On Some Properties of the Universal Power Series for Jacobi Sums

Yasutaka Ihara, Masanobu Kaneko and Atsushi Yukinari

Introduction

The subject of this paper is the l-adic power series $F_\rho(u, v)$ in two variables associated to each element ρ of the absolute Galois group $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$ over the rationals, constructed and studied in [PGC]. This was constructed by using pro-l étale coverings of $\boldsymbol{P}^1\backslash\{0, 1, \infty\}$, and was shown to be "universal" for Jacobi sums of l-power exponents. This study was then taken up, also by G. Anderson and R. Coleman, and we now have a deeper understanding of F_ρ. We shall prove two theorems on F_ρ, one on a (non-obvious) functional equation (Theorem A, § 1), and the other, on the determination of the coefficients (Theorem B, § 1) when $\rho \in \mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q}(\boldsymbol{\mu}_{l^\infty}))$. Since these results were also obtained by Anderson and Coleman (see below for details), the stress will be laid on the difference of methods in proofs.

To be more precise, denote by Ω_l the maximum abelian pro-l extension of the cyclotomic field $\boldsymbol{Q}(\boldsymbol{\mu}_{l^\infty})$ unramified outside l, and by Ω_l^{ur} the maximum everywhere unramified subextension of $\Omega_l/\boldsymbol{Q}(\boldsymbol{\mu}_{l^\infty})$;

$$\boldsymbol{Q}\subset\boldsymbol{Q}(\boldsymbol{\mu}_{l^\infty})\subset\Omega_l^{\mathrm{ur}}\subset\Omega_l.$$

Put

$$\mathfrak{g}_0=\mathrm{Gal}(\Omega_l/\boldsymbol{Q})\supset\mathfrak{g}_1=\mathrm{Gal}(\Omega_l/\boldsymbol{Q}(\boldsymbol{\mu}_{l^\infty}))\supset\mathfrak{g}_2=\mathrm{Gal}(\Omega_l/\Omega_l^{\mathrm{ur}}).$$

Then the association $\rho\longrightarrow F_\rho$ factors through a 1-cocycle

$$\mathfrak{g}_0\longrightarrow\mathscr{A}^\times,\qquad \mathscr{A}=\boldsymbol{Z}_l[[u, v]], \tag{1}$$

$\mathscr{A}^\times$ being regarded as a module over $\boldsymbol{Z}_l^\times=\mathfrak{g}_0/\mathfrak{g}_1$ by

$$j_\alpha\colon 1+u\longrightarrow(1+u)^\alpha,\ 1+v\longrightarrow(1+v)^\alpha\qquad(\alpha\in\boldsymbol{Z}_l^\times). \tag{2}$$

As shown in [PGC], the *special values* $F_\rho(\zeta-1, \zeta'-1)$ $(\zeta, \zeta'\in\boldsymbol{\mu}_{l^n}$, ρ: a

Received March 25, 1986.

Frobenius element of $p \neq l$) are connected with Jacobi sums (on 3 parameters $a, b, c \in (Z/l^n)$; $a+b+c=0$), while the *coefficients* of F_ρ are connected with the Kummer characters defined by some circular units in $\boldsymbol{Q}(\boldsymbol{\mu}_{l^\infty})$. An unpublished work of P. Deligne [D], on the construction of a certain circular Kummer character using special type of pro-l étale coverings of $\boldsymbol{P}^1 \setminus \{0, 1, \infty\}$, can be regarded as the determination of some of the coefficients of F_ρ. As for the problem to determine *all* coefficients of F_ρ, the first step is given in [PGC] Theorem 10. It provides the solution when ρ belongs to $\mathfrak{g}_2 = \mathrm{Gal}(\Omega_l/\Omega_l^{\mathrm{ur}})$, the inertia group above l in $\Omega_l/\boldsymbol{Q}(\boldsymbol{\mu}_{l^\infty})$. This gives in particular a factorization

$$F_\rho(u, v) = G_\rho(u)G_\rho(v)G_\rho(w) \qquad ((1+u)(1+v)(1+w)=1) \tag{3}$$

of F_ρ into three pieces when $\rho \in \mathfrak{g}_2$. Moreover, the formula for the coefficients of F_ρ carries over to the case $\rho \in \mathfrak{g}_1$, *provided* that the inertia-restrictions

$$\mathrm{Res}_m : \mathrm{Hom}_{Z_l^\times}(\mathfrak{g}_1, Z_l(m)) \longrightarrow \mathrm{Hom}_{Z_l^\times}(\mathfrak{g}_2, Z_l(m))$$

are *injective* for $m \geq 3$, odd (Corollary of Theorem 10 [PGC]). By Mazur-Wiles [MW], this injectivity is equivalent to the "standard conjecture" on the non-vanishing of $L_l(m, \omega^{1-m})$ (L_l: the l-adic L-function, ω: the Teichmüller character).

The next step was pushed forward by Anderson and by one of us, but Anderson obtained a stronger result. By tieing them in with his previous work [A_1], he proved a generalization of the factorization (3) for all $\rho \in \mathfrak{g}_0$, interpreting each factor (say, $G_\rho(u)$) as a "universal Gauss sum" modulo a power of $1+u$; cf. [A_2] in this Volume. Meanwhile, we also proved, independently and by a fairly different method, that F_ρ is of the form (3) for $\rho \in \mathfrak{g}_1$ (Theorem A_2, § 1). We shall present our proof in Section 2.

The third step, to determine all coefficients of F_ρ *for all* ρ, was made principally by Coleman (yet unpublished). He proved a formula for $\rho \in \mathfrak{g}_1$ during the Kyoto conference in October 1985 (which matches with the above cited conditional result), and later generalized it to all $\rho \in \mathfrak{g}_0$. On the other hand, shortly after October, two of us also succeeded in removing the injectivity assumption for Res_m in Corollary of Theorem 10 [PGC], thus giving an alternative proof for the coefficients-formula when $\rho \in \mathfrak{g}_1$ (Theorem B, § 1). Here, again, the methods are essentially different. While Coleman uses the result of Anderson mentioned above and his own theory of power residue symbols, our proof is based on the $\mathfrak{g}_2$-result in [PGC] and the injectivity of another type of inertia-restrictions explained below.

The formulation of the main results will be given in Section 1 (Theorems A_1, A_2, B). Here, we shall put our stress on the methods. Let $\rho \in \mathfrak{g}_1$. Then we shall show that the "amalgamated product" $F_\rho * F_\rho$ defined by

$$(4)\quad F_\rho(u, v)F_\rho(u', v') \in \boldsymbol{Z}_l[[u, v, u', v']]/[(1+u)(1+v)(1+u')(1+v')-1]$$

is symmetric in u, v, u', v'. This is based on the $\mathfrak{S}_4$-symmetricity of Jacobi sums on 4 parameters $a, b, a', b' \in (\boldsymbol{Z}/l^n)$ with $a+b+a'+b'=0$ $(n \geq 1)$. Then we shall prove that this $\mathfrak{S}_4$-symmetricity of $F_\rho * F_\rho$, combined with other properties of F_ρ already given in [PGC], gives the factorization (3). This study was motivated by a conversation with Deligne (April, 1985), who explained his idea to use amalgamation of two copies of $\pi_1(\boldsymbol{P}^1_{\boldsymbol{C}} \backslash \{0, 1, \infty\})$ along $\pi_1(S^1)$ (in the context of algebraic geometry) to obtain a similar type of restriction to the Galois image in $\mathrm{Aut}\, \pi_1^{\mathrm{pro}\text{-}l}(\boldsymbol{P}^1_{\boldsymbol{Q}} \backslash \{0, 1, \infty\})$. In the present situation, it is carried out by arithmetical means.

Now we indicate our method for the determination of the coefficients of F_ρ $(\rho \in \mathfrak{g}_1)$. By [PGC], F_ρ belongs to the "odd part" $N=(1+uvw\mathscr{A})^-$ of $1+uvw\mathscr{A}$, and hence $\rho \to F_\rho$ can be regarded as an element of $\mathrm{Hom}_{\boldsymbol{Z}_l^\times}(\mathfrak{g}_1, N)$. The proof of Theorem B consists of the following two steps.

(i) Proof of the injectivity of the inertia-restriction

$$\mathrm{Res}_N : \mathrm{Hom}_{\boldsymbol{Z}_l^\times}(\mathfrak{g}_1, N) \longrightarrow \mathrm{Hom}_{\boldsymbol{Z}_l^\times}(\mathfrak{g}_2, N).$$

(ii) Proof that the power series F'_ρ $(\rho \in \mathfrak{g}_1)$ defined by the "expected coefficients for F_ρ" also belongs to N.

Since F_ρ coincides with F'_ρ on $\mathfrak{g}_2$, they must coincide on $\mathfrak{g}_1$.

It was surprising to us that such an injectivity as (i) could be proved. In fact, if we do it *coefficientwise*, then we meet the injectivity of Res_m above, which seems to be much more difficult to prove. The point is as follows. Although N is, in a sense, merely a collection of all $\boldsymbol{Z}_l(m)$, it can also be presented as the projective limit $\varprojlim N^{(n)}$ of such $\boldsymbol{Z}_l[(\boldsymbol{Z}/l^n)^\times]$-modules $N^{(n)}(n \geq 1)$ that (a) each $N^{(n)}$ is l-torsion free, and (b) the injectivity of Res_N ultimately reduces to the vanishing of

$$(5)\qquad \mathrm{Hom}\,(\mathrm{Cl}\,(\boldsymbol{Q}(\boldsymbol{\mu}_{l^n})), N^{(n)})$$

for all $n \geq 1$, where $\mathrm{Cl}\,(\boldsymbol{Q}(\boldsymbol{\mu}_{l^n}))$ is the l-Sylow subgroup of the ideal class group of $\boldsymbol{Q}(\boldsymbol{\mu}_{l^n})$. Since the ideal class groups are finite, (5) vanishes by (a), and the injectivity of Res_N follows by (b). The proof of (ii) is based on a generalization of a lemma of Dwork.

Finally, in Section 4, we discuss some open questions related to the image of $\rho \to F_\rho \pmod{l}$.

We wish to thank G. Anderson, R. Coleman and P. Deligne for stimulating conversations.

§ 1. The main statements

Let l be a fixed rational prime, $\boldsymbol{Z}_l$ be the ring of l-adic integers, and $\mathscr{A}$ be the commutative $\boldsymbol{Z}_l$-algebra of formal power series:

$$\mathscr{A}=\boldsymbol{Z}_l[[u, v]]=\boldsymbol{Z}_l\,[[u, v, w]]/[(1+u)(1+v)(1+w)-1], \tag{1}$$

equipped with the Krull topology. An element of $\mathscr{A}$ will be denoted by $F=F(u, v)$, and also as $F(u, v, w)$ (a representative modulo the ideal $[(1+u)(1+v)(1+w)-1]$). Let $G_{\boldsymbol{Q}}=\mathrm{Gal}\,(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$ be the absolute Galois group over $\boldsymbol{Q}$, $\chi: G_{\boldsymbol{Q}}\to\boldsymbol{Z}_l^\times$ be the l-cyclotomic character describing the action of $G_{\boldsymbol{Q}}$ on the group $\boldsymbol{\mu}_{l^\infty}$ of l-power roots of unity in $\bar{\boldsymbol{Q}}$, and let $G_{\boldsymbol{Q}}$ act on $\mathscr{A}$ via the $\boldsymbol{Z}_l^\times$-action j_α: $1+u\to(1+u)^\alpha$, $1+v\to(1+v)^\alpha$, $1+w\to(1+w)^\alpha$ ($\alpha\in\boldsymbol{Z}_l^\times$). In [PGC], we constructed a continuous 1-cocycle

$$G_{\boldsymbol{Q}}\longrightarrow\mathscr{A}^\times \qquad (\rho\longrightarrow F_\rho=F_\rho(u, v, w)). \tag{2}$$

It is unramified outside l, and is "universal" for Jacobi sums on 3 parameters $a, b, c\in(\boldsymbol{Z}/l^n)$ with $a+b+c=0$. This 1-cocycle depends on the choice of a "coordinate system ι" related to $\pi_1^{\text{pro-}l}(\boldsymbol{P}^1\backslash\{0, 1, \infty\})$ (loc. cit I § 2), but its restriction to $G_{\boldsymbol{Q}(\mu_{l^\infty})}=\mathrm{Gal}\,(\bar{\boldsymbol{Q}}/\boldsymbol{Q}(\boldsymbol{\mu}_{l^\infty}))$, which is a continuous *homomorphism*

$$G_{\boldsymbol{Q}(\mu_{l^\infty})}\longrightarrow 1+uvw\mathscr{A}\subset\mathscr{A}^\times, \tag{3}$$

depends only on the choice of a basis $(\zeta_n)_{n\geq 1}$ of $T_l(\boldsymbol{G}_m)=\varprojlim_n\boldsymbol{\mu}_{l^n}$ (which is subject to ι).

For each $F=F(u, v)\in\mathscr{A}$, define $F*F$ to be the element of

$$\mathscr{A}*\mathscr{A}=\boldsymbol{Z}_l[[u, v, u', v']]/[(1+u)(1+v)(1+u')(1+v')-1]$$

represented by the product $F(u, v)F(u', v')$. (This algebra $\mathscr{A}*\mathscr{A}$ is a sort of "completed *amalgamated* free product $\mathscr{A}\hat{*}_{\boldsymbol{Z}_l[[w]]}\mathscr{A}$", but we denote it simply as $\mathscr{A}*\mathscr{A}$, for brevity of notations.) The first formulation of our first theorem is as follows.

Theorem A_1. *Let $\rho\in G_{\boldsymbol{Q}(\mu_{l^\infty})}$. Then $F_\rho\in\mathscr{A}$ is symmetric in u, v, w, and $F_\rho*F_\rho\in\mathscr{A}*\mathscr{A}$ is symmetric in u, v, u', v'.*

We shall show that these symmetricities w.r.t. $\mathfrak{S}_3$ and $\mathfrak{S}_4$ follow from the corresponding symmetricities of Jacobi sums (§ 2). The first symme-

tricity also allows a direct proof based on the definition of F_ρ. As for the second, the author learned that G. Anderson recently obtained it independently by a different method. Further symmetricities of Jacobi sums ($\mathfrak{S}_{r+1}$-symmetricity of the Jacobi sum on $r+1$ parameters $a_0, \cdots, a_r \in (Z/l^n)$ for $r \geq 4$) do *not* give any more new functional equations for F_ρ.

To state the second formulation of this theorem, change variables as

$$(4) \quad 1+u=\exp U,\ 1+v=\exp V,\ 1+w=\exp W \qquad (U+V+W=0).$$

Then

Theorem A_2. *Let $\rho \in G_{Q(\mu_{l^\infty})}$. Then F_ρ has an expansion of the form*

$$(5) \qquad F_\rho(u, v, w)=\exp \sum_{\substack{m\geq 3\\ odd}} \frac{\beta_m(\rho)}{m!}(U^m+V^m+W^m)$$

with $\beta_m(\rho) \in \boldsymbol{Z}_l$ ($m \geq 3$, odd).

This was obtained also by G. Anderson, independently, by a different method [A_2].

The next theme is the explicit determination of the coefficients $\beta_m(\rho)$ ($m \geq 3$, *odd*). Let Ω_l be the maximum *abelian* pro-l extension of $\boldsymbol{Q}(\boldsymbol{\mu}_{l^\infty})$ unramified outside l, and Ω_l^{ur} be the maximum everywhere unramified subextension of $\Omega_l/\boldsymbol{Q}(\boldsymbol{\mu}_{l^\infty})$. Put

$$(6) \qquad \mathfrak{g}_0=\mathrm{Gal}\,(\Omega_l/\boldsymbol{Q}) \supset \mathfrak{g}_1=\mathrm{Gal}\,(\Omega_l/\boldsymbol{Q}(\boldsymbol{\mu}_{l^\infty})) \supset \mathfrak{g}_2=\mathrm{Gal}\,(\Omega_l/\Omega_l^{\mathrm{ur}}).$$

Then $\mathfrak{g}_0/\mathfrak{g}_1=\mathrm{Gal}\,(\boldsymbol{Q}(\boldsymbol{\mu}_{l^\infty})/\boldsymbol{Q})$ can be identified with $\boldsymbol{Z}_l^\times$ via the l-cyclotomic character, and $\mathfrak{g}_1$, $\mathfrak{g}_2$ can be regarded as $\boldsymbol{Z}_l^\times$-modules via $(\mathfrak{g}_0/\mathfrak{g}_1)$-conjugation $g_1 \to g_0 g_1 g_0^{-1}$ ($g_0 \in \mathfrak{g}_0$, $g_1 \in \mathfrak{g}_1$). By [PGC] Section IV, the association $\rho \to F_\rho$ factors through a $\boldsymbol{Z}_l^\times$-homomorphism

$$(7) \qquad F\colon \mathfrak{g}_1 \longrightarrow N=(1+uvw\mathscr{A})^-=\{F \in \mathscr{A};\ F \equiv 1 \pmod{uvw},\ F\bar{F}=1\},$$

where $\bar{F}=F^{j-1}$. Accordingly, β_m ($m \geq 3$, *odd*) belongs to

$$(8) \qquad \mathrm{Hom}_{\boldsymbol{Z}_l^\times}(\mathfrak{g}_1, \boldsymbol{Z}_l(m)).$$

Now let χ_m ($m=0, 1, 2, \cdots$) be the standard element of (8) defined in [PCG] IV Section 7. Namely, put

$$(9) \qquad \varepsilon_n^{(m)}=\prod_{a \in (\boldsymbol{Z}/l^n)^\times} (\zeta_n^a-1)^{\langle a^{m-1}\rangle_n} \in \boldsymbol{Q}(\boldsymbol{\mu}_{l^n}) \qquad (n \geq 1,\ m \geq 0),$$

where $(\zeta_n)_{n\geq 1}$ is as above, and $\langle b \rangle_n$ denotes the unique integer in the

interval $[0, l^n)$ representing $b \bmod l^n$. Then χ_m is the unique homomorphism $\mathfrak{g}_1 \to \boldsymbol{Z}_l$ satisfying the equality

$$\zeta_n^{\chi_m(\rho)} = ((\varepsilon_n^{(m)})^{1/l^n})^{\rho - 1} \qquad \text{for all } \rho \in \mathfrak{g}_1,\ n \geq 1. \tag{10}$$

Theorem B. *The notation being as in Theorem* A_2,

$$\beta_m(\rho) = (1 - l^{m-1})^{-1} \chi_m(\rho) \qquad (m \geq 3,\ \textit{odd}) \tag{11}$$

holds for all $\rho \in \mathfrak{g}_1 = \mathrm{Gal}\,(\Omega_l / \boldsymbol{Q}(\boldsymbol{\mu}_{l^\infty}))$.

As explained in the Introduction, this was proved for $\rho \in \mathfrak{g}_2$ in [PGC] Theorem 10, and more recently, for $\rho \in \mathfrak{g}_1$ by Coleman. Note that a result of Deligne [D], combined with Theorem A_2, also gives the same formula (at least) for $m < l$ (cf. also [PGC] IV § 7). The method for our proof, given in Section 3, is totally different from these.

From Theorem B follows in particular that the Vandiver conjecture for l is valid if and only if β_m is surjective for all $m = 3, 5, \cdots, l-2$ $(l > 3)$.

§ 2. Proof of Theorems A_1, A_2.

Proof of Theorem A_1. Let $(\zeta_n)_{n \geq 1}$ be the basis of $T_l(\boldsymbol{G}_m)$ which determines the homomorphism (3) of Section 1. (Each ζ_n is a primitive element of $\boldsymbol{\mu}_{l^n}$, and $\zeta_{n+1}^l = \zeta_n$ $(n \geq 1)$.) For each $n \geq 1$, denote by $\mathscr{L}_n$ the set of all ordered triples (a, b, c) such that $a, b, c \in (Z/l^n) \setminus (0)$, $a+b+c = 0$, and such that at least one of a, b, c belongs to $(Z/l^n)^\times$. For $F = F(u, v, w) \in \mathscr{A}$ and $(a, b, c) \in \mathscr{L}_n$ $(n \geq 1)$, the special value

$$F(\zeta_n^a - 1, \zeta_n^b - 1, \zeta_n^c - 1) \tag{1}$$

is well-defined, because $a+b+c = 0$ (and the series obviously converges). We shall first prove the following two statements (I), (II) for any $\rho \in G_{\boldsymbol{Q}(\mu_{l^\infty})}$ and $n \geq 1$:

(I) $F_\rho(\zeta_n^a - 1, \zeta_n^b - 1, \zeta_n^c - 1)$, for $(a, b, c) \in \mathscr{L}_n$, is symmetric in a, b, c.

(II) Let $a, a', b, b' \in (\boldsymbol{Z}/l^n)$ be such that

$$a + a' + b + b' = 0$$
$$b, b' \not\equiv 0 \pmod{l},$$
$$a, a' \equiv 0 \pmod{l}, \text{ but } a, a' \neq 0;$$

(hence necessarily $n \geq 2$). Then

$$\begin{aligned} &F_\rho(\zeta_n^a - 1, \zeta_n^b - 1) F_\rho(\zeta_n^{a'} - 1, \zeta_n^{b'} - 1) \\ &\quad = F_\rho(\zeta_n^{a'} - 1, \zeta_n^b - 1) F_\rho(\zeta_n^a - 1, \zeta_n^{b'} - 1). \end{aligned} \tag{2}$$

In fact, for each fixed $n \geq 1$, we shall prove the statements of (I) (II) for all $\rho \in G_{\boldsymbol{Q}(\mu_{l^n})}$ (resp. $G_{\boldsymbol{Q}(\mu_{l^{n+1}})}$ when $l=2$). By continuity, it suffices to prove them when ρ is a Frobenius element of a prime divisor $\mathfrak{p}$ of $\boldsymbol{Q}(\mu_{l^n})$ such that $\mathfrak{p} \nmid l$. But for such ρ, $F_\rho(\zeta_n^a-1, \zeta_n^b-1, \zeta_n^c-1)$ $((a, b, c) \in \mathscr{L}_n)$ is, by Theorem 7 of [PGC] II Section 6, the Jacobi sum:

$$
\begin{aligned}
F_\rho(\zeta_n^a-1, \zeta_n^b-1, \zeta_n^c-1) &= -\sum_{\substack{x,y \in \boldsymbol{F}_q^\times \\ x+y+1=0}} \lambda_n(x)^a \lambda_n(y)^b \\
&= \frac{-1}{q-1} \sum_{\substack{x,y,z \in \boldsymbol{F}_q^\times \\ x+y+z=0}} \lambda_n(x)^a \lambda_n(y)^b \lambda_n(z)^c,
\end{aligned} \tag{3}
$$

where $q=N(\mathfrak{p})$, $\boldsymbol{F}_q$ is the finite field $\boldsymbol{Z}[\zeta_n]/\mathfrak{p}$, and $\lambda_n: \boldsymbol{F}_q^\times \to \boldsymbol{\mu}_{l^n}$ is the Teichmüller character determined by

$$
\lambda_n(x) \equiv x^{(q-1)/l^n} \pmod{\mathfrak{p}} \qquad (x \in \boldsymbol{F}_q^\times).
$$

Note that $\lambda_n(-1)=1$, because when $l=2$, we assumed $\rho \in G_{\boldsymbol{Q}(\mu_{l^{n+1}})}$ and hence $q \equiv 1 \pmod{l^{n+1}}$. Since the right side of (3) is symmetric in a, b, c, (I) follows.

Now, to prove (II) when ρ is a Frobenius element of $\mathfrak{p}$, let a, b, a', b' be as in (II). Then all the 4 triples

$$
(a, b, -a-b), (a', b', -a'-b'), (a', b, -a'-b), (a, b', -a-b')
$$

belong to $\mathscr{L}_n$, because $a+b, a'+b', a'+b, a+b' \not\equiv 0 \pmod{l}$; hence in particular $\neq 0$. Therefore, the formula

$$
F_\rho(\zeta_n^\alpha-1, \zeta_n^\beta-1) = -\sum_{\substack{x,y \in \boldsymbol{F}_q^\times \\ x+y+1=0}} \lambda_n(x)^\alpha \lambda_n(y)^\beta \tag{4}
$$

is valid for $(\alpha, \beta)=(a, b), (a', b'), (a', b), (a, b')$. On the other hand,

$$
\begin{aligned}
&\sum_{\substack{x,y,x',y' \in \boldsymbol{F}_q^\times \\ x+y+x'+y'=0}} \lambda_n(x)^a \lambda_n(y)^b \lambda_n(x')^{a'} \lambda_n(y')^{b'} \\
&\quad = \sum_{z \in \boldsymbol{F}_q} \Big\{ \sum_{\substack{x+y=z \\ x,y \neq 0}} \lambda_n(x)^a \lambda_n(y)^b \cdot \sum_{\substack{x'+y'=-z \\ x',y' \neq 0}} \lambda_n(x')^{a'} \lambda_n(y')^{b'} \Big\}.
\end{aligned} \tag{5}
$$

Since λ_n is surjective and $a+b, a'+b' \neq 0$, the summand for $z=0$ vanishes; hence (5) is equal to the sum over $z \in \boldsymbol{F}_q^\times$. The summand for each $z \in \boldsymbol{F}_q^\times$ may be rewritten as

$$\sum_{\substack{x+y=-1\\ x,y\neq 0}} \lambda_n(-xz)^a \lambda_n(-yz)^b \cdot \sum_{\substack{x'+y'=-1\\ x',y'\neq 0}} \lambda_n(x'z)^{a'} \lambda_n(y'z)^{b'},$$

which is independent of z, as $a+b+a'+b'=0$. And since $\lambda_n(-1)=1$, (5) is equal to

$$(5') \qquad \begin{aligned} &(q-1)\sum_{\substack{x+y=-1\\ x,y\neq 0}} \lambda_n(x)^a \lambda_n(y)^b \cdot \sum_{\substack{x'+y'=-1\\ x',y'\neq 0}} \lambda_n(x')^{a'} \lambda_n(y')^{b'} \\ &\quad = (q-1)F_\rho(\zeta_n^a - 1, \zeta_n^b - 1)F_\rho(\zeta_n^{a'} - 1, \zeta_n^{b'} - 1). \end{aligned}$$

Since (5) is a priori symmetric in a, b, a', b', and (4) holds for $(\alpha, \beta) = (a', b), (a, b')$, we deduce that (5′) is also equal to

$$(5'') \qquad (q-1)F_\rho(\zeta_n^{a'} - 1, \zeta_n^b - 1)F_\rho(\zeta_n^a - 1, \zeta_n^{b'} - 1).$$

This gives the proof of (II).

$\mathfrak{S}_3$-symmetricity. In [PGC] II, we studied the ideals

$$(6) \qquad \begin{aligned} \mathfrak{a}_m = \{&F = F(u, v, w) \in \mathscr{A};\ F(\zeta - 1, \zeta' - 1, \zeta'' - 1) = 0, \\ &\text{for all } \zeta, \zeta', \zeta'' \in \boldsymbol{\mu}_{l^m} \backslash \{1\} \text{ with } \zeta\zeta'\zeta'' = 1\} \end{aligned}$$

($m \geq 1$) of $\mathscr{A}$ and in particular proved that $\bigcap_{m\geq 1} \mathfrak{a}_m = (0)$ (cf. II § 4(14), § 1 (16)). Now the property (I) proved above for all $n \leq m$ implies that if $\rho \in G_{Q(\mu_{l^\infty})}$ and σ is any substitution of three letters u, v, w, then

$$F_\rho(u, v, w) - F_\rho(\sigma u, \sigma v, \sigma w)$$

belongs to $\mathfrak{a}_m$. Since $m \geq 1$ is arbitrary, this must vanish. Therefore, $F_\rho(u, v, w)$, as an element of $\mathscr{A}$, is symmetric in u, v, w.

$\mathfrak{S}_4$-symmetricity. Let u, u', v be 3 independent variables, and define $v' \in Z_l[[u, u', v]]$ by the equality

$$(1+u)(1+u')(1+v)(1+v') = 1.$$

(Note that v' has no constant term.) To prove the $\mathfrak{S}_4$-symmetricity of $F_\rho * F_\rho$ (for $\rho \in G_{Q(\mu_{l^\infty})}$), it suffices to prove that

$$(7) \qquad F_\rho(u, v)F_\rho(u', v') = F_\rho(u', v)F_\rho(u, v') \qquad (\rho \in G_{Q(\mu_{l^\infty})})$$

holds in $Z_l[[u, u', v]]$, because $\mathfrak{S}_4$ (on u, u', v, v') is generated by 3 transpositions $u \leftrightarrow v$, $u' \leftrightarrow v'$, and $u \leftrightarrow u'$. (These transpositions generate a transitive subgroup containing "$\mathfrak{S}_3$ on u, u', v", the full stabilizer of v'.) Now, to prove (7), fix ρ and put

$$G(u, u', v)=F_\rho(u, v)F_\rho(u', v')-F_\rho(u', v)F_\rho(u, v')$$
$$=\sum_{i=0}^{\infty} H_i(u, u')v^i,$$

with $H_i(u, u') \in Z_l[[u, u']]$. Then, by (II),

$$G(\zeta_n^a-1, \zeta_n^{a'}-1, \zeta_n^b-1)=0$$

holds as long as $a, a' \in (Z/l^n)\backslash(0)$, $b \in (Z/l^n)^\times$ and $a, a' \equiv 0 \pmod{l}$. (Note that $b'=-a-a'-b \not\equiv 0 \pmod{l}$.) So, if we fix $m \geq 1$ and $\alpha, \alpha' \in (Z/l^m)\backslash(0)$, and take $n=m+k$ $(k=1, 2, \cdots)$ and $a=l^k\alpha$, $a'=l^k\alpha'$ (the image of α, α' by the l^k-multiplication map $(\boldsymbol{Z}/l^m) \to (\boldsymbol{Z}/l^n)$), then

$$G(\zeta_m^\alpha-1, \zeta_m^{\alpha'}-1, \zeta_{m+k}^b-1)=0$$

for all $k \geq 1$ and $b \in (Z/l^{m+k})^\times$. But then, $G(\zeta_m^\alpha-1, \zeta_m^{\alpha'}-1, v)$, vanishes at $v=\zeta-1$ for infinitely many distinct values of $\zeta \in \boldsymbol{\mu}_{l^\infty}$. By Lemma 1 below, this implies that $G(\zeta_m^\alpha-1, \zeta_m^{\alpha'}-1, v)=0$, i.e., $H_i(\zeta_m^\alpha-1, \zeta_m^{\alpha'}-1)=0$ for each $i \geq 0$. This implies in particular that $H_i \in \mathfrak{a}_m$. Since $m \geq 1$ is arbitrary, this gives $H_i \in \bigcap_{m\geq 1} \mathfrak{a}_m=(0)$, all i. Therefore, $G=0$. This gives (7), and hence completes the proof of Theorem A_1.

Lemma 1. *Let k be a finite extension of $\boldsymbol{Q}_l$, $\mathfrak{o}$ be the ring of integers of k, and $G(u) \in \mathfrak{o}[[u]]$ be a formal power series of one variable over $\mathfrak{o}$. Suppose $G(\zeta-1)=0$ for infinitely many distinct elements ζ of $\boldsymbol{\mu}_{l^\infty}$. Then $G=0$.*

Proof. This is well-known, and can be verified immediately as follows. Suppose on the contrary that $G(u)=\sum_{i\geq 0} a_i u^i \neq 0$ $(a_i \in \mathfrak{o})$, and let i_0 be the smallest integer ≥ 0 such that $\mathrm{ord}_k(a_{i_0})=\mathrm{Min}_i\, \mathrm{ord}_k(a_i)$ (ord_k: the normalized additive valuation of k). Take n (≥ 1) so large that

$$l^{n-1} > i_0(l-1)^{-1}\, \mathrm{ord}_k\, l,$$

and let $\zeta \in \boldsymbol{\mu}_{l^\infty}$ be of order exactly l^n. Then

$$\mathrm{ord}_k(\zeta-1)^{i_0}=i_0(l^n-l^{n-1})^{-1}\, \mathrm{ord}_k\, l<1.$$

But then, it is easy to see that

$$\mathrm{ord}_k(a_{i_0}(\zeta-1)^{i_0}) < \mathrm{ord}_k(a_i(\zeta-1)^i), \qquad \text{all } i \neq i_0. \tag{8}$$

Therefore, $G(\zeta-1) \neq 0$, for all such ζ, a contradiction. q.e.d.

Proof of Theorem A_2. For each $F=F(u, v) \in \mathscr{A}$ with $F(0, 0)=1$, define its logarithm by $\log F=\sum_{m\geq 1}(-1)^{m-1}(F-1)^m/m$, and consider it as

an element of $\boldsymbol{Q}_l[[U, V]]$, where $U=\log(1+u)$, $V=\log(1+v)$. The involutive automorphism of $\mathscr{A}$ defined by $1+u\to(1+u)^{-1}$, $1+v\to(1+v)^{-1}$ (i.e., $U\to -U$, $V\to -V$) is denoted by the bar sign $*\to\bar{*}$. We shall reduce Theorem A_2 to:

Proposition 1. *Let* $F=F(u, v)\in\mathscr{A}$. *Then the following conditions* (i) (ii) *are equivalent*;

(i) $$F\equiv 1 \pmod{uvw},$$

$$F\cdot\bar{F}=1,$$

$$F \text{ is symmetric in } u, v, w,$$

$$F*F \text{ is symmetric in } u, v, u', v';$$

(ii) $\log F$ *is of the form*

$$\log F=\sum_{\substack{m\geq 3\\ odd}}\frac{\beta_m}{m!}(U^m+V^m+W^m), \tag{9}$$

where $W=-(U+V)$, $\beta_m\in\boldsymbol{Z}_l$.

Remark. As the following proof shows, (i) is also equivalent to an apparently weaker condition:

(i)′ $$F\equiv 1 \pmod{uv},$$

$$F(u, v)F(u', v')\equiv F(u', v)F(u, v') \bmod [(1+u)(1+v)(1+u')(1+v')-1].$$

When $F=F_\rho$ ($\rho\in G_{\boldsymbol{Q}(\mu_{l^\infty})}$), the first two properties in (i) are proved in [PGC], and the last two are given by Theorem A_1. Thus, Theorem A_2 is reduced to Proposition 1.

Proof of Proposition 1. We shall only prove the implication (i)′→(ii) (the implication (ii)→(i)→(i)′ is obvious). From the first congruence of (i)′ follows that $\log F$ is divisible by UV. Hence $\log F$ is of the form

$$-\sum_{i,j\geq 1}\frac{\beta_{ij}}{i!j!}U^iV^j, \tag{10}$$

with $\beta_{ij}\in\boldsymbol{Z}_l$. (That β_{ij} is integral follows automatically from the integrality of the coefficients of $F(u, v)$; cf. [PGC] IV § 2.) So, it remains to show, from the second congruence of (i)′, that β_{ij} *depends only on* $m=i+j$ and vanishes when m is even. This is immediately reduced to the following

Lemma 2. *Let m be a positive integer, and $g(x, y)$ be a homogeneous polynomial of degree m over a field of characteristic 0. Then, if m is odd, the following two conditions* (i) (ii) *are equivalent;*

(i) $g(x, y)$ *satisfies*

(*) $g(x, 0)=g(0, y)=0$,

(**) $g(x, y)+g(x', y')\equiv g(x', y)+g(x, y') \bmod (x+x'+y+y')$;

(ii) $g(x, y)$ *is a constant multiple of* $(x+y)^m-x^m-y^m$.

If m is even, the condition (i) *implies* $g(x, y)=0$.

Proof. The implication (ii)→(i) (for m: odd) is straightforward. To prove the rest, let $g(x, y)$ satisfy (i), and write

$$g(x, y)=\sum_{\substack{i,j\geq 0\\ i+j=m}} b_j x^i y^j, \qquad \text{and } \beta_j=i!j!b_j. \tag{11}$$

Then $b_0=b_m=0$, by (*). The congruence (**) says that the polynomial

$$g(x, y)+g(x', -x-x'-y) \tag{12}$$

is symmetric in x, x'. Therefore, the coefficient of y^j in (12) for each j, given by the formula below, is symmetric in x, x'.

$$\begin{aligned} &b_j x^i+\sum_{j\leq l\leq m} b_l(-1)^l\binom{l}{j}(x+x')^{l-j}x'^{m-l} \\ &\quad=b_j x^i+\sum_{0\leq p\leq i}\left\{b_{j+p}(-1)^{j+p}\binom{j+p}{j}\cdot\sum_{\mu=0}^{p}\binom{p}{\mu}x^\mu x'^{i-\mu}\right\} \end{aligned} \tag{13}$$

(put $l=j+p$). For $\mu, \nu\geq 0$, $\mu+\nu=i$, the coefficient of $x^\mu x'^\nu$ in the second term of (13) is given by

$$\begin{aligned} &\sum_{\mu\leq p\leq i}(-1)^{j+p}\binom{j+p}{j}\binom{p}{\mu}b_{j+p} \qquad (\text{put } q=i-p) \\ &\quad=\sum_{0\leq q\leq \nu}(-1)^{m-q}\binom{m-q}{j}\binom{i-q}{\mu}b_{m-q}=\frac{(-1)^m}{j!\mu!\nu!}\gamma_\nu, \end{aligned} \tag{14}$$

with

$$\gamma_\nu=\sum_{0\leq q\leq \nu}(-1)^q\binom{\nu}{q}\beta_{m-q} \tag{15}$$

(β_{m-q}, as in (11).) But since (13) is symmetric in x, x', (14) must be symmetric in μ, ν, unless μ or $\nu=0$ (this exception, as we have not yet taken the first term $b_j x^i$ in (13) into account). Therefore, $\gamma_\nu=\gamma_{i-\nu}$ for all ν, with $0<\nu<i$. Therefore, $\gamma_1=\gamma_{i-1}$ for $2\leq i\leq m$; hence

(16) $$\gamma_1=\gamma_2=\cdots=\gamma_{m-1}\overset{\text{put}}{=}\gamma.$$

Moreover, the coefficients of x^i and of x'^i in (13) must be equal; hence we obtain (noting that $b_0=b_m=0$):

$$b_j=\frac{(-1)^m}{i!j!}\gamma_i \qquad (i,j>0,\ i+j=m).$$

Therefore,

(17) $$\beta_j=(-1)^m\gamma_i \qquad (0<i<m).$$

Therefore, (16) gives

(18) $$\beta_1=\beta_2=\cdots=\beta_{m-1}\overset{\text{put}}{=}\beta.$$

Since $\beta_0=\beta_m=0$, we obtain

$$g(x,y)=\beta\cdot\sum_{\substack{i,j\geq 1\\ i+j=m}}\frac{x^iy^j}{i!j!}=\frac{\beta}{m!}((x+y)^m-x^m-y^m).$$

On the other hand, (15) and (18) gives $\gamma=-\beta$, and (17) gives $\beta=(-1)^m\gamma$. Therefore, $\beta=0$ when m is even. q.e.d.

§ 3. Proof of Theorem B

We may assume that l is odd. Indeed, 2 is a regular prime, and when l is regular the theorem is already established in [PGC] IV Corollary of Theorem 10.

Let $N=(1+uvw\mathscr{A})^-$ be the closed subgroup of $\mathscr{A}^\times$ defined by Section 1 (7). It is abelian, pro-l (cf. [PGC] III), and can be regarded also as a $\boldsymbol{Z}_l^\times$-submodule of $\mathscr{A}^\times$. A crucial point in our proof of Theorem B is the following

Key lemma. *The inertia-restriction*

(1) $$\mathrm{Hom}_{\boldsymbol{Z}_l^\times}(\mathfrak{g}_1, N)\longrightarrow\mathrm{Hom}_{\boldsymbol{Z}_l^\times}(\mathfrak{g}_2, N)$$

is injective.

In the proof of this lemma, the crucial and the only arithmetic point is the following Lemma 3. To state this, let $\mathfrak{a}_n$ ($n\geq 1$) be the ideal of $\mathscr{A}$ described in Section 2, i.e.,

(2) $$\mathfrak{a}_n=\{F=F(u,v,w)\in\mathscr{A};\ F(\zeta-1,\zeta'-1,\zeta''-1)=0 \text{ for all } \zeta,\zeta',\zeta''\in\boldsymbol{\mu}_{l^n}\backslash\{1\} \text{ with } \zeta\zeta'\zeta''=1\}$$

Clearly, $\mathfrak{a}_n$ contains $(1+u)^{l^n}-1$ and $(1+v)^{l^n}-1$; hence j_α for $\alpha \in 1+l^n\boldsymbol{Z}_l$ acts trivially on $\mathscr{A}/\mathfrak{a}_n$; hence the $\boldsymbol{Z}_l^\times$-action on $\mathscr{A}$ induces a $(\boldsymbol{Z}/l^n)^\times$-action on $\mathscr{A}/\mathfrak{a}_n$. Put

$$N_n = N \cap (1+\mathfrak{a}_n) = N \cap (1+uvw\mathfrak{a}_n). \tag{3}$$

Then N_n is a closed $\boldsymbol{Z}_l^\times$-stable subgroup of N, and the quotient N/N_n is a pro-l abelian group which is at the same time a $(\boldsymbol{Z}/l^n)^\times$-module. By [PGC] IV Section 4 lemma 2 (U. Jannsen), *the group N/N_n has no l-torsion.* (In fact N/N_n is a subgroup of $\Psi_1^{(n)}$.) Consider N/N_n as a $(\mathfrak{g}_0/\mathfrak{g}_2)$-module *via* the projection

$$\mathfrak{g}_0/\mathfrak{g}_2 \longrightarrow \mathfrak{g}_0/\mathfrak{g}_1 = \boldsymbol{Z}_l^\times \longrightarrow (\boldsymbol{Z}/l^n)^\times. \tag{4}$$

Lemma 3.

$$H^1(\mathfrak{g}_0/\mathfrak{g}_2,\ N/N_n) = 0 \qquad (n \geq 1).$$

(*The cohomology groups are those defined by continuous cocycles.*)

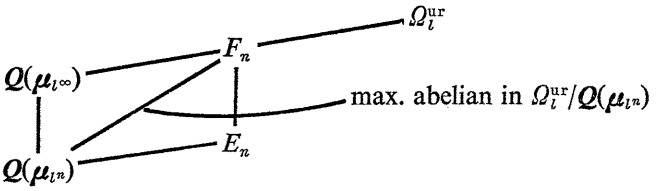
Proof of Lemma 3. Call $(\mathfrak{g}_0/\mathfrak{g}_2)_n$ the kernel of the composite homomorphism (4). Then we have an inflation-restriction exact sequence

$$\begin{aligned} 0 \longrightarrow H^1((\boldsymbol{Z}/l^n)^\times,\ N/N_n) &\longrightarrow H^1((\mathfrak{g}_0/\mathfrak{g}_2),\ N/N_n) \\ &\longrightarrow \mathrm{Hom}_{(\boldsymbol{Z}/l^n)^\times}((\mathfrak{g}_0/\mathfrak{g}_2)_n^{\mathrm{ab}},\ N/N_n), \end{aligned} \tag{5}$$

where $(\mathfrak{g}_0/\mathfrak{g}_2)_n^{\mathrm{ab}}$ is the abelianization of $(\mathfrak{g}_0/\mathfrak{g}_2)_n$. So, to prove Lemma 3, it suffices to prove that the two groups on both sides of $H^1((\mathfrak{g}_0/\mathfrak{g}_2),\ N/N_n)$ vanish.

(I) That $\mathrm{Hom}_{(\boldsymbol{Z}/l^n)^\times}((\mathfrak{g}_0/\mathfrak{g}_2)_n^{\mathrm{ab}},\ N/N_n) = 0$. This is the crucial part. The abelianization $(\mathfrak{g}_0/\mathfrak{g}_2)_n^{\mathrm{ab}}$ of $(\mathfrak{g}_0/\mathfrak{g}_2)_n$ is nothing but the Galois group of the maximum abelian subextension $F_n/\boldsymbol{Q}(\boldsymbol{\mu}_{l^n})$ of $\Omega_l^{\mathrm{ur}}/\boldsymbol{Q}(\boldsymbol{\mu}_{l^n})$. But F_n is nothing but the composite of $\boldsymbol{Q}(\boldsymbol{\mu}_{l^\infty})$ with the maximum unramified abelian pro-l extension E_n of $\boldsymbol{Q}(\boldsymbol{\mu}_{l^n})$:

(6)



In fact, it is clear that $E_n \subset F_n$ and that E_n is the maximum unramified subextension of $F_n/\boldsymbol{Q}(\boldsymbol{\mu}_{l^n})$. Therefore, E_n corresponds to the inertia group above $(\zeta_n - 1)$ in $F_n/\boldsymbol{Q}(\boldsymbol{\mu}_{l^n})$. Since the intersection of this inertia group

with $\mathrm{Gal}(F_n/\boldsymbol{Q}(\mu_{l^\infty}))$ is trivial ($F_n/\boldsymbol{Q}(\mu_{l^\infty})$ being unramified), we obtain $E_n \cdot \boldsymbol{Q}(\mu_{l^\infty}) = F_n$. Since $E_n \cap \boldsymbol{Q}(\mu_{l^\infty}) = \boldsymbol{Q}(\mu_{l^n})$,

$$\mathrm{Gal}(F_n/\boldsymbol{Q}(\mu_{l^n})) = \mathrm{Gal}(F_n/E_n) \times \mathrm{Gal}(F_n/\boldsymbol{Q}(\mu_{l^\infty})).$$

Therefore, to prove (I), it suffices to prove that

$$\begin{aligned}(7)\qquad &\mathrm{Hom}_{(\boldsymbol{Z}/l^n)^\times}(\mathrm{Gal}(F_n/\boldsymbol{Q}(\mu_{l^\infty}), N/N_n) \\ &= \mathrm{Hom}_{(\boldsymbol{Z}/l^n)^\times}(\mathrm{Gal}(F_n/E_n), N/N_n) = 0.\end{aligned}$$

Since $[F_n : \boldsymbol{Q}(\mu_{l^\infty})] = [E_n : \boldsymbol{Q}(\mu_{l^n})]$ is a *finite* power of l, being equal to the l-component of the class number of $\boldsymbol{Q}(\mu_{l^n})$, and since N/N_n *has no l-torsion*, as noted above, the first group of (7) must vanish. As for the second, since $(\boldsymbol{Z}/l^n)^\times$ acts trivially on $\mathrm{Gal}(F_n/E_n)$, it suffices to prove that N/N_n has no non-trivial $(\boldsymbol{Z}/l^n)^\times$-invariant element. But N being the *odd* part $(1+uvw\mathscr{A})^-$ of $1+uvw\mathscr{A}$, $(-1) \in (\boldsymbol{Z}/l^n)^\times$ acts on N/N_n (considered as an additive group) as the (-1)-multiplication. On the other hand, N/N_n is pro-l, with $l \neq 2$; hence the 2-multiplication on N/N_n is invertible. Therefore, N/N_n has no non-zero (-1)-invariant element; hence in particular no non-zero $(\boldsymbol{Z}/l^n)^\times$-invariant element. Therefore, the second group of (7) also reduces to 0. This settles (I).

(II) That $H^1((\boldsymbol{Z}/l^n)^\times, N/N_n) = 0$. Put $G = (\boldsymbol{Z}/l^n)^\times$, and call T its subgroup of order $l-1$. Then the group exact sequence $1 \to T \to G \to G/T \to 1$ gives the inflation-restriction exact sequence

$$(8)\qquad 0 \longrightarrow H^1(G/T, (N/N_n)^T) \longrightarrow H^1(G, N/N_n) \longrightarrow H^1(T, N/N_n).$$

As $T \ni -1$, the above argument gives $(N/N_n)^T = 0$. On the other hand, since N/N_n is pro-l and $|T| = l-1 \in \boldsymbol{Z}_l^\times$, $H^1(T, N/N_n) = 0$. Therefore,

$$H^1(G, N/N_n) = 0.$$

This completes the proof of Lemma 3.

Proof of the key lemma. First, note that the kernel of (1) is

$$\mathrm{Hom}_{\boldsymbol{Z}_l^\times}(\mathfrak{g}_1/\mathfrak{g}_2, N).$$

Then, consider the group exact sequence

$$(9)\qquad 1 \longrightarrow \mathfrak{g}_1/\mathfrak{g}_2 \longrightarrow \mathfrak{g}_0/\mathfrak{g}_2 \longrightarrow \mathfrak{g}_0/\mathfrak{g}_1 = \boldsymbol{Z}_l^\times \longrightarrow 1,$$

and the induced inflation-restriction-transgression exact sequence

$$(10)\qquad 0\longrightarrow H^1(Z_l^\times, N)\xrightarrow{\inf} H^1(\mathfrak{g}_0/\mathfrak{g}_2, N)\xrightarrow{\mathrm{res}}\mathrm{Hom}_{Z_l^\times}(\mathfrak{g}_1/\mathfrak{g}_2, N)$$
$$\xrightarrow{\mathrm{tg}} H^2(Z_l^\times, N).$$

This shows that the vanishing of the kernel of (1) is reduced to that of the two cohomology groups $H^1(\mathfrak{g}_0/\mathfrak{g}_2, N)$ and $H^2(Z_l^\times, N)$. First, $H^2(Z_l^\times, N)=0$, because N is pro-l and $Z_l^\times$ is the completion of the free cyclic group Z w.r.t. an "almost pro-l topology" defined by the sequence of ideals $(l^n(l-1))_{n\geq 0}$ of Z. Secondly, the vanishing of $H^1(\mathfrak{g}_0/\mathfrak{g}_2, N)$ can easily be reduced to that of $H^1(\mathfrak{g}_0/\mathfrak{g}_2, N/N_n)$ for all $n\geq 1$, i.e., to Lemma 3, as follows. Suppose that $F\colon \mathfrak{g}_0/\mathfrak{g}_2\to N$ is a continuous 1-cocycle. By Lemma 3, there exists, for each $n\geq 1$, an element $H_n\in N$ such that

$$(11)\qquad F_\rho\equiv H_n^{j\chi(\rho)^{-1}}\mod N_n\qquad(\rho\in\mathfrak{g}_0/\mathfrak{g}_2).$$

Since $\{N_n\}$ is a decreasing sequence, $H_m^{j\chi(\rho)^{-1}}\equiv H_n^{j\chi(\rho)^{-1}}\bmod N_k$ for any $m, n, k\in N$ with $m, n\geq k$. Letting $\chi(\rho)=-1$ and using $H_mH_m^{j-1}=H_nH_n^{j-1}=1$, we obtain $(H_m)^2\equiv(H_n)^2\bmod N_k$. Since $2\in Z_l^\times$, this implies $H_m\equiv H_n\bmod N_k$. On the other hand, since $\mathscr{A}=\varprojlim(\mathscr{A}/\mathfrak{a}_n)$ ([PGC] II), we have $N=\varprojlim(N/N_n)$. Therefore, if we put $H=\varprojlim H_n\in N$, then $F_\rho=H^{j\chi(\rho)^{-1}}$ for all $\rho\in\mathfrak{g}_0/\mathfrak{g}_2$; hence F must be a coboundary, and we obtain $H^1(\mathfrak{g}_0/\mathfrak{g}_2, N)=0$, as desired. This settles the proof of the key lemma.

Proof of Theorem B. For $\rho\in\mathfrak{g}_1=\mathrm{Gal}(\Omega_l/\boldsymbol{Q}(\boldsymbol{\mu}_{l^\infty}))$, put

$$(12)\qquad F'_\rho(u, v)=\exp\left\{\sum_{\substack{m\geq 3\\ odd}}\frac{(1-l^{m-1})^{-1}\cdot\chi_m(\rho)}{m!}(U^m+V^m+W^m)\right\}$$
$$\in \boldsymbol{Q}_l[[u, v]].$$

We shall show that all coefficients in $F'_\rho(u, v)$ are integral, i.e., $F'_\rho(u, v)\in Z_l[[u, v]]$. Since $\chi_m\in\mathrm{Hom}_{Z_l^\times}(\mathfrak{g}_1, Z_l(m))$, this will imply that $(\rho\to F'_\rho(u, v))\in\mathrm{Hom}_{Z_l^\times}(\mathfrak{g}_1, N)$. By Theorem 10 and the formula (Col) (§ 7) in [PGC] IV, F_ρ and F'_ρ coincide on $\mathfrak{g}_2$. Hence by the above key lemma they must coincide also on $\mathfrak{g}_1$, which will imply Theorem B.

To prove that $F'_\rho(u, v)\in Z_l[[u, v]]$, we need

Lemma 4. *Let $\hat{\boldsymbol{Q}}_l^{\mathrm{ur}}$ be the completion of the maximum unramified extension of $\boldsymbol{Q}_l$, $\hat{\boldsymbol{Z}}_l^{\mathrm{ur}}$ be its integer ring and φ be the Frobenius automorphism of $\hat{\boldsymbol{Q}}_l^{\mathrm{ur}}$ over $\boldsymbol{Q}_l$. Let*

$$f(u, v)=\sum_{i,j\geq 0}a_{ij}u^iv^j\in\hat{\boldsymbol{Q}}_l^{\mathrm{ur}}[[u, v]]$$

and assume that

$$a_{00} \in (\hat{\boldsymbol{Z}}_l^{\mathrm{ur}})^{\times},\ a_{10},\ a_{01} \in \hat{\boldsymbol{Z}}_l^{\mathrm{ur}}.$$

Then the following two conditions 1), 2) *are equivalent*:

1) $f(u, v) \in \hat{\boldsymbol{Z}}_l^{\mathrm{ur}}[[u, v]]$.

2) $(f(u, v))^l \cdot f^{\varphi}((1+u)^l-1, (1+v)^l-1)^{-1} \in 1+l\hat{\boldsymbol{Z}}_l^{\mathrm{ur}}[[u, v]]$,

where f^{φ} *is the power series obtained from* f *by letting* φ *act on its coefficients.*

Proof. 1)$\Rightarrow$2): If $f(u, v) \in \hat{\boldsymbol{Z}}_l^{\mathrm{ur}}[[u, v]]$, then

$$f^{\varphi}((1+u)^l-1, (1+v)^l-1) \equiv f^{\varphi}(u^l, v^l) \bmod l$$
$$\equiv (f(u, v))^l \bmod l.$$

So $(f(u, v))^l - f^{\varphi}((1+u)^l-1, (1+v)^l-1) \in l\hat{\boldsymbol{Z}}_l^{\mathrm{ur}}[[u, v]]$. Since

$$f^{\varphi}((1+u)^l-1, (1+v)^l-1) \in (\hat{\boldsymbol{Z}}_l^{\mathrm{ur}}[[u, v]])^{\times},$$ we get 2).

2)$\Rightarrow$1): If 2) holds, we can write

$$(f(u, v))^l = f^{\varphi}((1+u)^l-1, (1+v)^l-1)g(u, v), \tag{13}$$

$$g(u, v) = b_{00} + l \sum_{\substack{i, j \geq 0 \\ i+j \neq 0}} b_{ij} u^i v^j, \qquad b_{ij} \in \hat{\boldsymbol{Z}}_l^{\mathrm{ur}},\ b_{00} \equiv 1 \bmod l. \tag{14}$$

By assumption, $a_{ij} \in \hat{\boldsymbol{Z}}_l^{\mathrm{ur}}$ for $i+j \leqq 1$. We shall show by induction on $i+j$ that $a_{ij} \in \hat{\boldsymbol{Z}}_l^{\mathrm{ur}}$ for all i, j. Suppose $a_{ij} \in \hat{\boldsymbol{Z}}_l^{\mathrm{ur}}$ for $i+j<n$ $(n \geq 2)$. Let $i_0+j_0=n$. We compare the coefficients of $u^{i_0}v^{j_0}$ on both sides of (13). Put

$$A = \sum_{\substack{i, j \geq 0 \\ i+j \neq 0}} a_{ij}\, u^i v^j.$$

Then

$$(f(u, v))^l = (a_{00}+A)^l \tag{15}$$
$$= a_{00}^l + {}_lC_1 a_{00}^{l-1} A + {}_lC_2 a_{00}^{l-2} A^2 + \cdots + {}_lC_{l-1} a_{00} A^{l-1} + A^l.$$

By the induction hypothesis and the divisibility of ${}_lC_k$ $(1 \leq k \leq l-1)$ by l, the coefficient of $u^{i_0}v^{j_0}$ in

$${}_lC_2 a_{00}^{l-2} A^2 + \cdots + {}_lC_{l-1} a_{00} A^{l-1} \tag{16}$$

belongs to $l\hat{\boldsymbol{Z}}_l^{\mathrm{ur}}$. Further, the coefficient of $u^{i_0}v^{j_0}$ in A^l is congruent mod $l\hat{\boldsymbol{Z}}_l^{\mathrm{ur}}$ to

$$\begin{cases} 0, & \text{if } l \nmid i_0 \text{ or } l \nmid j_0, \\ a_{i_0 j_0}^l, & \text{if } l \mid i_0 \text{ and } l \mid j_0. \end{cases} \tag{17}$$

Here and in the following i_0', j_0', stand for i_0/l, j_0/l respectively. Thus the coefficient of $u^{i_0}v^{j_0}$ in $(f(u, v))^l$ is congruent mod $l\hat{\boldsymbol{Z}}_l^{\mathrm{ur}}$ to

$$(18)\qquad \begin{cases} la_{00}^{l-1}a_{i_0j_0}, & \text{if } l\nmid i_0 \text{ or } l\nmid j_0, \\ la_{00}^{l-1}a_{i_0j_0}+a_{i_0'j_0'}^{l}, & \text{if } l\mid i_0 \text{ and } l\mid j_0. \end{cases}$$

Next, we look at the coefficient of $u^{i_0}v^{j_0}$ on the right-hand side of (13), i.e.,

$$(19)\qquad \begin{aligned} &f^{\varphi}((1+u)^l-1, (1+v))^l-1)g(u, v) \\ &\quad =b_{00}f^{\varphi}((1+u)^l-1, (1+v)^l-1)+lf^{\varphi}((1+u)^l-1,(1+v)^l-1) \\ &\quad \times\Big(\sum_{\substack{i,j\geq 0\\ i+j\neq 0}} b_{ij}u^iv^j\Big). \end{aligned}$$

By the induction hypothesis, we see that the coefficient of $u^{i_0}v^{j_0}$ in the second term on the right-hand side of (19) lies in $l\hat{\boldsymbol{Z}}_l^{\mathrm{ur}}$. On the other hand, as $(1+u)^l-1\equiv u^l$ and $(1+v)^l-1\equiv v^l \pmod{l}$, the coefficient of $u^{i_0}v^{j_0}$ on the right-hand side of (19) is congruent mod $l\hat{\boldsymbol{Z}}_l^{\mathrm{ur}}$ to

$$(20)\qquad b_{00}l^n a_{i_0j_0}^{\varphi}+\begin{cases} 0, & \text{if } l\nmid i_0 \text{ or } l\nmid j_0, \\ b_{00}a_{i_0'j_0'}^{\varphi}, & \text{if } l\mid i_0 \text{ and } l\mid j_0. \end{cases}$$

Therefore, equating the coefficients of $u^{i_0}v^{j_0}$ on both sides of (13) gives

$$(21)\qquad \begin{cases} la_{00}^{l-1}a_{i_0j_0}-b_{00}l^n a_{i_0j_0}^{\varphi}\in l\hat{\boldsymbol{Z}}_l^{\mathrm{ur}}, & \text{if } l\nmid i_0 \text{ or } l\nmid j_0, \\ la_{00}^{l-1}a_{i_0j_0}+a_{i_0'j_0'}^{l}-(b_{00}l^n a_{i_0j_0}^{\varphi}+b_{00}a_{i_0'j_0'}^{\varphi})\in l\hat{\boldsymbol{Z}}_l^{\mathrm{ur}}, & \text{if } l\mid i_0 \text{ and } l\mid j_0. \end{cases}$$

Since $a_{i_0'j_0'}\in\hat{\boldsymbol{Z}}_l^{\mathrm{ur}}$ and $b_{00}\equiv 1 \bmod l$, we have $b_{00}a_{i_0'j_0'}^{\varphi}\equiv a_{i_0'j_0'}^{l} \bmod l$. Hence in both cases $la_{00}^{l-1}a_{i_0j_0}-b_{00}l^n a_{i_0j_0}^{\varphi}\in l\hat{\boldsymbol{Z}}_l^{\mathrm{ur}}$, i.e.,

$$a_{i_0j_0}(a_{00}^{l-1}-b_{00}l^{n-1}a_{i_0j_0}^{\varphi-1})\in\hat{\boldsymbol{Z}}_l^{\mathrm{ur}}.$$

Since $\mathrm{ord}_l(a_{i_0j_0})=\mathrm{ord}_l(a_{i_0j_0}^{\varphi})$, a_{00}, $b_{00}\in(\hat{\boldsymbol{Z}}_l^{\mathrm{ur}})^{\times}$, and $n\geq 2$, we must have $a_{i_0j_0}\in\hat{\boldsymbol{Z}}_l^{\mathrm{ur}}$. q.e.d.

Remarks. i) This lemma is an analogue of the so called "Dwork's lemma" ([Dw]).

ii) A similar assertion holds when $f(u, v)$ is replaced by a power series in any number of variables and the proof is completely analogous.

Since $F_{\rho}'(u, v)\equiv 1 \pmod{uv}$, $(\rho\in\mathfrak{g}_1)$, we may apply lemma 4 for $f=F_{\rho}'$. Using this lemma, we can show that

$$(22)\qquad F_{\rho}'(u, v)\in\boldsymbol{Z}_l[[u, v]] \qquad \text{if and only if}$$

$$\sum_{\substack{m\geq 3\\ odd}} \frac{\chi_m(\rho)}{m!}(U^m+V^m+W^m) \in Z_l[[u, v]].$$

In fact,

$$\begin{aligned} &F'_\rho(u, v) \in Z_l[[u, v]] \\ &\quad \Longleftrightarrow (F'_\rho(u, v))^l F'_\rho((1+u)^l-1, (1+v)^l-1)^{-1} \in 1+lZ_l[[u, v]] \\ &\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{(by Lemma 4)} \\ (23) \qquad &\quad \Longleftrightarrow \log\{(F'_\rho(u, v))^l F'_\rho((1+u)^l-1, (1+v)^l-1)^{-1}\} \in lZ_l[[u, v]] \\ &\quad \Longleftrightarrow \frac{1}{l}\{\log\{(F'_\rho(u, v))^l F'_\rho((1+u)^l-1, (1+v)^l-1)^{-1}\}\} \\ &\quad \in Z_l[[u, v]], \end{aligned}$$

and

$$\begin{aligned} &\frac{1}{l}\{\log\{(F'_\rho(u, v))^l F'_\rho((1+u)^l-1, (1+v)^l-1)^{-1}\}\} \\ (24) \qquad &\qquad = \sum_{\substack{m\geq 3\\ odd}} \frac{\chi_m(\rho)}{m!}(U^m+V^m+W^m). \end{aligned}$$

Hence the theorem is reduced to the following Proposition. Here, $G_\infty = \mathrm{Gal}(\boldsymbol{Q}(\mu_{l^\infty})/\boldsymbol{Q})$, $Z_l[[G_\infty]]$ is its completed group algebra over Z_l, and the power series algebra $Z_l[[t]]$ is considered as a $Z_l[[G_\infty]]$-module *via* the action of G_∞ on $Z_l[[t]]$ defined by $1+t \to (1+t)^{\chi(\rho)}$ ($\rho \in G_\infty$, χ: the l-cyclotomic character).

Proposition 2. *For each $\rho \in \mathfrak{g}_1$, there exists an element $\delta = \delta_\rho \in Z_l[[G_\infty]]$ such that*

$$(25) \qquad \sum_{\substack{m\geq 1\\ odd}} \frac{\chi_m(\rho)}{m!} T^m = \delta(1+t) \in Z_l[[t]] \qquad (1+t = \exp T).$$

In particular,

$$(26) \qquad \sum_{\substack{m\geq 3\\ odd}} \frac{\chi_m(\rho)}{m!}(U^m+V^m+W^m) \in Z_l[[u, v]] \qquad (U+V+W=0).$$

Proof. Fix any $\rho \in \mathfrak{g}_1$. For each $n \geq 1$ and each $\bar{a} \in (\boldsymbol{Z}/l^n)^\times$, choose and fix $b_{n,\bar{a}} \in Z_l$ satisfying $\{(\zeta_n^{\bar{a}}-1)^{1/l^n}\}^{\rho-1} = \zeta_n^{b_{n,\bar{a}}}$. Then, by the definition of χ_m,

$$(27) \qquad \chi_m(\rho) \equiv \sum_{\substack{a=1\\ (a,l)=1}}^{l^n-1} b_{n,\bar{a}} \cdot a^{m-1} \mod l^n,$$

where $\bar{a}=a \bmod l^n \in (\boldsymbol{Z}/l^n)^\times$.

Put

$$\delta_n=\sum_{\substack{a=1\\(a,l)=1}}^{l^n-1} b_{n,\bar{a}}\cdot a^{-1}\sigma_a \in \boldsymbol{Z}_l[G_\infty]\subset \boldsymbol{Z}_l[[G_\infty]], \tag{28}$$

where σ_a is the element of G_∞ defined by $\chi(\sigma_a)=a$. Let π_n be the projection from $\boldsymbol{Z}_l[[G_\infty]]$ to $(\boldsymbol{Z}/l^n)[G_n]$, where $G_n=\mathrm{Gal}(\boldsymbol{Q}(\mu_{l^n})/\boldsymbol{Q})$. We shall show that $\pi_n(\delta_{n+1}-\delta_n)=0$. First, we note the following.

For $\bar{a}\in(\boldsymbol{Z}/l^n)^\times$, we have $\zeta_n^{\bar{a}}-1=\prod_{\bar{a}_1}(\zeta_{n+1}^{\bar{a}_1}-1)$, where $\bar{a}_1$ runs over all elements of $(\boldsymbol{Z}/l^{n+1})^\times$ with $\bar{a}_1 \bmod l^n=\bar{a}$. Therefore,

$$\begin{aligned}\zeta_n^{b_{n,\bar{a}}}&=\{(\zeta_n^{\bar{a}}-1)^{1/l^n}\}^{\rho-1}\\ &=\{\prod_{\bar{a}_1}(\zeta_{n+1}^{\bar{a}_1}-1)^{1/l^n}\}^{\rho-1}=\{(\prod_{\bar{a}_1}(\zeta_{n+1}^{\bar{a}_1}-1)^{1/l^{n+1}})^{\rho-1}\}^l\\ &=\zeta_{n+1}^{cl}=\zeta_n^c,\end{aligned} \tag{29}$$

with

$$c=\sum_{\bar{a}_1} b_{n+1,\bar{a}_1}. \tag{30}$$

Therefore,

$$b_{n,\bar{a}}\equiv\sum_{\bar{a}_1} b_{n+1,\bar{a}_1} \mod l^n. \tag{31}$$

But since $\pi_n(a_1^{-1}\sigma_{a_1}-a^{-1}\sigma_a)=0$ for $a_1\equiv a \bmod l^n$, (28) and (31) give

$$\pi_n(\delta_{n+1}-\delta_n)=0.$$

It follows that $\lim_{n\to\infty}\delta_n=\delta\in\boldsymbol{Z}_l[[G_\infty]]$ exists. Now

$$\begin{aligned}\delta_n(1+t)&=\sum_{\substack{a=1\\(a,l)=1}}^{l^n-1} b_{n,\bar{a}}\cdot a^{-1}(1+t)^a\\ &=\sum_{\substack{a=1\\(a,l)=1}}^{l^n-1} b_{n,\bar{a}}\cdot a^{-1}\left(\sum_{m=0}^{\infty}\frac{a^m T^m}{m!}\right)\quad (T=\log(1+t))\\ &=\sum_{m=0}^{\infty}\left\{\sum_{\substack{a=1\\(a,l)=1}}^{l^n-1} b_{n,\bar{a}}\cdot a^{m-1}\right\}\frac{T^m}{m!}.\end{aligned} \tag{32}$$

Since this coefficient of $(T^m/m!)$ coincides with the right side of (27), we can write as

$$\sum_{m=0}^{\infty}\frac{\chi_m(\rho)}{m!}T^m-\delta_n(1+t)=l^n\sum_{m=0}^{\infty}\frac{c_m^{(n)}}{m!}T^m,\ c_m^{(n)}\in\boldsymbol{Z}_l, \tag{33}$$

or

$$(34)\qquad \sum_{m=0}^{\infty}\frac{\chi_m(\rho)}{m!}T^m-\delta(1+t)=\delta_n(1+t)-\delta(1+t)+l^n\sum_{m=0}^{\infty}\frac{c_m^{(n)}}{m!}T^m,$$

for any n.

Now, in general, if we expand $\sum_{m=0}^{\infty}(c_m/m!)T^m$ ($c_m\in \boldsymbol{Z}_l$) in t as $\sum_{m=0}^{\infty}d_m t^m$ ($d_m\in \boldsymbol{Q}_l$), then $(m!)^2 d_m\in \boldsymbol{Z}_l$. So, for each fixed $m\geq 0$, choose n so large that $l^n/(m!)^2\in \boldsymbol{Z}_l$, to conclude that the coefficient of t^m in (34) belongs to $\boldsymbol{Z}_l$, and then let $n\to\infty$ to conclude that it must be 0. Therefore, $\sum_{m=0}^{\infty}\frac{\chi_m(\rho)}{m!}T^m$ belongs to $\boldsymbol{Z}_l[[t]]$ and is equal to $\delta(1+t)$. We see (by direct computation) that $\chi_m=0$ for m; even. Therefore,

$$(35)\qquad \sum_{\substack{m\geq 1\\ odd}}\frac{\chi_m(\rho)}{m!}T^m=\delta(1+t).$$

Thus, we have also proved Theorem B. q.e.d.

Corollary 1 of Theorem B (Coleman).

$$\begin{aligned}&\boldsymbol{Q}(\boldsymbol{\mu}_{l^\infty},\ l^k\text{-torsion points on } \mathrm{Jac}\,(X^{l^n}+Y^{l^n}=Z^{l^n}) \text{ for all } k,\ n\geq 1)\\ &=\boldsymbol{Q}(\boldsymbol{\mu}_{l^\infty},\ \{\prod_{a\in(\boldsymbol{Z}/l^n)^\times}(\zeta_n^a-1)^{\langle a^{m-1}\rangle_n}\}^{1/l^n} \text{ for all } n\geq 1 \text{ and all } m\geq 3 \text{ odd})\\ &=\boldsymbol{Q}(\boldsymbol{\mu}_{l^\infty},\ c^{1/l^n} \text{ for all } c\in C_n \text{ and all } n\geq 1).\end{aligned}$$

Here C_n is the group of circular units in $\boldsymbol{Q}(\boldsymbol{\mu}_{l^n})$.

As for the second equality, see [IS].

The following corollary is due to G. Anderson [A_1, A_2] (the Γ-factorization). Compare this with the remark below Theorem 10 [PGC] IV Section 1.

Corollary 2 of Theorem B. *For $\rho\in \mathfrak{g}_1$, choose $a_\rho\in \hat{\boldsymbol{Z}}_l^{\mathrm{ur}}$ such that $a_\rho-a_\rho^\varphi=\chi_1(\rho)$, and put*

$$(36)\qquad \tilde{G}_\rho(t)=\exp\left\{\sum_{\substack{m\geq 3\\ odd}}\frac{\beta_m(\rho)}{m!}T^m\right\}\cdot(1+t)^{a_\rho}.$$

Then $\tilde{G}_\rho(t)\in \hat{\boldsymbol{Z}}_l^{\mathrm{ur}}[[t]]$ and

$$(37)\qquad F_\rho(u,v,w)=\tilde{G}_\rho(u)\tilde{G}_\rho(v)\tilde{G}_\rho(w).$$

Proof. The last equality is a direct consequence of Theorem A_2. (Note that $(1+u)(1+v)(1+w)=1$.) As

$$\frac{1}{l}\log\{\tilde{G}_\rho(t)^l\cdot\tilde{G}_\rho^\varphi((1+t)^l-1)^{-1}\}=\sum_{\substack{m\geq 1\\ odd}}\frac{\chi_m(\rho)}{m!}T^m \qquad \text{(by Theorem B)}$$

$$\in Z_l[[t]], \qquad \text{(by Proposition 2)}$$

we conclude by Lemma 4 that $\tilde{G}_\rho(t)\in\hat{Z}_l^{\mathrm{ur}}[[t]]$. q.e.d.

§ 4. Some open questions

We have thus proved that F_ρ ($\rho\in G_{Q(\mu_{l^\infty})}$) satisfies the equivalent conditions of Proposition 1. It is natural to ask whether these conditions characterize the image of $G_{Q(\mu_{l^\infty})}$ in $\mathscr{A}^\times$. (This answer turned out to be "no", due to Coleman.) More plausible would be a similar characterization of the image *modulo l*. As we have seen above, it is closely connected with the Vandiver conjecture at l. It also seems to be an interesting question to *construct* all power series in $(Z/l)[[u, v]]$ satisfying the conditions analogous to those of Proposition 1 (i). Here, we meet with the study of the power series $h(u)\in(Z/l)[[u]]$ satisfying the differential equations of the form

$$D^{l-1}(h)-D^{l-1}(h)_{u=0}=h-h^l,$$

where $D=(u+1)(d/du)$. (Such $h(u)$ appears in the v-adic expansion of $F(u, v)$ as

$$F(u, v)=1+h(u)v+\cdots).$$

Is there a totally different approach (e.g. from topology) to construct such power series in $(Z/l)[[u, v]]$?

Added in Proof. (i) Related result of Coleman (mentioned in the introduction) was addressed also in the Workshop on "Iwasawa theory and special values of L-functions" Jan. 1987, MSRI, Berkeley, USA, under the title "Anderson-Ihara theory". The authors understand that a detailed paper is in preparation.

(ii) Some results related to Section 4 have recently been obtained by H. Ichimura and M. Kaneko; "On the universal power series for Jacobi sums and the Vandiver conjecture" (preprint).

References

[A1] G. Anderson, Cyclotomy and an extension of the Taniyama group, Compositio Math., **57** (1986) 153–217.

[A2] ——, The hyperadelic gamma function: a précis, in this Volume, 1–19.

[D] P. Deligne, A letter to S. Bloch, February, 1984.

[Dw] B. Dwork, Norm residue symbol in local number fields, Abh. Math. Sem. Univ. Hamburg, **22** (1958), 180–190.

[IS] H. Ichimura and K. Sakaguchi, The non-vanishing of a certain Kummer character χ_m (after C. Soulé), and some related topics, in this Volume, 53–64.

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

[MW] B. Mazur and A. Wiles, Class fields of abelian extensions of Q, Invent. Math., **76** (1984), 179–330.

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