Advanced Studies in Pure Mathematics 2, 1983
Galois Groups and their Representations
pp. 89–97

On Unramified Extensions of Function Fields over Finite Fields

Yasutaka Ihara

Let k be an algebraic function field of one variable with genus g over a finite constant field $\boldsymbol{F}_q$, and S be a given *non-empty* set of prime divisors of k. Denote by k_S^{ur} the maximum unramified Galois extension of k in which all prime divisors of k belonging to S decompose completely. Since S is nonempty, the algebraic closure of $\boldsymbol{F}_q$ in k_S^{ur} must be finite over $\boldsymbol{F}_q$. In this report, we shall give a survey of our results on this type of extensions k_S^{ur}.

§ **1.***) First, one expects that if k_S^{ur}/k is an *infinite* extension, then S cannot be "too big". What is the natural quantitative result along this line? The Chebotarev density of S is of course 0, but we need a stronger result. By studying the behaviour of zeta functions of intermediate fields of k_S^{ur}/k near $s=\frac{1}{2}$, using the Weil's Riemann hypothesis for curves, we obtained the following

Theorem 1. *Suppose that M is an infinite unramified Galois extension of k. For each prime divisor P of k, let* deg P *denote its degree over $\boldsymbol{F}_q$, put $N(P)=q^{\deg P}$, and let $f(P)$ $(1\leq f(P)\leq\infty)$ denote the residue extension degree of P in M/k. Let $g\geq 1$. Then*

$$(1.1)\qquad \sum_{\substack{P\\ f(P)<\infty}} \frac{\deg P}{N(P)^{\frac{1}{2}f(P)}-1}\leq g-1\,,$$

the series on the left being convergent.

Corollary 1. *If k_S^{ur}/k is infinite, then*

$$(1.2)\qquad \sum_{P\in S} \frac{\deg P}{N(P)^{1/2}-1}\leq g-1\,.$$

In particular,

Received January 6, 1983.

*) The results of § 1 are obtained after the Symposium. Details will appear in [Ih 7].

Corollary 2 *If k_S^{ur}/k is infinite, and S consists only of a finite number of prime divisors of degree one, then*

$$|S| \leq (\sqrt{q}-1)(g-1)\,. \tag{1.3}$$

We have a similar result for algebraic number fields assuming the generalized Riemann hypothesis. In each case, the proof is based on the studies of $[K\colon k]^{-1}(d/ds)\log\zeta_K(s)$, its inverse Mellin transform, and their limit as $K \to M$, where K runs over the finite subextensions of M/k (cf. [Ih 7]).

A basic open question related to Theorem 1 is: *Does there exist M with which the set $\{P; f(P)<\infty\}$ is infinite?* On the other hand, we have a family of examples of *M/k for which the equality in* (1.1) (*and in fact,* Corollary 2 *with the equality*) *holds.* Such examples appear in connection with liftings of the Frobenius-like correspondence "$\Pi+\Pi'$" of k to characteristic 0, and with irreducible discrete subgroups of $PSL_2(\boldsymbol{R})\times PGL_2(F_{\mathfrak{p}})$ ($F_{\mathfrak{p}}$: a $\mathfrak{p}$-adic field, $q=N(\mathfrak{p})^2$). This will be discussed as one of the main subjects in the next sections.

§ 2. We shall meet with the case where the Galois group of k_S^{ur}/k is *isomorphic* with the profinite completion of some topological fundamental group. ([Ih 4] [Ih 5]).

Let $q=p^{2f}$, an *even* power of a prime p, and $C/\boldsymbol{F}_q$ be a smooth complete model of k. Let $C'/\boldsymbol{F}_q$ be its conjugate over $\boldsymbol{F}_{p^f}$, and let Π (resp. Π') be the graphs on $C\times C'$ of the *p^f-th* power morphisms $C\to C'$ (resp. $C'\to C$). Consider $\Pi+\Pi'\subset C\times C'$ as a reduced closed subscheme. Note that the set of singular points of $\Pi+\Pi'$ is:

$$\begin{aligned}\Pi\cap\Pi' &= \{(x,x')\in C\times C';\ x^{p^f}=x',\ x'^{p^f}=x\}\\ &\approx \text{the } \boldsymbol{F}_q\text{-rational points } x \text{ of } C\,.\end{aligned}$$

We shall be concerned with lifting of the triple $(C, C'; \Pi+\Pi')$ to characteristic 0 and its application to the Galois group of k_S^{ur}/k (for some S determined by the lifting). Let $\mathfrak{o}_{\mathfrak{p}}$ be the ring of integers of a $\mathfrak{p}$-adic field with residue field $\boldsymbol{F}_{p^f}$ (e.g. $\mathfrak{o}_{\mathfrak{p}}=W(\boldsymbol{F}_{p^f})$, the ring of Witt vectors), and $\mathfrak{o}_{\mathfrak{p}}^{(2)}$ be its unique unramified quadratic extension. By a *lifting* of $(C, C'; \Pi+\Pi')$ over $\mathfrak{o}_{\mathfrak{p}}^{(2)}$, we mean a triple $(\mathscr{C}, \mathscr{C}'; \mathscr{T})$, where $\mathscr{C}, \mathscr{C}'$ are smooth proper $\mathfrak{o}_{\mathfrak{p}}^{(2)}$-schemes that lift C, C' respectively, and $\mathscr{T}$ is an irreducible closed subscheme of $\mathscr{C}\times\mathscr{C}'$, flat over $\mathfrak{o}_{\mathfrak{p}}^{(2)}$, that lifts $\Pi+\Pi'$. (When k has a model C *over* $\boldsymbol{F}_{p^f}$, we look for liftings of $(C, C; \Pi+\Pi')$ *over* $\mathfrak{o}_{\mathfrak{p}}$, and this is sometimes easier.) We say that $(\mathscr{C}, \mathscr{C}'; \mathscr{T})$ is *symmetric*, if $\mathscr{C}$ and $\mathscr{C}'$ are conjugate over $\mathfrak{o}_{\mathfrak{p}}$ and if ${}^t\mathscr{T}=\mathscr{T}'$ (t: the transpose, $'$: the $\mathfrak{o}_{\mathfrak{p}}$-conjugation).

Suppose that $(\mathscr{C}, \mathscr{C}'; \mathscr{T})$ is a lifting of $(C, C'; \Pi+\Pi')$. Take any closed point $P=(x, x') \in \Pi \cap \Pi'$ and consider it as a point of $\mathscr{T}$ (via $\Pi+\Pi' \hookrightarrow \mathscr{T}$, the inclusion as the special fiber). When P is a *normal* point on $\mathscr{T}$, we say that $x \in C$ is a *special point* with respect to $(\mathscr{C}, \mathscr{C}'; \mathscr{T})$. *Let S be the set of all special points.* By definition, S consists only of $\boldsymbol{F}_q$-rational points of C. (The corresponding set of prime divisors of k of degree one will also be called the set of special points and denoted by S.) As for the cardinality of S, we have

Proposition 1. (i) $|S| \geq (\sqrt{q}-1)(g-1)$, (ii) *the equality holds if and only if the normalization $\mathscr{T}^*$ of $\mathscr{T}$ is unramified over $\mathscr{C}$ (resp. $\mathscr{C}'$) on the general fiber.*

Thus, we call $(\mathscr{C}, \mathscr{C}'; \mathscr{T})$ *unramified* when $|S|=(\sqrt{q}-1)(g-1)$, and *ramified* when $|S|>(\sqrt{q}-1)(g-1)$. Leaving aside the question of liftability till Section 3, we first discuss the main consequences assuming the existence of $(\mathscr{C}, \mathscr{C}'; \mathscr{T})$.

Assume that there exists a lifting $(\mathscr{C}, \mathscr{C}'; \mathscr{T})$ of $(C, C'; \Pi+\Pi')$ over $\mathfrak{o}_{\mathfrak{p}}^{(2)}$. Let $F_{\mathfrak{p}}$ denote the quotient field of $\mathfrak{o}_{\mathfrak{p}}$, and $\bar{F}_{\mathfrak{p}}$ its algebraic closure. Fix any isomorphism $\iota\colon \bar{F}_{\mathfrak{p}} \xrightarrow{\sim} \boldsymbol{C}$, $\boldsymbol{C}$ being the complex number field. Take base changes $\mathscr{C}\otimes\boldsymbol{C}$, $\mathscr{C}'\otimes\boldsymbol{C}$, $\mathscr{T}^*\otimes\boldsymbol{C}$ with respect to ι, and call $\mathfrak{R}$, $\mathfrak{R}'$, $\mathfrak{R}^0$ the corresponding compact Riemann surfaces. Let $\varphi\colon \mathfrak{R}^0 \to \mathfrak{R}$, $\varphi'\colon \mathfrak{R}^0 \to \mathfrak{R}'$ be the finite morphisms induced from the projections $\mathscr{T}^* \to \mathscr{C}$, $\mathscr{T}^* \to \mathscr{C}'$, respectively. Then φ, φ' have degree p^f+1. Take any base point $P^0 \in \mathfrak{R}^0$, and put $P=\varphi(P^0)$, $P'=\varphi'(P^0)$. Let $\pi_1(\mathfrak{R})$, $\pi_1(\mathfrak{R}')$, $\pi_1(\mathfrak{R}^0)$ be the topological fundamental groups of $\mathfrak{R}$, $\mathfrak{R}'$, $\mathfrak{R}^0$ w.r.t. P, P', P^0, and let

$$\Phi\colon \pi_1(\mathfrak{R}^0) \longrightarrow \pi_1(\mathfrak{R}), \qquad \Phi'\colon \pi_1(\mathfrak{R}^0) \longrightarrow \pi_1(\mathfrak{R}')$$

be the group homomorphisms induced from φ, φ'. Let Γ be the free product of $\pi_1(\mathfrak{R})$, $\pi_1(\mathfrak{R}')$ with amalgamation defined by Φ and Φ';

$$\Gamma = \pi_1(\mathfrak{R}) \underset{\pi_1(\mathfrak{R}^0)}{*} \pi_1(\mathfrak{R}').$$

Then Γ is a group defined by a finite number of generators and relations. It is the fundamental group of the space obtained by amalgamating the mapping cylinders of φ and of φ'. When $(\mathscr{C}, \mathscr{C}'; \mathscr{T})$ is unramified, φ, φ' are unramified; hence Φ, Φ' are *injective* and Γ is an *infinite* group. On the other hand, when $(\mathscr{C}, \mathscr{C}'; \mathscr{T})$ is ramified, both φ, φ' are ramified, and Φ and Φ' turn out to be *surjective*; hence $\Gamma \cong \pi_1(\mathfrak{R}^0)/N.N'$, where N, N' denote the kernels of Φ, Φ' respectively. Denote by $\hat{\Gamma}$ the profinite completion of Γ.

Theorem 2 [Ih 4] [Ih 5]*). *Suppose that* $(C, C'; \Pi+\Pi')$ *has a lifting* $(\mathscr{C}, \mathscr{C}'; \mathscr{T})$ *over* $\mathfrak{o}_p^{(2)}$, *and let* S *be the set of special points with respect to this lifting. Then*

(i) *the Galois group* $\mathrm{Gal}(k_S^{\mathrm{ur}}/k)$ *is isomorphic with* $\hat{\Gamma}$;

(ii) *the isomorphic groups of* (i) *are infinite groups if and only if* $|S|=(\sqrt{q}-1)(g-1)$.

The main point to be stressed here is that $\mathrm{Gal}(k_S^{\mathrm{ur}}/k)$ is strictly isomorphic with $\hat{\Gamma}$, *not excluding the pro-p-factors.* The key lemma for this is:

Lemma 1 (Ihara-Miki [Ih-Mi 1]). *Let* $\boldsymbol{Q}_p$ *be the p-adic number field. Let* $\mathfrak{K}$ *be a field containing* $\boldsymbol{Q}_p$, *which is complete with respect to a discrete valuation* $|\ \ |_{\mathfrak{K}}$ *extending the p-adic valuation of* $\boldsymbol{Q}_p$. *Suppose moreover that* $\mathfrak{K}$ *contains a prime element (for* $|\ \ |_{\mathfrak{K}}$) *which is algebraic over* $\boldsymbol{Q}_p$, *and that there is a value-preserving field-endomorphism* σ *of* $\mathfrak{K}$ *into* $\mathfrak{K}$ *inducing the* p^r*-th power map of the residue field for some* $r\in\boldsymbol{Z}$, $r\geq 1$. *Let* $\mathfrak{M}/\mathfrak{K}$ *be any finite extension. Then the following two conditions* (i) (ii) *on* $\mathfrak{M}$ *are equivalent*:

(i) *there exists a finite extension* $\boldsymbol{Q}_p'/\boldsymbol{Q}_p$ *such that* $\mathfrak{M}\boldsymbol{Q}_p'/\mathfrak{K}\boldsymbol{Q}_p'$ *is unramified,*

(ii) *for some positive integer* m, σ^m *extends to an endomorphism* $\tilde{\sigma}: \mathfrak{M}\rightarrow\mathfrak{M}$ *satisfying* $\mathfrak{M}^{\tilde{\sigma}}\cdot\mathfrak{K}=\mathfrak{M}$.

In applying this lemma, $\mathfrak{K}$ will be the completion of the function field of $\mathscr{C}$ along its special fiber C, and σ is induced from the "$\Pi'\circ\Pi$-part" of the algebraic correspondence ${}^t\mathscr{T}\circ\mathscr{T}$ of $\mathscr{C}$.

As for the assertion (ii) of Theorem 2, the "if" implication follows from the fact that in the unramified case, Γ is infinite *and residually finite* (i.e., $\Gamma\rightarrow\hat{\Gamma}$: injective; cf. [Ih 5] Section 3). The converse, conjectured in [Ih 5], is a direct consequence of Corollary 2 of Theorem 1.

§ 3. In view of Theorem 2, our attention will be focused on the following two problems.

(i) Give a method for deciding whether there exists a lifting $(\mathscr{C}, \mathscr{C}'; \mathscr{T})$ of $(C, C'; \Pi+\Pi')$ having a prescribed set of special points.

(ii) When $(\mathscr{C}, \mathscr{C}'; \mathscr{T})$ exists, give a method for calculating the group Γ explicitly. (The structure of Γ itself may depend on the choice of $\iota: \bar{F}_p \rightrightarrows \boldsymbol{C}$, although that of $\hat{\Gamma}$ doesn't.)

As for the first problem, we gave some answers in [Ih 3] [Ih 6], using deformation theory. They do not solve the problem completely, but give some criteria for the existence (and/or) uniqueness of $(\mathscr{C}, \mathscr{C}'; \mathscr{T})$. Further

*) In [Ih 4] [Ih 5], we used the letter q for $\sqrt{q}=p^f$.

results along this line (especially for the case $g=2$) were obtained by Y. Furukawa [F 1]. Here, we shall review some results of [Ih 6], taking $f=1$ (i.e., $q=p^2$) and $\mathfrak{o}_\mathfrak{p}=\boldsymbol{Z}_p=W(\boldsymbol{F}_p)$.

Let k_0 be an algebraic function field of one variable with exact constant field $\boldsymbol{F}_p$ and genus $g>1$, and put $k=k_0\cdot\boldsymbol{F}_{p^2}$. Let S_0 be a prescribed set of prime divisors of k_0 with degree ≤ 2 over $\boldsymbol{F}_p$, and S be the set of all prime divisors of k lying above S_0. Let C be a proper smooth model of k_0. We consider the question of existence and/or uniqueness of those liftings $(\mathscr{C}, \mathscr{C}'; \mathscr{T})$ of $(C, C; \Pi+\Pi')$ *over* $\boldsymbol{Z}_p$ whose special point set is *contained in* S. Denote by $H_i (i=1, 2)$ the number of primes of S_0 with degree i over $\boldsymbol{F}_p$, and put $H=|S|=H_1+2H_2$. Let U denote the $\boldsymbol{F}_p$-vector space of all holomorphic differential forms ξ of degree $p+1$ on C satisfying the condition that $\xi/\eta^{\otimes p}$ is an exact differential, where η is a fixed differential $\neq 0$ of degree one on C. Then U is independent of the choice of η, and is of dimension $2(p-1)(g-1)$. For each $Q\in S_0$, let κ_Q denote its residue field, t_Q be a local uniformization, and consider the linear map

$$\beta\colon U\ni\xi\longrightarrow(\operatorname*{Tr}_{\kappa_Q/\boldsymbol{F}_p}(\xi/(dt_Q)^{\otimes(p+1)})_Q)_{Q\in S_0}\in\boldsymbol{F}_p^{H_1+H_2},$$

where $(\ \ )_Q$ denotes the residue class at Q.

Theorem 3A. (i) *If β is injective, then there exists a symmetric lifting of $(C, C; \Pi+\Pi')$ over $\boldsymbol{Z}_p$ whose special points are contained in S*; (ii) *if β is moreover bijective, such lifting is unique.*

As an existence criterion, this applies only when $H_1+H_2\geq 2(p-1)(g-1)$; hence does not apply directly to the unramified situation $H=(p-1)(g-1)$. As for unramified lifting, we have

Theorem 3B. *There is at most one unramified lifting of $(C, C; \Pi+\Pi')$ over $\boldsymbol{Z}_p$ having a prescribed set of special points. When it exists, it is symmetric.*

Theorem 3C. *Suppose that $H=H_1=(p-1)(g-1)$, $p\neq 2$, β is surjective, and that there is an involutive automorphism of C leaving each point of S invariant. Then there exists a unique unramified symmetric lifting of $(C, C; \Pi+\Pi')$ over $\boldsymbol{Z}_p$ having S as the set of special points.*

This is a corollary of a more general result. The range of applicability is small, but is useful for giving examples. There are also criteria for *non-existence*. In fact, the liftings of $(C, C; \Pi+\Pi')$ to $\boldsymbol{Z}/p^2$ are completely classified in terms of some differentials of degree $p-1$ on C, and hence the non-existence of such differentials would imply that of liftings to $\boldsymbol{Z}/p^2$, and hence to $\boldsymbol{Z}_p$ (cf. [Ih 3] Example 2).

In each of the following three examples, there exists a unique symmetric lifting of $(C, C; \Pi+\Pi')$ over Z_p having S as the set of special points. For other examples of unique existence, non-existence, or non-unique existence, cf. [Ih 3] [Ih 6] [F 1].

Example 1 ($p=2$, $g=2$; ramified type).

$$k_0=\boldsymbol{F}_2(x, y); \qquad y^2+(x^3+x+1)y=x^2+x+1$$
$$S=\{(\infty, \infty), (\infty, 0)\}.$$

The unique liftability in this case follows from Theorem 3A. The reason why the special point set *coincides with* S (instead of just contained in S) is explained in [Ih 6] Section 3.1 Example 1.

Example 2 ($p=3$, $g=3$; unramified type).

$$k_0=\boldsymbol{F}_3(x, y); \qquad x=X/Z, \quad y=Y/Z;$$
$$X^3Y-XY^3+XYZ^2+Z^4=0,$$
$$S=\{(1:0:0), (0:1:0), (1:1:0), (1:-1:0)\}.$$

This unique liftability is an application of Theorem 3C.

Example 3 ($p=5$, $g=2$; unramified type).

$$k_0=\boldsymbol{F}_5(x, y); \qquad y^2=x^6+1$$
$$S=\{(0, 1), (0, -1), (\infty, \infty), (\infty, \infty)\}.$$

This unique liftability is an application of Corollary 2 of Theorem 3 of [Ih 6], and is also obtained from a Shimura curve by reduction mod p.

By Theorem 2 for $k=k_0\boldsymbol{F}_{p^2}$, we find that the extension k_S^{ur}/k is finite for Example 1, *and infinite for Examples* 2, 3.

As for the second problem, it is *left open*. To illustrate the nature of the problem, let C, S be as in Example 1, and $(\mathscr{C}, \mathscr{C}'; \mathscr{T})$ be the unique symmetric lifting of $(C, C; \Pi+\Pi')$ over Z_2 with the special point set S. Let $\mathfrak{R}$, $\mathfrak{R}'=\mathfrak{R}$, $\mathfrak{R}^0$ be the corresponding compact Riemann surfaces (w.r.t. ι), and φ: $\mathfrak{R}^0\to\mathfrak{R}$, φ': $\mathfrak{R}^0\to\mathfrak{R}'$ be the projections. Let τ be the involutive automorphism of $\mathfrak{R}^0$ induced from the symmetry of $\mathscr{T}$. Then the group Γ in question is

$$\Gamma=\pi_1(\mathfrak{R}^0)/N.N^\tau,$$

where N is the kernel of Φ: $\pi_1(\mathfrak{R}^0)\to\pi_1(\mathfrak{R})$, and the involution of $\pi_1(\mathfrak{R}^0)$ induced from τ is also denoted by τ. Now we can show (without knowing the algebraic equations for $(\mathscr{C}, \mathscr{C}'; \mathscr{T})$) that:

(a) $\mathfrak{R}$ has genus 2, and $\mathfrak{R}^0$ has genus 5;

(b) $\varphi' = \varphi \circ \tau$, deg $\varphi = 3$, and φ is ramified at exactly two points of $\mathfrak{R}^0$ with ramification index 2;

(c) the number of fixed points of τ on $\mathfrak{R}^0$ is 4.

From these data, we can determine

(A) the group structure of $\pi_1(\mathfrak{R}^0)$;

(B) its normal subgroup N, up to automorphisms of $\pi_1(\mathfrak{R}^0)$,

(C) the involutive automorphism τ of $\pi_1(\mathfrak{R}^0)$, up to conjugacy in the full automorphism group of $\pi_1(\mathfrak{R}^0)$.

But this still does not determine *the pair* $\{N, N^\tau\}$ up to automorphisms of $\pi_1(\mathfrak{R}^0)$, because the double coset space

$$\mathrm{Centralizer}(\tau)\backslash \mathrm{Aut}\,(\pi_1(\mathfrak{R}^0))/\mathrm{Normalizer}(N)$$

seems to be large and mysterious. The recent developments on the structure of the outer automorphism group of π_1 of compact Riemann surfaces still do not seem to help much.

§ 4. The unramified liftings of $(C, C'; \Pi + \Pi')$ over $\mathfrak{o}_\mathfrak{p}^{(2)}$ are in a close connection with discrete co-compact subgroups Γ of $PSL_2(\boldsymbol{R}) \times PGL_2^+(F_\mathfrak{p})$, where $PGL_2^+(F_\mathfrak{p})$ denotes the intermediate group of $PSL_2(F_\mathfrak{p}) \subset PGL_2(F_\mathfrak{p})$ corresponding to $\mathfrak{o}_\mathfrak{p}^\times F_\mathfrak{p}^{\times 2}/F_\mathfrak{p}^{\times 2}$ by the determinant. Put

$$V = PGL_2(\mathfrak{o}_\mathfrak{p}), \quad V' = \begin{pmatrix} \pi & 0 \\ 0 & 1 \end{pmatrix}^{-1} PGL_2(\mathfrak{o}_\mathfrak{p}) \begin{pmatrix} \pi & 0 \\ 0 & 1 \end{pmatrix}, \quad V^0 = V \cap V',$$

where π is a prime element of $F_\mathfrak{p}$, and let Γ_V, etc. be the projection to $PSL_2(\boldsymbol{R})$ of the intersection of Γ with $PSL_2(\boldsymbol{R}) \times V$, etc. Then Γ_V, etc. are discrete co-compact subgroups of $PSL_2(\boldsymbol{R})$. Let $\mathfrak{R}_\Gamma$, $\mathfrak{R}'_\Gamma$, $\mathfrak{R}^0_\Gamma$ be the compact Riemann surfaces corresponding to Γ_V, $\Gamma_{V'}$, Γ_{V^0} respectively, and $\varphi_\Gamma : \mathfrak{R}^0_\Gamma \to \mathfrak{R}_\Gamma$, $\varphi'_\Gamma : \mathfrak{R}^0_\Gamma \to \mathfrak{R}'_\Gamma$ be the canonical morphisms. Fix $\iota : \bar{F}_\mathfrak{p} \xrightarrow{\sim} \boldsymbol{C}$, as before.

Conjecture *There is a categorical equivalence between*

(A) *Unramified liftings* $(\mathscr{C}, \mathscr{C}'; \mathscr{T})$ *of some* $(C, C'; \Pi + \Pi')$ (*not specified*) *over* $\mathfrak{o}_\mathfrak{p}^{(2)}$ *such that the normalization* $\mathscr{T}^*$ *of* $\mathscr{T}$ *is regular* (*as a scheme*);

(B) *Torsion-free co-compact discrete subgroups* Γ *of* $PSL_2(\boldsymbol{R}) \times PGL_2^+(F_\mathfrak{p})$ *for which the topological closure of the projection of* Γ *to* $PSL_2(\boldsymbol{R})$ (*resp.* $PGL_2^+(F_\mathfrak{p})$) *coincides with* $PSL_2(\boldsymbol{R})$ (*resp. contains* $PSL_2(F_\mathfrak{p})$);

such that if Γ *corresponds with* $(\mathscr{C}, \mathscr{C}'; \mathscr{T})$ *then the system* $\{\mathfrak{R}_\Gamma \xleftarrow{\varphi_\Gamma} \mathfrak{R}^0_\Gamma \xrightarrow{\varphi'_\Gamma} \mathfrak{R}'_\Gamma\}$ *of Riemann surfaces obtained from* Γ *in the above manner corresponds with* $\{\mathscr{C} \leftarrow \mathscr{T}^* \rightarrow \mathscr{C}'\} \otimes_\iota \boldsymbol{C}$.

The functor (B)$\to$(A) is established by the combination of results by Shimura, Ihara, Morita, Ohta and Margulis, except for the regularity of $\mathscr{T}^*$, as follows.

(a) the arithmeticity of Γ (Margulis [Ma 1]),

(b) if Γ corresponds with some $(\mathscr{C}, \mathscr{C}'; \mathscr{T})$ and $\Gamma^* \subset \Gamma$ (finite index), then Γ^* corresponds with some $(\mathscr{C}^*, \mathscr{C}'^*; \mathscr{T}^*)$ (Ihara [Ih 4])

(c) (b) with $\Gamma^* \supset \Gamma$ (cf. Ohta [Oh 1] § 3.4)

(d) congruence relations for Shimura curves for almost all $\mathfrak{p}$ (Shimura [Sh 1]),

(e) (d) for individual $\mathfrak{p}$ for congruence subgroups whose level is coprime with p (not $\mathfrak{p}$) (Morita [Mo 1]; cf. [Oh 1] § 3.4 for methods for refinement to "$\mathfrak{p}$").

It should be added that (b) is based on the earlier work of [Ih-Mi 1] mentioned before, and (e) is based on the works of [Sh 1] and of [Ih 1].

For concrete description of arithmetically defined groups Γ, see [Ih 1] (b) Ch. 4. It is not known whether each Γ satisfies the congruence subgroup properties. The regularity of $\mathscr{T}^*$ is proved only when $F = \boldsymbol{Q}_p$ [Ih 2]. When $F = \boldsymbol{Q}_p$, $(\mathscr{C}, \mathscr{C}'; \mathscr{T})$ is always symmetric (Theorem 4, [Ih 6]).

As for the functor (A)$\to$(B), we constructed an infinite group Γ (§ 2, [Ih 4]) which has a natural embedding into $PSL_2(\boldsymbol{R})$, but what we could prove is only that Γ is a torsion-free co-compact discrete subgroup of $PSL_2(\boldsymbol{R}) \times \mathrm{Aut}(\mathfrak{T})$, where $\mathfrak{T}$ is the *tree* of $PGL_2^+(F_\mathfrak{p})$.

The association $\Gamma \to (\mathscr{C}, \mathscr{C}'; \mathscr{T}) \to \Gamma$ is the identity, and (B)$\to$(A) makes (B) a full subcategory of "(A) without regularity of $\mathscr{T}^*$" (cf. [Ih 4]).

§ 5. Finally, let $(\mathscr{C}, \mathscr{C}'; \mathscr{T})$ be any *unramified* lifting of $(C, C'; \Pi + \Pi')$ over $\mathfrak{o}_\mathfrak{p}^{(2)}$. Then, as we have shown in [Ih 4] Section 5, the group Γ describes, not only the structure of the Galois group $\mathrm{Gal}(k_S^{\mathrm{ur}}/k)$, but also all the Frobenius elements in k_S^{ur}/k in terms of some Γ-conjugacy classes. Since each discrete subgroup Γ of $PSL_2(\boldsymbol{R}) \times PGL_2^+(F_\mathfrak{p})$ satisfying the conditions of (B) determines $(\mathscr{C}, \mathscr{C}'; \mathscr{T})$ (and hence also k and S), it describes the Galois group of k_S^{ur}/k together with all Frobenius elements as in [Ih 4] Section 5. Thus, the problem raised in [Ih 1] as conjectures ((C1)$\sim$(C5) in (c) § 1.3) have been *solved affirmatively*, although in a very indirect way*).

References

[F1] Y. Furukawa, On the liftings of the Frobenius correspondences of algebraic curves of genus two over finite fields, to appear in J. Algebra.

[Ih 1] Y. Ihara, (a) The congruence monodromy problems, J. Math. Soc.

*) As for (C2), cf. also [Ih 2]. The elliptic modular case, which is the only case with cusps in view of [Ma 1], had been settled separately in earlier publications.

Japan, **20** (1968), 107–121.
(b) On congruence monodromy problems, Lect. Note Univ. Tokyo, **1** (1968), **2** (1969).
(c) Non-abelian classfields over function fields in special cases, Actes du Congres Intern. Math. Nice 1970, Tome **1**, 381–389.

[Ih 2] ——, On the differentials associated to congruence relations and the Schwarzian equations defining uniformizations, J. Fac. Sci. Univ. Tokyo Sect. IA Math., **21** (1974), 309–332.

[Ih 3] ——, On the Frobenius correspondences of algebraic curves, "Algebraic number theory", Papers contributed for the International Symposium, Kyoto, 1976, Japan Soc. Prom. Sci., (1977), 67–98.

[Ih 4] ——, Congruence relations and Shimura curves, I, Proc. Symp. in pure Math., **33** Part 2, (1977), 291–311, Amer. Math. Soc.; II, J. Fac. Sci. Univ. Tokyo Sect. IA, Math., **25** (1979), 301–361.

[Ih 5] ——, Congruence relations and fundamental groups, J. Algebra, **75** (1982), 445–451.

[Ih 6] ——, Lifting curves over finite fields together with the characteristic correspondence $\Pi+\Pi'$, ibid., **75** (1982), 452–483.

[Ih 7] ——, How many primes decompose completely in an infinite unramified Galois extension of a global field?, J. Math. Soc. Japan, **35** (1983), 693–709.

[Ih-Mi 1] Y. Ihara and H. Miki, Criteria related to potential unramifiedness and reduction of unramified coverings of curves, J. Fac. Sci. Univ. Tokyo, Sect. IA, Math., **22** (1975), 237–254.

[Ma-1] G. A.. Margulis, Цискретные Группы Цвижений Многообразий Неположительной Кривизны, Proc. Internat. Congress Math. (Vancouver 1974) **2**, 21-34.

[Mo 1] Y. Morita, Reduction mod $\mathfrak{P}$ of Shimura curves, Hokkaido Math. J., **10** (1981), 209–238.

[Oh 1] M. Ohta, On l-adic representations attached to automorphic forms, Japanese J. Math., 8 (1982), 1–47.

[Sh 1] G. Shimura, On canonical models of arithmetic quotients of bounded symmetric domains I, Ann. of Math., **91** (1970), 144–222; II, ibid., **92** (1970), 528–549.

Department of Mathematics
Faculty of Science
University of Tokyo
Hongo, Tokyo 113
Japan