J. Fac. Sci. Univ. Tokyo
Sect. IA, Math.
34 (1987), 245-269.

On the ramified congruence relations of algebraic curves

By Yoshihiro FURUKAWA

(Communicated by Y. Ihara)

Introduction

In this paper we shall study a certain relation between coverings of a curve over a finite field of characteristic $p>0$ and those of a system of curves over $\bar{Q}_p$.

Let $\mathcal{C}$ be a proper smooth curve over a discrete valuation ring R of characteristic *zero* with finite residue field $\boldsymbol{F}_q$, and C the reduction of $\mathcal{C}$. We assume that there exists a *symmetric correspondence* $\mathcal{T}$ on $\mathcal{C}\times\mathcal{C}$ whose special fibre consists of the graph of the qth power Frobenius morphism and its transpose. We consider the geometric generic fibre $\tilde{\mathfrak{X}}$ of the system $\mathfrak{X}=\{\mathcal{C}\xleftarrow{\varphi}\mathcal{T}^n\xrightarrow{{}^t\varphi}\mathcal{C}\}$, where $\mathcal{T}^n$ denotes the normalization of $\mathcal{T}$. Y. Ihara [8][9] established the comparison theory between the *finite étale coverings* of $\tilde{\mathfrak{X}}$ and *certain finite étale coverings* of C over $\boldsymbol{F}_{q^2}$. Furthermore, he constructed a group Γ whose profinite completion is canonically isomorphic to the algebraic fundamental group of $\tilde{\mathfrak{X}}$. The purpose of this paper is to extend his comparison theory to the case of certain ramified coverings of $\tilde{\mathfrak{X}}$ and C, while the construction of Γ has not yet been accomplished.

It seems quite important to consider not only étale coverings but also certain ramified coverings, as indicated in the case of the modular correspondences of the elliptic modular curve (cf. Ihara [5][6]). The crucial point is how to give a good condition on the ramifications of coverings of $\tilde{\mathfrak{X}}$ and C compatible with the ramification of φ. For that purpose, we define a $\{1, 2, \cdots; \infty\}$-valued function $\mathfrak{E}$ on the set of all points of the generic fibre $\mathcal{C}_\eta$ naturally determined by the ramification of φ_η, and consider such coverings of $\tilde{\mathfrak{X}}$ for which all ramification indices of points lying above $Q\in\mathcal{C}_\eta$ divide $\mathfrak{E}(Q)$. Here, for each point Q of $\mathcal{C}_\eta$, $\mathfrak{E}(Q)$ is the greatest common divisor of all ramification indices of $P\in\mathcal{T}^n_\eta$ lying above Q such that ${}^t\varphi_\eta$ is unramified at ${}^t\varphi_\eta(P)$. (When such a point

P does not exist, we put $\mathfrak{C}(Q)=\infty$.)

We now explain our main result. An F_{q^2}-rational point $x\in C$ is called *special* if the point (x, x^q) is a normal point of $\mathcal{T}$. If the set of branch points of φ_η has certain good properties (Definition 4 in § 1), there exists a canonical categorical equivalence between the following two categories. (For precise statement, see Theorem 1′ in § 1.)

(i) *Tamely ramified finite coverings* $f: C^*\longrightarrow C$ *over* F_{q^2} *satisfying the following*: (a) *for each* $Q\in C_\eta$, *all ramification indices of points of* C^* *lying above the specialization of* Q *divide* $\mathfrak{C}(Q)$, (b) *all points of* C^* *lying above the special points of* C *are* F_{q^2}*-rational.*

(ii) *Finite coverings* $\mathcal{F}: \mathcal{Y}\longrightarrow\tilde{\mathfrak{X}}$ *with* $\mathcal{Y}=\{Y_1\longleftarrow Y_0\longrightarrow Y_2\}$, *satisfying the condition that, for each* $Q\in C_\eta$, *all ramification indices of points of* Y_1 *and* Y_2 *lying above* Q *divide* $\mathfrak{C}(Q)$ *and are prime to* p.

While our result looks rather complicated, it should be noticed that it is a natural generalization of Ihara's comparison theorem in the elliptic modular case.

In principle the proof of our theorem closely follows that of Ihara in the unramified case. The key points in the ramified case are Main Lemma A in § 2 and Main Lemma B in § 3. The former, describing the local behavior of the inverse images of $\mathcal{T}$, serves to prove the existence of its local extensions. The latter supplements results of Ihara-Miki [11] which gave a criterion for potential good reduction of unramified coverings.

We state basic definitions and main result in § 1. In § 2, we prove the existence of the unique extension of $\mathcal{T}$. In § 3, we study the reduction of coverings of $\tilde{\mathfrak{X}}$. In the final section, we collect the results in § 2 and § 3, and complete the proof.

I express sincere gratitude to Professor Y. Ihara for kindly informing me of his theory of congruence relations. I am also very grateful to Professors K. Kato, F. Momose and T. Saito for valuable conversations.

1. Definitions and main theorems

In this section, we shall give basic definitions and the statements of our main results. Throughout, the word "*(algebraic) curve*" will mean a proper smooth irreducible (not necessarily absolutely irreducible) algebraic curve over a field. We use the following notation.

p : a *prime number*.
q : a *power* of p.
$\boldsymbol{F}_q$: the *finite field* with q elements.
R : a *complete discrete valuation ring* of characteristic 0 with residue field $\boldsymbol{F}_q$ and quotient field k.
π : a fixed *prime element* of R.
$\bar{k}$: the *algebraic closure* of k.
$R^{(d)}$: the unique *unramified extension* of R of degree d.

Let C be an algebraic curve over $\boldsymbol{F}_q$; then
Π_C : the *graph* on $C \times C$ of the qth power Frobenius morphism.
Π'_C : the *transpose* of Π_C.

Sometimes we write simply Π and Π' for them, when there is no fear of confusion. We consider $\Pi + \Pi'$ as a closed reduced subscheme of $C \times C$.

The word *point* will mean a closed point, unless otherwise stated. For a scheme (or a morphism) Z over a discrete valuation ring, Z_η denotes its *generic fibre* and Z_s its *special fibre*. But we always abbreviate the subscript "η" for points of generic fibres. Let X be an arbitrary scheme. For any irreducible closed subscheme Y of X, $\mathcal{O}_{X,Y}$ denotes the *local ring* of X at the generic point of Y. If X is integral, $K(X)$ denotes the *function field* of X. For any local ring A, $\hat{A}$ denotes the *completion* of A with respect to the maximal ideal of A. By abuse of language, we shall consider any non-zero integer as a *divisor* of ∞.

We shall use the word "*signature*" for curves over any field, in analogy with that for compact Riemann surfaces or Fuchsian groups. In general, let X be a curve over a field F. A *signature* on X is a $\{1, 2, \cdots; \infty\}$-valued function $e = e(P)$ defined on the set of all points P of X, such that $e(P) = 1$ except for a finite number of points of X. Let F' be a field containing F. Put $X' = X \otimes_F F'$. Then any signature on X can be extended naturally to a signature on X'. We shall use the same notation for it.

DEFINITION 1. We say that a covering $f: Y \longrightarrow X$ over F is admissible with respect to a signature e on X, if for each $P \in Y$, the ramification index of P divides $e(f(P))$.

Let A be any normal ring. A *system of three normal schemes* over A is a system $\mathcal{U} = \{U_1 \xleftarrow{\phi_1} U_0 \xrightarrow{\phi_2} U_2\}$, where U_i $(i = 0, 1, 2)$ are normal schemes over A and ϕ_1, ϕ_2 are finite A-morphisms. If $\mathcal{U} = \{U_1 \xleftarrow{\phi_1} U_0 \xrightarrow{\phi_2} U_2\}$, and $\mathcal{U}^*=\{U_1^*\xleftarrow{\phi_1^*}U_0^*\xrightarrow{\phi_2^*}U_2^*\}$ are systems of three normal schemes over A, a *finite morphism* $\mathcal{F}:\mathcal{U}^*\longrightarrow\mathcal{U}$ is a triple $\mathcal{F}=(f_1, f_0, f_2)$ of three finite A-morphisms $f_i: U_i^*\longrightarrow U_i$ $(i=0, 1, 2)$ satisfying the following two properties;

(i) $f_i\circ\phi_i^*=\phi_i\circ f_0$ $\quad(i=1, 2)$,
(ii) $K(U_0^*)\simeq K(U_i^*)\otimes_{K(U_i)}K(U_0)$ $\quad$ (canonically; $i=1, 2$).

When $\mathcal{F}$ is a finite morphism as above, we say that the pair $(\mathcal{U}^*, \mathcal{F})$ is a *finite covering* of $\mathcal{U}$ over A.

Now we shall give some brief review of definitions related to congruence relations (cf. [8] § 1). For a curve C over $\boldsymbol{F}_q$, we call $\mathcal{C}$ a *lifting* of C to R, if $\mathcal{C}$ is a proper smooth R-scheme such that $\mathcal{C}\otimes_R\boldsymbol{F}_q=C$. A pair $(\mathcal{C}, \mathcal{T})$ is called a *congruence relation* over R, if

(i) $\mathcal{C}$ is a lifting of a curve $C=\mathcal{C}_s$ over $\boldsymbol{F}_q$ to R;
(ii) $\mathcal{T}$ is an R-flat integral closed subscheme of $\mathcal{C}\times_R\mathcal{C}$, such that

$$\mathcal{T}\times_{(\mathcal{C}\times\mathcal{C})}(C\times C)=\Pi+\Pi'.$$

A congruence relation $(\mathcal{C}, \mathcal{T})$ (or simply $\mathcal{T}$) is called *symmetric*, if ${}^t\mathcal{T}=\mathcal{T}$, where ${}^t\mathcal{T}$ is the transpose of $\mathcal{T}$. Throughout this paper, all congruence relations will be assumed symmetric, and hereafter we omit the word "*symmetric*".

The ring of global sections $\Gamma(C, \mathcal{O}_C)$ of C must be $\boldsymbol{F}_q$ or $\boldsymbol{F}_{q^2}$. We say that a congruence relation $(\mathcal{C}, \mathcal{T})$ belongs to Case 1 if $\Gamma(C, \mathcal{O}_C)=\boldsymbol{F}_q$, and Case 2 if $\Gamma(C, \mathcal{O}_C)=\boldsymbol{F}_{q^2}$.

If $P\in\Pi\cap\Pi'$, the degree of P over $\boldsymbol{F}_q$, denoted $\deg P$, is at most 2. The two projections $\Pi+\Pi'\longrightarrow C$ induce one and the same bijection

$$\{\text{points } P \text{ of } \Pi\cap\Pi'\}\approx\{\text{closed points } Q \text{ of } C \text{ with } \deg Q\leq 2\}.$$

A point $Q\in C$ with $\deg Q\leq 2$ is called *special* (with respect to $\mathcal{T}$), if the local ring $\mathcal{O}_{\mathcal{T},P}$ of the corresponding point P is normal. We also call P special. A point $Q\in C$ or $P\in\Pi+\Pi'$ which is not special is called *ordinary*. Note that all points of C of degree >2 are ordinary.

Denote by $\mathcal{T}^n$ the *normalization* of $\mathcal{T}$. Let φ (resp. ${}^t\varphi$) be the *composite* of the first (resp. second) projection of $\mathcal{T}$ to $\mathcal{C}$ and the normalization map. Put

$$\mathcal{X}=\{\mathcal{C}\xleftarrow{\varphi}\mathcal{T}^n\xrightarrow{{}^t\varphi}\mathcal{C}\}.$$

This system is a system of three normal schemes over R. By definition, $\mathcal{X}$ is called a *CR-system* over R. Congruence relations and CR-systems are equivalent notions.

DEFINITION 2. A point $P\in\mathcal{T}_\eta^n$ is called *quasi-symmetric*, if $\varphi_\eta(P)={}^t\varphi_\eta(P)$.

The special fibre $\mathcal{T}_s^n$ consists of two irreducible components which can be identified with Π and Π'. These two components meet only at special points. We also call such a point special and all other points of $\mathcal{T}_s^n$ ordinary. For any ordinary point $P_s\in\mathcal{T}_s^n$, there exists a unique generization $P\in\mathcal{T}_\eta^n$ of P_s such that P is quasi-symmetric. By definition, P (resp. $\varphi_\eta(P)$) is the canonical lifting of P_s (resp. $\varphi_s(P_s)$). For more precise definition, see [8] § 3.

For a congruence relation $(\mathcal{C},\mathcal{T})$, the special points defined above can be considered distinctive points of $\mathcal{C}_s$. On the other hand, the branch points of φ_η stand out among the points of $\mathcal{C}_\eta$. The ramification of φ_η naturally determines a signature on $\mathcal{C}_\eta$ as follows. Let $\mathfrak{R}$ be a set of (not necessarily all) branch points of φ_η.

DEFINITION 3. For $Q\in\mathcal{C}_\eta$, $\mathfrak{E}(Q)$ denotes the greatest common divisor of all ramification indices $e(P/Q)$ of points $P\in\mathcal{T}_\eta^n$ lying above Q which are not quasi-symmetric. (If all points of $\mathcal{T}_\eta^n$ lying above Q are quasi-symmetric, we put $\mathfrak{E}(Q)=\infty$.) Then the signature on $\mathcal{C}_\eta$ associated with $\mathfrak{R}$ is a signature $\mathfrak{e}$ on $\mathcal{C}_\eta$, defined by:

$$\begin{aligned}\mathfrak{e}(Q)&=\mathfrak{E}(Q), && \text{if } Q\in\mathfrak{R},\\ \mathfrak{e}(Q)&=1\ , && \text{if } Q\notin\mathfrak{R}.\end{aligned}$$

Note that, in the case of the Kronecker congruence relations of the elliptic modular curve, above defined signature $\mathfrak{e}$ coincides with that defined by the modular group. We shall now describe $\mathfrak{e}$ explicitly. Put

$$\varphi_\eta^*(Q)=e_1P_1+\cdots+e_rP_r,\quad Q\in\mathfrak{R}.$$

I. *The case where Q_s is special.* There exists at most one quasi-symmetric point of $\mathcal{T}_\eta^n$ lying above Q. If P_1 is quasi-symmetric, P_1 is symmetric, P_1/Q is unramified and $\deg P_1=\deg Q$ over k. (See § 4 Lemma 4.1 and its Corollary.)

(i) If P_1 is quasi-symmetric,

$$\mathfrak{e}(Q)=(e_2,\cdots,e_r),$$

where ( ) denotes the greatest common divisor. Note that $\mathfrak{e}(Q)$ is a divisor of q, hence a power of p.

(ii) If there exist no quasi-symmetric points of $\mathcal{T}_\eta^n$ lying above Q,

$$\mathfrak{e}(Q)=(e_1, \cdots, e_r).$$

II. *The case where* Q_s *is ordinary.* Assume that $(P_1)_s \in \Pi$ $(e_1=1)$ and $(P_2)_s, \cdots, (P_r)_s \in \Pi'$. Furthermore, if Q is the canonical lifting of Q_s, suppose that P_2 is the canonical lifting of $(P_2)_s = \cdots = (P_r)_s$.

(i) If Q is not the canonical lifting of Q_s,

$$\mathfrak{e}(Q)=1.$$

(ii) If Q is the canonical lifting of Q_s and $r>2$ $(e_i<q)$,

$$\mathfrak{e}(Q)=(e_3, \cdots, e_r).$$

(iii) If Q is the canonical lifting of Q_s and $r=2$ $(e_2=q)$,

$$\mathfrak{e}(Q)=\infty.$$

After the manner of the modular curves, we call Q a *cusp* when $\mathfrak{e}(Q)=\infty$, and *elliptic* when $1<\mathfrak{e}(Q)<\infty$.

We shall always impose the following conditions on a set of branch points of φ_η.

DEFINITION 4. A set $\mathcal{R}$ consisting of branch points of φ_η is called *regular*, if $\mathcal{R}$ satisfies the following conditions:

(i) if $Q, Q' \in \mathcal{R}$ and $Q \neq Q'$, then $Q_s \neq Q'_s$,

(ii) $\deg Q = \deg Q_s$, for all $Q \in \mathcal{R}$.

REMARK. In the case of the elliptic modular curve, if $p=2$ or 3, $j=0$ and 12^3 have the same specialization, but if $p \geq 5$, $j=0, 12^3, \infty$ satisfy the above conditions.

Let $\mathcal{R}$ be a regular set of branch points of φ_η. Put $\mathcal{R}_s=\{Q_s | Q \in \mathcal{R}\}$.

DEFINITION 3^s. The signature on C associated with $\mathcal{R}$ (or the specialization of $\mathfrak{e}$) is a signature $\mathfrak{e}_s$ on C defined by:

$$\begin{aligned} \mathfrak{e}_s(Q_s) &= \mathfrak{e}(Q), && \text{if } Q_s \in \mathcal{R}_s, \\ \mathfrak{e}_s(Q_s) &= 1, && \text{if } Q_s \notin \mathcal{R}_s. \end{aligned}$$

We say that a finite covering $(\mathcal{X}^*, \mathcal{F})$ of $\mathcal{X}$ over R is a *finite CR-*

covering of $\mathcal{X}$, if $\mathcal{X}^*=\{\mathcal{C}^*\xleftarrow{\varphi^*}\mathcal{T}^*\xrightarrow{{}^t\varphi^*}\mathcal{C}^*\}$ is another CR-system over R, and $f_1=f_2$, where $\mathcal{F}=(f_1,f_0,f_2)$. Then finite CR-coverings of $\mathcal{X}$ form a subcategory of the category of finite coverings of $\mathcal{X}$ over R. By definition, a CR-covering $(\mathcal{X}^*,\mathcal{F})$ is *admissible* with respect to a signature e on $\mathcal{C}_\eta$, if $(f_1)_\eta$ is admissible with respect to e.

Let $(\mathcal{C},\mathcal{T})$ be a congruence relation over R and $\mathcal{X}$ the associated CR-system. Put $C=\mathcal{C}_s$. Let $\mathfrak{R}$ be a regular set of branch points of φ_η and $\mathfrak{e}$ the signature associated with $\mathfrak{R}$. Then our first result is the following

THEOREM 1. *The following two categories are canonically equivalent*:

(i) *Tamely ramified finite coverings $f:C^*\longrightarrow C$ over $\boldsymbol{F}_q$, admissible with respect to $\mathfrak{e}_s$, such that all closed points of C^* lying above the special points of C are of degree ≤ 2 over $\boldsymbol{F}_q$.*

(ii) *Finite CR-coverings $(\mathcal{X}^*,\mathcal{F})$ of $\mathcal{X}$, admissible with respect to $\mathfrak{e}$, such that $(f_1)_s$ is tamely ramified.*

Now, to each CR-system $\mathcal{X}$, we shall associate a CR-system $\mathcal{X}^+$ belonging to Case 2, in the following way. When $\mathcal{X}$ belongs to Case 2, we put $\mathcal{X}^+=\mathcal{X}$. When $\mathcal{X}$ belongs to Case 1, $\mathcal{X}^+$ is obtained by the twisted base change $\otimes_R R^{(2)}$ defined as follows. Let ι be the involutive automorphism of $R^{(2)}/R$. Then $\mathcal{X}^+=\{\mathcal{C}^+\xleftarrow{\varphi_1^+}\mathcal{T}^+\xrightarrow{\varphi_2^+}\mathcal{C}^+\}$ is defined by:

$$\mathcal{C}^+=\mathcal{C}\otimes_R R^{(2)},\quad \mathcal{T}^+=\mathcal{T}^n\otimes_R R^{(2)},$$
$$\varphi_1^+=\varphi\times 1,\quad \varphi_2^+={}^t\varphi\times\iota.$$

Put $X_i=\mathcal{C}^+\otimes_{R^{(2)}}\bar{k}$ $(i=1,2)$, $X_0=\mathcal{T}^+\otimes_{R^{(2)}}\bar{k}$, and $\varphi_i=\varphi_i^+\otimes_{R^{(2)}}\bar{k}$ $(i=1,2)$. Consider the system

$$\tilde{\mathcal{X}}=\mathcal{X}^+\otimes\bar{k}=\{X_1\xleftarrow{\varphi_1}X_0\xrightarrow{\varphi_2}X_2\}.$$

By definition, a finite covering $(\mathcal{Y},\mathcal{F})$ of $\tilde{\mathcal{X}}$ is *admissible* with respect to a signature e on $\mathcal{C}_\eta$, if f_i $(i=1,2)$ are admissible with respect to e, where $\mathcal{F}=(f_1,f_0,f_2)$. To compare coverings of C with those of $\tilde{\mathcal{X}}$, we replace C by C^+ which is defined to be $C\otimes\boldsymbol{F}_{q^2}$ in the Case 1, and C in the Case 2. Then our second result is the following

THEOREM 1′. *Suppose that there exists at least one special point Q_s, such that φ_η is unramified at all generizations of Q_s. Then the following two categories are canonically equivalent*:

(i) *Tamely ramified finite coverings $f:C^*\longrightarrow C^+$ over $\boldsymbol{F}_{q^2}$, admissible with respect to $\mathfrak{e}_s$, such that all points of C^* lying above the special points* *of* C^+ *are* $\boldsymbol{F}_{q^2}$*-rational.*

(ii) *Finite coverings* $(\mathcal{Y}, \mathcal{F})$ *of* $\tilde{\mathcal{X}}$ *over* $\bar{k}$, *admissible with respect to* $\mathfrak{e}$, *satisfying the condition that, for every point* P *of* Y_i $(i=1,2)$, *the ramification index of* P *is prime to* p, *where* $\mathcal{Y}=\{Y_1 \longleftarrow Y_0 \longrightarrow Y_2\}$.

REMARK. Let $Q \in C$ be a special point with respect to $\mathcal{T}$. Then φ_η is unramified at all generizations of Q if and only if Q is special with respect to $\mathcal{T}\otimes(R/(\pi^2))$ in the sense that $\mathcal{T}\otimes(R/(\pi^2))$ cannot be divided into two $R/(\pi^2)$-flat proper closed subschemes at Q. If the genus of C is not smaller than 2 and $q=p$, $\mathcal{T}\otimes(R/(\pi^2))$ has at least one special point by [10] Theorem 2. Therefore, in this case the assumption in Theorem 1′ is automatically satisfied.

The notion of a signature $\mathfrak{e}$ on C_η associated with $\mathcal{R}$ is an extension of that on the modular curve. We shall also show that, under somewhat stronger conditions, any finite covering $(\mathcal{Y}, \mathcal{F})$ of $\tilde{\mathcal{X}}$ is necessarily admissible with respect to $\mathfrak{e}$.

PROPOSITION 1. *Suppose that specializations of any two branch points of* φ_η *are mutually distinct. Let* $(\mathcal{Y}, \mathcal{F})$ *be a finite Galois covering of* $\tilde{\mathcal{X}}$, *such that* f_i $(i=1,2)$ *are ramified only at points belonging to* $\mathcal{R}$. *Then* $(\mathcal{Y}, \mathcal{F})$ *is admissible with respect to* $\mathfrak{e}$.

2. Liftings of congruence relations

In this section we shall investigate the possibility of "*pull-back*" of congruence relations. We adopt the same notation and definitions as in § 1. Let $(C, \mathcal{T})$ be a congruence relation over R and $\mathcal{X}=\{C \xleftarrow{\varphi} \mathcal{T}^n \xrightarrow{{}^t\varphi} C\}$ the associated CR-system. Recall that $C=C_s$, $\mathcal{R}$ is a regular set of branch points of φ_η and $\mathfrak{e}$ is the signature associated with $\mathcal{R}$.

Let $f: C^* \longrightarrow C$ be a finite covering of curves over $\boldsymbol{F}_q$. A finite covering $\tilde{f}: \mathcal{C}^* \longrightarrow \mathcal{C}$ over R is called a *lifting* of f to R, if $\mathcal{C}^*$ is a lifting of C^* to R and $\tilde{f}_s=f$.

DEFINITION 2.1. A congruence relation $\mathcal{T}^*$ on $\mathcal{C}^* \times \mathcal{C}^*$ is called an extension of $\mathcal{T}$ on $\mathcal{C}^* \times \mathcal{C}^*$ with respect to $\tilde{f}$, if $(\tilde{f}\times\tilde{f})(\mathcal{T}^*)=\mathcal{T}$.

This condition is equivalent to saying that the pair consisting of a CR-system $\mathcal{X}^*$ associated with $(\mathcal{C}^*, \mathcal{T}^*)$ and a morphism $\mathcal{F}: \mathcal{X}^* \longrightarrow \mathcal{X}$ induced from $\tilde{f}$ is a CR-covering of $\mathcal{X}$.

The purpose of this section is to prove the following

PROPOSITION 2. *Let $f: C^* \longrightarrow C$ be a tamely ramified finite covering over F_q which is admissible with respect to $\mathfrak{e}_s$, satisfying the condition that all closed points of C^* lying above the special points of C are of degree ≤ 2. Then there exist a unique lifting $\tilde{f}: \mathcal{C}^* \longrightarrow \mathcal{C}$ of f to R such that $\tilde{f}_\eta$ is admissible with respect to $\mathfrak{e}$, and a unique extension $\mathcal{T}^*$ on $\mathcal{C}^* \times \mathcal{C}^*$ of $\mathcal{T}$ with respect to $\tilde{f}$.*

We begin with local calculations. Let Q be a point of $\mathcal{C}_\eta$ such that $\deg Q = \deg Q_s$. By a suitable choice of a prime element x of Q, we have an isomorphism

$$\hat{\mathcal{O}}_{\mathcal{C}, Q_s} \simeq R'[[x]],$$

were $R' = R^{(d)}$ with $d = \deg Q$. Let $f(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + x^n$ ($a_0, \cdots, a_{n-1} \in \pi R'$) be an irreducible polynomial in x. Then $(f(x))$ is a prime ideal of $R'[[x]]$ of height *one* different from (π). Conversely, every prime ideal of height *one* different from (π) of $R'[[x]]$ must be generated by such an irreducible polynomial in x. We identify x with $\varphi^*(x)$. Put $y = {}^t x$. Let P_s be a point of $\mathcal{T}_s^n$ such that $\varphi_s(P_s) = Q_s$, and put

$$A = \hat{\mathcal{O}}_{\mathcal{T}^n, P_s}.$$

Then we see that:

(i) if Q_s is ordinary,

$$A \simeq \begin{cases} R'[[x]] & (\text{if } P_s \in \Pi) \\ R'[[y]] & (\text{if } P_s \in \Pi'), \end{cases}$$

(ii) if Q_s is special,

$$A \simeq R'[[X, Y]]/(XY - a\pi^l), \quad a \in (R')^\times,$$

where

$$\begin{aligned} X &= x - y^q + \pi F(x, y) \\ Y &= y - x^q + \pi G(x, y), \end{aligned} \tag{1}$$

with some $F, G \in R'[[x, y]]$. Note that (1) implies:

$$\begin{aligned} x &= X + Y^q + X^{q^2} + \cdots + \pi \Phi(X, Y) \\ y &= Y + X^q + Y^{q^2} + \cdots + \pi \Psi(X, Y), \end{aligned} \tag{2}$$

with some $\Phi, \Psi \in R'[[X]] + R'[[Y]]$.

Since there exists a symmetric local equation for $\mathcal{T}$ at Q_s ([10] p. 466, Proof of (II)), we may assume that $G={}^tF$ and $\Psi={}^t\Phi$. As usual, we may take X and Y so that $XY=\pi^l$, but in order to preserve the symmetry between X and Y, some unit a is necessary.

The proof of Proposition 2 is based on the following

MAIN LEMMA A. *Let e be any positive divisor of $\mathfrak{e}(Q)$ prime to p. By a suitable choice of eth roots s of x and t of y, $B=A[s,t]$ is expressed as follows.*

(i) *If Q_s is ordinary and $P_s\in\Pi$,*

$$B\simeq R'[[s]],\qquad t\equiv s^q \bmod (\pi);$$

(i)′ *If Q_s is ordinary and $P_s\in\Pi'$,*

$$B\simeq R'[[t]],\qquad s\equiv t^q \bmod (\pi);$$

(ii) *If Q_s is special,*

$$\begin{aligned} &B\simeq R'[[S,T]]/(ST-b\pi^{l'}),\qquad b\in(R')^\times,\\ &S^e=X,\quad T^e=Y,\\ &s\equiv t^q \bmod (\pi,S),\\ &t\equiv s^q \bmod (\pi,T).\end{aligned}$$

PROOF. (i) *The case where Q_s is ordinary.* It is easy to see that the proof in the case $P_s\in\Pi$ and that in the case $P_s\in\Pi'$ are symmetric. Therefore, we may assume that $P_s\in\Pi'$ and Q is the canonical lifting of Q_s. Recall that $\varphi_\eta^*(Q)=P_1+e_2P_2+e_3P_3+\cdots+e_rP_r$, where $(P_1)_s\in\Pi$, $(P_2)_s=\cdots=(P_r)_s=P_s$ and P_2 is the canonical lifting of P_s. Then we have $\mathfrak{e}(Q)=(e_3,\cdots,e_r)$ or $\mathfrak{e}(Q)=\infty$ according as $r>2$ or $r=2$. Since y is a prime element of ${}^tQ$, y is also a prime element of P_2 and we can take irreducible polynomials in y as prime elements of P_i $(i=3,\cdots,r)$.

Now we consider the decomposition of x into prime elements in $A=\hat{\mathcal{O}}_{\mathcal{T}^n,P_s}$. Since P_s is ordinary, x is of the form

$$x=y^q+\pi g(y)$$

in A with $g(y)\in R'[[y]]$. By the Weierstrass' lemma, we have

$$x=\varepsilon(a_0+a_1y+\cdots+a_{q-1}y^{q-1}+y^q),$$

with $\varepsilon\in 1+\pi R'[[y]]$ and $a_0,\cdots,a_{q-1}\in\pi R'$. Hence, in view of the decomposition of Q in $\mathcal{T}^n_\eta$, we obtain

$$x=\varepsilon y^{e_2}f_3(y)^{e_3}\cdots f_r(y)^{e_r}, \tag{3}$$

where

$$f_i(y)=a_{i,0}+a_{i,1}y+\cdots+a_{i,n_i-1}y^{n_i-1}+y^{n_i},$$

with $a_{i,0},\cdots,a_{i,n_i-1}\in\pi R'$, are irreducible polynomials ($i=3,\cdots,r$). Note that $e_2+\sum_{i=3}^{r}e_in_i=q$. By the definition of $\mathfrak{e}(Q)$, e divides e_i ($i=3,\cdots,r$). Put $e_i=ee_i'$ ($i=3,\cdots,r$). Furthermore, since $\varepsilon\equiv1\bmod(\pi)$, ε has an eth root in $R'[[y]]$. Denote by ε^* the eth root of ε in $R'[[y]]$ such that $\varepsilon^*\equiv1\bmod(\pi)$. Let t be any eth root of y. Then it follows from (3) that

$$x=(\varepsilon^*t^{e_2}f_3(y)^{e_3'}\cdots f_r(y)^{e_r'})^e.$$

We put

$$s=\varepsilon^*t^{e_2}f_3(y)^{e_3'}\cdots f_r(y)^{e_r'}\in R'[[t]]. \tag{4}$$

Then $s^e=x$ holds. As $y=t^e$ and $e_2+e\sum_{i=3}^{r}e_i'\cdot\deg f_i=q$, the right hand side of (4) is congruent to $t^q\bmod(\pi)$. Therefore, we conclude that $B\simeq R'[[t]]$ and $s\equiv t^q\bmod(\pi)$.

(ii) *The case where Q_s is special.* As e is prime to p, we may assume that there exist no quasi-symmetric points of $\mathcal{T}^n_\eta$ lying above Q. In the same manner as in the proof of Lemma 3 of Ihara [7] pp. 321-2, x can be decomposed into prime elements in A as follows. By (2) and Weierstrass' lemma, we have

$$\begin{aligned}Yx&=Y(X+Y^q+X^{q^2}+\cdots+\pi\Phi(X,Y))\\&=\eta(b_0+b_1Y+\cdots+b_qY^q+Y^{q+1})\end{aligned} \tag{5}$$

in A, with $\eta\in R'[[X]]+R'[[Y]]$ and $b_0,\cdots,b_q\in\pi R'$ satisfying the conditions that

$$\eta\equiv1+Y^{q^3-q}+Y^{q^5-q}+\cdots\bmod(\pi,X),$$
$$b_0\equiv a\pi^l\bmod(\pi^{l+1}).$$

The factorization of $b_0+b_1Y+\cdots+b_qY^q+Y^{q+1}$ into irreducible polynomials gives the decomposition of Q in $\mathcal{T}^n_\eta$. Hence we have

$$Yx=\eta h_1(Y)^{e_1}\cdots h_r(Y)^{e_r} \tag{6}$$

in A, where

$$h_i(Y)=b_{i,0}+b_{i,1}Y+\cdots+b_{i,m_i-1}Y^{m_i-1}+Y^{m_i},$$

with $b_{i,0},\cdots,b_{i,m_i-1}\in\pi R'$, are irreducible polynomials $(i=1,\cdots,r)$, and $\sum_{i=1}^{r}e_im_i=q+1$ holds. By the definition of $e(Q)$, e divides each e_i $(i=1,\cdots,r)$. Put $e_i=ee_i'$ $(i=1,\cdots,r)$. Since $\eta\equiv 1 \bmod (\pi, X, Y)$, η has an eth root in A. Denote by η^* the eth root of η such that $\eta^*\equiv 1 \bmod (\pi, X, Y)$. Then from the equation (6), we obtain

$$Yx=(\eta^*h_1(Y)^{e_1'}\cdots h_r(Y)^{e_r'})^e. \tag{7}$$

Similarly, by the symmetry of X and Y, we have

$$Xy=({}^t\eta^*h_1^t(X)^{e_1'}\cdots h_r^t(X)^{e_r'})^e. \tag{8}$$

Let s (resp. t) be an eth root of x (resp. y), and put

$$\begin{aligned} S&=t^{-1}\,{}^t\eta^*h_1^t(X)^{e_1'}\cdots h_r^t(X)^{e_r'}\in t^{-1}A\\ T&=s^{-1}\eta^*h_1(Y)^{e_1'}\cdots h_r(Y)^{e_r'}\in s^{-1}A. \end{aligned} \tag{9}$$

Then, by the equations (7) and (8), we see that $S^e=X$, $T^e=Y$ and $(ST)^e=XY=a\pi^l$. As can be easily seen from the equations (5) and (6), we have

$$\prod_{i=1}^{r}b_{i,0}^{e_i}=(\prod_{i=1}^{r}b_{i,0}^{e_i'})^e\equiv a\pi^l \bmod (\pi^{l+1}).$$

Hence e divides l and a has an eth root in R'. If we put $l=el'$, we obtain $ST=b\pi^{l'}$ with $b\in R'$ such that $b^e=a$. Furthermore, we get

$$\prod_{i=1}^{r}b_{i,0}^{e_i'}=b_0'b\pi^{l'},$$

with $b_0'\in(R')^\times$. Therefore we have

$$Ts=\eta^*(b_0'b\pi^{l'}+b_1'Y+\cdots+Y^{q+1/e})=\eta^*(b_0'ST+b_1'T^e+\cdots+T^{q+1}),$$

and hence

$$s=\eta^*(b_0'S+b_1'T^{e-1}+\cdots+T^q), \tag{10}$$

where the right hand side is congruent to $\eta^*(b_0'S+T^q) \bmod (\pi)$. Similarly, we have

$$t={}^t\eta^*(b_0''T+\cdots+S^q). \tag{11}$$

It follows immediately from (10) and (11) that $B=A[s,t]$ coincides with $R'[[S,T]]/(ST-b\pi^{l'})$.

Now we prove the last congruences. Note that $y-x^q=t^e-s^{qe}\in(\pi,T)$ and $x-y^q=s^e-t^{qe}\in(\pi,S)$. It follows from this and $ST\equiv 0 \bmod (\pi)$ that

$$t-\zeta_1 s^q\equiv 0 \bmod (\pi,T)$$
$$s-\zeta_2 t^q\equiv 0 \bmod (\pi,S)$$

with $\zeta_1,\zeta_2\in R'$ such that $\zeta_1^e=\zeta_2^e=1$. Therefore, replacing t by $\zeta_1 t$, we obtain

$$t-s^q\equiv 0 \bmod (\pi,T).$$

On the other hand, in view of (10) and (11), it holds that

$$t-s^q\equiv({}^t\eta^*-\eta^{*q}b_0^{\prime q})S^q \bmod (\pi,T)$$
$$s-t^q\equiv(\eta^*-{}^t\eta^{*q}b_0^{\prime\prime q})T^q \bmod (\pi,S).$$

Hence $t-s^q\equiv 0 \bmod (\pi,T)$ implies $s-t^q\equiv 0 \bmod (\pi,S)$. This completes the proof of Main Lemma A.

We now begin the proof of Proposition 2. First note that the unique liftability of tamely ramified coverings of C has already been established in Grothendieck-Murre [4].

LEMMA 2.1. (Grothendieck-Murre) *Let $f:C^*\longrightarrow C$ be a tamely ramified finite covering over F_q, which is ramified only at points of $\mathfrak{R}_s$. Then there exists a unique lifting $\tilde f:\mathcal{C}^*\longrightarrow\mathcal{C}$ of f to R, which is ramified only at prime divisors of $\mathcal{C}$ corresponding to points of $\mathfrak{R}$. Furthermore, for each $P\in\mathcal{C}_\eta^*$ such that $\tilde f_\eta(P)\in\mathfrak{R}$, the ramification index of P is equal to that of P_s.*

Let $\tilde f:\mathcal{C}^*\longrightarrow\mathcal{C}$ be the lifting of f to R as in the above lemma. Put $\Pi^*=\Pi_{C^*}$. We shall show that our problem is local: namely, for each $P\in\Pi^*+\Pi^{*\prime}$, we only have to construct a local extension $\mathcal{T}_P^*$ of $\mathcal{T}$ with respect to $\tilde f$ in a neighbourhood of P. For this purpose, we require the uniqueness of local extension of $\mathcal{T}$.

LEMMA 2.2. *For each $P\in\Pi^*+\Pi^{*\prime}$, there exists at most one extension $\mathcal{T}_P^*$ of $\mathcal{T}$ at P with respect to $\tilde f$.*

PROOF. Let $\hat K$ (resp. $\hat K^*$) be the completion of $K(\mathcal{C})$ (resp. $K(\mathcal{C}^*)$) with respect to the valuation defined by C (resp. C^*). Then $\mathcal{T}$ determines a Frobenius σ of $\hat{K}$ in the sense of [11] p. 238, Definition 1 (cf. also [11] p. 247). A local extension $\mathcal{T}_P^*$ of $\mathcal{T}$ also determines a Frobenius of $\hat{K}^*$ extending σ. Then the lemma follows from the uniqueness of the extension of σ to $\hat{K}^*$.

In consequence of Lemma 2.2, we can glue local extensions of $\mathcal{T}$.

LEMMA 2.3. *Suppose that, for each $P\in\Pi^*+\Pi^{*\prime}$, there exists an extension $\mathcal{T}_P^*$ of $\mathcal{T}$ at P with respect to $\tilde{f}$. Then there exists a unique extension $\mathcal{T}^*$ of $\mathcal{T}$ on $C^*\times C^*$ with respect to $\tilde{f}$.*

Now we shall construct an extension $\mathcal{T}_P^*$ of $\mathcal{T}$ at each point $P\in\Pi^*+\Pi^{*\prime}$. Put $(f\times f)(P)=Q\in\Pi+\Pi'$, $\mathrm{pr}_1(P)=P_1$ and $\mathrm{pr}_1(Q)=Q_1$. Take prime elements x of Q_1 and u of P_1, so that $\hat{\mathcal{O}}_{C,Q_1}\simeq R'[[x]]$ and $\hat{\mathcal{O}}_{C^*,P_1}\simeq R''[[u]]$, respectively. Then we may assume that $x=\alpha u'^e$ and $u'=\varepsilon u$, with $\alpha\in(R'')^\times$ and $\varepsilon\in R''[[u]]^\times$. Put $y={}^tx$, $v'={}^tu'$ and $A=\mathcal{O}_{\mathcal{T}^n,Q'}$ for $Q'\in\mathcal{T}_s^n$ lying above Q. In order to apply Main Lemma A to the construction of $\mathcal{T}_P^*$, it is necessary to extend the constant ring of A to R''. Let σ be the Frobenius automorphism of R''/R. Put $x'=\alpha^{-1}x$ and $y'=(\alpha^\sigma)^{-1}y$ (resp. $(\alpha^{\sigma^{-1}})^{-1}y$) if $P\in\Pi^*$ (resp. $\Pi^{*\prime}$). Then it is easily checked that replacing A by $A'=A\otimes_{R'}R''$ and x, y by x', y', Main Lemma A can be applied. Take eth roots s of x' and t of y' as in Main Lemma A and put $B=A'[s,t]$. Define an R'-homomorphism Φ from $\mathcal{O}_P=\mathcal{O}_{C^*\times C^*,P}$ to B by:

$$\Phi:\mathcal{O}_P\hookrightarrow\hat{\mathcal{O}}_P\simeq R''[[u',v']]\longrightarrow B$$

where the first homomorphism is the natural inclusion, and the latter sends u' (resp. v') to s (resp. t). Then $\mathrm{Ker}\,\Phi$ is a prime ideal of $\mathcal{O}_P$ of height one. Hence it determines a prime divisor $D_{P,Q'}$ at P.

(i) *The case where $P\notin\Pi^*$ and $f(P)\notin\Pi$, or $P\notin\Pi^{*\prime}$ and $f(P)\notin\Pi'$.* There is only one point Q' of $\mathcal{T}_s^n$ lying above Q. If we put $\mathcal{T}_P^*=D_{P,Q'}$, $\mathcal{T}_P^*$ is an extension of $\mathcal{T}$ at P by Main Lemma A.

(i)′ *The case where $P\notin\Pi^*$ or $P\notin\Pi^{*\prime}$, but $f(P)\in\Pi\cap\Pi'$.* In this case there are two points of $\mathcal{T}_s^n$ lying above Q. Take $Q'\in\mathcal{T}_s^n$ lying above Q so that Q' belongs to the component lying above Π (resp. Π'), if $P\in\Pi^*$ (resp. $\Pi^{*\prime}$). Then $\mathcal{T}_P^*=D_{P,Q'}$ is an extension of $\mathcal{T}$ at P by Main Lemma A.

(i)″ *The case where $P\in\Pi^*\cap\Pi^{*\prime}$ and $f(P_1)$ is ordinary.* Let Q', Q'' be two points of $\mathcal{T}_s^n$ lying above Q. Then, in view of Main Lemma A, $\mathcal{T}_P^*=D_{P,Q'}=D_{P,Q''}$ is an extension of $\mathcal{T}$ at P.

(ii) *The case where $f(P_1)$ is special.* Put $\mathrm{Ker}\,\Phi=(h)$. Since B is isomorphic to $(\widehat{\mathcal{O}_P/(h)})$, P is an ordinary double point on the special fibre of $D_{P,Q'}$ by Main Lemma A. Furthermore, the reduction of h is a divisor of $(y-x^q)(x-y^q) \bmod (\pi)$, hence a unit multiple of $(u-v^q)(v-u^q) \bmod (\pi)$ by the last congruences in Main Lemma A. This completes the proof of Proposition 2.

3. Reduction

In this section we shall study the reduction of coverings of the geometric generic fibre of a CR-system to prove the rest of the theorems.

Let $(C, \mathcal{T})$ be a congruence relation over R and $\mathcal{X}^+$ the associated CR-system over $R^{(2)}$ defined in §1. Recall that $\tilde{\mathcal{X}}=\mathcal{X}^+\otimes\bar{k}=\{X_1\xleftarrow{\varphi_1}X_0\xrightarrow{\varphi_2}X_2\}$ is a system of three normal schemes (i.e. curves) over $\bar{k}$. Let $(\mathcal{Y}, \mathcal{F})$ be a finite covering of $\tilde{\mathcal{X}}$ over $\bar{k}$ with $\mathcal{Y}=\{Y_1\xleftarrow{\phi_1}Y_0\xrightarrow{\phi_2}Y_2\}$ and $\mathcal{F}=(f_1, f_0, f_2)$. Then the purpose of this section is to prove the following

PROPOSITION 3. *Suppose that there exists at least one special point Q_s of C, such that φ_η is unramified at all generizations of Q_s. Let $(\mathcal{Y}, \mathcal{F})$ be a finite covering of $\tilde{\mathcal{X}}$ which is an object of the category* (ii) *defined in Theorem* 1′. *Then there exists a unique covering $f: C^*\longrightarrow C^+$ over $R^{(2)}$, satisfying the following conditions*:

(i) *$Y_i=C^*\otimes\bar{k}$ $(i=1, 2)$ and $f_i=f\otimes\bar{k}$ $(i=1, 2)$,*

(ii) *C^* is smooth over $R^{(2)}$ and the specialization $f_s: C^*_s\longrightarrow C^+$ is a tamely ramified covering of C^+ over $\boldsymbol{F}_{q^2}$, such that all points of C^*_s lying above the special points of C^+ are $\boldsymbol{F}_{q^2}$-rational.*

The proof of Proposition 3 consists of two parts. We first prove the fact that Y_i $(i=1, 2)$ have good reductions and next deal with the $\boldsymbol{F}_{q^2}$-rationality.

MAIN LEMMA B. *Let $(\mathcal{Y}, \mathcal{F})$ be a finite covering of $\tilde{\mathcal{X}}$, satisfying the following conditions*:

(i) *if $Q, Q'\in X_1$ (resp. X_2) and f_1 (resp. f_2) is ramified at Q, Q', then $Q_s\neq Q'_s$,*

(ii) *all ramification indices with respect to f_1 (resp. f_2) are prime to p.*

Then Y_1 (resp. Y_2) has good reduction.

In the unramified case, the fact that Y_1 and Y_2 have good reductions is based on the following two results; (I) a criterion for the potential good reduction of unramified coverings of curves (Ihara-Miki [11]); (II) Zariski-Nagata "*purity of branch locus*" ([3] X 3.1). The former is also applicable to the ramified case, but the latter can not be applied directly to ramified coverings. We introduce the method used in Popp [12]. Denote by $\bar{R}$ the ring of integers of $\bar{k}$. In general, let Z be a proper smooth $\bar{R}$-scheme whose special fibre is a curve over $\bar{F}_p$. The following two lemmas are cited from [12] Zwölfte Vorlesung.

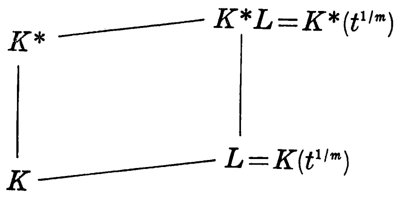
LEMMA 3.1. *Let $Q_1, \cdots, Q_n$ be points of Z_η whose specializations are all distinct. Then there exists a function t in $K(Z)$, such that the divisor of t is of the following form;*

$$(t)=P_1+P_2+\cdots+P_N-(Q_1+Q_2+\cdots+Q_n+\cdots+Q_N),$$

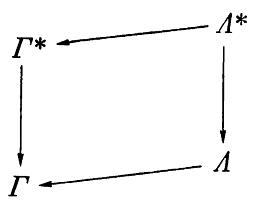
where $P_1, \cdots, P_N, Q_1, \cdots, Q_N$ are points of Z_η whose specializations are all distinct.

LEMMA 3.2. *Put $K=K(Z)$. Choose a function t on Z_η as in Lemma 3.1. Let m be any positive integer prime to p. Then the integral closure Z' of Z in $L=K(t^{1/m})$ is smooth over $\bar{R}$.*

PROOF OF MAIN LEMMA B. Put $K=K(X_1)$, $K^*=K(Y_1)$ and $\Gamma=\mathcal{C}^+\otimes_{R^{(2)}}\bar{R}$. Then $X_1=\Gamma\otimes_{\bar{R}}\bar{k}$. Denote by Γ^* the integral closure of Γ in K^*. Now we shall apply above lemmas to Γ and $\mathfrak{R}$. Choose a function $t\in K$ as in Lemma 3.1 and put $L=K(t^{1/m})$. Denote by Λ and Λ^* the integral closures of Γ in L and K^*L, respectively.



Function fields.



Schemes over $\bar{R}$.

Let V be the discrete valuation of K defined by Γ_s. By [11] Theorem 1B and the proof of Theorem 2A, V is unramified in K^*. By Lemma 3.2, V is also unramified in L for any positive integer m prime to p. Hence V must be unramified in K^*L. Therefore, the extension V_L of

V to L is unramified in K^*L/L. On the other hand, we can apply Abhyanker's lemma ([3] X 3.6) to K^*/L to conclude that, by a suitable choice of m prime to p, all discrete valuations of L trivial on $\bar{k}$ are unramified in K^*L/L. Therefore, by "*purity of branch locus*", Λ^* is étale over Λ. This implies that Λ^* is smooth over $\bar{R}$.

Now we shall show that the smoothness of Γ^* is deduced from that of Λ^*. As Λ^* is smooth over $\bar{R}$, its special fibre Λ_s^* is a smooth curve over $\bar{F}_p$. The covering $\Lambda^* \longrightarrow \Gamma^*$ is a finite Galois covering whose degree is prime to p. Let G be the automorphism group of Λ^* over Γ^*. Then G acts on Λ_s^* faithfully. Let $\{\operatorname{Spec} A^\lambda\}$ be an affine open covering of Λ^*. Put $A_s^\lambda = A^\lambda \otimes_R \bar{F}_p$ and $B_s^\lambda = \{a \in A_s^\lambda | a^\sigma = a, \forall \sigma \in G\}$. By the smoothness of Λ_s^*, A_s^λ is normal. Let b_s be any element of the quotient field of B_s^λ which is integral over B_s^λ. Then b_s is a fortiori integral over A_s^λ, hence contained in A_s^λ. Moreover, b_s is fixed by G. Hence b_s belongs to B_s^λ. This implies that B_s^λ is normal. Let Λ_s^{*G} be the scheme obtained by glueing the schemes $\operatorname{Spec} B_s^\lambda$, which is independent of the choice of affine open coverings of Λ^*. Then Λ_s^{*G} is normal, hence a smooth curve over $\bar{F}_p$. Since the order of G is prime to p, any element of B_s^λ can be lifted to a G-invariant element of A^λ. Indeed, for any element b_s of B_s^λ, take a lifting b of b_s to A^λ and put $b' = \frac{1}{|G|} \sum_{\sigma \in G} b^\sigma$. Then $b'^\sigma = b'$ for all $\sigma \in G$ and $b'_s = b_s$. Hence we obtain

$$\Lambda_s^{*G} = \Gamma_s^*.$$

This implies that Γ^* is smooth over $\bar{R}$.

Finally, as the conditions of f_1 and f_2 are symmetric, we can similarly prove that Y_2 has good reduction. This proves Main Lemma B.

Let V be as in the above proof. In consequence of the smoothness of Γ^* over $\bar{R}$, V is uniquely extended to a discrete valuation of K^*. Let k^u be the maximal unramified extension of k and R^u the ring of integers of k^u. Put $C^u = C^+ \otimes_{R^{(2)}} R^u$, $\mathcal{X}^u = \mathcal{X}^+ \otimes_{R^{(2)}} R^u$ and $K^u = K(C^u)$. Let M be the Galois closure of K^*/K^u. Then a discrete valuation of K is ramified in M/K if and only if it is ramified in K^*/K. Moreover, all ramification indices in M/K are prime to p. Therefore, by the same argument as in the above proof, V is uniquely extended to a discrete valuation of M. By [11] pp. 248-9, Proof of Theorem 2A, we obtain the following

COROLLARY. *Suppose that* f_i $(i=1, 2)$ *satisfy the conditions* (i) *and*

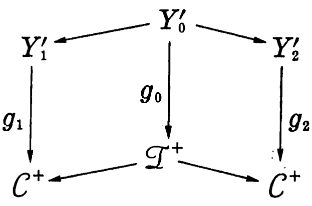
(ii) *of Main Lemma B. Then there exists a unique covering* $(\mathcal{Y}^u, \mathcal{F}^u)$ *of* $\mathcal{X}^u$ *over* R^u *such that*

$$(\mathcal{Y}^u, \mathcal{F}^u)\otimes_{R^u}\bar{k}=(\mathcal{Y}, \mathcal{F}).$$

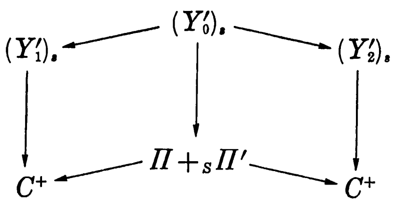
Let $(\mathcal{Y}^u, \mathcal{F}^u)$ be as in the above Corollary. Then we may assme that $(\mathcal{Y}^u, \mathcal{F}^u)$ is defined over a finite unramified extension R' of $R^{(2)}$ with residue field $F_{q'}$. Put $\mathcal{X}'=\mathcal{X}^+\otimes_{R^{(2)}}R'=\{X_1'\overset{\varphi_1'}{\longleftarrow}X_0'\overset{\varphi_2'}{\longrightarrow}X_2'\}$. Let $(\mathcal{Y}', \mathcal{F}')$ be a finite covering of $\mathcal{X}'$ over R' such that $(\mathcal{Y}', \mathcal{F}')\otimes_{R'}R^u=(\mathcal{Y}^u, \mathcal{F}^u)$. Put $\mathcal{Y}'=\{Y_1'\overset{\psi_1'}{\longleftarrow}Y_0'\overset{\psi_2'}{\longrightarrow}Y_2'\}$ and $\mathcal{F}'=(f_1', f_0', f_2')$. We first prove that $(f_i')_s$ $(i=1, 2)$ are defined over F_{q^2}.

LEMMA 3.3. *Let* $(\mathcal{Y}', \mathcal{F}')$ *be as above. Then there exists a unique finite covering* $f_s: C^*\longrightarrow C^+$ *over* F_{q^2}, *such that* $(Y_i')_s=C^*\otimes F_{q'}$ and $(f_i')_s=f_s\otimes F_{q'}$ $(i=1, 2)$.

PROOF. The proof closely follows that of Ihara [6] Proposition 4.2.1 and Lemma 4.2.6 in the unramified case. Denote by S the set of special points of C^+ and by $\Pi+_S\Pi'$ the join of Π and Π' crossing transversally at each (s, s^q) $(s\in S)$. Note that $(\mathcal{T}^+)_s=\Pi+_S\Pi'$. Let $\mathcal{G}=(g_1, g_0, g_2)$ be the composite of $\mathcal{F}'$ and the natural morphism $\mathcal{X}'=\mathcal{X}^+\otimes R'\longrightarrow\mathcal{X}^+$.



(over $R^{(2)}$)



(over F_{q^2})

Let $U\subset C^+$ be the open subscheme obtained by removing the closures of all branch points of $(\varphi_1^+)_\eta$. Put $U_i'=U$ $(i=1, 2)$, $U_0=(\varphi_1^+)^{-1}(U_1')\cap(\varphi_2^+)^{-1}(U_2')$, $V_0=g_0^{-1}(U_0)$, $U_i=\varphi_i^+(U_0)$ $(i=1, 2)$ and $V_i=\psi_i'(V_0)$ $(i=1, 2)$. The restrictions of g_i $(i=0, 1, 2)$ to V_i are all étale morphisms. Therefore, we can apply the argument used in [6] pp. 184–5, Proof of Lemma 4.2.6 to the following diagram

$$\begin{array}{ccccc} V_1 & \longleftarrow & V_0 & \longrightarrow & V_2 \\ \downarrow & & \downarrow & & \downarrow \\ U_1 & \longleftarrow & U_0 & \longrightarrow & U_2 \end{array}$$

to conclude that

$$(*) \qquad V_1 \times_{U_1} U_0 \simeq V_0 \simeq U_0 \times_{U_2} V_2 \qquad (\text{over } U_0).$$

Regard their special fibres as schemes over F_q. Since the restrictions of $(g_i)_s$ $(i=1, 2)$ to $(V_i)_s$ and those of $(\varphi_i^+)_s$ $(i=1, 2)$ to $(U_0)_s$ are all étale, $(V_i \times_{U_i} U_0)_s = (V_i)_s \times_{(U_i)_s} (U_0)_s$ $(i=1, 2)$ are isomorphic to the joins of $\Pi_{(V_i)_s}$ and $\Pi'_{(V_i)_s}$ crossing transversally above the double points of $\Pi +_S \Pi'$. Therefore, $(*)$ induces two isomorphisms $\Pi_{(V_1)_s} \longrightarrow \Pi_{(V_2)_s}$ over Π and $\Pi'_{(V_1)_s} \longrightarrow \Pi'_{(V_2)_s}$ over Π'. From them we obtain two isomorphisms

$$\varepsilon_1, \varepsilon_2 : (V_1)_s \longrightarrow (V_2)_s \qquad \text{over } U_s$$

such that

$$\varepsilon_2(y) = \varepsilon_1(y)^{q^2}$$

for any geometric points $y \in (V_1)_s$ lying above the special points of C^+. If we put $\varepsilon = \varepsilon_1^{-1} \circ \varepsilon_2$, we get

$$g_1 \circ \varepsilon = g_1, \quad \varepsilon(y) = y^{q^2}.$$

Since $(Y_i')_s$ $(i=1, 2)$ are algebraic curves over a field by Main Lemma B, $\varepsilon_1, \varepsilon_2$ and ε can be extended to global isomorphisms. By the assumption of Theorem 1′, U_s contains at least one special point. Therefore, by [6] Proposition 4.2.1, there exists a unique covering $f_s : C^* \longrightarrow C^+$ over F_{q^2}, such that $(Y_i')_s = C^* \otimes F_{q'}$ $(i=1, 2)$, and $(f_i')_s = f_s \otimes F_{q'}$ $(i=1, 2)$. This proves the lemma.

Let $f_s : C^* \longrightarrow C^+$ be as in Lemma 3.3. Now suppose that $(f_i)_\eta$ $(i=1, 2)$ are admissible with respect to $\mathfrak{e}$. Then it is easy to see that f_s is tamely ramified and admissible with respect to $\mathfrak{e}_s$. Furthermore, it follows immediately from Lemmas 3.2, 3.3 and the unique liftability of tamely ramified coverings (Lemma 2.1) that there exists a unique covering $(\mathcal{Y}^+, \mathcal{F}^+)$ of $\mathcal{X}^+$ over $R^{(2)}$, which satisfies the conditions of Proposition 3 except for the F_{q^2}-rationality of all points of C^* lying above the special points of C^+ in (ii). Therefore, in order to complete the proof of Proposition 3, we need the following

LEMMA 3.4. *Suppose that* $(\mathcal{Y}, \mathcal{T})$ *is an object of the category* (ii) *defined in Theorem* 1′. *Let* $f_s: C^* \longrightarrow C^+$ *be as in Lemma* 3.3. *Then all points of* C^* *lying above the special points of* C^+ *are* F_{q^2}*-rational.*

PROOF. It can be easily checked that we may assume that f_i $(i=0, 1, 2)$ are Galois coverings. Then f_s is also a Galois covering. Put $\Pi^* = \Pi_{C^*}$. In view of the proof of Lemma 3.3, we may put

$$\mathcal{Y}^+ = \{C^* \xleftarrow{\phi_1''} Y \xrightarrow{\phi_2''} C^*\} \quad \text{and} \quad \mathcal{T}^+ = (f, f_0, f),$$

with $C_s^* = C^*$. Then the special fibre Y_s consists of two irreducible components which are generically isomorphic to Π^* and $\Pi^{*\prime}$. Therefore, there exist two morphisms $j_1: \Pi^* \longrightarrow Y_s$ and $j_2: \Pi^{*\prime} \longrightarrow Y_s$ making the following diagrams commutative

Let P_1 be a point of C^* such that $f_s(P_1)$ is special, and $P \in Y_s$ any point lying above P_1. If P belongs to only one irreducible component of Y_s, $\mathcal{O}_{Y_s,P}$ must be isomorphic to $\mathcal{O}_{C^*,P_1}$, for C^* is a complete non-singular curve over F_{q^2}. Therefore, if $\hat{\mathcal{O}}_{Y_s,P} \neq \hat{\mathcal{O}}_{C^*,P_1}$, P belongs to both irreducible components of Y_s. Let y_1 be any geometric point of C^* corresponding to P_1, and y any geometric point of Y_s corresponding to P lying above y_1. Then $\mathrm{pr}_2(y) = y_1^q$ holds. Therefore, if y belongs to both irreducible components, $(y_1, y_1^q) \in \Pi^*$ and $(y_1^{q^2}, y_1^q) \in \Pi^{*\prime}$ must be mapped to y by j_1 and j_2, respectively. This implies that $y_1 = y_1^{q^2}$, and hence y_1 is F_{q^2}-rational.

Now we shall prove that P is an ordinary double point. By the assumption that f_s is a Galois covering, the ramification indices of P_1 and $\phi_2''(P)$ are equal and a divisor e of $e_s(f_s(P_1))$ prime to p. On the other hand, Y is equal to the normalizations in $K(Y)$ of $C^* \times_{C^+} \mathcal{T}^+$ (w.r.t. φ_1^+) and $\mathcal{T}^+ \times_{C^+} C^*$ (w.r.t. φ_2^+). In particular $\hat{\mathcal{O}}_{Y,P}$ contains both eth roots of prime elements of $f_s(P_1)$ and ${}^t f_s(P_1)$. Therefore, by Main Lemma A in § 2, P must be an ordinary double point. This settles the lemma and also completes the proof of Proposition 3.

4. Proofs of the theorems

We have already established most of our theorems by Proposition 2 in § 2 and Proposition 3 in § 3. In this section, we collect them and clarify the functors between each two categories in the theorems.

PROOF OF THEOREM 1. As for the functor (i)$\longrightarrow$(ii), it is defined by corresponding each covering $f: C^* \longrightarrow C$ over F_q satisfying the conditions in (i) to the CR-covering $(\mathcal{X}^*, \mathcal{F})$ associated with an extension $(\mathcal{C}^*, \mathcal{T}^*)$ of $(\mathcal{C}, \mathcal{T})$ on C^* whose existence and uniqueness are guaranteed by Proposition 2.

Conversely, the functor (ii)$\longrightarrow$(i) is defined as follows. Let $(\mathcal{X}^*, \mathcal{F})$ be an object of the category (ii). Put $\mathcal{X}^* = \{\mathcal{C}^* \xleftarrow{\varphi^*} \mathcal{T}^* \xrightarrow{{}^t\varphi^*} \mathcal{C}^*\}$ and $\mathcal{F} = (f, g, f)$. Then we correspond $(\mathcal{X}^*, \mathcal{F})$ to $f_s: \mathcal{C}_s^* \longrightarrow C$. It is easy to see that f_s is tamely ramified and admissible with respect to $\mathfrak{e}_s$. Let $(\mathcal{X}^{*+}, \mathcal{F}^+)$ be the CR-covering of $\mathcal{X}^+$ associated with $(\mathcal{X}^*, \mathcal{F})$. Then, by applying Lemma 3.4 to $(\mathcal{X}^{*+}, \mathcal{F}^+) \otimes_{R^{(2)}} \bar{k}$, we conclude that all closed points of $\mathcal{C}_s^*$ lying above the special points of C are of degree ≤ 2 over F_q.

Obviously, these two functors are mutually inverse, hence equivalence functors. This settles the proof of Theorem 1.

PROOF OF THEOREM 1′. The functor (i)$\longrightarrow$(ii) is defined by taking the composite of the functor (i)$\longrightarrow$(ii) in Theorem 1 and the base change $\otimes_{R^{(2)}} \bar{k}$.

On the other hand, the functor (ii)$\longrightarrow$(i) is defined by corresponding each object $(\mathcal{Y}, \mathcal{F})$ of the category (ii) to $f_s: \mathcal{C}_s^* \longrightarrow C^+$ defined in Proposition 3 which satisfies the conditions in (i). It follows immediately that these two functors are mutually inverse. This proves Theorem 1′.

Now we shall determine the quasi-symmetric points of $\mathcal{T}_\eta^n$ whose specializations are special. We use the same notation as in § 2. But we do not assume that $\deg Q = \deg Q_s$. Hence x is not necessarily a prime element of Q.

LEMMA 4.1. *Let $P \in \mathcal{T}_\eta^n$ and $\varphi_\eta(P) = Q \in \mathcal{C}_\eta$. Suppose that Q_s is special. Then P is quasi-symmetric if and only if there exists a prime element of P in $A = \hat{\mathcal{O}}_{\mathcal{T}^n, P_s}$ of the following form.*

$$h(Y)=b_0+b_1Y+\cdots+b_{n-1}Y^{n-1}+Y^n,$$

where $n=\deg Q$, $b_1, \cdots, b_{n-1}\in\pi R'$, $b_0b_0'=(a\pi^l)^n$, *and* $b_i'=b_0^{-1}(a\pi^l)^{n-i}b_{n-i}$ $(i=1, \cdots, n-1)$. *Furthermore, if* P *is quasi-symmetric,* P *is symmetric,* P/Q *is unramified and* $\deg P=\deg Q$ *over* k.

PROOF. Let $z=\alpha_0+\alpha_1+\cdots+\alpha_{n-1}x^{n-1}+x^n$ be an irreducible polynomial in x which is a prime element of Q. In the same manner as in the proof of Main Lemma A, we have

$$Y^nz=\eta(a_0+a_1Y+\cdots+a_{n(q+1)-1}Y^{n(q+1)-1}+Y^{n(q+1)})$$

in A, with $\eta\in A^\times$ and $a_0, \cdots, a_{n(q+1)-1}\in\pi R'$. Note that $\mathrm{ord}_\pi(a_0)=ln$. Suppose that the right hand side decomposes into irreducible polynomials as follows.

$$Y^nz=\eta h_1(Y)^{e_1}\cdots h_r(Y)^{e_r},$$

where the coefficients of the highest terms of $h_i(Y)$ are equal to 1. Assume that $h_1(Y)$ is a prime element of P and $\deg h_1=n_1$. Put $h_1(Y)=b_0+b_1Y+\cdots+b_{n_1-1}Y^{n_1-1}+Y^{n_1}$. Then $h_1(Y)$ can be described in terms of X as follows.

$$\begin{aligned}X^{n_1}h_1(Y)&=b_0X^{n_1}+b_1YX^{n_1}+\cdots+Y^{n_1}X^{n_1}\\&=b_0X^{n_1}+b_1a\pi^lX^{n_1-1}+\cdots+(a\pi^l)^{n_1}\\&=b_0(X^{n_1}+b_0^{-1}a\pi^lb_1X^{n_1-1}+\cdots+b_0^{-1}(a\pi^l)^{n_1}).\end{aligned}$$

Put

$$h^*(X)=b_0^*+b_1^*X+\cdots+b_{n_1-1}^*X^{n_1-1}+X^{n_1},$$

with $b_0^*=b_0^{-1}(a\pi^l)^{n_1}$ and $b_i^*=b_0^{-1}(a\pi^l)^{n_1-i}b_{n_1-i}$ $(i=1, \cdots, n_1-1)$. Then P is quasi-symmetric if and only if $h^*(Y)=h_i'(Y)$ for some i $(1\leq i\leq r)$. For $f\in R'[[Y]]$, let $\mathrm{ord}f$ denote the *order* of the constant term of f. Since $\mathrm{ord}f_1f_2=\mathrm{ord}f_1+\mathrm{ord}f_2$ for $f_1, f_2\in R'[[Y]]$, we have $\sum_{i=1}^r e_i\,\mathrm{ord}\,h_i=ln$. Put $\mathrm{ord}\,h_1=m_1$. Then it is obvious that $\mathrm{ord}\,h^*=ln_1-m_1$.

(i) *The case where* $h^*(Y)=h_i'(Y)$ $(i>1)$. We have

$$ln=\sum_{i=1}^r e_i\,\mathrm{ord}\,h_i\geq\mathrm{ord}\,h_1+\mathrm{ord}\,h^*=ln_1.$$

This implies that $n_1=n$ and $\varphi_\eta^*(Q)=P+P'$ with $\deg P=\deg P'=\deg Q$. As $\sum_{i=1}^r e_i\deg h_i=(q+1)n>2n$, this is impossible.

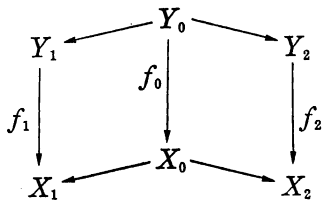
(ii) *The case where* $h^*(Y)=h_1^{\iota}(Y)$. In this case we have $m_1=\frac{1}{2}ln_1$, and hence

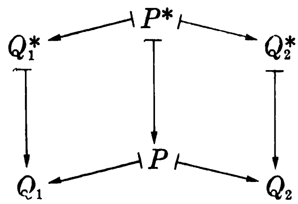
$$ln=\sum_{i=1}^{r} e_i \operatorname{ord} h_i \geq \frac{1}{2} ln_1 .$$

From this, we obtain $n_1=n$ or $2n$. If $n_1=2n$, we have $m_1=ln$, $\varphi_{\eta}^*(Q)=P$ and $\deg P=2\deg Q$, which is a contradiction. Now suppose that $n_1=n$. Then we have $\deg P=\deg Q$ and $\operatorname{ord} h_1=\frac{1}{2}ln$ which implies that $e_1=1$. This settles the lemma.

COROLLARY. *Let Q be a point of C_{η}. Then, if Q_s is special, there exists at most one quasi-symmetric point of $\mathcal{T}_{\eta}^{n}$ lying above Q.*

Finally, we shall prove Proposition 1. Consider the following diagrams, the left being as in § 1:





(Points)

Then Proposition 1 is a direct consequence of the following

LEMMA 4.2. *Suppose that specializations of any two branch points of φ_{η} are mutually distinct. Then, if $Q_1 \in \mathfrak{R}$ and $Q_2 \notin \mathfrak{R}$, the ramification index $e(Q_1^*/Q_1)$ is a divisor of $e(P/Q_1)$.*

PROOF. If $e(Q_1^*/Q_1)$ does not divide $e(P/Q_1)$, P^*/P must be ramified. On the other hand, as $Q_2 \notin \mathfrak{R}$, φ_2 and f_2 are both unramified at Q_2. In particular, P^*/P is unramified. Therefore, $e(Q_1^*/Q_1)$ divides $e(P/Q_1)$.

COMMENTS. 1. We have little knowledge of the ramifications of general congruence relations and can say almost nothing about the existence of congruence relations which satisfy given properties of ramifications. However, it is known that there exist some relations between the ramifications of congruence relations and the poles of the asociated differentials defined in [7].

2. Ihara's results in the unramified case involve those of fundamental groups. In the ramified case, the same problem is also significant. Fix an embedding $\bar{k}\hookrightarrow C$ and consider the system of compact Riemann surfaces $\{\mathfrak{R}_1\longleftarrow\mathfrak{R}_0\longrightarrow\mathfrak{R}_2\}$ corresponding to $\tilde{\mathfrak{X}}$. Let Δ_i $(i=1,2)$ be the Fuchsian groups corresponding to $\mathfrak{R}_i$ and the signature $\mathfrak{e}$. Let $\mathfrak{e}_0$ be any signature on $\mathfrak{R}_0$ and Δ_0 the Fuchsian group corresponding to $\mathfrak{R}_0$ and $\mathfrak{e}_0$. Then we can easily describe the conditions of the ramification of φ_η and those on $\mathfrak{e}_0$, for which there exist natural homomorphisms $\Delta_0\longrightarrow\Delta_i$ $(i=1,2)$ and for which they are injective. It seems quite possible that, when the natural homomorphisms $\Delta_0\longrightarrow\Delta_i$ exist and are injective, we will be able to extend Ihara's theory of fundamental groups to ramified congruence relations.

References

[1] Deligne, P. and M. Rapoport, Les schémas de modules de courbes elliptiques, Lecture Notes in Math. No. 349, Springer-Verlag, Berlin-Heidelberg-New York, 1973, 143–316.

[2] Grothendieck, A., Eléments de géométrie algébrique (EGA) I–IV, Publ. Math. IHES, 1960–67.

[3] Grothendieck, A., Revêtements étales et groupe fondamental (SGA 1), Lecture Notes in Math. No. 224, Springer Verlag, Berlin-Heidelberg-New York, 1971.

[4] Grothendieck, A. and J. P. Murre, The tame fundamental group of a formal neighbourhood of a divisor with normal crossings on a scheme, Lecture Notes in Math. No. 208, Springer-Verlag, Berlin-Heidelberg-New York, 1971.

[5] Ihara, Y., On congruence monodromy problems, Lecture Notes, Univ. Tokyo, Tokyo, vol. 1, 1968, vol. 2, 1969.

[6] Ihara, Y., On modular curves over finite fields, in "Discrete Subgroups of Lie Groups", Proc. Internat. Colloq., Bombay, Oxford Univ. Press, Oxford-New York, 1975, 161–202.

[7] Ihara, Y., 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.

[8] Ihara, Y., (a) Congruence relations and Shimura curves, Proc. Sympos. Pure Math, Vol. 33, Part 2, Amer. Math. Soc., Providence, R. I., 1979, 291–311; (b) Congruence relations and Shimura curves, II, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **25** (1979), 301–361.

[9] Ihara, Y., Congruence relations and fundamental grougs, J. Algebra **75** (1982), 445–451.

[10] Ihara, Y., Lifting curves over finite fields together with the characteristic correspondence $\Pi+\Pi'$, J. Algebra **75** (1982), 452–483.

[11] Ihara, Y. 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.

[12] Popp, H., Fundamentalgruppen algebraischer Mannigfaltigkeiten, Lecture Notes in Math. No. 176, Springer-Verlag, Berlin-Heidelberg-New York, 1970.
[13] Shimura, G., Introduction to the arithmetic theory of automorphic functions, Publ. Math. Soc. Japan, Iwanami Shoten and Princeton Univ. Press, 1971.

(Received July 24, 1986)

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