)$ if $i \neq j$. We have $\pi\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}\xi_{\lambda_i}^{(n_i)} = \lambda_i(a)\xi_{\lambda_i}^{(n_i)}$ for $a \in \mathfrak{O}^\times$. Therefore $f(\lambda_i) \leqq N$ holds. Moreover we have $\pi\begin{pmatrix} 1 & \varpi^N \\ 0 & 1 \end{pmatrix}\xi(x) = \psi(\varpi^N x)\xi(x) = \xi(x)$. We may assume that $N \geqq 2$. In (11), $f(\eta)$ must be equal to $n - N$ if $n - N \geqq 2$. Therefore if $n_i > 2N$ for some i, (11) contradicts the fact $f(\lambda_i) \leqq N$. Hence we get $n_i \leqq 2N$ for all $1 \leqq i \leqq n$. Considering $\pi\begin{pmatrix} 1 & 0 \\ \varpi^N & 1 \end{pmatrix}\xi = \xi$, we get $n_i \geqq -2N$ for

all $1 \leqq i \leqq n$ by the same argument. This proves (ii). The irreducibility is an immediate consequence from the uniqueness of the Kirillov model.

Let α be an element of $\mathrm{Aut}(C)$, the group of the field automorphisms of C. Let π be an irreducible admissible absolutely cuspidal representation of $GL_2(k)$. For every character λ of $k^\times$, we put $\varepsilon(\pi^\alpha \otimes \lambda, \psi^\alpha) = \varepsilon(\pi \otimes \lambda^{\alpha^{-1}}, \psi)^\alpha$ and $\varepsilon(s, \pi^\alpha \otimes \lambda, \psi^\alpha) = \varepsilon(\pi \otimes \lambda^{\alpha^{-1}}, \psi)^\alpha, q^{-f(s-1/2)}$ where $f = f(\pi \otimes \lambda^{\alpha^{-1}})$. Let ν be the quasicharacter of $k^\times$ defined by $\nu(x) = |x|$ and put $\varepsilon(s, \pi^\alpha \otimes \lambda \otimes \nu^{s'}, \psi^\alpha) = \varepsilon(s + s', \pi^\alpha \otimes \lambda, \psi^\alpha)$. It is easy to see that $\varepsilon(s, \pi^\alpha \otimes \lambda, \psi^\alpha)$ is well defined for every quasicharacter λ of $k^\times$. By the same method as the proof of Theorem 1, we can prove

Corollary. *Define the action of B on $\mathscr{S}(k^\times)$ by (3) using $\omega_\pi^\alpha, \psi^\alpha$ instead of ω_π and ψ and that of w by (2) using $\varepsilon(\pi^\alpha \otimes \chi(\omega_\pi^\alpha)^{-1}, \psi^\alpha)$ instead of $\varepsilon(\pi \otimes \chi\omega_\pi^{-1}, \psi)$ for every $\chi \in \hat{k}^\times$. Then this action defines an irreducible admissible absolutely cuspidal representation π^α of $GL_2(k)$.*

Remark 1. It seems possible to generalize Theorem 1 for GL_n and more general law of reciprocity, which is formulated in Gelfand-Kajdan [5].

§ 2. The restriction of $\pi(\sigma)$ to $GL_2(\mathfrak{O})$

Let the notation be as in the previous section. We take a quasicharacter χ of $k^\times$ such that $\sigma \otimes \chi$ has the minimum conductor c. Replacing σ by $\sigma \otimes \chi$, we may assume that $f(\sigma \otimes \chi) \geqq f(\sigma)$ for every quasicharacter χ of $k^\times$. Let us define a vector subspace V of $\mathscr{S}(k^\times)$. If $c = f(\sigma)$ is even, V is generated by $\xi_\lambda^{(f_0)}$ with $f(\lambda) \leqq f_0$, where $2f_0 = c$. We have $\dim V = (q-1)q^{f_0-1}$. If c is odd, V is generated by $\xi_\lambda^{(f_0-1)}$ with $f(\lambda) \leqq f_0 - 1$ and $\xi_\lambda^{(f_0)}$ with $f(\lambda) \leqq f_0$, where $2f_0 - 1 = c$. We have $\dim V = (q-1)(q+1)q^{f_0-2}$. Put $B(\mathfrak{O}) = B \cap GL_2(\mathfrak{O})$.

Proposition 1. *$\pi(w)$ and $\pi(b)$ $(b \in B(\mathfrak{O}))$ induce the automorphisms of V.*

This proposition follows from (9), (11) and Lemma 1. Therefore if (A) and (B) are satisfied, we obtain a representation $GL_2(\mathfrak{O}) \to \mathrm{Aut}(V)$ because $GL_2(\mathfrak{O})$ is generated by $B(\mathfrak{O})$ and w. We denote this conjectural representation by $\tau(\sigma)$ and it is easy to see that $\tau(\sigma)$ necessarily factors through the natural map $GL_2(\mathfrak{O}) \to GL_2(\mathfrak{O}/\varpi^{f_0})$. We note that we can check the existence of $\tau(\sigma)$ by finite calculations. If c is small, we can prove

Proposition 2. *Assume that $q = 2$, $c = 3$. Then $\tau(\sigma)$ exists if and only if $\varepsilon(\sigma \otimes \chi, \psi) = -\chi(-1)$, where χ is any character of $k^\times$ of conductor 2 such that $\chi^2 = 1$.*

Proposition 2 follows from (i), (ii) and Lemma 1, taking account of the relations between w and the elements of $B(\mathfrak{O})$ modulo ϖ^2. There exists a "non-dihedral" absolutely cuspidal representation of $GL_2(\boldsymbol{Q}_2)$ of conductor 3. This fact suggests that the above case already contains some new representations.

Suppose that an irreducible representation τ of $GL_2(\mathfrak{O})$ factors through $GL_2(\mathfrak{O}/\varpi^f)$. Put $N(\mathfrak{O}) = \left\{ g = \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \middle| u \in \mathfrak{O} \right\}$. We call τ strongly cuspidal of level f if every irreducible component χ_i is contained in $\tau | N(\mathfrak{O})$ with multiplicity 1 and χ_i does not factor through $\mathfrak{O} \to \mathfrak{O}/\varpi^{f-2}$. If every χ_i does not factor through $\mathfrak{O} \to \mathfrak{O}/\varpi^{f-1}$, τ is called "with primitive $N(\mathfrak{O})$-spectrum". These terminologies are due to Casselman [1]. It is easy to prove

Proposition 3. *Assume that $\tau(\sigma)$ exists. Then $\tau(\sigma)$ is a strongly cuspidal representation of level f_0.*

As stated in Introduction, we can compute the local functional equations for induced representations. Let τ be a strongly cuspidal representation of level f and ω a quasicharacter of $k^\times$ such that $\tau\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = \omega(a) \cdot 1_n$ $(n = \deg \tau)$ for $a \in \mathfrak{O}^\times$. We extend τ to a representation τ^* of $GL_2(\mathfrak{O}) \cdot Z$ by $\tau^*(gz) = \tau(g)\omega(z)$ for $g \in GL_2(\mathfrak{O})$, $z \in Z$. Define a matrix $A \in M_n(C)$ by $A = \int_{\mathfrak{O}^\times} \tau\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \psi(-\varpi^{-f}u)du$. Let χ be a quasicharacter of $k^\times$. For $t \in Z$, $t \geqq 0$ and $i \in \mathfrak{O}^\times$, we put

$$P(t, i) = \int_{i+\varpi^t\mathfrak{O}} \tau\begin{pmatrix} u^{-1} & 0 \\ 0 & 1 \end{pmatrix} \chi(u)^{-1} \tau\begin{pmatrix} 1 & (u-i)/\varpi^t \\ 0 & 1 \end{pmatrix} d^\times u$$

(if $t = 0$, we understand that $i + \varpi^0\mathfrak{O} = \mathfrak{O}^\times$).

Theorem 2. *When τ is with primitive $N(\mathfrak{O})$-spectrum, let π be the irreducible admissible absolutely cuspidal representation of $GL_2(k)$ defined by $\pi = \mathrm{Ind}(\tau^*, GL_2(\mathfrak{O}) \cdot Z \to GL_2(k))$. Then the local factor $\varepsilon(s, \pi \otimes \chi, \psi)$ is uniquely determined as the solution of*

$$\begin{aligned} A \cdot \Big[& \varepsilon(s, \pi \otimes \chi, \psi) \int_{\mathfrak{O}^\times} \tau\begin{pmatrix} u & 0 \\ 0 & 1 \end{pmatrix} \chi(u)\psi(-\varpi^{-f-t}u)d^\times u \\ & - \chi(\varpi^{2f+2t})\chi(-1)(q^{-2f-2t})^{s-1/2}\omega(\varpi^{f+t}) \\ & \cdot \int_{\mathfrak{O}^\times} \tau\begin{pmatrix} u & 0 \\ \varpi^t & -1 \end{pmatrix} \omega(u)^{-1}\chi(u)^{-1}\psi(-\varpi^{-f-t}u)d^\times u \Big] \cdot P(t, i) = 0 \end{aligned} \tag{12}$$

for every t and i. When τ is not with primitive $N(\mathfrak{O})$-spectrum, let π be an irreducible admissible absolutely cuspidal representation of $GL_2(k)$ such that

$\pi \oplus \pi \otimes \nu_0 = \mathrm{Ind}\,(\tau^*, GL_2(\mathfrak{O})\cdot Z \to GL_2(k))$. *Let* $2f_0 + 1$ *be the conductor of* π. *If* $f(\chi) \geqq f_0 + 1$, $\varepsilon(s, \pi \otimes \chi, \psi)$ *is uniquely determined as the solution of* (12) *for every* t *and* i.

We can make an explicit isomorphism from the representation space of π to its Kirillov model and Theorem 2 follows immediately. If τ is not with primitive $N(\mathfrak{O})$-spectrum and $f(\chi) \leqq f_0$, (12) has no solution. However, $\varepsilon(s, \pi \otimes \chi, \psi)$ can be determined in the following way. Let V be the representation space of τ. For a character ζ of $\mathfrak{O}$ which is contained in $\tau|N(\mathfrak{O})$, let u_ζ be a non-zero vector of V which transforms according to ζ. Let V_1 (resp. V_2) be the vector subspace of V which is spanned by u_ζ such that $f(\zeta) = f_0$ (resp. $f(\zeta) = f_0 + 1$), where $f(\zeta)$ denotes the integer such that $\varpi^{f(\zeta)}$ is the largest ideal of $\mathfrak{O}$ on which ζ is trivial. We may assume that $\omega(\varpi) = 1$. In V_1 (resp. V_2), we can take a vector $v_\lambda^{(i)} (i = 1, 2)$ such that $\tau\left(\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}\right) v_\lambda^{(i)} = \lambda(a) v_\lambda^{(i)}$, $a \in \mathfrak{O}^\times$, where λ is a given character of $k^\times$ such that $f(\lambda) \leqq f_0$ (resp. $f(\lambda) \leqq f_0 + 1$) and $\lambda(\varpi) = 1$. We can take $a \in \mathfrak{O}^\times$ such that $\zeta(x) = \psi(\varpi^{-f_0} a x)$ (resp. $\zeta(x) = \psi(\varpi^{-f_0-1} a x)$) if $u_\zeta \in V_1$ (resp. $u_\zeta \in V_2$) and $x \in \mathfrak{O}$. For each $i (i = 1, 2)$, determine $v_\lambda^{(i)}$ *simultaneously* up to a constant multiple by the relation $u_\zeta = c_\zeta \sum \lambda(a)^{-1} v_\lambda^{(i)} (c_\zeta \in \boldsymbol{C}^\times)$ for every ζ. We can write $\tau(w) v_\lambda^{(1)} = \varepsilon'(\pi \otimes \lambda^{-1}, \psi) v_{\omega\lambda^{-1}}^{(2)}$ with $\varepsilon'(\pi \otimes \lambda^{-1}, \psi) \in \boldsymbol{C}^\times$. Normalize the vectors $v_\lambda^{(2)}$ so that $\varepsilon'(\pi \otimes \lambda^{-1}, \psi)\varepsilon'(\pi \otimes \omega\lambda, \psi) = \omega(-1)$. This determines the vectors $v_\lambda^{(2)}$ up to the multiple by ± 1 when $v_\lambda^{(1)}$ are chosen. Then we have $\varepsilon(\pi \otimes \lambda, \psi) = \varepsilon'(\pi \otimes \lambda, \psi)$.

Remark 2. The ambiguity up to the sign is inevitable, because we have $\varepsilon(\pi \otimes \lambda, \psi) = -\varepsilon(\pi \otimes \nu_0 \otimes \lambda, \psi)$ for $\lambda \in \hat{k}^\times$, $f(\lambda) \leqq f_0$.

Remark 3. As an application, we can check the conjecture in finite steps when σ is given, because we have $\varepsilon(s, \pi \otimes \chi, \psi) = \varepsilon(s, \omega_\pi\chi, \psi)\varepsilon(s, \chi, \psi)$ when $f(\chi) \geqq f(\pi)$ if π is absolutely cuspidal and $\varepsilon(s, \sigma \otimes \chi, \psi) = \varepsilon(s, \omega\chi, \psi)\varepsilon(s, \chi, \psi)$ when $f(\chi) \geqq c$, where c is a constant which can be estimated explicitly when σ is given (cf. Deligne [3], p. 545–547).

§ 3. Partial results

To prove the conjecture, we may assume that σ factors through the natural map $W_k \to \mathrm{Gal}\,(K/k)$, where K is a finite Galois extension of k. Therefore we identify σ with a faithful irreducible representation $\mathrm{Gal}\,(K/k) \to GL_2(C)$.

Theorem 3. *We assume that* σ *is of tetrahedral type and* q *is an odd power of* 2. *Then* $\pi(\sigma)$ *exists.*

We shall indicate the outline of our proof. We may assume that the characteristic of k is 0 and the residual characteristic of k is 2. Let k_0 be the subfield of C generated by all the 2^n-th roots of unity ($n \in Z$, $n \geqq 1$). If not specified, we simply assume that σ is of tetrahedral type and do not assume that q is an odd power of 2.

Lemma 2. *There exists a finite Galois extension* K' *of* k, *a representation* σ' *of* $\mathrm{Gal}\,(K'/k)$ *in* $GL_2(C)$ *and a character* χ *of* $k^\times$ *such that* $(\sigma' \circ \pi') \otimes (\chi \circ T) = (\sigma \circ \pi)$ *and the character of* σ' *has values in* k_0, *where* π (*resp.* π') *is the natural map* $W_k \to \mathrm{Gal}\,(K/k)$ (*resp.* $W_k \to \mathrm{Gal}\,(K'/k)$) *and* T *is the transfer map* $W_k \to k^\times$.

By this lemma, we may assume that the character of σ is k_0-valued. Let L_1 be the subfield of K which corresponds to the center of $\mathrm{Gal}\,(K/k)$ and L be the subfield of L_1 which corresponds to the 2-Sylow subgroup of $\mathrm{Gal}\,(L_1/k) \cong A_4$. Put $\tilde{\sigma} = \sigma|\mathrm{Gal}\,(K/L)$. We see that $\tilde{\sigma}$ is irreducible and monomial. Hence there exists an absolutely cuspidal representation $\tilde{\pi} = \pi(\tilde{\sigma})$ of $GL_2(L)$. Let π be an irreducible admissible representation of $GL_2(k)$ which lifts to $\tilde{\pi}$ (π is written as $\pi_{\mathrm{pseudo}}(\sigma)$ in [9]. Our task is to show that $\pi_{\mathrm{pseudo}}(\sigma) = \pi(\sigma)$, if we choose π suitably.)

Lemma 3. *Let* $\mathrm{N}_{L/K}$ (*resp.* $\mathrm{Tr}_{L/K}$) *denote the norm* (*resp. the trace*) *map from* L *to* k. *We have* $\varepsilon(s, \tilde{\pi} \otimes \lambda \circ \mathrm{N}_{L/K}, \psi \circ \mathrm{Tr}_{L/K}) = \prod_\chi \varepsilon(s, \pi \otimes \lambda \otimes \chi, \psi)$ *for every quasicharacter* λ *of* $k^\times$, *where* χ *extends over all the characters of* $k^\times$ *which are trivial on* $\mathrm{N}_{L/K}(L^\times)$.

Proof. The representation $\pi \otimes \lambda$ lifts to $\tilde{\pi} \otimes \lambda \circ \mathrm{N}_{L/K}$. By this fact, we may assume that $\lambda = 1$. We can show, as a routine exercise, that there exists a finite Galois extension $\tilde{K}/\tilde{k}$ of algebraic number fields which satisfies the following conditions. (i) For an even place t of $\tilde{k}$ and a place u of $\tilde{K}$ lying above v, the localization $\tilde{K}_u/\tilde{k}_t$ is canonically isomorphic to K/k and $[\tilde{K}:\tilde{k}] = [K:k]$. (ii) Every even place $v(\neq t)$ splits completely in $\tilde{K}/\tilde{k}$. We define a representation $\tau = \sigma \circ \iota$ of $\mathrm{Gal}\,(\tilde{K}/\tilde{k})$, where ι is the isomorphism $\mathrm{Gal}\,(\tilde{K}/\tilde{k}) \xrightarrow{\sim} \mathrm{Gal}\,(K/k)$. Let $\tilde{L}$ be the subfield of K which corresponds to L under ι. Put $\tilde{\tau} = \tau|\mathrm{Gal}\,(\tilde{K}/\tilde{L})$. Because $\tilde{\tau}$ is monomial, the automorphic representation $\tilde{\phi} = \pi(\tilde{\tau})$ of $GL_2(\tilde{L}_A)$ exists. Let ϕ be an automorphic representation of $GL_2(\tilde{k}_A)$ which lifts to $\tilde{\phi}$. We may assume that $\phi_t = \pi$. We can see easily that $L(s, \tilde{\phi}) = \prod_{\tilde{\chi}} L(s, \phi \otimes \tilde{\chi})$, where $\tilde{\chi}$ extends over all the characters of $\tilde{k}_A^\times/\tilde{k}^\times$ which are trivial on $\mathrm{N}_{\tilde{L}_A/\tilde{k}_A}(\tilde{L}_A^\times/\tilde{L}^\times)$. Let $\tilde{\psi}$ be an additive character of $\tilde{k}_A/\tilde{k}$ such that

$\tilde{\psi}_t = \psi$. From the functional equations of $L(s, \tilde{\phi})$ and $L(s, \phi \otimes \tilde{\gamma})$, we have $\prod_{\tilde{\tau}} \prod_v \varepsilon_v(s, \phi_v \otimes \tilde{\gamma}_v, \tilde{\psi}_v) = \prod_w \varepsilon(s, \tilde{\phi}_w, (\psi \circ \mathrm{Tr}_{\tilde{L}_A/\tilde{k}_A})_w)$, where v (resp. w) extends over all the places of k (resp. L). If v is not even, we get $\prod_{\tilde{\tau}} \varepsilon(s, \phi_v \otimes \tilde{\gamma}_v, \tilde{\psi}_v) = \prod_w \varepsilon(s, \tilde{\phi}_w, (\psi \circ \mathrm{Tr}_{\tilde{L}_A/\tilde{k}_A})_w)$, where w extends over all the places of L which are above v (this is a consequence from Theorem A, [8]). From this, we can squeeze the desired relation $\varepsilon(s, \tilde{\pi}, \psi \circ \mathrm{Tr}_{L/k}) = \prod_\chi \varepsilon(s, \pi \otimes \chi, \psi)$.

Corollary. *If L/k is unramified, we have $\varepsilon(s, \pi \otimes \lambda, \psi)^3 = \varepsilon(s, \sigma \otimes \lambda, \psi)^3$ for every quasicharacter λ of $k^\times$.*

Lemma 4. *Assume that L/k is unramified and that $\varepsilon(\pi \otimes \lambda, \psi) = \varepsilon(\sigma \otimes \lambda, \psi)$ for every $\lambda \in \hat{k}^\times$ such that $\lambda(\varpi) = 1$. Then we have $\pi = \pi(\sigma)$.*

Proof. Form Cor., we have $f(\pi \otimes \lambda) = f(\sigma \otimes \lambda)$ for every quasicharacter λ of $k^\times$. Hence it is enough to prove $\omega = \omega_\pi$. This follows from the fact that $\varepsilon(\pi \otimes \lambda, \psi) = \varepsilon(\omega_\pi \lambda, \psi)\varepsilon(\lambda, \psi) = \varepsilon(\omega\lambda, \psi)\varepsilon(\lambda, \psi) = \varepsilon(\sigma \otimes \lambda, \psi)$ if $f(\lambda)$ is sufficiently large.

Remark 4. In the statement of the conjecture, the condition (iii) implies (i).

Let $\tilde{\pi}$ be as before. We identify $\tilde{\pi}$ with its Kirillov realization. For a character λ of $L^\times$, define an element $\xi_\lambda^{(n)}$ of $\mathscr{S}(L^\times)$ by (6). Let β be a generator of $\mathrm{Gal}(L/k)$. We can define an automorphism I_β of $\mathscr{S}(L^\times)$ by $I_\beta \xi_\lambda^{(n)} = \xi_{\lambda^\beta}^{(n)}$. Then we have $\tilde{\pi}(g^\beta) = I_\beta^{-1} \tilde{\pi}(g) I_\beta$. Let $\mathrm{Gal}(L/k) \times_s GL_2(L)$ be the semi-direct product defined using the natural injection $\mathrm{Gal}(L/k) \to \mathrm{Aut}(GL_2(L))$. Define a representation Π of $\mathrm{Gal}(L/k) \times_s GL_2(L)$ by $\Pi(\beta^i, g) = I_\beta^i \tilde{\pi}(g)$. Then by the definition of the lifting, we may assume that π satisfies the relation $\chi_\pi(\beta \times g) = \chi_\pi(h)$ if $Ng = g g^\beta g^{\beta^2}$ is conjugate to a regular semi-simple element h of $GL_2(k)$.

Lemma 5. *If h is a regular semi-simple element of $GL_2(k)$ we have $\chi_\pi(h)^\alpha = \chi_{\pi^\alpha}(h)$ for $\alpha \in \mathrm{Aut}(\boldsymbol{C})$.*

We can give a finite expression of $\chi_\pi(h)$ using the ε-function, and this formula proves Lemma 5. The computation is lengthy, so we omit the details.

Lemma 6. *Let k_1 be the subfield of $\boldsymbol{C}$ generated over $\boldsymbol{Q}$ by the values of all the characters of $O_L^\times$. If Ng is conjugate to a regular semi-simple element of $GL_2(k)$, $\chi_\Pi(\beta \times g)$ belongs to k_1.*

We can prove this lemma in a similar way as for Lemma 5.

Proof of Theorem 3. Let α be an element of $\mathrm{Aut}(\boldsymbol{C}/k_1)$. By Lemma 5 and 6, we have $\chi_\Pi(\beta \times g)^\alpha = \chi_\Pi(\beta \times g) = \chi_\pi(h)^\alpha = \chi_{\pi^\alpha}(h)$ if $Ng = g \cdot g^\beta \cdot g^{\beta^2}$ is conjugate to a regular semi-simple element h of $GL_2(k)$. This shows that π^α also lifts to $\tilde{\pi}$. Therefore we have $\pi^\alpha = \pi \otimes \chi$ where χ is a character of $k^\times$ which is trivial on $\mathrm{N}_{L/k}(L^\times)$. If $\chi = 1$ for every $\alpha \in \mathrm{Aut}(\boldsymbol{C}/k_1)$, we have $\varepsilon(\pi \otimes \lambda, \psi) \in k_1$ if λ is a character of $k^\times$ such that $\lambda(\varpi) = 1$. We also know that $\varepsilon(\sigma \otimes \lambda, \psi) \in k_1$ for such λ (cf. Dwork [4]). By Cor. of Lemma 3 and Lemma 4, we have $\pi = \pi(\sigma)$ because $e^{2\pi i/3} \notin k_1$. Therefore we may assume that there exists an automorphism $\alpha \in \mathrm{Aut}(\boldsymbol{C}/k_1)$ such that $\pi^\alpha = \pi \otimes \chi$ with $\chi \in \hat{k}^\times$ which is trivial on $\mathrm{N}_{L/k}(L^\times)$ and $\chi \neq 1$. Because $3 \nmid q - 1$, L/k is unramified and we see that $\chi | \mathfrak{O}_k^\times = id.$ and $\chi(\varpi) = \zeta$ where ζ is a primitive cubic root of unity. From $\varepsilon(\pi \otimes \lambda, \psi)^3 = \varepsilon(\sigma \otimes \lambda, \psi)^3$, we have $\varepsilon(\pi \otimes \lambda, \psi) = \zeta_\lambda \varepsilon(\sigma \otimes \lambda, \psi)$ where ζ_λ is a cubic root of unity. We assume that $\lambda \in \hat{k}^\times$ and $\lambda(\varpi) = 1$. We have $\varepsilon(\pi \otimes \lambda, \psi)^\alpha = \varepsilon(\pi^\alpha \otimes \lambda, \psi) = \varepsilon(\pi \otimes \lambda \otimes \chi, \psi) = \zeta^{-f} \varepsilon(\pi \otimes \lambda, \psi) = \zeta_\lambda^\alpha \varepsilon(\sigma \otimes \lambda, \psi)^\alpha = \zeta_\lambda^\alpha \varepsilon(\sigma \otimes \lambda, \psi)$ with $f = f(\pi \otimes \lambda)$. Therefore we get $\zeta_\lambda^\alpha / \zeta_\lambda = \zeta^{-f}$ with $f = f(\pi \otimes \lambda)$. If $f(\lambda) \geqq f(\pi)$, we have $f(\pi \otimes \lambda) = 2f(\lambda)$. Hence we see that $\zeta^\alpha = \zeta^2$ and $\zeta_\lambda^\alpha / \zeta_\lambda = \zeta_\lambda = \zeta^{-f}$. We get $\varepsilon(\pi \otimes \lambda \otimes \chi^{-1}, \psi) = \zeta^f \varepsilon(\pi \otimes \lambda, \psi) = \zeta^f \zeta_\lambda \varepsilon(\sigma \otimes \lambda, \psi) = \varepsilon(\sigma \otimes \lambda, \psi)$. This shows that $\pi(\sigma) = \pi \otimes \chi^{-1}$ and completes the proof.

§ 4. Artin L-functions

Let K/k be a finite Galois extension of algebraic number fields and σ a faithful 2-dimensional representation of $\mathrm{Gal}(K/k)$ of tetrahedral type. Let us define a cyclic cubic extension L of k in the exactly same manner as in § 3 and put $\tilde{\sigma} = \sigma | \mathrm{Gal}(K/L)$. Then the automorphic representation $\tilde{\pi} = \pi(\tilde{\sigma})$ of $GL_2(L_A)$ exists because $\tilde{\sigma}$ is irreducible and monomial. Let π be an automorphic representation of $GL_2(k_A)$ which lifts to $\tilde{\pi}$. Note that π is a constituent of the space of the cusp forms because $\tilde{\pi}$ is. We put the following hypothesis, which will be discussed at the end of this section.

(H) $\pi_v = \pi(\sigma_v) \otimes \chi_v$ if σ_v is reducible and v is a finite place of k, where χ_v is a character of $k_v^\times$ which is trivial on $N_{L_w/k_v}(L_w^\times)$ and w is a place of L lying above v.

We shall show that (H) implies the existence of the automorphic representation $\pi(\sigma)$ of $GL_2(k_A)$. By [9], we have $\pi_v = \pi(\sigma_v)$ when v is an infinite place. From (H), we have $(\omega_\pi)_v = (\omega_\sigma)_v \chi_v^2$ with $\omega_\sigma = \det \sigma$, considering the character induced on the center of $GL_2(k_v)$. Define a character η of $k_A^\times / k^\times$ by $\eta = \omega_\pi \omega_\sigma^{-1}$. We have $\eta_v^2 = \chi_v$ if σ_v is reducible and v is a finite place. Therefore $(\pi \otimes \eta^{-2})_v = \pi_v \otimes \chi_v^{-1} = \pi(\sigma_v)$ is σ_v is reducible and v is a finite place. Because η is trivial on $N_{L_A/k_A}(L_A^\times / L^\times)$, we have $(\pi \otimes \eta^{-2})_v = \pi(\sigma_v)$ if v is an infinite place. Let ω be a unitary character of $k_A^\times / k^\times$. It is easy to see that $L(s, \sigma \otimes \omega)$ does

not have a pole in the domain $\{s; Re(s) \leqq 0 \text{ or } Re(s) \geqq 1\}$ (cf. [15], p. 288). From this fact, we can see that $L(s, \sigma \otimes \omega)$ (which coincides with $L(s, \pi \otimes \omega)$ up to a finite number of Euler factors) is an entire function and the existence of $\pi(\sigma)$ follows.

If k is totally real and π corresponds to a holomorphic automorphic form (i.e. for every archimedean place v of k and place w of K which divides v, $K_w \cong \boldsymbol{C}$ and $\sigma_v \cong \chi_1 \oplus \chi_2$ where χ_1 (resp. χ_2) is the trivial (resp. non-trivial) representation of $\mathrm{Gal}(K_w/k_v) \cong \mathrm{Gal}(\boldsymbol{C}/\boldsymbol{R})$, then we can also argue in the following way, assuming (H). We may assume that the character of σ has its values in k_0, by a similar lemma as Lemma 2. Let α be an element of $\mathrm{Aut}(\boldsymbol{C}/k_0)$. By Prop. 4 of Shimura [11], we can see that there exists an automorphic representation π^α of $GL_2(k_A)$ which satisfies the following conditions. (i) $(\pi^\alpha)_v = \pi_v$ if v is an infinite place of k. (ii) For a set S of finite places of k which contains almost all places of k, $\pi_v = \pi(\mu_v, \delta_v)$ and $(\pi^\alpha)_v = \pi(\mu_v^\alpha, \delta_v^\alpha)$ if $v \in S$, where μ_v and δ_v are quasicharacters of $k_v^\times$. If $v \in S$ and w is a place of L which divides v, we have $\pi_v = \pi(\sigma_v) \otimes \chi_v$ from (H). We have $\pi_v^\alpha = \pi(\sigma_v)^\alpha \otimes \chi_v^\alpha = \pi(\sigma_v) \otimes \chi_v^\alpha$. We know that π^α also lifts to $\tilde{\pi}$ because $(\pi^\alpha)_v$ lifts $\tilde{\pi}_w$ at almost all places v of k. Therefore $\pi^\alpha = \pi \otimes \eta$ holds with a character η of $k_A^\times / k^\times$ which is trivial on $N_{L_A/k_A}(L_A^\times / L^\times)$. Hence we get $\chi_v^\alpha / \chi_v = \eta_v$ if $v \in S$. If $\chi_v^\alpha = \chi_v$ for every $\alpha \in \mathrm{Aut}(\boldsymbol{C}/k_0)$ and $v \in S$, we have $\chi_v = 1$ for every $v \in S$ and this is sufficient to obtain the conclusion. Assume that $\chi_v^\alpha \neq \chi_v$ for some $\alpha \in \mathrm{Aut}(\boldsymbol{C}/k_0)$ and $v \in S$. Then we have $\chi_v^\alpha / \chi_v = \chi_v = \eta_v$ for every $v \in S$. Therefore the automorphic representation $\pi \otimes \eta^{-1}$ of $GL_2(k_A)$ satisfies that $(\pi \otimes \eta^{-1})_v = \pi(\sigma_v)$ for almost all v. This shows $\pi(\sigma) = \pi \otimes \eta^{-1}$ as before.

Finally we observe that (H) is satisfied except for a set of places of k which has Kronecker density 0. Let U be the set of finite places of k which are unramified in K/k. We have $\pi_v = \pi(\mu_v, \delta_v)$ with characters μ_v and δ_v of $k_v^\times$ if $v \in U$. Let ϖ_v be a prime element of k_v. We assume that $v \in U$ remains prime in L. Then we can see easily that $|\mu_v(\varpi_v) + \delta_v(\varpi_v)| = 1$ if (H) is satisfied and $|\mu_v(\varpi_v) + \delta_v(\varpi_v)| = 2$ if (H) is not satisfied for v. Using Th. 19.14 of Jacquet [17] (see also Deligne-Serre [16], p. 519), we can see that

$$(*) \qquad \sum_{v \in U} |\mu_v(\varpi_v) + \delta_v(\varpi_v)|^2 Nv^{-s} = \log(1/s - 1) + 0(1) \qquad (s \to 1),$$

where Nv denotes the module of k_v. We have, by a standard argument, that

$$(**) \qquad \sum_{v \in U} |Trace(\sigma(F_v))|^2 Nv^{-s} = \log(1/s - 1) + 0(1) \qquad (s \to 1),$$

where F_v denotes the Frobenius conjugacy class of v. From $(*)$ and $(**)$, our observation follows immediately.

Note: § 4 was revised in March 1977. I would like to express my hearty thanks to Professor R. Langlands and his research fellow in IAS, who kindly let me be aware of a mistake.

References

[1] Casselman, W., The restriction of a representation of $GL_2(k)$ to $GL_2(\mathfrak{O})$, Math. Ann., **206** (1973), 311–318.
[2] ——, On representations of GL_2 and the arithmetic of modular curves, Modular Functions of One Variable II, 1972, 107–141, Lecture Notes in Math. **349**, Springer, Berlin 1973.
[3] Deligne, P., Les constantes des équations fonctionnelles des fonctions L. ibid., 501–597.
[4] Dwork. B., On the Artin root number, Amer. Jour. Math. **78** (1956), 444–472.
[5] Gelfand, I. M., and Kajdan, D. A., Representations of the group $GL(n,K)$ where K is a local field, Functional Anal. Appl. **6** (1972), 315–317.
[6] Godement, R., Notes on Jacquet-Langlands theory, Lecture note at Institute for advanced study, 1970.
[7] Jacquet, H., and Langlands, R. P., Automorphic forms on $GL(2)$, Lecture notes in Mathematics, **14**, Springer, 1970.
[8] Langlands, R. P., On the functional equations of the Artin L-functions, Yale university lecture note.
[9] ——, Base change for $GL(2)$, Lecture note at Institute for advanced study, 1975.
[10] Sally, P.J., and Shalika, J. A., Characters of the discrete series of representations of $SL(2)$ over a local field, P.N.A.S. **61** (1968), 1231-1237.
[11] Shimura, G., On some arithmetic properties of modular forms of one and several variables, Ann. of Math., **102** (1975), 491-515.
[12] Shintani, T., On liftings of holomorphic automorphic forms, U.S.-Japan seminar, Applications of automorphic forms to number theory, Ann Arbor. 1975.
[13] Weil, A., Sur la théorie du corps de classes, Jour. of Math. Soc. Japan Sec. IA, **3** (1951), 1–35.
[14] ——, Basic number theory, 2nd edition, Springer, Berlin, 1974.
[15] ——, Exercices dyadiques, Invent. Math. **27** (1974), 1–22.
[16] Deligne, P. and Serre, J. P., Formes modularies de poids 1, Ann. scient. Éc. Norm. Sup., *t.*7, 1974, 507–530.
[17] Jacquet, H., Automorphic forms on $GL(2)$, part II, Lecture notes in mathematics, 278, Springer, Berlin. 1972.

Department of Mathematics
Faculty of Science
Kyoto University
Kitashirakawa, Kyoto 606
Japan