The Grothendieck Conjecture on the Fundamental Groups of Algebraic Curves

Hiroaki Nakamura, Akio Tamagawa, Shinichi Mochizuki

The "Grothendieck Conjecture" in the title is, in a word, a conjecture to the effect that the arithmetic fundamental group of a hyperbolic algebraic curve completely determines the algebraic structure of the curve. Research concerning this problem was begun at the end of the 1980's by the first author (Nakamura), given significant impetus (including the case of positive characteristic) by the second author (Tamagawa), and brought to a final solution by means of a new p-adic interpretation of the problem due to the third author (Mochizuki).

In this paper, after briefly reviewing the background and history of the problem, we would like to report on how the Conjecture was gradually brought to a solution by the work of the three authors.

§1. The Arithmetic Fundamental Group — a Bridge between Algebraic Geometry and Group Theory —

§1.1. The Étale Fundamental Group

As is well-known, the usual "topological fundamental group" is a so-called homotopy invariant, i.e., invariant with respect to continuous deformations of shape. For instance, in the case of a compact complex algebraic curve, the only invariant of the curve determined by its topological fundamental group is its genus. Thus, taken alone, the topological fundamental group cannot possibly be a sufficiently fine invariant to distinguish the algebraic structure of different algebraic curves. Indeed, the "arithmetic fundamental group" appearing in the Grothendieck Conjecture is a notion which is naturally defined — as an extension of the notion of "Galois group" — by means of the notion of "*étale* (i.e., as opposed to topological) fundamental group" introduced by A. Grothendieck.

This notion of "étale fundamental group" was introduced into algebraic geometry in the 1960's in [SGA1] as an accounting device to keep track of the "Galois theory of schemes." According to [SGA1], given a geometric point $\bar{x}$ on a connected scheme X, the étale fundamental group $\pi_1(X, \bar{x})$ is defined as a group of permutations of a system of "sets of solutions" as follows: As Y ranges over all of the finite étale coverings (in the following, we shall frequently abbreviate this expression by the phrase "finite coverings") of X, the fiber sets $Y(\bar{x})$ over the geometric point $\bar{x}$ form a projective system of finite sets. Then $\pi_1(X, \bar{x})$ is defined as the group formed by all the self-permutations of this system that arise geometrically. Observe that, since it arises as the projective limit of permutation groups of the various finite sets $Y(\bar{x})$, this group admits a natural structure of profinite topological group[1)]. Since one knows that the isomorphism class (as a topological group) of the étale fundamental group does not depend on the choice

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX of base-point $\bar{x}$ appearing in the definition, in discussions where one is only concerned with the group-theoretic structure of the étale fundamental group, we shall frequently omit the base-point and write $\pi_1(X)$.

Given an arbitrary finite covering $Y \to X$, the set $Y(\bar{x})$ defines a continuous finite permutation representation of $\pi_1(X, \bar{x})$; moreover, this correspondence (that associates the permutation representation $Y(\bar{x})$ to the covering $Y \to X$) defines a categorical equivalence between the category of finite coverings of X and the category of continuous finite permutation representations of $\pi_1(X, \bar{x})$. In particular, (when Y is connected) the stabilization group at each point of $Y(\bar{x})$ determines a (conjugacy class of) open subgroup(s)[2)]; conversely, an open subgroup H of $\pi_1(X, \bar{x})$ determines (an equivalence class of) finite connected covering(s) $Y \to X$ corresponding to the permutation representation on the set of left cosets of $\pi_1(X, \bar{x})$ with respect to the subgroup H. This correspondence $H \leftrightarrow Y$ appears frequently in the discussions to come, so we will denote corresponding objects by the notation $Y = Y^H$, $H = H_Y$. In particular, one has the fundamental observation that H_Y is none other than the fundamental group $\pi_1(Y)$ of Y itself.

When the scheme X is a point, especially, when it is the spectrum $\mathrm{Spec}\,(K)$ of a field K, the fiber set $Y(\bar{x})$ of a connected finite covering Y is none other than the set of solutions of the algebraic equations defining Y, and the fundamental group $\pi_1(\mathrm{Spec}\,(K))$ may be identified with the absolute Galois group $\mathrm{Gal}(K) \stackrel{\mathrm{def}}{=} \mathrm{Gal}(\overline{K}/K)$, i.e., with the collection of "permutations of solutions" of all possible algebraic equations. (Here, $\overline{K}$ denotes the separable closure of K.)

In general, when one is given a morphism of schemes $f : X_1 \to X_2$ and a geometric point $\bar{x}_1$ on X_1, if one denotes the image of $\bar{x}_1$ in X_2 by $\bar{x}_2$, then one obtains an induced homomorphism $\pi_1(X_1, \bar{x}_1) \to \pi_1(X_2, \bar{x}_2)$. Indeed, the pull-back to X_1 (i.e., the fiber product with X_1 over the base X_2) of the finite étale covering $Y \to X_2$ is a finite étale covering $Y' \to X_1$ over X_1, and, moreover, one always has $Y(\bar{x}_2) \cong Y'(\bar{x}_1)$. Thus, one obtains the above homomorphism of fundamental groups by simply restricting the corresponding homomorphism of systems of permutation groups. If one changes the base-point $\bar{x}_1$, the resulting homomorphism of fundamental groups is equivalent to the previous one (by an appropriate commutative diagram). Thus, in the following, we shall frequently omit mention of the base-point and simply write $\pi_1(X_1) \to \pi_1(X_2)$.

When X is an algebraic variety defined over a field K, the natural morphisms $X \to \mathrm{Spec}\,(K)$ and $\mathrm{Spec}\,(\overline{K}) \to \mathrm{Spec}\,(K)$ induce a morphism $X_{\overline{K}} \to X$ ($X_{\overline{K}} \stackrel{\mathrm{def}}{=} X \times_K \overline{K}$). Moreover, one has an exact sequence of fundamental groups

$$1 \longrightarrow \pi_1(X_{\overline{K}}) \longrightarrow \pi_1(X) \xrightarrow{\mathrm{pr}_X} \mathrm{Gal}(K) \longrightarrow 1 \tag{1.1}$$

arising from these morphisms. The group $\pi_1(X_{\overline{K}})$, which forms the kernel of the projection pr_X, is called the "geometric" fundamental group of X. In the case when K is of characteristic 0, this group is isomorphic to the profinite completion (i.e., the projective limit of all the finite quotients) of the usual topological fundamental group of the corresponding complex manifold. Thus, in particular, it is invariant with respect to deformations[3)]. It is then natural to inquire as to how the "arithmetic" fundamental group $\pi_1(X)$ varies as an extension of $\mathrm{Gal}(K)$ (cf. (1.1)), as one deforms X.

In the above exact sequence (1.1), $\pi_1(X_{\overline{K}})$ is a normal subgroup of $\pi_1(X)$, hence determines a homomorphism $\pi_1(X) \to \mathrm{Aut}(\pi_1(X_{\overline{K}}))$ (by conjugating the subgroup $\pi_1(X_{\overline{K}})$ by elements of $\pi_1(X)$). This homomorphism clearly maps $\pi_1(X_{\overline{K}})$ into the group of inner automorphisms of $\pi_1(X_{\overline{K}})$. Thus, by taking quotients, one obtains a homomorphism — called an *outer Galois representation* —

$$\rho_X : \mathrm{Gal}(K) \to \mathrm{Out}(\pi_1(X_{\overline{K}})) \tag{1.2}$$

from $\mathrm{Gal}(K)$ to the outer automorphism group $\mathrm{Out}(\pi_1(X_{\overline{K}}))$ of the geometric fundamental group. Just now we defined $\rho_X : \mathrm{Gal}(K) \to \mathrm{Out}(\pi_1(X_{\overline{K}}))$ starting from $\mathrm{pr}_X : \pi_1(X) \to \mathrm{Gal}(K)$ by means of purely group-theoretic operations. Conversely, when the center of $\pi_1(X_{\overline{K}})$ is trivial, one can recover pr_X from ρ_X by means of purely group-theoretic operations. For instance, in the case of a *hyperbolic algebraic curve* (i.e., a smooth algebraic curve such that if g is its genus, and n is the number of points "at infinity," then $(g, n) \neq (0, 0), (0, 1), (0, 2), (1, 0)$) defined over a field of characteristic 0, the geometric fundamental group is isomorphic to either a nonabelian free group or the profinite completion of a (nonabelian) surface group, hence well-known to be center-free, so the above observation applies in this case. In this sort of situation, to consider "the outer Galois action ρ_X on $\pi_1(X_{\overline{K}})$" is equivalent to considering "the group $\pi_1(X)$ as an extension of $\mathrm{Gal}(K)$."

§1.2. Grothendieck's Anabelian Conjectures

In [G1-3], Grothendieck set forth a collection of conjectures based on his intuition that for varieties X which are "anabelian" (a vaguely defined class of manifolds that includes hyperbolic algebraic curves) and base fields K which are finitely generated over the prime field, the structure of $\pi_1(X)$ as an extension of $\mathrm{Gal}(K)$ (cf. (1.1)) should be sufficient to control the geometry of X.

Most notable among this collection of conjectures was the following general assertion, which Grothendieck referred to as the "Fundamental Conjecture of Anabelian Algebraic Geometry."

(GC1) "Fundamental Conjecture."

An anabelian algebraic variety X over a field K which is finitely generated over a prime field may be "reconstituted" from the structure of the arithmetic fundamental group $\pi_1(X)$ as a topological group equipped with its associated surjection $\mathrm{pr}_X : \pi_1(X) \to \mathrm{Gal}(K)$.

Here, the term "anabelian algebraic variety" means roughly "an algebraic variety whose geometry is controlled by its fundamental group, which is assumed to be 'far from abelian.' " This term was invented by Grothendieck. Since he refrained from giving a precise definition of this term in arbitrary dimension (i.e., for varieties of dimension > 1), and, moreover, used the term "reconstituted" in a similarly ambiguous fashion, it is to this day not clear precisely for which varieties the conjecture was asserted to hold in higher dimensions[4)]. For algebraic curves in characteristic 0, however, Grothendieck himself made the following explicit conjecture:

(GC2) The "Hom Conjecture." For hyperbolic algebraic curves X, Y over a field K which is finitely generated over the rationals, the natural map

$$\mathrm{Hom}_K(X,Y) \to \mathrm{Hom}_{\mathrm{Gal}(K)}(\pi_1(X), \pi_1(Y))/\sim$$

defines a bijective correspondence between dominant K-morphisms and equivalence classes of $\mathrm{Gal}(K)$-compatible open homomorphisms (modulo composition with an inner automorphism induced by an element of $\pi_1(Y_{\overline{K}})$). (In other words, open homomorphisms of the fundamental group always arise from algebro-geometric morphisms.)

As Grothendieck himself observes, the above conjecture bears some resemblance to the Tate Conjecture (proved by G. Faltings [F1]) concerning the 1-dimensional étale homology groups of abelian varieties:

$$\mathrm{Hom}_K(A,B)\otimes\hat{\mathbf{Z}} \cong \mathrm{Hom}_{\mathrm{Gal}(K)}(H_1(A_{\overline{K}},\hat{\mathbf{Z}}), H_1(B_{\overline{K}},\hat{\mathbf{Z}}))$$

(Here, A and B are abelian varieties defined over a global field K, and $\hat{\mathbf{Z}}$ is the profinite completion of $\mathbf{Z}$.) Moreover, if one applies the Tate Conjecture together with the "isogeny theorem" (as well as the Shafarevich Conjecture, etc., which were proven by Faltings along with the Tate Conjecture) to the Jacobian variety of the curves in question, it follows immediately that there are only finitely many curves with homology group H_1 isomorphic (as a Galois module) to the H_1 of a given proper algebraic curve of genus ≥ 2. If one observes that H_1 is just the abelianization of π_1, then one may regard the Fundamental Conjecture (GC1) as the assertion that, if one increases the data that one is given from just the homology group to the entire fundamental group, then the number of possibilities for a curve possessing the same invariant (i.e., the same π_1) is narrowed down from some unknown finite number to "just one." In fact, even effective versions of this sort of finiteness theorem (i.e., the Shafarevich conjecture, etc.) tend (with few exceptions[5)]) to give only inordinately large estimates for the number of such possibilities. Thus, from this point of view, there is quite a substantial gap between Grothendieck's conjectures (GC1), (GC2) and the Tate Conjecture applied to the Jacobian varieties of the curves in question. Grothendieck argued, in support of his conjecture, that the arithmetic fundamental group $\pi_1(X)$ possesses an "extraordinary rigidity," i.e., that the outer action (1.2) of its "arithmetic quotient" $\mathrm{Gal}(K)$ on its "geometric portion" $\pi_1(X_{\overline{K}})$ should be "extraordinarily rigid," citing by way of comparison the nontriviality of the Galois representations arising from cohomology theory which were studied by A. Weil and P. Deligne ([G3]).

Finally, among (unsolved) conjectures which may be rigorously formulated, one interesting conjecture is the following "Section Conjecture." A K-rational point $x \in X(K)$ of an algebraic variety X over K may be regarded as a section $x : \mathrm{Spec}\,(K) \to X$ of the structure morphism $X \to \mathrm{Spec}\,(K)$. Thus, a K-rational point x induces a ($\pi_1(X_{\overline{K}})$-conjugacy class of) section homomorphism(s) $\alpha_x : \mathrm{Gal}(K) \to \pi_1(X)$ which splits the fundamental exact sequence (1.1) discussed above.

(GC3) The Section Conjecture. For an X/K as in (GC2), every section homomorphism $\alpha : \mathrm{Gal}(K) \to \pi_1(X)$ of the projection $\mathrm{pr}_X : \pi_1(X) \to \mathrm{Gal}(K)$ arises either from a K-rational point of X (in the usual sense), or from the K-rational points "at infinity"[6)] of X.

We will discuss the (tangential) sections arising from the points at infinity in the following §. With respect to the Hom Conjecture, Grothendieck ([G2]) also mentions[7)] the possibility of extending the conjecture to the case where X is an arbitrary smooth algebraic variety and Y is an "elementary anabelian variety" (i.e., a variety obtained as the successive smooth fibration of families of hyperbolic curves). In this context, the Section Conjecture may be regarded as a variant of the Hom Conjecture where "X" is replaced by the spectrum of the base field[8)]. Grothendieck also considers the case where X and Y are replaced by the spectra of function fields and conjectures that a "birational version of the anabelian conjecture"[9)] holds in this case.

§1.3. Concerning the Arithmetic Fundamental Group

In his writings ([G1-3]), Grothendieck also discourses on various dreams of his ranging from the possibility of treating algebraic curves over number fields as graphs on topological surfaces ("dessins d'enfant") to the explicit description of the close relationship between the arithmetic fundamental groups of various moduli spaces of curves, to the possibility of revolutionizing the concept of a "space" by means of a new categorical point of view. On the other hand, G. V. Belyi's result ([B]) as the end of the 1970's to the effect that the outer Galois representation (1.2) in the case $K = \mathbf{Q}$, $X = \mathbf{P}^1 - \{0, 1, \infty\}$ is *injective* drew the attention of a large number of mathematicians as a classical example of the highly nontrivial relationship between Galois groups and fundamental groups. Ever since the appearance of this result, various research topics and unsolved problems arising both from [G1-3] and from other independent sources gradually came to be recognized as being related and continue to this day to be the focus of active research (e.g., the inverse Galois problem, mixed motives, adèlic special functions, the Grothendieck-Teichmüller group, etc.). With regard to the numerous important issues and recent developments concerning these topics, we apologize that due to the lack of space, we are unable to discuss these topics in detail in this paper, and instead restrict ourselves to quoting several reference books ([1–6]) and surveys ([I2], [H]). One may think of the "Grothendieck Conjecture" which is the topic of the present paper as being simply a branch – of a somewhat conceptual hue – on the great tree of numerous research topics (as discussed above) concerning the arithmetic fundamental group.

§2. From Finiteness Theorems to Rigidity Theorems
(mainly the case X: genus 0, K: number field)

§2.1. The Theorem of Anderson-Ihara

Any approach to the Grothendieck Conjecture must begin by addressing the question of precisely where in the extension structure (1.1) of the arithmetic fundamental group, or, alternatively, in the outer Galois representation (1.2) arising from this extension, one should look to find some sort of reflection of the algebraic structure of the original space. Now when one fixes a prime number l, the outer Galois representation (1.2) also naturally induces an outer action

$$\rho_X^{(l)} : \mathrm{Gal}(K) \to \mathrm{Out}(\pi_1^{(l)}(X_{\overline{K}}))$$

on the maximal pro-l quotient group[10] $\pi_1^{(l)}(X_{\overline{K}})$ of $\pi_1(X_{\overline{K}})$. In the 1980's, building on his previous work, Yasutaka Ihara ([I1]) initiated research on the pro-l outer Galois representation associated to $X = \mathbf{P}^1 - \{0, 1, \infty\}$, independently of Grothendieck and Deligne. This research led to the elucidation[11] of the deep arithmeticity (especially, the relationship to Jacobi sums and circular units) of this outer Galois representation. Moreover, Ihara's success spurred researchers[12] — mainly in Japan — to work on applications as well as generalizations to various other curves of Ihara's work.

Already by the late 1980's, the following fact came to be known as a theorem of G. Anderson-Ihara ([AI]). For a finite set $\Lambda \subset \mathbf{P}^1(K)$ that contains $0, 1, \infty$,

Theorem (Anderson – Ihara). The fixed field $K_X^{(l)}$ of the kernel of the pro-l outer Galois representation $\rho_X^{(l)}$ associated to a genus 0 curve $X = \mathbf{P}^1_K - \Lambda$ is the extension field of K obtained by adjoining to K all of the algebraic numbers arising by repeating the operations of taking the cross-ratio and l-th root.

This theorem gives a description of the subfield $K_X^{(l)}$ of $\overline{K}$ which arises naturally from the pro-l outer Galois representation $\rho_X^{(l)}$ by means of a system of "numbers" generated by a fixed procedure from the coordinates of the set $\Lambda \subset \mathbf{P}^1(K)$ of ramification points. From another point of view, this theorem may be regarded as giving an explicit construction, for each prime number l, of group-theoretic invariants (i.e., the system of numbers referred to above) with values in the subfield $K_X^{(l)}$ of $\overline{K}$, using nothing more than the structure of the arithmetic fundamental group $\pi_1(X)$ as a $\mathrm{Gal}(K)$-extension. Nakamura's idea was to approach the Grothendieck Conjecture by constructing, in a more systematic fashion, invariants of the arithmetic fundamental group which are defined as subfields of $\overline{K}$ like those above in such a way that these invariants would serve to distinguish distinct genus 0 algebraic curves more effectively.

§2.2. A Group-Theoretic Description of Galois Permutations

The point of the method of Anderson-Ihara is to translate the pro-l outer Galois representation on $\pi_1(\mathbf{P}^1 - \Lambda)$ into the language of Galois permutations of the "pro-cusp points" over Λ distributed on the "rim" of the pro-l universal covering of $\mathbf{P}^1 - \Lambda$; this serves to reduce the issue of understanding the outer Galois representation to the more manageable task of understanding the Galois permutations of the cuspidal points lying on the genus 0 covers of $\mathbf{P}^1 - \Lambda$. Thus, we shall first consider how to translate the phenomenon of "cuspidal points of a finite covering which are permuted by Galois" into group-theoretic language that is phrased entirely in terms of the group extension structure of the arithmetic fundamental group.

In general, let X be an affine hyperbolic curve (of arbitrary genus) defined over K, and let Y be a finite covering of X; Y^* its nonsingular compactification. Then the set of cuspidal points of Y is the set $\Sigma_Y \stackrel{\mathrm{def}}{=} Y^* - Y$. First of all, the natural field of definition of the covering Y may be obtained as the field K_Y fixed by the image of the open subgroup $H_Y = \pi_1(Y)$ (corresponding to the covering Y) under the projection $\mathrm{pr}_X : \pi_1(X) \to \mathrm{Gal}(K)$. Next, the geometric fundamental group of Y may be recovered as the intersection $H_Y \cap \pi_1(X_{\overline{K}})$. If g_Y is the genus of Y^*, and n_Y is the cardinality of $\Sigma_Y(\overline{K})$, then this geometric fundamental group is a nonabelian free profinite group of rank $2g_Y + n_Y - 1$. Taking the maximal pro-l abelian quotient of this group then gives the l-adic étale homology group $H_1(Y_{\overline{K}}, \mathbf{Z}_l)$ $(= \pi_1^{(l)}(Y_{\overline{K}})^{\mathrm{ab}})$; moreover, by conjugation, one sees that one obtains a structure of $\mathrm{Gal}(K_Y)$-module on this homology group. Now since the cyclotomic permutation representation[13)] on the set of cuspidal points (almost) includes into this homology group (as a submodule of rank $n_Y - 1$), it suffices to recover this submodule group-theoretically. That one can, in fact, do this is guaranteed by the Riemann-Weil Conjecture. Indeed, the quotient module of $H_1(Y_{\overline{K}}, \mathbf{Z}_l)$ by the "cuspidal part" in question is of rank $2g_Y$ and is, in fact, isomorphic to the l-adic Tate module (made up of the l-power torsion points) of the Jacobian variety of Y^*. The Riemann-Weil conjecture asserts that the radii of the eigenvalues (i.e., the "weights") of the Frobenius action arising from the action of $\mathrm{Gal}(K_Y)$ on this Tate module are of a different size from the eigenvalue(s) arising from a cyclotomic action. Thus, the cuspidal part of $H_1(Y_{\overline{K}}, \mathbf{Z}_l)$ may be distinguished from the rest of $H_1(Y_{\overline{K}}, \mathbf{Z}_l)$ group-theoretically.

§2.3. Finiteness Theorems ([N1])

Now let us consider, for instance, those Galois coverings Y of $X = \mathbf{P}^1_K - \Lambda$ $(\Lambda \supset \{0, 1, \infty\})$ whose field of definition is the field $K(\sqrt[N]{1})$ and whose Galois group over $X_{K(\sqrt[N]{1})}$ is equal to $(\mathbf{Z}/N\mathbf{Z})^{|\Lambda|-1}$. If one then computes the intersection, ranging over Y as above and all prime numbers l, of the fixed fields of the kernels of the Galois representations on the cupidal parts of each $H_1(Y_{\overline{K}}, \mathbf{Z}_l)$, one obtains the field $K((\lambda - \lambda')^{1/N} \mid \lambda, \lambda' \in \Lambda - \{\infty\})$. This field is an invariant which can be group-theoretically extracted from the surjection $\mathrm{pr}_X : \pi_1(X) \to \mathrm{Gal}(K)$, whenever a natural number N is given. If, moreover, one lets N vary, then it follows from a simple Kummer theory argument (together with the fact that the group of units of a number field is finitely generated) that the subgroup generated inside the multiplicative group $K^\times$ by the finite set $\{\lambda - \lambda' \mid \lambda, \lambda' \in \Lambda - \{\infty\}, \lambda \neq \lambda'\}$ is also, therefore, a group-theoretic invariant. This invariant shows, among other things, that (up to linear fractional transformations) there are only finitely many subsets $\Lambda \subset \mathbf{P}^1(K)$ that give rise to the same arithmetic fundamental group, as well as that, in the case of certain special number fields K, the (outer action on the meta-abelianization of the geometric) fundamental group already determines a curve of the form $\mathbf{P}^1 - \{$ 4 points$\}$.

§2.4. Rigidity Theorems

In order to use the information arising from the Galois permutations of the cuspidal points more efficiently, this time we would like to consider the information that one obtains from the cuspidal part $\subset H_1((Y^H)_{\overline{K}}, \mathbf{Z}_l)$ of the homology of the covering Y^H associated to H, where we let H vary, as a parameter, among *all* the open subgroups of $\pi_1(X)$. (As was stated in §2.2) this cupsidal part may be characterized by the weight filtration. Thus, if one considers the union of the cyclic subgroups I of $\pi_1(X_{\overline{K}})$ that land inside the cuspidal part of the l-adic homology (for all prime numbers l) of all open subgroups H of $\pi_1(X_{\overline{K}})$ that contain I, then one obtains a subset of $\pi_1(X_{\overline{K}})$ which may be constructed entirely group-theoretically from the $\mathrm{Gal}(K)$-extension group $\pi_1(X)$.

One can show that this subset is precisely the union of (all conjugates of) the "cuspidal isotropy subgroups," that is to say, the union of all the inertia groups $(\cong \hat{\mathbf{Z}})$ inside $\pi_1(X_{\overline{K}})$

at the points at infinity of X (i.e., the cuspidal points of X itself) — cf. the "anabelian weight filtration" of [N2,4]. One can then recover the decomposition groups inside $\pi_1(X)$ as the normalizers of the inertia groups. The section homomorphisms $\alpha : \mathrm{Gal}(K) \to \pi_1(X)$ of the projection $\mathrm{pr}_X : \pi_1(X) \to \mathrm{Gal}(K)$ whose images lie inside a decomposition group are then called the *tangential sections* arising from the K-rational points at infinity of X. Among those section homomorphisms that are at issue in Grothendieck's Section Conjecture (GC3), those arising from the K-rational points at infinity may thus be given a group-theoretic characterization in this way.

Now since we have given a group-theoretic characterization of the set of inertia groups (as well as the corresponding decomposition groups), if, for instance, we are given an isomorphism $\pi_1(X_1) \cong \pi_1(X_2)$ over $\mathrm{Gal}(K)$ between the arithmetic fundamental groups of two curvess X_1 and X_2 over K, then this group isomorphism must automatically preserve the set of inertia groups, as well as the residue fields of the various corresponding points at infinity (since these residue fields are just the fixed fields of the image under pr_X of the corresponding decomposition group in $\mathrm{Gal}(K)$). Therefore, if X_1 may be embedded in X_1', then X_2 may also be embedded in some X_2' such that $\pi_1(X_1') \cong \pi_1(X_2')$. In particular, the problem of reconstructing (from their arithmetic fundamental groups) curves $\mathbf{P}^1 - \{n \text{ points}\}$ of genus 0 (where n is arbitrary) may be reduced to the case where $n = 4$. If, moreover, one uses the fact that one can specify those geometric cyclic covers that ramify only at two points entirely in the language of fundamental groups and inertia groups, one sees that by applying the method of [N1], one can extract (as an invariant of $\pi_1(\mathbf{P}^1 - \{0, 1, \infty, \lambda\})$) the triple $\langle\lambda\rangle$, $\langle 1-\lambda\rangle$, $\langle\frac{\lambda}{\lambda-1}\rangle$ of multiplicative subgroups of $K^\times$. This is, in fact, sufficient to characterize the isomorphism class of $\mathbf{P}^1 - \{0, 1, \infty, \lambda\}$. In this way, one can show that hyperbolic algebraic curves of genus 0 over a field which is finitely generated over $\mathbf{Q}$ may be "reconstituted" from their arithmetic fundamental groups ([N2]).

Moreover, since the characterization of inertia groups may be applied even to the pro-l fundamental groups of affine curves of arbitrary genus, the possibility thus arose of approaching a version of the Grothendieck Conjecture reformulated for the pro-l fundamental group "quantitatively" via the lower central series (of the pro-l fundamental group). In particular, when one specializes this to the problem of computing the group of (Galois-compatible) automorphisms of the pro-l fundamental group, one can to some extent systematically obtain affirmative results by combining one's knowledge of the pro-l outer Galois representations of curves of higher genus and their configuration spaces by means of a method involving various filtrations (cf. the survey [N7], as well as [NTs],[NTa],[MT], etc.). One can regard this problem of reconstructing the automorphism groups of curves from the groups of Galois-compatible automorphisms of their geometric fundamental groups as a preliminary first step to the isomorphism version of (GC2). However, in order to obtain a more decisive breakthrough, one had to first wait for the work of Tamagawa (§3).

Incidentally, this procedure that we carried out above for the tangential sections arising from the points at infinity, i.e., of

> Distinguishing group-theoretically those section homomorphisms $\alpha : \mathrm{Gal}(K) \to \pi_1(X)$ of the extension group structure $\mathrm{pr}_X : \pi_1(X) \to \mathrm{Gal}(K)$ of the arithmetic fundamental group of an algebraic curve that *arise geometrically.*

may also be seen in the later work of Tamagawa and Mochizuki. Moreover, in the course of carrying out this procedure, it became standard in this later work to apply the method by "compiling in an anabelian fashion" the arithmetic-geometric data included in the étale cohomology groups of the covering curves Y^H that arise when one allows H to vary as a parameter among all the open subgroups of $\pi_1(X)$. On the other hand, the issues of just what geometric information one extracts from the étale cohomology of Y^H in the various arithmetic settings that arise (in the later work of Tamagawa and Mochizuki), and how one compiles this information in order to arrive at the final result are highly nontrivial problems which required more sophisticated technology and fresh ideas to solve. In the following sections, we will discuss the development of the ideas of Tamagawa and Mochizuki that were applied to solve these problems in various specific arithmetic settings. In order, however, to allow even non-specialist readers to get a taste of the evolution of the common issues that underlie these developments, we will attempt to proceed, step by step, in as pedestrian a fashion as is possible.

§3. The Grothendieck Conjecture and the Fundamental Groups of Algebraic Curves in Positive Characteristic

§3.1. The Grothendieck Conjecture over Finite Fields

In this §, we let k be a finite field, and X a (nonsingular) affine curve over k. One of the main results of Tamagawa ([T1]) states that the scheme X may be recovered from $\pi_1(X)$ (more precisely, this is an analogue of the isomorphism version of (GC2)). The proof of this result is modeled on the work of K. Uchida ([U]), who showed that the function field $k(X)$ may be recovered from its absolute Galois group $\mathrm{Gal}(k(X))$, and may be roughly divided into three steps:

(i) the group-theoretic characterization of the decomposition groups of each closed point of X^*;

(ii) the reconstruction of the multiplicative group $k(X)^\times$;

(iii) the reconstruction of the additive structure on $k(X) = k(X)^\times \cup \{0\}$.

Here, just as in §2, we denote the nonsingular compactification of X by X^*.

In Step (i), Uchida used an idea of Neukirch involving Brauer groups, but in our case, since the inertia groups of the closed points of X are trivial, the decomposition groups of these points are isomorphic to the absolute Galois group of their residue fields (which are finite fields), hence have no (nonzero) H^2. Thus, we shall use instead an idea that we explain in the following.

First, observe that each closed point of X defines a continuous group homomorphism

$$\alpha_x : \mathrm{Gal}(k(x)) = \pi_1(\mathrm{Spec}\,(k(x))) \to \pi_1(X)$$

such that $\mathrm{pr}_X \circ \alpha_x$ coincides with the natural injection $\mathrm{Gal}(k(x)) \hookrightarrow \mathrm{Gal}(k)$, and that the image of α_x is the decomposition group of x. In particular, when x is a k-rational point, the homomorphism α_x determines a section of pr_X. Below, for simplicity, we shall concentrate on this case (where x is k-rational). The problem then is to give a group-theoretic condition that will guarantee that an arbitrary section homomorphism α of pr_X in fact arises as the α_x of some $x \in X(k)$. (Observe that since $\mathrm{Gal}(k) \cong \hat{\mathbf{Z}}$ is a free profinite group, the precise analogue of the Section Conjecture (GC3) could not possibly hold.) First, let us note that the condition in question is equivalent to the following:

(∗) For any open subgroup H of $\pi_1(X)$ that contains the image $\mathrm{Im}(\alpha)$ of α, the set of k-rational points $Y^H(k)$ of the corresponding covering Y^H of X is nonempty.

Indeed, necessity follows immediately from the fundamental properties of the decomposition group, while sufficiency follows from the following argument: Since any projective limit of nonempty finite sets is itself nonempty, the (pro-)covering of X corresponding to the subgroup $\mathrm{Im}(\alpha)$ of $\pi_1(X)$ possesses a k-rational point. Hence, if one takes such a k-rational point of this (pro-)covering and denotes the image of this point in X by x, one sees immediately that $\alpha = \alpha_x$. Thus, it remains to solve the problem of how to determine group-theoretically from the arithmetic fundamental group whether or not (∗) holds, or, more generally, just when a curve over a finite field k admits a rational point. This problem may be solved by using the Lefshetz Trace Formula, which allows one to calculate the number (≥ 0) of rational points by means of the action of the Frobenius element on l-adic étale cohomology (where l is a prime number distinct from the characteristic of k). For the points at infinity $x \in \Sigma \stackrel{\mathrm{def}}{=} X^* - X$, the inertia group is nontrivial, so the section homomorphism α_x into the decomposition group is not uniquely determined; moreover, (unlike the case of points $x \in X(k)$) the image of α_x is a proper subgroup of the decomposition group. Nevertheless, in this case, as well, if one applies a slightly modified version of the above argument, for each $x \in \Sigma$, one can group-theoretically reconstruct the infinite set of all possible α_x's. Thus, one can reconstruct the decomposition group of x as the subgroup of $\pi_1(X)$ generated by the union of the images of all possible α_x's.

Step (ii) is almost the same as in [U]: one uses the reciprocity law of class field theory, applied to the function field $k(X)$. Originally, the point of class field theory was to calculate the abelianization of the Galois group of a field by means of some multiplicative groups arising from the field; here, however, we view things in reverse, i.e., we think of the data of the multiplicative groups associated to a field as being encoded inside the abelianized Galois group. Since we have already reconstructed the decomposition groups associated to each closed point x of X^* in Step (i), it thus follows from local class field theory that we have reconstructed (as the "Weil group part" of the abelianization of the decomposition group), for $x \in X$, the group $\widehat{K}_x^\times / \widehat{O}_x^\times$ ($\cong \mathbf{Z}$), and, for $x \in \Sigma$, the group $\widehat{K}_x^\times$, as well as the natural morphisms $\widehat{K}_x^\times / \widehat{O}_x^\times \to \pi_1(X)^{\mathrm{ab}}$ and $\widehat{K}_x^\times \to \pi_1(X)^{\mathrm{ab}}$. (Here, $\widehat{O}_x$ is the completion of the local ring $\mathcal{O}_{X^*,x}$, and $\widehat{K}_x$ denotes the quotient field of this completion.) Thus, the Artin map

$$\prod_{x \in X}{}' \widehat{K}_x^\times / \widehat{O}_x^\times \times \prod_{x \in \Sigma} \widehat{K}_x^\times \longrightarrow \pi_1(X)^{\mathrm{ab}}$$

may also be reconstructed group-theoretically just from $\pi_1(X)$, hence the same may be said of its kernel, which is simply the multiplicative group $k(X)^\times$. (Here, we use for the first time that X is *affine*. If $X = X^*$, then we are only able to reconstruct the group $k(X)^\times/k^\times$ of principal divisors.)

Step (iii) is the most technically difficult step. First of all, observe that in Step (ii), we reconstructed not only the multiplicative group $k(X)^\times$, but also the discrete valuation $\mathrm{ord}_x : k(X)^\times \to \mathbf{Z}$ associated to each closed point x of X^*, as well as (for $x \in \Sigma$) the (kernel of the) reduction map $\mathrm{Ker}(\mathrm{ord}_x) = \mathcal{O}^\times_{X^*,x} \to k(x)^\times$. Now in [U], one first reconstructs the additive structure of the base field k (or of $\bar{k}$), then (since "$\Sigma = X^*$"), by using the reduction map for an infinite number of points, one reconstructs the additive structure of the function field from the additive structure of the various residue fields. In our case, (since Σ is a finite set) this final part of the argument does not work. Instead, one takes "lots" of "nice" functions $f \in k(X)$ (i.e., functions "like" the function t on $X = \mathbf{P}^1_k - \{0, 1, \infty\} = \mathrm{Spec}\,(k[t, t^{-1}, (t-1)^{-1}])$); then, by using the various special properties of the rational function field, one recovers the additive structure of the subfield $k(f) \subset k(X)$; and finally, by "gluing together" the additive structures of these various subfields, one recovers the additive structure of the original function field $k(X)$.

§3.2. From Finite Fields to Finitely Generated Fields

When X is, in addition, *hyperbolic*, the results and proofs which we explained in §3.1 remain valid when one replaces the full (arithmetic) fundamental group $\pi_1(X)$ by the tame fundamental group $\pi_1^{\mathrm{tame}}(X)$ (which is a quotient of $\pi_1(X)$). In this §, we will explain how the isomorphism version of the Grothendieck Conjecture (GC2) for affine hyperbolic curves over fields which are finitely generated over the rational number field may be derived from our results concerning the tame fundamental group of affine hyperbolic curves over a finite field. In §1.2, we pointed out the analogy between the Tate Conjecture and the Grothendieck Conjecture, but in the case of the Tate Conjecture, it seems highly unlikely that it is possible to derive Faltings' Theorem via a simple argument which does not involve genuinely global considerations from Tate's Theorem (which amounts to the Tate Conjecture over finite fields). This is one difference between the arithmetic nature of these two conjectures (cf. also §4.1).

Since it is easy to derive the case over a finitely generated extension of the rational number field from the case over a number field, in the following we shall consider the case where K is a number field, and X is an affine hyperbolic curve over K. The problem is to show how to recover group-theoretically the tame fundamental group of the reduction of X at each finite prime of K from the arithmetic fundamental group of X itself. Here, a key role is played by the fact that one can determine whether or not a hyperbolic curve over a local field has good reduction by looking at whether or not the outer action of the inertia group (of the local field) on the pro-l fundamental group (where l is a prime number which is distinct from the characteristic of the residue field) is trivial. This fact is the analogue for hyperbolic curves of the good reduction criterion of Serre-Tate for abelian varieties. (This group-theoretic good reduction criterion for hyperbolic curves is due in the proper case to T. Oda ([O1,2]).)

Now we let v be a finite prime of K, K_v be the v-adic completion of K, O_v be its ring of integers, and k_v be its residue field. Then the absolute Galois group of K_v may be naturally regarded as a subgroup of the absolute Galois group of K; moreover, the geometric fundamental group of X coincides with the geometric fundamental group of X_{K_v}, so one may immediately recover the arithmetic fundamental group $\pi_1(X_{K_v})$ of X_{K_v} as $\mathrm{pr}_X^{-1}(\mathrm{Gal}(K_v))$ (in the notation of (1.1)). If we then apply to this arithmetic fundamental group the above criterion, we can determine group-theoretically whether or not X_{K_v} has good reduction. Thus, in the following, we shall assume that X_{K_v} has good reduction; then we let X_{O_v} be the "good" model of X_{K_v} over O_v, and X_{k_v} be its reduction modulo the maximal ideal of O_v. Since, under these circumstances, it is known that $\pi_1^{\mathrm{tame}}(X_{k_v})$ and $\pi_1(X_{O_v})$ are naturally isomorphic, one may identify $\pi_1^{\mathrm{tame}}(X_{k_v})$ with the quotient $\pi_1(X_{O_v})$ of $\pi_1(X_{K_v})$. In order to recover this quotient group-theoreticaly, it is sufficient to be able to determine group-theoretically, for every finite étale (Galois) covering of X_{K_v}, whether or not this covering can be extended to an étale covering over X_{O_v}. But by hyperbolicity, it follows that this is, in fact, equivalent to the (at first sight weaker) condition that the covering curve also have good reduction; thus, one may apply the preceding criterion to determine group-theoretically whether or not this condition holds. From the above argument, it thus follows that whenever a hyperbolic curve X over a number field K has good reduction at the prime v, one can reconstruct group-theoretically the tame fundamental group of the reduction X_{k_v} (as a certain subquotient of the arithmetic fundamental group of X).

Now if one is given an isomorphism $\pi_1(X_1) \cong \pi_1(X_2)$ over $\mathrm{Gal}(K)$ between the arithmetic fundamental groups of two affine hyperbolic curves X_1 and X_2 over a number field K, then from the above argument, one sees that one gets an induced isomorphism $\pi_1^{\mathrm{tame}}((X_1)_{k_v}) \cong \pi_1^{\mathrm{tame}}((X_2)_{k_v})$ at almost all of the primes v of K (i.e., those primes at which X_1 and X_2 have good reduction). Thus, one obtains an isomorphism $(X_1)_{k_v} \cong (X_2)_{k_v}$ from the above result concerning the tame fundamental groups of affine hyperbolic curves over finite fields. On the other hand, from the hyperbolicity of the curves (which implies, in particular, that the scheme Isom of isomorphisms between the two curves is finite over the base), it follows that at almost all v, one has:

$$\mathrm{Isom}(X_1, X_2) \cong \mathrm{Isom}((X_1)_{k_v}, (X_2)_{k_v})$$

which thus implies that $X_1 \cong X_2$. This completes the proof that one may derive the isomorphism version of (GC2) for affine hyperbolic curves over number fields from the result discussed above concerning tame fundamental groups of affine hyperbolic curves over finite fields.

Moreover, in [M1], Mochizuki derives an isomorphism version of (GC2) for proper hyperbolic curves over number fields from the above results on the tame fundamental group of affine hyperbolic curves over finite fields. Here, the key theorem that connects these two results is an isomorphism version of (GC2) for the "log fundamental group" of (nonsmooth) stable curves over finite fields.

§3.3. The Geometric Fundamental Group of Algebraic Curves in Positive Characteristic

In the case of characteristic 0, the isomorphism class of the geometric fundamental group of a curve is determined solely by its genus g and the number n of points at infinity of the curve, but this does not hold in positive characteristic. Indeed, in [T2], it is proven that the isomorphism class (as a scheme) of a curve of genus 0 over $\overline{\mathbf{F}}_p$ is completely determined by its (geometric) fundamental group. It is of interest to determine whether this sort of result holds in general for arbitrary (hyperbolic) algebraic curves over an algebraically closed field of positive characteristic, and whether or not an analogous result holds when "fundamental group" is replaced by "tame fundamental group."

§4. Motivation for the Version over Local Fields

§4.1. Global Fields and Local Fields

In §1, we introduced the Grothendieck Conjecture as a conjecture that concerns objects over *global fields*, i.e., fields such as finitely generated extensions of the rational number field, which have lots of primes. By contrast, Mochizuki's series of papers ([M1-4]) introduced the new point of view that one should in fact regard this conjecture as a p-adic analytic phenomenon whose natural base is a local, not a global, field. The Grothendieck Conjecture over local fields (§5.1), which was obtained by starting from this point of view, is a general result which includes the original conjecture (GC2) formulated over fields which are finitely generated over the rationals. Before we discuss this new point of view and the results that arose from it, however, we would first like to examine the circumstances that existed prior to Mochizuki's work which led people to believe that the the natural base field for the conjecture should be a global field.

(A) The Tate Conjecture for Abelian Varieties: As was discussed in §1, Grothendieck, in the course of formulating his anabelian conjectures, pointed out the analogy between these conjectures and the Tate Conjecture proved by Faltings ([F1]). This proof of Faltings, however, uses in an essential way such global tools as the theory of heights over number fields, together with the fact that, when one considers how the height varies under an isogeny of abelian varieties, the contributions that arise from the finite and infinite primes occur in such a way as to just cancel each other out. Moreover, unlike the case with number fields (and finite fields), over such local fields as $\mathbf{Q}_p$, not only does the Tate Conjecture not hold, but, in many cases, the gap between the two modules which are expected to be isomorphic is quite large. Thus, if one takes the point of view that

"The Grothendieck Conjecture= The Tate Conjecture for Hyperbolic Curves"

then it is most natural to consider a conjecture such as (GC2) only over global fields.

(B) Applications to Diophantine Geometry: Among those mathematicians who were involved with the anabelian philosophy in its early years, the Grothendieck Conjecture appears to have been thought of as a new approach to Diophantine Geometry, i.e., to the study of rational points on varieties over *global* fields. The following argument is representative of this approach. Suppose that we wish to show that a certain algebraic variety has only finitely many rational points. We then assume that there are infinitely many and attempt to derive a contradiction by showing that any rational point arising as a "limit" of this infinite set of rational points has various properties that are "too good to be true." In order to carry out this argument, however, one needs to know that the "limit" exists. Since a field like a number field is not complete with respect to any nontrivial topology, the existence of such a limit is by no means clear. On the other hand, since Galois representations (as in (1.2)) are, in some sense, analytic objects, it is comparatively easy to show that a sequence of such Galois representations always has a convergent subsequence (i.e., a subsequence whose limit exists, as a Galois representation). Thus, if one knows, as is asserted in the Section Conjecture (GC3), that rational points and Galois representations (which satisfy certain conditions) are, in fact, equivalent objects, then one can conclude the existence of a limit of a sequence of rational points from the existence of the limit of the corresponding sequence of Galois representations. If one refines this argument somewhat, then the possibility arises of deriving a new proof of the "Mordell Conjecture"[14)] for algebraic curves of high genus from the Section Conjecture (GC3). Thus, if one has in mind such essentially global applications as the preceding argument, then it is most natural to consider the Grothendieck Conjecture only over global fields.

It was under these circumstances that the transformation of ideas "from global to p-adic fields" was bought about by the work of Mochizuki. Below we would like to explain the point of view that gave rise to this transformation.

§4.2. The Analogy with the Uniformization Theory of Hyperbolic Riemann Surfaces

The thrust of the Grothendieck Conjecture is, in a word, that one can recover a hyperbolic curve from its associated outer Galois representation (1.2), i.e., from:

$$\text{The Geometric } \pi_1 \text{ of the Curve} + \text{Some Natural "Arithmetic Structure" on this } \pi_1$$

In fact, if one forgets about the global nature of the base field and interprets the expression "arithmetic structure" in a broad sense, then one sees that in fact a phenomenon analogous to this conjecture was already known to mathematicians in the nineteenth century. This phenomenon is the uniformization theory of hyperbolic Riemann surfaces.

If one is given a hyperbolic curve X over the complex number field $\mathbf{C}$, then X defines a Riemann surface $\mathcal{X}$ of hyperbolic type. Thus, the universal covering $\tilde{\mathcal{X}} \to \mathcal{X}$ of this Riemann surface $\mathcal{X}$ also admits a natural structure of Riemann surface. Now by the uniformization theorem for Riemann surfaces, one knows that $\tilde{\mathcal{X}}$ is holomorphically isomorphic to the upper half-plane $\mathfrak{H} \stackrel{\mathrm{def}}{=} \{z \in \mathbf{C} \mid \mathrm{Im}(z) > 0\}$. Thus, if one uses the fact that $\mathrm{Aut}(\tilde{\mathcal{X}}) \cong \mathrm{Aut}(\mathfrak{H}) = \mathrm{SL}_2(\mathbf{R})/\{\pm 1\}$, then one obtains a canonical representation (defined up to conjugation by an element of $\mathrm{SL}_2(\mathbf{R})/\{\pm 1\}$)

$$\rho_{\mathcal{X}} : \pi_1(\mathcal{X}) \to \mathrm{SL}_2(\mathbf{R})/\{\pm 1\} \tag{4.1}$$

from the action of the (usual topological) fundamental group $\pi_1(\mathcal{X})$ of the Riemann surface $\mathcal{X}$ on $\tilde{\mathcal{X}}$. Conversely, if one is given $\rho_{\mathcal{X}}$, then the action of $\pi_1(\mathcal{X})$ on the upper half plane $\mathfrak{H}$ is determined; thus, by forming the quotient of $\mathfrak{H}$ by this action, one can recover the Riemann surface $\mathcal{X}$, as well as the original algebraic curve X, practically effortlessly. Well aware of these circumstances in the world of complex analysis, and spurred on further by the observation that both the ρ_X of (1.2) and the $\rho_{\mathcal{X}}$ of (4.1) fit into the same pattern of "geometric π_1 of the curve + some 'arithmetic structure' on this π_1," Mochizuki was led to pose the following question:

> Is there a p-adic analogue of the phenomenon that one can (re)construct X (every so directly and naturally!) from the representation $\rho_{\mathcal{X}}$?

In fact, the p-adic version of the Grothendieck Conjecture (Theorem 5.1) that we will discuss below (§5) may be regarded as giving a sort of affirmative answer to this question[15)].

One classical method for concretely constructing the algebraic curve X from the action of the geometric fundamental group $\pi_1(\mathcal{X})$ on $\mathfrak{H}$ is to manufacture differential forms on $\mathfrak{H}$ which are invariant under the action of $\pi_1(\mathcal{X})$. If one can manufacture enough such differential forms, then one can define a morphism

$$\phi : \mathfrak{H} \to \mathbf{P}_{\mathcal{X}}$$

from the upper half-plane $\mathfrak{H}$ to some sort of projective space $\mathbf{P}_{\mathcal{X}}$. It follows immediately from the general theory of complex manifolds that the image of this morphism is an algebraic variety; moreover, in this case, (if one imposes a certain weak technical condition on X) it follows that this image is, in fact, equal to X itself. This argument is the same as that which is used to prove, when one constructs Shimura varieties as quotients of symmetric spaces, that these quotients are, in fact, algebraic varieties. In summary, the main point of this sort of argument is that although one may ultimately conclude that the differential forms that we use to define ϕ are, in fact, algebraic, *during the construction of* ϕ, these differential forms exist only as *analytic* objects on $\mathfrak{H}$. This point of view of "dealing with analytic presentations of algebraic differential forms" will also play an important role in the proof of Theorem 5.1 which we will discuss below.

§4.3. The Relationship to p -adic Hodge Theory

With regard to proving Theorem 5.1, the analogy with the theory over the field of complex numbers which we discussed in the preceding § provides us with at least one clue, but in order to actually realize this analogy in the p-adic world, one needs to employ fairly advanced technology. This technology is provided by the p-adic Hodge theory ([F2]) of Faltings. That theory which is referred to as "p-adic Hodge theory" has a long history going back to Tate's pioneering work in the mid-1960's; what is important here, however, is the deep similarity between this theory and the Grothendieck Conjecture. The main theme of p-adic Hodge theory is the so-called "comparison theorem" between the étale cohomology (equipped with its natural Galois action) and the de Rham cohomology of a variety over a p-adic field (such as a finite extension field of $\mathbf{Q}_p$). In other words, the sense, or conjecture, that there should exist some sort of "mysterious functor" that converts these two types of cohomologies into one another is the starting point of p-adic Hodge theory. Here, de Rham cohomology is an invariant of the variety obtained by compiling into a single complex the various properties of the polynomial functions and differentials of such functions on X. Observe that the set of morphisms between algebraic varieties which appears in the left-hand side of (GC2) belongs to the same world of algebraic geometry (i.e., polynomial functions). On the other hand, the geometric fundamental group equipped with its outer Galois action, which appears on the right-hand side of (GC2), is (if one ignores the difference between abelian and nonabelian), like the étale cohomology of X, an important and natural invariant of the étale site of the variety X under consideration. If one thinks about things in this way, then one sees that one may regard both the mysterious functor conjecture and the various anabelian conjectures[16)] (such as (GC2)) as asserting that some sort of "comparison theorem" — which realizes the philosophy

"Algebro-Geometric Structure $\Longleftrightarrow$ Étale Topology + Galois Action"

— holds. Let us remark, however, that although there is this general sort of "categorical similarity" between p-adic Hodge theory and the Grothendieck Conjecture, the gap between "abelian" and "nonabelian/anabelian" is highly nontrivial. Bridging this gap was thus a major technical obstacle that had to be surmounted in order to prove Theorem 5.1.

§5. The Grothendieck Conjecture over Local Fields

§5.1. The Main Theorem

In the following, we shall fix a prime number p, and we shall refer to any field which may be realized as a subfield of a finitely generated extension field of $\mathbf{Q}_p$ as a "sub-p-adic field." Typical examples of sub-p-adic fields are finitely generated extension fields of $\mathbf{Q}$ or $\mathbf{Q}_p$, as well as (for each positive integer N) the field obtained by taking the composite (in some algebraic closure of $\mathbf{Q}$) of all degree N extension fields of the rational number field $\mathbf{Q}$. (Note that this last example will, in general, be an infinite algebraic extension of $\mathbf{Q}$.) Mochizuki's main result ([M3]) is the following theorem:

Theorem 5.1. For any smooth algebraic variety S and any hyperbolic curve X (both) over a sub-p-adic field K, the natural maps

$$\begin{aligned}\mathrm{Hom}_K^{\mathrm{dom}}(S,X) &\to \mathrm{Hom}^{\mathrm{open}}_{\mathrm{Gal}(K)}(\pi_1(S),\pi_1(X))\\ &\to \mathrm{Hom}^{\mathrm{open}}_{\mathrm{Gal}(K)}(\pi_1^{(p)}(S),\pi_1^{(p)}(X))\end{aligned}$$

are bijections. Here, $\mathrm{Hom}_K^{\mathrm{dom}}$ denotes the "set of all dominant K-morphisms"; $\mathrm{Hom}^{\mathrm{open}}_{\mathrm{Gal}(K)}$ denotes the "set of all equivalent classes (relative to the action from the right of conjugation by $\pi_1(X_{\overline{K}})$) of open homomorphisms which are compatible with the projection to $\mathrm{Gal}(K)$"; and $\pi_1^{(p)}(V)$ is the natural pro-p analogue of $\pi_1(V)$, i.e., the quotient of $\pi_1(V)$ by $\mathrm{Ker}(\pi_1(V_{\overline{K}}) \to \pi_1^{(p)}(V_{\overline{K}}))$.

This theorem resolves conjecture (GC2) in a fairly strong form. In terms of the analogy with uniformization theory discussed in §4.2, the left-hand side is the set of S-valued points of X, i.e., the "physical entity" of the *algebraic* curve X, while the right-hand side is the set of "points" which arise directly from the "*analytic* object" consisting of the geometric fundamental group equipped with a certain arithmetic structure (i.e., the outer Galois action). In other words, just as in the case of the uniformization theory of Riemann surfaces, Theorem

5.1 asserts the equivalence of the physical entity defined by the hyperbolic *algebraic* curve and the *analytic* geometric object arising directly from the geometric fundamental group equipped with its arithmetic structure.

Moreover, as a corollary of a slight generalization (= Theorem A of [M3]) of Theorem 5.1, one has the following birational version of the Grothendieck Conjecture:

Corollary 5.2. For regular function fields L and M of arbitrary dimension over a field of constants K which is sub-p-adic, the natural map

$$\mathrm{Hom}_K(M, L) \to \mathrm{Hom}^{\mathrm{open}}_{\mathrm{Gal}(K)}(\mathrm{Gal}(L), \mathrm{Gal}(M))$$

is bijective. Here, Hom_K denotes the "set of ring homomorphisms over K"; and $\mathrm{Hom}^{\mathrm{open}}_{\mathrm{Gal}(K)}$ denotes the "set of equivalence classes (relative to the action from the right of conjugation by $\mathrm{Gal}(M \otimes_K \overline{K})$) of open homomorphisms which are compatible with the projection to $\mathrm{Gal}(K)$."

When the base field K is finitely generated over the rational number field, F. Pop proved an isomorphism version of this result prior to [M3] using a completely different method ([P2]).

Remarks. (i) Theorem 5.1 is stated as a result concerning varieties and hyperbolic curves over a field K, but in fact, a similar theorem to Theorem 5.1 holds if one takes for one's base any smooth algebraic variety over a sub-p-adic field (i.e., as opposed to just a sub-p-adic field, as in Theorem 5.1), and then lets S and X be smooth families over B of algebraic varieties and hyperbolic curves, respectively. In fact, such a result follows immediately (by observing that the function field of such a B is again a sub-p-adic field) from Theorem 5.1.

(ii) Another consequence of Theorem 5.1 is an isomorphism version of (GC2) for algebraic surfaces that may be obtained as the total space of a smooth family of hyperbolic curves over a base space which is itself a hyperbolic curve. For more details, we refer to [M4].

§5.2. Sketch of the Proof of Theorem 5.1

Let us continue this discussion by restricting to the most essential case, where the base field K is a finite extension of $\mathbf{Q}_p$. Moreover, for simplicity, let us assume that X and S are proper, non-hyperelliptic hyperbolic curves. Indeed, these various conditions have nothing to do with the essence of the proof, so the general case may be reduced immediately to the case which one assumes that these conditions hold. Finally, in Theorem 5.1, a total three Hom's appear, but we shall concentrate on the map between the first and third Hom's, since it is the most essential of the various maps that appear. The problem then is how to reconstruct X from $\pi_1^{(p)}(X) \to \mathrm{Gal}(K)$.

First, we let $T \stackrel{\mathrm{def}}{=} \pi_1^{(p)}(X_{\overline{K}})^{\mathrm{ab}}$. Thus, if X is a curve of genus g, then T is a free $\mathbf{Z}_p$-module of rank $2g$, which also admits a natural structure of $\mathrm{Gal}(K)$-module. Now as a consequence of the oldest part of "p-adic Hodge theory," which, in fact, goes back to Tate, if we denote the p-adic completion of $\overline{K}$ by $\mathbf{C}_p$, then we have a natural isomorphism:

$$(T \otimes_{\mathbf{Z}_p} \mathbf{C}_p)^{\mathrm{Gal}(K)} \cong D_X \stackrel{\mathrm{def}}{=} H^0(X, \omega_{X/K})$$

where the left-hand side is the $\mathrm{Gal}(K)$-invariant part of the module in parentheses, and the right-hand side is the g-dimensional K-vector space consisting of all the everywhere-regular differentials on X. Next, if we denote the projective space defined by D_X by the notation $\mathbf{P}_X$, then one knows from elementary algebraic geometry (by the assumption that X is non-hyperelliptic) that X may be canonically embedded inside $\mathbf{P}_X$. In another words, we have already succeeded in recovering completely group-theoretically from ρ_X the space $\mathbf{P}_X$, which serves as a "canonical container" for our curve X. Thus, the problem that we must solve is how to recover group-theoretically a certain special subvariety (namely, X) of $\mathbf{P}_X$.

At this point, we ask the reader to recall the analytic morphism $\phi : \mathfrak{H} \to \mathbf{P}_{\mathcal{X}}$ which appeared in §4.2. As was discussed in detail in §4.2, this morphism is defined by constructing algebraic differentials as analytic objects. Taking this as a hint, we would like to carry out an analogous (in some sense) construction in the present p-adic situation. Thus, we must determine what will take the place (in the p-adic case) of the upper half-plane $\mathfrak{H}$. In the proofs of [M2] and [M3], the role of the upper half-plane is played by a certain field which is obtained by first completing the function field of X at a p-adic valuation with certain "good properties," then taking the maximal tame extension of this completion, and finally, p-adically completing this maximal tame extension. In the following, we shall denote this field[17)] by L. This field L is, just like the finite extensions of $\mathbf{Q}_p$, a complete valuation field equipped with a p-adic valuation, but, unlike finite extensions of $\mathbf{Q}_p$, it contains one "geometric dimension." For instance, one manifestation of this geometric dimension is the fact that the residue field of L is the maximal separated extension of a function field in one variable over a finite field. Another important property of L, which follows immediately from its definition, is that it admits a natural (tautological) morphism

$$\xi : \mathrm{Spec}(L) \to X$$

Yet another remarkable property of this field L is that its isomorphism class does not depend on the moduli of X. This property is reminiscent of the fact that the isomorphism class (as a Riemann surface) of $\tilde{\mathcal{X}} \cong \mathfrak{H}$ does not depend on the moduli of $\mathcal{X}$.

One more thing guaranteed by the existence of the geometric dimension of L is the property that if one pulls back (by ξ) a nonzero differential on X to L to obtain a differential on $\mathrm{Spec}(L)$, then this pulled-back differential will always be nonzero. Thus, the operation of pulling back a differential on X to $\mathrm{Spec}(L)$ is a faithful operation, and, in fact, one may even regard this pulled-back differential as a sort of "analytic presentation" of the original algebraic differential. Relative to the analogy with the complex analytic case, this operation corresponds to the operation of pulling back a differential on a compact (hyperbolic) Riemann surface $\mathcal{X}$ to the upper half-plane $\mathfrak{H} \cong \tilde{\mathcal{X}}$ (where it has an "analytic presentation").

Now we would like to return to the problem of reconstructing X as a subvariety of $\mathbf{P}_X$ group-theoretically. As a consequence of Faltings' p-adic Hodge theory, any continuous homomorphism $\alpha : \mathrm{Gal}(L) \to \pi_1^{(p)}(X)$ (which satisfies certain weak, group-theoretic conditions) defines a morphism

$$\phi_\alpha : \mathrm{Spec}(L) \to \mathbf{P}_X$$

over K. In other words, for "analytic L-rational points," one obtains a p-adic analytic morphism ϕ_α which is analogous to the morphism $\phi : \mathfrak{H} \to \mathbf{P}_{\mathcal{X}}$ that appeared in the complex analytic discussion of §4.2. The problem then is to determine what happens to the image of the morphism ϕ_α. For instance, if α arises[18)] from a "geometric" L-rational point (i.e., element of $X(L)$) like ξ, then the closure of the scheme-theoretic image of ϕ_α coincides precisely with X. Thus,

if we can rewrite the condition "α arises geometrically" in terms in which, among the various objects associated to X, only $\pi_1^{(p)}(X) \to \mathrm{Gal}(K)$ appears *explicitly*,

then the proof of Theorem 5.1 will be complete.

At this point, we make use of the following argument, which was inspired by the proof of Tamagawa[19)]. The homomorphism α defines a section $\alpha_L : \mathrm{Gal}(L) \to \pi_1^{(p)}(X_L)$ of the arithmetic fundamental group $\pi_1^{(p)}(X_L) \to \mathrm{Gal}(L)$ of the curve X_L obtained by base-changing X from K to L. The image $\mathrm{Im}(\alpha_L)$ of this section homomorphism α_L in $\pi_1^{(p)}(X_L)$ forms a closed subgroup of $\pi_1^{(p)}(X_L)$ which is isomorphic to $\mathrm{Gal}(L)$. Thus, for each open subgroup $H \subseteq \pi_1^{(p)}(X_L)$ that contains this image, we obtain a finite étale cover $Y^H \to X_L$. Here, Y^H is a hyperbolic curve which is geometrically connected over L. Moreover, it is important to note that the "family of coverings" obtained by taking all the coverings $\{Y^H \to X_L\}$ which arise in this way *depends* on α. Thus, one can formulate the following condition on the section homomorphism α_L which arises from the homomorphism α:

(∗) For every open subgroup H of $\pi_1^{(p)}(X_L)$ which contains $\mathrm{Im}(\alpha_L)$, the set of L-rational points $Y^H(L)$ of Y^H is nonempty.

Let us suppose that this we know that this condition holds. If one then allows the open subgroup H to vary in a suitable fashion, then, since $Y^H(L) \neq \emptyset$, the various points of $Y^H(L)$ map down to points of $X_L(L)$. On the other hand, by applying the mod p^N version of [F2], one sees that, for each point of $X_L(L)$ which arises in this way, one can construct the mod p^N version of the preceding map ϕ_α; moreover, by using these maps, one can prove that the points of $X_L(L)$ that arise in this way necessarily converge to a certain specific point $x_\infty \in X_L(L)$. In fact, it also follows immediately from this construction that the homomorphism $\mathrm{Gal}(L) \to \pi_1^{(p)}(X)$ that arises from this point x_∞ necessarily coincides with the original homomorphism α. In other words, we have shown the geometricity of α. Thus, in summary, if we can just show that the condition (∗) that we just imposed on α_L is, in fact, purely "group-theoretic," then the proof of Theorem 5.1 will be complete.

The problem now is to find a "group-theoretic" criterion for the existence of an L-rational point of Y^H. In the present p-adic context, this problem is not amenable to a direct approach of "counting the number of rational points" as in the finite field case treated by Tamagawa, so one must resort to the following somewhat less direct argument. That is to say, instead of thinking about L-rational *points*, one must consider the existence of *line bundles* (of degree prime to p) which are rational over L. One reason for this is that line bundles define Chern classes, hence can be regarded as classes in the étale cohomology of the curve Y^H; moreover, the étale cohomology of a hyperbolic curve is naturally isomorphic to the group cohomology of its arithmetic fundamental group, hence is an entirely "group-theoretic" object. Thus, we see that the problem boils down to giving a group-theoretic characterization of those classes inside the relevant cohomology group that arise as the Chern classes of line bundles of degree prime to p. This problem may be handled[20)] by applying the theory of the p-adic exponential map of [BK]. In other words, unlike the case of L-rational *points* on Y^H, L-rational *line bundles* (of degree prime to p) admit a relatively straightforward group-theoretic existence criterion. On the other hand, one sees easily from elementary algebraic geometry that once one knows the existence of an L-rational line bundle of degree prime to p on Y^H, one can conclude the existence of an L-rational *ample* line bundle of degree prime to p on Y^H. Thus, by writing this line bundle as an effective divisor (which is étale over L), one sees that Y^H admits a rational point over an extension field of L whose degree (over L) is prime to p. On the other hand, since such an extension field is necessarily a tame extension of L, and since, moreover, L, by its very definition, does not have any nontrivial tame extensions, we thus conclude that Y^H already admits a rational point over L. In other words, the existence criterion for a line bundle as above is automatically also an existence criterion for L-rational points. Thus, by establishing this existence criterion, we see that we have completed the proof of Theorem 5.1.

Footnotes

1) A topological group which can be written as a projective limit of finite groups is called a *profinite group*. Equivalently, a profinite group is a compact, totally disconnected Hausdorff topological group.

2) For profinite groups, the open subgroups are the same as the closed subgroups of finite index.

3) Recent work of Tamagawa has begun to illuminate the extent to which, in positive characteristic, the geometric fundamental group depends quite essentially on the moduli of the curve in question. See [H], as well as §3.3 of the present paper, for more details.

4) Grothendieck indicates that in addition to hyperbolic algebraic curves, successive smooth fibrations of such curves, as well as moduli spaces of such curves should be considered as candidates for anabelian varieties (cf., e.g., [M4]). Recent work suggests that as a necessary condition for anabelianness, the geometric fundamental group should be more like a free group than like a matrix group (see [IN]).

5) For instance, in the case of elliptic curves without complex multiplication, if one combines various results of Faltings, one can argue that in fact, there is only one possibility (cf. [N6], 5.4).

6) If one writes K_∞ for the field obtained by adjoining all roots of unity to the base field K, then it is also conjectured that the sections arising from K-rational points of X may be characterized as those such that the action of $\alpha(\mathrm{Gal}(K_\infty))$ on $\pi_1(X_{\overline{K}})$ by conjugation does not admit any nontrivial fixed points.

7) This suggests that Grothendieck had in mind the "category-theoretic ideal" of thinking of X as a variable and reconstructing the set of X-rational points $Y(X) = \mathrm{Hom}(X, Y)$ of Y from the arithmetic fundamental group. The first person to (at least partially) realize this ideal was Mochizuki ([M3]) — cf. §5.

8) The fact that distinct rational points induce nonconjugate section homomorphisms was

shown by Grothendieck ([G3]) as an application of the Mordell-Weil Theorem. As an application of this fact, one can show the algebro-geometric analogue of the "Sunada Conjecture" of complex hyperbolic geometry for certain hyperbolic algebraic varieties (cf. [N5], [N7] 2.2). Moreover, Mochizuki has derived a pro-p version of the fact that "distinct rational points define nonconjugate section homomorphisms" from Theorem 5.1 (cf. [M3], Theorem C).

9) As far as this is concerned, one has the contributions of F.Pop ([P1,2]) and of Mochizuki (cf. §5). Moreover, Pop's work — including his method — builds on the long tradition of research on the "reconstitution of a number field from its absolute Galois group," starting with the original ideas of J. Neukirch ([Ne]) in the late 1960's, continuing with the work of M. Ikeda and K. Iwasawa, and finally, culminating in the late 1970's with the work of K. Uchida.

10) For a profinite group G, one refers to as the maximal pro-l quotient of G the largest quotient topological group of G which may be written as a projective limit of finite l-groups (i.e., finite groups whose order is a power of the prime number l).

11) As is implicit in the preface of [I1], Ihara began, from his own original point of view, the construction of a nonabelian class field theory for modular function fields over finite fields in the 1960's, and, by the beginning of the 1970's, had shown such things as the fact that among the tame coverings of $\mathbf{P}^1_\lambda - \{0, 1, \infty\}$ over $\mathbf{F}_{p^2}$, those which are controlled by the (congruence) subgroups of $\mathrm{SL}_2(\mathbf{Z}[\frac{1}{p}])$ may be characterized by the arithmetic condition of "complete decomposition of the set of supersingular λ-primes." This sort of research concerning the deep arithmeticity contained in the fundamental group of the projective line minus three points was spawn from Ihara's original (nonabelian) class field theory point of view, hence is of a completely different origin from Grothendieck's motivation (discussed in §1.1) for constructing an "algebro-geometric Galois theory." Moreover, the paper of Deligne contained in [2] deals with the issue of making the fundamental group of the projective line minus three points into a unipotent algebraic group in the context of the philosophy of motives; this approach may also be said to be of a distinct origin from those of Grothendieck and Ihara.

12) For the progress that occurred during this period, we refer mainly to [I2], as well as the papers contained in [1].

13) Here, we shall refer to the natural one-dimensional l-adic representation $\mathbf{Z}_l(1)$ arising from the action of the Galois group on the roots of unity simply as the "cyclotomic action (representation)," and we shall call the tensor product representation of this representation with the permutation representation on the set of cuspidal points as the "cyclotomic permutation representation."

14) This is the conjecture to the effect that a curve of genus at least 2 over a number field has only finitely many rational points. It was proven by Faltings in the same paper as the one in which the Tate Conjecture was proven ([F1]).

15) In fact, another affirmative answer to this question, albeit of a somewhat different nature, has also been obtained (cf. [M5-8] for more details).

16) In fact, the existence of the mysterious functor was also predicted by none other than Grothendieck himself. On the other hand, as far as the relationship between these two conjectures is concerned, there is no record that Grothendieck recognized — the general similarity in form of the two conjectures notwithstanding — that this relationship was so close as to

give rise to a proof of the sort that will be discussed in §5.2. Concerning the circumstances surrounding this state of affairs, we refer to the discussion of §4.1.

17) In fact, if one takes this as the definition of L, the following argument becomes slightly inaccurate, but in the interest of minimizing the introduction of inessential technical details, we hope that the reader will forgive this minor transgression.

18) The phrase "arises from a geometric rational point $\mathrm{Spec}(L) \to X$" means that it arises as the morphism $\mathrm{Gal}(L) = \pi_1(\mathrm{Spec}(L)) \to \pi_1(X) \to \pi_1^{(p)}(X)$ obtained by applying the functor π_1 to some morphism $\mathrm{Spec}(L) \to X$.

19) For more details, we refer to §3.1, (i).

20) For more details, we refer to [M3].

References

[AI] G.Anderson, Y.Ihara, *Pro-l branched coverings of* $\mathbf{P}^1$ *and higher circular l-units, Part 1*, Ann. of Math. **128** (1988), 271–293; *Part 2*, Intern. J. Math. **1** (1990), 119–148.

[B] G.V.Belyi, *On Galois extensions of a maximal cyclotomic field*, Izv. Akad. Nauk. SSSR **8** (1979), 267–276 (Russian); English transl. in Math. USSR Izv. **14** (1980), no. 2, 247–256.

[BK] S.Bloch, K.Kato, *L-functions and Tamagawa numbers of motives*, The Grothendieck Festschrift, Volume I, Birkhäuser, 1990, pp. 333–400.

[F1] G.Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), 349–366.

[F2] ———, *p-adic Hodge theory*, J. of the Amer. Math. Soc. **1** (1988), 255–299.

[SGA1] A.Grothendieck, M.Raynaud, *Revêtement Etales et Groupe Fondamental (SGA1)*, Lecture Note in Math., vol. 224, Springer, Berlin Heidelberg New York, 1971.

[G1] A.Grothendieck, *La longue marche à travers de la théorie de Galois, 1981*, in preparation by J.Malgoire (first few chapters available since 1996).

[G2] ———, *Esquisse d'un Programme, 1984*, in [6] vol.1, 7–48.

[G3] ———, *Letter to G.Faltings, June 1983*, in [6] vol.1, 49–58.

[H] D.Harbater, *Fundamental groups of curves in characteristic p*, Proc. ICM, Zürich (1994), 654–666.

[I1] Y.Ihara, *Profinite braid groups, Galois representations, and complex multiplications*, Ann. of Math. **123** (1986), 43–106.

[I2] ———, *Braids, Galois groups and some arithmetic functions*, Proc. ICM, Kyoto (1990), 99–120.

[IN] Y.Ihara, H.Nakamura, *Some illustrative examples for anabelian geometry in high dimensions*, in [6] vol.1, 127–138.

[MT] M.Matsumoto, A.Tamagawa, *Mapping-class-group action versus Galois action on profinite fundamental groups*, Preprint 1997.

[M1] S.Mochizuki, *The profinite Grothendieck conjecture for hyperbolic curves over number fields*, J. Math. Sci., Univ. Tokyo **3** (1996), 571–627.

[M2] ———, *The local pro-p Grothendieck conjecture for hyperbolic curves*, RIMS Preprint 1045, Kyoto Univ. (1995).

[M3] ———, *The local pro-p anabelian geometry of curves*, RIMS Preprint 1097, Kyoto Univ. (1996).

[M4] ———, *A Grothendieck conjecture-type result for certain hyperbolic surfaces*, RIMS Preprint 1104, Kyoto Univ. (1996).

[M5] ———, *A theory of ordinary p-adic curves*, Publ. of RIMS **32** (1996), 957–1151.

[M6] ———, *The generalized ordinary moduli of p-adic hyperbolic curves*, RIMS Preprint 1051, Kyoto Univ. (1995).

[M7] ———, *Combinatorialization of p-adic Teichmüller theory*, RIMS Preprint 1076, Kyoto Univ. (1996).

[M8] ———, *Correspondences on hyperbolic curves*, J. Pure Appl. Algebra **131** (1998), 227–244.

[N1] H.Nakamura, *Rigidity of the arithmetic fundamental group of a punctured projective line*, J. reine angew. Math. **405** (1990), 117–130.

[N2] ———, *Galois rigidity of the étale fundamental groups of punctured projective lines*, J. reine angew. Math. **411** (1990), 205–216.

[N3] ———, *On galois automorphisms of the fundamental group of the projective line minus three points*, Math. Z. **206** (1991), 617–622.

[N4] ———, *Galois rigidity of pure sphere braid groups and profinite calculus*, J. Math. Sci., Univ. Tokyo **1** (1994), 71–136.

[N5] ———, *Galois rigidity of algebraic mappings into some hyperbolic varieties*, Intern. J. Math. **4** (1993), 421–438.

[N6] ———, *On exterior Galois representations associated with open elliptic curves*, J. Math. Sci., Univ. Tokyo **2** (1995), 197–231.

[N7] ———, *Fukuyugengun no Garoa Gosei*, Sugaku **47** (1995), 1–17; English translation to appear in *Sugaku Exposition* (AMS).

[NTa] H.Nakamura, N.Takao, *Galois rigidity of pro-l pure braid groups of algebraic curves*, Trans. Amer. Math. Soc. (to appear).

[NTs] H.Nakamura, H.Tsunogai, *Some finiteness theorems on Galois centralizers in pro-l mapping class groups*, J. reine angew. Math. **441** (1993), 115–144.

[Ne] J.Neukirch, *Kennzeichnung der p-adischen und der endlichen algebraischen Zahlkörper*, Invent. math. **6** (1969), 296–314.

[O1] T.Oda, *A note on ramification of the Galois representation on the fundamental group of an algebraic curve*, J. Number Theory **34** (1990), 225–228.

[O2] ———, *A note on ramification of the Galois representation on the fundamental group of an algebraic curve, II*, J. Number Theory **53** (1995), 342–355.

[P1] F.Pop, *On Grothendieck's conjecture of birational anabelian geometry*, Ann. of Math. **138** (1994), 145–182.

[P2] ———, *On Grothendieck's conjecture of birational anabelian geometry II*, Preprint (June 1995).

[T1] A.Tamagawa, *The Grothendieck conjecture for affine curves*, Compositio Math. **109** (1997), no. 2, 135–194.

[T2] ———, *On the fundamental groups of curves over algebraically closed fields of characteristic* > 0, Preprint 1997.

[U] K.Uchida, *Isomorphisms of Galois groups of algebraic function fields*, Ann. of Math. **106** (1977), 589–598.

---

[1] Y.Ihara (ed.), *Galois Representations and Arithmetic Algebraic Geometry*, Advanced Studies in Pure Math., vol. 12, Kinokuniya Co. Ltd., North-Holland, 1987.

[2] Y.Ihara, K.Ribet, J.-P.Serre (eds.), *Galois Groups over* $\mathbf{Q}$, Math. Sci. Res. Inst. Publications, vol. 16, Springer, 1989.

[3] J.-P.Serre, *Topics in Galois Theory*, Jones and Bartlett Publ., 1992.

[4] L.Schneps (ed.), *The Grothendieck Theory of Dessins d'Enfants*, London Math. Soc. Lect. Note Ser., vol. 200, Cambridge Univ. Press, 1994.

[5] M.Fried et al. (eds.), *Recent Developments in the Inverse Galois Problem*, Contemp. Math., vol. 186, AMS, 1995.

[6] L.Schneps, P.Lochak (eds.), *Geometric Galois Actions; 1.Around Grothendieck's Esquisse d'un Programme, 2.The Inverse Galois Problem, Moduli Spaces and Mapping Class Groups*, London Math. Soc. Lect. Note Ser., vol. 242-243, Cambridge Univ. Press, 1997.