Invent. math. 86, 427–459 (1986)

Inventiones mathematicae
© Springer-Verlag 1986

On Galois representations arising from towers of coverings of $\mathbf{P}^1\backslash\{0,1,\infty\}$

Yasutaka Ihara

Department of Mathematics, Faculty of Science, University of Tokyo, Hongo, Bunkyo-ku, Tokyo 113, Japan

Summary. We propose a new way to describe, universally, the l-adic Galois representations associated to each "almost pro-l" tower of etale coverings of $\mathbf{P}^1\backslash\{0,1,\infty\}$. This generalizes our universal power series for Jacobi sums (cf. [I]) which arises from the tower of Fermat curves of degree l^n ($n\to\infty$), and contains the case of the tower of modular curves of level $2ml^n$ (m: fixed, $n\to\infty$) as another important special case. As a fundamental tool, we shall establish and use an "almost pro-l version" of the theorems of Blanchfield and of Lyndon in Fox free differential calculus.

§ 0. Introduction

(A) First, we recall the following classical situation. Suppose given a pair (X^*, G) of a complete smooth absolutely irreducible curve X^* over $\mathbf{Q}^*$ ($\mathbf{Q}\subset\mathbf{Q}^*\subset\bar{\mathbf{Q}}$) and a finite group G of $\mathbf{Q}^*$-automorphisms of X^*. Then the Tate module $T_l=T_l(\mathrm{Jac}\,X^*)$ of the Jacobian of X^* (at a prime l) can be regarded as a left module over the group ring $A=\mathbf{Z}_l[G]$, and the Galois group $G_{\mathbf{Q}^*}=\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}^*)$ acts on T_l as A-automorphisms, defining a Galois representation $G_{\mathbf{Q}^*}\to E^\times$ into the unit group of $E=\mathrm{End}_A T_l$. In general, E can be quite big and complicated to describe. But if T_l is (close to being) a *free* A-module of rank one, then E is (close to being) the anti-isomorphic dual A' of A, and we obtain an *anti-representation* (which looks like) $G_{\mathbf{Q}^*}\to A^\times$. This will be referred to as the *(quasi) skew CM-case*. The well-known case is where G is abelian and $\mathrm{Jac}\,X^*$ has complex multiplications arising from the G-action (the *CM-case*). Two questions arise.

(i) Is there any other (quasi) skew CM-case?

(ii) Would (quasi) skew-CM theory be useful?

But first, we remind ourselves of the principal difference between the CM (i.e., A: commutative) and the skew-CM (A: not necessarily commutative) cases. In the former case, the action of each $\rho\in G_{\mathbf{Q}^*}$ on T_l is *represented* by the left multiplication by an element $a\in A$, and the association $\rho\to a$ is really canonical.

On the other hand, in the latter case, it is only *measured* by the "right multiplication" of some $a' \in A$, and the association $\rho \to a'$ depends on the choice of an A-basis of T_l. So, the question (ii) is closely related to whether there is a "good choice" of an A-basis of T_l. Of course, it also depends on *how close* to a principal A-module our T_l is (in short, how *neat* it is).

(B) The main purpose of this paper is to give a partial answer to the above questions by showing:

(a) Roughly speaking, a quasi skew-CM theory holds when (X^*, G) is a Galois covering of $\mathbf{P}^1$ unramified outside 3 points.

(b) It can be made simple and neat, by consideration of an almost pro-l *tower* $\{X_n^*\}$ over $\mathbf{P}^1$ (instead of a single covering) and by passage to the projective limits. Moreover, there is a fairly good way to choose a "basis" for $\varprojlim T_l(\mathrm{Jac}\, X_n^*)$.

(c) Including the CM-case, the universal treatment for almost pro-l towers $\{X_n^*\}$ gives a new approach and some applications to Galois representations w.r.t. (e.g.) Fermat and modular curves.

There is a closely related work, developed independently by G. Anderson. He enlarges $T_l(\mathrm{Jac}\, X^*)$ to the Tate module of a certain well-chosen 1-*motive* to make it a principal A-module! While we use free differential calculus as a basic tool and put stress on the simplification at the limit, his method is geometric and treats each curve and ramification carefully and beautifully. His work, communicated to the author first in October 1985, will be partially presented in [A]. These two works, at the present stage, may be regarded as forming a pair with each other.

(C) Now we shall state our main results in a somewhat specialized form. Let $\{X_n^*\}_{n=0}^{\infty}$ be an almost pro-l tower of Galois coverings $X_n^*/\mathbf{P}^1$, unramified outside $0, 1, \infty$ and having infinite ramification indices at $0, 1, \infty$ (see § 1 for precise definitions). Put $\mathfrak{G} = \varprojlim \mathrm{Gal}(X_n^*/\mathbf{P}^1)$, $\mathscr{A} = \mathbf{Z}_l[[\mathfrak{G}]]$ (the completed group algebra), and $\mathfrak{T} = \varprojlim T_l(\mathrm{Jac}\, X_n^*)$. Let Q^* be a common field of definition for the Galois coverings $X_n^*/\mathbf{P}^1$. Our main results consist of:

(I) Construction of a "universal" anti-representation

$$\psi\colon G_{\mathbf{Q}^*} \to \mathscr{A}^\times \qquad \text{(Theorem A, § 1).}$$

(II) Explicit presentation of $\mathfrak{T}$ as a left $\mathscr{A}$-ideal A (Theorem B and Remark 1.5; § 1).

(III) Description of the $G_{\mathbf{Q}^*}$-action on $\mathfrak{T}$, as the right multiplication of $\psi(\rho)$ $(\rho \in G_{\mathbf{Q}^*})$ on A (Theorem C, Remark 1.5; § 1).

All depend simultaneously on the choice of a "coordinate system" described below.

The first step is to enlarge the tower $\{X_n^* \otimes \bar{\mathbf{Q}}\}$ by adding *all* pro-l coverings of $X_n^* \otimes \bar{\mathbf{Q}}$ unramified outside $0, 1, \infty$. Call $\mathfrak{F}$ the total Galois group of the enlarged tower over $\mathbf{P}^1_{\bar{\mathbf{Q}}}$. Then $\mathfrak{F}$ is a *free almost pro-l group* of rank 2, in the sense of § 2 (A). A choice of an ordered set of generators (x, y) for $\mathfrak{F}$ is the unique choice of a "coordinate system" made in this paper. This will determine all basic isomorphisms, (anti-)representations, etc. uniquely. The basic requirement for (x, y) is that each of $x, y, z=(xy)^{-1}$ is a *loop* around one of $0, 1, \infty$. Once $\bar{\mathbf{Q}}$ is embedded in $\mathbf{C}$, there is a standard choice for (x, y) (cf. § 3 (A)). Now our explicit presentation of the "Tate module" $\mathfrak{T}$ is based on the group-theoretic re-interpretation of $\mathfrak{T}$ *as the abelianization* $\mathfrak{N}^{\mathrm{ab}}$ *of the kernel* $\mathfrak{N}$ *of the projection* $\mathfrak{F} \to \mathfrak{G}$:

$$\begin{aligned} &1 \to \mathfrak{N} \to \mathfrak{F} \to \mathfrak{G} \to 1 \qquad \text{(exact)} \\ &\mathfrak{F}\text{: "free", } \mathfrak{T} \simeq \mathfrak{N}^{\mathrm{ab}} \qquad \text{(as left } \mathscr{A}\text{-modules).} \end{aligned} \tag{1}$$

By applying to (1) the "almost pro-l" version of the Blanchfield-Lyndon theorem in free differential calculus (§ 2), we obtain an explicit presentation

$$\mathfrak{T} = \mathfrak{N}^{\mathrm{ab}} \xrightarrow{\sim} \{(\xi, \eta) \in \mathscr{A}^{\oplus 2};\ \xi(\mathbf{x}-1) + \eta(\mathbf{y}-1) = 0\} \tag{2}$$

of $\mathfrak{T}$ as a left $\mathscr{A}$-module (Theorem B). Here, $\mathbf{x}$ (resp. $\mathbf{y}$) denotes the projection of x (resp. y) on $\mathfrak{G} \subset \mathscr{A}$. One may further identify the modules of (2) with the left $\mathscr{A}$-ideal $\mathscr{A}(\mathbf{x}-1) \cap \mathscr{A}(\mathbf{y}-1)$, via $(\xi, \eta) \leftrightarrow \xi(\mathbf{x}-1)$ ($\mathbf{x}-1, \mathbf{y}-1$ are not zero-divisors in $\mathscr{A}$).

Now the Galois group $G_{\mathbf{Q}^*}$ acts on $\mathfrak{T}$ as $\mathscr{A}$-automorphisms. From the above presentation of $\mathfrak{T}$, it is not clear what $\mathrm{End}_{\mathscr{A}} \mathfrak{T}$ looks like, and in particular, whether all $\mathscr{A}$-endomorphisms of $\mathscr{A}(\mathbf{x}-1) \cap \mathscr{A}(\mathbf{y}-1)$ are given by right-multiplications of those $\alpha \in \mathscr{A}$ satisfying $(\mathbf{x}-1)\alpha \in \mathscr{A}(\mathbf{x}-1)$ and $(\mathbf{y}-1)\alpha \in \mathscr{A}(\mathbf{y}-1)$. *But* $G_{\mathbf{Q}^*}$ *acts this way*! In fact, we can construct three anti-representations

$$\psi = \psi_{\{x, y\}}, \psi_x, \psi_y \colon G_{\mathbf{Q}^*} \to \mathscr{A}^{\times}, \tag{3}$$

related to each other by

$$(\mathbf{x}-1)\psi(\rho) = \psi_x(\rho)(\mathbf{x}-1), \qquad (\mathbf{y}-1)\psi(\rho) = \psi_y(\rho)(\mathbf{y}-1)$$

($\rho \in G_{\mathbf{Q}^*}$), such that the action of ρ on $\mathfrak{T}$ is given (via (2)) as

$$(\xi, \eta) \to (\xi, \eta) \begin{pmatrix} \psi_x(\rho) & 0 \\ 0 & \psi_y(\rho) \end{pmatrix},$$

or equivalently, as $\lambda \to \lambda \cdot \psi(\rho)$ ($\lambda \in \mathscr{A}(\mathbf{x}-1) \cap \mathscr{A}(\mathbf{y}-1)$) (Theorem C). The anti-representations (3) are constructed independently of the $G_{\mathbf{Q}^*}$-action on $\mathfrak{T}$ (Theorem A). They describe, not only the $G_{\mathbf{Q}^*}$-action on $\mathfrak{N}^{\mathrm{ab}}$, but also that on $\mathfrak{F}/[\mathfrak{N}, \mathfrak{N}]$ (modulo inner automorphisms by elements of $\mathfrak{N}^{\mathrm{ab}}$). However, in several important cases, this difference disappears, and the kernel of ψ *coincides* with that of the $G_{\mathbf{Q}^*}$-action on $\mathfrak{N}^{\mathrm{ab}}$ (§ 5).

The following is a direct corollary of Theorem C (§ 1): We can always find (*via* a certain specialization of ψ) an open subgroup of $G_{\mathbf{Q}^*}$ which acts *unipotently* on the group of l-division points of $\mathrm{Jac}\, X_n^*$ *for all* n. Here, of course, the point is that it is simultaneous for all n, and the chief reason is that the $G_{\mathbf{Q}^*}$-action is measured by the elements of $\mathscr{A}^{\times}$.

Typical examples are:

1) The tower of Fermat curves of degree l^n;

$$\mathfrak{G}=\mathbf{Z}_l\times\mathbf{Z}_l;$$

2) The tower of modular curves of level $2ml^n$ (m: fixed, $(m,l)=1$. Start with level 2, then $2m, 2ml, \ldots$).

$$\mathfrak{G}=(SL_2(\mathbf{Z}/m)\times SL_2(\mathbf{Z}_l))/\pm I \qquad (\text{if } (ml,2)=1).$$

3) Other standard nilpotent towers, such as the Heisenberg tower,

$$\mathfrak{G}=\left\{\begin{pmatrix}1 & a & c\\ 0 & 1 & b\\ 0 & 0 & 1\end{pmatrix};\ a,b,c\in\mathbf{Z}_l\right\}.$$

In our previous work [I], we studied the universal 1-cocycle

$$\psi\colon G_{\mathbf{Q}}\to\mathscr{A}^\times=\mathbf{Z}_l[[\mathbf{Z}_l\times\mathbf{Z}_l]]^\times=\mathbf{Z}_l[[u,v]]^\times$$

arising from the tower of Fermat curves, in connection with Jacobi sums, Coleman power series, larger Galois representations, etc. (cf. also [A] [IKY]). We hope that the study of our generalized anti-representation (or anti 1-cocycle, under a loosened assumption) will give, as in the Fermat case, further insight into the arithmetic of $T_l(\mathrm{Jac}\,X_n^*)$, and into the large Galois representation $\varphi_{\mathbf{Q}}\colon G_{\mathbf{Q}}\to\mathrm{Aut}\,\pi_1^{\text{pro-}l}\,(\mathbf{P}^1_{\mathbf{Q}}\backslash\{0,1,\infty\})$. Some aspects related to modular curves will be discussed in future publications (cf. also Example 3 § 1).

(D) The organization of this paper is as follows. In § 1, we shall present our main results (Theorems A–C) under a generalized form, together with some examples. In § 2, we shall establish an "almost pro-l" analogue of free differential calculus, including that of theorems of Blanchfield and of Lyndon. In § 3, we shall give proofs of results presented in § 1, and in § 4, discuss the dependence of ψ on the choice of the coordinate (x,y), together with some basic congruences satisfied by ψ. In § 5, we shall discuss the relation between the kernel of ψ and that of the $G_{\mathbf{Q}*}$-action on $\mathfrak{X}$.

The author is particularly grateful to Takayuki Oda and G. Anderson for valuable communications related to this subject. The idea to use free differential calculus which the author had vaguely in mind was first realized by Oda's alternative proof of Theorem 2 of [I] (a special case of Theorem 2.2 of this paper). It required pro-l justifications but prompted the present study. Communications with Anderson mentioned above helped in enlarging the scope which affected some descriptions in § 0 and § 5. He is also very grateful to B. Mazur and H. Sah for stimulating discussions, and to Harvard University for the hospitality during the spring of 1985, while this work was being developed.

§ 1. Preliminaries and statement of main results

(A) The completed group algebra. Let l be a fixed prime number, and $\mathbf{Z}_l$ be the ring of l-adic integers. For a profinite group $\mathfrak{G}$, its completed group

algebra $\mathscr{A}=\mathbf{Z}_l[\![\mathfrak{G}]\!]$ over $\mathbf{Z}_l$ is defined in the usual way, as follows. Let $\{N_\lambda\}_{\lambda\in\Lambda}$ be the set of all *open* normal subgroups of $\mathfrak{G}$, and for each $\lambda\in\Lambda$, put $G_\lambda=\mathfrak{G}/N_\lambda$. Then each G_λ is finite, and $\mathfrak{G}=\varprojlim G_\lambda$. For each pair (λ,m) of $\lambda\in\Lambda$ and a positive integer m, consider its usual group algebra $A_{\lambda,m}=(\mathbf{Z}/l^m)[G_\lambda]$ over $\mathbf{Z}/l^m$. For two pairs (λ,m) and (μ,n) such that $N_\lambda\subset N_\mu$ and $m\geqq n$, let $p_{(\mu,n)}^{(\lambda,m)}$ denote the ring homomorphism $A_{\lambda,m}\to A_{\mu,n}$ defined by $\sum_{g\in G_\lambda} a_g g\to\sum_{g\in G_\lambda} p_n^m(a_g)p_\mu^\lambda(g)$, where p_n^m: $\mathbf{Z}/l^m\to\mathbf{Z}/l^n$ and p_μ^λ: $G_\lambda\to G_\mu$ are canonical projections. Then $\{A_{\lambda,m}, p_{(\mu,n)}^{(\lambda,m)}\}$ forms a projective system of finite rings, and $\mathscr{A}$ is, by definition, its projective limit $\varprojlim A_{\lambda,m}$. It is naturally a $\mathbf{Z}_l$-algebra, and carries *a projective limit topology*, w.r.t. which $\mathscr{A}$ is compact. The augmentation homomorphisms $s_{\lambda,m}$: $A_{\lambda,m}\to\mathbf{Z}/l^m$ defined by $\sum a_g g\to\sum a_g$ induce a homomorphism s: $\mathscr{A}\to\mathbf{Z}_l$, called the augmentation homomorphism of $\mathscr{A}$. Its kernel $I=I_{\mathscr{A}}$, the augmentation ideal, is a two-sided closed ideal of $\mathscr{A}$. It is topologically nilpotent when $\mathfrak{G}$ is a pro-l group, but not always so in general. (For example, if $\mathfrak{G}=PSL_2(\mathbf{Z}_l)$ with $l>3$, then $\mathfrak{G}=[\mathfrak{G},\mathfrak{G}]$; hence $I=I^2=\ldots\neq 0$.) We shall consider $\mathfrak{G}$ as embedded in $\mathscr{A}^\times$, the group of invertible elements of $\mathscr{A}$, in the obvious manner.

For example, if $\mathfrak{G}$ is a free pro-l group of rank r generated by $x_1,\ldots,x_r$, then

$$\mathscr{A}\cong\mathbf{Z}_l[\![u_1,\ldots,u_r]\!]_{\mathrm{nc}}\quad\text{by } x_j-1\leftrightarrow u_j\ (1\leqq j\leqq r)$$

as topological $\mathbf{Z}_l$-algebras, where $\mathbf{Z}_l[\![u_1,\ldots,u_r]\!]_{\mathrm{nc}}$ denotes the algebra of formal power series in mutually *non-commutative* variables $u_1,\ldots,u_r$ over $\mathbf{Z}_l$, equipped with the Krull topology (cf. [S]). The augmentation s: $\mathscr{A}\to\mathbf{Z}_l$ corresponds to $f(u)\to f(0)$. Therefore, each element $\theta\in\mathscr{A}$ can be expressed *uniquely* in the form

$$s(\theta)\cdot 1+\sum_{j=1}^{r}\theta_j(x_j-1)\qquad(\theta_1,\ldots,\theta_r\in\mathscr{A}).$$

This defines "free differentiations" $\dfrac{\partial\theta}{\partial x_j}=\theta_j$ $(1\leqq j\leqq r)$, which will be generalized later to the case of *free almost pro-l* groups (§2).

As another well-known example, if $\mathfrak{G}\cong\mathbf{Z}_l\times\ldots\times\mathbf{Z}_l$ (r copies), then $\mathscr{A}\cong\mathbf{Z}_l[\![u_1,\ldots,u_r]\!]$ (by $x_j-1\leftrightarrow u_j$), the algebra of *commutative* formal power series in r variables over $\mathbf{Z}_l$. We shall also treat the cases such as $\mathfrak{G}=PSL_2(\mathbf{Z}_l)$, or $SL_2(\mathbf{Z}_l)$. In these cases, $\mathfrak{G}$ is no longer a pro-l group, but contains a pro-l open normal subgroup $\mathfrak{G}_1$, the principal congruence subgroup of level l. The completed group algebra $\mathscr{A}_1=\mathbf{Z}_l[\![\mathfrak{G}_1]\!]$ of $\mathfrak{G}_1$ is a certain quotient of $\mathbf{Z}_l[\![u_1,u_2,u_3]\!]_{\mathrm{nc}}$, and one can obtain an explicit presentation of $\mathscr{A}$ using that of $\mathscr{A}_1$.

(B) The given data. Let $K^*=\mathbf{Q}^*(t)$ be the rational function field of one variable over a subfield $\mathbf{Q}^*\subset\bar{\mathbf{Q}}$ (the algebraic closure of $\mathbf{Q}$). The main object we start with is an infinite algebraic extension L^*/K^*, containing no non-trivial constant field extensions and satisfying the following conditions (i)–(iii), where $L=L^*\cdot\bar{\mathbf{Q}}$ and $K=K^*\cdot\bar{\mathbf{Q}}=\bar{\mathbf{Q}}(t)$ (the composite fields).

(i) L/K is a Galois extension and is *unramified outside* $t=0, 1, \infty$.

(ii) L/K is an *almost pro-l* extension, i.e., L contains a finite Galois extension K_1/K such that L/K_1 is a pro-l extension.

(iii) The ramification indices of $0, 1, \infty$ in L/K are *infinite.*

Note here that L/L^* is a Galois extension with $\mathrm{Gal}(L/L^*) \simeq \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}^*)$ (canonically), and that L/K^* is also Galois (whose Galois group being generated by $\mathrm{Gal}(L/K)$ and $\mathrm{Gal}(L/L^*)$).

Now let M be the maximum pro-l extension of L which is unramified outside the places $t=0, 1, \infty$ of K. Then M/K^* is a Galois extension (because the condition characterizing the extension M/L is $\mathrm{Gal}(L/K^*)$-invariant). Therefore, M/K, M/L^* are also Galois. Define

$$\mathfrak{N}=\mathrm{Gal}(M/L), \qquad \mathfrak{F}=\mathrm{Gal}(M/K), \qquad \mathfrak{G}=\mathrm{Gal}(L/K),$$

$$1 \to \mathfrak{N} \to \mathfrak{F} \to \mathfrak{G} \to 1 \quad \text{(exact)};$$

$$\begin{tikzcd}[arrows=dash]
 & M \arrow[d, "\mathfrak{N}"] \arrow[dd, bend left=60, "\mathfrak{F}"] \\
L^* \arrow[r] \arrow[d] & L \arrow[d, "\mathfrak{G}"] \\
\mathbf{Q}^*(t)=K^* \arrow[r] \arrow[d] & K=\bar{\mathbf{Q}}(t) \arrow[d] \\
\mathbf{Q}^* \arrow[r] & \bar{\mathbf{Q}}
\end{tikzcd}$$

The group $\mathrm{Gal}(M/K^*)$ acts on itself from the left by inner automorphisms $\mathrm{Int}(g)$: $g_1 \to g g_1 g^{-1}$. Every group action which is canonically induced from this will be called *the natural action.* For example, $G_{\mathbf{Q}^*}=\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}^*) \simeq \mathrm{Gal}(L/L^*)$ acts naturally on $\mathfrak{G}$, and hence on its completed group algebra $\mathscr{A}=\mathbf{Z}_l[[\mathfrak{G}]]$. This action will be denoted by J_ρ ($\rho \in G_{\mathbf{Q}^*}$). Note that this action is trivial ($J_\rho = 1$, all ρ) if and only if L^*/K^* is itself a Galois extension. Also, $G_{\mathbf{Q}^*}$ and $\mathfrak{G}$ (hence also $\mathscr{A}$) act naturally on the abelianization $\mathfrak{N}^{\mathrm{ab}}=\mathfrak{N}/[\mathfrak{N}, \mathfrak{N}]$ of $\mathfrak{N}$. Thus, $\mathfrak{N}^{\mathrm{ab}}$ is a left $\mathscr{A}$-module on which $G_{\mathbf{Q}^*}$ acts semi-linearly; $\rho(\alpha v)=J_\rho(\alpha)\rho(v)$ ($\rho \in G_{\mathbf{Q}^*}$, $\alpha \in \mathscr{A}$, $v \in \mathfrak{N}^{\mathrm{ab}}$).

Note also that $\mathfrak{N}$ is a pro-l group, and that $\mathfrak{F}$ contains a pro-l open normal subgroup $\mathfrak{F}_1=\mathrm{Gal}(M/K_1)$ (K_1: as in the condition (ii)). Since the inertia groups in characteristic 0 are (topologically) cyclic, the above condition (iii) implies that each inertia group above $t=0, 1$ or ∞ in M/K is a quotient of the profinite completion $\hat{\mathbf{Z}}$ of $\mathbf{Z}$ isomorphic to a group of the form $\mathbf{Z}_l \times (\mathbf{Z}/m)$, with some $m \geqq 1$, $m \not\equiv 0 \pmod{l}$. We write $m=m_0, m_1, m_\infty$ for $t=0, 1, \infty$, respectively. Let $\tilde{0}$ (resp. $\tilde{1}$, $\tilde{\infty}$) be a place of M above $t=0$ (resp. $1, \infty$), and x (resp. y, z) be a generator of its inertia group in $\mathfrak{F}=\mathrm{Gal}(M/K)$. By a topological reason, *we may choose* $\tilde{0}, \tilde{1}, \tilde{\infty}$ *and* x, y, z *in such a way that* $\mathfrak{F}$ *is (topologically) generated by* x *and* y, *and that* $xyz=1$ (see § 3 (A)). The choice of such a triple (x, y, z) is our second given data, which plays the role of a "coordinate system".

Finally, note that M/L is "essentially unramified", in the sense that each inertia group above $t=0, 1, \infty$ in M/K is *isomorphically* mapped to that in L/K. In fact, since M/L is pro-l and the ramification indices in L/K are divisible by l^∞, M is the composite of *unramified* pro-l extensions of K_n for all

n. We shall denote by $\mathbf{x}, \mathbf{y}, \mathbf{z}$ the projections of x, y, z on $\mathfrak{G}$, respectively. They have the *same* orders, $m_0 l^\infty$, $m_1 l^\infty$, $m_\infty l^\infty$, as x, y, z, respectively.

(C) The main results. Now suppose given L^*/K^* and (x, y, z), and denote by $\mathscr{A} = \mathbf{Z}_l[[\mathfrak{G}]]$ the completed group algebra of $\mathfrak{G} = \mathrm{Gal}(L/K)$, considered also as a G_{Q^*}-module as described above. We shall construct a continuous anti 1-cocycle

$$\psi = \psi_{\{x,y\}}\colon\ G_{Q^*} \to \mathscr{A}^\times,$$

which contains all information about the representations of G_{Q^*} in the Tate module $T_l(\mathrm{Jac}\, X_n)$ of the Jacobian of the curve X_n corresponding to K_n ($n = 0, 1, \ldots$). In particular, when L^*/K^* is a Galois extension, ψ will be an anti-representation. The construction of ψ is based on the following two Propositions:

Proposition 1.1. *Let $\mathfrak{F} = \mathrm{Gal}(M/K)$, $x, y \in \mathfrak{F}$ be as above, and $\mathscr{B} = \mathbf{Z}_l[[\mathfrak{F}]]$ be the completed group algebra of $\mathfrak{F}$. Then each element $\theta \in \mathscr{B}$ can be expressed uniquely as*

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

where $s\colon \mathscr{B} \to \mathbf{Z}_l$ is the augmentation homomorphism.

For the proof, see § 3 (A). We define the free differentiation by $\frac{\partial \theta}{\partial x} = \theta_1$, $\frac{\partial \theta}{\partial y} = \theta_2$.

For each $\rho \in G_{Q^*}$, let $\tilde{\rho} \in \mathrm{Gal}(M/L^*)$ be an extension of ρ. Then $f \to \tilde{\rho} f \tilde{\rho}^{-1}$ ($f \in \mathfrak{F}$) induces an automorphism of $\mathfrak{F}$. On the other hand, let $\chi\colon G_{Q^*} \to \hat{\mathbf{Z}}^\times$ be the cyclotomic character.

Proposition 1.2. *The notation being as above, and $\sim$ denoting conjugacy in $\mathfrak{F}$,*

$$\tilde{\rho}\, x\, \tilde{\rho}^{-1} \sim x^\alpha, \qquad \tilde{\rho}\, y\, \tilde{\rho}^{-1} \sim y^\alpha, \qquad \tilde{\rho}\, z\, \tilde{\rho}^{-1} \sim z^\alpha,$$

where $\alpha = \chi(\rho)$.

This is essentially the same as [I] I § 2 (Prop. 2). Now, $\rho, \tilde{\rho}$ being as above, choose $s, t \in \mathfrak{F}$ such that

$$\tilde{\rho}\, x\, \tilde{\rho}^{-1} = s\, x^\alpha s^{-1}, \qquad \tilde{\rho}\, y\, \tilde{\rho}^{-1} = t\, y^\alpha t^{-1} \qquad (\alpha = \chi(\rho)).$$

Consider s, t as elements of $\mathscr{B} = \mathbf{Z}_l[[\mathfrak{F}]]$. Then, by the definition of free differentiation,

$$s - t = \frac{\partial(s-t)}{\partial x}(x-1) + \frac{\partial(s-t)}{\partial y}(y-1),$$

or

$$s - \frac{\partial(s-t)}{\partial x}(x-1) = t - \frac{\partial(t-s)}{\partial y}(y-1).$$

Let $\pi\colon \mathscr{B} \to \mathscr{A}$ be the canonical projection induced from the canonical homomorphism $\mathfrak{F} \to \mathfrak{G}$.

Theorem A. *For each $\rho \in G_{Q^*}$, choose $\tilde{\rho} \in \mathrm{Gal}(M/L^*)$ and $s, t \in \mathfrak{F}$ as above. Then the element*

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

of $\mathscr{A}$ depends only on ρ, and belongs to $\mathscr{A}^{\times}$. Moreover, if we call this element $\psi(\rho)$, the mapping ψ: $G_{Q^*} \to \mathscr{A}^{\times}$ gives a continuous anti 1-cocycle, i.e.,

$$\psi(\rho' \circ \rho) = J_{\rho'}(\psi(\rho)) \cdot \psi(\rho') \qquad (\rho, \rho' \in G_{Q^*}).$$

The dependence of $\psi = \psi_{\{x,y\}}$ on the choice of the coordinate system (x, y) will be described later (§ 4).

The second main result is concerned with an explicit presentation of the projective limit $\varprojlim T_l(\mathrm{Jac}\, X_n)$ as a submodule of $\mathscr{A}^{\oplus 2}$. Let $L = \bigcup K_n$, with K_n/K: finite Galois, and put $K_n^* = L^* \cap K_n$. Let X_n^* be the complete smooth Q^*-curve with function field K_n^*, and $X_n = X_n^* \otimes \bar{Q}$. Let J_n^* (resp. J_n) be the Jacobian of X_n^* (resp. X_n), and $T_l(J_n^*) = T_l(J_n)$ be their Tate module at l. Consider the projective limit $\varprojlim T_l(J_n^*)$ as a G_{Q^*}-module, and also as a left $\mathscr{A}$-module in the natural manner (i.e., via the natural actions of G_{Q^*} and $\mathfrak{G}$ on $T_l(J_n^*)$ for each n). First, we assert the following

Proposition 1.3. *There is a canonical isomorphism $\mathfrak{N}^{\mathrm{ab}} \simeq \varprojlim T_l(J_n^*)$ commuting with the actions of G_{Q^*} and $\mathscr{A}$.*

Proof. For each $n \geqq 0$, let K_n^{urab} denote the maximum unramified abelian pro-l extension of K_n. Then $\mathrm{Gal}(K_n^{\mathrm{urab}}/K_n)$ is canonically isomorphic with $T_l(J_n^*)$. On the other hand, by the assumption (iii) on the ramifications of $0, 1, \infty$ in L/K, every finite abelian pro-l extension of K_n in M is contained in K_m^{urab} for some $m \geqq n$. Therefore, $\bigcup K_n^{\mathrm{urab}}$ coincides with the maximum abelian pro-l extension L^{ab} of L in M, i.e., the field corresponding to $[\mathfrak{N}, \mathfrak{N}]$. Therefore, $\mathfrak{N}^{\mathrm{ab}} = \mathrm{Gal}(L^{\mathrm{ab}}/L) \simeq \varprojlim \mathrm{Gal}(K_n^{\mathrm{urab}}/K_n)$ is canonically isomorphic with $\varprojlim T_l(J_n^*)$, the isomorphism obviously commuting with the actions of G_{Q^*} and $\mathscr{A}$. *q.e.d.*

Now consider the mapping

$$\mathfrak{N} \ni n \to \left(\pi\left(\frac{\partial n}{\partial x}\right), \pi\left(\frac{\partial n}{\partial y}\right)\right) \in \mathscr{A}^{\oplus 2}. \qquad (**)$$

Then:

Theorem B. *The mapping $(**)$ induces an isomorphism*

$$\mathfrak{N}^{\mathrm{ab}} \xrightarrow{\sim} \mathfrak{X} = \{(\xi, \eta) \in \mathscr{A}^{\oplus 2};\ \xi(\mathrm{x} - 1) + \eta(\mathrm{y} - 1) = 0\}$$

of left $\mathscr{A}$-modules. This isomorphism is also bicontinuous.

This is a special case of an "almost pro-l version" of a theorem of Blanchfield and of Lyndon in free differential calculus (cf. § 2). By Prop. 1.3 and Th B, we shall identify $\varprojlim T_l(J_n^*)$ with the left $\mathscr{A}$-submodule $\mathfrak{X} \subset \mathscr{A}^{\oplus 2}$ given in Th B.

Our third main result describes the action of G_{Q^*} on $\mathfrak{X}$ in terms of two "transforms" ψ_x and ψ_y of ψ, as follows:

Theorem C. *For each $\rho \in G_{Q^*}$, its action on $\mathfrak{X}$ is obtained by the restriction to $\mathfrak{X}(\subset \mathscr{A}^{\oplus 2})$ of the left $\mathscr{A}$ semi-linear automorphism of $\mathscr{A}^{\oplus 2}$ defined by*

$$(\xi,\eta)\to(J_\rho(\xi),J_\rho(\eta))\begin{pmatrix}\psi_x(\rho) & 0\\ 0 & \psi_y(\rho)\end{pmatrix},$$

where $\psi_x(\rho)$ (resp. $\psi_y(\rho)$) is the unique element of $\mathscr{A}^\times$ satisfying

$$\psi_x(\rho)(\mathbf{x}-1)=(J_\rho(\mathbf{x})-1)\,\psi(\rho)$$

$$(resp.\ \ \psi_y(\rho)(\mathbf{y}-1)=(J_\rho(\mathbf{y})-1)\,\psi(\rho)),$$

$\psi(\rho)$ being as in Theorem A.

In fact, each of $\psi_x,\psi_y\colon G_{Q^*}\to\mathscr{A}^\times$ is also a continuous anti 1-cocycle, given explicitly as

$$\psi_x(\rho)=\pi\left(s\frac{x^{\chi(\rho)}-1}{x-1}\right)+(1-J_\rho(\mathbf{x}))\,\pi\left(\frac{\partial(s-t)}{\partial x}\right),$$

$$\psi_y(\rho)=\pi\left(t\frac{y^{\chi(\rho)}-1}{y-1}\right)+(1-J_\rho(\mathbf{y}))\,\pi\left(\frac{\partial(t-s)}{\partial y}\right).$$

(Cf. § 3 (B) for justification of the quotient symbols $(x^{\chi(\rho)}-1)/(x-1)^{-1}$, etc.) The uniqueness statement follows from:

Proposition 1.4. *None of the elements* $\mathbf{x}-1,\mathbf{y}-1,\mathbf{z}-1$ *of* $\mathscr{A}=\mathbf{Z}_l[[\mathfrak{G}]]$ *are right (or left) zero divisors of* $\mathscr{A}$.

These proofs will be given in § 3. When L^*/K^* is a Galois extension, ψ,ψ_x,ψ_y are anti-representations having the same kernel. This kernel is obviously contained in the kernel of the action of G_{Q^*} on $\mathfrak{X}$. Whether they coincide seems to be a question of a delicate nature. Comparison of these two kernels, from various aspects, will be given in § 5, together with some examples where they coincide.

Remark 1.5. In view of Proposition 1.4, we may identify $\mathfrak{X}$ with the left $\mathscr{A}$-ideal $\Lambda=\mathscr{A}(\mathbf{x}-1)\cap\mathscr{A}(\mathbf{y}-1)$, via $\mathfrak{X}\ni(\xi,\eta)\leftrightarrow\xi(\mathbf{x}-1)=-\eta(\mathbf{y}-1)\in\Lambda$. Then what Theorem C claims is that $\rho\in G_{Q^*}$ acts on Λ via $\Lambda\ni\lambda\to J_\rho(\lambda)\,\psi(\rho)\in\Lambda$. This description is simpler in form (so, we employed it in the Introduction); on the other hand, this presentation of $\mathfrak{N}^{\mathrm{ab}}$ as a left $\mathscr{A}$-ideal is specific for the 3-point ramification case. So, we preferred to formulate Theorems B, C in the above form here.

Finally, we shall present one direct application of Theorem C. Consider the action of $G_{\mathbf{Q}^*}$ on the group ${}_lJ_n^*$ of l-division points of the Jacobian J_n^* of X_n^* $(n\geqq 0)$. Since ${}_lJ_n^*\simeq\mathbf{F}_l^{2g_n}$, g_n being the genus of X_n^*, this action gives a linear representation of $G_{\mathbf{Q}^*}$ in $GL_{2g_n}(\mathbf{F}_l)$ (and, in fact, in $GSp_{2g_n}(\mathbf{F}_l)$) for each n. As the "prime-to-l" part of the order of the group $GSp_{2g_n}(\mathbf{F}_l)$ is unbounded (as $n\to\infty$), it is not *a priori* obvious whether there exists a *finite* Galois extension $\mathbf{Q}^{**}/\mathbf{Q}^*$ such that the action of $G_{\mathbf{Q}^{**}}$ on ${}_lJ_n^*$ is *unipotent for all* $n\geqq 0$. But Theorem C gives the following

Corollary. *Assume that L^*/K^* is a Galois extension. Then there exists a finite Galois extension $\mathbf{Q}^{**}/\mathbf{Q}^*$ such that the action of $G_{\mathbf{Q}^{**}}$ on ${}_lJ_n^*$ is unipotent for all*

$n \geqq 0$. *More precisely, let* $\mathfrak{G}_1$ *be the maximum open normal pro-l subgroup of* $\mathfrak{G}$, *put* $G = \mathfrak{G}/\mathfrak{G}_1$ *(a finite group), and let* α: $\mathscr{A} \to \mathbf{F}_l[G]$ *be the projection. Then it suffices to choose as* $\mathbf{Q}^{**}/\mathbf{Q}^*$ *the extension corresponding to the kernel of the composite anti-representation*

$$\alpha \circ \psi \colon G_{\mathbf{Q}^*} \to \mathscr{A}^\times \to \mathbf{F}_l[G]^\times.$$

The composite $s \circ \alpha \circ \psi \colon G_{\mathbf{Q}^*} \to \mathbf{F}_l^\times$ *of* $\alpha \circ \psi$ *with the augmentation homomorphism* s: $\mathbf{F}_l[G] \to \mathbf{F}_l$ *is the identity map.*

In particular, when L^*/K^* is a pro-l extension, $G_{\mathbf{Q}^*}$ itself acts unipotently on ${}_lJ_n^*$ for all $n \geqq 0$.

Proof. Let J be the kernel of α. Then J is an open two-sided ideal of $\mathscr{A}$ generated by l and I_1, where I_1 is the augmentation ideal of $\mathscr{A}_1 = \mathbf{Z}_l[\![\mathfrak{G}_1]\!]$. Since $\mathfrak{G}_1$ is a pro-l group, I_1 is topologically nilpotent. Since $g^{-1} I_1 g = I_1$ for any $g \in \mathfrak{G}$, J is also topologically nilpotent. Therefore, $1 + J$ is an open normal subgroup of $\mathscr{A}^\times$. Moreover, as J is topologically nilpotent and $l \in J$, $1 + J$ is a pro-l group. Denote by $\mathbf{Q}^{**}/\mathbf{Q}^*$ the finite Galois extension corresponding to the kernel of $\alpha \circ \psi$. Then $G_{\mathbf{Q}^{**}} = \psi^{-1}(1+J)$; hence $G_{\mathbf{Q}^{**}}$ is a pro-l group modulo $\operatorname{Ker}\psi$. Since $\operatorname{Ker}\psi = \operatorname{Ker}\psi_x = \operatorname{Ker}\psi_y$, Theorem C implies that $G_{\mathbf{Q}^{**}}$ acts on $\mathfrak{X}$, and hence also on the image of $\mathfrak{X}$ in ${}_lJ_n^*$ $(n \geqq 0)$, *through some pro-l group*. Therefore, $G_{\mathbf{Q}^{**}}$ acts unipotently on the image of $\mathfrak{X} \to {}_lJ_n^*$. But it acts trivially on the cokernel which is $G_{\mathbf{Q}^*}$-isomorphic to a subquotient of $\mathrm{Gal}(L/K)$. Therefore, $G_{\mathbf{Q}^{**}}$ acts unipotently on ${}_lJ_n^*$ for all $n \geqq 0$. Finally, since $\psi(\rho) \equiv \pi(s) \bmod \mathscr{A}(x-1)$, $\psi(\rho) - 1$ is contained in the augmentation ideal of $\mathscr{A}$: hence $s \circ \alpha \circ \psi = 1$. *q.e.d.*

Remark 1.6. (i) Even if we choose K_1 to be the field corresponding to $\mathfrak{G}_1$, the above Corollary does *not* mean that $\rho \in G_{\mathbf{Q}^*}$ acts unipotently on ${}_lJ_n^*$ for all n if so for $n = 1$ (or even if it acts trivially on ${}_lJ_1^*$). There are differences of delicate nature.

(ii) The basic congruences (§4) satisfied by ψ, ψ_x and ψ_y give further informations about the image of $\alpha \circ \psi$.

(iii) It may be an interesting problem to find out $\mathbf{Q}^{**}$ *explicitly* for the case of modular curves of level $2ml^n$ $(n \to \infty)$.

(D) Examples

Example 1. (The maximum pro-l tower.) Take L: the maximum pro-l extension of $K = \bar{\mathbf{Q}}(t)$ unramified outside $0, 1, \infty$. Then $M = L$, and $(\mathfrak{F} =)$ $\mathfrak{G} = \mathrm{Gal}(L/K)$ is a free pro-l group of rank 2, generated by such elements x, y, that x, y and $z = (xy)^{-1}$ each generates an inertia group above $0, 1, \infty$ respectively.

$$\mathscr{A} = \mathbf{Z}_l[\![\mathfrak{G}]\!] \cong \mathbf{Z}_l[\![u, v]\!]_{\mathrm{nc}}, \quad \text{by } x - 1 \leftrightarrow u, \ y - 1 \leftrightarrow v.$$

There is a good way to lower the field of constants of L to $\mathbf{Q}^* = \mathbf{Q}$, using the following "Belyi's normalization". For each $\rho \in G_{\mathbf{Q}}$ and its extension $\tilde{\rho} \in \mathrm{Gal}(L/\mathbf{Q}(t))$, one always has $\tilde{\rho} x \tilde{\rho}^{-1} \sim x^{\chi(\rho)}$, $\tilde{\rho} y \tilde{\rho}^{-1} \sim y^{\chi(\rho)}$, $\tilde{\rho} z \tilde{\rho}^{-1} \sim z^{\chi(\rho)}$

(Prop. 1.2). But there is a *unique* choice of $\tilde{\rho}$ such that $\tilde{\rho}\, y\, \tilde{\rho} \approx y^{\chi(\rho)}$ and $\tilde{\rho}\, z\, \tilde{\rho}^{-1} = z^{\chi(\rho)}$, where $\approx$ denotes conjugacy by some element of $[\mathfrak{G}, \mathfrak{G}]$ ([I] I § 4). Define

L^*: the set of elements of L invariant by this $\tilde{\rho}$ for all $\rho \in G_{\mathbf{Q}}$;
(a subfield such that $L^* \cdot \bar{\mathbf{Q}} = L$, $L^* \cap \bar{\mathbf{Q}} = \mathbf{Q}$).

The J_ρ-action of $G_{\mathbf{Q}}$ on $\mathscr{A}$ is a very large Galois representation unramified outside l. In this example, the J_ρ-action itself is already complicated, and its study should perhaps precede the study of the anti 1-cocycle ψ: $G_{\mathbf{Q}} \to \mathscr{A}^\times$. We note only that the abelianization of ψ; ψ^{ab}: $G_{\mathbf{Q}} \to \mathscr{A}^\times \to (\mathscr{A}^{\mathrm{ab}})^\times$ gives the 1-cocycle in the Fermat case (Example 2 below) whose restriction to $G_{\mathbf{Q}(\mu_{l^\infty})}$ is a non-trivial homomorphism [I]. Therefore, ψ cannot be a coboundary.

Since $\mathfrak{N} = \{1\}$, Theorems B, C are empty in this case.

Example 2. (The Fermat tower.) Take L: the maximum *abelian* pro-l extension of $K = \bar{\mathbf{Q}}(t)$ unramified outside $0, 1, \infty$; i.e., $L = K(t^{1/l^n}, (t-1)^{1/l^n}; n = 0, 1, 2, \ldots)$. Then $\mathfrak{G} = \mathrm{Gal}(L/K) \cong \mathbf{Z}_l \times \mathbf{Z}_l$ and $\mathscr{A} \cong \mathbf{Z}_l[[u, v]]$ are the *abelianizations* of the corresponding objects in Ex. 1. The subfield L^* over $\mathbf{Q}^* = \mathbf{Q}$ is obtained as the intersection of L with "L^* of Ex. 1". Then, $L^* \cdot \bar{\mathbf{Q}} = L$, and $L^* \cdot \mathbf{Q}(\mu_{l^\infty})$ is the standard model of L over $\mathbf{Q}(\mu_{l^\infty})$, i.e., the field generated over $\mathbf{Q}(\mu_{l^\infty})(t)$ by the l^n-th roots of t and $t-1$ for all $n \geqq 0$ (cf. [I] I § 4). The J_ρ-action of $G_{\mathbf{Q}}$ on $\mathscr{A}$ is:

$$1 + u \to (1+u)^{\chi(\rho)}, \qquad 1 + v \to (1+v)^{\chi(\rho)}.$$

M: the maximum pro-l extension of K unramified outside $0, 1, \infty$ (the field L in Ex. 1),

$$\begin{tikzcd}
1 \arrow[r] & \mathfrak{N} \arrow[r] \arrow[d, equal] & \mathfrak{F} \arrow[r] \arrow[d, equal] & \mathfrak{G} \arrow[r] \arrow[d, equal] & 1 \\
& \mathrm{Gal}(M/L) \arrow[d, equal] & \mathrm{Gal}(M/K) & \mathrm{Gal}(L/K) \arrow[d, equal] & \\
& {[\mathfrak{F}, \mathfrak{F}]} & \text{free pro-}l\text{, rank 2} & \mathfrak{F}^{\mathrm{ab}} &
\end{tikzcd}$$

$$\begin{aligned} \mathfrak{N}^{\mathrm{ab}} \simeq \mathfrak{T} &= \{(\xi, \eta) \in \mathscr{A}^{\oplus 2};\ \xi\, u + \eta\, v = 0\} \\ &= \mathscr{A} \cdot (-v, u) \qquad \text{(a free } \mathscr{A}\text{-module, rank 1).} \end{aligned}$$

This element $(-v, u) \in \mathfrak{T}$ corresponds to the element of $\mathfrak{N}^{\mathrm{ab}}$ represented by $[x, y] = x y x^{-1} y^{-1} \in \mathfrak{N} = [\mathfrak{F}, \mathfrak{F}]$. For each $\rho \in G_{\mathbf{Q}}$, define $F_\rho \in \mathscr{A}^\times$ by $\rho(-v, u) = F_\rho \cdot (-v, u)$. On the other hand,

$$\rho(-v, u) = (J_\rho(-v)\, \psi_x(\rho),\ J_\rho(u)\, \psi_y(\rho)) \qquad \text{(Th. C).}$$

Therefore, ψ, ψ_x and ψ_y for this case are given by

$$\psi(\rho) = \frac{u\, v}{J_\rho(u\, v)} F_\rho, \qquad \psi_x(\rho) = \frac{v}{J_\rho(v)} F_\rho, \qquad \psi_y(\rho) = \frac{u}{J_\rho(u)} F_\rho.$$

The power series F_p was studied in detail in [I] in connection with complex multiplications of Fermat curves and Jacobi sums. Further results on F_p will be given in [IKY] (cf. also [A]).

Example 3. (The modular tower.)[1] Regard $K=\bar{\mathbf{Q}}(t)$ as the field of modular functions of level 2 over $\bar{\mathbf{Q}}$, and t as a λ-function giving an isomorphism $\Gamma\backslash\mathfrak{H}\xrightarrow{\sim}\mathbf{P}^1\backslash\{0,1,\infty\}$, where Γ is the principal congruence subgroup of level 2 in $PSL_2(\mathbf{Z})$ and $\mathfrak{H}$ is the complex upper half plane. Fix a positive integer m with $(m,l)=1$ and put

$$L=\bigcup_n \begin{pmatrix}\text{the field of modular functions}\\ \text{of level } 2m\,l^n \text{ over } \bar{\mathbf{Q}}\end{pmatrix},$$

$$\mathfrak{G}=\mathrm{Gal}(L/K)=\varprojlim_n \{g\in SL_2(\mathbf{Z}/2m\,l^n);\ g\equiv I\ (\mathrm{mod}\ 2)\}/\pm I.$$

(For example, $\mathfrak{G}\simeq PSL_2(\mathbf{Z}_l)$ if $m=1$ and $l\neq 2$.) As for L^* and $\mathbf{Q}^*$, there are various choices. We only note here that the standard model of L over the cyclotomic field $\mathbf{Q}(\mu_{2ml^\infty})$ can be lowered, in a "standard way", to a model L^* over

$$\begin{aligned}\mathbf{Q}^* &=\mathbf{Q}(\mu_{2m},\sqrt{\pm l}) \quad \text{with } \pm l\equiv 1\ (\mathrm{mod}\ 4)\ \ldots\ l\neq 2,\\ &=\mathbf{Q}(\mu_{2m},\sqrt{-1},\sqrt{2}) \qquad\qquad\qquad \ldots\ l=2,\end{aligned}$$

which is a *Galois* extension over $K^*=\mathbf{Q}^*(t)$. So, for this choice of $\mathbf{Q}^*$ and L^*, the J_p-action of $G_{\mathbf{Q}^*}$ on $\mathscr{A}=\mathbf{Z}_l[[\mathfrak{G}]]$ is trivial. We may assume that the projections of x, y, z on $\mathfrak{G}$ correspond to

$$\begin{pmatrix}1 & 2\\ 0 & 1\end{pmatrix},\quad \begin{pmatrix}1 & 0\\ -2 & 1\end{pmatrix},\quad \begin{pmatrix}1 & -2\\ 2 & -3\end{pmatrix},$$

respectively. The left $\mathscr{A}$-module

$$\mathfrak{N}^{\mathrm{ab}}\simeq\mathfrak{T}=\{(\xi,\eta)\in\mathscr{A}^{\oplus 2};\ \xi(\mathbf{x}-1)+\eta(\mathbf{y}-1)=0\}$$

in this case is neither free nor cyclic. (For example, if $m=1$ and $l\neq 3$, we can prove, by using supersingular Frobeniuses, that the minimum number of generators of $\mathfrak{T}$ (as $\mathscr{A}$-module) is 2.)

The kernel of the anti-representation ψ: $G_{\mathbf{Q}^*}\to\mathscr{A}^\times$ coincides with that of the action of $G_{\mathbf{Q}^*}$ on $\mathfrak{T}$ (§ 5 (D)). This anti-representation ψ in the modular case has an additional property that an element of $\mathscr{A}$ of the form

$$\psi(\rho)+\chi_l(\rho)\,\psi(\rho)^{-1} \qquad (\rho\in G_{\mathbf{Q}^*},\ \chi_l\colon G_{\mathbf{Q}^*}\to\mathbf{Z}_l^\times\colon \text{the } l\text{-cyclotomic character})$$

commutes with all elements of $\psi(G_{\mathbf{Q}^*})$ (the congruence relation for Hecke operators). There are many interesting problems related to specializations of ψ. For example, what is the image of $\psi\otimes\mathbf{F}_l$: $G_{\mathbf{Q}^*}\to\mathbf{F}_l[[\mathfrak{G}]]^\times$? In the Fermat case, this question is closely related to the Vandiver conjecture [IKY]. Another basic specialization gives a transparent way to connect modular forms of

[1] Details for this case will be given in a separate article

weight 2 (level $2ml^{\infty}$) with those of weight $d+2$ (level $2m$). Roughly speaking, the symmetric tensor representation of the "$PSL_2(\mathbf{Z}_l)$-part" of $\mathfrak{G}$, of an even degree d, induces an algebra representation $\mathscr{A}\to M_{d+1}(\mathbf{Z}_l[PSL_2(\mathbf{Z}/m)])$; hence the composite anti-representations

$$\psi^{(d)}, \psi_x^{(d)}, \psi_y^{(d)}\colon\ G_{\mathbf{Q}^*}\to\mathscr{A}^{\times}\to GL_{d+1}(\mathbf{Z}_l[PSL_2(\mathbf{Z}/m)]).$$

These specializations of ψ, ψ_x, ψ_y are *not* conjugate to each other, and $\psi_x^{(d)}\oplus\psi_y^{(d)}\ominus\psi^{(d)}$ ($\ominus$ in a certain sense) is closely connected with the Galois representations studied by Shimura [Sh], Deligne [De], and Ohta [O]. A recent work of Hida [H] should also be closely related, because our ψ is universal for the representation of $G_{\mathbf{Q}^*}$ in $T_l(\mathrm{Jac}\,X_n^*)$ of the modular curves X_n^* of level $2ml^n$ over $\mathbf{Q}^*$, while Hida's representation in $GL_2(\mathbf{Z}_l[\![t]\!])$ describes its "l-ordinary portion".

There are also other interesting towers with $\mathfrak{G}=SL_2(\mathbf{Z}_l)$ (instead of mod $\pm I$), or

$$\mathfrak{G}=\begin{pmatrix}1 & \mathbf{Z}_l & \mathbf{Z}_l\\ 0 & 1 & \mathbf{Z}_l\\ 0 & 0 & 1\end{pmatrix}.$$

2. Free differential calculus on free almost pro-l groups

(A) Free almost pro-l groups. Let F be an abstract free group of rank r generated by $x_1,\dots,x_r$ ($r\geqq 1$), and $F_1\subset F$ be a normal subgroup of finite index. Then F_1 is again free, with rank r_1, where $r_1-1=(r-1)(F:F_1)$. Let N run over all normal subgroups of F contained in F_1 such that F_1/N is a finite l-group, and form the projective limit $\mathfrak{F}=\varprojlim(F/N)$. In other words, $\mathfrak{F}$ is the completion of F with respect to the pro-l topology of F_1. The profinite group $\mathfrak{F}$ constructed this way will be called a *free almost pro-l group of rank r*. It contains an open normal subgroup $\mathfrak{F}_1=\varprojlim(F_1/N)$ which is a free pro-l group of the "correct rank" r_1, i.e., $r_1-1=(\mathfrak{F}:\mathfrak{F}_1)(r-1)$. Conversely, if a profinite group $\mathfrak{F}$ generated by r elements contains an open normal subgroup $\mathfrak{F}_1$ which is a free pro-l group with the correct rank, then $\mathfrak{F}$ is a free almost pro-l group of rank r with respect to any set of r generators $\bar{x}_1,\dots,\bar{x}_r$ of $\mathfrak{F}$. Namely, in this case, the homomorphism from the abstract free group of rank r, $F=\langle x_1,\dots,x_r\rangle$, into $\mathfrak{F}$ defined by $x_j\to\bar{x}_j$ ($1\leqq j\leqq r$) is injective, and $\mathfrak{F}$ is the completion of F w.r.t. the pro-l topology of the preimage F_1 of $\mathfrak{F}_1$. This follows immediately from the (well-known) fact that a free pro-l group of finite rank cannot be isomorphic with its proper quotient. (This last statement is obvious, because the proper quotient group cannot have as many open normal subgroups of a given index l^n as the original group for all n.) It is also easy to see that if a free almost pro-l group of finite rank is pro-l, then it is free pro-l, and that any open subgroup of a free almost pro-l group of finite rank is again a free almost pro-l group with the correct rank. We shall identify $x_j\in F$ with its image $\bar{x}_j\in\mathfrak{F}$ ($1\leqq j\leqq r$).

(B) **Theorem 2.1.** *Let $\mathfrak{F}$ be a free almost pro-l group of rank r generated by $x_1, \ldots, x_r$, $\mathscr{B} = \mathbf{Z}_l[[\mathfrak{F}]]$ be its completed group algebra over $\mathbf{Z}_l$, and s: $\mathscr{B} \to \mathbf{Z}_l$ be the augmentation homomorphism. Then every element θ of $\mathscr{B}$ can be expressed uniquely in the form*

$$\theta = s(\theta) \cdot 1 + \sum_{j=1}^{r} \theta_j (x_j - 1) \qquad (\theta_1, \ldots, \theta_r \in \mathscr{B}), \tag{\#}$$

where $1 = 1_{\mathfrak{F}}$ is the identity element of $\mathfrak{F}$. Moreover, for each j, $\theta \to \theta_j$ gives a continuous $\mathbf{Z}_l$-linear map of $\mathscr{B}$ onto itself.

Definition. $\dfrac{\partial \theta}{\partial x_j} = \theta_j \quad (1 \leqq j \leqq r)$.

Remark. When $r = 1$, $\mathfrak{F}$ *is of the form* $(\mathbf{Z}/m) \times \mathbf{Z}_l$, with $(m, l) = 1$. Hence

$$\mathscr{B} \simeq (\mathbf{Z}_l[t]/(t^m - 1))[[u]],$$

and the augmentation homomorphism s: $\mathscr{B} \to \mathbf{Z}_l$ is induced by the substitutions $u \to 0$, $t \to 1$. In this case, the above theorem is reduced to the elementary fact that the ideal of $\mathbf{Z}_l[t]$ generated by $(t^m - 1)(t-1)^{-1}$ and $t - 1$ is (1).

Before proving Theorem 2.1, we give a list of basic rules for free differential calculus $\partial/\partial x_j$, each of which is (as in the classical abstract case) an immediate consequence of the definition of $\partial/\partial x_j$.

0) $\dfrac{\partial}{\partial x_j}$: $\mathscr{B} \to \mathscr{B}$ is continuous and $\mathbf{Z}_l$-linear $(1 \leqq j \leqq r)$;

i) $\dfrac{\partial x_i}{\partial x_j} = \delta_{ij}$ (the Kronecker symbol) $(1 \leqq i, j \leqq r)$;

ii) $\dfrac{\partial(\alpha\beta)}{\partial x_j} = \dfrac{\partial \alpha}{\partial x_j} \cdot s(\beta) + \alpha \dfrac{\partial \beta}{\partial x_j} \quad (\alpha, \beta \in \mathscr{B})$;

iii) $\dfrac{\partial(f^{-1})}{\partial x_j} = -f^{-1} \dfrac{\partial f}{\partial x_j} \quad (f \in \mathfrak{F})$;

iv) Let $f \in \mathfrak{F}$ and $\alpha \in \hat{\mathbf{Z}}$. Then

$$\frac{\partial(f^\alpha)}{\partial x_j} = \beta \frac{\partial f}{\partial x_j},$$

where β is any element of $\mathscr{B}$ such that $\beta(f-1) = f^\alpha - 1$ (it exists; cf. § 3 (B)).

v) If σ is any automorphism of $\mathfrak{F}$, extended to that of $\mathscr{B}$ in the obvious way, and if $\partial/\partial(\sigma x_j)$ is the free differentiation with respect to $\{\sigma x_j\}$, then

$$\frac{\partial(\sigma\beta)}{\partial(\sigma x_j)} = \sigma \frac{\partial \beta}{\partial x_j} \qquad (\beta \in \mathscr{B});$$

vi) if $\mathfrak{F}_1$ is any open subgroup of $\mathfrak{F}$, with free (almost pro-l) generators $y_1, \ldots, y_{r_1}$, then

$$\frac{\partial\theta}{\partial x_j}=\sum_{i=1}^{r_1}\frac{\partial\theta}{\partial y_i}\frac{\partial y_i}{\partial x_j}\qquad(\theta\in\mathbf{Z}_l[\![\mathfrak{F}_1]\!]),$$

where we regard $\mathbf{Z}_l[\![\mathfrak{F}_1]\!]$ as embedded in $\mathbf{Z}_l[\![\mathfrak{F}]\!]$.

(C) Proof of Theorem 2.1. This will be reduced to the two known cases, the abstract case and the pro-l case. Let our group $\mathfrak{F}$ be constructed as in (A), from an abstract free group F on $x_1,\dots,x_r$ and its normal subgroup F_1 of finite index, as $\mathfrak{F}=\varprojlim(F/N)$, where N runs over all normal subgroups of F contained in F_1 such that $(F_1:N)$ is a power of l. Let $F=\coprod_\lambda F_1c_\lambda$ be the left F_1-coset decomposition of F, and $\mathbf{Z}[F]$ (resp. $\mathbf{Z}[F_1]$) be the group ring of F (resp. F_1) over $\mathbf{Z}$ (formal *finite* $\mathbf{Z}$-linear combinations of elements of F (resp. F_1)). Then $\mathbf{Z}[F]=\bigoplus_\lambda\mathbf{Z}[F_1]c_\lambda$, as $\mathbf{Z}$-modules. By a theorem of Fox [F] (cf. also [B], [MKS]), every element of $\mathbf{Z}[F]$ can be expressed uniquely as

$$\theta=s(\theta)\cdot 1+\sum_{j=1}^{r}\theta_j(x_j-1)\qquad(\theta_1,\dots,\theta_r\in\mathbf{Z}[F]),$$

where s: $\mathbf{Z}[F]\to\mathbf{Z}$ is the augmentation homomorphism (sum of coefficients). Write $\theta_j=\frac{\partial\theta}{\partial x_j}$ (classical free differential calculus). We shall show that each $\frac{\partial}{\partial x_j}$: $\mathbf{Z}[F]\to\mathbf{Z}[F]$ $(1\leqq j\leqq r)$ is *continuous* w.r.t. the topology of $\mathbf{Z}[F]$ which is induced from our topology of $\mathscr{B}=\mathbf{Z}_l[\![\mathfrak{F}]\!]$ via the canonical injection $\mathbf{Z}[F]\to\mathscr{B}$.

For this purpose, take any $\theta=\sum_\lambda\theta_\lambda c_\lambda\in\mathbf{Z}[F]$, with $\theta_\lambda\in\mathbf{Z}[F_1]$. Then θ is "small" if its image in $(\mathbf{Z}/l^m)[F/N]$ vanishes for some "large" m and "small" N. Since N is always contained in F_1, θ is small if and only if each θ_λ is. Now,

$$\frac{\partial\theta}{\partial x_j}=\sum_\lambda\left(\frac{\partial\theta_\lambda}{\partial x_j}+\theta_\lambda\cdot\frac{\partial c_\lambda}{\partial x_j}\right)=\sum_\lambda\left(\sum_{i=1}^{r_1}\frac{\partial\theta_\lambda}{\partial y_i}\cdot\frac{\partial y_i}{\partial x_j}\right)+\sum_\lambda\theta_\lambda\frac{\partial c_\lambda}{\partial x_j},$$

where $y_1,\dots,y_{r_1}$ is a free generator of F_1 (free differential calculus in the abstract case). But $\frac{\partial}{\partial y_i}$: $\mathbf{Z}[F_1]\to\mathbf{Z}[F_1]$ $(1\leqq i\leqq r_1)$ is continuous w.r.t. the topology induced from that of $\mathbf{Z}_l[\![\mathfrak{F}_1]\!]$, because it is a restriction to $\mathbf{Z}[F_1]$ of a continuous free differentiation of $\mathbf{Z}_l[\![\mathfrak{F}_1]\!]\simeq\mathbf{Z}_l[\![u_1,\dots,u_{r_1}]\!]_{\mathrm{nc}}$ (§1 (A)). Therefore, when θ is small, θ_λ and $\frac{\partial\theta_\lambda}{\partial y_i}$ are small for all λ and i. Hence each $\frac{\partial\theta}{\partial x_j}$ is also small. This proves that $\frac{\partial}{\partial x_j}$: $\mathbf{Z}[F]\to\mathbf{Z}[F]$ is continuous. Therefore, we can extend $\frac{\partial}{\partial x_j}$ to a continuous ($\mathbf{Z}_l$-linear) mapping $\frac{\partial}{\partial x_j}$: $\mathscr{B}\to\mathscr{B}$. By continuity, we obtain the formula

$$\theta=s(\theta)\cdot 1+\sum_{j=1}^{r}\frac{\partial\theta}{\partial x_j}(x_j-1)$$

for any $\theta \in \mathscr{B}$. The above rules i)–vi) also follow from the classical case by passage to the limit. The uniqueness of θ_j in Th. 2.1 follows directly by applying $\frac{\partial}{\partial x_j}$ to both sides of the formula (#). The surjectivity of $\frac{\partial}{\partial x_j}$: $\mathscr{B} \to \mathscr{B}$ is obvious. *q.e.d.*

(D) As before, let $\mathfrak{F}$ be a free almost pro-l group of rank r $(<\infty)$ generated by $x_1, \ldots, x_r$, and $\mathfrak{N}$ be any closed normal pro-l subgroup of $\mathfrak{F}$. Put $\mathfrak{G} = \mathfrak{F}/\mathfrak{N}$, $\mathscr{B} = \mathbf{Z}_l[[\mathfrak{F}]]$, $\mathscr{A} = \mathbf{Z}_l[[\mathfrak{G}]]$, and let π: $\mathscr{B} \to \mathscr{A}$ denote the projection (which is obvious continuous).

Then the action $n \to f n f^{-1}$ $(n \in \mathfrak{N}, f \in \mathfrak{F})$ of $\mathfrak{F}$ on $\mathfrak{N}$ induces an action of $\mathfrak{G}$ on $\mathfrak{N}^{\mathrm{ab}} = \mathfrak{N}/[\mathfrak{N}, \mathfrak{N}]$, which gives $\mathfrak{N}^{\mathrm{ab}}$ a structure of a left $\mathscr{A}$-module. The following theorem is an almost pro-l version of a theorem of Blanchfield and of Lyndon [F] in abstract free differential calculus. (The Blanchfield theorem corresponds to the injectivity, and the Lyndon's to the surjectivity of (*).)

Theorem 2.2[2]. *The mapping* $n \to \left(\pi\left(\frac{\partial n}{\partial x_1}\right), \ldots, \pi\left(\frac{\partial n}{\partial x_r}\right)\right)$ *of* $\mathfrak{N}$ *into* $\mathscr{A}^{\oplus r}$ *induces an isomorphism of left* $\mathscr{A}$*-modules:*

$$\mathfrak{N}^{\mathrm{ab}} \xrightarrow{\sim} \mathfrak{X} = \left\{(\xi_1, \ldots, \xi_r) \in \mathscr{A}^{\oplus r};\ \sum_{j=1}^{r} \xi_j(\mathbf{x}_j - 1) = 0\right\}. \qquad (*)$$

This isomorphism is also bicontinuous.

Proof. Put $K = \operatorname{Ker} \pi$, the kernel of π. Then K is a closed two-sided ideal of $\mathscr{B} = \mathbf{Z}_l[[\mathfrak{F}]]$ contained in the augmentation ideal I, and $\mathscr{A} \simeq \mathscr{B}/K$. Denote by $K.I$ the closed two-sided ideal of $\mathscr{B}$ generated by elements of the form $k.i$ $(k \in K, i \in I)$. Since K is a left $\mathscr{B}$-module, K/K^2 is naturally a left $\mathscr{A}$-module. Since $K^2 \subset K.I$, $K/K.I$ can also be regarded as a left $\mathscr{A}$-module. The proof of Th. 2.2 consists in establishing two $\mathscr{A}$-isomorphisms $\mathfrak{N}^{\mathrm{ab}} \xrightarrow{\sim} K/K.I$ and $K/K.I \xrightarrow{\sim} \mathfrak{X}$ whose composite is to give the desired $\mathscr{A}$-isomorphism (*).

(I) That $K/K.I \xrightarrow{\sim} \mathfrak{X}$. Consider a continuous additive homomorphism

$$K \ni k \to \left(\pi\left(\frac{\partial k}{\partial x_1}\right), \ldots, \pi\left(\frac{\partial k}{\partial x_r}\right)\right) \in \mathscr{A}^{\oplus r}. \qquad (\#)$$

We shall check that this induces an $\mathscr{A}$-isomorphism $K/K.I \xrightarrow{\sim} \mathfrak{X}$. First, take $k \in K$ and $i \in I$. Then, since $s(i) = \pi(k) = 0$,

$$\frac{\partial(k.i)}{\partial x_j} = \frac{\partial k}{\partial x_j} s(i) + k \frac{\partial i}{\partial x_j} \xrightarrow{\pi} 0;$$

hence (#) factors through $K/K.I$. Moreover, if $b \in \mathscr{B}$ and $a = \pi(b) \in \mathscr{A}$, then

$$\frac{\partial(b\,k)}{\partial x_j} = \frac{\partial b}{\partial x_j} s(k) + b \frac{\partial k}{\partial x_j} = b \frac{\partial k}{\partial x_j} \xrightarrow{\pi} a \cdot \pi\left(\frac{\partial k}{\partial x_j}\right);$$

[2] The author wishes to thank Takayuki Oda and Hans Sah for valuable discussions related to this theorem

hence (#) induces an $\mathscr{A}$-homomorphism $K/K.I\to\mathscr{A}^{\oplus r}$. Since $k=\sum_j\left(\frac{\partial k}{\partial x_j}\right)(x_j-1)$ and $\pi(k)=0$, the image is obviously contained in $\mathfrak{T}$. Therefore, (#) induces an $\mathscr{A}$-homomorphism

$$K/K.I\to\mathfrak{T}. \qquad (\#\#)$$

Injectivity of (##). If $k\in K$ is in the kernel of (#), then $\frac{\partial k}{\partial x_j}\in K$ for all j; hence $k=\sum_j\left(\frac{\partial k}{\partial x_j}\right)(x_j-1)\in K.I$.

Surjectivity of (##). Take any $(\xi_j)\in\mathfrak{T}$, and $\tilde{\xi}_j\in\mathscr{B}$ for each j with $\pi(\tilde{\xi}_j)=\xi_j$. Put $k=\sum_j\tilde{\xi}_j(x_j-1)$. Then $\pi(k)=0$; hence $k\in K$. On the other hand, $\tilde{\xi}_j=\frac{\partial k}{\partial x_j}$; hence $\xi_j=\pi\left(\frac{\partial k}{\partial x_j}\right)$; hence (#) maps k to (ξ_j).

Therefore, (##) is bijective.

(II) That $\mathfrak{N}^{\mathrm{ab}}\xrightarrow{\sim}K/K.I$. This is induced from a continuous mapping $n\to n-1\pmod{K.I}$ of $\mathfrak{N}\to K/K.I$. Since

$$nn'-1=(n-1)+(n'-1)+(n-1)(n'-1)\equiv(n-1)+(n'-1)\mod K.I$$

for any $n,n'\in\mathfrak{N}$, the above mapping $\mathfrak{N}\to K/K.I$ is a group homomorphism. Since $K/K.I$ is abelian, this induces an additive group homomorphism

$$\mathfrak{N}^{\mathrm{ab}}\to K/K.I. \qquad (!)$$

Moreover, if $n\in\mathfrak{N}$, $f\in\mathfrak{F}$, then $fnf^{-1}-1=f(n-1)+f(n-1)(f^{-1}-1)\equiv f(n-1)\mod K.I$; hence (!) is an $\mathscr{A}$-homomorphism.

Surjectivity of (!). It is clear that $K=\operatorname{Ker}\pi$ is generated, as an additive topological group, by elements of the form $(n-1)f$ $(n\in\mathfrak{N},\ f\in\mathfrak{F})$. (Note that $f(n-1)=(fnf^{-1}-1)f$.) But since $(n-1)f=(n-1)+(n-1)(f-1)\equiv(n-1)\mod K.I$, the image of (!) is dense. By compactness of $\mathfrak{N}^{\mathrm{ab}}$, (!) must be surjective.

Injectivity of (!). Let $I_{\mathfrak{N}}$ denote the augmentation ideal of $\mathbf{Z}_l[\![\mathfrak{N}]\!]$. Then $K=I_{\mathfrak{N}}\cdot\mathscr{B}$ (K being generated by $(n-1)f$; $n\in\mathfrak{N}$, $f\in\mathfrak{F}$). Therefore, $K.I=I_{\mathfrak{N}}\cdot I$. Now let $n\in\mathfrak{N}$ be such that $n-1\in K.I$. Then $n-1\in I_{\mathfrak{N}}\cdot I$. Let U be any open normal pro-l subgroup of $\mathfrak{F}$, put $\mathfrak{N}^*=\mathfrak{N}\cdot U$, and let $I_{\mathfrak{N}^*}$ be the augmentation ideal of $\mathbf{Z}_l[\![\mathfrak{N}^*]\!]$. Then $n-1\in I_{\mathfrak{N}}\cdot I\subset I_{\mathfrak{N}^*}\cdot I$. Let $\mathfrak{F}=\coprod_{\lambda=1}^{m}\mathfrak{N}^*c_\lambda$ $(c_1=1,\ m=(\mathfrak{F}:\mathfrak{N}^*))$ be a left $\mathfrak{N}^*$-coset decomposition of $\mathfrak{F}$. Then $\mathscr{B}=\bigoplus_\lambda\mathbf{Z}_l[\![\mathfrak{N}^*]\!]\,c_\lambda$ as modules; hence

$$I=I_{\mathfrak{N}^*}\oplus\bigoplus_{\lambda\neq1}\mathbf{Z}_l[\![\mathfrak{N}^*]\!]\cdot(c_\lambda-1).$$

Therefore,

$$n-1\in I_{\mathfrak{N}^*}\cdot I=(I_{\mathfrak{N}^*})^2\oplus\bigoplus_{\lambda\neq1}I_{\mathfrak{N}^*}(c_\lambda-1).$$

But since $n-1\in\mathbf{Z}_l[\![\mathfrak{N}^*]\!]$, it must belong to $(I_{\mathfrak{N}^*})^2$. But since $\mathfrak{N}^*$ is an open pro-l subgroup of $\mathfrak{F}$, $\mathfrak{N}^*$ must be a *free* pro-l group of finite rank. Therefore, by a well-known fact about the completed group algebra of a free pro-l group of finite rank [S], we conclude from $n-1\in(I_{\mathfrak{N}^*})^2$ that $n\in[\mathfrak{N}^*, \mathfrak{N}^*]$.

Finally, to conclude from this that $n\in[\mathfrak{N}, \mathfrak{N}]$, it is enough to show that $f(n)=1$ for any homomorphism f: $\mathfrak{N}\to A$ into a finite abelian (discrete) group A. Since f has an open kernel, there exists an open normal pro-l subgroup $U\subset\mathfrak{F}$ such that $f=1$ on $\mathfrak{N}\cap U$. But then, f extends to $\mathfrak{N}^*=\mathfrak{N}\cdot U\to A$. Since $n\in[\mathfrak{N}^*, \mathfrak{N}^*]$, we obtain $f(n)=1$. This proves that $n\in[\mathfrak{N}, \mathfrak{N}]$; and hence the injectivity of (!).

Since $\dfrac{\partial(n-1)}{\partial x_j}=\dfrac{\partial n}{\partial x_j}$ $(n\in\mathfrak{N})$, the composite of the above two $\mathscr{A}$-isomorphisms gives the $\mathscr{A}$-isomorphism of Theorem 2.2. Since $(*)$ is continuous (because the free differentiations are so) and $\mathfrak{N}^{\mathrm{ab}}$ is compact, $(*)$ is bicontinuous. *q.e.d.*

§ 3. Proofs for § 1

(A) On the group $\mathfrak{F}$; proof of Theorem B. Let $\mathfrak{H}$ be the complex upper half plane, and Γ be the principal congruence subgroup of level 2 in $PSL_2(\mathbf{Z})$ acting on $\mathfrak{H}$ in the usual manner;

$$\tau\to\gamma\tau=(a\tau+b)(c\tau+d)^{-1};\qquad \gamma=\pm\begin{pmatrix}a&b\\c&d\end{pmatrix}\in\Gamma,\ \tau\in\mathfrak{H}.$$

Then Γ acts freely on $\mathfrak{H}$ and, as is well-known, $\Gamma\backslash\mathfrak{H}\cong\mathbf{P}^1_{\mathbf{C}}\backslash\{0,1,\infty\}$ as Riemann surface; hence $\Gamma\cong\pi_1(\mathbf{P}^1_{\mathbf{C}}\backslash\{0,1,\infty\})$. The fuchsian group Γ has 3 inequivalent cusps, represented by $\tau=i\infty, 0$ and 1, and their stabilizers in Γ are free cyclic groups generated by

$$x=\begin{pmatrix}1&2\\0&1\end{pmatrix},\quad y=\begin{pmatrix}1&0\\-2&1\end{pmatrix}\quad\text{and}\quad z=(xy)^{-1}=\begin{pmatrix}1&-2\\2&-3\end{pmatrix},$$

respectively. As is well-known, Γ is a free group of rank 2 generated by x, y. There are 6 distinct isomorphisms λ: $\Gamma\backslash\mathfrak{H}\xrightarrow{\sim}\mathbf{P}^1_{\mathbf{C}}\backslash\{0,1,\infty\}$ (the "λ-functions"), depending on how we associate 3 cusps to 3 missing points $\{0,1,\infty\}$ of $\mathbf{P}^1_{\mathbf{C}}\backslash\{0,1,\infty\}$. To fix our notation, we shall normalize λ by the condition:

$$\lambda(i\infty)=0,\qquad \lambda(0)=1,\qquad \lambda(1)=\infty. \tag{$*$}$$

For each subgroup $\Gamma'\subset\Gamma$ with finite index, denote by $K_C(\Gamma')$ the field of modular functions w.r.t. Γ'. In particular, $K_C(\Gamma)=C(\lambda)$. Consider its subfield $K(\Gamma)=\bar{\mathbf{Q}}(\lambda)$. Then, as is well-known and easy to prove, $K_C(\Gamma')$ for each Γ' contains a unique finite extension $K(\Gamma')/K(\Gamma)$ such that $K(\Gamma')\cdot C=K_C(\Gamma')$. Now let Γ' run over all subgroups of Γ with finite indices, and put $\mathfrak{M}=\bigcup K(\Gamma')$. Then $\mathfrak{M}$ is the maximum Galois extension of $K(\Gamma)=\bar{\mathbf{Q}}(\lambda)$ unramified outside $\lambda=0,1,\infty$. The group Γ acts on $\mathfrak{M}$ as $f(\tau)\to f(\gamma^{-1}\tau)$ $(\gamma\in\Gamma,\ f\in\mathfrak{M})$, and the injection $\Gamma\hookrightarrow\mathrm{Gal}(\mathfrak{M}/K(\Gamma))$ defined by this action gives the profinite completion of Γ. (In other words, Galois theory holds between subgroups of Γ with finite indices and finite subextensions of $\mathfrak{M}/K(\Gamma)$, under the correspondence $\Gamma' \leftrightarrow K(\Gamma')$.)

If we fix a normal subgroup $\Gamma_1 \subset \Gamma$ of finite index and let Γ' run over only those normal subgroups of Γ contained in Γ_1 such that Γ_1/Γ' is an l-group, then $\mathfrak{M}^{(\Gamma_1)} = \bigcup K(\Gamma')$ is the maximum pro-l extension of $K(\Gamma_1)$ unramified outside $0, 1, \infty$. In this case, $\mathrm{Gal}(\mathfrak{M}^{(\Gamma_1)}/\mathrm{K}(\Gamma))$ is the completion of Γ w.r.t. the pro-l topology of Γ_1 and hence is a free almost pro-l group of rank 2 generated by x, y. Note that x, y, z can be regarded as generators of the inertia group of the place of $\mathfrak{M}$ (or $\mathfrak{M}^{(\Gamma_1)}$) above $\lambda = 0, 1, \infty$, determined by the cusps $\tau = i\infty, 0, 1$, respectively.

Now let $K = \bar{\mathbf{Q}}(t) \subset K_1 \subset L \subset M$ be as in § 1 (B), and fix an embedding $\bar{\mathbf{Q}} \hookrightarrow C$. Then K can be identified with $K(\Gamma)$ via $t \leftrightarrow \lambda$, and this identification isomorphism $K \xrightarrow{\sim} K(\Gamma)$ extends to an isomorphism $K_1 \xrightarrow{\sim} K(\Gamma_1)$ (for some Γ_1), and further to $M \xrightarrow{\sim} \mathfrak{M}^{(\Gamma_1)}$. Therefore, $\mathfrak{F} = \mathrm{Gal}(M/K)$ is isomorphic to the completion of Γ w.r.t. the pro-l topology of Γ_1. In particular, $\mathfrak{F}$ is a free almost pro-l group of rank 2 generated by x, y, and x, y and $z = (xy)^{-1}$ each generates some inertia group above $0, 1, \infty$, respectively. Therefore, Prop. 1.1 and Theorem B (§ 1) are immediate corollaries of Theorem 2.1 and Theorem 2.2, respectively.

(B) Some lemmas. For the proof of Theorems A, C, we shall need the following three lemmas (lemma 3.1–3.3). Their variations (lemma 3.1′, 3.2′) will also be used later.

Lemma 3.1. *Let $\mathfrak{G}$ be a profinite group, l be a prime, and g be an element of $\mathfrak{G}$ whose order is divisible by l^∞,* i.e., *the l-component of the order of g in the finite factor groups of $\mathfrak{G}$ is unbounded. Then $g-1$ is not a right (or left) zero-divisor of $\mathbf{Z}_l[\![\mathfrak{G}]\!]$.*

Proof. Suppose $\alpha(g-1) = 0$, with $\alpha \in \mathbf{Z}_l[\![\mathfrak{G}]\!]$. Let $\mathfrak{G} = \varprojlim G_\lambda$, with each G_λ finite, and g_λ (resp. α_λ) be the projection of g (resp. α) on G_λ (resp. $\mathbf{Z}_l[G_\lambda]$). Denote by D_λ the cyclic subgroup of G_λ generated by g_λ, and by $d_\lambda = |D_\lambda|$ its cardinality, i.e., the order of g_λ in G_λ. Now $\alpha_\lambda(g_\lambda - 1) = 0$ implies that α_λ is divisible by $\beta_\lambda = \sum_{\sigma \in D_\lambda} \sigma$ from the right. But if $\lambda > \mu$, $G_\lambda \to G_\mu$, then β_λ projects to $(d_\mu^{-1} d_\lambda)\beta_\mu$. Fix μ and let $\lambda \to \infty$. Then by our assumption on g, we have $d_\mu^{-1} d_\lambda \to 0$ (l-adically). Therefore, α_μ, which is divisible by $(d_\mu^{-1} d_\lambda)\beta_\mu$ from the right for all λ, must vanish for any μ. Therefore, $\alpha = 0$. *q.e.d.*

Proposition 1.4 is a special case where $\mathfrak{G} = \mathrm{Gal}(L/K)$ and $g = \mathbf{x}, \mathbf{y}$ or $\mathbf{z}$. (Their orders are divisible by l^∞; § 1 (B).)

Using multiples of $\sum_{\sigma \in G_\lambda} \sigma$ instead of β_λ, we obtain, exactly in the same manner, the following similar assertion.

Lemma 3.1′. *Let $\mathfrak{G}$ be a profinite group whose order is divisible by l^∞,* i.e., *the l-component of the order of finite factor groups of $\mathfrak{G}$ is unbounded. Let I be the augmentation ideal of $\mathbf{Z}_l[\![\mathfrak{G}]\!]$, and suppose that $\alpha \in \mathbf{Z}_l[\![\mathfrak{G}]\!]$ satisfies $\alpha \cdot I = 0$ (or $I \cdot \alpha = 0$). Then $\alpha = 0$.*

Now, in general, if $\mathfrak{G}$ is a profinite group, $g\in\mathfrak{G}$, and $\alpha\in\hat{\mathbf{Z}}$, then $g^\alpha-1$ is always divisible by $g-1$ in $\mathbf{Z}_l[[\mathfrak{G}]]$ from either side, as can be verified easily by passage to the finite quotients of $\mathfrak{G}$. (Conversely, if $g, g'\in\mathfrak{G}$, $m\geqq 1$, and $(g'-1)^m$ is divisible by $g-1$ in one way, then g' must be of the form $g'=g^\alpha$ ($\alpha\in\hat{\mathbf{Z}}$). We shall need this later, but only when $m=2$; cf. the proof of Theorem 5.1.) In particular, when the order of g in $\mathfrak{G}$ is divisible by l^∞, $g^\alpha-1$ is *uniquely* divisible by $g-1$ from either side (lemma 3.1). The two quotients coincide, because the equalities

$$g^\alpha-1=(g-1)\beta=\beta'(g-1) \qquad (\beta,\beta'\in\mathbf{Z}_l[[\mathfrak{G}]])$$

give

$$(g-1)\beta(g-1)=(g^\alpha-1)(g-1)=(g-1)(g^\alpha-1)=(g-1)\beta'(g-1);$$

hence $\beta=\beta'$. This quotient $\beta=\beta'$ will be denoted by $\dfrac{g^\alpha-1}{g-1}$.

Now we shall go on to the next

Lemma 3.2. *Let $\mathfrak{F}$ be a free almost pro-l group of rank 2 generated by x, y, and σ be an automorphism of $\mathfrak{F}$ such that*

$$\sigma(x)=s\,x^\alpha s^{-1}, \qquad \sigma(y)=t\,y^\beta t^{-1}$$

with some $s, t\in\mathfrak{F}$, $\alpha, \beta\in\hat{\mathbf{Z}}^\times$. Then, for any $f\in\mathfrak{F}$,

$$\begin{aligned}\frac{\partial(\sigma(f))}{\partial x}&=\sigma\left(\frac{\partial f}{\partial x}\right)\left\{s\frac{x^\alpha-1}{x-1}+(1-\sigma(x))\frac{\partial(s-t)}{\partial x}\right\}+(1-\sigma(f))\frac{\partial t}{\partial x},\\ \frac{\partial(\sigma(f))}{\partial y}&=\sigma\left(\frac{\partial f}{\partial y}\right)\left\{t\frac{y^\beta-1}{y-1}+(1-\sigma(y))\frac{\partial(t-s)}{\partial y}\right\}+(1-\sigma(f))\frac{\partial s}{\partial y}.\end{aligned} \qquad (\#)$$

Here, the automorphism of $\mathbf{Z}_l[[\mathfrak{F}]]$ induced from σ is also denoted by σ.

First, we prove a more general

Lemma 3.2′. *Let $\mathfrak{F}$ be a free almost pro-l group of rank r generated by $x_1, \dots, x_r$, and σ be any automorphism of $\mathfrak{F}$. Put $\sigma x_i=u_i x_i$ with $u_i\in\mathfrak{F}$ ($1\leqq i\leqq r$), and take any element $f\in\mathfrak{F}$. Then, for each j ($1\leqq j\leqq r$),*

$$\frac{\partial(\sigma(f))}{\partial x_j}=\sigma\left(\frac{\partial f}{\partial x_j}\right)u_j+\sum_{k=1}^{r}\left\{\sigma\left(\frac{\partial f}{\partial x_k}\right)\right\}\cdot\left(\frac{\partial u_k}{\partial x_j}\right). \qquad (!)$$

Proof. Each side of (!), as a function of f, satisfies the 1-cocycle relation $\alpha(fg)=\alpha(f)+\sigma(f)\alpha(g)$ ($f, g\in\mathfrak{F}$). Moreover, it is continuous. Such functions are obviously determined by their values at the generators of $\mathfrak{F}$. Therefore, it is enough to check (!) only when $f=x_i$ ($1\leqq i\leqq r$). But then, both sides of (!) are equal to

$$\frac{\partial(u_i x_i)}{\partial x_j}=\frac{\partial u_i}{\partial x_j}+u_i\,\delta_{ij}.$$

q.e.d.

Proof of lemma 3.2. This is a special case of lemma 3.2′, where $r=2$, $x_1=x$, $x_2=y$, $u_1=s\,x^\alpha s^{-1}x^{-1}$, $u_2=t\,y^\beta t^{-1}y^{-1}$. The formulas follow directly from lemma

3.2′, if we only note that

$$f-1=\frac{\partial f}{\partial x}(x-1)+\frac{\partial f}{\partial y}(y-1). \quad q.e.d.$$

Now let $\mathfrak{F}$ be a free almost pro-l group of rank 2. Two ordered pairs (x, y), (x_1, y_1) of generators of $\mathfrak{F}$ will be called *equivalent*, if $x_1 \sim x^\alpha$ and $y_1 \sim y^\beta$ with some $\alpha, \beta \in \hat{Z}^\times$ ($\sim$: conjugacy). When (x, y), (x_1, y_1) are such, we shall define an element $e_{(x,y)}^{(x_1,y_1)} \in \mathbf{Z}_l[[\mathfrak{F}]]$, as follows. Choose any $s, t \in \mathfrak{F}$ and $\alpha, \beta \in \hat{Z}^\times$ with

$$x_1 = s x^\alpha s^{-1}, \qquad y_1 = t y^\beta t^{-1}.$$

We shall show that the element

$$e_{(x,y)}^{(x_1,y_1)} = s - \frac{\partial (s-t)}{\partial x}(x-1) = t - \frac{\partial (t-s)}{\partial y}(y-1)$$

of $\mathbf{Z}_l[[\mathfrak{F}]]$ *depends only on* (x, y) *and* (x_1, y_1). For this purpose, let $s', t' \in \mathfrak{F}$ and $\alpha', \beta' \in \hat{Z}^\times$ be another choice for s, t and α, β. Then from the equalities

$$s x^\alpha s^{-1} = s' x^{\alpha'} s'^{-1} (= x_1), \qquad t y^\beta t^{-1} = t' y^{\beta'} t'^{-1} (= y_1)$$

follow that

$$(1-x_1)\frac{\partial s}{\partial x} + s\frac{x^\alpha - 1}{x-1} = (1-x_1)\frac{\partial s'}{\partial x} + s'\frac{x^{\alpha'}-1}{x-1}, \tag{1}$$

$$(1-y_1)\frac{\partial t}{\partial x} = (1-y_1)\frac{\partial t'}{\partial x}. \tag{2}$$

Since x_1, y_1 is a generator of $\mathfrak{F}$, y_1 is of infinite order, and since $\mathfrak{F}$ is an almost pro-l group, the order of y_1 is divisible by l^∞. Therefore, by lemma 3.1, $1-y_1$ in (2) can be cancelled, and we obtain

$$\frac{\partial t}{\partial x} = \frac{\partial t'}{\partial x}. \tag{3}$$

Now multiply $x-1$ on both sides of (1) from the right, to obtain

$$(1-x_1)\frac{\partial s}{\partial x}(x-1) + (x_1-1)s = (1-x_1)\frac{\partial s'}{\partial x}(x-1) + (x_1-1)s'.$$

Again, $x_1 - 1$ can be cancelled, and we obtain

$$s - \frac{\partial s}{\partial x}(x-1) = s' - \frac{\partial s'}{\partial x}(x-1). \tag{4}$$

But (3) and (4) give

$$s - \frac{\partial (s-t)}{\partial x}(x-1) = s' - \frac{\partial (s'-t')}{\partial x}(x-1),$$

as desired.

Therefore, $e_{(x,y)}^{(x_1,y_1)}$ depends only on x, y, x_1, y_1. It is clear that

$$e_{(x,y)}^{(x,y)}=1, \qquad e_{(y,x)}^{(y_1,x_1)}=e_{(x,y)}^{(x_1,y_1)}.$$

Lemma 3.3. *Let (x, y), (x_1, y_1), (x_2, y_2) be mutually equivalent ordered pairs of generators of a free almost pro-l group $\mathfrak{F}$ of rank 2. Then*

$$e_{(x,y)}^{(x_2,y_2)}=e_{(x_1,y_1)}^{(x_2,y_2)}\, e_{(x,y)}^{(x_1,y_1)}. \tag{$*$}$$

Proof. Put

$$x_1=s_1 x^{\alpha_1} s_1^{-1}, \qquad x_2=s_2 x_1^{\alpha_2} s_2^{-1}=(s_2 s_1)\, x^{\alpha_1\alpha_2}(s_2 s_1)^{-1},$$
$$y_1=t_1 y^{\beta_1} t_1^{-1}, \qquad y_2=t_2 y_1^{\beta_2} t_2^{-1}=(t_2 t_1)\, y^{\beta_1\beta_2}(t_2 t_1)^{-1},$$

$(s_i, t_i \in \mathfrak{F}, \alpha_i, \beta_i \in \hat{Z}^{\times}; i=1,2)$. Then,

$$\begin{aligned} e_{(x,y)}^{(x_2,y_2)} &= s_2 s_1-\frac{\partial(s_2 s_1-t_2 t_1)}{\partial x}(x-1)\\ &= s_2 s_1-\frac{\partial(s_2-t_2)}{\partial x}(x-1)-\left(s_2\frac{\partial s_1}{\partial x}-t_2\frac{\partial t_1}{\partial x}\right)(x-1), \end{aligned}$$

and

$$e_{(x_1,y_1)}^{(x_2,y_2)}\cdot e_{(x,y)}^{(x_1,y_1)}=\left(s_2-\frac{\partial(s_2-t_2)}{\partial x_1}(x_1-1)\right)\left(s_1-\frac{\partial(s_1-t_1)}{\partial x}(x-1)\right).$$

Put

$$\theta=s_2-t_2, \qquad e=e_{(x,y)}^{(x_1,y_1)}=s_1-\frac{\partial(s_1-t_1)}{\partial x}(x-1).$$

Then

$$-e_{(x,y)}^{(x_2,y_2)}+e_{(x_1,y_1)}^{(x_2,y_2)}\cdot e_{(x,y)}^{(x_1,y_1)}=\frac{\partial\theta}{\partial x}(x-1)+\theta\frac{\partial t_1}{\partial x}(x-1)-\frac{\partial\theta}{\partial x_1}(x_1-1)e. \tag{\#}$$

But since $\theta=\frac{\partial\theta}{\partial x}(x-1)+\frac{\partial\theta}{\partial y}(y-1)$, and $\frac{\partial\theta}{\partial x_1}=\frac{\partial\theta}{\partial x}\frac{\partial x}{\partial x_1}+\frac{\partial\theta}{\partial y}\frac{\partial y}{\partial x_1}$, (#) is equal to

$$\frac{\partial\theta}{\partial x}\xi+\frac{\partial\theta}{\partial y}\eta,$$

where

$$\xi=x-1+(x-1)\frac{\partial t_1}{\partial x}(x-1)-\frac{\partial x}{\partial x_1}(x_1-1)\,e,$$

$$\eta=(y-1)\frac{\partial t_1}{\partial x}(x-1)-\frac{\partial y}{\partial x_1}(x_1-1)\,e.$$

Therefore, the proof of our lemma is reduced to that of the vanishing of ξ and η. Now, to check that ξ and η vanish, consider two 2×2 matrices over $\mathbf{Z}_l[[\mathfrak{F}]]$;

$$A=\begin{pmatrix}\frac{\partial x_1}{\partial x} & \frac{\partial x_1}{\partial y}\\ \frac{\partial y_1}{\partial x} & \frac{\partial y_1}{\partial y}\end{pmatrix}, \qquad A'=\begin{pmatrix}\frac{\partial x}{\partial x_1} & \frac{\partial x}{\partial y_1}\\ \frac{\partial y}{\partial x_1} & \frac{\partial y}{\partial y_1}\end{pmatrix}.$$

Then $AA'=A'A=I_2$; hence it is enough to prove that $A\begin{pmatrix}\xi\\ \eta\end{pmatrix}=\begin{pmatrix}0\\0\end{pmatrix}$. But by a straightforward calculation using

$$x_1-1=\frac{\partial x_1}{\partial x}(x-1)+\frac{\partial x_1}{\partial y}(y-1), \quad y_1-1=\frac{\partial y_1}{\partial x}(x-1)+\frac{\partial y_1}{\partial y}(y-1),$$

we obtain

$$A\begin{pmatrix}\xi\\ \eta\end{pmatrix}=\begin{pmatrix}\frac{\partial x_1}{\partial x}(x-1)+(x_1-1)\frac{\partial t_1}{\partial x}(x-1)-(x_1-1)\,e\\ \frac{\partial y_1}{\partial x}(x-1)+(y_1-1)\frac{\partial t_1}{\partial x}(x-1)\end{pmatrix}.$$

But from $x_1=s_1x^{\alpha_1}s_1^{-1}$ and $y_1=t_1y^{\beta_1}t_1^{-1}$, we obtain

$$\frac{\partial x_1}{\partial x}=(1-x_1)\frac{\partial s_1}{\partial x}+s_1\frac{x^{\alpha_1}-1}{x-1}, \quad \frac{\partial y_1}{\partial x}=(1-y_1)\frac{\partial t_1}{\partial x};$$

hence also

$$\frac{\partial x_1}{\partial x}(x-1)=(x_1-1)\left[s_1-\frac{\partial s_1}{\partial x}(x-1)\right].$$

Therefore, $A\begin{pmatrix}\xi\\ \eta\end{pmatrix}=\begin{pmatrix}0\\0\end{pmatrix}$. *q.e.d.*

Remark. When there exist automorphisms σ_1: $(x,y)\to(x_1,y_1)$, σ_2: $(x_1,y_1)\to(x_2,y_2)$ of $\mathfrak{F}$, lemma 3.3 can also be proved by using lemma 3.2.

Corollary 1. $e_{(x,y)}^{(x_1,y_1)}\cdot e_{(x_1,y_1)}^{(x,y)}=1$. *In particular,* $e_{(x,y)}^{(x_1,y_1)}$ *belongs to the unit group* $\mathbf{Z}_l[\![\mathfrak{F}]\!]^\times$.

The notation being as in lemma 3.2, define $e_{(x,y)}(\sigma)$ by

$$e_{(x,y)}(\sigma)=e_{(x,y)}^{(\sigma x,\sigma y)}\in\mathbf{Z}_l[\![\mathfrak{F}]\!]^\times.$$

Then

Corollary 2. (i) $$e_{(y,x)}(\sigma)=e_{(x,y)}(\sigma),$$

(ii) $$e_{(x,y)}(\sigma'\circ\sigma)=\sigma'(e_{(x,y)}(\sigma))\,e_{(x,y)}(\sigma'),$$

for any two automorphisms σ, σ' of $\mathfrak{F}$ leaving the equivalence class of (x,y) invariant.

Proof. (i) is obvious. (ii) follows immediately from lemma 3.3 and from the obvious identity

$$\sigma'(e_{(x,y)}^{(x_1,y_1)})=e_{(\sigma'x,\sigma'y)}^{(\sigma'x_1,\sigma'y_1)}$$

(cf. § 2 (B) (v)).

(C) Proofs of Theorems A, C. They are easily reduced to lemma 3.2 and 3.3, as follows.

Proof of Theorem A. For $\rho\in G_{\mathbf{Q}^*}$, choose an extension $\tilde\rho\in\mathrm{Gal}(M/L^*)$. Let $\mathfrak{F}=\mathrm{Gal}(M/K)$, x, y be as in § 1, and σ denote the automorphism of $\mathfrak{F}$ defined by

$\sigma(f)=\tilde{\rho} f \tilde{\rho}^{-1}$ $(f \in \mathfrak{F})$. Then $\sigma(x)=s x^{\alpha} s^{-1}$ and $\sigma(y)=t y^{\beta} t^{-1}$, with $\alpha=\beta=\chi(\rho)$ and with some $s, t \in \mathfrak{F}$ (Prop. 1.2). Therefore, by lemma 3.3,

$$e_{(x,y)}(\sigma)=e_{(x,y)}^{(\sigma x, \sigma y)}=s-\frac{\partial(s-t)}{\partial x}(x-1)$$

is independent of the choice of s, t. If we replace $\tilde{\rho}$ by $n\tilde{\rho}$ with some $n \in \mathfrak{N}$, then σ will be replaced by $\operatorname{Int}(n) \circ \sigma$, $\operatorname{Int}(n)$ being the inner automorphism $f \to n f n^{-1}$ of $\mathfrak{F}$; hence s, t will be replaced by $n s$, $n t$, respectively. But since

$$\frac{\partial(n s)}{\partial x}=n \frac{\partial s}{\partial x}+\frac{\partial n}{\partial x}, \quad \frac{\partial(n t)}{\partial x}=n \frac{\partial t}{\partial x}+\frac{\partial n}{\partial x},$$

we obtain $e_{(x,y)}(\operatorname{Int}(n) \circ \sigma)=n \cdot e_{(x,y)}(\sigma)$. Therefore, the projection $\pi(e_{(x,y)}(\sigma))$ on $\mathscr{A}$ depends only on $(x, y$ and) ρ. By Cor. 1 of lemma 3.3, this belongs to $\pi(\mathbf{Z}_l[[\mathfrak{F}]]^{\times}) \subset \mathscr{A}^{\times}$. The equality $\psi(\rho' \circ \rho)=\mathrm{J}_{\rho'}(\psi(\rho)) \cdot \psi(\rho')$ follows immediately from the equality (ii) of Cor. 2 of lemma 3.3. It is easy to check that ψ is continuous. *q.e.d.*

Proof of Theorem C. Let ρ, $\tilde{\rho}$, s, t be as above, and put

$$\psi_x(\rho)=\pi\left(s \frac{x^{\chi(\rho)}-1}{x-1}\right)+(1-J_\rho(\mathbf{x}))\, \pi\left(\frac{\partial(s-t)}{\partial x}\right),$$

$$\psi_y(\rho)=\pi\left(t \frac{y^{\chi(\rho)}-1}{y-1}\right)+(1-J_\rho(\mathbf{y}))\, \pi\left(\frac{\partial(t-s)}{\partial y}\right).$$

Then

$$\psi_x(\rho)(\mathbf{x}-1)=(J_\rho(\mathbf{x})-1)\, \psi(\rho), \quad \psi_y(\rho)(\mathbf{y}-1)=(J_\rho(\mathbf{y})-1)\, \psi(\rho), \tag{$*$}$$

because $\pi(s)\, \mathbf{x}^{\chi(\rho)}=J_\rho(\mathbf{x})\, \pi(s)$, $\pi(t)\, \mathbf{y}^{\chi(\rho)}=J_\rho(\mathbf{y})\, \pi(t)$.

By lemma 3.1, $\psi_x(\rho)$ and $\psi_y(\rho)$ are determined by the equations $(*)$ (and in particular, they depend only on ρ). Since ψ is an anti 1-cocycle, ψ_x and ψ_y are also.

Now take any $n \in \mathfrak{N}$. Then ρ acts on $\mathfrak{T} \simeq \mathfrak{N}^{\mathrm{ab}}$ (via Th. B) as

$$\left(\pi\left(\frac{\partial n}{\partial x}\right), \pi\left(\frac{\partial n}{\partial y}\right)\right) \to \left(\pi\left(\frac{\partial \sigma(n)}{\partial x}\right), \pi\left(\frac{\partial \sigma(n)}{\partial y}\right)\right).$$

By lemma 3.2 for $f=n$, we obtain

$$\frac{\partial \sigma(n)}{\partial x}=\sigma\left(\frac{\partial n}{\partial x}\right) \cdot\left\{s \frac{x^{\chi(\rho)}-1}{x-1}+(1-\sigma(x)) \frac{\partial(s-t)}{\partial x}\right\}+(1-\sigma(n)) \frac{\partial t}{\partial x};$$

hence

$$\pi\left(\frac{\partial \sigma(n)}{\partial x}\right)=J_\rho\left(\pi\left(\frac{\partial n}{\partial x}\right)\right) \psi_x(\rho).$$

Similarly, from

$$\frac{\partial \sigma(n)}{\partial y}=\sigma\left(\frac{\partial n}{\partial y}\right) \cdot\left\{t \frac{y^{\chi(\rho)}-1}{y-1}+(1-\sigma(y)) \frac{\partial(t-s)}{\partial y}\right\}+(1-\sigma(n)) \frac{\partial s}{\partial y}$$

follows

$$\pi\left(\frac{\partial\sigma(n)}{\partial y}\right)=J_\rho\left(\pi\left(\frac{\partial n}{\partial y}\right)\right)\psi_y(\rho).$$

Therefore, ρ acts on $\mathfrak{X}$ as

$$\left(\pi\left(\frac{\partial n}{\partial x}\right),\pi\left(\frac{\partial n}{\partial y}\right)\right)\to\left(J_\rho\left(\pi\left(\frac{\partial n}{\partial x}\right)\right),J_\rho\left(\pi\left(\frac{\partial n}{\partial y}\right)\right)\right)\begin{pmatrix}\psi_x(\rho) & 0\\ 0 & \psi_y(\rho)\end{pmatrix}.$$

This proves Theorem C. *q.e.d.*

§ 4. Dependence on the coordinates

We defined three anti 1-cocycles ψ, ψ_x, ψ_y: $G_{\mathbf{Q}^*}\to\mathscr{A}^\times$ using two special generators x, y of $\mathfrak{F}=\mathrm{Gal}(M/K)$. To indicate their dependence on x, y, we denote (in this section) ψ, ψ_x and ψ_y by $\psi_{\{x,y\}}=\psi_{\{y,x\}}$, $\psi_{x/\{x,y\}}$ and $\psi_{y/\{x,y\}}$ respectively ($\{x,y\}$: unordered pair). Note that they are defined as long as x and y generate $\mathfrak{F}$ *and* each of x, y generates some inertia group above one of $\{0,1,\infty\}$. Their dependence on the choice of x, y is as follows. If ψ, ψ' are anti 1-cocycles $G_{\mathbf{Q}^*}\to\mathscr{A}^\times$ and $\alpha\in\mathscr{A}$, we shall express as

$$\psi\xrightarrow{\alpha}\psi'$$

the relation

$$J_\rho(\alpha)\,\psi(\rho)=\psi'(\rho)\,\alpha\qquad(\forall\rho\in G_{\mathbf{Q}^*}).$$

(i) If $x_1=s\,x^\alpha s^{-1}$, $y_1=t\,y^\beta t^{-1}$ ($s,t\in\mathfrak{F}$, $\alpha,\beta\in\hat{\mathbf{Z}}^\times$), and x_1, y_1 also generate $\mathfrak{F}$, then

$$\psi_{\{x,y\}}\xrightarrow{\pi\left(e^{(x_1,y_1)}_{(x,y)}\right)}\psi_{\{x_1,y_1\}},$$

where $e^{(x_1,y_1)}_{(x,y)}$ is as in § 3. This follows immediately from lemma 3.3.

(ii) If (x,y,z) is as in § 1 (B), then $\psi_{z/\{y,z\}}$, $\psi_{\{y,z\}}$, $\psi_{y/\{y,z\}}$ etc. are also defined, and they are related to each other as follows.

$$\begin{tikzcd}
 & & \psi_{\{x,y\}} \arrow[dl, "\mathbf{y-1}"'] \arrow[dr, "\mathbf{x-1}"] & & \\
 & \psi_{y/\{x,y\}} \arrow[dl, shift left, "\mathbf{y^{-1}}"] & & \psi_{x/\{x,y\}} \arrow[dr, shift left, "\mathbf{z}"] & \\
\psi_{z/\{z,x\}} \arrow[ur, shift left, "\mathbf{y}"] & & & & \psi_{z/\{y,z\}} \arrow[ul, shift left, "\mathbf{z^{-1}}"] \\
 & \psi_{\{z,x\}} \arrow[ul, "\mathbf{z-1}"] \arrow[d, "\mathbf{x-1}"'] & & \psi_{\{y,z\}} \arrow[ur, "\mathbf{z-1}"'] \arrow[d, "\mathbf{y-1}"] & \\
 & \psi_{x/\{z,x\}} \arrow[rr, shift left, "\mathbf{x^{-1}}"] & & \psi_{y/\{y,z\}} \arrow[ll, shift left, "\mathbf{x}"] &
\end{tikzcd}$$

Here, modulo symmetry, the only "new relation" to be checked is

$$\psi_{x/\{x,y\}} \xrightarrow{\mathrm{z}} \psi_{z/\{y,z\}},$$

and this can be checked easily from the definitions.

Congruences. From the definition and from the above cycle relations, we can easily deduce the following congruences. Here, for each $\rho \in G_{\mathbf{Q}^*}$, $\tilde{\rho}$ is an extension of ρ to an element of $\mathrm{Gal}(M/L^*)$, and s, t, u are any elements of $\mathfrak{F}$ such that

$$\tilde{\rho}\, x\, \tilde{\rho}^{-1} = s\, x^{\alpha} s^{-1}, \quad \tilde{\rho}\, y\, \tilde{\rho}^{-1} = t\, y^{\alpha} t^{-1}, \quad \tilde{\rho}\, z\, \tilde{\rho}^{-1} = u\, z^{\alpha} u^{-1} \quad (\alpha = \chi(\rho)).$$

Proposition 4.1.

(i)
$$\begin{aligned} \psi_{\{x,y\}}(\rho) &\equiv s \mod \mathscr{A}(\mathrm{x}-1), \\ &\equiv t \mod \mathscr{A}(\mathrm{y}-1), \end{aligned}$$

(ii)
$$\begin{aligned} \psi_{x/\{x,y\}}(\rho) &\equiv s\,\frac{\mathrm{x}^{\alpha}-1}{\mathrm{x}-1} \mod (J_{\rho}(\mathrm{x})-1)\mathscr{A}, \\ &\equiv u\,\frac{(\mathrm{x\,y})^{\alpha}-1}{\mathrm{x\,y}-1} \mod (J_{\rho}(\mathrm{x\,y})-1)\mathscr{A}; \end{aligned}$$

(iii)
$$\begin{aligned} \psi_{y/\{x,y\}}(\rho) &\equiv t\,\frac{\mathrm{y}^{\alpha}-1}{\mathrm{y}-1} \mod (J_{\rho}(\mathrm{y})-1)\mathscr{A}, \\ &\equiv J_{\rho}(\mathrm{x})^{-1} u\,\frac{(\mathrm{x\,y})^{\alpha}-1}{\mathrm{x\,y}-1}\,\mathrm{x} \mod (J_{\rho}(\mathrm{y\,x})-1)\mathscr{A}. \end{aligned}$$

In the Fermat case, these congruences served as generic congruences for Jacobi sums [I] § II. This system of 6 congruences is "complete" in a certain group theoretic sense (similar to [I] Theorem 3B).

§ 5. Comparison of the two kernels

In § 5, we assume that L^*/K^* is a Galois extension, or equivalently, that the action of $G_{\mathbf{Q}^*}$ on $\mathscr{A} = \mathbf{Z}_l[[\mathfrak{G}]]$ is trivial. Then ψ, ψ_x, ψ_y: $G_{\mathbf{Q}^*} \to \mathscr{A}^{\times}$ are anti-homomorphisms, related to each other by

$$(\mathrm{x}-1)\,\psi(\rho) = \psi_x(\rho)\,(\mathrm{x}-1), \quad (\mathrm{y}-1)\,\psi(\rho) = \psi_y(\rho)\,(\mathrm{y}-1) \quad (\rho \in \mathrm{G}_{\mathbf{Q}^*}), \qquad (1)$$

and the action of ρ on $\mathfrak{N}^{\mathrm{ab}}$ $(\subset \mathscr{A}^{\oplus 2}$, via Theorem B) is given by the right multiplication of the diagonal matrix

$$\begin{pmatrix} \psi_x(\rho) & 0 \\ 0 & \psi_y(\rho) \end{pmatrix} \quad \text{(cf. Theorem C).}$$

By (1) and Proposition 1.4, ψ, ψ_x, ψ_y have the common kernel. Denote by k_1 (resp. k_2) the Galois extension of $\mathbf{Q}^*$ corresponding to the kernel of the action of $G_{\mathbf{Q}^*}$ on $\mathfrak{N}^{ab}$ (resp. the kernel of ψ). It is clear that $k_1 \subset k_2$. We shall clarify the difference of roles played by these two extensions k_1 and k_2 of $\mathbf{Q}^*$.

(A) First, consider the left $\mathscr{A}$-ideal $A = \mathscr{A}(\mathbf{x}-1) \cap \mathscr{A}(\mathbf{y}-1)$, and its $\mathbf{Z}_l$-submodule

$$D = \{\lambda \in A;\ A \cdot \lambda = 0\}.$$

Then, since $D^2 = 0$, $1 + D$ is a subgroup of $\mathscr{A}^\times$ isomorphic to the additive group D.

Theorem 5.1. *An element ρ of $G_{\mathbf{Q}^*}$ acts trivially on $\mathfrak{N}^{ab}$ if and only if $\psi(\rho) \in 1 + D$. In particular, $(\psi(\rho)-1)^2 = 0$ for $\rho \in G_{k_1}$.*

Proof. By Remark 1.5 (§1), $\rho \in G_{\mathbf{Q}^*}$ acts trivially on $\mathfrak{N}^{ab} \simeq \mathfrak{T}$ if and only if $A \cdot (\psi(\rho)-1) = 0$. Therefore, it remains only to check that if $\rho \in G_{k_1}$ then $\psi(\rho) - 1 \in A$. To check this, take any extension $\tilde{\rho} \in \mathrm{Gal}(M/L^*)$ of $\rho \in G_{\mathbf{Q}^*}$ and, as before, put

$$\tilde{\rho}\, x\, \tilde{\rho}^{-1} = s\, x^{\chi(\rho)} s^{-1}, \qquad \tilde{\rho}\, y\, \tilde{\rho}^{-1} = t\, y^{\chi(\rho)} t^{-1} \quad (s, t \in \mathfrak{F}). \tag{2}$$

Then, since ρ acts trivially on $\mathfrak{G} = \mathfrak{F}/\mathfrak{N}$,

$$n_1 = s\, x^{\chi(\rho)} s^{-1} x^{-1} \quad \text{and} \quad n_2 = t\, y^{\chi(\rho)} t^{-1} y^{-1}$$

belong to $\mathfrak{N}$. Therefore, A contains the elements

$$\begin{aligned} \pi\left(\frac{\partial n_1}{\partial x}\right)(x-1) &= \pi\left((1-x)\frac{\partial s}{\partial x} + s\frac{x^{\chi(\rho)}-1}{x-1} - 1\right)(x-1) \\ &= \pi\left\{(1-x)\left(\frac{\partial s}{\partial x}(x-1) - s + 1\right)\right\}, \end{aligned} \tag{3}$$

and

$$\pi\left(\frac{\partial n_2}{\partial x}\right)(x-1) = \pi\left\{(1-y)\frac{\partial t}{\partial x}(x-1)\right\}. \tag{4}$$

Now suppose $\rho \in G_{k_1}$. Then the right multiplication of $\psi(\rho) - 1$ annihilates A; in particular, the elements (3) and (4). Therefore, it annihilates

$$\pi\left(\frac{\partial s}{\partial x}(x-1) - s + 1\right) \quad \text{and} \quad \pi\left(\frac{\partial t}{\partial x}(x-1)\right).$$

But since

$$\psi(\rho) - 1 = \pi\left(s - 1 - \frac{\partial(s-t)}{\partial x}(x-1)\right),$$

the right multiplication of $\psi(\rho) - 1$ annihilates $\psi(\rho) - 1$ itself;

$$(\psi(\rho) - 1)^2 = 0. \tag{5}$$

Now, from (5) we obtain

$$(\pi(s) - 1)^2 \in \mathscr{A}(\mathbf{x} - 1), \tag{6}$$

because $(\mathbf{x}-1)\pi(s)=\pi(s)(\mathbf{x}^{\chi(\rho)^{-1}}-1)$. And from (6) we obtain $\pi(s)\in\langle\mathbf{x}\rangle$. In fact, take any finite quotient G of $\mathfrak{G}$, and project $\mathscr{A}$ onto $\mathbf{Z}_l[G]$. Call $\bar{\mathbf{s}}$, $\bar{\mathbf{x}}$ the projections of $\mathbf{s}$, $\mathbf{x}$ on G, respectively, and let d be the order of $\bar{\mathbf{x}}$ in G. Then (6) implies

$$(\bar{s}-1)^2\sum_{j=0}^{d-1}\bar{\mathbf{x}}^j=0;$$

hence

$$\sum_{j=0}^{d-1}\bar{s}^2\,\bar{\mathbf{x}}^j+\sum_{j=0}^{d-1}\bar{\mathbf{x}}^j=2\sum_{j=0}^{d-1}\bar{s}\,\bar{\mathbf{x}}^j$$

in $\mathbf{Z}_l[G]$. But since $\bar{\mathbf{x}}^j$ $(0\leqq j\leqq d-1)$ are distinct elements of G, this equality can hold only when

$$\sum\bar{s}^2\,\bar{\mathbf{x}}^j=\sum\bar{\mathbf{x}}^j=\sum\bar{s}\,\bar{\mathbf{x}}^j.$$

Therefore, $\bar{s}\in\langle\bar{\mathbf{x}}\rangle$. Since G is an arbitrary finite quotient of $\mathfrak{G}$, we obtain $\pi(s)\in\langle\mathbf{x}\rangle$. Similarly, $\pi(t)\in\langle\mathbf{y}\rangle$. Therefore, $s\in\mathfrak{N}\langle x\rangle$ and $t\in\mathfrak{N}\langle y\rangle$; or in other words, we can choose s and t from $\mathfrak{N}$. But then,

$$\psi(\rho)-1=-\pi\left(\frac{\partial(s-t)}{\partial x}\right)(\mathbf{x}-1)=-\pi\left(\frac{\partial(t-s)}{\partial y}\right)(\mathbf{y}-1)\in\Lambda. \quad q.e.d.$$

Now let $\rho\in G_{k_1}$. Then we have shown above that $\tilde{\rho}\,x\,\tilde{\rho}^{-1}$ (resp. $\tilde{\rho}\,y\,\tilde{\rho}^{-1}$) is conjugate to $x^{\chi(\rho)}$ (resp. $y^{\chi(\rho)}$) by some element of $\mathfrak{N}$. Similarly, by using y, z instead of x, y, we can show that $\tilde{\rho}\,z\,\tilde{\rho}^{-1}$ is conjugate to $z^{\chi(\rho)}$ by some element of $\mathfrak{N}$. Since the $\tilde{\rho}$-conjugation does not change x, y, z mod $\mathfrak{N}$, this implies that $x^{\chi(\rho)-1}$, $y^{\chi(\rho)-1}$ and $z^{\chi(\rho)-1}$ belong to $\mathfrak{N}$. But since each inertia group above $t=0, 1, \infty$ in M/K is canonically isomorphic to that in L/K (§ 1 (B)), this implies that

$$x^{\chi(\rho)}=x, \qquad y^{\chi(\rho)}=y, \qquad z^{\chi(\rho)}=z \quad \text{in } \mathfrak{F},$$

or equivalently,

$$\chi(\rho)\equiv 0 \pmod{m\,l^{\infty}}, \tag{7}$$

where $m=lcm(m_0, m_1, m_\infty)$, the least common multiple of the "prime-to l" part of the ramification indices of $0, 1, \infty$ in L/K. Therefore,

$$\tilde{\rho}\,x\,\tilde{\rho}^{-1}\approx x, \qquad \tilde{\rho}\,y\,\tilde{\rho}^{-1}\approx y, \qquad \tilde{\rho}\,z\,\tilde{\rho}^{-1}\approx z \quad (\rho\in G_{k_1}), \tag{8}$$

where $\approx$ denotes conjugacy by some element of $\mathfrak{N}$.

A *place* of M (or any of its subfields containing $\mathbf{Q}^*(t)$) will always mean a place relative to its constant field. It will be called *cuspidal* if it lies above $t=0, 1$ or ∞.

Corollary 1. (i) *Cuspidal places of L^* are k_1-rational*; (ii) k_1 *contains the groups μ_m, μ_{l^∞} of the m-th and the l^∞-th roots of unity.*

Proof. (i) Let P be a place of M above $t=0$ having $\langle x\rangle$ as its inertia group in M/K. Take any $\rho\in G_{\mathbf{Q}^*}$ and its extension $\tilde{\rho}\in\mathrm{Gal}(M/L^*)$. Then $\rho\circ P\circ\tilde{\rho}^{-1}$ is also a place of M which coincides with P on K; hence $\rho\circ P\circ\tilde{\rho}^{-1}=P\circ s^{-1}$ with some $s\in\mathfrak{F}$. But then, $\tilde{\rho}\,x\,\tilde{\rho}^{-1}=s\,x^{\chi(\rho)}s^{-1}$. Now let $\rho\in G_{k_1}$. Then $s\in\mathfrak{N}\langle x\rangle$, as shown above. Therefore, $\rho \circ P \circ \tilde{\rho}^{-1}$ coincides with P on L; hence $\rho \circ P$ coincides with P on L^*, for all $\rho \in G_{k_1}$. Therefore, the residue field of L^* w.r.t. P is contained in k_1. Since L^*/K^* is a Galois extension, this implies that all places of L^* above $t=0$ (and similarly, $t=1, \infty$) are k_1-rational. (ii) is obvious (either by (7), or by (i)).

Corollary 2. *k_2/k_1 is a pro-l abelian extension with the Galois group isomorphic to a closed additive subgroup of D. In particular, if $\mathscr{A}$ contains no element $\alpha \neq 0$ with $\alpha^2=0$, then $k_1=k_2$.*

Corollary 3. *$k_1=k_2$ if $\mathfrak{G}$ is abelian.*

In fact, if G is any finite abelian quotient of $\mathfrak{G}$, $\mathbf{Q}_l[G]$ is a direct sum of commutative fields. Hence $\alpha \in \mathscr{A}$, $\alpha^2=0$ implies $\alpha=0$.

This applies to the tower of Fermat curves of degree $m l^{\infty}$.

(B) Now denote by L^{ab} the intermediate field of M/L corresponding to $[\mathfrak{N}, \mathfrak{N}]$, i.e., the maximum abelian extension of L *in* M. Then $\mathrm{Gal}(L^{\mathrm{ab}}/K) \simeq \mathfrak{F}/[\mathfrak{N}, \mathfrak{N}]$. Denote by $\mathrm{Out}_{\mathfrak{N}^{\mathrm{ab}}}(\mathfrak{F}/[\mathfrak{N}, \mathfrak{N}])$ the quotient of the group of those automorphisms of $\mathfrak{F}/[\mathfrak{N}, \mathfrak{N}]$ which stabilize $\mathfrak{N}$, modulo the group of inner automorphisms by elements of $\mathfrak{N}^{\mathrm{ab}}=\mathfrak{N}/[\mathfrak{N}, \mathfrak{N}]$. Then the natural action of $\mathrm{Gal}(L^{\mathrm{ab}}/L^*)$ on $\mathfrak{F}/[\mathfrak{N}, \mathfrak{N}]$ (§ 1 (B)) induces a homomorphism

$$G_{\mathbf{Q}^*} \to \mathrm{Out}_{\mathfrak{N}^{\mathrm{ab}}}(\mathfrak{F}/[\mathfrak{N}, \mathfrak{N}]). \tag{\#}$$

Proposition 5.2. *The kernel of ψ coincides with that of* (#).

Remark. This shows that *if* every automorphism of $\mathfrak{F}/[\mathfrak{N}, \mathfrak{N}]$ which acts identically on both $\mathfrak{F}/\mathfrak{N}=\mathfrak{G}$ and $\mathfrak{N}^{\mathrm{ab}}$ is necessarily an inner automorphism by an element of $\mathfrak{N}^{\mathrm{ab}}$ (or equivalently, if $H^1(\mathfrak{G}, \mathfrak{N}^{\mathrm{ab}})=0$), then $k_1=k_2$. At present, the author knows very little about this cohomology group $H^1(\mathfrak{G}, \mathfrak{N}^{\mathrm{ab}})$. At any rate, the action of $G_{\mathbf{Q}^*}$ gives only a special type of automorphisms of $\mathfrak{F}/[\mathfrak{N}, \mathfrak{N}]$. So, even if $H^1(\mathfrak{G}, \mathfrak{N}^{\mathrm{ab}}) \neq 0$, it is still possible that k_1 coincides with k_2.

Proposition 5.2 is an immediate consequence of the preceding results in (A) and the following two lemmas. So, we shall omit its proof.

Lemma 5.3. *The centralizer in $\mathfrak{N}^{\mathrm{ab}}$ of each of the projection of x, y, z on $\mathfrak{F}/[\mathfrak{N}, \mathfrak{N}]$ is trivial. In particular, $\mathfrak{N}^{\mathrm{ab}}$ contains no non-trivial central element of $\mathfrak{F}/[\mathfrak{N}, \mathfrak{N}]$.*

Proof. It suffices to prove that $(\mathrm{x}-1)\bar{n}=0$ ($\bar{n} \in \mathfrak{N}^{\mathrm{ab}}$) implies $\bar{n}=0$. But since $\mathfrak{N}^{\mathrm{ab}} \subset \mathscr{A}^{\oplus 2}$ as left $\mathscr{A}$-module (Theorem B), this is an immediate consequence of Proposition 1.4. *q.e.d.*

To state the next lemma, let $\rho \in G_{k_1}$, $\tilde{\rho} \in \mathrm{Gal}(M/L^*)$ be an extension of ρ, and $s, t \in \mathfrak{N}$ be such that

$$\tilde{\rho} x \tilde{\rho}^{-1}=s x s^{-1}, \quad \tilde{\rho} y \tilde{\rho}^{-1}=t y t^{-1} \tag{9}$$

(cf. (8) above).

Lemma 5.4. *$\psi(\rho)=1$ if and only if $s\equiv t$* $\bmod[\mathfrak{N},\mathfrak{N}]$.

Proof. As $s,t\in\mathfrak{N}$,

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

Therefore, $\psi(\rho)=1$ if and only if

$$\pi\left(\frac{\partial(s-t)}{\partial x}\right)=\pi\left(\frac{\partial(s-t)}{\partial y}\right)=0.$$

But by Theorem 2.2, this is equivalent with $s^{-1}t\in[\mathfrak{N},\mathfrak{N}]$. *q.e.d.*

(C) For a field k with $\mathbf{Q}^*\subset k\subset\bar{\mathbf{Q}}$, a *weak* (resp. *strong*) k-model of L^{ab} will mean any field Ω which fits into the diagram (10) below (the inclusion of fields) and satisfies the condition that Ω/L^*k (resp. Ω/K^*k) is a Galois extension.

$$\begin{tikzcd}
 & L^{\mathrm{ab}}=\Omega\cdot\bar{\mathbf{Q}} \arrow[dd, dash] \\
\Omega \arrow[ur, dash] \arrow[dd, dash] & \\
 & L \arrow[dd, dash] \\
L^*k \arrow[ur, dash] \arrow[dd, dash] & \\
 & K \arrow[dd, dash] \\
K^*k \arrow[ur, dash] \arrow[dd, dash] & \\
 & \bar{\mathbf{Q}} \\
\Omega\cap\bar{\mathbf{Q}}=k \arrow[ur, dash] &
\end{tikzcd} \tag{10}$$

A strong k-model is unique, because $\mathfrak{N}^{\mathrm{ab}}$ contains no non-trivial central element of $\mathfrak{F}/[\mathfrak{N},\mathfrak{N}]$ (lemma 5.3). In terms of k-models, the fields $k=k_1$ and k_2 are characterized as follows.

Proposition 5.5. *$k=k_1$ (resp. k_2) is the smallest extension of $\mathbf{Q}^*$ such that L^{ab} has a weak (resp. strong) k-model.*

Proof. It is obvious that the existence of a weak k-model implies $k\supset k_1$. The existence of a strong k-model implies that, for each $\rho\in G_k$, we can choose $\tilde{\rho}$ and $s,t\in\mathfrak{N}$ (cf. (9) above) so that the automorphism $x\to\tilde{\rho}x\tilde{\rho}^{-1}=sxs^{-1}$, $y\to\tilde{\rho}y\tilde{\rho}^{-1}=tyt^{-1}$ of $\mathfrak{F}/[\mathfrak{N},\mathfrak{N}]$ is the identity map. But then, $s,t\in[\mathfrak{N},\mathfrak{N}]$ by lemma 5.3; hence $\rho\in G_{k_2}$ by lemma 5.4. Therefore, $k\supset k_2$. Conversely, suppose that $\rho\in G_{k_2}$. Then by lemma 5.4, we can choose an extension $\tilde{\rho}\in\mathrm{Gal}(L^{\mathrm{ab}}/L^*k_2)$ of ρ which centralizes $\mathfrak{F}/[\mathfrak{N},\mathfrak{N}]$. Such a $\tilde{\rho}$ is unique, and the common fixed field of $\tilde{\rho}$ $(\rho\in G_{k_2})$ gives the strong k_2-model of L^{ab}. Finally, to prove the existence of a weak k_1-model, choose any k_1-rational place P of L^*k_1. As we know (Cor. 1 of Theorem 5.1), the cuspidal places of L^*k_1 are k_1-rational. We assert that there is a *unique* weak k_1-model Ω_P of L^{ab} in which P decomposes completely (i.e., all places of Ω_P above P are k_1-rational). This is equivalent to saying that, for each $\rho\in G_{k_1}$, there exists a *unique* extension $\rho_P\in\mathrm{Gal}(L^{\mathrm{ab}}/L^*k_1)$ such that

$$\rho\circ\tilde{P}\circ\rho_P^{-1}=\tilde{P}, \tag{11}$$

where $\tilde{P}$ is any extension of P to a place of L^{ab}. (As $\mathfrak{N}^{ab}$ is central in $\mathrm{Gal}(L^{ab}/L^* k_1)$ (by the definition of k_1), the condition (11) is independent of the choice of $\tilde{P}$.) But this is obvious; the existence of ρ_P is a formal consequence of the k_1-rationality of P, and the uniqueness is that of the "unramifiedness" of L^{ab}/L (in the sense of § 1 (B)). *q.e.d.*

Proposition 5.6. (i) *For each cuspidal place P of $L^* k_1$, there exists a unique weak k_1-model Ω_P of L^{ab} in which P splits completely*; (ii) *k_2 is the smallest extension of k_1 such that $\Omega_P \cdot k_2$ is independent of P. Moreover, $\Omega_P \cdot k_2$ is the strong k_2-model of L^{ab}.*

Proof. (i) is already proved above. As for (ii), the latter assertion is obvious. It remains to check that if $k \supset k_1$ is such that $\Omega_P \cdot k = \Omega_Q \cdot k$ for any cuspidal places P, Q of $L^* k_1$ then $k \supset k_2$. Take two cuspidal places $\tilde{P}$ (resp. $\tilde{Q}$) of L^{ab} having $\langle x \rangle$ (resp. $\langle y \rangle$) as their inertia groups, and let P (resp. Q) be their restrictions to $L^* k_1$. Take $\rho \in G_k$. Then $\rho_P = \rho_Q$; hence

$$\rho_P x \rho_P^{-1} \equiv x, \qquad \rho_P y \rho_P^{-1} \equiv y \mod [\mathfrak{N}, \mathfrak{N}].$$

But then, $\psi(\rho) = 1$ by lemma 5.3 and 5.4. *q.e.d.*

To proceed further, we need the following "finiteness" assumption on the extension L/K.

[Assumption (F)] Let K_n/K ($n \geqq 0$) denote the maximum Galois subextension of L/K such that the l-component of the ramification index of each of $t = 0, 1, \infty$ in K_n/K is a divisor of l^n. Then $[K_n : K]$ is *finite* for all $n \geqq 0$.

This assumption is satisfied in several important cases, e.g., Examples 2, 3 of § 1.

Let X_n^* be the proper smooth $\mathbf{Q}^*$-curve with function field $K_n^* = K_n \cap L^*$, and J_n^* be its Jacobian. Note that $K_n^{urab} \cap L = K_n$, where K_n^{urab} is the maximum unramified abelian pro-l extension of K_n ($n \geqq 0$).

Theorem 5.7. *Under the assumption* (F),

(i) *k_1 is generated over $\mathbf{Q}^*$ by the l-power torsion points of J_n^* for all $n \geqq 0$;*

(ii) *k_2 is generated over k_1 by the l-power division points of the cuspidal points of $J_n^* \otimes k_1$ for all $n \geqq 0$.*

Here, a cuspidal point of $J_n^* \otimes k_1$ means a point determined by a cuspidal prime divisor of degree 0 on $X_n^* \otimes k_1$.

Corollary. If the cuspidal points of $J_n^* \otimes k_1$ ($n \geqq 0$) are torsion points, then $k_1 = k_2$.

Proof. If the order of a cuspidal point $u \in J_n^* \otimes k_1$ is finite, the l-multiplication acts surjectively on $Z u +_{l^\infty} J_n^*$. *q.e.d.*

This applies to the case of modular curves (see (D) below).

Proof of Theorem 5.7. (i) Since $K_n^{urab} \cap L = K_n$, the projection $\mathfrak{N}^{ab} \to T_l(J_n^*)$ is surjective. (ii) This is just a geometric re-interpretation of Proposition 5.6 (ii). *q.e.d.*

(D) Examples for which $k_1=k_2$ holds. (1) The maximum pro-l tower (Example 1, §1 (D)). Denote (newly) by $\mathbf{Q}^*$ the field corresponding to the kernel of the J_ρ-action of $G_{\mathbf{Q}}$ on $\mathscr{A}$. Then $L^*\cdot\mathbf{Q}^*/K^*\cdot\mathbf{Q}^*$ is Galois. For this extension, we have $k_1=\mathbf{Q}^*$, because $\mathfrak{T}=(0)$. Moreover, $k_2=k_1$ by Theorem 5.1. Indeed, $D\subset\Lambda\simeq\mathfrak{T}=(0)$. Therefore, $\operatorname{Ker}\psi$ coincides with $G_{\mathbf{Q}^*}$.

(2) *The Fermat tower* (Example 2, §1 (D)). By Corollary 3 of Theorem 5.1, $k_1=k_2$ holds when L^*/K^* is abelian.

(3) *The modular tower* (Example 3, §1 (D)). By a theorem of Manin-Drinfield [M] [Dr], the assumption for the Corollary of Theorem 5.7 is satisfied in this case.

(4) When $\mathfrak{G}$ is pro-l, put $\mathscr{A}_0=\mathscr{A}\otimes\mathbf{F}_l=\mathbf{F}_l[\![\mathfrak{G}]\!]$, and consider the associative algebra $\operatorname{Gr}\mathscr{A}_0=\bigoplus I_0^m/I_0^{m+1}$, where I_0 denotes the augmentation ideal of $\mathscr{A}_0$. It is clear that if $\operatorname{Gr}\mathscr{A}_0$ has no non-zero element whose square vanishes then it is also the case for $\mathscr{A}$, and hence $k_1=k_2$ holds for any $\mathfrak{G}$-tower L^*/K^* (Corollary 1 of Theorem 5.1). The structure of $\operatorname{Gr}\mathscr{A}_0$ is easier to determine than that of $\mathscr{A}$ itself. In fact, $\operatorname{Gr}\mathscr{A}_0$ is the restricted universal enveloping algebra of the restricted Lie algebra $\bigoplus(\mathfrak{G}(m)/\mathfrak{G}(m+1))$, where $\{\mathfrak{G}(m)\}$ is the Zassenhaus filtration of $\mathfrak{G}$ (cf. [L], Appendix A3). In particular, when $\mathfrak{G}=\mathfrak{F}/\mathfrak{F}(n)$, where $\mathfrak{F}$ is the free pro-l group of rank 2 and $\{\mathfrak{F}(n)\}$ is its central descending series ($\mathfrak{F}=\mathfrak{F}(1)$), $\operatorname{Gr}\mathscr{A}_0$ has an "expected structure" and in particular has no zero-divisors, as has been checked by H. Kamezawa (Master's theses, Univ. Tokyo, 1986). For example, if

$$\mathfrak{G}=\mathfrak{F}/\mathfrak{F}(3)\cong\text{the Heisenberg group over } \mathbf{Z}_l,$$

then $\operatorname{Gr}\mathscr{A}_0$ is the quotient of $\mathbf{F}_l[\![u,v]\!]_{\mathrm{nc}}$ (the non-commutative polynomials in two variables u,v over $\mathbf{F}_l$) by the ideal generated by $[u[u,v]]$ and $[v[u,v]]$. This is easily seen to be free of zero-divisors.

Incidentally, the algebra $\operatorname{Gr}\mathscr{A}_0$ for the groups

$$\mathfrak{G}=\left\{\begin{pmatrix} a & b\\ c & d\end{pmatrix}\in SL_2(\mathbf{Z}_l);\ a\equiv d\equiv 1,\ c\equiv 0 \pmod{l^r}\right\}\dots \qquad \begin{matrix}(l>3 \text{ and } r\geqq 1,\\ \text{or } l=3 \text{ and } r\geqq 2),\end{matrix}$$

$$=\left\{\begin{pmatrix} a & b\\ c & d\end{pmatrix}\in SL_2(\mathbf{Z}_l);\ a\equiv d\equiv 1,\ b\equiv c\equiv 0 \pmod{2}\right\}\Big/\pm I\dots \qquad (l=2),$$

are isomorphic to the above algebra $\operatorname{Gr}\mathscr{A}_0$ for the Heisenberg group. One can apply this to give an alternative proof for $k_1=k_2$ for the modular tower of level $2l^\infty$.

References

[A] Anderson, G.: The hyperadelic gamma function. Adv. Studies in Pure Math. (in press, 1986)

[B] Birman, J.: Braids, links, and mapping class groups. Ann. Math. Studies **82**, Princeton Univ. Press, 1974

[De] Deligne, P.: Formes modulaires et représentations l-adiques. Sém. Bourbaki 68/69, exp. 355; Lecture Notes in Math., vol. 179, pp. 139–186. Berlin-Heidelberg-New York: Springer 1971

[Dr] Drinfeld, V.G.: Two theorems on modular curves. Funct. Anal. Appl. 7-**2**, 155–156 (1973)

[F] Fox, R.H.: Free differential calculus I. Ann. Math. **57**, 547–560 (1953)

[H] Hida, H.: Galois representations into $GL_2(\mathbf{Z}_p[\![x]\!])$ attached to ordinary cusp forms. Invent. Math. **85**, 545–613 (1986)

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

[IKY] Ihara, Y., Kaneko, M., Yulkinari, A.: On some properties of the universal power series for Jacobi sums. Adv. Studies in Pure Math. (in press, 1986)

[K] Kamezawa, H.: Master's thesis. Univ. Tokyo 1985

[L] Lazard, M.: Groupes analytiques p-adiques. Publ. Math. IHES **26**, (1965)

[M] Manin, J.I.: Parabolic points and zeta-functions of modular curves. Izv. Akad. Nauk SSSR Ser Mat. **36**, (1) 19–64 (1972) AMS transl.

[MKS] Magnus, W., Karrass, A., Solitar, D.: Combinatorial group theory. Interscience 1966

[O] Ohta, M.: On l-adic representations attached to automorphic forms. Jap. J. Math. **8**, 1–47 (1982)

[S] Serre, J.-P.: Cohomologie galoisienne. Lecture Notes in Math., vol. 5. Berlin-Heidelberg-New York: Springer 1965

[Sh] Shimura, G.: An l-adic method in the theory of automorphic forms. Preprint 1968

Oblatum 18-II-1986