71. A Note on the Universal Power Series for Jacobi Sums

By Humio ICHIMURA
Department of Mathematics, Yokohama City University

(Communicated by Shokichi IYANAGA, M. J. A., Sept. 12, 1989)

§ 1. **Introduction.** This note is a supplement of our previous work [5], and we use the same notation as in [5].

Let l be a fixed odd prime number. Ihara [7] constructed for each element ρ of $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q}(\mu_{l^\infty}))$ an l-adic two variable power series $F_\rho(u, v)$ by using a tower of Fermat curves. Some properties of $F_\rho(u, v)$ were studied by [7], Anderson [1], Coleman [3], Ihara-Kaneko-Yukinari [8], etc. In particular, it is proved that the power series $F_\rho(u, v)$ is universal for Jacobi sums and "hence" can be written as a product of three copies of a certain one variable power series. We denote by $g_\rho(t)$ the "twisted log" of the one variable power series, which is known to be an element of $\boldsymbol{Z}_l[[t]]$ (cf. [8]).

The purpose of this note is to describe the difference (if any) between the "expected" image of the homomorphism

$$\tilde{\boldsymbol{g}}: \quad \mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q}(\mu_{l^\infty})) \ni \rho \longrightarrow g_\rho(t) \bmod l \in \boldsymbol{F}_l[[t]]$$

and its actual image by means of Iwasawa invariants of the l-cyclotomic field $\boldsymbol{Q}(\mu_{l^\infty})$.

To be more precise, denote by $\tilde{\mathcal{V}}^-$ the additive group consisting of all the power series $g(t)$ in $\boldsymbol{F}_l[[t]]$ satisfying

$$D^{l-1}g = g \quad \text{and} \quad g((1+t)^{-1}-1) = -g(t).$$

Here, $D=(1+t)d/dt$ is a differential operator on $\boldsymbol{F}_l[[t]]$. Then, this module $\tilde{\mathcal{V}}^-$ is the "expected" image in the following sense:

Theorem 1 ([5, Th. 3′]). *$\mathrm{Im}\,\tilde{\boldsymbol{g}} \subset \tilde{\mathcal{V}}^-$, and both sides coincide if and only if the Vandiver conjecture is valid.*

Let λ be Iwasawa's λ-invariant of the cyclotomic $\boldsymbol{Z}_l$-extension of the real cyclotomic field $\boldsymbol{Q}(\cos(2\pi/l))$. In § 2, we define an invariant ε of a certain Galois group over $\boldsymbol{Q}(\mu_{l^\infty})$, which is very similar to its ν-invariant. Our result is

Theorem 2. *The cardinality of the quotient $\tilde{\mathcal{V}}^-/(\mathrm{Im}\,\tilde{\boldsymbol{g}})$ is finite and is equal to $l^{\lambda+\varepsilon}$.*

On the other hand, Coleman [3] proved that the power series $g_\rho(t)$ satisfies some non obvious functional equations and that these functional equations characterize the image of the homomorphism

$$\boldsymbol{g}: \quad \mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q}(\mu_{l^\infty})) \ni \rho \longrightarrow g_\rho(t) \in \boldsymbol{Z}_l[[t]]$$

if and only if the Vandiver conjecture is valid. In [5, Th. 2], we described the difference between the "expected" image of $\boldsymbol{g}$ and its actual image by means of Iwasawa type invariant of $\boldsymbol{Q}(\mu_{l^\infty})$. Theorems 1 and 2 are modulo l version of these results.

§2. Definition of ε. In this section, we define the invariant ε and give a simple remark on the invariant λ mentioned in §1.

Let Ω_l^- be the "odd part" of the maximum pro-l abelian extension over $\boldsymbol{Q}(\mu_{l^\infty})$ unramified outside l, and put $\mathfrak{G}=\mathrm{Gal}(\Omega_l^-/\boldsymbol{Q}(\mu_{l^\infty}))$. We denote by Λ and Λ_1 the completed group rings $\boldsymbol{Z}_l[[\boldsymbol{Z}_l^\times]]$ and $\boldsymbol{Z}_l[[1+l\boldsymbol{Z}_l]]$ respectively. We identify Λ_1 with the power series ring $\boldsymbol{Z}_l[[t]]$ by $1+l\leftrightarrow 1+t$. The Galois group $\mathfrak{G}$ admits a Λ-module structure and also a $\boldsymbol{Z}_l[\Delta]$-module structure in the usual way, here $\Delta=\mathrm{Gal}(\boldsymbol{Q}(\mu_l)/\boldsymbol{Q})$. For a $\boldsymbol{Z}_l[\Delta]$-module M and an integer j, we denote by $M^{(j)}$ the ω^j-eigenspace of M, ω being the Teichmüller character of Δ. In what follows, i denotes an odd integer with $1\leq i\leq l-2$. It is known that the free part $\mathfrak{H}^{(i)}=\mathfrak{G}^{(i)}/(\mathrm{Tor}_{\Lambda_1}\mathfrak{G}^{(i)})$, $\mathrm{Tor}_{\Lambda_1}\mathfrak{G}^{(i)}$ being the Λ_1-torsion part of $\mathfrak{G}^{(i)}$, is pseudo-isomorphic to Λ_1. Hence there exists an injective Λ-homomorphism $\iota\colon \mathfrak{H}^{(i)}\to\Lambda_1$ with a finite cokernel. As is easily seen, the image $\mathfrak{A}_i$ of ι depends only on $\mathfrak{H}^{(i)}$ and not on the choice of ι. We define

$$\varepsilon_i=\mathrm{Min}\{\deg g\,|\,\text{all distiguished polynomials } g \text{ in } \mathfrak{A}_i\},\qquad \varepsilon=\sum_i\varepsilon_i.$$

Here, we regard the constant power series 1 ($\in\Lambda_1$) as a distinguished polynomial of degree zero. This invariant ε_i is a kind of Iwasawa's ν-invariant of $\mathfrak{H}^{(i)}$.

As for the invariant λ mentioned in §1, we see that it is equal to Iwasawa's λ-invariant of the torsion Λ_1-submodule $\mathrm{Tor}_{\Lambda_1}\mathfrak{G}$ of $\mathfrak{G}$ by using the "Spiegelung Satz" (cf. [5, §3.1]). Further, we denote by λ_i Iwasawa's λ-invariant of $\mathrm{Tor}_{\Lambda_1}\mathfrak{G}^{(i)}$. Then we have $\lambda=\sum_i\lambda_i$.

§3. Proof of Theorem 2. It is known that the homomorphisms $\boldsymbol{g}$ and $\tilde{\boldsymbol{g}}$ factor through $\mathfrak{G}$ (cf. [7]), and we denote the induced homomorphisms $\mathfrak{G}\to\boldsymbol{Z}_l[[t]]$ and $\mathfrak{G}\to\boldsymbol{F}_l[[t]]$ also by $\boldsymbol{g}$ and $\tilde{\boldsymbol{g}}$ respectively. We put $\boldsymbol{g}^{(i)}=\boldsymbol{g}|_{\mathfrak{G}^{(i)}}$ and $\tilde{\boldsymbol{g}}^{(i)}=\tilde{\boldsymbol{g}}|_{\mathfrak{G}^{(i)}}$. Since the induced homomorphisms $\boldsymbol{g}$ and $\tilde{\boldsymbol{g}}$ are compatible with the action of Λ (cf. [7]), we see from Theorem 1 that $\mathrm{Im}\,\tilde{\boldsymbol{g}}^{(i)}\subset\widetilde{\mathcal{V}}^{(i)}$. To prove Theorem 2, it suffices to prove the following Δ-decomposed version:

Theorem 2′. *The cardinality of the quotient $\widetilde{\mathcal{V}}^{(i)}/(\mathrm{Im}\,\tilde{\boldsymbol{g}}^{(i)})$ is finite and is equal to $l^{\lambda_i+\varepsilon_i}$.*

For the convenience of readers, we state here the theorem of Coleman referred to in §1. Let $\mathcal{V}^{(i)}$ be the ω^i-eigenspace of the Λ-module

$$\mathcal{V}=\{g\in\boldsymbol{Z}_l[[t]]\,|\,\sum_{\zeta^l=1}g(\zeta(1+t)-1)=0\}.$$

Theorem C ([3]). $\mathrm{Im}\,\boldsymbol{g}^{(i)}\subset\mathcal{V}^{(i)}$, *and both sides coincide if and only if the Vandiver conjecture for $(l-i)$-part is valid, i.e., the ω^{l-i}-eigenspace of the l-class group of $\boldsymbol{Q}(\cos(2\pi/l))$ is trivial.*

Let g_i be a characteristic power series of $\mathrm{Tor}_{\Lambda_1}\mathfrak{G}^{(i)}$. The following is essential in the proof of Theorem 2′.

Proposition 1. $\mathrm{Im}\,\boldsymbol{g}^{(i)}\subset g_i\cdot\mathcal{V}^{(i)}$ *and $(g_i\cdot\mathcal{V}^{(i)})/(\mathrm{Im}\,\boldsymbol{g}^{(i)})$ is finite.*

Remark. This is a quantitative version of Theorem C. An assertion a little weaker than Prop. 1 is given in [5, Prop. 3].

Proof of Prop. 1. First we deal with the case $i=1$. By Theorem C and the Stickelberger theorem (see e.g. [9, Prop. 6.16]), we see that $\mathrm{Im}\,\boldsymbol{g}^{(1)}=$

$\mathcal{CV}^{(1)}$. By using the Stickelberger theorem again, we obtain $g_1=1$. So, Prop. 1 is valid when $i=1$. Next, assume $i\neq 1$.
Let $\mathfrak{T}$ be the inertia group of an extension of l in $\Omega_l^-/\boldsymbol{Q}(\mu_{l^\infty})$, and let f_i be a characteristic power series of the torsion Λ_1-module $\mathfrak{G}^{(i)}/\mathfrak{T}^{(i)}$. In [5, Prop. 5(1)], we have given a relation between the homomorphism $\boldsymbol{g}^{(i)}$ from $\mathfrak{G}^{(i)}$ to $\mathcal{CV}^{(i)}$ and the Coleman's isomorphism $\lambda\circ[\mathrm{Col}]$ from $\mathfrak{T}^{(i)}$ onto $\mathcal{CV}^{(i)}$ as follows. For the definition of $\lambda\circ[\mathrm{Col}]$, see [2] or [5, §3].

$$f_i\cdot\mathfrak{G}^{(i)}\subset\mathfrak{T}^{(i)}\quad\text{and for}\quad \rho\in\mathfrak{G}^{(i)},\ \boldsymbol{g}^{(i)}(\rho)=\lambda\circ[\mathrm{Col}](f_i\cdot\rho).$$

As before, $\mathfrak{H}^{(i)}$ denotes the free part $\mathfrak{G}^{(i)}/(\mathrm{Tor}_{\Lambda_1}\mathfrak{G}^{(i)})$ of $\mathfrak{G}^{(i)}$. Since $\mathrm{Ker}\,\boldsymbol{g}^{(i)}=\mathrm{Tor}_{\Lambda_1}\mathfrak{G}^{(i)}$ (cf. [5, §3.1]), $\boldsymbol{g}^{(i)}$ induces an injective homomorphism from $\mathfrak{H}^{(i)}$ to $\mathcal{CV}^{(i)}$, which we denote by $\bar{\boldsymbol{g}}^{(i)}$. Let $\overline{\mathfrak{T}}^{(i)}$ be the subgroup of $\mathfrak{H}^{(i)}$ defined by $\overline{\mathfrak{T}}^{(i)}=\mathfrak{T}^{(i)}$ modulo $\mathrm{Tor}_{\Lambda_1}\mathfrak{G}^{(i)}$, which is canonically isomorphic to $\mathfrak{T}^{(i)}$ (cf. [6, Prop. 2]). Hence, $\lambda\circ[\mathrm{Col}]$ induces an isomorphism from $\overline{\mathfrak{T}}^{(i)}$ onto $\mathcal{CV}^{(i)}$, which we denote by $\overline{\lambda\circ[\mathrm{Col}]}$. From [5, Prop. 5(1)] recalled above, it follows that

$$f_i\cdot\mathfrak{H}^{(i)}\subset\overline{\mathfrak{T}}^{(i)}\quad\text{and for}\quad \rho\in\mathfrak{H}^{(i)},\ \bar{\boldsymbol{g}}^{(i)}(\rho)=\overline{\lambda\circ[\mathrm{Col}]}(f_i\cdot\rho).$$

As is easily seen from [6, Prop. 2], the power series f_i is divisible by g_i and f_i/g_i is a characteristic power series of the torsion Λ_1-module $\mathfrak{H}^{(i)}/\overline{\mathfrak{T}}^{(i)}$. Let ι be (as in §2) an embedding of $\mathfrak{H}^{(i)}$ into Λ_1 with a finite cokernel. Since $\mathfrak{T}^{(i)}$ is isomorphic to Λ_1 (see e.g. [2]), we see that $\iota(\overline{\mathfrak{T}}^{(i)})=(f_i/g_i)\cdot\Lambda_1$. Hence, $f_i\cdot\mathfrak{H}^{(i)}\subset g_i\cdot\overline{\mathfrak{T}}^{(i)}$ and $(g_i\cdot\overline{\mathfrak{T}}^{(i)})/(f_i\cdot\mathfrak{H}^{(i)})$ is finite. Now, the assertion of Prop. 1 for $i\neq 1$ follows from the above relation between $\bar{\boldsymbol{g}}^{(i)}$ and $\overline{\lambda\circ[\mathrm{Col}]}$.

Proof of Theorem 2′. Recall that $\mathcal{CV}^{(i)}\bmod l=\tilde{\mathcal{CV}}^{(i)}$ (cf. [5]). Hence, by Prop. 1, we get $\mathrm{Im}\,\tilde{\boldsymbol{g}}^{(i)}\subset g_i\cdot\tilde{\mathcal{CV}}^{(i)}$ and $(g_i\cdot\tilde{\mathcal{CV}}^{(i)})/(\mathrm{Im}\,\tilde{\boldsymbol{g}}^{(i)})$ is finite. Since Iwasawa's μ-invariant of $\mathrm{Tor}_{\Lambda_1}\mathfrak{G}^{(i)}$ is zero (cf. Ferrero-Washington [4]), we may assume that g_i is a distinguished polynomial of degree λ_i. Therefore, since $\mathcal{CV}^{(i)}$ is isomorphic to $\Lambda_1=\boldsymbol{Z}_l[[t]]$ (cf. [2]), the quotient $\tilde{\mathcal{CV}}^{(i)}/g_i\cdot\tilde{\mathcal{CV}}^{(i)}$ is finite and its cardinality is l^{λ_i}. Since $\mathcal{CV}^{(i)}\simeq\Lambda_1$, we may identify $g_i\cdot\mathcal{CV}^{(i)}$ with Λ_1. Then, by Prop. 1, the homomorphism $\bar{\boldsymbol{g}}^{(i)}$ gives an injective homomorphism from $\mathfrak{H}^{(i)}$ to Λ_1 with a finite cokernel. Therefore, by the very definition of ε_i and that $\mu=0$, we see that the cardinality of the quotient $(g_i\cdot\tilde{\mathcal{CV}}^{(i)})/(\mathrm{Im}\,\tilde{\boldsymbol{g}}^{(i)})$ is l^{ε_i}. This completes the proof.

§4. The Galois group $\mathfrak{G}$ and the Vandiver conjecture. In this section, we give an alternative proof of the following well known fact by using the homomorphism $\boldsymbol{g}^{(i)}$.

Proposition 2. *The following conditions are equivalent:*

(i) *The Vandiver conjecture for* $(l-i)$*-part is valid.*

(ii) $\mathfrak{G}^{(i)}$ *is torsion free and cyclic over* Λ_1

(iii) $\mathfrak{G}^{(i)}$ *is cyclic over* Λ_1.

(i)$\Rightarrow$(ii): Under the Vandiver conjecture for $(l-i)$-part, $\mathrm{Im}\,\boldsymbol{g}^{(i)}=\mathcal{CV}^{(i)}$ by Theorem C, and $\boldsymbol{g}^{(i)}$ is injective by [6, §3.2 Corollary]. Hence, $\mathfrak{G}^{(i)}\simeq\mathcal{CV}^{(i)}$. Therefore, since $\mathcal{CV}^{(i)}$ is free and cyclic over Λ_1, so is $\mathfrak{G}^{(i)}$.

(ii)$\Rightarrow$(i): Since $\mathrm{Ker}\,\boldsymbol{g}^{(i)}=\mathrm{Tor}_{\Lambda_1}\mathfrak{G}^{(i)}$ (cf. [5, §3.1]), we see from the assumption that $\boldsymbol{g}^{(i)}$ is injective and $g_i=1$. So, by Prop. 1, $\mathcal{V}^{(i)}/(\mathrm{Im}\,\boldsymbol{g}^{(i)})$ is finite. Since $\mathfrak{G}^{(i)}$ is cyclic, $\mathrm{Im}\,\boldsymbol{g}^{(i)}=\alpha\cdot\mathcal{V}^{(i)}$ for some $\alpha\in\Lambda_1$. By the finiteness of $\mathcal{V}^{(i)}/(\mathrm{Im}\,\boldsymbol{g}^{(i)})$, we see that α is a unit of Λ_1. Therefore, $\mathcal{V}^{(i)}=\mathrm{Im}\,\boldsymbol{g}^{(i)}$. Hence, by Theorem C, the Vandiver conjecture for $(l-i)$-part is valid.

(ii)$\Rightarrow$(iii): Obvious.

(iii)$\Rightarrow$(ii): Assume that $\mathfrak{G}^{(i)}$ is cyclic over Λ_1. Then, since the free part $\mathfrak{H}^{(i)}$ of $\mathfrak{G}^{(i)}$ is pseudo-isomorphic to Λ_1, $\mathfrak{G}^{(i)}$ must be isomorphic to Λ_1.

References

[1] G. W. Anderson: The hyperadelic gamma function. Inv. Math., **95**, 63–131 (1989).

[2] R. Coleman: Local units modulo circular units. Proc. AMS., **89**, 1–7 (1983).

[3] ——: Anderson-Ihara theory, Gauss sums and circular units. Adv. St. in Pure Math., **17**, 55–72 (1989).

[4] B. Ferrero and L. C. Washington: The Iwasawa invariant μ_p vanishes for abelian number fields. Ann. of Math., **109**, 377–395 (1979).

[5] H. Ichimura and M. Kaneko: On the universal power series for Jacobi sums and the Vandiver conjecture. J. Number Theory, **31**, 312–334 (1989).

[6] H. Ichimura and K. Sakaguchi: The non-vanishing of a certain Kummer character χ_m (after Soulé), and some related topics. Adv. St. in Pure Math., **12**, 53–64 (1987).

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

[8] Y. Ihara, M. Kaneko, and A. Yukinari: On some properties of the universal power series for Jacobi sums. Adv. St. in Pure Math., **12**, 65–86 (1987).

[9] L. C. Washington: Introduction to Cyclotomic Fields. Springer-Verlag, New York (1982).