JOURNAL OF NUMBER THEORY 31, 312–334 (1989)

On the Universal Power Series for Jacobi Sums and the Vandiver Conjecture*

HUMIO ICHIMURA† AND MASANOBU KANEKO‡

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

Communicated by Y. Ihara

Received February 20, 1988

We shall study some explicit connections between (1) the Vandiver conjecture on the class number of the real cyclotomic field $\mathbb{Q}(\cos(2\pi/l))$ and (2) the images of various Galois representations induced from the power series representation (constructed and studied by Ihara, Anderson, Coleman, etc.) of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}(\mu_{l^\infty}))$ which describes universally the Galois action on the Fermat curves of l-power degrees. One such connection was first discovered by Coleman. In the case of the original power series representation, we shall also describe the difference between the "expected image" and the actual Galois image in terms of a certain invariant of Iwasawa type.

INTRODUCTION

In his study of Galois representations arising from the pro-l etale coverings of $\mathbb{P}^1\setminus\{0, 1, \infty\}$, Y. Ihara [6] constructed for each element ρ of the absolute Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ over the rationals an l-adic power series $F_\rho(u, v)$ in two variables which was shown to be universal for Jacobi sums. Some properties of the power series F_ρ have been investigated by Y. Ihara [6], G. Anderson [1], R. Coleman [4], and Ihara, Kaneko, and Yukinari [7]. Especially, F_ρ for $\rho\in\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}(\mu_{l^\infty}))$ satisfies some non-obvious functional equations [1, 7].

The aim of this paper is to study the image of the homomorphism $\rho\mapsto F_\rho$ from $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}(\mu_{l^\infty}))$ to the multiplicative group $\mathbb{Z}_l[[u, v]]^\times$. We first show that the functional equations mentioned above characterize the image and its reduction modulo l if and only if the Vandiver conjecture at l is valid (Theorem 1). This means in particular that the Galois image is

* A part of this paper is taken from a part of the first named author's doctoral dissertation submitted to the University of Tokyo (1987).

† Department of Mathematics, Yokohama City University, 22-2, Seto, Kanazawa-ku, Yokohama 236, Japan.

‡ Department of Mathematics, Faculty of Science, Osaka University, Toyonaka, Osaka 560, Japan.

0022-314X/89 $3.00

completely described when the class number of the field $\mathbb{Q}(\cos(2\pi/l))$ is not divisible by l (e.g., when l is regular or less than 125,000). Also the theorem might present a new aspect of the Vandiver conjecture. Next we look at the "Vandiver gap," i.e., the difference (if any) between the expected image and the actual Galois image. We give an explicit description of this gap in terms of a certain invariant of Iwasawa type (Theorem 2).

There are two other versions of Theorem 1. The first is due to R. Coleman and is concerned with the image of the homomorphism $\rho \mapsto g_\rho$, where g_ρ is the "twisted log" of a factor of F_ρ [4, Th. 7.3]. The second is related to the reduction modulo l of the coefficient $h_\rho(u)$ of v in the v-adic expansion of $F_\rho(u, v)$. As is pointed out in [7, Sect. 4], $h_\rho \bmod l$ satisfies a certain differential equation in characteristic l. As the power series h_ρ and g_ρ are closely related with each other, $g_\rho \bmod l$ satisfies a similar type of differential equation. We shall show that the image of the homomorphisms $\rho \mapsto h_\rho \bmod l$ and $\rho \mapsto g_\rho \bmod l$ are characterized by these differential equations if and only if the Vandiver conjecture is valid (Theorems 3 and 3').

We thank Y. Ihara for his advice and encouragement.

1. The Main Results

1.1. *Preliminaries*

Let $\bar{\mathbb{Q}}$ be the algebraic closure of the rational number field $\mathbb{Q}$ in the complex number field. Let l be a fixed prime number, μ_{l^n} be the group of l^nth roots of unity in $\bar{\mathbb{Q}}$, and put $\mu_{l^\infty} = \bigcup_{n \geq 1} \mu_{l^n}$. Let $\zeta = (\zeta_n)_{n \geq 1}$ be a fixed generator of the l-adic Tate module $T_l(\mathbb{G}_m)$, i.e., $\zeta_n \in \mu_{l^n} \setminus \mu_{l^{n-1}}$ and $\zeta_{n+1}^l = \zeta_n$. In [6, Th. A], Ihara constructed a homomorphism (associated to ζ)

$$\mathbf{F}\colon \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}(\mu_{l^\infty})) \ni \rho \mapsto F_\rho(u, v) \in \mathbb{Z}_l[[u, v]]^\times$$

for which the power series $F_\rho(u, v)$ describes "universally" the action of ρ on the l-adic Tate modules of abelian varieties of Fermat type of l-power degree. According to the work of Anderson [1], Coleman [4], and Ihara, Kaneno, and Yukinari [7], we have an explicit formula for F_ρ as follows. For any odd integer $m \geq 1$ and any integer $n \geq 1$, put

$$\varepsilon_n(m) = \prod_{\substack{1 \leq a \leq l^n \\ (a, l) = 1}} (\zeta_n^a - 1)^{a^{m-1}}.$$

Define a Kummer character $\chi_m\colon \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}(\mu_{l^\infty})) \to \mathbb{Z}_l$ by the relations

$$(\varepsilon_n(m)^{1/l^n})^{\rho - 1} = \zeta_n^{\chi_m(\rho)} \qquad \text{for all} \quad \rho \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}(\mu_{l^\infty})), \quad n \geq 1.$$

Then, we have an expansion

$$F_\rho(u, v) = \exp\left\{ \sum_{\substack{m \geq 3 \\ \text{odd}}} \frac{(1 - l^{m-1})^{-1} \chi_m(\rho)}{m!} (U^m + V^m + W^m) \right\},$$

where $U = \log(1+u)$, $V = \log(1+v)$, $W = \log(1+w)$, and $w (\in \mathbb{Z}_l[[u, v]])$ is defined by $(1+u)(1+v)(1+w) = 1$. Put

$$g_\rho(t) = \sum_{\substack{m \geq 1 \\ \text{odd}}} \frac{\chi_m(\rho)}{m!} T^m, \qquad T = \log(1+t).$$

The power series g_ρ is the "twisted log" of a "factor" of F_ρ and is an element of $\mathbb{Z}_l[[t]]$. (See [7, Cor. 2 of Th. B] and its proof.) Further, put

$$\mathscr{V}^- = \left\{ g \in \mathbb{Z}_l[[t]]; \sum_{\zeta^l = 1} g(\zeta(1+t) - 1) = 0, g((1+t)^{-1} - 1) = -g \right\}.$$

Then, Coleman [4] proved the following

THEOREM C (R. Coleman). *Assume l is odd. Then,*

$$\{ g_\rho; \rho \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}(\mu_{l^\infty})) \} \subset \mathscr{V}^-,$$

and both sides coincide if and only if the Vandiver conjecture at l is valid.

1.2. *The Main Results*

In the following, we always assume that l is odd. Through the isomorphism

$$\mathbb{Z}_l[[u, v]] \simeq \mathbb{Z}_l[[u, v, w]]/((1+u)(1+v)(1+w) - 1),$$

we often regard an element of $\mathbb{Z}_l[[u, v]]$ as a representative in $\mathbb{Z}_l[[u, v, w]]$ modulo the ideal $((1+u)(1+v)(1+w) - 1)$. For each $F = F(u, v) \in \mathbb{Z}_l[[u, v]]$, define $F * F$ to be the element of

$$\mathbb{Z}_l[[u, v, u', v']]/((1+u)(1+v)(1+u')(1+v') - 1)$$

represented by the product $F(u, v)\, F(u', v')$ (cf. [7, Sect. 1]).

Let $\mathfrak{F}$ be the multiplicative group of all $F = F(u, v) \in \mathbb{Z}_l[[u, v]]^\times$ satisfying the following five conditions:

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

(ii) $F\bar{F} = 1$, where $\bar{F} = F((1+u)^{-1} - 1, (1+v)^{-1} - 1, (1+w)^{-1} - 1)$,

(iii) F is symmetric in u, v, w,

(iv) $F * F$ is symmetric in u, v, u', v',

(v) $\prod_{\zeta^l=1} F(\zeta(1+u)-1, \zeta(1+v)-1) = F((1+u)^l-1, (1+v)^l-1)$.

Further, let $\tilde{\mathfrak{F}}$ be the multiplicative group of all $\tilde{F} = \tilde{F}(u, v) \in \mathbb{F}_l[[u, v]]^\times$ satisfying the same type of conditions as (i)–(iv). Note that the reduction of the relation (v) modulo l or rather modulo the prime element of $\mathbb{Q}_l(\zeta_1)$ is trivial. It follows from the results recalled in Section 1.1 (or more precisely, from [7, Prop. 1] combined with Theorem C) that F_ρ and $F_\rho \bmod l$ ($\rho \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}(\mu_{l^\infty}))$) belong to $\mathfrak{F}$ and $\tilde{\mathfrak{F}}$, respectively. Our first result is the following.

THEOREM 1. *The following conditions are equivalent*:

(i) *The Vandiver conjecture at l is valid.*

(ii) $\mathrm{Im}\, \mathbf{F} = \mathfrak{F}$.

(iii) $\mathrm{Im}\, \mathbf{F}$ modulo $l = \tilde{\mathfrak{F}}$.

Especially, if l is a regular prime or less than 125,000 (see e.g., [12, p. 157]), the equalities (ii) and (iii) hold. We note here that there is an analogous result of K. Iwasawa [9, Th. 8] which relates the Vandiver conjecture with a module generated by Jacobi sums of exponent l.

The second result is a "quantitative version" of Theorem 1. The group ring $\Lambda = \mathbb{Z}_l[[\mathbb{Z}_l^\times]]$ acts on the multiplicative group $\mathbb{Z}_l[[u, v]]^\times$ in the usual manner, i.e., the element $j_\alpha \in \Lambda$ corresponding to $\alpha \in \mathbb{Z}_l^\times$ acts as $j_\alpha \cdot u = (1+u)^\alpha - 1$, $j_\alpha \cdot v = (1+v)^\alpha - 1$. Then, $\mathfrak{F}$ is a Λ-submodule and furthermore the cokernel $\mathfrak{F}/(\mathrm{Im}\, \mathbf{F})$ turns out to be a Λ-module (see Section 3.1). Let $(\mathfrak{F}/\mathrm{Im}\, \mathbf{F})(-1)$ be the "Tate twist" of the cokernel. It will be shown in Section 3.1 that the modules $\mathfrak{F}/(\mathrm{Im}\, \mathbf{F})$ and $(\mathfrak{F}/\mathrm{Im}\, \mathbf{F})(-1)$ are finitely generated and torsion over Λ. For each integer $n \geqq 1$, let A_n be the l-Sylow subgroup of the ideal class group of $\mathbb{Q}(\mu_{l^n})$. Put $A_\infty = \lim_{n \to \infty} A_n$ and let A_∞^+ be its "even part." It is well known that the module $\mathrm{Hom}_{\mathbb{Z}_l}(A_\infty^+, \mathbb{Q}_l/\mathbb{Z}_l)$ is a finitely generated torsion Λ-module. Here, $j_\alpha \in \mathbb{Z}_l^\times$ acts on $f \in \mathrm{Hom}_{\mathbb{Z}_l}(A_\infty^+, \mathbb{Q}_l/\mathbb{Z}_l)$ by the rule $(j_\alpha \cdot f)(a) = f(j_\alpha^{-1} \cdot a)$. Regard $(\mathfrak{F}/\mathrm{Im}\, \mathbf{F})(-1)$ and $\mathrm{Hom}_{\mathbb{Z}_l}(A_\infty^+, \mathbb{Q}_l/\mathbb{Z}_l)$ as $\Lambda_1 = \mathbb{Z}_l[[1 + l\mathbb{Z}_l]]$ ($\simeq \mathbb{Z}_l[[t]]$)-modules. Then,

THEOREM 2. *The two torsion Λ_1-modules* $(\mathfrak{F}/\mathrm{Im}\, \mathbf{F})(-1)$ *and* $\mathrm{Hom}_{\mathbb{Z}_l}(A_\infty^+, \mathbb{Q}_l/\mathbb{Z}_l)$ *have the same characteristic power series.*

The third result is formulated in two ways. Let $h_\rho(u)$ be the coefficient of v in the v-adic expansion of $F_\rho(u, v)$;

$$F_\rho(u, v) = 1 + h_\rho(u)v + \cdots.$$

Let $\mathscr{D}$ be the differential operator on $\mathbb{F}_l[[t]]$ as follows. For $g \in \mathbb{F}_l[[t]]$, define

$$\mathscr{D}(g) = D^{l-1}g - D^{l-1}g|_{t=0} - g + g(t^l),$$

where $D = (1+t)(d/dt)$. In [7, Sect. 4], it is pointed out that $h_\rho \bmod l$ satisfies $\mathscr{D}(h_\rho(t) \bmod l) = 0$. Further, it is easily seen that $h_\rho(t)$ is "even," i.e., $h_\rho((1+t)^{-1}-1) = h_\rho(t)$. Then

THEOREM 3. *We have an inclusion*

$$\{h_\rho \bmod l;\ \rho \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}(\boldsymbol{\mu}_{l^\infty}))\}$$
$$\subset \{h \in \mathbb{F}_l[[t]];\ \mathscr{D}(h) = 0,\ h((1+t)^{-1}-1) = h(t)\}.$$

Further, both sides coincide if and only if the Vandiver conjecture at l is valid.

This result can be reformulated as

THEOREM 3′. *We have an inclusion*

$$\{g_\rho \bmod l;\ \rho \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}(\boldsymbol{\mu}_{l^\infty}))\}$$
$$\subset \{g \in \mathbb{F}_l[[t]];\ (D^{l-1}-1)g = 0,\ g((1+t)^{-1}-1) = -g(t)\}.$$

Further, both sides coincide if and only if the Vandiver conjecture at l is valid.

This is a "modulo l version" of Theorem C.

Theorems 1, 2, and 3 are proved in Sections 2, 3, and 4, respectively.

1.*N. Notations*

We identify $G_\infty = \mathrm{Gal}(\mathbb{Q}(\boldsymbol{\mu}_{l^\infty})/\mathbb{Q})$ with $\mathbb{Z}_l^\times$ via the action of G_∞ on the Tate module $T_l(\mathbb{G}_m)$. For $\alpha \in \mathbb{Z}_l^\times$, j_α denotes the element of G_∞ such that $j_\alpha(\zeta) = \zeta^\alpha$.

Set $\Delta = \mathrm{Gal}(\mathbb{Q}(\boldsymbol{\mu}_l)/\mathbb{Q})$. Let ω denote the Teichmüller character; $\omega: \Delta \to \mathbb{Z}_l^\times$. For an integer i and a Δ-module M, $M^{(i)} = M^{(i \bmod (l-1))}$ denotes the ω^i-eigenspace of M. Further, M^- (resp. M^+) denotes the maximal subspace of M on which j_{-1} acts as (-1)-multiplication (resp. j_{-1} acts trivially).

Set $\Gamma = \mathrm{Gal}(\mathbb{Q}(\boldsymbol{\mu}_{l^\infty})/\mathbb{Q}(\boldsymbol{\mu}_l))$. We choose j_{1+l} as a generator of Γ. We identify $\Lambda_1 = \mathbb{Z}_l[[\Gamma]]$ with the ring $\mathbb{Z}_l[[t]]$ by $j_{1+l} \leftrightarrow 1+t$.

The Galois groups G_∞, Γ, and Δ act on the multiplicative groups $\mathbb{Z}_l[[u,v]]^\times$, $\mathbb{Z}_l[[t]]^\times$ and the additive groups $\mathbb{Z}_l[[u,v]]$, $\mathbb{Z}_l[[t]]$ by $j_\alpha(1+u) = (1+u)^\alpha$, etc.

Suppose X is a Galois group with $\mathbb{Z}_l^\times$-action. For each integer m, we denote by $\mathrm{Hom}_{\mathbb{Z}_l^\times}(X, \mathbb{Z}_l(m))(\mathbb{Z}_l(m)$: the Tate twist) the $\mathbb{Z}_l$-module con-

sisting of all continuous homomorphisms $\beta: X \to \mathbb{Z}_l$ satisfying $\beta(j_\alpha \cdot \rho) = \alpha^m \beta(\rho)$ for all $\alpha \in \mathbb{Z}_l^\times$ and $\rho \in X$.

2. Proof of Theorem 1

2.1. *Relations between* $\mathscr{V}^-$, $\mathfrak{F}$, *and* $\tilde{\mathfrak{F}}$

We deduce Theorem 1 from Theorem C. For this purpose, we investigate relations between $\mathscr{V}^-$, $\mathfrak{F}$, and $\tilde{\mathfrak{F}}$. With the natural action of $\mathbb{Z}_l^\times$ on the rings of l-adic power series or their reduction modulo l (see Section 1.N), we consider $\mathfrak{F}$, $\tilde{\mathfrak{F}}$, and $\mathscr{V}^-$ as Λ-modules. We shall prove in Sections 2.2 and 2.4 the following propositions.

Proposition 1. *The map*

$$\begin{array}{ccc} \mathscr{V}^- & \longrightarrow & \mathfrak{F} \\ \cup & & \cup \\ g(t) = \sum_{\substack{m \geq 1 \\ \text{odd}}} \frac{a_m}{m!} T^m & \mapsto & F_g(u,v) = \exp\left(\sum_{\substack{m \geq 3 \\ \text{odd}}} \frac{(1-l^{m-1})^{-1} a_m}{m!} (U^m + V^m + W^m) \right) \end{array}$$

is well defined and gives a Λ-isomorphism from $\mathscr{V}^-$ to $\mathfrak{F}$.

Proposition 2. *The reduction modulo l from $\mathfrak{F}$ to $\tilde{\mathfrak{F}}$ is a Λ-isomorphism.*

Since the power series g_ρ is mapped to F_ρ by the homomorphism in Proposition 1, Theorem 1 follows immediately from Theorem C and Propositions 1 and 2.

Let Λ^- be the "odd part" of Λ, i.e., $\Lambda^- = ((1 - j_{-1})/2)\Lambda$. Since $\mathscr{V}^-$ is a free Λ^--module generated by the power series $\sum_{m \geq 1,\ \text{odd}} (1/m!) T^m$ (see [3]), we get from the above propositions the following

Corollary. $\mathfrak{F}$ (*resp.* $\tilde{\mathfrak{F}}$) *is a free* Λ^-*-module generated by* $F(u,v) = \exp(\sum_{m \geq 3,\ \text{odd}} ((1-l^{m-1})^{-1}/m!)(U^m + V^m + W^m))$ (*resp.* $F(u,v) \bmod l$).

2.2. *Proof of Proposition* 1

By [7, Prop. 1], the module $\mathfrak{F}$ coincides with the multiplicative group of all power series $F \in \mathbb{Z}_l[[u,v]]^\times$ such that

$$F(0,0) = 1,$$

$$\log F = \sum_{\substack{m \geq 3 \\ \text{odd}}} \frac{a_m}{m!} (U^m + V^m + W^m) \qquad \text{with} \quad a_m \in \mathbb{Z}_l,$$

and

$$\prod_{\zeta^l=1} F(\zeta(1+u)-1, \zeta(1+v)-1) = F((1+u)^l-1, (1+v)^l-1).$$

Let $\mathfrak{F}'$ be the additive group of all power series $G \in \mathbb{Z}_l[[u, v]]$ such that

$$G(u, v) = \sum_{\substack{m \geq 3 \\ \text{odd}}} \frac{a_m}{m!}(U^m + V^m + W^m) \qquad \text{with} \quad a_m \in \mathbb{Z}_l$$

and

$$\sum_{\zeta^l=1} G(\zeta(1+u)-1, \zeta(1+v)-1) = 0,$$

which admits, in the natural manner, a Λ-module structure.

LEMMA 1. *The map*

$$\mathfrak{F} \ni F \mapsto \log F - \frac{1}{l} \log F((1+u)^l-1, (1+v)^l-1) \in \mathfrak{F}'$$

is well defined and gives a Λ-isomorphism from $\mathfrak{F}$ to $\mathfrak{F}'$.

This lemma follows immediately from the lemma of Dieudonné and Dwork (see, e.g., [7, Lem. 4]).

LEMMA 2. *The map*

$$\begin{array}{ccc} \mathscr{V}^- & \longrightarrow & \mathfrak{F}' \\ \cup & & \cup \\ g(t) = \sum_{\substack{m \geq 1 \\ \text{odd}}} \frac{a_m}{m!} T^m & \mapsto & G_g(u, v) = \sum_{\substack{m \geq 3 \\ \text{odd}}} \frac{a_m}{m!}(U^m + V^m + W^m) \end{array}$$

is well defined and gives a Λ-isomorphism from $\mathscr{V}^-$ to $\mathfrak{F}'$.

Proposition 1 follows immediately from Lemmas 1 and 2.

Now, we prove Lemma 2. It is clear that the map in the lemma is well defined and is a Λ-homomorphism. First, we prove the injectivity. For $g = \sum_{m \geq 1, \text{ odd}} (a_m/m!) T^m \in \mathscr{V}^-$, assume $G_g = 0$. Then, $a_m = 0$ for all odd integers $m \geq 3$. Therefore, $g(t) = a_1 \log(1+t) \in \mathbb{Z}_l[[t]]$. Hence, $a_1 = 0$ and $g = 0$. Next, we prove the surjectivity. Let $G = \sum_{m \geq 3, \text{ odd}} (a_m/m!)(U^m + V^m + W^m)$ be any element of $\mathfrak{F}'$. Let $\partial_u = (1+u)(\partial/\partial u) = \partial/\partial U$ and $\partial_v = (1+v)(\partial/\partial v) = \partial/\partial V$ be the differential operators on $\mathbb{Z}_l[[u, v]]$. By a simple calculation, we get

$$\partial_u \partial_v G = \sum_{\substack{m \geq 3 \\ \text{odd}}} \frac{a_m}{(m-2)!} W^{m-2}.$$

From this, we see that the power series $h(t)=\sum_{m\geqslant 3,\ \mathrm{odd}}(a_m/(m-2)!)T^{m-2}$ is an element of $\mathbb{Z}_l[[t]]$. Since $G\in\mathfrak{F}'$, G satisfies the relation

$$\sum_{\zeta^l=1} G(\zeta(1+u)-1,\zeta(1+v)-1)=0.$$

By letting ∂_u and ∂_v act on both sides, we get

$$\sum_{\zeta^l=1}(\partial_u\partial_v G)(\zeta(1+u)-1,\zeta(1+v)-1)=0.$$

When $1+u$ and $1+v$ are replaced respectively by $\zeta(1+u)$ and $\zeta(1+v)$, $1+w=(1+u)^{-1}(1+v)^{-1}$ is replaced by $\zeta^{-2}(1+w)$. Since $l\neq 2$, we see from the above that $\sum_{\zeta^l=1}h(\zeta(1+t)-1)=0$. Hence, $h\in\mathscr{V}^-$. But since $D^2\mathscr{V}^-=\mathscr{V}^-$ (see [3]), there exists $g\in\mathscr{V}^-$ such that $D^2g=h$. We easily see that $G_g=G$. This proves the surjectivity.

2.3. *Some Lemmas for the Proof of Proposition* 2

In this subsection, we prove some lemmas which we need in the proof of Proposition 2.

Let $\hat{\mathbb{Z}}_l^{ur}$ be the ring of integers of the completion $\hat{\mathbb{Q}}_l^{ur}$ of the maximum unramified extension of $\mathbb{Q}_l$, and let φ be the Frobenius automorphism of $\hat{\mathbb{Q}}_l^{ur}$ over $\mathbb{Q}_l$. Put

$$\hat{\mathbb{Z}}_l^{ur}[[t]]^0=\{G\in\hat{\mathbb{Z}}_l^{ur}[[t]]^\times;\ g(0)\equiv 1\ (\mathrm{mod}\ l)\}.$$

LEMMA 3. *If* $(1+t)^\alpha\in\hat{\mathbb{Z}}_l^{ur}[[t]]$ *for* $\alpha\in\hat{\mathbb{Z}}_l^{ur}$, *then* $\alpha\in\mathbb{Z}_l$.

Proof. By the lemma of Dieudonné and Dwork (see, e.g., [7, Lem. 4]), $(1+t)^\alpha\in\hat{\mathbb{Z}}_l^{ur}[[t]]$ implies that

$$\frac{1}{l}\log\{(1+t)^\alpha)^l/((1+t)^l)^{\alpha^\varphi}\}$$

$$=(\alpha-\alpha^\varphi)\log(1+t)\in\hat{\mathbb{Z}}_l^{ur}[[t]].$$

Hence $\alpha-\alpha^\varphi=0$, i.e., $\alpha\in\mathbb{Z}_l$.

LEMMA 4. *If* $G(t)\in\hat{\mathbb{Z}}_l^{ur}[[t]]^0$ *satisfies* $G(u)\,G(v)\,G(w)=1$, *then* $G(t)=(1+t)^\alpha$ *for some* $\alpha\in\mathbb{Z}_l$.

Proof. Write

$$G(t)=\exp\left\{\sum_{m=0}^{\infty}\frac{a_m}{m!}T^m\right\},\qquad T=\log(1+t),\quad a_m\in\hat{\mathbb{Z}}_l^{ur}.$$

Then, by the condition,

$$\exp\left\{\sum_{m=0}^{\infty}\frac{a_m}{m!}(U^m+V^m+W^m)\right\}=1.$$

Hence $a_m=0$ for $m\neq 1$. Therefore, $G(t)=\exp\{a_1T\}=(1+t)^{a_1}$. By Lemma 3, $a_1\in\mathbb{Z}_l$.

LEMMA 5. *If* $(1+t)^{\alpha}\equiv 1 \bmod l$ $(\alpha\in\mathbb{Z}_l)$, *then* $\alpha=0$.

LEMMA 6. *Let* $\mathbb{F}_l$ *be the algebraic closure of* $\mathbb{F}_l$. *If* $\tilde{G}\in\bar{\mathbb{F}}_l[[t]]^{\times}$ *satisfies* $\tilde{G}((1+u)(1+v)-1)=\tilde{G}(u)\,\tilde{G}(v)$, *then there exists* $c\in\mathbb{Z}_l$ *such that* $\tilde{G}(t)\equiv(1+t)^c \bmod l$.

Proof of Lemmas 5 *and* 6. Let $\mathrm{End}_{\bar{\mathbb{F}}_l}(\hat{\mathbb{G}}_m)$ denote the endomorphism ring of 1-dimensional formal multiplicative group $\hat{\mathbb{G}}_m$ over $\bar{\mathbb{F}}_l$. It is well known that the homomorphism

$$\mathbb{Z}_l\ni c\mapsto(1+t)^c-1 \ (\mathrm{mod}\ l)\in\mathrm{End}_{\bar{\mathbb{F}}_l}(\hat{\mathbb{G}}_m)$$

is an isomorphism. Lemma 5 follows from this. On the other hand, the condition in Lemma 6 implies that $\tilde{G}(t)-1$ is an endomorphism of $\hat{\mathbb{G}}_m$ over $\bar{\mathbb{F}}_l$. Hence, from the above, $\tilde{G}(t)=(1+t)^c \ (\mathrm{mod}\ l)$ for some $c\in\mathbb{Z}_l$.

LEMMA 7. *If* $F(u,v)\in\mathfrak{F}$, *then there exists* $G(t)\in\hat{\mathbb{Z}}_l^{ur}[[t]]^{\times}$ *such that*

$$G(0)=1,$$

$$G((1+t)^{-1}-1)=G(t)^{-1},$$

$$\prod_{\zeta^l=1}G(\zeta(1+t)-1)=G^{\varphi}((1+t)^l-1),$$

and

$$F(u,v)=G(u)\,G(v)\,G(w).$$

Similarly, if $\tilde{F}(u,v)\in\tilde{\mathfrak{F}}$, *then there exists* $\tilde{G}(t)\in\bar{\mathbb{F}}_l[[t]]^{\times}$ *such that*

$$\tilde{G}(0)=1,\qquad \tilde{G}((1+t)^{-1}-1)=\tilde{G}(t)^{-1},$$

and

$$\tilde{F}(u,v)=\tilde{G}(u)\,\tilde{G}(v)\,\tilde{G}(w).$$

Proof. We easily see that the conditions (ii) and (iii) for $\mathfrak{F}$ (or $\tilde{\mathfrak{F}}$) (Section 1.2) imply that

$$F(u,v)\,F((1+u)(1+v)-1,w')=F(u,(1+v)(1+w')-1)\,F(v,w')$$

(u, v, w'; independent variables). Hence, from the conditions (i)–(iii) for $\mathfrak{F}$ (resp. $\bar{\mathfrak{F}}$), we can define[1] for each element $F(u, v) \in \mathfrak{F}$ (resp. $\bar{\mathfrak{F}}$) a two-dimensional formal group G_F over $\mathbb{Z}_l$ (resp. $\mathbb{F}_l$) by the law

$$(X_1, X_2)[+]_{G_F}(Y_1, Y_2)$$
$$= ((1+X_1)(1+Y_1)F(X_2, Y_2) - 1, (1+X_2)(1+Y_2) - 1).$$

The formal group G_F is an extension of $\hat{\mathbb{G}}_m$ by $\hat{\mathbb{G}}_m$, and $F(u, v) - 1$ is a 2-cocycle of this extension. But since there exist no non-trivial extensions of $\hat{\mathbb{G}}_m$ by $\hat{\mathbb{G}}_m$ over $\hat{\mathbb{Z}}_l^{ur}$ (resp. $\bar{\mathbb{F}}_l$), it must be a 2-coboundary, i.e., there exists $G(t) \in \hat{\mathbb{Z}}_l^{ur}[[t]]^\times$ (resp. $\bar{\mathbb{F}}_l[[t]]^\times$) such that $G(0) = 1$ and $F(u, v) = G(u)\,G(v)/G((1+u)(1+v) - 1)$. Further, because of the condition (iv) for $\mathfrak{F}$ (resp. $\bar{\mathfrak{F}}$), we get $G((1+t)^{-1} - 1) = G(t)^{-1}$. Hence, $F(u, v) = G(u)G(v)G(w)$.

In the following, let $F \in \mathfrak{F}$ and $G(t)$ be as above. Noting that l is odd and $F^\varphi = F$, we see from the condition (v) for $\mathfrak{F}$ that

$$\prod_{\zeta^l = 1} G(\zeta(1+u) - 1)\,G(\zeta(1+v) - 1)\,G(\zeta(1+w) - 1)$$
$$= G^\varphi((1+u)^l - 1)\,G^\varphi((1+v)^l - 1)\,G^\varphi((1+w)^l - 1).$$

Put

$$G'(t) = \prod_{\zeta^l = 1} G(\zeta(1+t) - 1).$$

Then $G'(t) \in \hat{\mathbb{Z}}_l^{ur}[[t]]$ and

$$G'(t) \equiv G(t)^l \equiv G^\varphi((1+u)^l - 1) \bmod l.$$

So if we put

$$H(t) = G'(t)/G^\varphi((1+t)^l - 1) \,(\in \hat{\mathbb{Z}}_l^{ur}[[t]]^\times),$$

we have

$$H(t) \equiv 1 \bmod l \qquad \text{and} \qquad H(u)\,H(v)\,H(w) = 1.$$

From this, we conclude by Lemmas 4 and 5 that $H = 1$, i.e.,

$$\prod_{\zeta^l = 1} G(\zeta(1+t) - 1) = G^\varphi((1+t)^l - 1).$$

LEMMA 8. *If* $G \in \hat{\mathbb{Z}}_l^{ur}[[t]]$ *satisfies* $G(t) \equiv 1 \mod l$ *and* $\prod_{\zeta^l = 1} G(\zeta(1+t) - 1) = G^\varphi((1+t)^l - 1)$, *then* $G(t) = 1$.

[1] This construction of G_F from F was pointed out to the authors by G. Anderson. We are very grateful to him.

Proof. Applying [2, Lem. 13(i)] successively to G, we get $G^{\varphi^i} \equiv 1 \bmod l^{i+1}$ for all $i \geqslant 1$. Hence $G = 1$.

LEMMA 9. *Put*

$$\mathscr{M} = \{G \in \hat{\mathbb{Z}}_l^{ur}[[t]]^0; \prod_{\zeta^l = 1} G(\zeta(1+t)-1) = G^{\varphi}((1+t)^l - 1)\}$$

and

$$\mathscr{M}^- = \{G \in \mathscr{M}; G((1+t)^{-1}-1) = G(t)^{-1}\}.$$

Then,

$$\mathscr{M} \bmod l = 1 + t\bar{\mathbb{F}}_l[[t]]$$

and

$$\mathscr{M}^- \bmod l = (1 + t\bar{\mathbb{F}}_l[[t]])^-$$

$$\overset{\text{def}}{=} \{\tilde{G} \in 1 + t\bar{\mathbb{F}}_l[[t]]; \tilde{G}((1+t)^{-1}-1) = \tilde{G}(t)^{-1}\}.$$

Proof. Let $\mathscr{N}$ be the Coleman norm operator on $\hat{\mathbb{Z}}_l^{ur}[[t]]^0$. The power series $\mathscr{N}G$ $(G \in \hat{\mathbb{Z}}_l^{ur}[[t]]^0)$ is characterized by

$$\prod_{\zeta^l = 1} G(\zeta(1+u)-1) = (\mathscr{N}G)^{\varphi}((1+u)^l - 1)$$

(see [2]). The condition for $\mathscr{M}$ is none other than $\mathscr{N}G = G^{\varphi}$. Take any $G \in \hat{\mathbb{Z}}_l^{ur}[[t]]^0$. By [2. IV], the limit $\mathscr{N}^{\infty}G = \lim_{i \to \infty}(\mathscr{N}^i G)^{\varphi^{-i}} \in \hat{\mathbb{Z}}_l^{ur}[[t]]$ exists and it satisfies

$$\mathscr{N}(\mathscr{N}^{\infty}G) = (\mathscr{N}^{\infty}G)^{\varphi} \qquad \text{and} \qquad \mathscr{N}^{\infty}G \equiv G \bmod l.$$

The first part of the lemma follows from this. Next, let $\tilde{G} \in (1 + t\bar{\mathbb{F}}_l[[t]])^-$ and take $G \in \mathscr{M}$ such that $G \bmod l = \tilde{G}$. Then $G((1+t)^{-1}-1) = G(t)^{-1} \bmod l$. Put $H(t) = G((1+t)^{-1}-1)\,G(t)$. Then $H(t) \equiv 1 \bmod l$. Since $\prod_{\zeta^l=1} G(\zeta(1+t)-1) = G^{\varphi}((1+t)^l - 1)$, we get $\prod_{\zeta^l=1} H(\zeta(1+t)-1) = H^{\varphi}((1+t)^l - 1)$. Hence, by Lemma 9, $H(t) = 1$. Therefore, $G(t) \in \mathscr{M}^-$. This proves the lemma.

2.4. *Proof of Proposition* 2

It is clear that the reduction modulo l from $\mathfrak{F}$ to $\tilde{\mathfrak{F}}$ is a Λ-homomorphism. First, we prove its surjectivity. Take any $\tilde{F} \in \tilde{\mathfrak{F}}$. By Lemma 7, there exists $\tilde{G} \in \bar{\mathbb{F}}_l[[t]]$ such that

$$\tilde{G}(0) = 1,$$

$$\tilde{G}((1+t)^{-1}-1) = \tilde{G}(t)^{-1},$$

and

$$\tilde{F}(u, v) = \tilde{G}(u)\,\tilde{G}(v)\,\tilde{G}(w).$$

Further, by Lemma 9, there exists $G \in \hat{\mathbb{Z}}_l^{ur}[[t]]^0$ such that

$$G((1+t)^{-1}-1) = G(t)^{-1},$$

$$\prod_{\zeta^l=1} G(\zeta(1+t)-1) = G^{\varphi}((1+t)^l - 1),$$

and

$$G \bmod l = \tilde{G}.$$

Since l is odd, the conditions $G(0) \equiv 1 \bmod l$ and $G((1+t)^{-1}-1) = G(t)^{-1}$ imply $G(0) = 1$. Because

$$G(u)\,G(v)\,G(w) \bmod l = \tilde{F}(u, v) \in \mathbb{F}_l[[u, v]],$$

we have

$$G^{\varphi}(u)\,G^{\varphi}(v)\,G^{\varphi}(w) \equiv G(u)\,G(v)\,G(w) \bmod l.$$

Then, if we put $H(t) = G^{\varphi}/G$, we have by Lemma 6,

$$H(t) \equiv (1+t)^c \bmod l \qquad \text{for some} \quad c \in \mathbb{Z}_l.$$

Write

$$H(t) = (1+t)^c\,H'(t), \qquad H' \in \hat{\mathbb{Z}}_l^{ur}[[t]].$$

Then,

$$H'(t) \equiv 1 \bmod l$$

and

$$\prod_{\zeta^l=1} H'(\zeta(1+t)-1) = H'^{\varphi}((1+t)^l - 1).$$

So by Lemma 8, $H' = 1$. Hence $G^{\varphi}(t) = G(t) \cdot (1+t)^c$. Then if we put $F = G(u)\,G(v)\,G(w)$, we get $F^{\varphi} = F$, i.e., $F \in \mathbb{Z}_l[[u, v]]^{\times}$ and $F \in \mathfrak{F}$. Since $F \bmod l = \tilde{F}$, the surjectivity holds. Next, we prove the injectivity. Let $F \in \mathfrak{F}$ satisfy $F \bmod l = 1$. By Lemma 7, we can write $F = G(u)\,G(v)\,G(w)$ where $G(t) \in \hat{\mathbb{Z}}_l^{ur}[[t]]^{\times}$ such that

$$G(0) = 1,$$

$$G((1+t)^{-1}-1) = G^{-1},$$

and

$$\prod_{\zeta^l=1} G(\zeta(1+t)-1) = G^{\varphi}((1+t)^l-1).$$

Since $F \equiv 1 \mod l$, we get $G(u)\,G(v) \equiv G(w)^{-1} \bmod l$ and hence $G(u)\,G(v) \equiv G((1+u)(1+v)-1) \bmod l$. Therefore, by Lemma 6, $G(t) \equiv (1+t)^c \bmod l$ for some $c \in \mathbb{Z}_l$. If we put $G'(t) = G(t)(1+t)^{-c}$, then

$$\prod_{\zeta^l=1} G'(\zeta(1+t)-1) = G'^{\varphi}((1+t)^l-1)$$

and

$$G'(t) \equiv 1 \mod l.$$

Hence by Lemma 8, $G' = 1$. This shows that $F = 1$ and completes the proof of Proposition 2.

3. Proof of Theorem 2

3.1. *Relations between* Im **F**, Ker **F**, *and Ideal Class Groups*

In this subsection, we state two propositions on the image and the kernel of the homomorphism

$$\mathbf{g}\colon \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}(\boldsymbol{\mu}_{l^\infty})) \ni \rho \mapsto g_\rho \in \mathscr{V}^-$$

(cf. Section 1.1). Theorem 2 is then an immediate consequence of these propositions and Proposition 1.

Let Ω_l be the maximum pro-l abelian extension over $\mathbb{Q}(\boldsymbol{\mu}_{l^\infty})$ unramified outside l and $\Omega_l^-/\mathbb{Q}(\boldsymbol{\mu}_{l^\infty})$ be the "odd part" of $\Omega_l/\mathbb{Q}(\boldsymbol{\mu}_{l^\infty})$. Put $\mathfrak{G} = \mathrm{Gal}(\Omega_l^-/\mathbb{Q}(\boldsymbol{\mu}_{l^\infty}))$. It is known that the Galois representation **F** (resp. **g**) factors through $\mathfrak{G}$ and the induced homomorphism **F** (resp. **g**): $\mathfrak{G} \to \mathfrak{F}$ (resp. $\mathscr{V}^-$) is compatible with the action of Λ (see [6, Th. 1]). Here, $j_\alpha \in \mathbb{Z}_l^\times$ acts on $\mathfrak{G}$ by conjugation and on $\mathscr{V}^-$ in the natural way (see Section 1.*N*). Hence, the groups $\mathscr{V}^-/(\mathrm{Im}\,\mathbf{g})$ and $\mathrm{Ker}\,\mathbf{g}$ ($\subset \mathfrak{G}$) admit Λ-module structures. We easily see that the modules $\mathscr{V}^-/(\mathrm{Im}\,\mathbf{g})$ and $\mathrm{Ker}\,\mathbf{g}$ are finitely generated and torsion over Λ_1 and further that $\mathrm{Ker}\,\mathbf{g} = \mathrm{Tor}\,\mathfrak{G}$ by using (1) a theorem of Iwasawa on the structure of $\mathfrak{G}$ as a Λ-module (see, e.g., [12, Th. 13.31]), (2) $\mathscr{V}^- \simeq \Lambda^-$ [3, Th. 3] and (3) Ω_l^- is unramified over the intermediate field of $\Omega_l^-/\mathbb{Q}(\boldsymbol{\mu}_{l^\infty})$ fixed by $\mathrm{Ker}\,\mathbf{g}$ [5, Prop. 2]. In Section 3.3, we shall prove the following

Proposition 3. *The torsion Λ_1-modules* $\mathrm{Ker}\,\mathbf{g}$ *and* $\mathscr{V}^-(\mathrm{Im}\,\mathbf{g})$ *have the same characteristic power series.*

In Section 3.4, we shall prove the following

PROPOSITION 4. *The Λ-modules* $(\mathrm{Ker}\,\mathbf{g})(-1)$ *and* $\mathrm{Hom}(A_\infty^+, \mathbb{Q}_l/\mathbb{Z}_l)$ *are isomorphic.*

3.2. *Realization of g_ρ as a Coleman Power Series*

The purpose of this subsection is to realize the power series g_ρ as an "additive Coleman power series" (i.e., the "logarithm" of a usual Coleman power series). First, we recall some facts and introduce some notations.

Let $\mathfrak{U}_n$ be the group of principal units of the l^nth local cyclomotic field $\mathbb{Q}_l(\zeta_n)$ and $\mathfrak{U} = \varprojlim \mathfrak{U}_n$ be the projective limit w.r.t. the relative norm. Coleman [2] constructed a natural embedding [Col] from $\mathfrak{U}$ into the multiplicative group $\mathbb{Z}_l[[t]]^0 = \{G \in \mathbb{Z}_l[[t]]^\times; G(0) \equiv 1 \pmod{l}\}$ which is associated to the fixed basis ζ of $T_l(\mathbb{G}_m)$. For us, the composite homomorphism $\lambda \circ [\mathrm{Col}]$ is more convenient. Here, λ is the homomorphism from $\mathbb{Z}_l[[t]]^0$ to the additive group $\mathbb{Z}_l[[t]]$;

$$G \mapsto \lambda G = \log G - \frac{1}{l} \log G((1+t)^l - 1).$$

Put

$$\mathscr{V} = \left\{ g \in \mathbb{Z}_l[[t]]; \sum_{\zeta^l = 1} g(\zeta(1+t) - 1) = 0 \right\}.$$

Coleman proved that the image of $\lambda \circ [\mathrm{Col}]$ is contained in $\mathscr{V}$ and further, completely described the image [3, Th. 4].

For each integer $m \geqslant 0$, we denote by δ_m the mth Coates–Wiles homomorphism (associated to the fixed basis ζ of $T_l(\mathbb{G}_m)$): $\mathfrak{U} \to \mathbb{Z}_l$ (see, e.g., [12, p. 137]). Since $\delta_1(\zeta^s) = s$, we have a decomposition

$$\mathfrak{U}^- = \{\varepsilon \in \mathfrak{U}^-; \delta_1(\varepsilon) = 0\} \oplus \{\zeta^s; s \in \mathbb{Z}_l\}.$$

Let $\mathfrak{T}$ be the inertia group of an extension of l in $\Omega_l^-/\mathbb{Q}(\mu_{l^\infty})$. By class field theory, $\mathfrak{T}$ is isomorphic to the group $\mathfrak{U}^-$ modulo the closure of the group of global units (see, e.g., [12, Cor. 13.6]). Hence, we may identify $\mathfrak{T}$ with the group $\{\varepsilon \in \mathfrak{U}^-; \delta_1(\varepsilon) = 0\}$. In the following, we regard the homomorphism $\lambda \circ [\mathrm{Col}]$ (resp. δ_m) as one from $\mathfrak{T}$ to $\mathbb{Z}_l[[t]]$ (resp. $\mathbb{Z}_l$).

For an odd integer i with $1 \leqslant i \leqslant l-2$, let $f_i(t)$ ($\in \mathbb{Q}_l[[t]]$) be the power series corresponding to l-adic L-function $L_l(s, \omega^{1-i})$, namely, $f_i((1+l)^s - 1) = L_l(s, \omega^{1-i})$. Recall that for $i \neq 1$, $f_i \in \mathbb{Z}_l[[t]]$ and for $i = 1$, $f_1 = f_1'/(t-l)$ with $f_1' \in \mathbb{Z}_l[[t]]^\times$. We regard $f_i (i \neq 1)$ and f_1^{-1} as an element of $\Lambda_1 = \mathbb{Z}_l[[1 + l\mathbb{Z}_l]] \simeq \mathbb{Z}_l[[t]]$.

Now, the power series g_ρ is realized as an additive Coleman power series

as follows. Recall that (as in Section 1.*N*) $\mathfrak{G}^{(i)}$ and $\mathfrak{T}(i)$ are the ω^i-eigenspace of $\mathfrak{G}$ and $\mathfrak{T}$, respectively.

PROPOSITION 5. (1) *When* $i \neq 1$; $f_i \mathfrak{G}^{(i)} \subset \mathfrak{T}^{(i)}$ *and for* $\rho \in \mathfrak{G}^{(i)}$, $g_\rho(t) = \lambda \circ [\mathrm{Col}](f_i \rho)$. (2) *When* $i = 1$; $\mathfrak{G}^{(1)} = \mathfrak{T}^{(1)}$ *and for* $\rho \in \mathfrak{G}^{(1)}$, $f_1^{-1} * g_\rho = \lambda \circ [\mathrm{Col}](\rho)$. (* *denotes the usual action of* Λ_1 *on* $\mathbb{Z}_l[[t]]$.)

Proof of Proposition 5. The proof is based upon [6, Th. 10] which asserts that for $\rho \in \mathfrak{T}^{(i)}$,

$$g_\rho(t) = \lambda \circ [\mathrm{Col}](f_i \rho), \qquad i \neq 1,$$
$$f_1^{-1} * g_\rho(t) = \lambda \circ [\mathrm{Col}](\rho), \qquad i = 1.$$

The assertion (2) follows immediately from the above because $\mathfrak{G}^{(1)} = \mathfrak{T}^{(1)}$ by the Stickelberger theorem (see, e.g., [12, Prop. 6.16]). Assume $i \neq 1$. By a theorem of Mazur and Wiles [11], f_i is a characteristic power series of the torsion Λ_1-module $\mathfrak{G}^{(i)}/\mathfrak{T}^{(i)}$. But since $\mathfrak{G}^{(i)}/\mathfrak{T}^{(i)}$ has no non-trivial finite Λ_1-submodule (see, e.g., [12, Prop. 13.28]), we see that $f_i \mathfrak{G}^{(i)} \subset \mathfrak{T}^{(i)}$. Therefore, we can consider the homomorphism

$$\mathfrak{G}^{(i)} \ni \rho \mapsto \lambda \circ [\mathrm{Col}](f_i \rho) \in \mathbb{Z}_l[[t]].$$

Now, by [6, Th. 10], this homomorphism coincides on $\mathfrak{T}^{(i)}$ with the homomorphism $\mathbf{g}^{(i)} = \mathbf{g} | \mathfrak{G}^{(i)}$. Hence, they coincide on the whole Galois group $\mathfrak{G}^{(i)}$, i.e., $g_\rho = \lambda \circ [\mathrm{Col}](f_i \rho)$ for all $\rho \in \mathfrak{G}^{(i)}$, by the following

LEMMA 10. *The inertia restriction*

$$\mathrm{Hom}_{\mathbb{Z}_l^\times}(\mathfrak{G}^{(i)}, \mathbb{Z}_l[[t]]) \to \mathrm{Hom}_{\mathbb{Z}_l^\times}(\mathfrak{T}^{(i)}, \mathbb{Z}_l[[t]])$$

is injective for any odd integer i *with* $1 \leqslant i \leqslant l-2$.

Proof of Lemma 10. Let $\mathscr{f} \in \mathrm{Hom}_{\mathbb{Z}_l^\times}(\mathfrak{G}^{(i)}, \mathbb{Z}_l[[t]])$. We easily see that for $\rho \in \mathfrak{G}^{(i)}$, the power series $\mathscr{f}_\rho$ can be written in the form

$$\mathscr{f}_\rho(t) = \sum_{m \equiv i} \frac{a_m(\rho)}{m!} T^m$$

with $a_m \in \mathrm{Hom}_{\mathbb{Z}_l^\times}(\mathfrak{G}^{(i)}, \mathbb{Z}_l(m))$. Here, the summation is taken over all integers m (>0) with $m \equiv i \pmod{l-1}$. Assume that $\mathscr{f} \neq 0$ but $\mathscr{f} | \mathfrak{T}^{(i)} = 0$. Then, $a_m | \mathfrak{T}^{(i)} = 0$ for all integers $m \equiv i \pmod{l-1}$. From a theorem of Mazur and Wiles [11], the inertia restriction

$$\mathrm{Hom}_{\mathbb{Z}_l^\times}(\mathfrak{G}^{(i)}, \mathbb{Z}_l(m)) \to \mathrm{Hom}_{\mathbb{Z}_l^\times}(\mathfrak{T}^{(i)}, \mathbb{Z}_l(m)) \qquad (m \equiv i \pmod{l-1})$$

is injective if and only if $L_l(m, \omega^{1-i}) \neq 0$. But since there are only finitely many m such that $L_l(m, \omega^{1-i}) = 0$, $a_m = 0$ except for a finite number of m. Let M be the largest m such that $a_m \neq 0$. Then,

$$\mathscr{f}_\rho(t) = \sum_{\substack{m \equiv i \\ m \leqslant M}} \frac{a_m(\rho)}{m!} T^m \in \mathbb{Z}_l[[t]].$$

Hence, $D^{M-1}\mathscr{f}_\rho(t) = a_M(\rho)T \in \mathbb{Z}_l[[t]]$. This is a contradiction because $T = \log(1+t) \notin \mathbb{Z}_l[[t]]$ and $a_M(\rho) \neq 0$ for some $\rho \in \mathfrak{G}^{(i)}$. This proves the lemma.

Now the proof of Proposition 5 is completed.

COROLLARY 1. [4, Formula (5.4), VII].

$$f_1^{-1} * \{g_\rho; \rho \in \mathfrak{G}^{(1)}\} = \lambda \circ [\mathrm{Col}](\mathfrak{T}^{(1)}) \qquad \textit{and} \qquad \mathrm{Im}\, \mathbf{g} \subset \mathscr{V}^-.$$

Proof. This follows immediately from Proposition 5 and [3, Th. 4].

Let $\dagger$ denote the action of Λ_1 on $\mathbb{Z}_l[[t]]$ such that $j_\alpha \dagger f = \alpha \cdot j_\alpha * f$ $(j_\alpha \in \Gamma, f \in \mathbb{Z}_l[[t]])$.

COROLLARY 2. *Let i be any odd integer with $1 \leqslant i \leqslant l-2$ and ρ be any element of $\mathfrak{G}^{(i)}$.*

When $i \neq 1$, $h_\rho(t) = -D \log[\mathrm{Col}](f_i \rho)(t)$.

When $i = 1$, $f_1^{-1} \dagger h_\rho(t) = -D \log[\mathrm{Col}](\rho)(t)$.

Proof. By the coefficient formula of F_ρ (see Section 1.1), we get

$$h_\rho((1+t)^l - 1) - h_\rho(t) = Dg_\rho(t).$$

When $i \neq 1$, we see from the above and Proposition 5(1) that

$$\begin{aligned} &h_\rho(t) + (D \log[\mathrm{Col}](f_i \rho))(t) \\ &\quad = h_\rho((1+t)^l - 1) + (D \log[\mathrm{Col}](f_i \rho))((1+t)^l - 1). \end{aligned}$$

From this, we see that the left hand side is a constant. Since $F_\rho \equiv 1 \pmod{uvw}$, $h_\rho(0) = 0$, and since $i \neq 1$, we see that $(D \log[\mathrm{Col}](f_i \rho))(0) = 0$ (see [3, Th. 4]). Therefore, $h_\rho(t) = -(D \log[\mathrm{Col}](f_i \rho))(t)$. Next assume $i = 1$. Noting that $f_1^{-1} \dagger Dg_\rho = D(f_1^{-1} * g_\rho)$, we get the assertion from Proposition 5(2).

From Corollary 2, we immediately obtain

COROLLARY 3. *When* $i \neq 1$, $\{h_\rho; \rho \in \mathfrak{G}^{(i)}\} \subset D\log[\mathrm{Col}](\mathfrak{T}^{(i)})$.
When $i = 1$, $f_1^{-1}\dagger\{h_\rho; \rho \in \mathfrak{G}^{(1)}\} = D\log[\mathrm{Col}](\mathfrak{T}^{(1)})$.

3.3. *Proof of Proposition* 3

Let i be any odd integer with $1 \leqslant i \leqslant l-2$ and $\mathbf{g}^{(i)}$ be as before the homomorphism

$$\mathbf{g}^{(i)}: \mathfrak{G}^{(i)} \ni \rho \mapsto g_\rho \in \mathscr{V}^{(i)}.$$

It suffices to prove that $\mathrm{Ker}\,\mathbf{g}^{(i)}$ and $\mathscr{V}^{(i)}/(\mathrm{Im}\,\mathbf{g}^{(i)})$ have the same characteristic power series.

First, assume $i = 1$. By the Stickelberger theorem (see, e.g., [12, Prop. 6.16]), $\mathfrak{G}^{(i)}$ is torsion free over Λ_1 and hence $\mathrm{Ker}\,\mathbf{g}^{(i)} = \{0\}$. On the other hand, we see from Theorem C and the Stickelberger theorem that $\mathrm{Im}\,\mathbf{g}^{(1)} = \mathscr{V}^{(1)}$. Hence, the assertion is valid when $i = 1$.

In the following, we always assume $i > 1$. Put

$\Omega_l^{(i)}$: the subextension of $\Omega_l^-/\mathbb{Q}(\boldsymbol{\mu}_{l^\infty})$ fixed by $\bigoplus_{i' \neq i} \mathfrak{G}^{(i')}$,

$M^{(i)}$: the maximum unramified subextension of $\Omega_l^{(i)}/\mathbb{Q}(\boldsymbol{\mu}_{l^\infty})$,

C: the subextension of $\Omega_l^-/\mathbb{Q}(\boldsymbol{\mu}_{l^\infty})$ fixed by $\mathrm{Ker}\,\mathbf{g}$,

$C^{(i)} := \Omega_l^{(i)} \cap C$,

$L^{(i)} := M^{(i)} \cap C$,

$\mathfrak{H}^{(i)} := \mathrm{Gal}(C^{(i)}/\mathbb{Q}(\boldsymbol{\mu}_{l^\infty}))$.

Note that since $\Omega_l^{(i)}/C^{(i)}$ is unramified (see [5, Prop. 2]), $C^{(i)}M^{(i)} = \Omega_l^{(i)}$ and the inertia group $\mathfrak{T}^{(i)}$ ($\subset \mathfrak{H}^{(i)}$) of an extension of l in $C^{(i)}/\mathbb{Q}(\boldsymbol{\mu}_{l^\infty})$ is canonically isomorphic to $\mathfrak{T}^{(i)}$. Let h_i be a characteristic power series of the torsion Λ_1-module $\mathrm{Gal}(L^{(i)}/\mathbb{Q}(\boldsymbol{\mu}_{l^\infty}))$. Then, by using a theorem of Mazur and Wiles [11], we see that f_i/h_i is a characteristic power series of $\mathrm{Ker}\,\mathbf{g}^{(i)} = \mathrm{Gal}(\Omega_l^{(i)}/C^{(i)}) \simeq \mathrm{Gal}(M^{(i)}/L^{(i)})$. On the other hand, we see that

$$\mathscr{V}^{(i)}/(\mathrm{Im}\,\mathbf{g}^{(i)}) \simeq \mathfrak{T}^{(i)}/f_i\mathfrak{G}^{(i)}$$

from Proposition 5(1) and the fact that (since $i \neq 1$) the homomorphism $\lambda \circ [\mathrm{Col}]: \mathfrak{T}^{(i)} \to \mathscr{V}^{(i)}$ is an isomorphism (see [3, Th. 4]). Since $\Omega_l^{(i)}/C^{(i)}$ is unramified, the restriction $\mathfrak{G}^{(i)} \to \mathfrak{H}^{(i)}$ induces an isomorphism: $\mathfrak{T}^{(i)}/f_i\mathfrak{G}^{(i)} \simeq \mathfrak{T}^{(i)}/f_i\mathfrak{H}^{(i)}$. By using [12, Th. 13.31] and $\mathrm{Ker}\,\mathbf{g}^{(i)} = \mathrm{Tor}\,\mathfrak{G}^{(i)}$ (see Section 3.1), we see that $\mathfrak{H}^{(i)}$ is pseudo-isomorphic (in the sense of [12]) to Λ_1. Hence, by the very definition of h_i, the Λ_1-submodule $\mathfrak{T}^{(i)} \cap h_i\mathfrak{H}^{(i)}$ of $\mathfrak{H}^{(i)}$ is of finite index both in $\mathfrak{T}^{(i)}$ and in $h_i\mathfrak{H}^{(i)}$. From this, we see that $\mathfrak{T}^{(i)}/f_i\mathfrak{H}^{(i)}$ is pseudo-isomorphic to $h_i\mathfrak{H}^{(i)}/f_i\mathfrak{H}^{(i)}$. But since $\mathfrak{H}^{(i)}$ is pseudo-isomorphic to Λ_1, f_i/h_i is a characteristic power series of $\mathscr{V}^{(i)}/(\mathrm{Im}\,\mathbf{g}^{(i)})$. This proves the proposition.

3.4. *Proof of Proposition* 4

Proposition 4 is more or less known. So, we shall only sketch the proof briefly.

Let X be the submodule of $\mathbb{Q}(\mu_{l^\infty})^\times \otimes \mathbb{Q}_l/\mathbb{Z}_l$ such that

$$\Omega_l = \mathbb{Q}(\mu_{l^\infty}, a^{1/l^n}; \quad \text{all} \quad a \otimes l^{-n} \in X).$$

Then, we have the Kummer pairing:

$$\mathrm{Gal}(\Omega_l/\mathbb{Q}(\mu_{l^\infty})) \times X \to \mu_{l^\infty}.$$

We easily see that

$$C = \mathbb{Q}(\mu_{l^\infty}, \varepsilon^{1/l^n}; \text{ all units } \varepsilon \text{ of } \mathbb{Q}(\mu_{l^\infty}) \text{ and all } n \geqslant 1)$$

from [4, Section 4; 7, Cor. 1 of Th. B] and the fact that for $n \geqslant 1$, $[E_n : C_n]$ is finite. Here, E_n (resp. C_n) denotes the groups of units (resp. the group of circular units) of $\mathbb{Q}(\mu_{l^\infty})$. Therefore, we obtain from the above Kummer pairing, a Λ-isomorphism

$$\mathrm{Gal}(\Omega_l/C)(-1) \simeq \mathrm{Hom}(X/(E_\infty \otimes \mathbb{Q}_l/\mathbb{Z}_l), \mathbb{Q}_l/\mathbb{Z}_l).$$

Here, $E_\infty = \bigcup_n E_n$. Taking the "even part" of both sides, we obtain the proposition because $X/(E_\infty \otimes \mathbb{Q}_l/\mathbb{Z}_l) \simeq A_\infty$ (see, e.g., [12, p. 293]).

4. Proofs of Theorems 3 and 3′

4.1. *(Additive) Coleman Power Series Modulo l*

Coleman characterized completely the image of the homomorphism $\lambda \circ [\mathrm{Col}]$ from the group $\mathfrak{U}$ of local units to the additive group $\mathbb{Z}_l[[t]]$ by means of his "trace" operator [3, Th. 4]. In this subsection, we shall determine the structure of the image of $\lambda \circ [\mathrm{Col}] \bmod l$ by means of a certain differential operator on $\mathbb{F}_l[[t]]$.

Proposition 6. *Put* $\tilde{\mathscr{V}} = \mathscr{V} \bmod l$. *Then*

(i) *there is an exact sequence of* $\tilde{\Lambda} = \mathbb{F}_l[[\mathbb{Z}_l^\times]]$*-modules,*

$$1 \to T_l(\mathbb{G}_m)/T_l(\mathbb{G}_m)^l \to \mathfrak{U}/\mathfrak{U}^l \to \{g \in \tilde{\mathscr{V}}; Dg|_{t=0} = 0\} \to 0,$$

$$\cup \qquad\qquad \cup$$

$$\varepsilon \longrightarrow \lambda \circ [\mathrm{Col}](\varepsilon) \bmod l$$

(ii) $\tilde{\mathscr{V}} = \{g \in \mathbb{F}_l[[t]]; (D^{l-1}-1)g = 0\}$,

(iii) $\tilde{\mathscr{V}}$ *is a free* $\tilde{\Lambda}$*-module generated by* $1+t$.

PROPOSITION 6'. *Put* $F(t) = \sum_{m \geqslant 1}((1-l^m)^{-1}/m!)T^m$. *Then,* $F \in \mathbb{Z}_l[[t]]$. *Put* $\tilde{F} = F \bmod l$ *and* $\tilde{\mathscr{W}} = \tilde{\Lambda} \cdot \tilde{F} + \mathbb{F}_l$. *Then*

(i) *there is an isomorphism of* $\tilde{\Lambda}$*-modules,*

$$\begin{array}{ccc} \mathfrak{U}/\mathfrak{U}^l & \to & \{g \in \tilde{\mathscr{W}}; D^{l-1}g|_{t=0} = 0\} \otimes \tilde{\boldsymbol{\mu}}_{l-1}, \\ \cup & & \cup \\ \varepsilon & \longrightarrow & D\log[\mathrm{Col}](\varepsilon) \bmod l \otimes \eta \end{array}$$

here, $\tilde{\boldsymbol{\mu}}_{l-1}$ *denotes the group of* $(l-1)$*st roots of unity in* $\bar{\mathbb{F}}_l$ *and* η *is its generator, and on* $\tilde{\boldsymbol{\mu}}_{l-1}$, $j_\alpha \in \mathbb{Z}_l^\times$ *acts by* $\eta^{j_\alpha} = \eta^\alpha$,

(ii) $\tilde{\mathscr{W}} = \{g \in \mathbb{F}_l[[t]]; \mathscr{D}(g) = 0\}$ (*see Section* 1.2 *for the definition of* $\mathscr{D}$),

(iii) *the* $\tilde{\Lambda}$*-torsion submodule of* $\tilde{\mathscr{W}}$ *is* $\mathbb{F}_l$.

Proofs of Propositions 6 *and* 6'. Since $\mathscr{V}$ is a free Λ-module generated by $1+t$ [3, Lem. 2] and $\mathbb{Z}_l[[t]] = \mathscr{V} + \mathbb{Z}_l[[(1+t)^l - 1]]$ (direct sum) [3, Th. 3], we get $\tilde{\mathscr{V}} = \tilde{\Lambda} \cdot (1+t)$ and $\mathbb{F}_l[[t]] = \tilde{\mathscr{V}} + \mathbb{F}_l[[t^l]]$. For $g \in \mathbb{F}_l[[t]]$ and $j_\alpha \in \mathbb{Z}_l^\times$, we see that

$$(D^{l-1}-1)(j_\alpha g) = \alpha^{l-1} j_\alpha D^{l-1} g - j_\alpha g = j_\alpha((D^{l-1}-1)g)$$

because $\alpha^{l-1} \equiv 1 \pmod{l}$. Hence, for any $\omega \in \tilde{\Lambda}$, $(D^{l-1}-1)(\omega(1+t)) = \omega(D^{l-1}-1)(1+t)$. But since $D(1+t) = 1+t$, we see that $(D^{l-1}-1)\tilde{\mathscr{V}} = \{0\}$. On the other hand, since $D(t^l) = l(1+t)t^{l-1} = 0$, we get $(D^{l-1}-1)(g(t^l)) = -g(t^l)$. This proves (ii) of Proposition 6. Let $\omega \in \Lambda$. Assume $\omega(1+t) \equiv 0 \pmod{l}$. Then, we see that $(1/l)((\omega(1+t)) \in \mathscr{V}$ by [3, Lem. 2]. Hence, $(1/l)(\omega(1+t)) = \omega'(1+t)$ for some $\omega' \in \Lambda$. But since $\mathscr{V}$ is free over Λ, we obtain $\omega = l\omega'$. This proves (iii) of Proposition 6. The assertion (i) of Proposition 6 follows easily from [3, Th. 4]. We easily see that $F(t) - F((1+t)^l - 1) = t$. Using this relation, we see that $F(t) \in \mathbb{Z}_l[[t]]$. By a method similar to the proof of [3, Th. 3], we obtain $\mathbb{Z}_l[[t]] = \Lambda \cdot F + \mathbb{Z}_l + (1-\sigma)\mathbb{Z}_l[[t]]$; here $\sigma(t) = (1+t)^l - 1$. Then, the proof of (ii) and (iii) of Proposition 6' goes through similarly to that of Proposition 6. From [3, Th. 4], it follows that the power series $D\log[\mathrm{Col}](\varepsilon)(t)$ is an element of $\mathbb{Z}_l[[t]]$. The relation $(D^{l-1}-1)(\lambda \circ [\mathrm{Col}](\varepsilon) \bmod l) = 0$ implies that

$$\mathscr{D}(D\log[\mathrm{Col}](\varepsilon) \bmod l) = 0.$$

Hence, the map in (i) of Proposition 6′ is well defined. Further, by using [3, Th. 4] again, we see that the map is bijective Λ-homomorphism.

4.2. *Proofs of Theorems* 3 *and* 3′

Theorems 3 and 3′ follow from Proposition 5 (and its corollaries), Proposition 6, 6′, and the following

PROPOSITION 7. *The following conditions are equivalent.*

(1) *The Vandiver conjecture at l is valid.*

(2) *For any odd integer i with $3 \leqslant i \leqslant l-2$,*

$$\{g_\rho \bmod l;\ \rho \in \mathfrak{G}^{(i)}\} = \lambda \circ [\mathrm{Col}](\mathfrak{T}^{(i)}) \bmod l.$$

(2′) *For any odd integer i with $3 \leqslant i \leqslant l-2$,*

$$\{h_\rho \bmod l;\ \rho \in \mathfrak{G}^{(i)}\} = D \log[\mathrm{Col}](\mathfrak{T}^{(i)}) \bmod l.$$

Proof. (1) $\Rightarrow$ (2), (2′): Assume the Vandiver conjecture at l. Let i be any odd integer with $3 \leqslant i \leqslant l-2$. Then, under the assumption, $\mathfrak{G}^{(i)}/\mathfrak{T}^{(i)} \simeq \Lambda_1/(f_i)$ (see, e.g., [12, Th. 10.16]) and $\mathfrak{G}^{(i)} \simeq \Lambda_1$ (see, e.g., [10, Th. 4.1]). From these, we obtain $f_i \cdot \mathfrak{G}^{(i)} = \mathfrak{T}^{(i)}$. The implication (1) $\Rightarrow$ (2) (resp. (1) $\Rightarrow$ (2′)) follows immediately from this and Proposition 5 (resp. Cor. 2 of Prop. 5).

(2) $\Rightarrow$ (1): Let i be any odd integer with $3 \leqslant i \leqslant l-2$. By Proposition 6, $\lambda \circ [\mathrm{Col}](\mathfrak{T}^{(i)}) \bmod l$ is a free $\tilde{\Lambda}_1 = \mathbb{F}_l[[1 + l\mathbb{Z}_l]]$-module generated by the power series

$$\sum_{m \equiv i} \frac{1}{m!} T^m \bmod l = \frac{1}{i!} t^i + \cdots \qquad \bmod l.$$

Hence, under the condition (2), there exists $\rho \in \mathfrak{G}^{(i)}$ such that $\chi_i(\rho) \equiv 1 \pmod l$ for each odd integer i with $3 \leqslant i \leqslant l-2$. Therefore, the condition (1) follows by [5, Prop. 4].

(2′) $\Rightarrow$ (1): This can be proved similarly as above.

Remark. Our differential operators $D^{l-1} - 1$ and $\mathscr{D}$ on $\mathbb{F}_l[[t]]$ are closely related to the Coleman trace operator $\mathscr{S}$ on $\mathbb{Z}_l[[t]]$ as follows. Since $\mathscr{S}(g) \equiv 0 \pmod l$ for any $g \in \mathbb{Z}_l[[t]]$ (see [3]), $(1/l)\mathscr{S}$ induces an operator on $\mathbb{F}_l[[t]]$. Put

$$\tilde{\mathscr{S}} = \sigma \circ \left(\left(\frac{1}{l} \mathscr{S} \right) \bmod l \right),$$

where $\sigma(t)=t^l$. Then, by using some results in [3, Sect. 2], we can prove that $D^{l-1}-1=-\tilde{\mathscr{P}}$ and

$$\mathscr{D}(g)=-\tilde{\mathscr{P}}(g)+(\tilde{\mathscr{P}}-1)g|_{t=0}+\sigma(g) \qquad \text{for} \quad g\in\mathbb{F}_l[[t]].$$

APPENDIX: Interpretation of the Power Series "g_ρ" as a Measure on $\mathbb{Z}_l$, and an Alternative Proof of Theorem C

As is shown in the proofs of [7, Prop. 2; and 5, Prop. 3], we can interpret the power series Dg_ρ as a certain $\mathbb{Z}_l$-valued measure on $\mathbb{Z}_l$ (see also [1, Sect. 3]). We first recall this interpretation and then as its application, we give an alternative proof of the latter half of Theorem C which is somewhat more direct compared with Coleman's proof.

Let $\zeta=(\zeta_n)_n$ be the generator of $T_l(\mathbb{G}_m)$ fixed in Section 1.1. For each $n\geqslant 1$ and $\rho\in\mathfrak{G}$, define a map

$$\delta_{\rho,n}\colon \mathbb{Z}/l^n\to\mathbb{Z}/l^n$$

by

$$\begin{aligned}\{(\zeta_n^a-1)^{1/l^n}\}^{\rho-1}&=\zeta_n^{\delta_{\rho,n}(a)} \qquad \text{if} \quad a\in(\mathbb{Z}/l^n)^\times\\ \delta_{\rho,n}(a)&=0 \qquad \text{otherwise.}\end{aligned} \tag{$*$}$$

Then, the system $\{\delta_{\rho,n}\}_n$ defines a $\mathbb{Z}_l$-valued measure on $\mathbb{Z}_l$. Identify $\mathbb{Z}_l[[t]]$ with $\varprojlim_n(\mathbb{Z}/l^n)[\mathbb{Z}/l^n]$ by $1+t\leftrightarrow\varprojlim\gamma_n$ where γ_n is a fixed generator of $\mathbb{Z}/l^n$ (written multiplicatively) such that γ_{n+1} corresponds to γ_n under the natural map $\mathbb{Z}/l^{n+1}\to\mathbb{Z}/l^n$. Then, we easily see that the measure $\{\delta_{\rho,n}\}_n$ corresponds to the power series Dg_ρ.

Before we begin describing an alternative proof of Theorem C, we need the following claim. Let $\mathscr{V}^+$ be the "even part" of $\mathscr{V}$, i.e., $\mathscr{V}^+=\{g\in\mathscr{V};\, g((1+t)^{-1}-1)=g(t)\}$. For $g\in\mathbb{Z}_l[[t]]$, denote by $\{\delta_{g,n}\}_n$ the measure (distribution) corresponding to g.

Claim. *A power series g belongs to $\mathscr{V}^+$ if and only if the distribution $\{\delta_{g,n}\}_n$ satisfies*

$$\begin{aligned}\delta_{g,n}(a)&=0 \qquad \text{if} \quad l\mid a\\ \delta_{g,n}(-a)&=\delta_{g,n}(a)\end{aligned} \tag{$**$}$$

for all $n\geqslant 1$.

Proof of Claim. Assume $g \in \mathscr{V}^+$ and let $g_n = g \bmod((1+t)^{l^n}-1)$. By the isomorphism

$$\mathbb{Z}_l[[t]]/((1+t)^{l^n}-1) \simeq \mathbb{Z}_l[\mathbb{Z}/l^n] \qquad (1+t \leftrightarrow \gamma_n),$$

g_n corresponds to $\sum_{a=0}^{l^n-1} \tilde{\delta}_{g,n}(a)\gamma_n^a$. Here, $\tilde{\delta}_{g,n}$ is a function from $\mathbb{Z}/l^n$ to $\mathbb{Z}_l$ which reduces to $\delta_{g,n}$ modulo l^n. Noting that $(1+t)^{-1}$ corresponds to γ_n^{-1}, we get $\delta_{g,n}(-a) = \delta_{g,n}(a)$ from the identity $g((1+t)^{-1}-1) = g$. The equality $\sum_{\zeta^l=1} g(\zeta(1+t)-1) = 0$ implies $\sum_{\zeta^l=1} g_n(\zeta(1+t)-1) = 0$ in $\mathbb{Z}_l[\zeta_1][t]/((1+t)^{l^n}-1)$. Therefore, in $\mathbb{Z}_l[\zeta_1][\mathbb{Z}/l^n]$, we have

$$\sum_{\zeta^l=1} \sum_{a=0}^{l^n-1} \tilde{\delta}_{g,n}(a)(\zeta\gamma_n)^a = \sum_{a=0}^{l^n-1} \tilde{\delta}_{g,n}(a)\left(\sum_{\zeta^l=1} \zeta^a\right)\gamma_n^a = 0. \qquad (***)$$

Here, $\sum_{\zeta^l=1} \zeta^a = l$ if $l \mid a$ and $=0$ otherwise. Hence, $(***)$ implies $\delta_{g,n}(a) = 0$ if $l \mid a$. Obviously, we can reverse the above arguments. Therefore, the proof of the claim is completed.

Now, we begin our alternative proof. Let

$$C_n = \mathbb{Q}(\boldsymbol{\mu}_{l^n}, (\zeta_n^a - 1)^{1/l^n}; 1 \leqslant a \leqslant \frac{l^n-1}{2}, (a, l) = 1)$$

and $H_n = \mathrm{Gal}(C_n/\mathbb{Q}(\boldsymbol{\mu}_{l^n}))$. Then, $C = \bigcup_n C_n$ is the field corresponding to the kernel of the Galois representation $\mathbf{F}$. Put $\mathfrak{H} = \mathrm{Gal}(C/\mathbb{Q}(\boldsymbol{\mu}_{l^\infty})) = \varprojlim H_n$. First, assume the Vandiver conjecture at l. By the analytic class number formula and a theorem of Iwasawa [8], this conjecture is equivalent to the condition that for all $n \geqslant 1$, the l-units $\zeta_n^a - 1$ $(1 \leqslant a \leqslant (l^n-1)/2, (a, l) = 1)$ are multiplicatively independent modulo $(\mathbb{Q}(\boldsymbol{\mu}_{l^n})^\times)^{l^n}$. Take any $g \in \mathscr{V}^-$. We want to show that $g = g_\rho$ for some $\rho \in \mathfrak{H}$. Since the differential operator D induces an isomorphism from $\mathscr{V}^+$ to $\mathscr{V}^-$ [3], $g = Df$ for a power series $f \in \mathscr{V}^-$. From the assumption, we can define an element $\rho_{f,n} \in H_n$ for each n by the formula

$$\{(\zeta_n^a - 1)^{1/l^n}\}^{\rho_{f,n}-1} = \zeta_n^{\delta_{f,n}(a)}, \qquad 1 \leqslant a \leqslant \frac{l^n-1}{2}, (a, l) = 1.$$

By the distributive relation

$$\sum_{\substack{\bar{a} \in \mathbb{Z}/l^{n+1} \\ \bar{a} \equiv a (\mathrm{mod}\ l^n)}} \delta_{f,n+1}(\bar{a}) \equiv \delta_{f,n}(a) \qquad \bmod l^n,$$

we get $\rho_{f,n+1}|_{C_n} = \rho_{f,n}$, which assures that $\{\rho_{f,n}\}_n$ defines an element ρ_f of $\mathfrak{H}$. By the very definition of $\rho_{f,n}$ and what we have recalled above, the power series f is nothing but $D(g_{\rho_f})$. Hence, $g = g_{\rho_f}$. Conversely, assume $\{g_\rho; \rho \in \mathfrak{G}\} = \mathscr{V}^-$. Then, we have $\{Dg_\rho; \rho \in \mathfrak{G}\} = \mathscr{V}^+$. This means that any measure satisfying (**) in the claim is of the form $\{\delta_{\rho,n}\}_n$ for some $\rho \in \mathfrak{H}$, where $\delta_{\rho,n}$ is defined by the formula (*). In particular, for any $\delta_1 : \mathbb{Z}/l \to \mathbb{Z}/l$ satisfying (**), there exists some $\rho_1 \in H_1$ such that $\delta_1 = \delta_{\rho_1,1}$. This implies that $\zeta_1^a - 1$ $(1 \leqslant a \leqslant (l-1)/2)$ are multiplicatively independent modulo $(\mathbb{Q}(\zeta_1)^\times)^l$ and hence the Vandiver conjecture holds. This completes the proof of (the latter half of) Theorem C.

REFERENCES

1. G. W. ANDERSON, The hyperadelic gamma function: A précis, *Adv. Stud. Pure Math.* **12** (1987), 1–19.
2. R. COLEMAN, Division values in local fields, *Invent. Math.* **53** (1979), 91–116.
3. R. COLEMAN, Local units modulo circular units, *Proc. Amer. Math. Soc.* **89** (1983), 1–17.
4. R. COLEMAN, Anderson–Ihara theory: Gauss sums and circular units, *Adv. Stud. Pure Math.* **17**, in press.
5. H. ICHIMURA AND K. SAKAGUCHI, The non-vanishing of a certain Kummer character χ_m (after Soulé), and some related topics, *Adv. Stud. Pure Math.* **12** (1987), 53–64.
6. Y. IHARA, Profinite braid groups, Galois representations and complex multiplications, *Ann. of Math.* **123** (1986), 43–106.
7. Y. IHARA, M. KANEKO, AND A. YUKINARI, On some properties of the universal power series for Jacobi sums. *Adv. Stud. Pure Math.* **12** (1987), 65–86.
8. K. IWASAWA, A note on class numbers of algebraic number fields, *Abh. Math. Sem. Univ. Hamburg* **20** (1956), 257–258.
9. K. IWASAWA, A note on Jacobi sums, *Sympos. Math.* **15** (1975), 447–459.
10. S. LANG, "Cyclotomic Fields," Springer-Verlag, New York, 1978.
11. B. MAZUR AND A. WILES, Class fields over abelian extensions over $\mathbb{Q}$, *Invent. Math.* **76** (1984), 179–330.
12. L. WASHINGTON, "Introduction to Cyclotomic Fields," Springer-Verlag, New York, 1982.