Advanced Studies in Pure Mathematics 12, 1987
Galois Representations and Arithmetic Algebraic Geometry
pp. 53–64

The Non-Vanishing of a Certain Kummer Character χ_m (after C. Soulé), and Some Related Topics

H. Ichimura and K. Sakaguchi

§ 1. Introduction

Let l be an odd prime number, and Ω_l be the maximum pro-l abelian extension of the cyclotomic field $\boldsymbol{Q}(\mu_{l^\infty})$ unramified outside l. This extension $\Omega_l/\boldsymbol{Q}(\mu_{l^\infty})$ and its Galois group $\mathfrak{G}$ are very important (and familiar) objects in Iwasawa theory, and the structure of $\mathfrak{G}$ as a $\boldsymbol{Z}_l^\times$ ($\cong \mathrm{Gal}(\boldsymbol{Q}(\mu_{l^\infty})/\boldsymbol{Q})$)-module has been investigated by Iwasawa ([Iw1] [Iw2]), Coates ([Coa]), Mazur and Wiles ([MW]), etc. In connection with Ihara's universal power series for Jacobi sums ([Ih] [IKY]), we are particularly interested in the groups

$$(1) \qquad \mathrm{Hom}_{\boldsymbol{Z}_l^\times}(\mathfrak{G}, \boldsymbol{Z}_l(m)),$$

for positive integers m, and their "standard elements" χ_m which appear in Soulé [S3], Deligne [D] and Ihara [Ih]. The main purpose of this report is to give an exposition of the basic results, mainly due to Soulé [S2] [S3], on the structure of the group (1) and the non-vanishing of χ_m (for $m \geqq 3$, odd). The reason for writing this report is that, although these works seem to be well-known among the K-theorists, they are "buried" under a mass of generalities in K-theory and hence are not so familiar among the wider public in number theory. The second purpose of this report is to present various related remarks, in connection with Ihara's power series, the Vandiver conjecture, etc.

The first main theorem to be reviewed is the following.

Theorem A (Tate [T], Lichtenbaum [L], Soulé [S2]).

$$\mathrm{Hom}_{\boldsymbol{Z}_l^\times}(\mathfrak{G}, \boldsymbol{Z}_l(m)) \cong \begin{cases} \boldsymbol{Z}_l \cdots m \geqq 1, \textit{ odd} \\ \{0\} \cdots m \geqq 2, \textit{ even.} \end{cases}$$

To write down the second, let us recall the definition of the element $\chi_m \in \mathrm{Hom}_{\boldsymbol{Z}_l^\times}(\mathfrak{G}, \boldsymbol{Z}_l(m))$. Choose a basis $(\zeta_n)_{n \geq 1}$ of the Tate module

Received March 13, 1986.

$$T_l(\boldsymbol{G}_m)=\boldsymbol{Z}_l(1),$$

i.e. ζ_n is a primitive l^n-th root of unity with $\zeta_{n+1}^l=\zeta_n$, and put

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

Then χ_m is defined by the relations

$$((\varepsilon_n^{(m)})^{1/l^n})^{\rho-1}=\zeta_n^{\chi_m(\rho)} \qquad (\rho\in\mathfrak{G}, n\geqq 1).$$

Its dependence on the choice of $(\zeta_n)_{n\geq 1}$ is only up to multiplication by elements of $\boldsymbol{Z}_l^\times$. One may expect that χ_m generates the group $\mathrm{Hom}_{\boldsymbol{Z}_l^\times}(\mathfrak{G}, \boldsymbol{Z}_l(m))$. This would be implied by the Vandiver conjecture at l (see Section 3–3). In his letter [S3], Soulé informed Ihara that the group $H_{\acute{e}t}^1(\boldsymbol{Z}[1/l], \boldsymbol{Z}_l(m))$ is generated, up to torsion, by higher analogues of cyclotomic units. His result implies, in our terminology, the following

Theorem B. *For any odd integer $m\geqq 1$, $\chi_m\neq 0$.*

This shows that χ_m generates a subgroup of the group $\mathrm{Hom}_{\boldsymbol{Z}_l^\times}(\mathfrak{G}, \boldsymbol{Z}_l(m))$ with a finite index.

The keystone for the proofs of Theorems A, B is the vanishing of a certain cohomology group (Theorem 1 in Section 2), in which some deep results in K-theory were essentially used. But this part will be touched only briefly.

We close this section by describing how these characters χ_m and Theorems A, B are related to the Galois representation

$$\psi\colon \mathfrak{G}\ni\rho\longmapsto F_\rho\in\boldsymbol{Z}_l[[u, v]]^\times$$

constructed in [Ih]. For $i, j\geqq 1$, let $\beta_{i,j}(\rho)/i!j!$ be the coefficient of U^iV^j in $\log F_\rho$ ($\in\boldsymbol{Q}_l[[U, V]]$) where $U=\log(1+u)$, $V=\log(1+v)$. Then

$$\beta_{i,j}\in\mathrm{Hom}_{\boldsymbol{Z}_l^\times}(\mathfrak{G}, \boldsymbol{Z}_l(m))$$

with $m=i+j$. Therefore, by Theorems A, B, $\beta_{i,j}$ is a constant multiple ($\in\boldsymbol{Q}_l$) of χ_m. Recently, R. Coleman and Ihara-Kaneko-Yukinari [IKY] proved that

$$(2) \qquad \beta_{i,j}=(1-l^{m-1})^{-1}\cdot\chi_m.$$

The image of ψ is contained in the subgroup

$$\Psi_1=1+uv(u+v+uv)\boldsymbol{Z}_l[[u, v]]$$

of $Z_l[[u, v]]^{\times}$. The group Ψ_1 admits a canonical filtration $\{\Psi_1(m)\}_{m\geqq 3}$ defined by

$$\Psi_1(m)=1+uv(u+v+uv)I^{m-3} \qquad (m\geqq 3),$$

where I denotes the ideal $I=(u, v)$ of $Z_l[[u, v]]$. Let $\mathfrak{G}(m)$ $(m\geqq 3)$ be the filtration of $\mathfrak{G}$ defined by $\mathfrak{G}(m)=\psi^{-1}(\Psi_1(m))$. Then $\alpha\in Z_l^{\times}$ acts on the quotient module $\mathfrak{G}(m)/\mathfrak{G}(m+1)$ by the multiplication by α^m, and $\beta_{i,j}$ $(i+j=m)$ induces an injective morphism

$$\mathfrak{G}(m)/\mathfrak{G}(m+1)\longrightarrow Z_l(m)$$

as $Z_l^{\times}$-modules. It is known that $\mathfrak{G}(m)/\mathfrak{G}(m+1)=\{0\}$ when m is even $\geqq 2$ ([Ih], p. 84). On the other hand, for any odd integer $m\geqq 3$, by (2) and Theorem B, $\beta_{i,j}$ $(i+j=m)$ is a non zero map. Therefore $\mathfrak{G}(m)/\mathfrak{G}(m+1)$ is a free Z_l-module of rank one when m is odd $\geqq 3$.

§ 2. Proofs of Theorems A, B

2-1. A key result for the proofs of Theorems A, B is the following.

Theorem 1. *Let l be an odd prime number, F a number field, O_F the integer ring of F and m be an integer $\geqq 2$. Then*

$$H^2_{\acute{e}t}(\mathrm{Spec}\,(O_F[1/l]), (Q_l/Z_l)(m))=\{0\}.$$

This theorem was proved for $m=2$ by S. Lichtenbaum ([L], Propositions 9, 6), and then in general by Soulé ([S1], Théorème 5). The proof uses the theory of Chern classes:

$$K_{2m-k}(F; Z/l^n)\longrightarrow H^k_{\acute{e}t}(\mathrm{Spec}\,(F); (\mu_{l^n})^{\otimes m})$$

defined and studied in [S1], which is a remarkable generalization of Tate's isomorphism ([T]):

$$K_2(F)/l^n\cdot K_2(F)\xrightarrow{\sim} H^2(F; (\mu_{l^n})^{\otimes 2}),$$

and depends on Borel's calculation of the rank of $K_i(O_F)$.

We will now consider the l-cyclotomic extensions of any number field F. Set $F_n=F(\mu_{l^n})$ for $n\geqq 0$, and $F_\infty=\bigcup_n F_n$. Let O_n be the integer ring of F_n, and $E_n=(O_n[1/l])^{\times}$ be the group of all l-units of F_n. Let

$$\mathfrak{A}_n=\mathrm{Pic}\,(O_n[1/l])_{(l\text{-prim})}$$

denote the l-Sylow subgroup of the l-ideal class group of F_n, and set $\mathfrak{A}=\varinjlim \mathfrak{A}_n$ (the inductive limit being taken with respect to the natural maps $\mathfrak{A}_n \to \mathfrak{A}_{n+1}$). Set $G_\infty = \mathrm{Gal}(F_\infty/F)$ and consider $\mathfrak{A}$ as a $Z_l[[G_\infty]]$-module.

Corollary 1a. (i) $\mathfrak{A}(m-1)_{G_\infty}=\{0\}$, (ii) $\mathfrak{A}(m-1)^{G_\infty}$ *is a finite group, for any integer* $m \geqq 2$.

Here in general, if M is a $Z_l[[\mathrm{G}_\infty]]$-module, we denote by $M(i)$ the i-fold Tate twist; $M(i)=M \otimes Z_l(1)^{\otimes m}$, and by M_{G_∞} (resp. M^{G_∞}) the G_∞-coinvariant (resp. invariant) module of M.

Let L be the maximum unramified abelian pro-l extension of F_∞. Then $\mathrm{Gal}(L/F_\infty)$ is also a $Z_l[[\mathrm{G}_\infty]]$-module.

Corollary 1b. $\mathrm{Gal}(L/F_\infty)(m-1)_{G_\infty}$ *and* $\mathrm{Gal}(L/F_\infty)(m-1)^{G_\infty}$ *are finite groups, for any integer* $m \geqq 2$.

Proof of Corollaries. First we note the facts that, for any finitely generated torsion $Z_l[[\mathrm{G}_\infty]]$-module M, M^{G_∞} is finite if and only if M_{G_∞} is so (e.g. [Coa] p. 349), and that $\mathrm{Hom}(\mathfrak{A}, Q_l/Z_l)$ and $\mathrm{Gal}(L/F_\infty)$ are finitely generated torsion $Z_l[[\mathrm{G}_\infty]]$-modules ([Iw2]).

Corollary la follows immediately from Theorem 1, Kummer's exact sequence ([Iw2], Lemma 10):

$$(3)\quad 0 \longrightarrow (\varinjlim E_n) \otimes (Q_l/Z_l) \longrightarrow H^1_{\acute{e}t}(O_{F_\infty}[1/l], (Q_l/Z_l)(1)) \longrightarrow \mathfrak{A} \longrightarrow 0,$$

and the fact that

$$H^2_{\acute{e}t}(O_F[1/l], (Q_l/Z_l)(m)) \cong H^1_{\acute{e}t}(O_{F_\infty}[1/l], (Q_l/Z_l)(m))_{G_\infty}.$$

Let L' be the maximum unramified abelian pro-l extension of F_∞ in which all primes of F_∞ over l are completely decomposed. K. Iwasawa has proved ([Iw2], Theorem 11) that $\mathrm{Hom}(\mathfrak{A}, Q_l/Z_l)$ and $\mathrm{Gal}(L'/F_\infty)$ are quasi-isomorphic as finitely generated torsion Λ-modules (here, $\sigma \in G_\infty$ acts on $\alpha \in \mathrm{Hom}(\mathfrak{A}, Q_l/Z_l)$ by $\sigma(\alpha)=\alpha \cdot \sigma$). Note that $\mathrm{Gal}(L/L')(m-1)_{G_\infty}$ is finite (cf. [Iw2], Theorem 9). Corollary 1b now follows from Corollary 1a.

Remark. By using a theorem of Mazur and Wiles ([MW]) on the "Main conjecture" of Iwasawa, one can show that, for any even integer m, the following two statements are equivalent

(i) $L_l(1-m, \omega^m) \neq 0$,

(ii) $\mathrm{Gal}(L/F_\infty)(m-1)_{G_\infty}$ is finite.

Here, $L_l(s, \ )$ is the l-adic L-function and ω is the Teichmüller character. On the other hand, we know that $L_l(1-m, \omega^m)=(l^m-1)\cdot B_m/m \neq 0$, for even integers $m \geqq 2$ (B_m: the m-th Bernoulli number (cf. [W], p. 57)). Therefore, for even integers m, these corollaries follow without using K-theory. But for odd integers, we gain nothing in this way.

2-2. Let Ω_l be the maximum abelian pro-l extension of F_∞ unramified outside l, and set $\mathfrak{G} = \mathrm{Gal}(\Omega_l/F_\infty)$. Thus $\mathfrak{G}$ is naturally a $\boldsymbol{Z}_l[[\mathrm{G}_\infty]]$-module. For each integer m, we will denote by $\mathrm{Hom}_{G_\infty}(\mathfrak{G}, \boldsymbol{Z}_l(m))$ the $\boldsymbol{Z}_l$-module consisting of all continuous homomorphisms $\psi: \mathfrak{G} \to \boldsymbol{Z}_l$ satisfying

$$\psi(\rho^\sigma) = \kappa(\sigma)^m \cdot \psi(\rho), \qquad (\rho \in \mathfrak{G}, \sigma \in G_\infty),$$

where $\kappa: G_\infty \to \boldsymbol{Z}_l^\times$ is the l-cyclotomic character.

We can attach, to each projective system of l-units, an element of $\mathrm{Hom}_{G_\infty}(\mathfrak{G}, \boldsymbol{Z}_l(m))$, as follows (([S2] § 1). Set $\bar{E} = \varprojlim E_n/E_n^{l^n}$, where the projective limit is taken with respect to the norms. For each $e = (e_n) \in \bar{E}$, put

$$\varepsilon_n^{(m)}(e) = \prod_{\sigma \in \mathrm{Gal}\,(F_n/F)} e_n^{\sigma \cdot \langle \kappa(\sigma)^{m-1} \rangle_n}, \qquad n \geqq 1; \tag{4}$$

where in general, for each $\alpha \in \boldsymbol{Z}_l$, we denote by $\langle \alpha \rangle_n$ the unique integer in the interval $[0, l^n)$ which is congruent to α modulo l^n. Let $\chi_e^{(m)}$ denote the Kummer character associated with the system of l-units $\{\varepsilon_n^{(m)}(e)\}_{n \geqq 1}$; namely, $\chi_e^{(m)}$ is the unique homomorphism $\mathfrak{G} \to \boldsymbol{Z}_l$ determined by

$$\zeta_n^{\chi_e^{(m)}(\rho)} = \{(\varepsilon_n^{(m)}(e))^{1/l^n}\}^{\rho - 1} \qquad (\rho \in \mathfrak{G}, n \geqq 1). \tag{5}$$

We can obtain, in this way, a homomorphism

$$\begin{array}{rcl} \psi_m: \bar{E}(m-1)_{G_\infty} & \longrightarrow & \mathrm{Hom}_{G_\infty}(\mathfrak{G}, \boldsymbol{Z}_l(m)) \\ \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\ (e_n \otimes \zeta_n^{\otimes m-1})_n & \longmapsto & \chi_e^{(m)} \quad . \end{array}$$

We have the following basic lemma about ψ_m established by Soulé in [S2] Section 1.

Lemma 1. *The kernel and cokernel of ψ_m are finite when $m \geqq 2$.*

We now outline the derivation of this lemma from Corollary 1a. By the definition, ψ_m is the composite of two morphisms:

$$\bar{E}(m-1)_{G_\infty} \xrightarrow{\alpha} \varprojlim_n \mathfrak{E}(m-1)_{(l^n)}^{G_\infty} \xrightarrow{\beta} \mathrm{Hom}_{G_\infty}(\mathfrak{G}, \boldsymbol{Z}_l(m)),$$

where $\mathfrak{E} = (\varinjlim_n E_n) \otimes (\boldsymbol{Q}_l/\boldsymbol{Z}_l)$, and the suffix "$(l^n)$" indicates the subgroup of elements annihilated by l^n.

First, the map α is defined by $e \mapsto (\varepsilon_n^{(m)}(e))_n$ as in (4). Using a theorem of Iwasawa ([Iw2], Lemma 7, Theorem 15) on the structure of $\mathfrak{E}$ as a $\boldsymbol{Z}_l[[\mathrm{G}_\infty]]$-module, it is not hard to see that the kernel and cokernel of α are finite when $m \geqq 2$ (see [S2], Lemmas 2 and 3).

Secondly, the map β is defined as in (5). From (3), we get an exact sequence

$$0 \longrightarrow \mathfrak{E}(m-1)_{(l^n)}^{G_\infty} \xrightarrow{\beta_n} \mathrm{Hom}_{G_\infty}(\mathfrak{G}, (\boldsymbol{Q}_l/\boldsymbol{Z}_l)(m))_{(l^n)} \longrightarrow \mathfrak{A}(m-1)_{(l^n)}^{G_\infty}.$$

Note that β is the projective limit of β_n. We know from Corollary 1a that $\mathfrak{A}(m-1)^{G_\infty}$ is finite when $m \geqq 2$. Hence β is bijective. This completes the proof.

On the other hand, again according to Theorem 15 in [Iw2], we have

Lemma 2.

$$\mathrm{rank}\, \bar{E}(m-1)_{G_\infty} = \begin{cases} r_1 + r_2 \cdots m \ \mathit{odd} \geqq 3 \\ r_2 \qquad \cdots m \ \mathit{even} \geqq 2. \end{cases}$$

From Lemmas 1 and 2, we obtain

Theorem 2.

$$\mathrm{rank}\ \mathrm{Hom}_{G_\infty}(\mathfrak{G}, \boldsymbol{Z}_l(m)) = \begin{cases} r_1 + r_2 \cdots m \ \mathit{odd} \geqq 3 \\ r_2 \qquad \cdots m \ \mathit{even} \geqq 2. \end{cases}$$

In the case of $F = \boldsymbol{Q}$, this yields Theorem A except for $m=1$. For the case $m=1$, see Section 3–1.

2-3. From now on we shall consider the case of $F = \boldsymbol{Q}$, and assume $m \geqq 2$ (for $m=1$, see Section 3–3). Let χ_m be as in Section 1, so that, by definition,

$$\chi_m = \psi_m((\zeta_n - 1)_n) \in \mathrm{Hom}_{G_\infty}(\mathfrak{G}, \boldsymbol{Z}_l(m)).$$

Let $C_n \subset E_n$ be the subgroup of cyclotomic units, generated by the elements $(\zeta_n - 1)/(\zeta_n^\sigma - 1)$ ($\sigma \in \mathrm{Gal}(\boldsymbol{Q}(\mu_{l^n})/\boldsymbol{Q})$). Set $\bar{C} = \varprojlim C_n/C_n^{l^n} \subset \bar{E}$, and denote by $\mathfrak{C}_m$ the subgroup of $\mathrm{Hom}_{G_\infty}(\mathfrak{G}, \boldsymbol{Z}_l(m))$ generated by the elements $\psi_m(c)$ ($c \in \bar{C}$).

In [S3], Soulé proved the following theorem (in fact he proved a slightly different and general statement).

Theorem 3. *$\mathfrak{C}_m$ is a subgroup of* $\mathrm{Hom}_{G_\infty}(\mathfrak{G}, \boldsymbol{Z}_l(m))$ *with a finite index when $m \geqq 2$.*

The statement of Theorem B for $m \geqq 3$ follows immediately from Theorem 3. Indeed, let g be a primitive root mod l^2 (then g is a primitive root of mod l^n for all $n \geqq 1$), and set $\eta = ((\zeta_n - 1)/(\zeta_n^g - 1)) \in \bar{C}$. It is easy to see that $\chi_m(\eta) = (1 - g^{1-m}) \cdot \chi_m$. Since η generates $\bar{C}$ as a $\boldsymbol{Z}_l[[\mathrm{G}_\infty]]$-module, it follows from Theorem 2 (or A) and Theorem 3 that $\chi_m \neq 0$ for any odd integer $m \geqq 3$.

Proof of Theorem 3. Since the map ψ_m finite kernel and cokernel (Lemma 1), it suffices to show that $\bar{E}(m-1)_{G_\infty}/\bar{C}(m-1)_{G_\infty}$ is finite. Let U_n be the group of principal units of $\boldsymbol{Q}(\mu_{l^n})$, $E_{n,1} = E_n \cap U_n$, and $C_{n,1} = C_n \cap U_n$. Set $\mathfrak{U} = \varprojlim U_n$, $\bar{E}_1 = \varprojlim E_{n,1}/E_{n,1}^{l^n}$ and $\bar{C}_1 = \varprojlim C_{n,1}/C_{n,1}^{l^n}$. Then $\bar{E}_1$ and $\bar{C}_1$ are $\boldsymbol{Z}_l[[\mathrm{G}_\infty]]$-modules. Note that when $m \geqq 2$, $\bar{E}(m-1)_{G_\infty}/\bar{C}(m-1)_{G_\infty}$ is finite if and only if $(\bar{E}_1/\bar{C}_1)(m-1)_{G_\infty}$ is so. Hence it is enough to show that $(\bar{E}_1/\bar{C}_1)\ (m-1)_{G_\infty}$ is finite when $m \geqq 2$.

Let L and Ω_l be as before, and consider the following well-known exact sequence of $\boldsymbol{Z}_l[[\mathrm{G}_\infty]]$-modules (e.g. [W], Proposition 13.6).

$$\begin{aligned}(6)\qquad & 0 \longrightarrow (\bar{E}_1/\bar{C}_1)^+ \longrightarrow (\mathfrak{U}/\bar{C}_1)^+ \longrightarrow \mathrm{Gal}\,(\Omega_l/\boldsymbol{Q}(\mu_{l^\infty}))^+ \\ & \longrightarrow \mathrm{Gal}\,(L/\boldsymbol{Q}(\mu_{l^\infty}))^+ \longrightarrow 0.\end{aligned}$$

Here the suffix "$+$" indicates the plus part of $G_\infty(\cong \boldsymbol{Z}_l^\times)$-modules. It has been shown ([Iw1]) that these groups are finitely generated torsion Λ-modules. From a theorem of Iwasawa ([Iw1], Proposition 12) on the characteristic power series of $(\mathfrak{U}/\bar{C}_1)^+$, and a theorem of Mazur and Wiles, it follows that $(\mathfrak{U}/\bar{C}_1)^+$ has the same characteristic power series as $\mathrm{Gal}\,(\Omega_l/\boldsymbol{Q}(\mu_{l^\infty}))^+$ (which can be expressed in terms of l-adic L-functions). Thus from (6), $(\bar{E}_1/\bar{C}_1)^+$ and $\mathrm{Gal}\cdot(L/\boldsymbol{Q}(\mu_{l^\infty}))^+$ have the same characteristic power series. On the other hand, by Corollary 1b, $\mathrm{Gal}\,(L/\boldsymbol{Q}(\mu_{l^\infty})\ (m-1)_{G_\infty}$ is finite when $m \geqq 2$. Hence $(\bar{E}_1/\bar{C}_1)\ (m-1)_{G_\infty}$ is finite, as claimed.

§ 3. Some related remarks

In this section, we give four remarks related to Kummer characters χ_m. In the first paragraph we review some basic facts on the restriction homomorphism $\mathrm{Hom}_{G_\infty}(\mathfrak{G}, \boldsymbol{Z}_l(m)) \rightarrow \mathrm{Hom}_{G_\infty}(\mathcal{U}, \boldsymbol{Z}_l(m))$ where $\mathcal{U}$ is the inertia group of an extension of l in $\Omega_l/\boldsymbol{Q}(\mu_{l^\infty})$. Secondly, we consider the field corresponding to the subgroup $\bigcap_{m:\mathrm{odd}} \mathrm{Ker}\,\chi_m$ in $\mathfrak{G}$ and show that under the Vandiver conjecture for l, it coincides with Ω_l^- (=the "minus part" of $\Omega_l/\boldsymbol{Q}(\mu_{l^\infty})$). This is basically due to Coleman. Thirdly, we show that the Vandiver conjecture for l is valid if and only if, $\chi_3, \chi_5, \cdots, \chi_{l-2}$ are surjective. In the final paragraph, we show how to construct a certain unramified subextension of $\Omega_l/\boldsymbol{Q}(\mu_{l^\infty})$ in a very explicit way by using the l-units $\varepsilon_n^{(m)}$.

3-1. On the inertia restriction

$$\mathrm{Hom}_{G_\infty}(\mathfrak{G}, \boldsymbol{Z}_l(m)) \to \mathrm{Hom}_{G_\infty}(\mathcal{U}, \boldsymbol{Z}_l(m)),$$

the following facts are basic.

Proposition 1. *Let m be an odd integer $\geqq 3$ and let $\varphi_m(\in \mathrm{Hom}_{G_\infty}(\mathcal{U}, \boldsymbol{Z}_l(m)))$ be the Coates-Wiles homomorphism (see e.g.* [W] p. 307).

(i) $\mathrm{Hom}_{G_\infty}(\mathfrak{G}, \boldsymbol{Z}_l(m)) \to \mathrm{Hom}_{G_\infty}(\mathcal{U}, \boldsymbol{Z}_l(m))$ *is injective if and only if $L_l(m, \omega^{1-m}) \neq 0$,*

(ii) $\mathrm{Hom}_{G_\infty}(\mathcal{U}, \boldsymbol{Z}_l(m)) \cong \boldsymbol{Z}_l$ *and* $\varphi_m \neq 0$,

(iii) $\chi_m | \mathcal{U} = (1 - l^{m-1}) L_l(m, \omega^{1-m}) \varphi_m$.

(i) is an easy consequence of a theorem of Mazur and Wiles [MW] and is also given in [S2] Section 3–2. The isomorphism

$$\mathrm{Hom}_{G_\infty}(\mathcal{U}, \boldsymbol{Z}_l(m)) \cong \boldsymbol{Z}_l$$

is due to a theorem of Iwasawa on the structure of $\mathcal{U}$ as a $\boldsymbol{Z}_l[[\mathrm{G}_\infty]]$-module. That $\varphi_m \neq 0$ and (iii) are proved by Coleman.

Remark. When m is an odd integer with $m \geqq 3$ and $L_l(m, \omega^{1-m}) \neq 0$, the assertions of Theorems A and B follow from the above proposition without using K-theory. So far, we have known no odd integer m such that $L_l(m, \omega^{1-m}) = 0$.

When $m = 1$, we see that $\mathfrak{G}^{(1)} = \mathcal{U}^{(1)}$ by using the Stickelberger theorem (see e.g. [W], Proposition 6.16). Here, for a $\boldsymbol{Z}_l[\Delta]$-module M and an integer i with $0 \leqq i \leqq l-2$, $M^{(i)}$ denotes the ω^i-eigenspace of the $\Delta = \mathrm{Gal}(\boldsymbol{Q}(\mu_l)/\boldsymbol{Q})$-decomposition of M. Hence,

$$\mathrm{Hom}_{G_\infty}(\mathfrak{G}^{(1)}, \boldsymbol{Z}_l(m)) \cong \mathrm{Hom}_{G_\infty}(\mathcal{U}^{(1)}, \boldsymbol{Z}_l(m)) \qquad (\cong \boldsymbol{Z}_l, \text{ by [Iw1]}).$$

This gives Theorem A when $m = 1$.

3-2. For an odd integer $m \geqq 1$, let K_m be the subextension of $\Omega_l/\boldsymbol{Q}(\mu_{l^\infty})$ corresponding to the kernel of χ_m. Then we easily see that (1) K_m is normal over $\boldsymbol{Q}$ and (2) $G_\infty(\overset{\sim}{\to}_\kappa \boldsymbol{Z}_l^\times)$ acts on the $\boldsymbol{Z}_l$-module $\mathrm{Gal}(K_m/\boldsymbol{Q}(\mu_{l^\infty}))$ by $\sigma \cdot g = \kappa^m(\sigma) g$ ($\sigma \in G_\infty, g \in \mathrm{Gal}(K_m/\boldsymbol{Q}(\mu_{l^\infty}))$). Theorems A and B imply that K_m is the unique $\boldsymbol{Z}_l$-extension satisfying (1) and (2).

Let Cyclo denote the composite of all the $\boldsymbol{Z}_l$-extensions K_m (m: odd $\geqq 1$). By the definition, Cyclo$\subset \Omega_l^-$. By the relation (2) in Section 1, the field Cyclo coincides with the subextension of $\Omega_l/\boldsymbol{Q}(\mu_{l^\infty})$ corresponding to the kernel of Ihara's Galois representation ψ. For this field (or the kernel of ψ), we show first the following

Proposition 2. *Ω_l^- is unramified over* Cyclo.

Proof. It suffices to show that $(\bigcap_{\geqq 3}^{m:\ odd} \operatorname{Ker} \chi_m) \cap \mathcal{U} = \{1\}$. By Proposition 1 (iii), $\bigcap_{\geqq 3}^{m:\ odd} \operatorname{Ker} \chi_m \cap \mathcal{U} = \bigcap'_m \operatorname{Ker} \varphi_m$, where the second intersection is taken over all odd integers $m \geqq 3$ such that $L_l(m, \omega^{1-m}) \neq 0$. But since φ_m is "almost continuous" in m (see e.g. [W] Proposition 13.51, 52), $\bigcap'_m \operatorname{Ker} \varphi_m = \bigcap_{\geqq 1}^{m:\ odd} \operatorname{Ker} \varphi_m$. Finally, by the injectivity of Coleman's embedding (see e.g. [W] Proposition 13.38), $\bigcap_{\geqq 1}^{m:\ odd} \operatorname{Ker} \varphi_m = \{1\}$. This proves the proposition.

We next prove

Proposition 3. Cyclo $= \boldsymbol{Q}(\mu_{l^\infty}, c^{1/l^n}$; *all* $n \geqq 1$ *and all cyclotomic units* c *in* $\boldsymbol{Q}(\mu_{l^\infty}))$.

This was orally communicated to us by Coleman. The following proof is due to Sakaguchi.

Proof. It suffices to show that for any $e = (e_n)_n \in \bar{E}$, the fixed field of the subgroup $\bigcap_{\geqq 1}^{m:\ odd} \operatorname{Ker} \chi_e^{(m)}$ in $\mathfrak{G}$ coincides with the field $\boldsymbol{Q}(\mu_{l^\infty}, (e_n^{\sigma_a})^{1/l^n}$; all $n \geqq 1$ and all $a \in \boldsymbol{Z}_l^\times)$. Here σ_a denotes the automorphism of $\boldsymbol{Q}(\mu_{l^\infty})/\boldsymbol{Q}$ such that $\zeta_n^{\sigma_a} = \zeta_n^a$ for all n. For $\rho \in \mathfrak{G}$, we define a map $\lambda_{e,\rho}^{(n)}: \boldsymbol{Z}/l^n \rightarrow \boldsymbol{Z}/l^n$ by

$$((e_n^{\sigma_a})^{1/l^n})^{\rho-1} = \zeta_n^{\lambda_{e,\rho}^{(n)}(a)} \qquad \text{if } a \in (\boldsymbol{Z}/l^n)^\times$$

$\lambda_{e,\rho}^{(n)}(a) \equiv 0\ (l^n)$ otherwise. Then it is easy to see that the system $\{\lambda_{e,\rho}^{(n)}\}_{n \geqq 1}$ defines a $\boldsymbol{Z}_l$-valued measure $\lambda_{e,\rho}$ on $\boldsymbol{Z}_l$. By the definition of $\chi_e^{(m)}$, we get

$$\chi_e^{(m)}(\rho) = \int_{\boldsymbol{Z}_l} x^{m-1} d\lambda_{e,\rho} = D^{m-1} f_{e,\rho}(0),$$

where $D = (1+T)d/dT$ and $f_{e,\rho} \in \boldsymbol{Z}_l[[\mathrm{T}]]$ is the power series corresponding to $\lambda_{e,\rho}$. Therefore, $\rho \in \bigcap_{\geqq 1}^{m:\ odd} \operatorname{Ker} \chi_e^{(m)}$ if and only if ρ fixes $(e_n^{\sigma_a})^{1/l^n}$ for all natural numbers n and all $a \in \boldsymbol{Z}_l^\times$. The proposition follows from this.

It is known that under the Vandiver conjecture[*] for l, the maximum unramified pro-l abelian extension of $\boldsymbol{Q}(\mu_{l^\infty})$ is contained in the field $\boldsymbol{Q}(\mu_{l^\infty}, c^{1/l^n}$; all $n \geqq 1$ and all cyclotomic units c in $\boldsymbol{Q}(\mu_{l^\infty}))$ (see e.g. [Col] p. 6). Therefore, we get from Propositions 2 and 3,

Corollary. *Under the Vandiver conjecture for l,* Cyclo $= \Omega_l^-$.

3-3. The Vandiver conjecture for l is valid if and only if the

[*] For the Vandiver conjecture and its equivalent form, see [W] p. 157.

Kummer characters $\chi_3, \chi_5, \cdots, \chi_{l-2}\colon \mathfrak{G} \to \boldsymbol{Z}_l$ are surjective. More precisely,

Proposition 4.[**] *Let i be an odd integer with $1 \leqq i \leqq l-2$.*

(i) *If $m \equiv 1(l-1)$, χ_m is surjective.*

(ii) *If $i > 1$ and $m \equiv i(l-1)$, χ_m is surjective if and only if*

$$(E^+/C(E^+)^l)^{(l-i)} = \{0\},$$

where E^+ (resp. C) denotes the group of units (resp. cyclotomic units) of $\boldsymbol{Q}(\cos 2\pi/l)$.

From this proposition and Theorem A, we get

Corollary. *χ_m generates* $\mathrm{Hom}_{G_\infty}(\mathfrak{G}, \boldsymbol{Z}_l(m))$ *over $\boldsymbol{Z}_l$ for all odd integers $m \geqq 1$ if and only if the Vandiver conjecture for l is valid.*

Proof of Proposition 4. First, by the definitions of χ_m and $\varepsilon_n^{(m)}$, χ_m is surjective if and only if $\varepsilon_1^{(m)} \notin \boldsymbol{Q}(\mu_l)^{\times l}$. Now let $m \equiv 1(l-1)$. Then by a direct calculation, $\varepsilon_1^{(m)} \equiv l\ (\boldsymbol{Q}(\mu_l)^{\times l})$. But $l \notin \boldsymbol{Q}(\mu_l)^{\times l}$, because $\boldsymbol{Q}(l^{1/l})$ is non-abelian over $\boldsymbol{Q}$. Next, assume that $i > 1$ and $m \equiv i\,(l-1)$. Then since $\sum_{a=1}^{l-1} a^{m-1} \equiv 0(l)$, $\varepsilon_1^{(m)}$ is congruent to a cyclotomic unit $\prod_{a=1}^{l-1}((\zeta_1^a - 1)/(\zeta_1 - 1))^{a^{i-1}}$ modulo $\boldsymbol{Q}(\mu_l)^{\times l}$. We see that this cyclotomic unit modulo $C \cap (E^+)^l$ is a generator of $(C/C \cap (E^+)^l)^{(l-i)}$ over $\boldsymbol{Z}/l$. Therefore, χ_m is surjective if and only if $(C/C \cap (E^+)^l)^{(l-i)} \neq \{0\}$, hence if and only if $(E^+/C(E^+)^l)^{(l-i)} = \{0\}$. This proves the proposition.

3-4. Generators of the maximum unramified subextension of $\Omega_l^-/\boldsymbol{Q}(\mu_{l^\infty})$ are given in [Col] Theorem 10. In this paragraph, we show how to construct a certain unramified subextension of $\Omega_l^-/\boldsymbol{Q}(\mu_{l^\infty})$ more explicitly than in [Col] by using the l-units $\varepsilon_n^{(m)}$.

Let i be an odd integer with $1 \leqq i \leqq l-2$ and $\Omega_l^{(i)}$ be the fixed field of $\bigoplus_{j \neq i} \mathfrak{G}^{(j)}$. For $i = 1$, or $i > 1$ such that the Bernoulli number B_{l-i} is not divisible by l, it is known that $\Omega_l^{(i)}/\boldsymbol{Q}(\mu_{l^\infty})$ contains no unramified subextension (see e.g. [W] Proposition 6.16). So, in the following, we always assume $i > 1$ and $l | B_{l-i}$. Let $g_i(T)$ ($\in \boldsymbol{Z}_l[[T]]$) be the distinguished polynomial corresponding to $L_l(s, \omega^{1-i})$. Then $\deg g_i(T) \geqq 1$ because $i > 1$ and $l | B_{l-i}$. We shall construct an unramified subextension of $\Omega_l^{(i)}/\boldsymbol{Q}(\mu_{l^\infty})$ which is "associated" to a root of g_i of degree one over $\boldsymbol{Q}_l$. Set $d_m = \mathrm{ord}_l\, L_l(m, \omega^{1-m})$ $(= \mathrm{ord}_l\, g_i((1+l)^m - 1) \leqq \infty)$. Then since g_i is a distinguished polynomial with $\deg g_i \geqq 1$, $d_m > 0$.

Proposition 5. *For any natural number $m \equiv i\ (l-1)$, the maximum unramified subextension of $K_m/\boldsymbol{Q}(\mu_{l^\infty})$ is given by $\boldsymbol{Q}(\mu_{l^\infty}, (\varepsilon_{d_m}^{(m)})^{1/l^{d_m}})$ if*

[**] This was communicated to us by Ihara.

$L_l(m, \omega^{1-m}) \neq 0$. *Otherwise,* K_m *is unramified over* $\boldsymbol{Q}(\mu_{l^\infty})$.

This proposition is easily obtained by using Proposition 1 (iii) and the fact that $\varphi_m(\mathscr{U}) = \boldsymbol{Z}_l$ if $m \not\equiv 1\ (l-1)$ (see e.g. [W] Proposition 13.51).

Let α be a root of g_i of degree one[*] over $\boldsymbol{Q}_l$ and e its multiplicity. Then, $\alpha \in l\boldsymbol{Z}_l$; hence α is approximated by integers of the form $(1+l)^m - 1$ with $m \equiv i\ (l-1)$. Let L_α be the subextension of $\Omega_l^{(i)}/\boldsymbol{Q}(\mu_{l^\infty})$ obtained by adjoining all the numbers $(\varepsilon_{d_m}^{(m)})^{1/l^{d_m}}$ where m runs over all natural numbers for which $m \equiv i\ (l-1)$ and $(1+l)^m - 1$ is closer to α than any root β $(\neq \alpha)$ of g_i. Then by Proposition 5, L_α is unramified over $\boldsymbol{Q}(\mu_{l^\infty})$. We consider $\mathrm{Gal}(L_\sigma/\boldsymbol{Q}(\mu_{l^\infty}))$ as a Λ-module in the natural way. On the structure of this Galois group as a Λ-module, we show the following

Proposition 6. *Under the Vandiver conjecture for* l, $\mathrm{Gal}(L_\alpha/\boldsymbol{Q}(\mu_{l^\infty}))$ *is isomorphic to* $\Lambda/(T-\alpha)^e$ *as a* Λ*-module, up to finite kernel and cokernel.*

Proof. It is easily seen that for any natural number m such that $m \equiv i\ (l-1)$ and $(1+l)^m - 1$ is sufficiently close to α, $d_m = \mathrm{ord}_l\,((1+l)^m - 1)^e + \rho$ for a constant ρ which depends only on α. Let τ_m be a generator of the cyclic group

$$\mathrm{Gal}\,(\boldsymbol{Q}(\mu_{l^\infty}, (\varepsilon_{d_m}^{(m)})^{1/l^{d_m}})/\boldsymbol{Q}(\mu_{l^\infty})).$$

Then it is easily seen that

$$(T-\alpha)^j \cdot \tau_m = \tau_m^{\{(1+l)^m - 1 - \alpha\}^j}.$$

But the Vandiver conjecture for l implies that the order of τ_m is d_m (cf. Section 3–3). So, the order of $(T-\alpha)^e \cdot \tau_m$ is l^ρ and the order of $(T-\alpha)^{e-1} \cdot \tau_m$ is $l^{\mathrm{ord}_l\{(1+l)^m - 1 - \alpha\} + \rho}$. Therefore, by a theorem of Mazur and Wiles [MW] we see that $\mathrm{Gal}\,(L_\alpha/\boldsymbol{Q}(\mu_{l^\infty}))$ is isomorphic to $\Lambda/(T-\alpha)^e$ up to finite kernel and cokernel.

[*] When $l < 125000$, it is known that $\deg g_i = 1$ (see e.g. [W] p. 201). The authors know no example such that g_i has a root of degree 2 over $\boldsymbol{Q}_l$.

References

[Coa] J. Coates, p-adic L-functions and Iwasawa's theory, Algebraic Number Fields (Durham Symposium, 1975; ed. by A. Fröhlich), 269–357. Academic Press: London, 1977.

[Col] R. Coleman, Local units modulo circular units, Proc. Amer. Math. Soc., **89** (1983), 1–7.

[D] P. Deligne, Letters to S. Bloch.

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

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

[Iw1] K. Iwasawa, On some modules in the theory of cyclotomic fields, J. Math. Soc. Japan, **16** (1964), 42–82.

[Iw2] ——, On Z_l extensions of algebraic number fields, Ann. of Math., **98** (1973), 246–326.

[L] S. Lichtenbaum, On the values of zeta and L-functions I, Ann. of Math., **96** (1972), 338–360.

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

[S1] C. Soulé, K-théorie des anneaux d'entiers de corps de nombres et cohomologie étale, Invent. Math., **55** (1979), 251–295.

[S2] ——, On higher p-adic regulators, Alg. K-theory, evanston 1980, Springer Lecture Notes in Mathematics, vol. **854** (1981), 372–401.

[S3] ——, Letter to Y. Ihara.

[T] J. Tate, Relations between K_2 and Galois cohomology, Invent. Math., **36** (1976), 257–274.

[W] L. Washington, Introduction to cyclotomic fields, Graduate Texts in Mathematics, Springer-Verlag: New York, 1982.

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