GALOIS REPRESENTATIONS CONNECTED WITH HYPERBOLIC CURVES

1992 Math. USSR Izv. 39 1281

(http://iopscience.iop.org/0025-5726/39/3/A10)

Изв. Акад. Наук СССР
Сер. Матем. Том 55 (1991), № 6

Math. USSR Izvestiya
Vol. 39 (1992), No. 3

UDC 512.7

GALOIS REPRESENTATIONS CONNECTED WITH HYPERBOLIC CURVES

V. A. VOEVODSKIĬ

ABSTRACT. The author considers Galois group actions on the fundamental groups of curves of hyperbolic type, and proves certain cases of Grothendieck's conjecture about the possibility of recovering a curve from its Galois representation.

INTRODUCTION

This paper is devoted to the proof of some theorems, related to the "fundamental conjectures of an abelian algebraic geometry" of Grothendieck which were formulated by him in a letter to Faltings in 1983 and in the unpublished manuscript [1]. In §1 the concept of an elementary anabelian variety is introduced and the exact formulation of these conjectures is given. Unfortunately, I was unable to prove them even in the simplest cases, and that is why I am basically concerned with a weakened version of the first of them, which I simply call *the weak conjecture.* I devote §2 to the proof of the easy parts of those conjectures. At the end the weak conjecture for curves of genus 0 is proved. A slightly different proof was independently obtained in [2]. §3 is devoted to the proof of the weak conjecture in genus 1 and to the formulation of an analogous result for hyperelliptic curves of higher genera, which is stated without proof. Finally, in §4 I discuss the question of describing the image of the Galois representations associated with curves of genus 0, which is not immediately related to Grothendieck's conjectures. The results obtained here allow me to give a description of this image modulo a conjecture of purely combinatorial nature. The results of §2 make it possible to obtain certain information about the normalizer of this image and to reduce the first conjecture for genus 0 to the aforementioned assumption of combinatorial nature.

I am grateful to G. Belyĭ and F. Bogomolov for useful discussions, and also to G. Shabat, who acquainted me with the remarkable work [1].

§1. THE FUNDAMENTAL CONJECTURES OF ANABELIAN ALGEBRAIC GEOMETRY

The term "anabelian algebraic geometry" ("géométrie algébrique anabélienne") was introduced by Grothendieck. In the broad sense it means the part of algebraic geometry which studies the geometry and arithmetic of algebraic varieties which are maximally "nonabelian" in a certain sense. In a letter to Faltings (1983) and in the manuscript [1] Grothendieck formulated the two "fundamental conjectures" of anabelian algebraic geometry. The first of them is an anabelian analogue of Serre's conjecture about the isogenies (now proved by Faltings). The abelian analogue of the second one would be the conjecture about the absence of infinitely divisible elements

1991 *Mathematics Subject Classification.* Primary 14H45.

in the group $H^1(\mathrm{Gal}(\overline{K}/K), A(\overline{K}))$ for an abelian variety A over a field of finite type over $\mathbf{Q}$.

Unfortunately, apparently no one knows a good definition of anabelian varieties. However, it is clear that they should include at least the "elementary anabelian varieties" whose definition I proceed to describe.

Everywhere below, K denotes a field of finite type over $\mathbf{Q}$. It will be convenient for us to regard K as imbedded in $\mathbf{C}$. Denote by $\overline{K}$ its algebraic closure in $\mathbf{C}$. For a scheme X over K, denote by $\overline{X}$ the scheme $X \times_K \operatorname{Spec}\overline{K}$ defined over $\overline{K}$. Similarly, for $f\colon X \to Y$ denote by $\overline{f}$ the corresponding morphism $\overline{X} \to \overline{Y}$.

Definition 1.1. The *class of elementary anabelian varieties over* $\overline{K}$ is defined by the following conditions:

1. $\operatorname{Spec}\overline{K}$ is anabelian.
2. A curve defined over $\overline{K}$ is anabelian if and only if its fundamental group is not abelian.
3. If $\overline{X}$ and $\overline{Y}$ are anabelian, so is $\overline{X} \amalg \overline{Y}$.
4. If $\overline{E} \to \overline{B}$ is a bundle whose base and fibers over all geometric points are anabelian, then E is anabelian. (For our purposes it suffices to assume that $\overline{E} \to \overline{B}$ is a bundle if $\overline{E}(\mathbf{C}) \to \overline{B}(\mathbf{C})$ is a topological locally trivial bundle.)

Remark. Perhaps it would be worthwhile to broaden our definition by regarding X as anabelian if there exists a modular family of anabelian varieties over it, i.e., if it is "étale" over some moduli space of anabelian varieties [4]. However, we know so little about these varieties today that by working in such a general situation, we would deprive ourselves of the last opportunity to prove meaningful results.

A variety X over K is called an *elementary anabelian variety* if $\overline{X}$ is anabelian in the sense of the definition above. Everywhere below, the term anabelian variety means elementary anabelian variety.

A justification of the term "anabelian" can be found in the simple fact that the fundamental groups of these varieties are centerless [2]. Moreover, they are all spaces of the type $K(\pi, 1)$, which apparently also plays a role.

To formulate Grothendieck's conjectures we will need two constructions related to the étale fundamental group. All necessary details can be found in [5] and [6].

Proposition 1.1. *Let X be a geometrically connected scheme over the field K, and let $\overline{p} \in X(\overline{K})$. Then the sequence of morphisms $\overline{X} \to X \to \operatorname{Spec}K$ induces an exact sequence of fundamental groups*

$$1 \to \pi_1(\overline{X}, \overline{p}) \to \pi_1(X, \overline{p}) \to \pi_1(\operatorname{Spec}K) \to 1. \tag{1.1}$$

For the proof, see [5].

The group $\pi_1(\operatorname{Spec}K)$ is canonically isomorphic to the Galois group $\mathrm{Gal}(\overline{K}/K)$. I will denote it by Γ_K or simply by Γ. Denote by $\mathrm{Out}(G)$ the group of the exterior automorphisms of the group G, i.e. the quotient of $\mathrm{Aut}(G)$ by the automorphisms of the type $g \to hgh^{-1}$, $h \in G$. For anabelian varieties the sequence (1.1) can be recovered completely from the representation it defines:

$$\pi_X\colon \Gamma \to \mathrm{Out}(\pi_1(\overline{X}, \overline{p})), \tag{1.2}$$

since in this case $\pi_1(\overline{X})$ has no center. Observe that the groups of $\mathrm{Out}(\pi_1(\overline{X}, \overline{p}))$ of exterior automorphisms are canonically isomorphic for different $\overline{p}$, and hence we can write simply $\mathrm{Out}(\pi_1(\overline{X}))$.

Consider now the K-point $p\colon \operatorname{Spec}K \to X$ of the scheme X. It determines a splitting of the sequence (1.1). Denote by $S(X)$ the set of the classes of splittings of

(1.1) equivalent under conjugation by elements of $\pi_1(\overline{X}, \overline{p})$ (like $\operatorname{Out}(\pi_1(\overline{X}))$, this set does not depend on $\overline{p}$). We have gotten a map

$$(1.3) \qquad \imath\colon X(K) \to S(X),$$

which is (in an obvious manner) functorial with respect to morphisms of schemes as well as extensions of fields.

Each element s of $S(X)$ determines a class of equivalent (under conjugations by inner automorphisms) liftings of π_X to π_X $(s\colon \Gamma \to \operatorname{Aut}(\pi_1(\overline{X}, \overline{p})))$. In the anabelian case the assigning $s \to \pi_X(s)$ is obviously bijective.

By fixing an element s_0 of $S(X)$ we can define the marked cohomology set $H^1(\Gamma, \pi_1(\overline{X}, \overline{p}))$, and, as we know (see, for example, [3]), there exists a canonical bijection

$$S(X) \to H^1(\Gamma, \pi_1(\overline{X}, \overline{p}))$$

mapping s_0 to the marked element of H^1. If $s_0 = \imath(p)$ for some $p \in X(K)$, then I will denote by $\imath_p$ the composition of $\imath$ with the above bijection.

Example. Let X be a geometrically connected commutative algebraic group over K. Then $\pi_1(\overline{X}, 0)$ is canonically isomorphic to the projective limit $\varprojlim X_n(\overline{K})$, where $X_n(\overline{K})$ is the group of points of order n on $X(\overline{K})$. Consider the sequence of Galois cohomology associated with the short exact sequence

$$0 \to X_n(\overline{K}) \to X(\overline{K}) \to X(\overline{K}) \to 0.$$

It defines an inclusion

$$X(K)/nX(K) \to H^1(\Gamma, X_n(\overline{K})).$$

It is easy to see that the map $\imath_0$ is the composition of the projective limit of these inclusions with the natural map

$$X(K) \to \varprojlim X(K)/nX(K).$$

In particular, $\imath_0$ is injective if and only if $X(K)$ does not contain infinitely divisible elements.

Let us return to the anabelian case. Denote by $S_0(X)$ the subsets in $S(X)$ consisting of those s for which there is no nontrivial g in $\pi_1(\overline{X}, \overline{p})$ such that $\pi_X(s)(\gamma)(g) \equiv g^{\varepsilon(\gamma)}$ for all $\gamma \in \Gamma$ (here $\varepsilon\colon \Gamma \to \widehat{\mathbf{Z}}^*$ is the cyclotomic character).

For groups G_1 and G_2 endowed with an exterior action of Γ (i.e. with representation of the type (1.2)) denote by $\operatorname{Extisom}_\Gamma(G_1, G_2)$ the set of classes of homomorphisms $G_1 \to G_2$ compatible (in the obvious sense) with the actions of Γ and equivalent with respect to compositions with inner automorphisms.

Now we are ready to state Grothendieck's conjectures.

Conjecture 1. *Let X and Y be geometrically connected anabelian varieties over K. Then the natural map*

$$(1.4) \qquad \operatorname{Isom}_K(X, Y) \to \operatorname{Extisom}_\Gamma(\pi_1(\overline{X}), \pi_1(\overline{Y}))$$

is bijective. (The right-hand side is the set of all exterior isomorphisms compatible with the representations π_X and π_Y.)

Conjecture 2. *If X is anabelian and geometrically connected, then the map $\imath$ establishes a one to one correspondence between $X(K)$ and $S_0(X)$.*

Remark. It is not so hard to show that giving a splitting of the sequence (1.1) is equivalent to giving a compatible family of K-models for the étale coverings of $\overline{X}$

defined over K, or, in other words, to giving a K-model of the subscheme which is a universal cover for $\overline{X}$. As will be shown later, for a complete anabelian variety X one has $S_0(X) \equiv S(X)$, and Conjecture 2 in this case asserts in particular that $X(K)$ is not empty if and only if the universal covering of $\overline{X}$ is defined over K.

In the form they are stated here, as far as I know, these conjectures have not been proved for a single anabelian variety (except of course for $\operatorname{Spec} K$). The following weakened version of Conjecture 1, which I will call just the weak conjecture, is simpler.

Weak Conjecture. *If X and Y are geometrically connected abelian varieties whose fundamental groups are isomorphic as exterior Γ-modules, then $\overline{X}$ and $\overline{Y}$ are isomorphic as varieties.*

§2. Elementary facts

This section is essentially devoted to the proof of the "easy parts" of Grothendieck's conjectures. These are, first, the injectivity of the maps (1.3) and (1.4) for anabelian varieties, and second, the proof of the "correctness" of Conjecture 2, i.e. of the fact that the image of an anabelian variety X under ι lies in $S_0(X)$. An almost trivial consequence of the statements obtained in the process of proving those facts is the weak conjecture for curves of genus 0, which is proved at the end of the section.

Definition 2.1. A geometrically connected quasicompact scheme X over K is called *étale approximable* if, for all finite extensions E of K, the maps $\iota_E\colon X(E) \to S(X(E))$ are injective.

Remark. Roughly speaking, the étale approximability of a scheme X means that for any two points $p, q \in X(E)$ there is an étale covering $f\colon Y \to X$ such that Γ acts in a different manner on $f^{-1}(\overline{p})$ and $f^{-1}(\overline{q})$.

The main theorem of this section is the following.

Theorem 1. (a) *All anabelian varieties are étale approximable.*

(b) *The image of the map ι for anabelian X lies in $S_0(X)$.*

Theorem 1(a) implies the injectivity of the maps (1.3) and (1.4).

Proof. We argue by induction on the dimension of X. Start with anabelian curves. Clearly, if X is étale approximable, Z is geometrically connected and $Z \to X$ is an inclusion, then Z is étale approximable. Thus the proof of the étale approximability of the anabelian curves reduces to proving the étale approximability for abelian varieties (for genus greater than 0) and for $\mathbf{G}_m$ (for genus 0). For this it suffices to use the computations done in Example 1.1, the Mordell-Weil theorem, and the elementary fact that there are no infinitely divisible elements in the multiplicative group of the field K.

It is harder to prove Theorem 1(b). First one needs to understand how the group Γ acts on those elements of the fundamental group of an anabelian curve which correspond to "punctures". Let X be an anabelian curve and let $\widetilde{X}$ be its projectivization. A *puncture* on X is any K-point $p \in \widetilde{X}(K)/X(K)$. It is clear for geometrical reasons that to each puncture there corresponds a conjugacy class of a cyclic subgroup of $\pi_1(\overline{X}, \overline{p})$. We will describe this correspondence in the language of algebraic geometry. Denote by X_p the curve obtained by adding to X the puncture p. Let $\mathscr{O}_p^h$ be the Henselization of the local ring of the point $p \in X_p(K)$ [6]. We have the obvious commutative diagram of morphisms of schemes

$$\begin{tikzcd}
\operatorname{Spec} K(\mathcal{O}_p^h) \arrow[r] \arrow[d] & X \arrow[d, "\iota"] \\
\operatorname{Spec} \mathcal{O}_p^h \arrow[r] & X_p
\end{tikzcd} \tag{2.1}$$

$(K(\mathcal{O}_p^h)$ denotes the field of fractions of the ring $\mathcal{O}_p^h)$. Let $\overline{y}$ be a geometric point of $\operatorname{Spec} K(\mathcal{O}_p^h)$. The field $K(\mathcal{O}_p^h) \otimes \overline{K}$ is the field of fractions of a strictly Henselian discrete valuation ring, and therefore $\pi_1(\operatorname{Spec} K(\mathcal{O}_p^h) \otimes \overline{K}, \overline{y}) \equiv \widehat{\mathbf{Z}}(1)$.

Hence the morphism $\overline{f}$ determines a homomorphism $\overline{f}_*\colon \widehat{\mathbf{Z}}(1) \to \pi_1(\overline{X}, \overline{y})$, whose image we denote by I_p. Since we are taking special care of the base points, it is defined only up to conjugation. Of course we could have defined I_p on the language of the Galois groups (as the inertia subgroup), but our definition has the advantage that it immediately permits us to prove the following lemma.

Lemma 2.1. *Let ρ be a generator in I_p and let $q \in X(K)$. Then the action of Γ on ρ with respect to the lifting $\pi_X(\iota(q))$ is of the type $\rho \to x_\gamma \rho^{\varepsilon(\gamma)} x_\gamma^{-1}$, where $\varepsilon\colon \Gamma \to \widehat{\mathbf{Z}}^*$ is the cyclotomic character.*

The images $[x_\gamma]$ of the elements x_γ in $\pi_1(\overline{X}_p, \overline{q})$ are well defined, and the map $\gamma \to [x_\gamma]$ is a cocycle whose cohomology class coincides with $\iota_q(p)$.

Proof. It follows immediately from the definition of Henselization that

$$\pi_1(\operatorname{Spec} \mathcal{O}_p^h, \overline{y}) \equiv \Gamma,$$

and so we have the following commutative diagram of fundamental groups, related to (2.1) (I am skipping the base points):

$$\begin{tikzcd}
1 \arrow[d] & 1 \arrow[d] \\
\widehat{\mathbf{Z}}(1) \arrow[r, "\overline{f}_*"] \arrow[d] & \pi_1(\overline{X}) \arrow[d] \\
\pi_1(\operatorname{Spec} K(\mathcal{O}_p^h)) \arrow[r, "f_*"] \arrow[d] & \pi_1(X) \arrow[d] \\
\Gamma \arrow[r, "\iota(p)"] \arrow[d] & \pi_1(X_p) \\
1 &
\end{tikzcd} \tag{2.2}$$

It is clear that the only nontrivial part of the lemma is the one about the coincidence of the cohomology classes. Choose a continuous section s of the homomorphism $\pi_1(\operatorname{Spec} K(\mathcal{O}_p^h)) \to \Gamma$. We want to show that

$$\iota(q)(\gamma)\iota(p)(\gamma)^{-1} \equiv [x_\gamma].$$

Obviously

$$f_* s(\gamma)^{-1} \rho f_* s(\gamma) \equiv \rho^{\varepsilon(\gamma)^{-1}},$$

from which we get

$$x_\gamma \rho x_\gamma \equiv \imath(q)(\gamma)\rho^{\varepsilon(\gamma)^{-1}}\imath(q)(\gamma)^{-1} \equiv \imath(q)(\gamma)f_*s(\gamma)^{-1}\rho f_*s(\gamma)\imath(q)(\gamma)^{-1},$$

and since the centralizer of ρ in $\pi_1(X)$ coincides with $\langle\rho\rangle$ [8], we have

$$x_\gamma \equiv \imath(q)(\gamma)f_*s(\gamma)^{-1} \quad (\text{mod } \langle\rho\rangle),$$

and, after going to $\pi_1(X_p)$,

$$[x_\gamma] \equiv \imath(q)(\gamma)\imath(p)(\gamma)^{-1}.$$

The lemma is proved.

This lemma shows that if X is an étale approximable curve over K and $p \in X(K)$, then, knowing the action of Γ on $\pi_1(\overline{X} - \{p\})$ and the conjugacy class of I_p, we can recover $\imath(p)$ in $S(X)$, and hence the point p itself. Part 2) of the following proposition gives a characterization of the subgroups I_p in terms of the representation π_X.

Proposition 2.2. *Let X be an anabelian curve over K. Then*:

a) Γ *acts on the conjugacy classes of* $\pi_1(\overline{X})$ *without fixed elements.*

b) *If $g \in \pi_1(\overline{X})$ and $\gamma(g)$ is conjugate to $g^{\varepsilon(\gamma)}$ for each $\gamma \in \Gamma$, then $g \in \mathrm{I}_p$ for some puncture p.*

Proof. Observe first that by passing if necessary to a finite extension of K we can choose a lift of π_X to a $\pi' \colon \Gamma \to \mathrm{Aut}(\pi_1(\overline{X}))$. We fix this lift throughout the whole proof. Let $g \in \pi_1(\overline{X}, \overline{p})$ and let $\gamma(g)$ be conjugate to g for all elements $\gamma \in \Gamma$. If H is a subgroup of finite index in $\pi_1(\overline{X}, \overline{p})$ that contains g, then one can find a subgroup Γ_0 of finite index in Γ such that H is Γ_0-invariant and $\gamma(g) \equiv h(\gamma)gh(\gamma)^{-1}$ for $\gamma \in \Gamma_0$ and $h(\gamma) \in H$. Thus the class of g in H^{ab} is Γ_0-invariant. But H^{ab} can be identified with the full Tate module of the Albanese variety of the covering corresponding to H. This variety is an extension of an abelian variety by a torus, and from the Mordell-Weil theorem we get that the class of g in H is equal to zero. It remains only to observe that if in a profinite group an element belongs to the closure of the commutant of each subgroup of finite index containing it, then this element is the identity.

We now prove part b).

Lemma 2.3. *Let X be an anabelian curve over K, and let $A \subset \pi_1(\overline{X})$ be the union of the conjugacy classes of the subgroups I_p for all punctures p on $\overline{X}$. For an element $g \in \pi_1(\overline{X})$ to belong to A, it is necessary and sufficient that for each open subgroup H of $\pi_1(\overline{X})$ the condition $\langle g\rangle \cap H \subset \langle A \cap H\rangle$ holds.*

For the proof, see [2].

Let g be an element of $\pi_1(\overline{X})$ such that $\gamma(g)$ is conjugate to $g^{\varepsilon(\gamma)}$ for all $\gamma \in \Gamma$, and let H be an open subgroup of $\pi_1(\overline{X}, \overline{p})$. Passing to a finite extension, we may assume that H is Γ-invariant and that for all $\gamma \in \Gamma$ the element $\gamma(g)$ is H-conjugate to $g^{\varepsilon(\gamma)}$. Let g^n be the generator of $\langle g\rangle \cap H$. Then Γ acts on the class g^n in H^{ab} by the formula

$$[g^n] \to \varepsilon(\gamma)[g^n].$$

Let X_H be the covering of X corresponding to H and let $\widetilde{X}_H$ be its projectivization. Taking Lemma 2.3 into account, we see that it suffices to prove that the image of $[g^n]$ in $\pi_1(\widetilde{X}_H)^{\mathrm{ab}}$ is equal to zero. This follows from the identification $\pi_1(\widetilde{X}_H)^{\mathrm{ab}} \equiv T(\mathrm{Alb}(\widetilde{X}_H))$ and the well-known properties of the action of Γ on the

Tate modules of abelian varieties (for instance from the analogue of the Riemann conjecture, proved in this case by Weil [8]). Proposition 2.2 is proved.

Now we can finish the proof of Theorem 1. Part (a) for dimension 1 is already proved. Assume that it is proved for dimension n and that $\dim X \equiv n+1$. Consider a bundle $F \to X \to B$ with anabelian F and B. Without loss of generality we can assume that $F(K)$ is anabelian. Choose a point $p \in F(K)$. We have the following commutative diagram of punctured sets with exact rows:

$$\begin{tikzcd}
 & F(K) \arrow[r] \arrow[d] & X(K) \arrow[r] \arrow[d] & B(K) \arrow[d] \\
H^0(\Gamma, \pi_1(\overline{B})) \arrow[r] & H^1(\Gamma, \pi_1(F)) \arrow[r] & H^1(\Gamma, \pi_1(\overline{X})) \arrow[r] & H^1(\Gamma, \pi_1(B))
\end{tikzcd}$$

The injectivity of the map ι for X follows from this diagram and from the fact that $H^0(\Gamma, \pi_1(\overline{B})) \equiv 0$ (this can be proved by a trivial induction starting with Proposition 2.2(a)).

The induction step in the proof of part (b) is trivial, and it suffices for us to deal with case of curves. Let $p \in X(K)$ and $g \in \pi_1(\overline{X})$ be such that

$$\iota(p)(\gamma) g \iota(p)(\gamma)^{-1} \equiv g^{\varepsilon(\gamma)}$$

for all $\gamma \in \Gamma$. It follows from Proposition 2.2(b) that $g \in \langle \rho \rangle$ for some puncture q of X and some generator ρ of I_q. We obtain then from Lemma 2.1 that the class of $\iota_q(p)$ is trivial. But, obviously, X_q is étale approximable, and so we get $p \equiv q$, which is, of course, impossible. This completes the proof of Theorem 1.

Observe now that from Lemma 2.1 and Proposition 2.2 the weak conjecture for genus 0 follows easily in the following form.

Proposition 2.4. *Let X and Y be curves of genus 0 over K. Then for every isomorphism $f_*\colon \pi_1(\overline{X}) \to \pi_1(\overline{Y})$ compatible with the action of Γ there exists an isomorphism $\overline{f}\colon \overline{X} \to \overline{Y}$ such that $\mathrm{I}_{\overline{f}(\overline{p})}$ is conjugate to $f_*(\mathrm{I}_{\overline{p}})$ for any puncture $\overline{p}$ of $\overline{X}$.*

§3. The weak conjecture for genus 1 and for complete hyperelliptic curves of genus greater than 1

Theorem 2. *Let E_1 and E_2 be affine curves over K of genus one. Then the existence of an isomorphism $\pi_1(\overline{E}_1) \to \pi_1(\overline{E}_2)$ compatible with the representations π_{E_1} and π_{E_2} implies that $\overline{E}_1 \approx \overline{E}_2$.*

Proof. The proof of this theorem, strange as it may seem, is "effective" (in contrast to the proof of the theorem about the isogenies of elliptic curves which is its abelian analogue [7]). More precisely, I will construct an "algorithm" which, given $G \equiv \pi_1(\overline{E}, \overline{p})$ and a representation $\pi\colon \Gamma \to \mathrm{Out}(G)$, allows us to compute the coefficients of the standard equation $y^2 = P_3(x)$ and the coordinates of the punctures of the (x, y)-plane. Probably, using the same methods one can prove the stronger statement about the existence of the endomorphism $E_1 \approx E_2$ over K.

So let G be our group. I will assume that a lift $\tilde{\pi}\colon \Gamma \to \mathrm{Aut}(G)$ of π is given, but none of our constructions depend on this particular choice. Using Proposition 2.2, choose generators $\rho_0, \rho_1, \dots, \rho_n$ in the cyclic groups corresponding to the punctures $p_1, \dots, p_n$. We may, obviously, assume that p_0 is the identity of the group law on the projectivization of E. Denote by H the unique normal subgroup of G for which $\rho_i \in H$ and $G/H \approx \mathbf{Z}/2\mathbf{Z} \otimes \mathbf{Z}/2\mathbf{Z}$. Let ρ_{ij} $(0 < i < n, 1 < j < 4)$ be representatives of the conjugacy classes of H belonging to $G_{\rho_i} G^{-1}$ respectively. We may assume that $\rho_{i1} \equiv \rho_i$. It is obvious that H together with the induced outer action of Γ is isomorphic to $\pi_1(\overline{E} - \{p_{ij}, 0 \leq i \leq n, 1 \leq j \leq 4\})$, where the p_{ij} are such that $2p_{ij} \equiv p_i$.

On H there exist Γ-equivariant homomorphisms

$$x_*: H \to \widehat{\mathbf{Z}}(1), \qquad y_*: H \to \widehat{\mathbf{Z}}(1),$$

which have the following properties:

(a) $x_*(\rho_{ij}) \equiv y_*(\rho_{ij}) \equiv 0$ for $i \geq 1$;

(b) $x_*(\rho_{02}) \equiv 2\rho$, $x_*(\rho_{01}) \equiv -2\rho$, $x_*(\rho_{03}) \equiv x_*(\rho_{04}) \equiv 0$, $y_*(\rho_{01}) \equiv -3\rho$, and $y_*(\rho_{02}) \equiv y_*(\rho_{03}) \equiv y_*(\rho_{04}) \equiv \rho$,
where ρ is a generator of $\widehat{\mathbf{Z}}(1)$. (As x_* and y_* one can take for instance the homomorphisms induced by the ordinary functions x and y, which obviously lift to morphisms $E - \{p_{01}, p_{02}, p_{03}, p_{04}\} \to \mathbf{G}_m$, since the p_{0j} are points of order two on E.)

Let the action of Γ on ρ_{ij} be

$$\gamma: \rho_{ij} \to x_{ij}(\gamma)\rho_{ij}^{\varepsilon(\gamma)}x_{ij}(\gamma)^{-1}.$$

It is easy to see that the elements

$$x(\xi_{ij})(\gamma) :\equiv x_*(x_{ij}(\gamma)) - x_*(x_{03}(\gamma)),$$
$$y(\xi_{ij})(\gamma) :\equiv y_*(x_{ij}(\gamma)) - y_*(x_{11}(\gamma))$$

are well defined if $(i, j) \neq (0, 1), (0, 2)$ for $x(\xi_{ij})$ and $(i, j) \neq (0, 1)$ for $y(\xi_{ij})$, and that they determine cocycles from $Z^1(\Gamma, \widehat{\mathbf{Z}}(1))$. Our "algorithm" and therefore the proof of the theorem are completed by the following lemma.

Lemma 3.1. (a) *There exists a unique* (*up to a sign*) *element* $\delta \in \widehat{\mathbf{Z}}^*$ *such that* $\delta x(\xi_{ij})$ *and* $\delta y(\xi_{ij})$ *belong to* K.

(b) *The curve* E *is isomorphic to the curve given by the equation*

$$y^2 \equiv x(x-1)(x - \iota_1^{-1}(\delta x(\xi_{01}))).$$

(c) *The* (x, y) *coordinates of the points* p_{ij}, $i \geq 1$, *are given by the pairs* $(\iota^{-1}(\delta x(\xi_{ij})), \iota^{-1}(\delta y(\xi_{ij})))$.

Proof. The only fact one really needs to prove is that any x_* and y_* satisfying (a) and (b) up to multiplication by ε from $\widehat{\mathbf{Z}}^*$ coincide with the homomorphisms induced by the standard functions x and y. For this it suffices to prove that if E is a complete curve of genus 1 over K, then there is no Γ-equivariant homomorphism $\pi_1(\overline{E}) \to \widehat{\mathbf{Z}}(1)$. This is a simple consequence of the Mordell-Weil theorem (more precisely, even from Mordell's theorem).

This concludes the proofs of Lemma 3.1 and Theorem 2.

Before we go to the hyperelliptic curves of higher genus we prove another simple (modulo Belyĭ's theorem—see §4) property of the representations for anabelian curves of genus 0 and 1.

Proposition 3.2. *Let* S *be an anabelian curve of genus* 0 *or* 1. *Then the representation* π_S *is injective.*

Proof. The case of curves of genus 0 is trivial (modulo Belyĭ's theorem), and thus we can assume that S is an affine curve of genus 1. Consider, as in the proof of Theorem

2, the subgroup H in $\pi_1(\overline{S})$ corresponding to the standard isogeny of degree 4. Obviously, it suffices to show the injectivity of the lift of π_S to $\pi' : \Gamma \to \mathrm{Out}(H)$ and to consider only the case when E has a unique puncture. Then H is obviously imbedded in $\pi_1(\overline{\mathbf{P}}^1 - \{0, 1, \infty, \lambda\})$ as a subgroup of index 2, and the required result follows trivially from Belyĭ's theorem (see §4) and from the fact that Γ does not have finite normal subgroups.

Remark. It seems quite plausible to assume that the representations π_S are injective for all affine anabelian curves S.

Theorem 3. *Let S_1 and S_2 be hyperelliptic curves, and let there exist an isomorphism $\pi_1(\overline{S}_1) \to \pi_1(\overline{S}_2)$ which commutes with the hyperelliptic involutions and is compatible with the action of Γ. Then $\overline{S}_1 \approx \overline{S}_2$.*

§4. The representations π_S for genus zero

This section is devoted to the proof of a theorem which gives, modulo a certain combinatorial conjecture, a characterization of the image of the representations π_S for curves of the type

$$\mathbf{P}^1 - \{0, 1, \infty, x_1, \dots, x_n\}, \qquad x_i \in \mathbf{Q}.$$

Using this theorem and the results of §2, I shall reduce the strong version of Conjecture 1 for curves of genus 0 to this combinatorial conjecture.

Let $S \equiv \mathbf{P}^1 - \{0, 1, \infty, x_1, \dots, x_n\}$, $x_i \in \mathbf{Q}$. The fundamental group of S can be given by corepresentations of the type

$$\pi_1(\overline{S}) \equiv \langle \rho_0, \rho_1, \rho_\infty, \rho_{x_1}, \dots, \rho_{x_n} : \rho_0 \cdots \rho_{x_n} \equiv 1 \rangle,$$

where ρ_* is assigned to the corresponding puncture. For convenience I assume that the generators are fixed. The group $\pi_1(\overline{S})$ I denote by G. Let A be the subgroup in $\mathrm{Out}(G)$ consisting of those exterior automorphisms α for which $\alpha(\rho_*)$ is conjugate to $\rho_*^{\varepsilon(\alpha)}$ for all $* \in \{0, 1, \infty, x_1, \dots, x_n\}$ and for some $\varepsilon(\alpha) \in \widehat{\mathbf{Z}}^*$. Lemma 2.1 implies that for any curve of the indicated type the image of π_S is contained in A. Let $\widetilde{A}$ be the preimage of H in $\mathrm{Aut}(G)$, and let $\tilde{\pi}$ be a lift of π_S to a homomorphism $\Gamma \to \widetilde{A}$. For an open subgroup H in G, denote by $p_H : S_H \to \mathbf{P}^1$ the corresponding unramified covering. Clearly, if $\alpha \in \widetilde{A}$ then the coverings corresponding to H and $\alpha(H)$ have the "same" ramification points. More precisely, one can define a bijection from the set of ramification points of p_H to the set of ramification points of $p_{\alpha(H)}$ that preserves the ramification multiplicities and is natural with respect to inclusions of subgroups. For a ramification point p on S_H I denote by $\alpha(p)$ the corresponding point on $S_{\alpha(H)}$.

Denote by $\lambda(a, b, c, d)$ the cross-ratio of four different points a, b, c, d on $\mathbf{P}^1$. Let $\widetilde{A}_0$ be the subgroup of $\widetilde{A}$ consisting of those automorphisms α for which for any two subgroups H_1 and H_2 of genus 0 in G with ramification points a_i, b_i, c_i, d_i, $i = 1, 2$, of the coverings p_{H_i} respectively, the equality

$$\lambda(a_1, b_1, c_1, d_1) \equiv \lambda(a_2, b_2, c_2, d_2)$$

yields the equality

$$\lambda(\alpha(a_1), \alpha(b_1), \alpha(c_1), \alpha(d_1)) \equiv \lambda(\alpha(a_2), \alpha(b_2), \alpha(c_2), \alpha(d_2)).$$

Observe that for $\gamma \in \Gamma$ we have

$$\lambda(\tilde{\pi}(\gamma)(a), \tilde{\pi}(\gamma)(b), \tilde{\pi}(\gamma)(c), \tilde{\pi}(\gamma)d)) \equiv \gamma(\lambda(a, b, c, d)),$$

and hence the image of $\tilde{\pi}$ lies in $\widetilde{A}_0$. Moreover it is obvious that $\mathrm{Int}(G) \subset \widetilde{A}_0$. Let A_0 be the image of $\widetilde{A}_0$ in $\mathrm{Out}(G)$.

Proposition 4.1. *There exists a homomorphism* $\widetilde{\mathscr{H}}\colon \widetilde{A}_0 \to \Gamma$, *such that*

(a) $\operatorname{Int}(G) \subset \ker\widetilde{\mathscr{H}}$, *and*

(b) $\widetilde{\mathscr{H}}\tilde{\pi} \equiv \mathrm{Id}_\Gamma$.

Proof. First we state Belyĭ's theorem in a form convenient for our subsequent considerations.

Theorem [8]. *Let* $x_1, \dots, x_n \in \overline{\mathbf{Q}}$. *Then there exists a polynomial* f *such that* $f(x_1) \equiv \cdots \equiv f(x_n) \equiv 0$ *whose finite critical values are only* 0 *and* 1.

We call such a polynomial a *Belyĭ polynomial* of the points $x_1, \dots, x_n$. Let $x \in \overline{\mathbf{Q}}$. Consider the subgroup H of genus 0 in G corresponding to some Belyĭ polynomial of the points $0, 1$, and x. For $\alpha \in \widetilde{A}_0$ set

$$\alpha(x) \equiv \lambda(\alpha(0), \alpha(1), \alpha(\infty), \alpha(x)).$$

It is clear from the definition of $\widetilde{A}_0$ that $\alpha(x)$ does not depend on the freedom in choosing H and that this construction defines an action of $\widetilde{A}_0$ on $\overline{\mathbf{Q}}$ by permutations. Moreover, it is obvious that $\tilde{\pi}(\gamma)(x)$ coincides with $\gamma(x)$ under the canonical action of Γ on $\overline{\mathbf{Q}}$, and $\gamma(x) = x$ for $\gamma \in \operatorname{Int}(G)$. To prove the proposition it remains to check that the map transforming x into $\alpha(x)$ is a field homomorphism. It is easy to see that the validity of the following conditions is sufficient for this.

(i) $\alpha(0) \equiv 0$ and $\alpha(1) \equiv 1$.

(ii) If $a + b \equiv 2c$, then $\alpha(a) + \alpha(b) \equiv 2\alpha(c)$.

(iii) If $ab \equiv c^2$, then $\alpha(a)\alpha(b) \equiv \alpha(c)^2$.

The first is obvious. To prove that (ii) holds, consider the polynomial $f((z-c)^2)$ where f is a Belyĭ polynomial for c^2, $(1-c)^2$, $(a-c)^2 \equiv (b-c)^2$, and 0. The subgroup $H \subset G$ corresponding to it is contained in the subgroup H' corresponding to f, and this inclusion corresponds to the covering $z \to (z-c)^2$. It follows immediately from the definition of $\widetilde{A}_0$ that the covering φ corresponding to the inclusion $\alpha(H) \subset \alpha(H')$ has the following properties:

1) $\deg\varphi \equiv 2$.

2) $\varphi(\alpha(a) \equiv \varphi(\alpha(b))$.

3) φ is ramified at the points $\alpha(c)$ and $\alpha(\infty)$.

After the normalization $\alpha(\infty) \equiv \infty$ we get that $\varphi(z) \equiv p(z - \alpha(c))^2 + q$ for some $p, q \in \overline{\mathbf{Q}}$. Now we obtain the required identity from 2).

Condition (iii) can be checked similarly. The proposition is proved.

Proposition 4.3. *The normalizer of the image of the group* Γ *in* A *is contained in* A_0.

Proof. For simplicity we carry out the proof in the case $n \equiv 3$. Let $\alpha \in \widetilde{A}_0$, let H_1 and H_2 be subgroups of genus 0 in G, and let a_i, b_i, c_i, and d_i be the ramification points of the corresponding coverings. We want to show that

$$\lambda(\alpha(a_1), \dots, \alpha(d_1)) \equiv \lambda(\alpha(a_2), \dots, \alpha(d_2)),$$

if $\lambda(a_1, \dots, d_1) \equiv \lambda(a_2, \dots, d_2)$ and the image of α in $\operatorname{Out}(G)$ normalizes $\pi_S(\Gamma)$.

Using Proposition 2.4, we can reduce the problem to constructing an isomorphism between the corresponding fundamental groups. Let

$$G_i \equiv \pi_1(S_{H_i} - \{a_i, b_i, c_i, d_i\}),$$
$$G_i^\alpha \equiv \pi_1(S_{\alpha(H_i)} - \{\alpha(a_i), \alpha(b_i), \alpha(c_i), \alpha(d_i)\}).$$

Obviously G_1 and G_1^α can be identified with suitable subfactors of G. In this way the automorphism α induces an isomorphism $\alpha_1 \colon G_1 \to G_1^\alpha$. Consider the diagram

$$\begin{tikzcd} G_1^\alpha \arrow[r, "\alpha_2^{-1}\varphi\alpha_1"] \arrow[d, "\alpha_1"'] & G_2^\alpha \arrow[d, "\alpha_2"] \\ G_1 \arrow[r, "\varphi"] & G_2 \end{tikzcd}$$

in which φ is some Γ-equivariant isomorphism. To finish the proof it remains only to observe that the condition $\alpha\Gamma\alpha^{-1} \subset \Gamma \pmod{\operatorname{Int}(G)}$ guarantees the Γ-equivariancy of $\alpha_2^{-1}\varphi\alpha_1$.

Denote by $\mathscr{H}$ the descent of $\widetilde{\mathscr{H}}$ to a homomorphism $A_0 \to \Gamma$.

Conjecture. $\ker\mathscr{H} \equiv 1$.

Obviously from Propositions 2.4 and 4.3 it follows that our conjecture that $\mathscr{H}$ does not have a kernel implies Grothendieck's first conjecture for genus 0 in its strong form. On the other hand, one can show that for its proof it will be sufficient to prove the triviality of the intersection of all open subgroups of genus 0 in G, which is a purely combinatorial problem. (For the 1-completion of G an analogous result was proven by Ihara [9].)

Bibliography

1. A. Grothendieck, *Esquisse d'un programme*, manuscript, 1984.
2. Hiroaki Nakamura, *Galois rigidity of the étale fundamental groups of punctured projective lines*, J. Reine Angew. Math. **411** (1990), 205–216.
3. Jean-Pierre Serre, *Cohomologie galoisienne*, 3rd ed., Lecture Notes in Math., vol. 5, Springer-Verlag, Berlin, 1964.
4. David Mumford, *Picard groups of moduli problems*, Arithmetical Algebraic Geometry (Proc. Conf., Purdue Univ., 1963), Harper & Row, New York, 1965, pp. 33–81.
5. A. Grothendieck et al., *Revêtements étales et groupe fondamental*, Séminaire de Géométrie Algébrique du Bois-Marie 1960–1961 (SGA-1), Lecture Notes in Math., vol. 224, Springer-Verlag, Berlin, 1971.
6. James S. Milne, *Étale cohomology*, Princeton Univ. Press, Princeton, N.J., 1980.
7. Jean-Pierre Serre, *Abelian l-adic representations and elliptic curves*, Benjamin, New York, 1968.
8. André Weil, *Variétés abéliennes et courbes algébriques*, Actualités Sci. Indust., vol. 1064, Hermann, Paris, 1948.
9. Yasutaka Ihara, *Profinite braid groups, Galois representations and complex multiplications*, Ann. of Math. (2) **123** (1986), 43–106.

Received 16/MAY/90

Translated by T. PANTEV