A Version of the Grothendieck Conjecture for p-adic Local Fields

by Shinichi MOCHIZUKI*

Section 0: Introduction

The purpose of this paper is to prove an absolute version of the Grothendieck Conjecture for local p-adic fields (given as Theorem 4.2 in the text):

Theorem : *Let K and K' be finite extensions of $\mathbf{Q}_p$. Let $Isom_{\mathbf{Q}_p}(K, K')$ denote the set of $\mathbf{Q}_p$-algebra isomorphisms of K with K'. Let $Out_{Filt}(\Gamma_K, \Gamma_{K'})$ denote the set of outer isomorphisms of filtered groups between the absolute Galois groups of K and K' equipped with the filtrations defined by the higher (i.e., with index > 0) ramification groups in the upper numbering. Then the natural morphism*

$$Isom_{\mathbf{Q}_p}(K, K') \to Out_{Filt}(\Gamma_K, \Gamma_{K'})$$

induced by "looking at the morphism induced on absolute Galois groups" is a bijection.

On the one hand, one knows (cf. the Remark in [4] following Theorem 4.2) that the Grothendieck Conjecture cannot hold in the naive sense (i.e., if one removes the condition of "compatibility with the filtrations" from the outer isomorphisms considered – see, e.g., [8]), so one must put *some* sort of condition on the outer isomorphisms of Galois groups that one considers. The condition discussed here is that they preserve the higher ramification groups. One can debate how natural a condition this is, but at least it gives some sort of idea of how "good" an outer isomorphism of Galois groups must be in order to arise "geometrically."

Historical Remark: I originally set out to prove the naive version of the above Theorem, only to discover that this was, in fact, false. Thus, I decided to add the "preservation of filtration" condition because this seemed to be a sort of minimal natural condition that would allow me to complete the proof that I had envisaged (i.e., the proof discussed in this paper). Later, after submitting this paper for publication, I was informed, however, by the referee that in fact, just such a result (as the above Theorem) had been explicitly

1980 Mathematics Subject Classification: 12B15
* Research Institute for Mathematical Sciences, Kyoto University, Kyoto 606, Japan; email: motizuki@kurims.kyoto-u.ac.jp

conjectured in discussions following a talk at the Institute for Advanced Study in Princeton in the Fall of 1993, and, moreover, that this conjecture may have existed in the "folklore" even earlier than this. At the time I proved this result, however, I was entirely unaware that this result had, in fact, been conjectured by others.

Theorem 4.2 is proved by first showing that outer isomorphisms of the type considered necessarily take Hodge-Tate representations to Hodge-Tate representations; then one concludes by using a well-known classification result for abelian Hodge-Tate representations. Thus, Theorem 4.2 can be regarded as an application of p-adic Hodge theory. In fact, careful inspection will reveal that the proof of Theorem 4.2 runs, in many respects, in a fashion parallel to the proof of the main result of [7] (although it is, of course, technically much simpler than the proof of [7]).

The result of this paper was motivated by a question of A. Schmidt relative to the results of [7]: Namely, in [7], a *relative* Grothendieck Conjecture-type result for hyperbolic curves over local p-adic fields was proven. The question of A. Schmidt was whether or not such a result could be extended to an absolute Grothendieck Conjecture-type result for hyperbolic curves over local p-adic fields. At the present time, the author is unable to prove such an absolute result, but nonetheless, it seems that a result such as Theorem 4.2 (whose proof belongs to the same circle of ideas as the proof of the main result of [7]) might be a useful first step in this direction.

Finally, the author would like to thank A. Tamagawa for useful discussions during which he presented the proof of Theorem 4.2, as well as A. Schmidt for posing (via email) the motivational question discussed above.

Section 1: The Cyclotomic Character and Inertia

Let p be a prime number. Let K be a *p-adic local field*. By this, we shall mean in this paper that K is a finite extension of $\mathbf{Q}_p$. Fix an algebraic closure $\overline{K}$ of K. Let $\Gamma_K \stackrel{\mathrm{def}}{=} Gal(\overline{K}/K)$. The purpose of this paper is to examine to what extent K can be recovered "group-theoretically" from Γ_K. Here (and throughout the paper), when we say that an object associated to K can be recovered "group-theoretically" from Γ_K, we mean that given another local p-adic field K', together with an isomorphism of topological groups $\alpha : \Gamma_K \cong \Gamma'_K$, the object associated to K is necessarily taken by α to the corresponding object associated to K'. That is to say, the use of this term "group-theoretically" is the same as in [7]. In this first Section, we observe that the cyclotomic character and the inertia subgroup of Γ_K can be recovered group-theoretically from Γ_K. It should be remarked that the results of this Section are well-known (see the Remark at the end of this Section for bibliographical information).

We begin by reviewing duality. Suppose that M is a $\mathbf{Z}_p$-module of finite length equipped with a continuous Γ_K-action. Then one knows (see, e.g., [2], Proposition 3.8) that one has a natural isomorphism of Galois cohomology modules

$$H^i(K, M) \cong H^{2-i}(K, M^\vee(1))^\vee$$

for $i \geq 0$. Here, the "(1)" is a Tate twist, and the superscripted "$\vee$"'s denote the "Pontrjagin dual" (i.e., $Hom(-, \mathbf{Q}_p/\mathbf{Z}_p)$). Suppose that M is isomorphic as a $\mathbf{Z}_p$-module to $\mathbf{Z}/p^n\mathbf{Z}$ (for some $n \geq 1$). Then it follows from the above isomorphism that M is isomorphic as a Γ_K-module to $\mathbf{Z}/p^n\mathbf{Z}(1)$ if and only if $H^2(K, M) \cong \mathbf{Z}/p^n\mathbf{Z}$. This is clearly a group-theoretic condition on M. Thus, we conclude that the isomorphism class of the Γ_K-module $\mathbf{Z}_p(1)$ can be recovered group-theoretically from Γ_K.

Proposition 1.1: *The cyclotomic character $\chi : \Gamma_K \to \mathbf{Z}_p{}^\times$ can be recovered entirely group-theoretically from Γ_K.*

Now recall from local class field theory (see, e.g., [3]) that we have a natural isomorphism

$$\Gamma_K^{ab} \cong (K^\times)^\wedge$$

where the superscripted "ab" denotes the abelianization, and "$(K^\times)^\wedge$" denotes the profinite completion of $K^\times = K - \{0\}$. Let k be the residue field of $\mathcal{O}_K$ (the ring of integers of K). Thus, k is the field of $q = p^f$ elements. Now it is well-known that $(K^\times)^\wedge$ fits into an exact sequence of topological groups:

$$0 \to U_K \to (K^\times)^\wedge \to \widehat{\mathbf{Z}} \to 0$$

where $U_K \stackrel{\mathrm{def}}{=} \mathcal{O}_K^\times$. In particular, one thus sees that the prime-to-p part of the torsion subgroup of $(K^\times)^\wedge$ has precisely $q - 1$ elements, and that the pro-p quotient of $(K^\times)^\wedge$ is the direct sum of a torsion group and a free $\mathbf{Z}_p$-module of rank $[K : \mathbf{Q}_p] + 1$. (Here we use the p-adic logarithm on an open subgroup of U_K to identify it (modulo torsion) with an open subgroup of K.) Thus, it follows from the above isomorphism that

Proposition 1.2: *The number q of elements in the residue field of $\mathcal{O}_K$, and well as the absolute degree $[K : \mathbf{Q}_p]$ of K, can be recovered entirely group-theoretically from Γ_K.*

Now let $H \subseteq \Gamma_K$ be an open subgroup. Let $L \supseteq K$ be the extension field of K corresponding to H. By applying Proposition 1.2 to L and H, we see that the number q_L of elements in the residue field of $\mathcal{O}_L$ can be recovered group-theoretically from $H \subseteq \Gamma_K$. Note, moreover, that L is unramified over K if and only $q_L = q^{[\Gamma_K : H]}$. Thus, we see that we have obtained the following

Corollary 1.3: *The inertia subgroup $I_K \subseteq \Gamma_K$ can be determined group-theoretically from Γ_K.*

Remark: It follows, in particular, from the results of this Section that (i) $[K : \mathbf{Q}_p]$ and (ii) the maximal abelian (over $\mathbf{Q}_p$) subfield of K are determined group-theoretically by Γ_K. That (i) and (ii) are determined by Γ_K is stated in [4] (the Remark following Theorem 4.2), although the proofs of these facts given in the references of [4] are somewhat different both in substance and in point of view from what we have done in this Section. Moreover, the content of Propositions 1.1 and 1.2 is also essentially contained in [8], and Corollary 1.3 is explicitly stated in §1 of [9].

Section 2: Higher Ramification Groups

Recall that the p-adic logarithm defines a natural isomorphism of U_K (modulo torsion) onto an open subgroup of K. In particular, it defines an isomorphism of $U_K \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ with K. Now, for any finite extension L of K (corresponding to some subgroup $\Gamma_L \subseteq \Gamma_K$), we have a commutative diagram

$$\begin{array}{ccc} U_K \otimes_{\mathbf{Z}_p} \mathbf{Q}_p & \longrightarrow & U_L \otimes_{\mathbf{Z}_p} \mathbf{Q}_p \\ \big\downarrow{\scriptstyle log} & & \big\downarrow{\scriptstyle log} \\ K & \longrightarrow & L \end{array}$$

(where the horizontal maps are the natural inclusions). Moreover, if we regard U_K (respectively, U_L) as a subgroup of Γ_K^{ab} (respectively, Γ_L^{ab}) then the morphism $U_K \to U_L$ may be recovered group-theoretically by means of the "Verlagerung, or transfer, map" (see, e.g., [6], Chapter VII, §8). We thus obtain the following result:

Proposition 2.1: *The Γ_K-module $\overline{K}$ may be recovered group-theoretically from Γ_K.*

Note, however, that at this point, the *multiplicative structure on* $\overline{K}$ (i.e., its structure as a field, as opposed to just as an additive group with Γ_K-action) has yet to be recovered group-theoretically.

Now let $v \geq 0$ be a real number. Then we shall denote by $\Gamma_K^v \subseteq \Gamma_K$ the *higher ramification group associated to the number v in the "upper numbering"* (see, e.g., [3], p. 155). Let us denote by $U_K^v \subseteq U_K$ the subgroup $1 + m_K^n$, where $m_K \subseteq \mathcal{O}_K$ is the maximal ideal, and n is the unique integer for which $n - 1 < v \leq n$. Then it is well-known (Theorem 1 of [3], p. 155) that the image of Γ_K^v in Γ_K^{ab} is equal to $U_K^v \subseteq U_K$. Let e_K be the *absolute ramification index of* K (i.e., the ramification index of K over $\mathbf{Q}_p$). Note that, by Proposition 1.2, it follows that e_K can be recovered group-theoretically from Γ_K. Suppose that we are given (in addition to Γ_K) the subgroup $\Gamma_K^v \subseteq \Gamma_K$ for some $v = r \cdot e_K$, where $r \geq 2$ is an integer. Then it follows that we know the subgroup $U_K^v \subseteq U_K$. Moreover, it follows from the theory of the p-adic logarithm (see, e.g., [5], Chapter IV, §1) that the submodule

$$p^{-r} \cdot U_K^v \subseteq U_K \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$$

corresponds to the submodule $\mathcal{O}_K \subseteq K$ under the isomorphism induced by the p-adic logarithm.

Now let us denote by $\overline{K}^\wedge$ the *p-adic completion of the field $\overline{K}$*. Thus, $\overline{K}^\wedge$ is the quotient field of the p-adic completion of the ring of integers $\mathcal{O}_{\overline{K}}$. Then we see that we have obtained the following result:

Proposition 2.2: *Suppose that we are given the following group-theoretic data: the topological group Γ_K, together with the indexed filtration Γ_K^v for all $v > 0$. Then the Γ_K-modules $\mathcal{O}_{\overline{K}}$, and $\overline{K}^\wedge$ can be recovered group-theoretically from this group-theoretic data.*

Proof: To obtain $\mathcal{O}_{\overline{K}}$, we simply apply the above discussion to finite extensions L of K, and use Proposition 2.1. Note that when we pass to an open subgroup $\Gamma_L \subseteq \Gamma_K$, since the upper numbering is not compatible with passage to subgroups, one must first convert to the lower numbering (which *is* compatible with passage to subgroups), and then convert back to the upper numbering for Γ_L. (See, e.g., [6], Chapter IV, for more details on the properties of the upper and lower numberings.) It is for this reason that we need *all* the Γ_K^v for $v > 0$ (note that we already have $\Gamma_K^0 = I_K$ by Corollary 1.3), rather than just Γ_K^v for sufficiently large v.

To obtain $\overline{K}^\wedge$, we note that $\overline{K}^\wedge$ is just the p-adic completion of $\mathcal{O}_{\overline{K}}$ tensored over $\mathbf{Z}_p$ with $\mathbf{Q}_p$. $\bigcirc$

Before proceeding, it will be convenient to formalize the hypothesis of the preceding Proposition. Let G be a topological group. We would like to consider filtrations G^v on G indexed by a real number v, as follows:

Definition 2.3: *We shall call a collection of closed normal subgroups $\{G^v\}$ of G (where v ranges over all positive real numbers) a filtration on G if $G^{v_1} \subseteq G^{v_2}$ whenever $v_1 \geq v_2$.*

There are obvious notions of morphisms and isomorphisms between filtered groups, which we leave to the refer to formalize. Moreover, because of the normality assumption on the G^v, there is also a notion of *outer isomorphisms* (i.e., isomorphisms, considered modulo inner isomorphisms) between filtered groups. Note that Γ_K is equipped with a natural filtration defined by the Γ_K^v. Thus, Proposition 2.2 may be reformulated as stating that the Γ_K-module $\overline{K}^\wedge$ may be recovered group-theoretically from the filtered group Γ_K.

Section 3: Hodge-Tate Representations

Next, let us observe the following formal consequence of Proposition 2.2: Let V be a finite dimensional $\mathbf{Q}_p$-vector space equipped with a continuous action by Γ_K. For any integer i, let $d_V(i)$ be the $\mathbf{Q}_p$-dimension of the space of Γ_K-invariants of $V(-i) \otimes_{\mathbf{Q}_p} \overline{K}^{\wedge}$. Let d_V be the sum of the $d_V(i)$ as i ranges over all the integers. It is well-known ([1], Chapter III, §1.2) that $d_V \leq dim_{\mathbf{Q}_p}(V)$. Moreover, if $d_V = dim_{\mathbf{Q}_p}(V)$, then the Γ_K-module V is called *Hodge-Tate.*

Corollary 3.1: *Given a continuous $\mathbf{Q}_p[\Gamma_K]$-vector space of finite $\mathbf{Q}_p$-dimension, the issue of whether or not V is Hodge-Tate (as well as the invariants $d_V(i)$) can be determined entirely group-theoretically from the filtered group Γ_K.*

We shall especially be interested in the following type of representation: Let E be a finite Galois extension of $\mathbf{Q}_p$ containing K. Let us suppose that the Γ_K-module V is equipped with an E-action, and that V has dimension one over E. Thus, $End_E(V) = E$, and the Γ_K action on V is given by some representation $\rho_V : \Gamma_K \to E^\times$, which necessarily factors through Γ_K^{ab}. Now we make the following

Definition 3.2: *We shall call the $E[\Gamma_K]$-module V uniformizing if the restriction of ρ_V to some open subgroup I of U_K ($\subseteq \Gamma_K^{ab}$) is the morphism $I \to E^\times$ induced by restricting some morphism of fields $K \hookrightarrow E$ to $I \subseteq U_K \subseteq K$.*

By class field theory, it follows immediately that uniformizing V exist.

Now one knows ([1], Chapter III, Appendix, §5) that V (as in the paragraph preceding Definition 3.2) is uniformizing if and only if $d_V(1) = [E : K]$; $d_V(0) = [E : K] \cdot ([K : \mathbf{Q}_p] - 1)$. Thus, we obtain the following

Corollary 3.3: *Given a continuous $E[\Gamma_K]$-module V of E-dimension 1, the issue of whether or not V is uniformizing can be determined entirely group-theoretically from the filtered group Γ_K.*

Section 4: The Main Theorem

Let K and K' be local p-adic fields. Let us assume that we are given an isomorphism $\alpha : \Gamma_K \cong \Gamma_{K'}$ of filtered groups. Let V be a uniformizing $E[\Gamma_K]$-module, for some Galois extension E of $\mathbf{Q}_p$ which contains both K and K'. Note that α allows us to regard V also as an $E[\Gamma_{K'}]$-module. Moreover, by Corollary 3.3, it follows that V is also a uniformizing

$E[\Gamma_{K'}]$-module. Thus, it follows that there exist open submodules $I \subseteq U_K$ and $I' \subseteq U_{K'}$ such that the isomorphism $U_K \cong U_{K'}$ induced by α maps I onto I', and moreover, the resulting isomorphism $\alpha_I : I \cong I'$ fits into a commutative diagram

$$\begin{array}{ccc} I & \xrightarrow{\alpha_I} & I' \\ \downarrow & & \downarrow \\ E^\times & \xrightarrow{id_{E^\times}} & E^\times \end{array}$$

where the vertical morphisms are induced by field inclusions $\iota : K \hookrightarrow E$ and $\iota' : K' \hookrightarrow E$. Since I (respectively, I'), regarded as a subset of $U_K \subseteq K$ (respectively, $U_{K'} \subseteq K'$), generates K (respectively, K') as a $\mathbf{Q}_p$-vector space (by Lemma 4.1 below), it thus follows that $Im(\iota) = Im(\iota')$. In other words, K and K' may be realized as the same subfield of E, i.e., the field inclusions ι and ι' induce an isomorphism of fields $\alpha_K : K \cong K'$ whose restriction to $I \subseteq U_K \subseteq K$ is α_I.

Lemma 4.1 : *If $I \subseteq U_K$ is an open subgroup, then the $\mathbf{Q}_p$-vector space generated by I in K is equal to K.*

Proof: Let $Z \subseteq K$ be the $\mathbf{Q}_p$-subspace of K generated by I. Note that U_K is open in K (in the p-adic topology). Thus, I is open in K. Moreover, if $z \in Z$, then it follows from the definition of Z that $z + I \stackrel{\text{def}}{=} \{z + i \mid i \in I\}$ is also contained in Z. On the other hand, $z + I$ is open in K. Thus, it follows that Z is open in K. On the other hand, if $Z \neq K$, then (since the p-adic topology on $\mathbf{Q}_p$ is not discrete), it would follow that Z is not open in K. This contradiction shows that $Z = K$, thus completing the proof of the Lemma. ○

In other words, we have proven the following result:

Theorem 4.2: *Let K and K' be finite extensions of $\mathbf{Q}_p$. Let $Isom_{\mathbf{Q}_p}(K, K')$ denote the set of $\mathbf{Q}_p$-algebra isomorphisms of K with K'. Let $Out_{Filt}(\Gamma_K, \Gamma_{K'})$ denote the set of outer isomorphisms of filtered groups between the absolute Galois groups of K and K' equipped with the filtrations defined by the higher (i.e., with index > 0) ramification groups in the upper numbering. Then the natural morphism*

$$Isom_{\mathbf{Q}_p}(K, K') \to Out_{Filt}(\Gamma_K, \Gamma_{K'})$$

induced by "looking at the morphism induced on absolute Galois groups" is a bijection.

Proof: That this morphism is injective follows by looking at the induced isomorphism between $\Gamma_K^{ab} \cong (K^\times)^\wedge$ and $\Gamma_{K'}^{ab} \cong ((K')^\times)^\wedge$. (Alternatively, the more group-theoretically oriented reader may prefer to regard the injectivity of this morphism as a consequence of the fact that the centralizer of Γ_K in $\Gamma_{\mathbf{Q}_p}$ is trivial.) Now let us show that the morphism is surjective. Let $\alpha : \Gamma_K \cong \Gamma_{K'}$ be an isomorphism that is compatible with the filtrations. Then, in the preceding paragraph, we constructed a field isomorphism $\alpha_K : K \cong K'$. To see that the morphism induced by α_K is equal to the original α (up to composition with an inner isomorphism), it suffices simply to construct the analogues $\alpha_L : L \cong L'$ of α_K for corresponding finite extensions L and L' of K and K', and then conclude via a standard general nonsense argument. ○

Remark Concerning the Motivation for Theorem 4.2: Let X_K be a *closed* hyperbolic curve over K (as in [7]). Let Π_X be the absolute fundamental group of X_K. Thus, Π_X fits into an exact sequence of topological groups

$$1 \rightarrow \Delta_X \rightarrow \Pi_X \rightarrow \Gamma_K \rightarrow 1$$

where $\Delta_X \subseteq \Pi_X$ is the geometric fundamental group of X_K (i.e., the fundamental group of $X_K \otimes_K \overline{K}$). The main result of [7] implies that X_K can be functorially reconstructed from the morphism $\Pi_X \rightarrow \Gamma_K$. The question of A. Schmidt referred to in Section 0 was whether or not X_K can, in fact, be reconstructed from Π_X alone.

At the present time, the author has not succeeded in doing this, but nevertheless, one can make the following observations. First of all, by an argument similar to that of Proposition 1.1 (using Poincaré duality), one can at least reconstruct the cyclotomic character $\Pi_X \rightarrow \Gamma_K \rightarrow \mathbf{Z}_p{}^\times$ group-theoretically. Once one has the cyclotomic character, one can use it to consider $H^1(\Pi_X, \mathbf{Z}_p(1))$, which is surjected onto by $H^1(\Gamma_K, \mathbf{Z}_p(1))$. This allows one to reconstruct the quotient $\Pi_X \rightarrow \Pi_X/\Delta_X$ group-theoretically. What is still missing at this point, however, is an argument that would allow one to reconstruct (group-theoretically) the isomorphism $\Pi_X/\Delta_X \cong \Gamma_K$ induced by the natural morphism $\Pi_X \rightarrow \Gamma_K$. At the time of writing, the author does not see how to do this. Furthermore, the argument just discussed for reconstructing the cyclotomic character group-theoretically breaks down in the case when the curve X_K is affine. Thus, at any rate, it seems that in order to prove an "absolute Grothendieck Conjecture-type result for hyperbolic curves over local fields," some fundamentally new ideas are needed. It is hoped that Theorem 4.2 could serve as a first step in this direction.

Bibliography

[1] J.-P. Serre, *Abelian l-adic Representations and Elliptic Curves*, W. A. Benjamin, Inc., 1968.

[2] S. Bloch and K. Kato, *L-Functions and Tamagawa Numbers* in The Grothendieck Festschrift, Volume I, Birkhäuser, 1990, pp. 333-400.

[3] J.-P. Serre, *Local Class Field Theory* in *Algebraic Number Theory*, ed. J.W.S. Cassels and A. Fröhlich, Academic Press, 1967.

[4] J. Koenigsmann, *From p-rigid Elements to Valuations (with a Galois-characterization of p-adic Fields)*, *J. reine* angew. *Math.* **465** (1995), pp. 165-182.

[5] N. Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, Graduate Texts in *Mathematics* **58**, Springer Verlag, 1977.

[6] J.-P. Serre, *Local Fields*, Graduate Texts in *Mathematics* **67**, Springer Verlag, 1979.

[7] S. Mochizuki, *The Local Pro-p Grothendieck Conjecture for Hyperbolic Curves*, RIMS Preprint No. 1045, 1995.

[8] M. Jarden, J. Ritter, *On the Characterization of Lcoal Fields by their Absolute Galois Groups*, *J. Number Th.* **11** (1979), pp. 1-13.

[9] F. Pop, *Galoissche Kennzeichnung p-adisch abgescholessener Körper*, *J.* reine angew. *Math.* **392** (1988), pp. 145-175.