J. Math. Soc. Japan
Vol. 20, Nos. 1-2, 1968

The congruence monodromy problems

Dedicated to Professor Shôkichi Iyanaga on his 60th birthday

By Yasutaka IHARA

(Received Aug. 31, 1967)

Introduction

This is a summary of the forthcoming lecture note [1]. All details and proofs of the theorems will be given in [1], and are omitted here.

§ 0-1. **The problems.** Let $G=\mathrm{PSL}_2(R)\times\mathrm{PSL}_2(k_\mathfrak{p})$, where R and $k_\mathfrak{p}$ are the real number field and a $\mathfrak{p}$-adic number field with $N\mathfrak{p}=q$ respectively, and $\mathrm{PSL}_2=\mathrm{SL}_2/\pm 1$. Let Γ be a torsion-free discrete subgroup of G with compact quotient, having a dense image of projection in each component of G. Our subject is such a discrete subgroup Γ. This study was motivated by the following series of conjectures which were suggested by our previous work [2]*. Since our group Γ is essentially nonabelian (see § 1-5, property (iv)), the readers will see that, by our conjectures, Γ would describe a "*non-abelian class field theory*" over an algebraic function field of one variable with finite constant field F_{q^2}. We would like to call the problems of determination of the validity of these conjectures, *the congruence monodromy problems.*

Conjectures**. With each Γ, we can associate an algebraic function field K of one variable with finite constant field F_{q^2} and with genus $g\geqq 2$, and a finite set $\mathfrak{S}(K)$ consisting of $(q-1)(g-1)$ prime divisors of K of degree one over F_{q^2}, satisfying the following properties. Here, the elements of $\mathfrak{S}(K)$ are called *the exceptional prime divisors,* while all other prime divisors of K are called *the ordinary prime divisors.*

CONJECTURE 1. *The ordinary prime divisors P of K are in one-to-one correspondence with the pairs $\{\gamma_P^{\pm 1}\}_\Gamma$ of mutually inverse primitive elliptic conjugacy classes of Γ* (see § 1 for the definitions).

CONJECTURE 2. *The finite unramified extensions K' of K, in which all $(q-1)(g-1)$ exceptional prime divisors of K are decomposed completely, are in*

* The proofs of results stated in [2] will also be given in [1]. There is some overlap between a part of § 2 of [2] and § 1 of this paper.

** See also § 3.

one-to-one correspondence with the subgroups Γ' of Γ with finite indices. Moreover, this one-to-one correspondence satisfies the Galois theory.

CONJECTURE 3. *The law of decomposition of ordinary prime divisors P of K in K' is described by the corresponding $\{\gamma_P^{\pm 1}\}_\Gamma$ and Γ'. Namely, decompose the Γ-conjugacy class $\{\gamma_P\}_\Gamma$ into a disjoint union of Γ'-conjugacy classes:*

$$\{\gamma_P\}_\Gamma = \{\gamma_{P,1}\}_{\Gamma'} \cup \cdots \cup \{\gamma_{P,t}\}_{\Gamma'},$$

and for each i, let f_i be the smallest positive integer such that $\gamma_{P,i}^{f_i}$ is contained in Γ'. Then we have $\sum_{i=1}^{t} f_i = (\Gamma : \Gamma')$, and our conjecture asserts that the decomposition of P in K' is of type:

$$P = P_1' P_2' \cdots P_t',$$

where P_i' $(1 \leqq i \leqq t)$ are prime divisors of K' with relative degrees f_i $(1 \leqq i \leqq t)$ respectively.

§ 0-2. Results. Now, our results, summarized in § 1 and § 2, are still far from the solution of the problems, but seem encouraging.

In § 1, we shall define *primitive elliptic conjugacy classes* P of Γ, their *degrees* $\deg P$, and the ζ *function* $\zeta_\Gamma(u) = \prod_P (1-u^{\deg P})^{-1}$, where P runs over the pairs of mutually inverse primitive elliptic conjugacy classes. Then, the result of the computation of $\zeta_\Gamma(u)$ is given in Theorem 1, which states that $\zeta_\Gamma(u)$ is a rational function of u of the form:

$$\zeta_\Gamma(u) = \frac{\prod_{i=1}^{g} (1-\alpha_i u)(1-\alpha_i' u)}{(1-u)(1-q^2 u)} \times (1-u)^{(q-1)(g-1)},$$

where $\alpha_i \alpha_i' = q^2$ for $1 \leqq i \leqq g$, and g $(\geqq 2)$ is the genus of a certain algebraic function field L_0 of one variable over the complex number field C. This agrees with conjecture 1, because if conjecture 1 is true, then $\zeta_\Gamma(u)$ must be of this form, with the first factor equal to the congruence ζ function of K over F_{q^2}.

Now, we expect that the questioned field K is obtained by some "reduction mod $\mathfrak{P}$" of the function field L_0 (the definition of L_0 is given in § 2-1), and so, our first problem is to lower the field of constants of L_0. However, we find that it is more essential to consider some infinite extension L of L_0 on which the group $G_\mathfrak{p} = \mathrm{PSL}_2(k_\mathfrak{p})$ acts as an automorphism group over C, and to lower the field of constants of L. Thus, in § 2-1, we shall define what we call *a $G_\mathfrak{p}$-field*. Roughly speaking, it is a field, one dimensional and infinitely generated over its *constant field*, on which the group $G_\mathfrak{p} = \mathrm{PSL}_2(k_\mathfrak{p})$ acts as an automorphism group. Then, we shall show that $G_\mathfrak{p}$-fields over the complex number field C are in one-to-one correspondence with the group Γ (Theorem 2).

Now, our main result is that a $G_{\mathfrak{p}}$-field over C is always the constant field extension of some $G_{\mathfrak{p}}$-field over an algebraic number field of finite degree, and that if the former is irreducible (see § 2-2), then *the latter is essentially unique* (Theorem 4). Thus, it seems that our problems are reduced to some "arithmetic theory" of $G_{\mathfrak{p}}$-fields over algebraic number fields.

In § 3, our conjectures are repeated a little more precisely, and in § 4-1, some examples of Γ, which are obtained from certain quaternion algebra, are given. For these Γ, the fields L_0 belong to those classes of function fields which have been studied in detail by G. Shimura [3], but even in these cases neither of our conjectures have been proved*. The only example for which our conjectures are partly proved is given in § 4-2.

The author would like to express his hearty thanks particularly to Professor G. Shimura, and to Professors A. Weil and R. P. Langlands, for their interest in this subject and valuable discussions with the author during his stay in Princeton in 1965-1967.

Throughout the following, for any element γ of any group Γ, $\{\gamma\}_\Gamma$ will denote the conjugacy class of Γ containing γ.

§ 1. Group Γ and its ζ function

§ 1-1. Let R be the field of real numbers, and put $G_R=\mathrm{PSL}_2(R)=\mathrm{SL}_2(R)/\pm 1$. Let, on the other hand, $k_{\mathfrak{p}}$ be a $\mathfrak{p}$-adic number field with the ring of integers $\mathfrak{o}_{\mathfrak{p}}$ and the maximal ideal $\mathfrak{p}$ of $\mathfrak{o}_{\mathfrak{p}}$ with $N\mathfrak{p}=q$, and put $G_{\mathfrak{p}}=\mathrm{PSL}_2(k_{\mathfrak{p}})=\mathrm{SL}_2(k_{\mathfrak{p}})/\pm 1$. We form the direct product $G=G_R\times G_{\mathfrak{p}}$, and consider it as a topological group in a natural manner. For any subset S of G, we denote by S_R resp. $S_{\mathfrak{p}}$ the images of the set-theoretical projections of S to G_R resp. $G_{\mathfrak{p}}$. Thus in particular, for any element x of G, x_R resp. $x_{\mathfrak{p}}$ are the real resp. $\mathfrak{p}$-adic components of x; $x=x_R\times x_{\mathfrak{p}}$.

Now, let Γ be a subgroup of G satisfying the following conditions.

(Γ1) *The projection maps $\Gamma\to\Gamma_R$, $\Gamma\to\Gamma_{\mathfrak{p}}$ are injective, and the images Γ_R, $\Gamma_{\mathfrak{p}}$ are dense in G_R, $G_{\mathfrak{p}}$ respectively.*

(Γ2) *Γ is discrete in G, and the quotient G/Γ is compact.*

Actually, these conditions are not independent; in fact by the simplicity of the groups G_R, $G_{\mathfrak{p}}$, we can show easily that the injectivities of the projection maps $\Gamma\to\Gamma_R$, $\Gamma\to\Gamma_{\mathfrak{p}}$ are the consequences of the rest of the conditions in (Γ1) and (Γ2). By this remark, it becomes clear that if Γ is a subgroup of G satisfying (Γ1) and (Γ2), then subgroups Γ' of G which are commensurable with

* But we get some useful informations from his results [3], which are very encouraging. See § 4-1.

Γ also satisfy (Γ1) and (Γ2).

Put

$$U_\mathfrak{p} = \mathrm{PSL}_2(\mathfrak{o}_\mathfrak{p}) = \mathrm{SL}_2(\mathfrak{o}_\mathfrak{p})/\pm 1\,,$$

$$\Gamma^0 = \Gamma \cap (G_R \times U_\mathfrak{p})\,,$$

and let Γ_R^0 be the projection of Γ^0 to G_R.
Then, under (Γ1), the condition (Γ2) is equivalent to the following:

(Γ2′) *Γ_R^0 is discrete in G_R and the quotient G_R/Γ_R^0 is compact.*

Moreover, for the sake of simplicity, we assume throughout § 1 that:

(Γ3) *Γ is torsion-free; i.e., Γ has no elements of finite order other than the identity element I.*

It can be shown that a subgroup Γ of G satisfying (Γ1) and (Γ2) contains a subgroup with finite index which is torsion-free (cf. [**1**]).

§ 1-2. Now, the group $G_R = \mathrm{PSL}_2(R)$ acts on the complex upper half plane $\mathfrak{h} = \{z \in C \mid \mathrm{Im}\, z > 0\}$ as:

$$G_R \ni g_R = \pm\begin{pmatrix} a & b \\ c & d \end{pmatrix}: \quad \mathfrak{h} \ni z \longrightarrow g_R \cdot z = \frac{az+b}{cz+d} \in \mathfrak{h}\,.$$

For each $z \in \mathfrak{h}$, put

$$\Gamma_z = \{\gamma \in \Gamma \mid \gamma_R \cdot z = z\}\,.$$

PROPOSITION. *If $z \in \mathfrak{h}$ is such that $\Gamma_z \neq \{I\}$, then Γ_z is an infinite cyclic group. Moreover, if $\gamma \in \Gamma_z$, $\gamma \neq I$, and if $\pm\{\lambda_\mathfrak{p}, \lambda_\mathfrak{p}^{-1}\}$ are the eigenvalues of $\gamma_\mathfrak{p} \in G_\mathfrak{p} = \mathrm{PSL}_2(k_\mathfrak{p})$, then $\lambda_\mathfrak{p}$, $\lambda_\mathfrak{p}^{-1}$ belong to $k_\mathfrak{p}$, and do not belong to the group of $\mathfrak{p}$-adic units $\mathfrak{o}_\mathfrak{p}^\times$. In particular, they are distinct.*

In fact, put $G_{z,R} = \{g_R \in G_R \mid g_R \cdot z = z\}$. Then, $G_{z,R}$ is isomorphic to the one-dimensional real torus group T, and hence is abelian. Now we have $(\Gamma_z)_R \cong \Gamma_z \cong (\Gamma_z)_\mathfrak{p}$ canonically, and since $\Gamma_z \neq \{I\}$ and Γ_z is torsion-free, it is infinite. So, $(\Gamma_z)_R$ is an infinite subgroup of $G_{z,R} \cong T$, and hence is abelian (and dense in $G_{z,R}$). But Γ_z, as a subgroup of Γ, must be discrete in G, and so (since $(\Gamma_z)_R$ is dense in the compact subgroup $G_{z,R}$ of G_R), $(\Gamma_z)_\mathfrak{p}$ must be discrete in $G_\mathfrak{p}$. Therefore, $(\Gamma_z)_\mathfrak{p}$ is a torsion-free, discrete abelian subgroup of $G_\mathfrak{p}$. Now our proposition follows easily from this. q. e. d.

We shall call an element γ ($\neq I$) of Γ *elliptic* if it is contained in Γ_z for some $z \in \mathfrak{h}$. So, $\gamma \in \Gamma$ is elliptic if and only if γ_R has imaginary eigenvalues, and for such γ, the point $z \in \mathfrak{h}$ such that $\gamma \in \Gamma_z$ is unique. So, we may denote such γ also by $\gamma = \gamma_z$. Since the ellipticity remains unchanged by taking Γ-conjugate elements, we shall call the Γ-conjugacy class $\{\gamma\}_\Gamma$ containing γ *elliptic* if γ is so. For any elliptic Γ-conjugacy class $\{\gamma\}_\Gamma$, we shall define its *degree*, $\deg\{\gamma\}_\Gamma$, by

$$\deg\{\gamma\}_\Gamma = |V_\mathfrak{p}(\lambda_\mathfrak{p})|,$$

where $\pm\{\lambda_\mathfrak{p}, \lambda_\mathfrak{p}^{-1}\}$ are the eigenvalues of $\gamma_\mathfrak{p}$, and $V_\mathfrak{p}$ is the normalized additive valuation of $k_\mathfrak{p}$. Since $\lambda_\mathfrak{p} \notin \mathfrak{o}_\mathfrak{p}^\times$, $\deg\{\gamma\}_\Gamma$ is a positive integer, and it is clear that for any integer r, we have $\deg\{\gamma^r\}_\Gamma = |r|\deg\{\gamma\}_\Gamma$. The following lemma makes clear the relation between $\deg\{\gamma\}_\Gamma$ and the elementary divisors of $\gamma_\mathfrak{p}$. It is well-known in elementary divisor theory that for any $x_\mathfrak{p} \in G_\mathfrak{p}$, there exist $u_\mathfrak{p}, u'_\mathfrak{p} \in U_\mathfrak{p} = \mathrm{PSL}_2(\mathfrak{o}_\mathfrak{p})$ such that $u_\mathfrak{p} x_\mathfrak{p} u'_\mathfrak{p}$ is of the form $\pm\begin{pmatrix}\alpha_\mathfrak{p} & 0\\ 0 & \alpha_\mathfrak{p}^{-1}\end{pmatrix}$ with some $\alpha_\mathfrak{p} \in k_\mathfrak{p}$, and that $l(x_\mathfrak{p}) = |V_\mathfrak{p}(\alpha_\mathfrak{p})|$ depends only on $x_\mathfrak{p}$, and not on the special choice of $u_\mathfrak{p}, u'_\mathfrak{p} \in U_\mathfrak{p}$.

LEMMA. *Let $\{\gamma\}_\Gamma$ be an elliptic Γ-conjugacy class. Then, we have*

$$\deg\{\gamma\}_\Gamma = \operatorname*{Min}_{\delta\in\Gamma} l((\delta^{-1}\gamma\delta)_\mathfrak{p}) = \operatorname*{Min}_{x_\mathfrak{p}\in G_\mathfrak{p}} l(x_\mathfrak{p}^{-1}\gamma_\mathfrak{p}x_\mathfrak{p}).$$

§ 1-3. Consider all points $z \in \mathfrak{h}$ such that $\Gamma_z \neq \{I\}$. Such points will be called *Γ-fixed points*. Two Γ-fixed points z, z' will be called *Γ-equivalent* if there exists $\gamma \in \Gamma$ such that $z' = \gamma_R \cdot z$. We shall denote by $\mathfrak{P}(\Gamma)$ the totality of all Γ-equivalence classes of all Γ-fixed points. Then, it is clear that $\mathfrak{P}(\Gamma)$ can be identified with the totality of all Γ-conjugacy classes of all subgroups Γ_z, where z runs over all Γ-fixed points. We shall call an elliptic element $\gamma = \gamma_z$ *primitive* if it generates Γ_z. Being primitive or not also remains unchanged by taking Γ-conjugate elements, and so we shall call $\{\gamma\}_\Gamma$ *primitive* if γ is so.

PROPOSITION. *Let $\{\gamma\}_\Gamma$ be an elliptic Γ-conjugacy class. Then, $\{\gamma^{-1}\}_\Gamma \neq \{\gamma\}_\Gamma$.*

In fact, it is enough to show that γ_R^{-1} and γ_R are not conjugate in $G_R = \mathrm{PSL}_2(R)$. Suppose, on the contrary, that we had $\gamma_R^{-1} = g_R^{-1}\gamma_R g_R$ with $g_R \in G_R$. Then, if z is the fixed point of γ_R, $g_R^{-1}z$ is also fixed by γ_R; hence $g_R^{-1}z = z$, and hence g_R^{-1} commutes with γ_R. So, we get $\gamma_R^{-1} = \gamma_R$, which is impossible since Γ is torsion-free. q. e. d.

So, there is a natural one-to-two correspondence between $\mathfrak{P}(\Gamma)$ and the set of all primitive elliptic Γ-conjugacy classes:

$$\mathfrak{P}(\Gamma) \ni \{\Gamma_z\}_\Gamma \longleftrightarrow \{\gamma_z\}_\Gamma, \{\gamma_z^{-1}\}_\Gamma.$$

Finally, for each $P \in \mathfrak{P}(\Gamma)$, we put

$$\deg P = \deg\{\gamma\}_\Gamma = \deg\{\gamma^{-1}\}_\Gamma,$$

where $\{\gamma^{\pm 1}\}_\Gamma$ are the primitive elliptic Γ-conjugacy classes which correspond to P.

§ 1-4. Now we shall define the ζ function $\zeta_\Gamma(u)$ of Γ by

$$\zeta_\Gamma(u) = \prod_{P\in\mathfrak{P}(\Gamma)} (1-u^{\deg P})^{-1},$$

or, equivalently, by:

$$\begin{cases} \zeta_\Gamma(0)=1 \\ \log \zeta_\Gamma(u)=\sum_{m=1}^{\infty} N_m u^m/m\,, \end{cases}$$

with

$$N_m=\sum_{\substack{P\in\mathfrak{P}(\Gamma)\\ \deg P\mid m}} \deg P \qquad (m\geqq 1)\,.$$

Then, we can prove that N_m are finite, and after some lengthy computation, we get the following result.

THEOREM 1. *Our ζ function $\zeta_\Gamma(u)$ is a rational function of u of the form:*

$$\zeta_\Gamma(u)=\frac{Q(u)}{(1-u)(1-q^2u)}\times(1-u)^{(q-1)(g-1)}\,,$$

where $q=N\mathfrak{p}$, g is the genus of the Riemann surface $\mathfrak{h}/\Gamma_R^0$, and $Q(u)$ is a polynomial of u of degree $2g$ with rational integral coefficients and with $Q(0)=1$, satisfying the functional equation

$$(qu)^{2g}Q(q^{-2}u^{-1})=Q(u)\,;$$

or equivalently, $Q(u)$ is of the form:

$$Q(u)=\prod_{i=1}^{g}(1-\alpha_i u)(1-\alpha_i' u), \quad \textit{with} \quad \alpha_i\alpha_i'=q^2 \ (1\leqq i\leqq g)\,.$$

We also have an inequality:

$$|\alpha_i|,\ |\alpha_i'|\leqq q^2, \qquad \alpha_i,\ \alpha_i'\neq 1,\ q^2 \qquad (1\leqq i\leqq g)\,.$$

As for the proof, and for more explicit determination of $Q(u)$, cf. [1].

REMARK. If we do not assume (Γ3), then we must modify the definitions of $\mathfrak{P}(\Gamma)$, $\zeta_\Gamma(u)$, etc. But under a suitable modification, our Theorem 1 holds also for such general case.

§1-5. *Some properties of Γ.* Here, we shall state, without proof, some simple properties of the group Γ satisfying (Γ1) and (Γ2). As for the proof, cf. [1].

(i). Γ is finitely generated and defined by a finite number of relations.

(ii). Γ is residually finite, i.e., the intersection of all subgroups of Γ with finite indices is $\{I\}$.

(iii). Γ contains a subgroup Γ' with finite index which is torsion-free.

(iv). The commutator subgroup $[\Gamma,\Gamma]$ of Γ is of finite index in Γ, and if Γ is torsion-free, then the group index $(\Gamma:[\Gamma,\Gamma])$ is a divisor of $Q(1)^2$, where $Q(u)$ is the numerator of the main factor of $\zeta_\Gamma(u)$ (see Theorem 1).

(v). Γ has no non-trivial deformation in G.

§ 2. Analytic theory of $\mathrm{PSL}_2(k_\mathfrak{p})$-fields

Throughout § 2, Γ is a subgroup of $G=G_R\times G_\mathfrak{p}$ satisfying (Γ1) and (Γ2), and Q resp. C are the fields of rational numbers resp. complex numbers.

§ 2-1. As before, let $U_\mathfrak{p}=\mathrm{PSL}_2(\mathfrak{o}_\mathfrak{p})$, and put

$$U_\mathfrak{p}^0=U_\mathfrak{p},\qquad U_\mathfrak{p}^n=\{x\in \mathrm{SL}_2(\mathfrak{o}_\mathfrak{p})\mid x\equiv \pm 1(\mathrm{mod}\,\mathfrak{p}^n)\}/\pm 1\qquad (n\geqq 1).$$

So we have a descending sequence $U_\mathfrak{p}^0\supset U_\mathfrak{p}^1\supset\cdots$ of open compact subgroups of $G_\mathfrak{p}$ satisfying $\bigcap_{n=0}^{\infty} U_\mathfrak{p}^n=\{I\}$. Put

$$\Gamma^n=\Gamma\cap(G_R\times U_\mathfrak{p}^n)\qquad (n\geqq 0).$$

Remark that Γ^0 agrees with the previously defined one. So, we have a descending sequence $\Gamma_R^0\supset\Gamma_R^1\supset\cdots$ of discrete subgroups of G_R with compact quotients, where each $\Gamma_R^n=(\Gamma^n)_R$ is a normal subgroup of Γ_R^0 with finite index, and $\bigcap_{n=0}^{\infty}\Gamma_R^n=\{I\}$. Now, let L_n ($n\geqq 0$) be the field of automorphic functions with respect to Γ_R^n, i.e., L_n is the field of all meromorphic functions $f(z)$ on the complex upper half plane $\mathfrak{h}$ which are invariant by the action of Γ_R^n on $\mathfrak{h}$. So, we have an increasing sequence $L_0\subset L_1\subset\cdots$ of algebraic function fields of one variable over the complex number field C, where each L_n is a finite Galois extension of L_0. We remark that we can take $n_0\geqq 0$ such that $U_\mathfrak{p}^{n_0}$ (and hence *a priori* $\Gamma_R^{n_0}$) is torsion-free. So, for such n_0 and for any $n\geqq n_0$, the extension L_n/L_{n_0} is unramified.

Now, put $L=\bigcup_{n=0}^{\infty}L_n$. Then $G_\mathfrak{p}$ acts effectively on L as a group of automorphisms* of L over C in the following manner. Let $g_\mathfrak{p}\in G_\mathfrak{p}$ and $f(z)\in L$. Take any $n\geqq 0$ such that $f(z)\in L_n$, and take any $\gamma\in\Gamma\cap(G_R\times U_\mathfrak{p}^n g_\mathfrak{p}^{-1})$ ($\neq\phi$, since $\Gamma_\mathfrak{p}$ is dense in $G_\mathfrak{p}$ by (Γ1)). Then, $f(\gamma_R\cdot z)$ depends only on $f(z)$ and $g_\mathfrak{p}$, and does not depend on the choices of n and γ. So, put $g_\mathfrak{p}(f(z))=f(\gamma_R\cdot z)$. Then, it can be checked immediately that for given $g_\mathfrak{p}$, the map $L\ni f(z)\to g_\mathfrak{p}(f(z))\in L$ is an automorphism of L over C, that $g_\mathfrak{p}(h_\mathfrak{p}(f(z)))=(g_\mathfrak{p}h_\mathfrak{p})f(z)$ holds for any $g_\mathfrak{p}$, $h_\mathfrak{p}\in G_\mathfrak{p}$ and $f(z)\in L$; and that this action of $G_\mathfrak{p}$ on L is effective. Moreover, it is clear that for each $n\geqq 0$, $U_\mathfrak{p}^n$ acts trivially on L_n, that $U_\mathfrak{p}^n$ is the group of *all* automorphisms of L over L_n, and that the only $G_\mathfrak{p}$-fixed elements of L are elements of C.

In general, let k be a field, and let L be the union of an increasing sequence $L_0\subset L_1\subset\cdots\subset L_n\subset\cdots$ of algebraic function fields of one variable** with the

---

* By this, we do *not* mean that $G_\mathfrak{p}$ is the group of *all* automorphisms of L over C.

** By this, we mean that each L_n is a regular extension of k (i.e., L_n is finitely and separably generated over k, and k is algebraically closed in L_n), and $\dim_k L_n=1$.

common constant field k, satisfying the following.

($L1$) *There exists* $n_0 \geqq 0$ *such that for any* $n \geqq n_0$, L_n *is unramified over* L_{n_0}.

($L2$) *The group* $G_\mathfrak{p} = \mathrm{PSL}_2(k_\mathfrak{p})$ *acts effectively on* L *as a group of automorphisms of* L *over* k *in such a way that the Galois theory holds between* L_n *and* $U_\mathfrak{p}^n$ *for each* $n \geqq 0$; *namely,* $U_\mathfrak{p}^n$ *acts trivially on* L_n, *and* $U_\mathfrak{p}^n$ *is the group of all automorphisms of* L *over* L_n. *Moreover, we assume that the only* $G_\mathfrak{p}$*-fixed elements of* L *are elements of* k.

Here too, we do not mean that $G_\mathfrak{p}$ is the group of *all* automorphisms of L over k.

Now, such a pair $\{L/k, G_\mathfrak{p}\}$ satisfying ($L1$) and ($L2$) will be called simply *a* $G_\mathfrak{p}$*-field over* k. Two such $\{L/k, G_\mathfrak{p}\}$ and $\{L'/k, G_\mathfrak{p}\}$, with the common k and $G_\mathfrak{p}$, are called *isomorphic* if there exists an isomorphism of L onto L' over k that commutes with the action of $G_\mathfrak{p}$.

We have shown that if Γ is given, then we can construct $\{L/C, G_\mathfrak{p}\}$, a $G_\mathfrak{p}$-field over the complex number field C. Conversely, we can show that given any $\{L/C, G_\mathfrak{p}\}$, a subgroup Γ of $G = G_R \times G_\mathfrak{p}$ satisfying ($\Gamma 1$) and ($\Gamma 2$) is defined; and that in this manner subgroups Γ of G satisfying ($\Gamma 1$) and ($\Gamma 2$) are in one-to-one correspondence with all $\{L/C, G_\mathfrak{p}\}$, where Γ are considered up to conjugacy in G, and $\{L/C, G_\mathfrak{p}\}$, up to isomorphisms. Let us sketch the proof. Given $\{L/C, G_\mathfrak{p}\}$, consider the set Σ of all non-equivalent places of L over C. Then Σ carries a natural complex structure, by which Σ is a one dimensional complex manifold, each connected component of which is isomorphic to the complex upper half plane* $\mathfrak{h}$. The group $G_\mathfrak{p}$ acts effectively on Σ as a group of automorphisms in a natural manner, and hence acts as a permutation group on the set of all connected components of Σ. Moreover, for each $n \geqq 0$, $U_\mathfrak{p}^n$ acts transitively on the set of all connected components of Σ, and hence if we take any connected component Σ_0 of Σ and put

$$\Gamma_\mathfrak{p} = \{g_\mathfrak{p} \in G_\mathfrak{p} \mid g_\mathfrak{p} \cdot \Sigma_0 = \Sigma_0\}^{**},$$

then $\Gamma_\mathfrak{p}$ is a *dense* subgroup of $G_\mathfrak{p}$. On the other hand, $\Gamma_\mathfrak{p}$ acts on $\Sigma_0 \cong \mathfrak{h}$ as a group of automorphisms, and hence can be identified with a subgroup Γ_R of $G_R = \mathrm{PSL}_2(R) \cong$ the automorphism group of $\mathfrak{h}$. Let Γ be the subgroup of $G = G_R \times G_\mathfrak{p}$ formed of all $\gamma_R \times \gamma_\mathfrak{p}$, where γ_R, $\gamma_\mathfrak{p}$ are corresponding elements of Γ_R, $\Gamma_\mathfrak{p}$ respectively. Then, we can show that Γ satisfies ($\Gamma 1$) and ($\Gamma 2$), and that this process of obtaining Γ from $\{L/C, G_\mathfrak{p}\}$ is the inverse of the process of construction of $\{L/C, G_\mathfrak{p}\}$ from Γ described at the beginning of § 2. We sum-

* It is easy to see that each connected component of Σ is isomorphic to $\mathfrak{h}/\Delta$, with some discrete subgroup Δ of G_R; but it is less trivial to show that $\Delta = \{I\}$.

** So, there are as many connected components of Σ as $G_\mathfrak{p}/\Gamma_\mathfrak{p}$. Its cardinal number is $\aleph$-infinity.

marize it in the following theorem.

THEOREM 2. *Subgroups Γ of $G=G_R\times G_\mathfrak{p}$ satisfying (Γ1) and (Γ2) are in one-to-one correspondence with $G_\mathfrak{p}$-fields L over C.*

§2-2. Now let us fix Γ and the corresponding $\{L/C, G_\mathfrak{p}\}$. Then, if Δ is a subgroup of G containing Γ as a subgroup of finite index, and if $\{M/C, G_\mathfrak{p}\}$ is the $G_\mathfrak{p}$-field which corresponds to Δ, then we can regard M as a $G_\mathfrak{p}$-invariant subfield of L containing C, where the action of $G_\mathfrak{p}$ on M coincides with the restriction to M of the action of $G_\mathfrak{p}$ on L. We also have $[L:M]=(\Delta:\Gamma)<\infty$. Conversely, if M is any $G_\mathfrak{p}$-invariant subfield of L such that $M\supsetneqq C$, then we can show easily that $[L:M]<\infty$ and that $\{M/C, G_\mathfrak{p}\}$ is a $G_\mathfrak{p}$-field obtained from some $\Delta\supset\Gamma$ with $(\Delta:\Gamma)=[L:M]<\infty$. So, we have:

PROPOSITION. *Given Γ and the corresponding $\{L/C, G_\mathfrak{p}\}$, subgroups $\Delta\supset\Gamma$ of G with $(\Delta:\Gamma)<\infty$ and $G_\mathfrak{p}$-invariant subfields M of L with $M\supsetneqq C$ correspond in a one-to-one manner.*

We shall call Γ *maximal* if there is no such Δ other than Γ itself, and $\{L/C, G_\mathfrak{p}\}$ *irreducible* if there is no such M other than L itself. So if Γ corresponds to $\{L/C, G_\mathfrak{p}\}$, then,

$\{L/C, G_\mathfrak{p}\}$ is irreducible if and only if Γ is maximal.

We remark that any Γ is contained in a maximal one*. In fact, if $\Delta\supset\Gamma$ and $(\Delta:\Gamma)<\infty$, then, since $\Gamma_\mathfrak{p}$ is dense in $G_\mathfrak{p}$ we have $\Delta_\mathfrak{p}=\Delta^n\cdot\Gamma_\mathfrak{p}$ for any $n\geqq 0$, and hence $(\Delta:\Gamma)=(\Delta_R^n:\Gamma_R^n)$ for any $n\geqq 0$. But Γ_R^0 is a discrete subgroup of G_R with compact quotient, and hence $(\Delta_R^0:\Gamma_R^0)$, and hence also $(\Delta:\Gamma)$, is bounded. This also shows that if Γ_R^0 is a maximal Fuchsian group, then Γ itself is maximal.

§2-3. Let $\{L/C, G_\mathfrak{p}\}$ be any $G_\mathfrak{p}$-field over C, and let $\mathrm{Aut}(L/C)$ be the group of *all* automorphisms of the field L which are trivial on C. Then, by the definition of $\{L/C, G_\mathfrak{p}\}$, the group $G_\mathfrak{p}$ is contained in $\mathrm{Aut}(L/C)$, but may not coincide with the whole group $\mathrm{Aut}(L/C)$. The following theorem is basic for our later studies (as for the proof, cf. [1]).

THEOREM 3. *The group $G_\mathfrak{p}$ is a characteristic subgroup of $\mathrm{Aut}(L/C)$ with finite index.*

Here, the essential point is the finiteness of the group index $(\mathrm{Aut}(L/C):G_\mathfrak{p})$; that $G_\mathfrak{p}$ is a characteristic subgroup follows immediately from this and from the simplicity of the group $G_\mathfrak{p}=\mathrm{PSL}_2(k_\mathfrak{p})$.

COROLLARY. *The centralizer Z of $G_\mathfrak{p}$ in $\mathrm{Aut}(L/C)$ is finite. If, moreover, $\{L/C, G_\mathfrak{p}\}$ is irreducible, then $Z=\{I\}$.*

---

* Actually, we can prove moreover that for given Γ, there are at most finitely many Δ. So, for given $\{L/C, G_\mathfrak{p}\}$, the number of M is also finite.

In fact, $Z \cap G_\mathfrak{p}$ is contained in the center of $G_\mathfrak{p}$, and hence is trivial; and since $(\mathrm{Aut}(L/C) : G_\mathfrak{p}) < \infty$, Z is finite. So, let M be the subfield of L corresponding to the finite automorphism group Z. Then M is $G_\mathfrak{p}$-invariant, and obviously $M \supsetneq C$. So, if $\{L/C, G_\mathfrak{p}\}$ is irreducible, we get $M = L$, and hence $Z = \{I\}$.

§ 2-4. Let $\{L/C, G_\mathfrak{p}\}$ be a $G_\mathfrak{p}$-field over C. A subfield L_k of L is called *a good subfield* of $\{L/C, G_\mathfrak{p}\}$ over $k = L_k \cap C$ if L_k is $G_\mathfrak{p}$-invariant and if $L_k \cdot C = L$. In this situation, it follows easily that L_k and C must be linearly disjoint over k. If L_k is a good subfield of $\{L/C, G_\mathfrak{p}\}$ over k, then it follows easily that $\{L_k/k, G_\mathfrak{p}\}$ is also a $G_\mathfrak{p}$-field over k; and for any k' with $k \subset k' \subset C$, the composite $L_{k'} = L_k \cdot k'$ is a good subfield of $\{L/C, G_\mathfrak{p}\}$ over k'. Now our main theorem of § 2 runs as follows.

THEOREM 4. *Let $\{L/C, G_\mathfrak{p}\}$ be a $G_\mathfrak{p}$-field over C. Then, there exists an algebraic number field k of finite degree over Q and a good subfield L_k of $\{L/C, G_\mathfrak{p}\}$ over k. If, moreover, the centralizer Z of $G_\mathfrak{p}$ in $\mathrm{Aut}(L/C)$ is trivial, then good subfields of $\{L/C, G_\mathfrak{p}\}$ are essentially unique; namely, there exists a good subfield L_{k_0} over an algebraic number field k_0 of finite degree, such that all other good subfields are those obtained by the composite $L_{k_0} \cdot k$ of L_{k_0} and fields k with $k_0 \subset k \subset C$. (On the other hand, if $Z \neq \{I\}$, then good subfields are not essentially unique.)*

As for the proof, cf. [1]. Unfortunately, it is too lengthy to be reproduced here. It is based on property (v) of § 1-5, Theorems 2 and 3, and on some group theoretical properties of $G_\mathfrak{p}$.

By this, and by the corollary of Theorem 3, we get:

COROLLARY 1. *If $\{L/C, G_\mathfrak{p}\}$ is irreducible, then it has an essentially unique good subfield L_{k_0} over an algebraic number field k_0 of finite degree.*

In short, any $G_\mathfrak{p}$-field over the complex number field C is the constant field extension of some $G_\mathfrak{p}$-field over an algebraic number field; and if the former is irreducible, then it is (essentially) uniquely so. It is a fundamental open problem to determine the relation between this k_0 and $k_\mathfrak{p}$.

So far, we defined good subfields L_k over k to be $G_\mathfrak{p}$-invariant subfields of L satisfying $L_k \cdot C = L$, $L_k \cap C = k$, and looked for "smallest possible" good subfields. However, we can impose stronger conditions on the definition of good subfields; for example, instead of $G_\mathfrak{p}$-invariance, we can impose $\mathrm{Aut}(L/C)$-invariance. With this definition, Theorem 4 is also valid, and the condition of the triviality of the centralizer of $G_\mathfrak{p}$ in $\mathrm{Aut}(L/C)$ can be replaced by the triviality of the center of $\mathrm{Aut}(L/C)$; and thus we get the essential uniqueness of good subfields for a wider class of $\{L/C, G_\mathfrak{p}\}$.

Finally, let $\bar{Q}$ be the algebraic closure of the field of rational numbers Q, and let k' be any field with $\bar{Q} \subset k' \subset C$. Let $\{L/C, G_\mathfrak{p}\}$ be any $G_\mathfrak{p}$-field over C.

So, L can be considered as defined from Γ as in § 2-1. Let the definition of good subfields be either of the above defined ones. Then, by Theorem 1, there is a good subfield L_k over an algebraic number field k, and hence there is a good subfield $L_{k'}=L_k\cdot k'$ over k'. On the other hand, we can show easily that if $L_{k'}$ is *any* good subfield of $\{L/C, G_\mathfrak{p}\}$ over k' with $\bar{Q}\subset k'\subset C$, then $L_{k'}$ consists of all $f(z)\in L$ such that the values of f at all Γ-fixed points are contained in $k'\cup\{\infty\}$. So, we get:

COROLLARY 2. *If $\bar{Q}\subset k'\subset C$, then there is a unique good subfield $L_{k'}$ of $\{L/C, G_\mathfrak{p}\}$ over k'. It consists of all $f(z)\in L$ whose values at all Γ-fixed points are contained in $k'\cup\{\infty\}$. (So, of course, $L_{k'}=L_{\bar{Q}}\cdot k'$.)*

§ 3. Conjectures (The congruence monodromy problems)

§ 3-1. Now, we are in the situation to state our series of conjectures explicitly.

CONJECTURE 0. *With each Γ satisfying (Γ1), (Γ2) and (Γ3), we can associate an algebraic function field K of one variable with finite constant field F_{q^2} and with genus g, satisfying the properties stated in the following conjectures. Here, $q=N\mathfrak{p}$, and g is the genus* of $\mathfrak{h}/\Gamma_R^0$.*

CONJECTURE 1. *Denoting by $\mathfrak{P}(K)$ the set of all prime divisors of K over F_{q^2}, there exists a finite subset $\mathfrak{S}(K)$ of $\mathfrak{P}(K)$ consisting of $(q-1)(g-1)$ prime divisors of K of degree one over F_{q^2}, and a one-to-one correspondence between $\mathfrak{P}(\Gamma)$ and $\mathfrak{P}(K)$-$\mathfrak{S}(K)$ which preserves the degrees of elements of $\mathfrak{P}(\Gamma)$ and of $\mathfrak{P}(K)-\mathfrak{S}(K)$;*

$$\mathfrak{P}(K)-\mathfrak{S}(K)\underset{1:1}{\longleftrightarrow}\mathfrak{P}(\Gamma),$$

and which agrees with the following conjectures.

CONJECTURE 2. *There exists a one-to-one correspondence between the set of all subgroups Γ' of Γ with finite indices and that of all finite extensions K' of K satisfying the following conditions* (i), (ii).

(i) *K'/K is unramifild.*

(ii) *All prime divisors of K belonging to $\mathfrak{S}(K)$ are decomposed completely in K'.*

Moreover, this one-to-one correspondence $K'\leftrightarrow\Gamma'$ satisfies the Galois theory.

REMARK. The constant field of K' must also be F_{q^2}, because of (ii).

Now let $\mathfrak{R}$ be the union of all K' satisfying (i), (ii). So, $\mathfrak{R}$ is the maximum unramified extension of K in which all prime divisors P of K with $P\in\mathfrak{S}(K)$ are decomposed completely. Then, by the above conjecture 2, the Galois group

* Or, what is the same, the genus of the function field L_0. Since Γ, and hence Γ_R^0, is torsion-free, we have $g\geqq 2$.

$\mathfrak{G}=\mathfrak{G}(\mathfrak{K}/K)$ of $\mathfrak{K}$ over K can be identified with the projective limit of all finite factor groups of Γ. But we know that Γ is residually finite (see § 1-5, (ii)), and hence the natural homomorphism of Γ into $\mathfrak{G}$ is injective. So, we shall consider Γ as a (dense) subgroup of $\mathfrak{G}$. For each prime divisor $P\in\mathfrak{P}(K)-\mathfrak{S}(K)$, let $\{\gamma_P^{\pm 1}\}_\Gamma\in\mathfrak{P}(\Gamma)$ be the corresponding mutually inverse pair of primitive elliptic Γ-conjugacy classes. Since Γ is a subgroup of $\mathfrak{G}$, $\{\gamma_P^{\pm 1}\}_\Gamma$ defines a mutually inverse pair of $\mathfrak{G}$-conjugacy classes, which will be denoted by $\{\gamma_P^{\pm 1}\}_{\mathfrak{G}}$. On the other hand, let $\left(\begin{smallmatrix}\mathfrak{K}/K\\ P\end{smallmatrix}\right)$ be the Frobenius substitution of P in $\mathfrak{K}/K$. It is a conjugacy class of the Galois group $\mathfrak{G}$ of $\mathfrak{K}/K$.

CONJECTURE 3*. *The notations being as above, we have*

$$\left(\begin{smallmatrix}\mathfrak{K}/K\\ P\end{smallmatrix}\right)=\{\gamma_P^{\pm 1}\}_{\mathfrak{G}}\quad \textit{for all } P\in\mathfrak{P}(K)-\mathfrak{S}(K),$$

where the sign ± 1 *is left as an ambiguity.*

REMARK. If $P\in\mathfrak{S}(K)$, then, by conjecture 2, we have $\left(\begin{smallmatrix}\mathfrak{K}/K\\ P\end{smallmatrix}\right)=1$.

Finally, the notations being as above, K' is the field associated with Γ'; $\mathfrak{S}(K')$ is the set of all prime divisors of K' which lie on $\mathfrak{S}(K)$; and by the notation of § 0-1, $\{\gamma_{P,i}^{\pm f_i}\}_{\Gamma'}$ *is the mutually inverse pair of primitive elliptic conjugacy classes of Γ' which corresponds to P_i' $(1\leqq i\leqq t$; where the suffices are assumed to be suitably chosen). So, $\mathfrak{K}'$ (i.e., $\mathfrak{K}$ for K') coincides with $\mathfrak{K}$.*

§ 3-2. *Connection with the results of* § 1. In § 1, we defined the ζ function of Γ; $\zeta_\Gamma(u)=\prod_{P\in\mathfrak{P}(\Gamma)}(1-u^{\deg P})^{-1}$, and Theorem 1 asserts that it is of the form:

$$\zeta_\Gamma(u)=\frac{\prod_{i=1}^{g}(1-\alpha_i u)(1-\alpha_i' u)}{(1-u)(1-q^2u)}\times(1-u)^{(q-1)(g-1)};\qquad \alpha_i\alpha_i'=q^2\ (1\leqq i\leqq g).$$

This suggests the possibility that the first factor of $\zeta_\Gamma(u)$, i.e.,

$$\frac{\prod_{i=1}^{g}(1-\alpha_i u)(1-\alpha_i' u)}{(1-u)(1-q^2u)}$$

is a congruence ζ function of some algebraic function field K of one variable with genus g and with the constant field F_{q^2}. Now if it is so, then for each $n\geqq 1$, we have:

* This is a stronger form of the conjecture 3 given in the introduction. It does not contradict "Tschebotareff's density theorem". In fact, T's density theorem "on Γ-side" can be proved by using $Q(q^{-1})\neq 0$ (Theorem 1) and its generalizations to L-functions of Γ.

the number of prime divisors of K with degree n

$$= \text{the number of } P \in \mathfrak{P}(\Gamma) \text{ with degree } n + \begin{cases} 0 \cdots n > 1 \\ (q-1)(g-1) \cdots n = 1 . \end{cases}$$

Actually, this is not the original reason that motivated the author to entertain conjectures 0, 1; but, in any case, this agrees with the conjectures 0, 1. As conjectures 0, 1 were so, conjectures 2, 3 were also suggested by the elliptic modular case (see § 4-2, and [2]), and we cannot explain the reasonings of conjectures 2, 3 only with the results of § 1. The only thing we can say here is this; if we assume conjectures 2 and 3, then the reason for "the existence of $(q-1)(g-1)$ prime divisors of K of degree one which do not correspond to any $\{\gamma_P^{\pm 1}\}_\Gamma \in \mathfrak{P}(\Gamma)$ (conjecture 1)" can be explained most clearly!

As for § 1-5, we remark that it gives a pleasant exercise to interpret the assertions of § 1-5 (ii), (iv) in view of our conjectures.

§ 3-3. *Connection with the results of* § 2. This is more vague and incomplete. The motivation for the study of § 2 lies in trying to obtain the questioned K out of Γ. Our conjecture implicitly assumes that K is obtained by "reduction mod $\mathfrak{P}$" of L_0; and so, our study in § 2 is the first thing that should be done along this line. Our results seem encouraging.

§ 4. Examples

§ 4-1. Let F be a totally real algebraic number field of finite degree, and let B be a divison quaternion algebra over F, in which all but one infinite prime of F are ramified. Let $\mathfrak{p}$ be a finite prime of F which is unramified in B, and let $\mathfrak{o}$ be an order of B containing the maximal order of F. Put $\mathfrak{o}^{(\mathfrak{p})} = \bigcup_{n=0}^{\infty} \mathfrak{p}^{-n}\mathfrak{o}$, and let Γ be the quotient by the center of the group of all elements x of B such that $x^{-1}\mathfrak{o}^{(\mathfrak{p})}x = \mathfrak{o}^{(\mathfrak{p})}$ and that $n(x) \in R^2, F_{\mathfrak{p}}^2$. Let ι_∞ resp. $\iota_{\mathfrak{p}}$ be the embeddings of F into R resp. $F_{\mathfrak{p}}$ defined with respect to the infinite prime of F unramified in B resp. $\mathfrak{p}$, where $F_{\mathfrak{p}}$ is the $\mathfrak{p}$-adic completion of F. Then the tensor products $B \underset{F}{\otimes} R$ resp. $B \underset{F}{\otimes} F_{\mathfrak{p}}$, defined with respect to ι_∞ resp. $\iota_{\mathfrak{p}}$, are isomorphic over R resp. $F_{\mathfrak{p}}$ to $M_2(R)$ resp. $M_2(F_{\mathfrak{p}})$; and by this, we can regard Γ as a subgroup of $G = \mathrm{PSL}_2(R) \times \mathrm{PSL}_2(F_{\mathfrak{p}})$. Now, it is a simple exercise in arithmetic of algebraic groups to check that Γ satisfies $(\Gamma 1)$ and $(\Gamma 2)$. On the other hand, up to commensurability, these are the only examples of Γ satisfying $(\Gamma 1)$ and $(\Gamma 2)$ that we know so far. We do not know whether such Γ satisfy "the congruence subgroup properties".

Now, for these Γ, the Fuchsian groups Γ_R^0 belong to those classes for which the quotients $\mathfrak{h}/\Gamma_R^0$ have been studied in detail by G. Shimura [3], where

much of the deepest results on arithmetic of elliptic modular functions have been generalized to these cases by using his theory of moduli of abelian varieties. Although neither of our conjectures have been proved for these cases, it is expected that the study of these cases will help us give a further insight for the general case. The following is some information on these Γ which we get directly from [3]. Here, we assume that $\mathfrak{o}$ is maximal.

(i) *The ζ function.* For such Γ, it follows directly from the results of [3] (and from our explicit formula for $Q(u)$, cf. [1]) that the main factor

$$\frac{Q(u)}{(1-u)(1-q^2u)}$$

of $\zeta_\Gamma(u)$ coincides with the congruence ζ function of some algebraic function field K over F_{q^2}, *for almost all* $\mathfrak{p}$. The field K is obtained by "reduction mod $\mathfrak{P}$" of L_0.

(ii) *The field k_0 (in Theorem 4).* Since $\mathfrak{o}$ is maximal, Γ is maximal in the sense of § 2-2, and hence we get an algebraic number field k_0. It turns out (by [3]) that the composite $k_0 \cdot F$ is a class field over F, whose ideal class group can be explicitly written down. (Added in proof. k_0 contains F. Cf. [1].)

§ 4-2. *Elliptic modular case ("quasi-example")**. Let p be a rational prime number other than 2 or 3, let $\boldsymbol{Z}$ be the ring of rational integers, and put

$$\boldsymbol{Z}^{(p)} = \{a/p^n \mid a, n \in \boldsymbol{Z}\}, \qquad \Gamma = \mathrm{PSL}_2(\boldsymbol{Z}^{(p)}).$$

Then Γ can be considered as a discrete subgroup of $G = G_R \times G_p$, where $G_R = \mathrm{PSL}_2(R)$, $G_p = \mathrm{PSL}_2(Q_p)$, and Q_p is the p-adic number field. Let Z_p be the ring of p-adic integers, put $U_p = \mathrm{PSL}_2(Z_p)$, and put $\Gamma^0 = \Gamma \cap (G_R \times U_p)$. Then it is clear that $\Gamma^0 = \mathrm{PSL}_2(Z)$, and hence its projection Γ^0_R is a discrete subgroup of G_R, but the quotient is not compact. So, the quotient G/Γ is not compact, but since G_R/Γ^0_R has finite invariant volume, we see easily that G/Γ also has finite invariant volume.

Now, since G/Γ is not compact, we must modify our conjectures. The modified conjectures are partly proved for the above Γ and its congruence subgroups, and the results are stated in [2]. As for the above $\Gamma = \mathrm{PSL}_2(\boldsymbol{Z}^{(p)})$, conjecture 1 (modified) is true for $K = F_{p^2}(\tilde{j})$, the rational function field, and here $\mathfrak{S}(K)$ is the set of all *supersingular moduli j*. Namely, an element j of a finite field of characteristic p is called supersingular, if the elliptic curve with modulus j has no points of order p; and it is known that such j is contained in F_{p^2} and hence defines a prime divisor of $K = F_{p^2}(\tilde{j})$ of degree one. Conjecture 2 (modified) is proved only for the pairs of such Γ' that contain

* As for the details of this section, cf. [2] for a rough sketch, and [1] for more detailed statements and proofs.

some congruence subgroup of Γ and such K' that are obtained by the division of the elliptic curve with modulus $\tilde{j}$. Whether they exhaust all Γ' and K' is an open problem. Conjecture 3 is true *for these* Γ' and K'. All these are consequences of modern theory of elliptic curves (by M. Deuring, J. Igusa, etc.).

ADDED IN PROOF. After this paper was submitted, the author learned that J. Mennicke and J. P. Serre had succeeded in proving the congruence subgroup property for $\Gamma = \mathrm{PSL}_2(Z^{(p)})$ (cf. [**4**]). Mennicke has stronger results on this group Γ, and Serre's results are on more general SL_2 type groups. However, the first idea is due to Mennicke (cf. [**4**], [**5**]).

University of Tokyo

References

[1] Y. Ihara, On congruence monodromy problems, Lecture note at Princeton University, 1967 Spring Term, to appear.

[2] Y. Ihara, Algebraic curves mod $\mathfrak{p}$ and arithmetic groups, Proceedings of Symposia in Pure Mathematics, Vol. 9, 1966, p. 265–271.

[3] G. Shimura, Construction of class fields and zeta functions of algebraic curves, Ann. of Math., **85** (1967), 58–159.

[4] J. Mennicke, On Ihara's modular group, Invent. Math., **4** (1967), 202–228.

[5] J. P. Serre, Le problème des groupes de congruence pour SL_2, (unpublished manuscript).