J. Fac. Sci. Univ. Tokyo
Sect. IA, Math.
36 (1989), 1-7.

On the coefficients of the universal power series for Jacobi sums

By Humio ICHIMURA

(Communicated by Y. Ihara)

§ 1. Introduction

The main aim of this article is to give a simple proof of a result in Ihara-Kaneko-Yukinari [5] on the coefficients of the "universal power series for Jacobi sums".

Let $\overline{\boldsymbol{Q}}$ be the algebraic closure of the rational number field $\boldsymbol{Q}$ in the complex number field, l be a fixed odd prime number and μ_{l^n} be the group of l^n-th roots of unity in $\overline{\boldsymbol{Q}}$. Let $\zeta=(\zeta_n)_{n\geq 1}$ be a fixed generator of the l-adic Tate module $T_l(\boldsymbol{G}_m)$, *i.e.*, ζ_n is a primitive element of μ_{l^n} and $\zeta_{n+1}^l=\zeta_n$ $(n\geqq 1)$. By using a tower of Fermat curves, Ihara [4] constructed a Galois representation (associated to the basis ζ)

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

which is "universal" for Jacobi sums. The coefficients of the power series $F_\rho(u,v)$ were determined as follows by Anderson [1], Coleman [3] and Ihara-Kaneko-Yukinari [5]. For any odd integer $m\geqq 1$ and any integer $n\geqq 1$, put

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

Let $\chi_m\colon \mathrm{Gal}(\overline{\boldsymbol{Q}}/\boldsymbol{Q}(\mu_{l^\infty}))\to\boldsymbol{Z}_l$ be the unique homomorphism satisfying

$$\zeta_n^{\chi_m(\rho)}=(\varepsilon_n(m)^{1/l^n})^{\rho-1},\qquad \text{for all } n\geqq 1 \text{ and } \rho\in\mathrm{Gal}(\overline{\boldsymbol{Q}}/\boldsymbol{Q}(\mu_{l^\infty})).$$

Then, it has been proved ([1], [3], [5]) that

$$F_\rho(u,v)=\exp\Big\{\sum_{\substack{m\geqq 3\\ \text{odd}}}\frac{(1-l^{m-1})^{-1}\cdot\chi_m(\rho)}{m!}(U^m+V^m+W^m)\Big\}. \tag{1}$$

Here, $U=\log(1+u)$, $V=\log(1+v)$ and $W=-(U+V)$. The proof of the coefficient formula (1) in [5] differs very much from those in [1] and [3].

We shall give a simplification of the proof in [5]. Further, we shall give a remark on the kernel of the representation $\boldsymbol{F}$.

§ 2. Simplified proof of the coefficient formula

§ 2-1. Simplified proof of the coefficient formula

Let Ω_l^- be the odd part of the maximal pro-l abelian extension of $\boldsymbol{Q}(\mu_{l^\infty})$ unramified outside l, and put $\mathfrak{G}=\mathrm{Gal}(\Omega_l^-/\boldsymbol{Q}(\mu_{l^\infty}))$. The Galois representation $\boldsymbol{F}$ factors through $\mathfrak{G}$, and the power series $F_\rho(u,v)$ for $\rho\in\mathfrak{G}$ can be written as

$$F_\rho(u,v)=\exp\left\{\sum_{\substack{m\geqq 3\\ \text{odd}}}\sum_{\substack{j,k>0\\ j+k=m}}\frac{\beta_{j,k}(\rho)}{j!k!}U^jV^k\right\} \tag{2}$$

with

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

(cf. [4, p. 96]). Here, $\boldsymbol{Z}_l^\times=\mathrm{Gal}(\boldsymbol{Q}(\mu_{l^\infty})/\boldsymbol{Q})$ acts on $\mathfrak{G}$ by conjugation and $\boldsymbol{Z}_l(m)$ denotes the Tate twist of the module $\boldsymbol{Z}_l$ with a trivial $\boldsymbol{Z}_l^\times$-action. From the definition, the homomorphism χ_m also factors through $\mathfrak{G}$. To prove the coefficient formula, it suffices to show that

$$(*)\qquad \beta_{j,k}(\rho)=(l^{m-1}-1)^{-1}\chi_m(\rho),\quad m=j+k,\qquad \text{for all}\quad \rho\in\mathfrak{G}.$$

Let $\mathfrak{U}_n$ be the group of principal units of the local l^n-th cyclotomic field $\boldsymbol{Q}_l(\zeta_n)$ and let $\mathfrak{U}$ be the projective limit of $\mathfrak{U}_n$ w.r.t. the relative norm. For each integer m ($\geqq 0$), let $\phi_m\colon \mathfrak{U}\to\boldsymbol{Z}_l$ be the m-th Coates-Wiles homomorphism w.r.t. the fixed basis ζ (cf. [11, p. 307]). By class field theory, we can identify the inertia group $\mathfrak{T}$ of an extension of l in $\Omega_l^-/\boldsymbol{Q}(\mu_{l^\infty})$ with a certain submodule of the odd part $\mathfrak{U}^-$ of $\mathfrak{U}$ (cf. [7, § 3-2]). It is known that the restrictions $\beta_{j,k}|\mathfrak{T}$ and $\phi_m|\mathfrak{T}$ are related with each other by

$$\beta_{j,k}|\mathfrak{T}=L_l(m,\omega^{1-m})\phi_m|\mathfrak{T},\qquad m=j+k\qquad ([4,\ \text{Th. } 10]). \tag{3}$$

Here, ω is the Teichmüller character of $\Delta=\mathrm{Gal}(\boldsymbol{Q}(\zeta_1)/\boldsymbol{Q})$ and $L_l(*,\omega^{1-m})$ is the l-adic L-function. As for the homomorphism χ_m, Coleman proved, by using some results of [2], that

$$\chi_m|\mathfrak{T}=(l^{m-1}-1)L_l(m,\omega^{1-m})\phi_m|\mathfrak{T},\quad m\geqq 3,\ \text{odd}. \tag{4}$$

By the above relations, the assertion (*) holds for $\rho\in\mathfrak{T}$. To prove (*) for all $\rho\in\mathfrak{G}$, we shall extend the relations (3) and (4) to those on the whole

Galois group $\mathfrak{G}$. But since the homomorphism ϕ_m is not defined on $\mathfrak{G}$, we have to throw the whole Galois group into the inertia group $\mathfrak{T}$ as follows. Let i be any fixed odd integer with $1 \leqq i \leqq l-2$. When $i \neq 1$, we denote by f_i the power series in $\boldsymbol{Z}_l[[t]]$ corresponding to the l-adic L-function $L_l(s, \omega^{1-i})$, *i.e.*, $f_i((1+l)^s-1)=L_l(s, \omega^{1-i})$. We regard the power series f_i as an element of the group ring $\Lambda=\boldsymbol{Z}_l[[1+l\boldsymbol{Z}_l]]$ by the isomorphism $\Lambda \cong \boldsymbol{Z}_l[[t]]$ $(, 1+l \mapsto 1+t)$. For a Λ-module M, we denote by $M^{(i)}$ the ω^i-eigenspace of M. The following lemma is known (cf. [7, § 3]).

LEMMA 1. (i) *When* $i \neq 1$, $f_i \cdot \mathfrak{G}^{(i)} \subset \mathfrak{T}^{(i)}$. (ii) *When* $i=1$, $\mathfrak{G}^{(1)}=\mathfrak{T}^{(1)}$.

The assertion (*) for $\rho \in \mathfrak{G}^{(1)}$ follows immediately from Lemma 1 (ii) and the relations (3), (4). For $i \neq 1$ and $\rho \in \mathfrak{G}^{(i)}$, we see from Lemma 1 (i) that the homomorphism ϕ_m is defined for $f_i \cdot \rho$. The assertion (*) for $i \neq 1$ and $\rho \in \mathfrak{G}^{(i)}$ follows from the following lemmas.

LEMMA 2. *Assume* $i \neq 1$. *For all odd integers* m $(\geqq 3)$ *and integers* j, k (>0) *with* $j+k=m$, *and for all* $\rho \in \mathfrak{G}^{(i)}$, $\beta_{j,k}(\rho)=\phi_m(f_i \cdot \rho)$.

LEMMA 3. *Assume* $i \neq 1$. *For all odd integers* m $(\geqq 3)$ *and all* $\rho \in \mathfrak{G}^{(i)}$, $\chi_m(\rho)=(l^{m-1}-1) \cdot \phi_m(f_i \cdot \rho)$.

PROOF OF LEMMA 2. For $\varepsilon \in \mathfrak{T}$ $(\subset \mathfrak{U}^-)$, let $g_\varepsilon(t)$ $(\in \boldsymbol{Z}_l[[t]]^\times)$ denote the Coleman power series of ε w.r.t. the fixed basis ζ of $T_l(\boldsymbol{G}_m)$. We define an element $H_\varepsilon(u, v)$ of $\boldsymbol{Z}_l[[u, v]]^\times$ by

$$H_\varepsilon(u, v)=g_\varepsilon(u)g_\varepsilon(v)g_\varepsilon(w)\,.$$

Here, w is the element of $\boldsymbol{Z}_l[[u, v]]^\times$ defined by $(1+u)(1+v)(1+w)=1$. By the definition of the Coates-Wiles homomorphisms, the power series H_ε can be written as

$$H_\varepsilon(u, v)=\exp\left\{\sum_{\substack{m \geqq 3 \\ \text{odd}}} \sum_{\substack{j,k>0 \\ j+k=m}} \frac{\phi_m(\varepsilon)}{j!k!} U^j V^k\right\}. \tag{5}$$

As is easily seen, the power series $F_\rho(u, v)$ and $H_\varepsilon(u, v)$ belong to the subgroup $\mathcal{F}=\{F \in \boldsymbol{Z}_l[[u, v]]^\times\,;\ F(0, 0) \equiv 1 \pmod{l}\}$ of $\boldsymbol{Z}_l[[u, v]]^\times$. Consider the following two homomorphisms

$$\mathfrak{G}^{(i)} \ni \rho \longmapsto F_\rho(u, v) \in \mathcal{F}\,,$$

$$\mathfrak{G}^{(i)} \ni \rho \longmapsto H_{f_i \cdot \rho}(u, v) \in \mathcal{F}\,.$$

Both homomorphisms are elements of the module $\mathrm{Hom}_{Z_l^\times}(\mathfrak{G}^{(i)}, \mathcal{F})$, and by (3)

(and (2), (5)), they coincide on the inertia group $\mathfrak{T}^{(i)}$. But, since the inertia restriction

$$\text{(6)} \qquad \mathrm{Hom}_{Z_l^\times}(\mathfrak{G}^{(i)}, \mathcal{F}) \longrightarrow \mathrm{Hom}_{Z_l^\times}(\mathfrak{T}^{(i)}, \mathcal{F})$$

is injective ([5, Key Lemma]), the above homomorphisms coincide on the whole Galois group $\mathfrak{G}^{(i)}$. Hence, $F_\rho = H_{f_i \cdot \rho}$ for all $\rho \in \mathfrak{G}^{(i)}$. By comparing the coefficients of the above two power series, we obtain the lemma.

PROOF OF LEMMA 3. Consider the following two homomorphisms

$$\mathfrak{G}^{(i)} \ni \rho \longmapsto \chi_m(\rho) \in \boldsymbol{Z}_l\,,$$

$$\mathfrak{G}^{(i)} \ni \rho \longmapsto (l^{m-1}-1)\phi_m(f_i \cdot \rho) \in \boldsymbol{Z}_l\,.$$

They are elements of the module $\mathrm{Hom}_{Z_l^\times}(\mathfrak{G}^{(i)}, \boldsymbol{Z}_l(m))$. Hence, in particular, they are trivial when $m \not\equiv i \pmod{l-1}$. In the following, we deal with the case where $m \equiv i \pmod{l-1}$. By the relation (4), the above homomorphisms coincide on the inertia group $\mathfrak{T}^{(i)}$. On the other hand, the inertia restriction

$$\mathrm{Hom}_{Z_l^\times}(\mathfrak{G}^{(i)}, \boldsymbol{Z}_l(m)) \longrightarrow \mathrm{Hom}_{Z_l^\times}(\mathfrak{T}^{(i)}, \boldsymbol{Z}_l(m))$$

is injective if and only if $L_l(m, \omega^{1-i}) \neq 0$ by a theorem of Mazur and Wiles (see e.g. [11, § 13.6]). But since there exist only finitely many m such that $L_l(m, \omega^{1-i}) = 0$, we see that $\chi_m(\rho) = (l^{m-1}-1)\phi_m(f_i \cdot \rho)$ except for only finitely many m. But we easily see from the definition that χ_m is continuous (l-adically) in m, and it is known that so is $(l^{m-1}-1)\phi_m$ (see e.g. [11, p. 309]). Therefore, $\chi_m(\rho) = (l^{m-1}-1)\phi_m(f_i \cdot \rho)$ for all $m \equiv i\ (l-1)$ and all $\rho \in \mathfrak{G}^{(i)}$.

§ 2-2. An alternative proof of Key Lemma in [5]

The injectivity of the inertia restriction (6) ([5, Key Lemma]) was essential in the proof of Lemma 2. Since its proof in [5] is rather complicated, we shall give, in this subsection, a simple alternative proof.

When $i=1$, the injectivity of (6) follows immediately from Lemma 1 (ii). In the following, we assume $i \neq 1$. Since the additive group $\boldsymbol{Z}_l[[u, v]]$ is easier to deal with than the multiplicative group $\mathcal{F}$, we map $\mathcal{F}$ into $\boldsymbol{Z}_l[[u, v]]$ by the following homomorphism λ:

$$\begin{array}{ccc} \mathcal{F} & \longrightarrow & \boldsymbol{Z}_l[[u, v]] \\ \cup\!\!| & & \cup\!\!| \\ F(u, v) & \longmapsto & \log F(u, v) - \dfrac{1}{l}\log F((1+u)^l - 1, (1+v)^l - 1)\,. \end{array}$$

This is well defined by the lemma of Dieudonné and Dwork (cf. [5, Lem.

4]). We easily see that the kernel of λ is

$$\{(1+u)^a(1+v)^b\ ;\ a, b\in \boldsymbol{Z}_l\}$$

and hence contained in $\mathfrak{F}^{(1)}$. So, the homomorphism $\lambda|\mathfrak{F}^{(i)}$ $(i\neq 1)$ is injective. Therefore, since the image of any $\boldsymbol{Z}_l^\times$-homomorphism of $\mathfrak{G}^{(i)}$ to $\mathfrak{F}$ is contained in $\mathfrak{F}^{(i)}$, it suffices to prove the injectivity of the inertia restriction

$$\text{(7)}\qquad \mathrm{Hom}_{\boldsymbol{Z}_l^\times}(\mathfrak{G}^{(i)}, \boldsymbol{Z}_l[[u, v]]) \longrightarrow \mathrm{Hom}_{\boldsymbol{Z}_l^\times}(\mathfrak{T}^{(i)}, \boldsymbol{Z}_l[[u, v]])\,.$$

Let f be any element of the module $\mathrm{Hom}_{\boldsymbol{Z}_l^\times}(\mathfrak{G}^{(i)}, \boldsymbol{Z}_l[[u, v]])$. The power series $f_\rho(u, v)$ $(\rho\in\mathfrak{G}^{(i)})$ in $\boldsymbol{Z}_l[[u, v]]$ can be written as

$$\text{(8)}\qquad f_\rho(u, v)=\sum_{m\equiv i}\sum_{\substack{j,k\geqq 0\\ j+k=m}}\frac{a_{j,k}(\rho)}{j!\,k!}U^jV^k$$

with

$$a_{j,k}\in\mathrm{Hom}_{\boldsymbol{Z}_l^\times}(\mathfrak{G}^{(i)}, \boldsymbol{Z}_l(m)),\qquad m=j+k\,.$$

Here, the summation $\sum_{m\equiv i}$ is taken over all integers m (>0) such that $m\equiv i \pmod{l-1}$. Assume that $f|\mathfrak{T}^{(i)}=0$ but $f\neq 0$. From the first assumption, we see that $a_{j,k}=0$ except for only finitely many (j, k) by using an argument in the proof of Lemma 3. But by the second assumption, there exists (j, k) with $a_{j,k}\neq 0$. Let J be the largest j such that $a_{j,k}\neq 0$ for some k and K be the largest k such that $a_{J,k}\neq 0$. By exchanging the roles of j and k if necessary, we may assume $J>0$. Let $\partial_u=(1+u)\dfrac{\partial}{\partial u}=\dfrac{\partial}{\partial U}$ and $\partial_v=(1+v)\dfrac{\partial}{\partial v}=\dfrac{\partial}{\partial V}$ be differential operators on $\boldsymbol{Z}_l[[u, v]]$. By letting $(\partial_v)^K(\partial_u)^{J-1}$ act on both sides of (8), we see that

$$(\partial_v)^K(\partial_u)^{J-1}f_\rho(u, v)=a_{J,K}(\rho)\cdot U\in\boldsymbol{Z}_l[[u, v]]\,.$$

This is a contradiction because $U=\log(1+u)$ is not in $\boldsymbol{Z}_l[[u, v]]$ and $a_{J,K}(\rho)\neq 0$ for some $\rho\in\mathfrak{G}^{(i)}$. This completes the proof of the injectivity of the inertia restriction (6).

§ 3. A note on the kernel of F.

Let K be the subextension of $\Omega_l/\boldsymbol{Q}(\mu_{l^\infty})$ corresponding to the kernel of the Galois representation $\boldsymbol{F}$. As a corollary of the coefficient formula $\beta_{j,k}=(l^{m-1}-1)\chi_m$ $(m=j+k)$, one sees (as in [3] and [5]) that the field K coincides with the field

$$C=\boldsymbol{Q}(\mu_{l^\infty}, \varepsilon_n(m)^{1/l^n}\ ;\ \text{all } n\geqq 1 \text{ and all } m\geqq 3,\ \text{odd})\,.$$

For these fields K and C, see also [8, § 3-2] and [6, § 2]. In this section, we shall show that this result follows also from the inertia restriction data for $\beta_{j,k}$ ((3) of § 2) and the following theorem of C. Soulé.

THEOREM S. ([9, p. 376], [10])

(i) $\mathrm{Hom}_{Z_l^\times}(\mathfrak{G}, \boldsymbol{Z}_l(m)) \cong \boldsymbol{Z}_l$ *for all* $m \geqq 1$, *odd.*
(ii) $\chi_m \neq 0$ *for all* $m \geqq 1$, *odd.*

For this theorem, see also [8].

First, by Theorem S, $\beta_{j,k} = c_{j,k} \cdot \chi_m$ $(m = j+k)$ for some $c_{j,k} \in \boldsymbol{Q}_l$. Hence, $\mathrm{Ker}\,\beta_{j,k} \supset \mathrm{Ker}\,\chi_m$. But, since the field K (resp. C) corresponds to the subgroup $\bigcap_{j,k} \mathrm{Ker}\,\beta_{j,k}$ (resp. $\bigcap_m \mathrm{Ker}\,\chi_m$) of $\mathfrak{G}$, we see that $K \subset C$. By using (3) in § 2, we see that the extension Ω_l^-/K is unramified. For the proof, see [8, § 3]. Therefore, the extension C/K is unramified and hence $\mathrm{Gal}(C/K)$ is a torsion Λ-module. Assume for an element ρ of $\mathrm{Gal}(C/\boldsymbol{Q}(\mu_{l^\infty})) = \mathfrak{G}/(\bigcap_m \mathrm{Ker}\,\chi_m)$ and a non-zero element $g(t)$ of Λ that $g \cdot \rho = 1$. Then, for all odd integers $m \geqq 1$, $0 = \chi_m(g \cdot \rho) = g((1+l)^m - 1)\chi_m(\rho)$. Since $g(t)$ has only finitely many roots, $\chi_m(\rho) = 0$ for almost all m's. But since χ_m is continuous (l-adically) in m, $\chi_m(\rho) = 0$ for all odd integers m. Hence, $\rho = 1$. Therefore, $\mathrm{Gal}(C/\boldsymbol{Q}(\mu_{l^\infty}))$ and especially its submodule $\mathrm{Gal}(C/K)$ are free over Λ. From this, we get $K = C$.

References

[1] Anderson, G. W., The hyperadelic gamma function, Invent. Math. **95** (1989), 63-131.
[2] Coleman, R., The dilogarithm and the norm residue symbol, Bull. Soc. Math. France **109** (1981), 373-402.
[3] Coleman, R., Anderson-Ihara theory: Gauss sums and circular units, Adv. St. in Pure Math. **17** (in press).
[4] Ihara, Y., Profinite braid groups, Galois representations and complex multiplications, Ann. of Math. **123** (1986), 43-106.
[5] Ihara, Y., Kaneko, M. and A. Yukinari, On some properties of the universal power series for Jacobi sums, Adv. St. in Pure Math. **12** (1987), 65-86.
[6] Ichimura, H., A note on a global version of the Coleman embedding, Proc. Japan Acad. **62** (1986), 347-349.
[7] Ichimura, H. and M. Kaneko, On the universal power series for Jacobi sums and the Vandiver conjecture, J. Number Theory **31** (in press).
[8] Ichimura, H. and K. Sakaguchi, On the non-vanishing of a certain Kummer character χ_m (after Soulé), and some related topics, Adv. St. in Pure Math. **12** (1987), 53-64.
[9] Soulé, C., On higher p-adic regulators, Lecture Notes in Math. vol. 854, Springer Verlag, Berlin-Heiderberg-New York, 1980, 372-401.
[10] Soulé, C., Letter to Y. Ihara.

[11] Washington, L., Introduction to Cyclotomic Fields, Springer-Verlag, New York, 1982.

(Received April 23, 1988)
(Revised October 26, 1988)

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