Advanced Studies in Pure Mathematics 12, 1987
Galois Representations and Arithmetic Algebraic Geometry
pp. 173–188

Some Problems on Three Point Ramifications and Associated Large Galois Representations

Yasutaka Ihara

Dedicated to Professor Ichiro Satake for his 60th birthday

Introduction

Let $\boldsymbol{Q}$ be the rational number field, $\bar{\boldsymbol{Q}}$ be its algebraic closure, and l be a fixed prime number. Then the absolute Galois group $G_{\boldsymbol{Q}}=\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$ admits a canonical representation

$$\varphi=\varphi_{\boldsymbol{Q}}: G_{\boldsymbol{Q}}\longrightarrow \mathrm{Out}\, \pi_1^{\text{pro-}l}(\boldsymbol{P}^1_{\bar{\boldsymbol{Q}}}\backslash\{0, 1, \infty\}),$$

in the outer automorphism group of the pro-l fundamental group of the punctured projective line, which arises from the exact sequence

$$1\longrightarrow \pi_1^{\text{pro-}l}(\boldsymbol{P}^1_{\bar{\boldsymbol{Q}}}\backslash\{0, 1, \infty\})\longrightarrow \pi_1^{\text{pro-}l}(\boldsymbol{P}^1_{\boldsymbol{Q}}\backslash\{0, 1, \infty\})\longrightarrow G_{\boldsymbol{Q}}\longrightarrow 1.$$

Recently, several authors started (perhaps more or less independently) to work on this type of "large Galois representations"; Belyĭ [3], Grothendieck [7], Deligne [5], [6], the author [9], [10], etc. In this report, we pose and discuss various basic open problems related to this represetation φ and its natural "subrepresentations" ψ.

§ 1. The Galois representation φ

(1–1) First, let us repeat the definition of the Galois representation $\varphi_{\boldsymbol{Q}}$ more precisely in terms of function fields. Let M be the maximum pro-l extension of the rational function field $K=\bar{\boldsymbol{Q}}(t)$ unramified outside $t=0, 1, \infty$. Then $M/\boldsymbol{Q}(t)$ is also a Galois extension. So, identifying the two Galois groups $\mathrm{Gal}(K/\boldsymbol{Q}(t))$ and $G_{\boldsymbol{Q}}=\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$ in the obvious way, we obtain an exact sequence of Galois groups

$$1\longrightarrow \mathrm{Gal}(M/K)\longrightarrow \mathrm{Gal}(M/\boldsymbol{Q}(t))\longrightarrow G_{\boldsymbol{Q}}\longrightarrow 1.$$

Put $\mathfrak{F}=\mathrm{Gal}(M/K)$ and $\tilde{\mathfrak{F}}=\mathrm{Gal}(M/\boldsymbol{Q}(t))$. Then the composite of three canonical homomorphisms

Received April 9, 1986.

$$\tilde{\mathfrak{F}} \longrightarrow \mathrm{Int}\,\tilde{\mathfrak{F}} \xrightarrow{\mathrm{Res}} \mathrm{Aut}\,\mathfrak{F} \longrightarrow \mathrm{Out}\,\mathfrak{F}$$

factors through G_Q and defines the homomorphism

$$\varphi_Q\colon G_Q \longrightarrow \mathrm{Out}\,\mathfrak{F}; \qquad \mathfrak{F} = \mathrm{Gal}\,(M/K).$$

Here, for any topological group X, Aut X, Int X and Out X=Aut X/Int X denote the groups of automorphisms, inner automorphisms and outer automorphisms of X, respectively. The canonical homomorphism $X \to \mathrm{Int}\,X$ is defined by $x \to \mathrm{Int}\,x$, where $(\mathrm{Int}\,x)y = xyx^{-1}$ $(x, y \in X)$, and Res: $\mathrm{Int}\,\tilde{\mathfrak{F}} \to \mathrm{Aut}\,\mathfrak{F}$ is the restriction homomorphism.

(1–2) This definition, starting from $\boldsymbol{P}^1 \backslash \{0, 1, \infty\}$ over $\boldsymbol{Q}$, can of course be generalized to the case of an arbitrary scheme over any field. But here, we want to look closely at this special case which is *rigid* with respect to deformations and which gives a *canonical* representation of G_Q determined only by l. While the ordinary linear representation of the Galois group is a representation in the automorphism group of a *vector space*, our representation is in the (outer) automorphism group of the Galois group $\mathfrak{F} = \mathrm{Gal}\,(M/K)$ which is isomorphic to the *free pro-l group of rank* 2. (In the general case, what corresponds to Gal (M/K) is the geometric part of the pro-l fundamental group of the given scheme, which, except for the case of curves, is usually either difficult to determine or too small.)

We may also replace "pro-l" by either "almost pro-l", or "profinite". Namely:

(i) *The almost pro-l case.* Choose any *finite Galois* extension K'/K unramified outside $t=0, 1, \infty$, and define M to be the maximum pro-l extension of K' unramified outside $t=0, 1, \infty$. Then Gal (M/K) is a *free almost pro-l group* of rank 2 in the sense of [10], i.e., the completion of the abstract free group F of rank 2 with respect to the pro-l topology of some normal subgroup $F' \subset F$ of finite index. If an intermediate field $\boldsymbol{Q}^*$ $(\boldsymbol{Q} \subset \boldsymbol{Q}^* \subset \bar{\boldsymbol{Q}})$ is such that $K'/\boldsymbol{Q}^*(t)$ is a Galois extension, we obtain a representation of G_{Q^*} in Out (Gal (M/K)).

(ii) *The profinite case.* Take M to be the maximum Galois extension of K unramified outside 0, 1, ∞. Then Gal (M/K) is the free profinite group of rank 2, and we obtain a canonical representation of G_Q in Out (Gal (M/K)).

These two cases are equally important as the pro-l case, but we shall mainly restrict our attention to the pro-l case and occasionally give remarks related to other cases.

As a final remark here, we note that one may also replace the base field $\boldsymbol{Q}$ by any other perfect field k with characteristic $\neq l$ (without changing the structure of Gal(M/K)). But the only basic cases are $k=\boldsymbol{Q}$ and $k=\boldsymbol{F}_p=\boldsymbol{Z}/p$ $(p\neq l)$. The representation φ_k for other cases can be obtained from $\varphi_{\boldsymbol{Q}}$ or $\varphi_{\boldsymbol{F}_p}$ by restriction. (Even then, the study of $\varphi_{\boldsymbol{Q}_l}$ ($\boldsymbol{Q}_l$: the l-adic number field) is of an independent interest.) We shall mainly consider the case over $\boldsymbol{Q}$, and abbreviate as $\varphi=\varphi_{\boldsymbol{Q}}$.

(1–3) Two basic problems are:

(P1) What is the kernel of φ?

(P2) What is the image of φ?

(1–4) *About* (P1). (i) Let k_φ denote the Galois extension over $\boldsymbol{Q}$ corresponding to the kernel of φ. Then k_φ has the following interpretation. For any intermediate field k of $\bar{\boldsymbol{Q}}/\boldsymbol{Q}$, a *k-model* of M will mean any intermediate field M_k of $M/k(t)$ such that $M_k\cdot\bar{\boldsymbol{Q}}=M$ and $M_k\cap\bar{\boldsymbol{Q}}=k$. It will be called a *Galois* k-model if moreover $M_k/k(t)$ is a Galois extension. Now, in each of the pro-l, almost pro-l and the profinite case, the group Gal(M/K) has trivial center. (In fact, a free pro-l (resp. almost pro-l, profinite) group of finite rank>1 has trivial center.) From this follows immediately that *k_φ is the smallest algebraic extension of $\boldsymbol{Q}$ for which M has a Galois k_φ-model.*

Incidentally, as for non-Galois models of M, there is a convenient $\boldsymbol{Q}$-model $M_{\boldsymbol{Q}}$ used by Beylĭ [3] (also by Deligne [6] and the author [9]) cf. [9] I § 4.

(ii) In the profinite case, Belyĭ [3] proved that φ is *injective*. He proved this by showing that every algebraic curve defined over an algebraic number field can be realized as a finite covering of $\boldsymbol{P}^1$ unramified outside 0, 1, ∞. In particular, an elliptic curve with any given absolute invariant $j\in\bar{\boldsymbol{Q}}$ is so, and this leads to that $k_\varphi=\bar{\boldsymbol{Q}}$.

(iii) In the pro-l case, k_φ cannot be as large as $\bar{\boldsymbol{Q}}$, because *k_φ must be a pro-l extension of the cyclotomic field $\boldsymbol{Q}(\boldsymbol{\mu}_{l^\infty})$ unramified outside l* ([5], [9] § I). Thus, one may ask:

(P1′) Is k_φ in the pro-l case the maximum pro-l extension of $\boldsymbol{Q}(\boldsymbol{\mu}_{l^\infty})$ unramified outside l?

Our present knowledge is so narrow, and we cannot even put it as a conjecture.

A closely related geometric question is this:

(P3) Which curve over $\bar{\boldsymbol{Q}}$ (or $\bar{\boldsymbol{Q}}_l$) can be realized as an l-covering of $\boldsymbol{P}^1$ unramified outside 0, 1, ∞?

Here, an *l-covering* means a finite covering such that the degree of *its Galois closure* is a *power of l.*

We know that such curves have good reduction outside l [9] § I. As for the special fiber above l of the *integral closure of $\boldsymbol{P}^1_{\boldsymbol{Z}_l}$* in such a covering of $\boldsymbol{P}^1_{\bar{\boldsymbol{Q}}_l}$, what we know at present is the following elementary

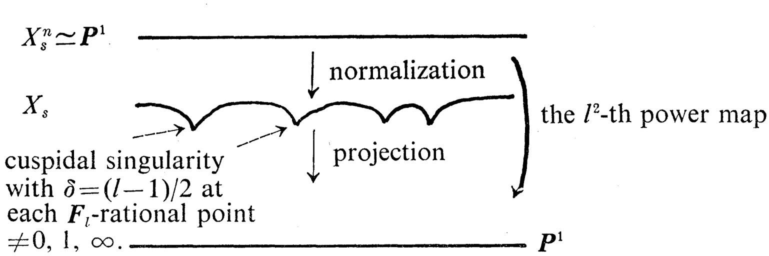
Theorem 1. *Let* $\boldsymbol{P}^1_{\boldsymbol{Z}_l}=\operatorname{Spec}\boldsymbol{Z}_l[t]\cup\operatorname{Spec}\boldsymbol{Z}_l[t^{-1}]$ *be the projective t-line over* $\boldsymbol{Z}_l$ *with the geometric general fiber* $\boldsymbol{P}^1_{\bar{\boldsymbol{Q}}_l}$. *Let* $X_{\bar{\eta}}/\boldsymbol{P}^1_{\bar{\boldsymbol{Q}}_l}$ *be an l-covering of degree* l^n $(n\geqslant 1)$ *unramified outside* $t=0, 1, \infty$, *and X be the integral closure of* $\boldsymbol{P}^1_{\boldsymbol{Z}_l}$ *in* $X_{\bar{\eta}}$. *Then the special fiber* X_s *of X is an integral scheme, and its normalization* X_s^n, *considered as a* $\boldsymbol{P}^1_{\bar{\boldsymbol{F}}_l}$*-scheme via the projection* $X_s\to\boldsymbol{P}^1_{\bar{\boldsymbol{F}}_l}$, *is isomorphic to*

$$\operatorname{Spec}\bar{\boldsymbol{F}}_l[t^{1/l^n}]\cup\operatorname{Spec}\bar{\boldsymbol{F}}_l[t^{-1/l^n}],$$

i.e., the unique purely inseparable covering $\boldsymbol{P}^1_{\bar{\boldsymbol{F}}_l}\to\boldsymbol{P}^1_{\bar{\boldsymbol{F}}_l}$ *of degree* l^n.

For example, if $X_{\bar{\eta}}$ is the Fermat covering of level l corresponding to the function field $\bar{\boldsymbol{Q}}_l(t^{1/l},(1-t)^{1/l})$, then X_s is the projective t_1-line $(t_1=t^{1/l^2})$ *with cuspidal singularities* at each of the $(l-2)$ distinct $\boldsymbol{F}_l$-rational points $t_1=a$ of $\boldsymbol{P}^1_{\bar{\boldsymbol{F}}_l}\backslash\{0, 1, \infty\}$, and the completion of the local ring of X_s at $t_1=a$ is given by

$$\bar{\boldsymbol{F}}_l[[T^2, T^l]],\qquad T=t_1-a.$$



The proof of Theorem 1 is reduced to this Fermat case by passage to the Frattini subcovering of (a suitable enlargement of) $X_{\bar{\eta}}$.

(1–5) *About* (P2). The Galois group $\mathfrak{F}=\operatorname{Gal}(M/K)$ is equipped with the conjugacy classes of three special subgroups, the inertia groups above $t=0, 1, \infty$. The outerly action of $G_{\boldsymbol{Q}}$ on $\mathfrak{F}$ respects this structure. To be more precise, call any place of M over $\bar{\boldsymbol{Q}}$ lying above $t=0, 1, \infty$, a *cuspidal place* of M. Then the inertia group in M/K of a cuspidal place is (topologically) generated by a single element, and hence is a quotient of $\hat{\boldsymbol{Z}}$. It is isomorphic to $\boldsymbol{Z}_l$ (resp. $(\boldsymbol{Z}/m)\times\boldsymbol{Z}_l$ with some $m\not\equiv 0 \pmod{l}$, resp. $\hat{\boldsymbol{Z}}$), according to whether the case is pro-l (resp. almost pro-l, resp. profinite). A *primitive parabolic element* is a generator of one of such an inertia group, and an $\mathfrak{F}$-conjugacy class of such an element is a *primitive parabolic conjugacy class*. Call $\tilde{\Phi}$ the group of all $\sigma\in\operatorname{Aut}\mathfrak{F}$ that raises each primitive parabolic conjugacy class c to some power c^α ($\alpha \in \hat{\boldsymbol{Z}}^\times$). Here, α depends on σ but not on c. Define $\Phi=\tilde{\Phi}/\mathrm{Int}\,\mathfrak{F}\subset\mathrm{Out}\,\mathfrak{F}$. Then $\varphi(G_{\boldsymbol{Q}})$ is contained in Φ. Moreover, it is contained in the $\mathfrak{S}_3$-symmetric part $S\Phi$ defined as follows. Let the symmetric group $\mathfrak{S}_3$ act on $K=\bar{\boldsymbol{Q}}(t)$ as the group of linear fractional transformations stabilizing and acting on $\{0, 1, \infty\}$ as the group of permutations (the "λ-group"). The fixed field is $\bar{\boldsymbol{Q}}(j)$, with

$$j=2^8(t^2-t+1)^3/t^2(1-t)^2.$$

The exact sequence of Galois groups

$$1\longrightarrow\mathfrak{F}\longrightarrow\mathrm{Gal}\,(M/\bar{\boldsymbol{Q}}(j))\longrightarrow\mathfrak{S}_3\longrightarrow 1$$

defines an *injective* homomorphism $\mathfrak{S}_3\hookrightarrow\mathrm{Out}\,\mathfrak{F}$. We define $S\Phi$ to be the centralizer of $\mathfrak{S}_3$ in Φ. One checks easily that $\varphi(G_{\boldsymbol{Q}})\subset S\Phi$. These are rather obvious restrictions of the image. Deligne thinks that the image is much smaller than $S\Phi$, and our study of the ψ-representation ([9] II, IV; cf. § 3) seems to support this. See also [11] "the $\mathfrak{S}_4$-symmetricity of $F_\rho * F_\rho$", and [1].

The situation is completely parallel in the profinite case. Namely, the groups Φ and $S\Phi$ are defined analogously, and $\varphi(G_{\boldsymbol{Q}})\subset S\Phi$. As φ is injective in this case, φ induces an *isomorphism* between $G_{\boldsymbol{Q}}$ and its image.

Now for the "coordinate system". Recall that the topological fundamental group $\Gamma=\pi_1(\boldsymbol{P}^1_{\boldsymbol{C}}\backslash\{0, 1, \infty\})$ is a free group of rank 2 generated by such loops x_C, y_C, z_C around 0, 1, ∞, respectively that $x_C y_C z_C=1$. Therefore, its completion $\mathfrak{F}$ is free pro-l (resp. almost pro-l, or profinite, depending on the case) with rank 2, generated by such x and y that x, y and $z=(xy)^{-1}$ each generates some inertia group above 0, 1 and ∞, respectively. The group $\tilde{\Phi}$ can be expressed as

$$\tilde{\Phi}=\left\{\sigma \in \mathrm{Aut}\,\mathfrak{F};\; \begin{matrix}\sigma x \sim x^\alpha \\ \sigma y \sim y^\alpha \\ \sigma z \sim z^\alpha\end{matrix}\ (\exists\alpha \in \hat{\boldsymbol{Z}}^\times)\right\}.$$

As for the exponent α, if the case is pro-l (resp. profinite), it is uniquely determined by σ as an element of $\boldsymbol{Z}_l^\times$ (resp. $\hat{\boldsymbol{Z}}^\times$), called the norm $N(\sigma)$ of σ. For $\rho \in G_{\boldsymbol{Q}}$, $\chi(\rho)=N(\varphi(\rho))$ is the l-cyclotomic (resp. the cyclotomic) character describing the action of ρ on the group of l-powerth (resp. all) roots of unity.

As for the freedom in the choice of (x, y): If we only impose that they generate $\mathfrak{F}$ and each of $x, y, z=(xy)^{-1}$ is primitive parabolic above 0, 1, ∞, respectively, then the choice of (x, y) is up to $\tilde{\Phi}$-transforms. But if we further impose that they come from x_C, y_C via an embedding $\bar{\boldsymbol{Q}}\subset\boldsymbol{C}$, then this will define a narrower class. The triple (x_C, y_C, z_C) described above is, roughly speaking, unique up to simultaneous Γ-conjugation, and it is precisely so if we impose x_C any y_C to be positively oriented. The class of (x, y) thus defined is unique up to $\widetilde{\varphi(G_Q)}$-transformations, where $\widetilde{\varphi(G_Q)}$ is the preimage of $\varphi(G_Q)$ in Aut $\mathfrak{F}$. This means that, for a free pro-l (or profinite) group $\mathfrak{F}$ of rank 2 given together with a set of free generators (x, y), there is a uniquely determined subgroup of Out $\mathfrak{F}$ that corresponds with $\varphi(G_Q)$. What is THIS?

(1–6) *Similar problems for* φ_{Q_l}. The representation $\varphi_{Q_l}: G_{Q_l} \to \Phi$ can be identified with the restriction of φ_Q to the decomposition group of an (arbitrary) extension $\bar{l}/l$ to $\bar{Q}$. Therefore, Image $\varphi_{Q_l} \subset$ Image φ_Q, and as for the kernel, the Galois extension k_{φ_l}/Q_l corresponding to Ker φ_{Q_l} can be identified with the $\bar{l}$-adic completion of k_φ.

At present, we have nothing to add about the image. As for k_{φ_l}/Q_l, it is obvious that k_{φ_l} is *some* pro-l extension over $Q_l(\mu_{l^\infty})$. But at least when l is a *regular prime*, $k_{\varphi_l}/Q_l(\mu_{l^\infty})$ cannot be the maximum pro-l extension. In fact, denote by Σ_l the maximum pro-l extension over $Q_l(\mu_{l^\infty})$ (or equivalently, over $Q_l(\mu_l)$), and Σ' the maximum pro-l extension over $Q(\mu_{l^\infty})$ (or equivalently, over $Q(\mu_l)$) unramified outside l. Call Σ'_l the $\bar{l}$-adic completion of Σ', which can be regarded as a Galois subextension of $\Sigma_l/Q_l(\mu_{l^\infty})$. The minimum number of generators of the pro-l groups Gal $(\Sigma_l/Q_l(\mu_l))$ and Gal $(\Sigma'/Q(\mu_l))$ are $l+1$ and $\frac{1}{2}(l+1)$ respectively. (Here and in the following, when $l=2$, $\frac{1}{2}(l+1)$ should be replaced by 2.) Now, if l is regular, then it follows (by Frattinization and the Hilbert classfield theory) that Gal $(\Sigma'/Q(\mu_l)) \simeq$ Gal $(\Sigma'_l/Q_l(\mu_l))$ canonically, and from [13] Satz 11.5 follows directly that this group is a free pro-l group of rank $\frac{1}{2}(l+1)$. Since $k_\varphi \subset \Sigma'$, we conclude that if l is regular, the minimum number of generators of Gal $(k_{\varphi_l}/Q_l(\mu_l))$ is *at most* $\frac{1}{2}(l+1)$, and if furthermore (P1′) is valid then Gal $(k_{\varphi_l}/Q_l(\mu_l))$ must be a free pro-l group of rank $\frac{1}{2}(l+1)$.

(P4) What is k_{φ_l}? What is the structure of the pro-l group Gal $(k_{\varphi_l}/Q_l(\mu_l))$? (Is it free with rank $\frac{1}{2}(l+1)$?)

Unfortunately, the choice of standard generators of the Demůskin group Gal $(\Sigma_l/Q_l(\mu_l))$ seems "too arbitrary" to study Gal $(k_{\varphi_l}/Q_l(\mu_l))$ as its quotient.

(1–7) φ_{F_p} *for* $p \neq l$. The representation φ_{F_p}: Gal $(\bar{F}_p/F_p) \to \Phi$ is determined by the image of the Frobenius element. Its conjugacy class is the same as the one determined by the φ_Q-image of a Frobenius above p. This conjugacy class is contained in the subset $\{\sigma \in \Phi; N(\sigma)=p\}$, but as shown in [9] I, this set consists of more than one Φ-conjugacy class (and in fact, infinitely many Φ-conjugacy classes; cf. Kanako [12]).

(P5) Can one give a good parametrization of Φ-conjugacy classes and pinpoint the Frobenius conjugacy class?

§2. Approximation of φ; the canonical filtration of G_Q

(2–1) In Sections 2 and 3, we shall consider two different types of "approximations" of φ. First, in Section 2, we restrict ourselves to the pro-l case and consider the first type. This arises from the filtration $\{\mathfrak{F}(m)\}_{m\geqslant 1}$ of the free pro-l group $\mathfrak{F}=\mathrm{Gal}(M/K)$ by the descending central series; $\mathfrak{F}(1)=\mathfrak{F}$, $\mathfrak{F}(m+1)=[\mathfrak{F}, \mathfrak{F}(m)]$ $(m\geqslant 1)$. Here, [,] is the commutator operation (closure of the algebraic commutator). Take any positive integer m. Then each outer automorphism of $\mathfrak{F}$ induces an outer automorphism of $\mathfrak{F}/\mathfrak{F}(m+1)$ and hence an automorphism of its center $\mathfrak{F}(m)/\mathfrak{F}(m+1)$. Therefore, Φ and hence also G_Q act outerly on $\mathfrak{F}/\mathfrak{F}(m+1)$, and in particular on $\mathfrak{F}(m)/\mathfrak{F}(m+1)$. We have three things here to look at.

(i) First, $\mathfrak{F}(m)/\mathfrak{F}(m+1)$ is a free $\boldsymbol{Z}_l$-module of finite rank

$$\rho_m=\frac{1}{m}\sum_{d\mid m}\mu\left(\frac{m}{d}\right)2^d; \qquad \text{(Witt)};$$

hence $\mathrm{Aut}(\mathfrak{F}(m)/\mathfrak{F}(m+1))\simeq GL_{\rho_m}(\boldsymbol{Z}_l)$. But for any $\sigma\in\mathrm{Aut}\,\mathfrak{F}$, the action of σ on $\mathfrak{F}(m)/\mathfrak{F}(m+1)$ is determined by its action on $\mathfrak{F}/\mathfrak{F}(2)\simeq\boldsymbol{Z}_l^{\oplus 2}$. In particular, for $\sigma\in\Phi$, it acts on $\mathfrak{F}(m)/\mathfrak{F}(m+1)$ via scalar multiplication by $N(\sigma)^m$. Therefore, this representation of G_Q in $\mathfrak{F}(m)/\mathfrak{F}(m+1)$ is simply the scalar representation given by $\rho\to\chi(\rho)^m$ $(\rho\in G_Q)$.

(ii) Each quotient $\mathfrak{F}/\mathfrak{F}(m+1)$ is a finitely generated pro-l group, and is nilpotent with finite level. So, as Deligne did in [6], one may look at its Malcev's Lie algebra $\mathfrak{g}_m$ over $\boldsymbol{Q}$, and try to determine the Galois image in $\mathrm{Der}(\mathfrak{g}_m)/\mathrm{Int}(\mathfrak{g}_m)$; the algebra of outer derivations of $\mathfrak{g}_m$. By using the Belyǐ lifting of φ, one may replace Out $\mathfrak{F}$ by Aut $\mathfrak{F}$, and $\mathrm{Der}(\mathfrak{g}_m)/\mathrm{Int}(\mathfrak{g}_m)$ by $\mathrm{Der}(\mathfrak{g}_m)$. In [6], Deligne gives a description of the Galois image in $\mathrm{Der}(\mathfrak{g}_m)$ modulo some ideal. It corresponds to some essential part of the study [9] of the Galois representation in $\mathrm{Out}(\mathfrak{F}/[\mathfrak{F}(2), \mathfrak{F}(2)])$ (cf. [9] IV §7).

(iii) Let $\Phi(m)$ $(m\geqslant 1)$ denote the kernel of the homomorphism $p_m^1:\Phi\to\mathrm{Out}(\mathfrak{F}/\mathfrak{F}(m+1))$. Then $\Phi(1)$ is the kernel of the norm N: $\Phi\to\boldsymbol{Z}_l^\times$, and $\{\Phi(m)\}_{m\geqslant 1}$ gives a descending filtration of Φ. For $m\geqslant 2$, $\Phi(m)$ is the same as the group $\Phi_1(m)$ of [9]. In particular, $\Phi(1)=\Phi(2)=\Phi(3)$, and $[\Phi(m), \Phi(n)]\subset\Phi(m+n)$ $(m, n\geqslant 1)$. For each $m\geqslant 2$, the quotient $\mathrm{gr}^m\,\Phi=\Phi(m)/\Phi(m+1)$ is a free $\boldsymbol{Z}_l$-module of rank $2\rho_m-\rho_{m+1}$. The group $\Phi/\Phi(1)\simeq\boldsymbol{Z}_l^\times$ acts on $\mathrm{gr}^m\,\Phi$ via conjugation $\mathrm{Int}\,\sigma$ $(\sigma\in\Phi)$, and this action is nothing but the α^m-multiplication $(\alpha\in\boldsymbol{Z}_l^\times)$. As for the symmetric part $S\Phi$ of Φ, we also put $S\Phi(m)=S\Phi\cap\Phi(m)$. Then $\mathrm{gr}^m\,S\Phi=S\Phi(m)/S\Phi(m+1)$ can be considered naturally as a submodule of $\mathrm{gr}^m\,\Phi$, and its rank is approximately 1/6 times rank $\mathrm{gr}^m \Phi$. More precisely, it is given by the following formula of Deligne*);

$$\mathrm{rank}\ \mathrm{gr}^m S\Phi = \alpha_m - \beta_{m+1} \qquad (m \geqslant 3,\ l \neq 2, 3),$$

with

$$\alpha_m = (r_m : \pi) = \frac{1}{3m} \sum_{\substack{d \mid m \\ m/d \not\equiv 0 \ (\mathrm{mod}\ 3)}} \left\{ \mu\left(\frac{m}{d}\right) 2^d - \varepsilon_m \right\},$$

$$\beta_m = (r_m : 1) = \frac{1}{6m} \left\{ \sum_{d \mid m} \delta\left(\frac{m}{d}\right) \mu\left(\frac{m}{d}\right) 2^d + 2\varepsilon_m \right\},$$

where

$$\varepsilon_m = \begin{cases} -1 \cdots m = 3^\alpha \\ 2 \cdots m = 2 \cdot 3^\alpha \\ 0 \cdots \text{otherwise} \end{cases}, \qquad \delta(m) = \begin{cases} 1 \cdots & m \equiv \pm 1 \\ 3 \cdots & 3 \\ 4 \cdots & \pm 2 \\ 6 \cdots & 0 \end{cases} \quad (\mathrm{mod}\ 6).$$

Here, r_m is the character of the $\mathfrak{S}_3$-action on $\mathfrak{F}(m)/\mathfrak{F}(m+1)$, and π is the irreducible character of $\mathfrak{S}_3$ with degree 2. For small m we have

m	2	3	4	5	6	7	8	9	10	11	12
rank $\mathrm{gr}^m \Phi$	0	1	0	3	0	6	4	13	12	37	40
rank $\mathrm{gr}^m S\Phi$	0	1	0	1	0	2	1	4	2	9	7

Now call $G_{Q(m)}$ the kernel of $p_m \circ \varphi: G_Q \to \mathrm{Out}(\mathfrak{F}/\mathfrak{F}(m+1))$. In other words, $G_{Q(m)} = \varphi^{-1}(\Phi(m))$. Then $\{G_{Q(m)}\}_{m \geqslant 1}$ gives a descending filtration of G_Q such that $\bigcap_m G_{Q(m)} = G_{k_\infty}$. We have

$$Q(\boldsymbol{\mu}_{l^\infty}) = Q(1) = Q(2) = Q(3) \subset Q(4) = Q(5) \subset Q(6) \cdots.$$

The basic properties of this tower are:

(a) $\{Q(m)\}_{m \geqslant 1}$ is an increasing sequence of Galois extensions of Q, with $Q(1) = Q(\boldsymbol{\mu}_{l^\infty})$.

(b) Each extension $Q(m)/Q(1)$ is pro-l, and is unramified outside l;

(c) $\mathrm{Gal}(Q(m+1)/Q(m))$ is central in $\mathrm{Gal}(Q(m+1)/Q(1))$.

(d) Consider $\mathrm{Gal}(Q(m+1)/Q(m))$ as a Z_l-module. Then the natural action of $Z_l^\times = \mathrm{Gal}(Q(1)/Q)$ on $\mathrm{Gal}(Q(m+1)/Q(m))$ is given by the α^m-multiplication ($\alpha \in Z_l^\times$).

*) This formula appears already in his letter [5]; the author also calculated it independently.

(2–2)

(P6) Determine the sequence $\{\boldsymbol{Q}(m)\}$ explicitly. Is each $\boldsymbol{Q}(m)$ maximal under the conditions (a) ~ (d)?

For each $m \geqslant 1$, the quotient $\mathrm{gr}^m G_{\boldsymbol{Q}} = \mathrm{Gal}(\boldsymbol{Q}(m+1)/\boldsymbol{Q}(m))$ can be identified with the submodule of $\mathrm{gr}^m S\Phi$ consisting of the image of $G_{\boldsymbol{Q}(m)}$. Hence $\mathrm{gr}^m G_{\boldsymbol{Q}}$ is a free $\boldsymbol{Z}_l$-module of finite rank $\leqslant$ rank $\mathrm{gr}^m S\Phi$.

(P6′) Determine rank $\mathrm{gr}^m G_{\boldsymbol{Q}}$ $(m \geqslant 1)$.

What we know at present about this rank is as follows.

Proposition 1. *We have* $c'_m \leqslant \mathrm{rank}\ \mathrm{gr}^m G_{\boldsymbol{Q}} \leqslant c_m$, *where*

$$c'_m = \begin{cases} 1 \cdots m\colon odd \geqslant 3 \\ 0 \cdots otherwise, \end{cases} \qquad c_m = \begin{cases} a_m - b_m + 1 \cdots m\colon odd \geqslant 3 \\ a_m \qquad\quad \cdots otherwise, \end{cases}$$

with $a_m = \mathrm{rank}\ \mathrm{gr}^m S\Phi$ *(given above), and* $b_m = [(m+3)/6]$ $(m\colon odd \geqslant 3)$. *Here,* $[*]$ $(* \in \boldsymbol{Q})$ *denotes the greatest integer* $\leqslant *$.

m	1	2	3	4	5	6	7	8	9	10	11
c_m	0	0	1	0	1	0	2	1	3	2	8
rank $\mathrm{gr}^m G_{\boldsymbol{Q}}$	0	0	1	0	1	0	1 or 2	0 or 1	$1 \leqslant\ \leqslant 3$	$0 \leqslant\ \leqslant 2$	$1 \leqslant\ \leqslant 8$

(P7) Can $\mathrm{gr}^m G_{\boldsymbol{Q}}$ be non-trivial for some even m?

When $l=2$, there exists some $m \geqslant 7$ such that rank $\mathrm{gr}^m G_{\boldsymbol{Q}} > c'_m$ (cf. § 3).

(2–3) *An interpretation of* $\boldsymbol{Q}(m)$ *in terms of the Belyĭ's* $\boldsymbol{Q}$*-models.* Let $M_{\boldsymbol{Q}}$ be the $\boldsymbol{Q}$-model of M corresponding to the Belyĭ's representative [9] I § 4, $K(m+1)$ $(m \geqslant 1)$ be the subextension of M/K corresponding to $\mathfrak{F}(m+1)$ and put $K(m+1)_{\boldsymbol{Q}} = K(m+1) \cap M_{\boldsymbol{Q}}$. Then $K(m+1)_{\boldsymbol{Q}}$ is a $\boldsymbol{Q}$-model of $K(m+1)$, but it is not Galois over $\boldsymbol{Q}(t)$.

Proposition 2. (i) $k = \boldsymbol{Q}(m)$ $(m \geqslant 1)$ *is the smallest Galois extension of* $\boldsymbol{Q}$ *which makes* $K(m+1)_{\boldsymbol{Q}} \cdot k/\boldsymbol{Q}(t) \cdot k$ *a Galois extension.*

(ii) $\boldsymbol{Q}(m+1)$ *coincides with the residue field of each cuspidal place of* $K(m+1)_{\boldsymbol{Q}} \cdot \boldsymbol{Q}(m)$.

The proof is an easy exercise using [9] I.

§ 3. Subrepresentations ϕ

(3–1) The approximation of φ of the second type is, roughly speaking, as follows. Suppose $\mathfrak{n} \subset \mathfrak{F}$ is a normal subgroup invariant by the action of the Galois group $G_{\boldsymbol{Q}^*}$, for some $\boldsymbol{Q} \subset \boldsymbol{Q}^* \subset \bar{\boldsymbol{Q}}$, and suppose we know already the (outerly) action of G_{Q^*} on the quotient $\mathfrak{g}=\mathfrak{F}/\mathfrak{n}$. Consider the "finer" quotient $\mathfrak{F}^*=\mathfrak{F}/[\mathfrak{n},\mathfrak{n}]$. The main subject of Section 3 is a certain group theoretic framework convenient to describe the G_{Q^*}-action on $\mathfrak{F}^*$. An advantage of considering this extension $\mathfrak{F}^*\to\mathfrak{g}$ is that $\mathfrak{F}^*$ has trivial center (under a mild assumption on $\mathfrak{n}$). The main "new part" to describe is the G_{Q^*}-action on $\mathfrak{n}^*=\mathfrak{n}/[\mathfrak{n},\mathfrak{n}]$ which (again, under a mild assumption on $\mathfrak{n}$) can be identified with the projective limit $\varprojlim T_l(\mathrm{Jac}\, X_n^*)$ of the Tate module of the Jacobian of X_n^*, where $\{X_n^*/\boldsymbol{P}^1\}$ is the $\mathfrak{g}$-tower corresponding to $\mathfrak{n}$. The basic reference for Section 3 is [10].

(3–2) To be more precise, let $\mathfrak{F}$ be a free almost pro-l group of rank 2, $\{x, y\}$ be a generator of $\mathfrak{F}$, and put $z=(xy)^{-1}$. Let $\mathfrak{n}$ be a closed normal subgroup of $\mathfrak{F}$ such that $\mathfrak{n}$ is pro-l and

$$\mathfrak{n}\cap\langle x\rangle=\mathfrak{n}\cap\langle y\rangle=\mathfrak{n}\cap\langle z\rangle=1.$$

Put $\mathfrak{n}^*=\mathfrak{n}/[\mathfrak{n},\mathfrak{n}]$, $\mathfrak{F}^*=\mathfrak{F}/[\mathfrak{n},\mathfrak{n}]$ and $\mathfrak{g}=\mathfrak{F}/\mathfrak{n}$;

$$1\longrightarrow\mathfrak{n}^*\longrightarrow\mathfrak{F}^*\longrightarrow\mathfrak{g}\longrightarrow 1 \qquad \text{(exact).}$$

Denote by x^* (resp. y^*, z^*) the projection of x (resp. y, z) on $\mathfrak{F}^*$.

Theorem 2. (i) *The centralizer of x^* (resp. y^*, z^*) in $\mathfrak{F}^*$ is the cyclic group topologically generated by x^* (resp. y^*, z^*);*
(ii) *the center of $\mathfrak{F}^*$ is trivial.*

As for (i), one can prove a little more, that if $s^*x^*s^{*-1}$ ($s^*\in\mathfrak{F}^*$) is a power of x^* then s^* must be a power of x^* (and similarly for y^*, z^*). These proofs reduce easily to Lemma 5.3 of [10] by using free differentiations.

Now let us define the group "Φ for $\mathfrak{F}/[\mathfrak{n},\mathfrak{n}]$", called Ψ, as follows.

$$\Psi=\left\{\sigma\in\mathrm{Aut}\,\mathfrak{F}^*;\ \sigma\mathfrak{n}^*=\mathfrak{n}^*,\ \begin{matrix}\sigma x^*\sim x^{*\alpha}\\ \sigma y^*\sim y^{*\alpha}\\ \sigma z^*\sim z^{*\alpha}\end{matrix}(\exists\alpha\in\hat{\boldsymbol{Z}}^\times)\right\}/\mathrm{Int}(\mathfrak{F}^*,\mathfrak{n}^*),$$

where $\sim$ denotes conjugacy in $\mathfrak{F}^*$, and $\mathrm{Int}(\mathfrak{F}^*,\mathfrak{n}^*)$ denotes the group of all inner automorphisms of $\mathfrak{F}^*$ of the form $\mathrm{Int}\,n$ ($n\in\mathfrak{n}^*$). The exponent α is again determined uniquely by σ (call it also $\alpha=N(\sigma)$). This group contains a normal subgroup

$$\Psi_1=\left\{\sigma\in\mathrm{Aut}\,\mathfrak{F}^*;\ \begin{matrix}\sigma x^*\approx x^*\\ \sigma y^*\approx y^*\\ \sigma z^*\approx z^*\end{matrix}\right\}/\mathrm{Int}(\mathfrak{F}^*,\mathfrak{n}^*),$$

where $\approx$ denotes conjugacy by element of $\mathfrak{n}^*$.

Our first result related to these groups is the existence of a certain anti 1-cocycle $\varepsilon\colon \Psi\to\mathscr{A}^\times$, where $\mathscr{A}=\boldsymbol{Z}_l\,[[\mathfrak{g}]]$, the completed group algebra of $\mathfrak{g}$. Before stating this result, we need some preliminaries.

(3–3) Denote by $\mathscr{B}=\boldsymbol{Z}_l[[\mathfrak{F}]]$ (resp. $\mathscr{A}=\boldsymbol{Z}_l[[\mathfrak{g}]]$) the completed group algebra of $\mathfrak{F}$ (resp. $\mathfrak{g}$) over $\boldsymbol{Z}_l$, and $\pi\colon \mathscr{B}\to\mathscr{A}$ the projection. As $\mathfrak{F}$ is a free almost pro-l group of rank 2 generated by x and y, $\mathscr{B}$ is equipped with the free differentiations $\partial/\partial x$, $\partial/\partial y\colon \mathscr{B}\to\mathscr{B}$ defined as follows. Every element $\theta\in\mathscr{B}$ is expressed *uniquely* as

$$\theta=s(\theta)\cdot 1_{\mathfrak{F}}+\theta_1(x-1)+\theta_2(y-1) \qquad (\theta_1,\,\theta_2\in\mathscr{B})$$

where $s\colon \mathscr{B}\to\boldsymbol{Z}_l$ is the augmentation homomorphism. We define $\partial\theta/\partial x=\theta_1$, $\partial\theta/\partial y=\theta_2$ (cf. [10] Theorem 2.1).

Now the group Ψ acts naturally on the quotient $\mathfrak{g}$ of $\mathfrak{F}^*$, and hence also on $\mathscr{A}$ and $\mathscr{A}^\times$. Note that Ψ_1 is contained in the kernel of this action. A continuous map $\varepsilon\colon \Psi\to\mathscr{A}^\times$ will be called an anti 1-cocycle, if

$$\varepsilon(\sigma'\circ\sigma)=\sigma'(\varepsilon(\sigma))\cdot\varepsilon(\sigma'), \qquad \text{for all } \sigma,\,\sigma'\in\Psi.$$

(3–4) The following theorems are basic for the presentations of Ψ and Ψ_1.

Theorem 3. *There exists a unique continuous anti 1-cocycle*

$$\varepsilon\colon \Psi\to\mathscr{A}^\times$$

satisfying the following property. For any $\sigma\in\Psi$, any $\tilde\sigma\in\operatorname{Aut}\mathfrak{F}^*$ representing σ, and any $\alpha\in\hat{\boldsymbol{Z}}^\times$, s, $t\in\mathfrak{F}$ such that $sx^\alpha s^{-1}$ (resp. $ty^\alpha t^{-1}$) represents $\tilde\sigma x^*$ (resp. $\tilde\sigma y^*$) modulo $[\mathfrak{n},\mathfrak{n}]$, one has

$$\varepsilon(\sigma)=\pi\left(s-\frac{\partial(s-t)}{\partial x}(x-1)\right)=\pi\left(t-\frac{\partial(t-s)}{\partial y}(y-1)\right).$$

The proof is parallel to that of Theorem A in [10].

Theorem 4. (i) *For $\sigma\in\Psi$, $\varepsilon(\sigma)=1$ if and only if $\sigma=1$.*
(ii) *The restriction of ε to Ψ_1 gives an anti-isomorphism*

$$\varepsilon_1\colon \Psi_1\to[1+\mathscr{R}(\boldsymbol{x}-1)\cap\mathscr{R}(\boldsymbol{y}-1)]^\times$$

where $\boldsymbol{x}$ (resp. $\boldsymbol{y}$) is the projection of x (resp. y) on $\mathfrak{g}\subset\mathscr{A}$, and $\mathscr{R}$ is the right ideal of $\mathscr{A}$ defined by

$$\begin{aligned}\mathscr{R}&=\{r\in\mathscr{A};\,(\boldsymbol{x}-1)r\in(\boldsymbol{x}\boldsymbol{y}-1)\mathscr{A}\}\\&=\{r\in\mathscr{A};\,(\boldsymbol{y}-1)r\in(\boldsymbol{y}\boldsymbol{x}-1)\mathscr{A}\}.\end{aligned}$$

Note that in the pro-l case every element of $1+\mathscr{R}(\boldsymbol{x}-1)\cap\mathscr{R}(\boldsymbol{y}-1)$ is invertible. The proof of Theorem 4 can be obtained by the combination of methods used in [9] II (proof of Theorem 3B) and [10] § 3.

Thus if $\varDelta$ denotes the image of the canonical homomorphism $\delta\colon\varPsi\to\operatorname{Aut}\mathfrak{g}$, then $\varPsi$ *can be embedded* into the semi-direct product $\varDelta\ltimes(\mathscr{A}^\times)^\circ$ via (δ,ε), where $(\mathscr{A}^\times)^\circ$ denotes the aniti-isomorphic dual of $\mathscr{A}^\times$.

(3–5) Consider now the restriction homomorphism $\mu\colon\varPsi\to\operatorname{Aut}\mathfrak{n}^*$. How can this be explicitly presented? The following two theorems answer this question.

Theorem 5 ([10] § 1). *Consider the pro-l abelian group $\mathfrak{n}^*$ as a left $\mathfrak{g}$-module by conjugation, and hence also as a left $\mathscr{A}$-module. Then as left $\mathscr{A}$-modules,*

$$\mathfrak{n}^*\xrightarrow{\sim}\mathscr{A}(\boldsymbol{x}-1)\cap\mathscr{A}(\boldsymbol{y}-1)\qquad(\textit{canonically}).$$

This is induced from the mapping

$$\mathfrak{n}\ni n\longrightarrow\pi(\partial n/\partial x)(\boldsymbol{x}-1)=-\pi(\partial n/\partial y)(\boldsymbol{y}-1)\in\mathscr{A}(\boldsymbol{x}-1)\cap\mathscr{A}(\boldsymbol{y}-1).$$

Theorem 6. *The action of $\sigma\in\varPsi$ on $\mathfrak{n}^*$, when translated to an action on $\mathscr{A}(\boldsymbol{x}-1)\cap\mathscr{A}(\boldsymbol{y}-1)$ via Theorem 5, is given as*

$$\alpha\longrightarrow\sigma(\alpha)\cdot\varepsilon(\sigma)\qquad(\alpha\in\mathscr{A}(\boldsymbol{x}-1)\cap\mathscr{A}(\boldsymbol{y}-1)).$$

The proof is completely parallel to that of Theorem C of [10].

(3–6) *The Galois representation in $\varPsi$.* A natural representation of the Galois group $G_{\boldsymbol{Q}^*}$ in $\varPsi$ arises when there is an infinite Galois extension L/K and its $\boldsymbol{Q}^*$-model $L^*/\boldsymbol{Q}^*(t)$ $(\boldsymbol{Q}\subset\boldsymbol{Q}^*\subset\bar{\boldsymbol{Q}})$, satisfying the following properties.

(i) L/K is unramified outside $t=0,1,\infty$;

(ii) L/K is an almost pro-l extension, i.e., $\mathfrak{g}=\operatorname{Gal}(L/K)$ contains an open normal pro-l subgroup;

(iii) the ramification index of each of $0,1,\infty$ in L is infinite;

(iv) $L^*\cdot\bar{\boldsymbol{Q}}=L$, $L^*\cap\bar{\boldsymbol{Q}}=\boldsymbol{Q}^*$ (but $L^*/\boldsymbol{Q}^*(t)$ need not be Galois).

There are many interesting examples of L, such as those obtained from the tower of Fermat (or Heisenberg) curves of level l^n $(n\to\infty)$, the tower of modular curves of level $2ml^n$ $(n\to\infty)$, etc. (cf. [10]). Since we shall later refer to the "Fermat case", we recall here what this means. With the notation of Section 2 (2–3), this is the pro-l case with $L=K(2)$, $\boldsymbol{Q}^*=\boldsymbol{Q}$, and $L^*=K(2)_{\boldsymbol{Q}}$ (hence $\mathfrak{g}=\mathfrak{F}/\mathfrak{F}(2)=\boldsymbol{Z}_l\times\boldsymbol{Z}_l$).

Now L and L^* being given, denote by M the maximum pro-l extension of L unramified outside 0, 1, ∞, and put

$$\mathfrak{n}=\mathrm{Gal}\,(M/L), \quad \mathfrak{F}=\mathrm{Gal}\,(M/K), \quad \mathfrak{g}=\mathrm{Gal}\,(L/K)$$
$$1\longrightarrow\mathfrak{n}\longrightarrow\mathfrak{F}\longrightarrow\mathfrak{g}\longrightarrow 1 \qquad \text{(exact)}.$$

Then $\mathfrak{F}$ is a free almost pro-l group of rank 2 generated by two such elements x, y that x, y and $z=(xy)^{-1}$ each generates some inertia group above 0, 1, ∞ respectively. Note that $\mathfrak{n}$ satisfies the assumptions of (3–2). Identify $G_{\boldsymbol{Q}^*}$ with $\mathrm{Gal}\,(L/L^*)=\mathrm{Gal}\,(M/L^*)/\mathfrak{n}$ in the canonical way, and for each $\rho\in G_{\boldsymbol{Q}^*}$ choose an element $\rho^*\in\mathrm{Gal}\,(M/L^*)$ which lifts ρ. Then the conjugation $\mathrm{Int}\,\rho^*$ induces an automorphism of $\mathfrak{F}$ which is well-defined by ρ *modulo* inner automorphisms by elements of $\mathfrak{n}$. Clearly, $\mathrm{Int}\,\rho^*$ stabilizes $\mathfrak{n}$ and hence also $[\mathfrak{n}, \mathfrak{n}]$. Thus, $\rho\rightarrow\mathrm{Int}\,\rho^*$ induces a homomorphism

$$\psi\colon G_{\boldsymbol{Q}^*}\longrightarrow\Psi.$$

Note that the natural action of $G_{\boldsymbol{Q}^*}$ on $\mathfrak{g}$, or on $\mathfrak{n}^*$ factors through ψ.

The composite $\varepsilon\circ\psi\colon G_{\boldsymbol{Q}^*}\rightarrow\mathscr{A}^\times$ is the anti 1-cocycle constructed and studied in [10]. (In [10], $\varepsilon\circ\psi$ is denoted as ψ. It is constructed without making explicit reference to the group Ψ; cf. also [9] § II for the case $\mathfrak{n}=[\mathfrak{F}, \mathfrak{F}]$.) The composite $\mu\circ\psi\colon G_{\boldsymbol{Q}^*}\rightarrow\mathrm{Aut}\,\mathfrak{n}^*$ is the natural action of $G_{\boldsymbol{Q}^*}$ on $\mathfrak{n}^*=\varprojlim T_l\,(\mathrm{Jac}\,X_n^*)$, and by Theorems 4, 5, this can be explicitly presented as the "twisted right multiplication" of

$$\varepsilon(\psi(\rho))\in\mathscr{A}^\times \quad \text{on} \quad \mathfrak{n}^*\simeq\mathscr{A}(x-1)\cap\mathscr{A}(y-1) \quad (\rho\in G_{\boldsymbol{Q}^*}).$$

(3–7)
(P8) What is the kernel $\mathrm{Ker}\,\psi=\mathrm{Ker}\,(\varepsilon\circ\psi)$?
(P9) What is the image of $\varepsilon\circ\psi$ in $\mathscr{A}^\times$?

In the Fermat case, both questions are closely related to the Vandiver conjecture, as shown by Coleman [4].

(3–8) Since Φ and Ψ are, roughly speaking, outer automorphism groups of $\mathfrak{F}$ and of $\mathfrak{F}^*=\mathfrak{F}/[\mathfrak{n}, \mathfrak{n}]$ respectively, one wants to connect them by a "canonical homomorphism" $\gamma\colon\Phi\rightarrow\Psi$ and study its image and the kernel. This would help obtain some information on the representation φ from that on ψ. But strictly speaking, there is no canonical homomorphism $\gamma\colon\Phi\rightarrow\Psi$ unless one replaces $\mathrm{Int}\,(\mathfrak{F}^*; \mathfrak{n}^*)$ by $\mathrm{Int}\,\mathfrak{F}^*$ and makes a further assumption on $\mathfrak{n}$ that $\mathfrak{n}$ is Φ-invariant. Here, the latter assumption on $\mathfrak{n}$ would not be so harmful, because we are mostly interested in the case where $\mathfrak{n}$ is a characteristic subgroup of $\mathfrak{F}$. But the former replacement would define a group Ψ' for which an analogue of Theorem 3 would be more complicated (at least in general). So, here, we simply restrict our attention to some suitable subgroups of Φ and Ψ, imposing the following assumption on $\mathfrak{n}$;

$$\langle x\rangle \cap \langle y\rangle \cap \langle z\rangle = (1) \qquad \text{on } \mathfrak{g}.$$

This is satisfied if $\mathfrak{g}$ has trivial center, or if $\mathfrak{F}$ is pro-l and $\mathfrak{n}\subset[\mathfrak{F},\mathfrak{F}]$. Let $\Psi_1\subset\Psi$ be as given in (3–2), and put

$$\Phi_1=\Phi_{1,\mathfrak{n}}=\left\{\sigma\in \mathrm{Aut}\,\mathfrak{F};\ \begin{matrix}\sigma x\approx x\\ \sigma y\approx y\\ \sigma z\approx z\end{matrix}\right\}/\mathrm{Int}\,(\mathfrak{F};\mathfrak{n}),$$

where $\approx$ denotes conjugacy by element of $\mathfrak{n}$, and $\mathrm{Int}\,(\mathfrak{F};\mathfrak{n})$ denotes the group of inner automorphisms of $\mathfrak{F}$ of the form $\mathrm{Int}\, n$ ($n\in\mathfrak{n}$). Under the above assumption on $\mathfrak{n}$, the canonical homomorphisms $\Phi_1\to\mathrm{Out}\,\mathfrak{F}$, $\Psi_1\to\mathrm{Out}\,\mathfrak{F}^*$ are injective; hence Φ_1 can also be considered as a subgroup of Φ. There is an obvious homomorphism

$$\gamma_1\colon \Phi_1\longrightarrow\Psi_1,$$

and we have $\gamma_1\circ\varphi(\rho)=\psi(\rho)$ for all $\rho\in G_{Q^*}$ such that $\varphi(\rho)\in\Phi_1$.

(P 10) What is the image of $\varepsilon\circ\gamma_1$ in $[1+\mathscr{R}(\boldsymbol{x}-1)\cap\mathscr{R}(\boldsymbol{y}-1)]^\times$?

In the Fermat case, this is answered in [9] III (Theorem 8). Namely, the image of $\varepsilon\circ\gamma_1$ in this case is precisely the "odd part" of $[1+\mathscr{R}(\boldsymbol{x}-1)\cap\mathscr{R}(\boldsymbol{y}-1)]=1+uvw\mathscr{A}$.

(3–9) Now put $\Theta=\mathrm{Ker}\,\gamma_1$ and $G_{k_\psi}=\mathrm{Ker}\,\psi$. It is easy to see that $\varphi(G_{k_\psi})\subset\Phi_1$, and then that $\varphi(G_{k_\psi})\subset\Theta$;

$$\begin{array}{ccccccccc} & & & & G_{k_\psi} & & & & \\ & & & \theta\swarrow & \downarrow\varphi & \searrow\text{trivial} & & & \\ 1 & \longrightarrow & \Theta & \longrightarrow & \Phi_1 & \xrightarrow[\gamma_1]{} & \Psi_1 & \longrightarrow & 1. \end{array}$$

This defines a representation $\theta\colon G_{k_\psi}\to\Theta$, which factors through a faithful representation $\mathrm{Gal}\,(k_\varphi k_\psi/k_\psi)\to\Theta$. The question whether φ is richer than ψ, for a given $\mathfrak{n}$, is equivalent to asking whether θ is non-trivial. Interesting concrete problems arise if one specifies $\mathfrak{n}$ and looks at the filtrations of these groups and morphisms compatible to the filtration of Φ defined in Section 2. But we shall restrict our attention to the Fermat case.

(3–10) Now, the Fermat case. In this case, $\Phi_1=\Phi(1)$, and Φ_1 and Ψ_1 coincide with the groups treated in [9] under the same symbols. Obviously, $\boldsymbol{Q}(\boldsymbol{\mu}_{l^\infty})\subset k_\psi\subset k_\varphi$. Moreover, k_ψ is *abelian* over $\boldsymbol{Q}(\boldsymbol{\mu}_{l^\infty})$ [9]. Define a filtration $\{\Psi_1(m)\}_{m\geqslant 1}$ of Ψ_1 using the descending central series $\{\mathfrak{F}^*(m)\}_{m\geqslant 1}$ of $\mathfrak{F}^*=\mathfrak{F}/[\mathfrak{n},\mathfrak{n}]=\mathfrak{F}/[\mathfrak{F}(2),\mathfrak{F}(2)]$. Namely, $\Psi(m)$ is the kernel of the canonical homomorphism $\Psi_1\to \mathrm{Out}(\mathfrak{F}^*/\mathfrak{F}^*(m+1))$. Correspondingly, we define another filtration of $G_{\boldsymbol{Q}}$, by $G_{\boldsymbol{Q}[m]}=\psi^{-1}(\Psi_1(m))$. Then $\boldsymbol{Q}[1]=\boldsymbol{Q}(\boldsymbol{\mu}_{l^\infty})$, and $\{\boldsymbol{Q}[m]\}_{m\geqslant 1}$ satisfies all properties (a)$\sim$(d) for $\boldsymbol{Q}(m)$. (Besides this, $\boldsymbol{Q}[m]/\boldsymbol{Q}(\boldsymbol{\mu}_{l^\infty})$ is abelian, and $\cup\,\boldsymbol{Q}[m]=k_\psi$.) It is clear that $\boldsymbol{Q}[m]\subset\boldsymbol{Q}(m)$ for each $m\geqslant 1$.

Theorem 7. *The Galois group* $\mathrm{Gal}(\boldsymbol{Q}[m]/\boldsymbol{Q}[m+1])$ $(m\geqslant 1)$ *is a free* $\boldsymbol{Z}_l$*-module of rank* $c'_m=1$ $(m$*:odd*$\geqslant 3)$, $=0$ (*otherwise*).

This is a direct consequence of the combination of [11] Theorem B (first proved by Coleman [4]) and [8] Theorem B (by C. Soulé). From all these follow that $k_\varphi=k_\psi$ if and only if $\boldsymbol{Q}[m]=\boldsymbol{Q}(m)$ for all $m\geqslant 1$, or equivalently, rank $\mathrm{gr}^m G_{\boldsymbol{Q}}=c'_m$ for all $m\geqslant 1$.

Corollary. *θ in the Fermat case is non-trivial if and only if there exists some $m\geqslant 7$ with* rank $\mathrm{gr}^m G_{\boldsymbol{Q}}>c'_m$.

(Incidentally, Proposition 1 (§2) follows by using the above filtration of Ψ_1. In fact, $\mathrm{Gal}(\boldsymbol{Q}[m]/\boldsymbol{Q}[m+1])$ can be regarded as a submodule of $\mathrm{gr}^m\,\Psi_1$, and it lies in $\mathrm{gr}^m\,S\Psi_1^-$, where $-$ specifies the "odd part" [9] III, and S specifies the $\mathfrak{S}_3$-symmetric part (analogous to $S\Phi$). The number $b_m=[(m+3)/6]$ is the rank of $\mathrm{gr}^m\,S\Psi_1^-$, and this gives Proposition 1.)

At present, it is only for $l=2$ that we know the non-triviality of θ;

Proposition 3. *When $l=2$, θ is non-trivial.*

To prove the non-triviality of θ, it suffices to show that $k_\varphi/\boldsymbol{Q}(\boldsymbol{\mu}_{l^\infty})$ is *non*-abelian. When $l=2$, this last statement can be checked by using the following two special circumstances.

(i) When $l=2$, the modular curves of 2-power levels constitute a pro-2 tower of coverings of $\boldsymbol{P}^1$ unramified outside 0, 1, ∞ (because $\boldsymbol{P}^1$ can be regarded as the modular curve of level 2 with cusps at 0, 1, ∞).

(ii) There exists an elliptic curve over $\boldsymbol{Q}$ with conductor 2^7, which is a Weil curve and has no CM [15].*)

For $l>3$, one may try to use Heisenberg curves instead, but at present, the author does not know whether their Jacobians do not really have enough CM.

---

*) The author is grateful to M. Asada for pointing out this fact together with the reference.

References

[1] Anderson, G., The hyperadelic gamma function, this volume,

[2] Asada, M. and Kaneko, M., On the automorphism group of some pro-l fundamental groups, this volume,

[3] Belyĭ G. V., On Galois extensions of a maximal cyclotomic field, Izv. Akad. Nauk. USSR, **43** (1979) 2; (Math. USSR Izv., **14** (1980) 2, 247–256).

[4] Coleman, R, Algebra Colloquium lecture at Univ. of Tokyo, Oct. 22, 1985 (still unpublished).

[5] Deligne, P., Letters to A. Grothendieck; Nov. 19 (1982), and an earlier one, undated.

[6] ——, Letters to S. Bloch; Feb. 2, March 14 (1984).

[7] Grothendieck, A., Esquisse d'une programme, mimeographed note (1984).

[8] Ichimura, H. and Sakaguchi, K., The non-vanishing of a certain Kummer character χ_m (after C. Soulé) and some related topics, this volume,

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

[10] ——, On Galois representations arising from towers of covering of $P^1\backslash\{0, 1, \infty\}$; Invent Math., **86** (1986), 427–459.

[11] Ihara, Y., Kaneko, M. and Yukinari, A., On some properties of the universal power series for Jacobi sums, this volume

[12] Kaneko, M., On conjugacy classes of the pro-l braid group of degree 2; Proc. Japan Acad., **62A** (1986), 274–277.

[13] Koch, H., *Galoissche Theorie der p-Erweiterungen, Springer* (1970).

[14] Kohno, T. and Oda, T., The lower central series of the pure braid group of an algebraic curve, this volume

[15] Ogg, A. P., Abelian curves of 2-power conductor, Proc. Camb. Phil. Soc., **62** (1966), 143–148.

Department of Mathematics
Faculty of Science
University of Tokyo
Hongo 7, Tokyo 113, Japan