Math. J. Okayama Univ. **65** (2023), 117–123

A NOTE ON FIELDS GENERATED BY JACOBI SUMS

Yuichiro Hoshi

Abstract. In the present paper, we study fields generated by Jacobi sums. In particular, we completely determine the field obtained by adjoining, to the field of rational numbers, all of the Jacobi sums "of two variables" with respect to a fixed maximal ideal of the ring of integers of a fixed prime-power cyclotomic field.

Introduction

Throughout the present paper, let us fix

- a prime number l,
- a positive integer N, and
- a maximal ideal $\mathfrak{p}$ of the ring $\mathfrak{o}$ of integers of the finite Galois extension K of $\mathbb{Q}$ obtained by adjoining to $\mathbb{Q}$ a primitive l^N-th root of unity.

Write $G \overset{\text{def}}{=} \mathrm{Gal}(K/\mathbb{Q})$ for the Galois group of the finite Galois extension $K/\mathbb{Q}$, $D \subseteq G$ for the decomposition subgroup associated to $\mathfrak{p}$, $\kappa(\mathfrak{p}) \overset{\text{def}}{=} \mathfrak{o}/\mathfrak{p}$ for the residue field at $\mathfrak{p}$, and p for the characteristic of $\kappa(\mathfrak{p})$. Suppose that $p \neq l$. Write, moreover, $\chi\colon \kappa(\mathfrak{p})^\times \to \boldsymbol{\mu}_{l^N}(K) \subseteq K^\times$ for the homomorphism determined by the l^N-th power residue symbol at $\mathfrak{p}$. Following [6], for each positive integer n and each element $a = (a_1, \ldots, a_n)$ of $\mathbb{Z}^n$, let us define the *Jacobi sum* associated to $a \in \mathbb{Z}^n$ as follows [cf. [6], (I)]:

$$\mathbf{j}_a \overset{\text{def}}{=} (-1)^{n+1} \sum_{\substack{(x_1,\ldots,x_n)\in(\kappa(\mathfrak{p})^\times)^n \\ \sum_j x_j = -1}} \prod_{i=1}^{n} \chi(x_i)^{a_i} \in \mathfrak{o}.$$

In the present paper, we discuss intermediate extensions of the finite Galois extension $K/\mathbb{Q}$ obtained by adjoining to $\mathbb{Q}$ Jacobi sums. Let us recall that *T. Ono*, *M. Kida*, and *A. Gyoja* [cf. [2], [3], [5]] and *N. Aoki* [cf. [1]] have studied these intermediate extensions. Note that we have an equality $\mathbb{Q}(\mathbf{j}_b;\, b \in \mathbb{Z}^2) = \mathbb{Q}(\mathbf{j}_c;\, c \in \mathbb{Z}^m, m \geq 1)$ [cf. Proposition 2.1, (ii)].

The main result of the present paper is as follows:

Theorem A. *The following assertions hold:*

(i) *If K^D is totally real, then $\mathbb{Q}(\mathbf{j}_a;\, a \in \mathbb{Z}^2) = \mathbb{Q}$.*

Mathematics Subject Classification. 11L05, 11R18.
Key words and phrases. Jacobi sum.

(ii) *If K^D is not totally real, then* $\mathbb{Q}(\mathbf{j}_a;\, a \in \mathbb{Z}^2) = K^D$.

Note that one verifies easily that Theorem A in the case where l is odd, and $N = 1$ [i.e., in the "odd prime cyclotomic field case"] may also be derived from [2], Theorem 2, together with a similar argument to the argument applied in the proof of Theorem A. The author of the present paper will apply Theorem A to the study of *geometrically pro-l anabelian geometry for tripods over finite fields*. Then this "known" result [i.e., Theorem A in the "odd prime cyclotomic field case"] is *not sufficient* for this application. Moreover, Theorem A could not be found in literature. This is one main motivation of the study of the "prime-power cyclotomic field case" in the present paper.

1. Some Lemmas

We shall write $\Lambda \overset{\text{def}}{=} \mathbb{Z}/l^N\mathbb{Z}$. Moreover, for each $t \in \Lambda^\times$, we shall write $\sigma_t \in G$ for the unique element which induces the t-th power map on the subgroup $\boldsymbol{\mu}_{l^N}(K) \subseteq K^\times$. Then one verifies easily that the assignment "$t \mapsto \sigma_t$" determines an isomorphism $\Lambda^\times \overset{\sim}{\to} G$ of groups. Moreover, one also verifies easily that the subgroup $D \subseteq G$ coincides with the subgroup $\langle \sigma_p \rangle \subseteq G$ generated by σ_p, i.e., corresponds, via the isomorphism $\Lambda^\times \overset{\sim}{\to} G$, to the subgroup of $\Lambda^\times$ generated by the image of p in $\Lambda^\times$.

Definition 1.1. Let m be a positive integer. Then we shall write $\mathcal{L}[m] \subseteq \mathbb{Z}$ for the set of integers $\widetilde{t}$ such that the inequalities $0 < \widetilde{t} < m$ hold, and, moreover, the integer $\widetilde{t}$ is prime to m.

Remark. Observe that one verifies easily that, in the situation of Definition 1.1, the natural surjective map $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/m\mathbb{Z}$ restricts to a bijective map $\mathcal{L}[m] \overset{\sim}{\to} (\mathbb{Z}/m\mathbb{Z})^\times$.

Lemma 1.2. *The following assertions hold:*

(i) *Let m be a positive integer, $\widetilde{t}$ an element of $\mathcal{L}[m]$, r a positive integer, and d an element of $\{0, 1\}$. For a rational number $s \in \mathbb{Q}$, write $[s]$ for the "integral part" of s [i.e., the largest integer which is less than or equal to s] and $\langle s \rangle \overset{\text{def}}{=} s - [s]$ for the "fractional part" of s. Then*

$$\left[(rm + d)\left\langle \frac{\widetilde{t}}{m} \right\rangle\right] = r\widetilde{t}.$$

(ii) *Let N_0 be a positive integer such that $N_0 \leq N$. For each positive integer r, write $r + \mathcal{L}[l^{N_0}] \subseteq \mathbb{Z}$ for the set of integers $\widetilde{t}$ such that*

$\widetilde{t} - r \in \mathcal{L}[l^{N_0}]$. *Then*

$$\mathcal{L}[l^N] = \bigsqcup_{i=0}^{l^{N-N_0}-1} (il^{N_0} + \mathcal{L}[l^{N_0}]).$$

Proof. These assertions are immediate. □

Lemma 1.3. *Let* $\rho\colon \Lambda^\times \to \mathbb{C}^\times$ *be an odd Dirichlet character. Then*

$$\sum_{\widetilde{t} \in \mathcal{L}[l^N]} \widetilde{t} \cdot \rho(t) \neq 0$$

— where, for each $\widetilde{t} \in \mathcal{L}[l^N]$*, we write* $t \in \Lambda^\times$ *for the image of* $\widetilde{t}$ *in* Λ [*cf. Remark following Definition* 1.1].

Proof. Write

$$N_0 \overset{\text{def}}{=} \min\{\, i \in \{1, 2, \dots, N\} \mid 1 + l^i\Lambda \subseteq \mathrm{Ker}(\rho)\,\}$$

and $\Lambda_0 \overset{\text{def}}{=} \mathbb{Z}/l^{N_0}\mathbb{Z}$. Then one verifies easily that the *odd*, hence also *nontrivial*, Dirichlet character $\rho\colon \Lambda^\times \to \mathbb{C}^\times$ factors as the composite of the natural surjective homomorphism $\Lambda^\times \twoheadrightarrow \Lambda_0^\times$ and a *primitive odd* Dirichlet character $\rho_0\colon \Lambda_0^\times \to \mathbb{C}^\times$. Now let us observe that since ρ_0 is *odd*, hence also *nontrivial*, it follows that, for each integer i such that $0 \leq i \leq l^{N-N_0} - 1$,

$$\sum_{\widetilde{t} \in \mathcal{L}[l^{N_0}]} (il^{N_0} + \widetilde{t}) \cdot \rho(t) = il^{N_0} \cdot \sum_{t \in \Lambda_0^\times} \rho_0(\underline{t}) + \sum_{\widetilde{t} \in \mathcal{L}[l^{N_0}]} \widetilde{t} \cdot \rho_0(\underline{t}) = \sum_{\widetilde{t} \in \mathcal{L}[l^{N_0}]} \widetilde{t} \cdot \rho_0(\underline{t})$$

— where, for each $\widetilde{t} \in \mathcal{L}[l^{N_0}]$, we write $\underline{t} \in \Lambda_0^\times$ for the image of $\widetilde{t}$ in Λ_0 [cf. Remark following Definition 1.1]. Thus, it follows immediately from Lemma 1.2, (ii), that

$$\sum_{\widetilde{t} \in \mathcal{L}[l^N]} \widetilde{t} \cdot \rho(t) = l^{N-N_0} \cdot \sum_{\widetilde{t} \in \mathcal{L}[l^{N_0}]} \widetilde{t} \cdot \rho_0(\underline{t}).$$

In particular, to verify Lemma 1.3, we may assume without loss of generality, by replacing "(N, ρ)" by (N_0, ρ_0), that ρ_0 is *primitive*. On the other hand, if ρ_0 is *primitive*, then Lemma 1.3 is well-known [cf., e.g., [4], Chapter VII, §2, Exercise 4]. This completes the proof of Lemma 1.3. □

Lemma 1.4. *The following assertions hold:*

(i) *Let* T *be a group of order* 2, C *a cyclic* 2*-group, and* H *a subgroup of* $T \times C$ *that does not contain the subgroup* $T \times \{1\}$*. Then there exist not necessarily distinct two subgroups* H_1, H_2 *of* $T \times C$ *such that*

- *$T \times \{1\} \not\subseteq H_1$, $T \times \{1\} \not\subseteq H_2$*
- *both $(T \times C)/H_1$ and $(T \times C)/H_2$ are cyclic, and, moreover,*
- *$H = H_1 \cap H_2$.*

(ii) *Suppose that K^D is not totally real. Then there exist not necessarily distinct two odd Dirichlet characters ρ_1, $\rho_2 \colon \Lambda^\times \to \mathbb{C}^\times$ such that the intersection $\mathrm{Ker}(\rho_1) \cap \mathrm{Ker}(\rho_2)$ coincides with the subgroup of $\Lambda^\times$ generated by the image of p in $\Lambda^\times$.*

Proof. First, we verify assertion (i). If the quotient of $T \times C$ by H is *cyclic*, then the subgroups $H_1 \overset{\mathrm{def}}{=} H$, $H_2 \overset{\mathrm{def}}{=} H$ satisfy the desired condition in the statement of assertion (i). Thus, to verify assertion (i), we may assume without loss of generality that the quotient of $T \times C$ by H is *not cyclic*, which implies that there exists an element c_0 of the group C *of order* 2. In particular, to verify assertion (i), we may assume without loss of generality — by replacing "T", "C" by the respective images of T, C in $(T \times C)/H$ — that $H = \{1\}$. Then if one writes $t_0 \in T$ for the unique *nontrivial* element of T and $H_1 \subseteq T \times C$ for the subgroup of $T \times C$ generated by (t_0, c_0), then one verifies easily that the subgroups H_1, $H_2 \overset{\mathrm{def}}{=} \{1\} \times C$ satisfy the desired condition in the statement of assertion (i). This completes the proof of assertion (i).

Next, we verify assertion (ii). If l is *odd*, then since $\Lambda^\times$ is *cyclic*, assertion (ii) is immediate. If $l = 2$, then assertion (ii) follows immediately from assertion (i). This completes the proof of assertion (ii), hence also of Lemma 1.4. □

2. Proof

It seems to the author that the three assertions discussed in Proposition 2.1 below are likely to be well-known. However, the author decided to give proofs of these assertions here for the sake of the reader and the sake of completeness.

Proposition 2.1. *Let n be a positive integer and $a = (a_1, \ldots, a_n)$ an element of $\mathbb{Z}^n$. Then the following assertions hold:*

(i) *The inclusion $\mathbf{j}_a \in K^D$ holds.*

(ii) *The inclusion $\mathbf{j}_a \in \mathbb{Q}(\mathbf{j}_b;\, b \in \mathbb{Z}^2)$ holds.*

(iii) *Suppose that K^D is totally real. Then the inclusion $\mathbf{j}_a \in \mathbb{Q}$ holds.*

Proof. First, we verify assertion (i). Let us first observe that it is immediate that the homomorphism $\chi \colon \kappa(\mathfrak{p})^\times \to \boldsymbol{\mu}_{l^N}(K) \subseteq K^\times$ is *D-equivariant*, i.e., relative to the respective natural actions of D on $\kappa(\mathfrak{p})^\times$ and $K^\times$. Thus, assertion (i) follows immediately from the definition of the Jacobi sum $\mathbf{j}_a$. This completes the proof of assertion (i).

Next, we verify assertion (ii). Let us recall from the first and second displays of [6], p.492, that if $n \geq 3$, and $a_1+a_2 \in l^N\mathbb{Z}$ (respectively, $a_1+a_2 \notin l^N\mathbb{Z}$), then

$$\mathsf{j}_a = \mathsf{j}_{(a_2)} \cdot \mathsf{j}_{(a_3,\dots,a_n)} \cdot \#\kappa(\mathfrak{p})$$

$$(\text{respectively, } \mathsf{j}_a = \mathsf{j}_{(a_1+a_2)} \cdot \mathsf{j}_{(a_1,a_2)} \cdot \mathsf{j}_{(a_1+a_2,a_3,\dots,a_n)}).$$

Thus, assertion (ii) follows immediately from the easily verified fact that the Jacobi sum in the case where $n = 1$ is *contained* in $\{\pm 1\}$. This completes the proof of assertion (ii).

Finally, we verify assertion (iii). Let us first observe that one verifies easily that either $l^N = 2$ or $\#D \in 2\mathbb{Z}$. If $l^N = 2$, which implies that $\mathbb{Q} = K$, then assertion (iii) is immediate. Suppose that $\#D \in 2\mathbb{Z}$, which implies that $\#\kappa(\mathfrak{p})$ is the square of a rational number. If $\{a_1, \dots, a_n\} \subseteq l^N\mathbb{Z}$, then it follows from the equality

$$\mathsf{j}_a = \#\kappa(\mathfrak{p})^{-1} \cdot \Big(1 - \big(1 - \#\kappa(\mathfrak{p})\big)^n\Big)$$

of [6], (2), that assertion (iii) holds. Suppose that $\{a_1, \dots, a_n\} \not\subseteq l^N\mathbb{Z}$. Then since $\#\kappa(\mathfrak{p})$ is the square of a rational number as mentioned above, and $\mathsf{j}_a \in K^D$ [cf. assertion (i)], which implies that j_a is a real number, it follows from the equality

$$|\mathsf{j}_a|^2 = \#\kappa(\mathfrak{p})^{s-2}$$

— where we write $a_{n+1} \overset{\text{def}}{=} \sum_{i=1}^{n} a_i$ and $s \overset{\text{def}}{=} \#\{\, i \in \{1, \dots, n+1\} \mid a_i \in l^N\mathbb{Z} \,\}$ — of [6], (10), that assertion (iii) holds. This completes the proof of assertion (iii), hence also of Proposition 2.1. □

Definition 2.2. Let n be a positive integer and a an element of $\mathbb{Z}^n$. Then we shall write $\underline{\mathbb{Q}(\mathsf{j}_a)}$ for the intermediate extension of the finite Galois extension $K/\mathbb{Q}$ that corresponds to the subgroup of G consisting of the elements whose actions on $\mathfrak{o}$ preserve the principal ideal of $\mathfrak{o}$ generated by $\mathsf{j}_a \in \mathfrak{o}$.

Remark. Observe that it follows immediately from Proposition 2.1, (i), (ii), together with the various definitions involved, that, in the situation of Definition 2.2, we have inclusions

$$\mathbb{Q} \subseteq \underline{\mathbb{Q}(\mathsf{j}_a)} \subseteq \mathbb{Q}(\mathsf{j}_a) \subseteq \mathbb{Q}(\mathsf{j}_b;\, b \in \mathbb{Z}^2) \subseteq K^D \subseteq K.$$

Definition 2.3. Let n be a positive integer. Then we shall write $(1^{[n]}) \in \mathbb{Z}^n$ for the element of $\mathbb{Z}^n$ each of whose n components is given by $1 \in \mathbb{Z}$.

Lemma 2.4. *Suppose that K^D is not totally real. Let r be a positive integer and d an element of $\{0, 1\}$. Then $\underline{\mathbb{Q}(\mathsf{j}_{(1^{[rl^N+d]})})} = \mathbb{Q}(\mathsf{j}_{(1^{[rl^N+d]})}) = K^D$.*

Proof. Let us first observe that it follows from the displayed inclusions of Remark following Definition 2.2 that, to verify Lemma 2.4, it suffices to verify the inclusion $K^D \subseteq \mathbb{Q}(\underline{\mathbf{j}_{(1^{[rl^N+d]})}})$. Next, let us also observe that it follows immediately from [6], (8), that the assignment "$\mathfrak{p} \mapsto \mathbf{j}_{(1^{[rl^N+d]})}$" is a *function of type (S)* in the sense of [5], §1, i.e., in the case where we take the "(k, K)" of [5], §1, to be $(\mathbb{Q}, K)$; moreover, it follows from [6], (9), together with Lemma 1.2, (i), that the "ω" of [5], §1, for this function of type (S) is given by

$$\sum_{\widetilde{t} \in \mathcal{L}[l^N]} r\widetilde{t} \cdot \sigma_{-t}^{-1}$$

— where, for each $\widetilde{t} \in \mathcal{L}[l^N]$, we write $t \in \Lambda^\times$ for the image of $\widetilde{t}$ in Λ [cf. Remark following Definition 1.1]. In particular, it follows from [5], (2.4), that, for each $\sigma \in G$, this element σ is *contained* in the subgroup $\mathrm{Gal}(K/\mathbb{Q}(\underline{\mathbf{j}_{(1^{[rl^N+d]})}})) \subseteq G$ if and only if this element $\sigma \in G \xrightarrow{\sim} \Lambda^\times$ is *contained* in the kernel of every Dirichlet character $\rho\colon \Lambda^\times \to \mathbb{C}^\times$ such that ρ maps the image of p in $\Lambda^\times$ to $1 \in \mathbb{C}^\times$, and, moreover,

$$\sum_{\widetilde{t} \in \mathcal{L}[l^N]} \widetilde{t} \cdot \rho(t) \neq 0.$$

Thus, the desired inclusion $K^D \subseteq \mathbb{Q}(\underline{\mathbf{j}_{(1^{[rl^N+d]})}})$ follows immediately from Lemma 1.3 and Lemma 1.4, (ii). This completes the proof of Lemma 2.4. □

Remark. Note that [2], Theorem 2, may be regarded as Lemma 2.4 in the case where l is odd, and the equality $(N, r, d) = (1, 1, 1)$ holds. Moreover, Lemma 2.4 in the case where l is odd, and the equality $(N, r, d) = (1, 1, 1)$ holds may also be derived from [1], Lemma 6.2 [cf. also [1], Remark 6.6]. On the other hand, no result that claims explicitly the two equalities in the statement of Lemma 2.4 in the case where $N > 1$ [i.e., the "prime-power cyclotomic field case"] could be found in literature. Here, let us recall that one may find [1], Theorem 0.4, that establishes a concrete description of the field $\mathbb{Q}(\mathbf{j}_a)$ in the "prime-power cyclotomic field case" [cf. also some results proved in [1], §7].

Proof of Theorem A. Assertion (i) follows from Proposition 2.1, (iii). Next, we verify assertion (ii). Let us first observe that it follows from Lemma 2.4 that $\mathbb{Q}(\mathbf{j}_{(1^{[l^N]})}) = K^D$. Thus, assertion (ii) follows from the displayed inclusions of Remark following Definition 2.2. This completes the proof of Theorem A. □

Acknowledgements

The author would like to thank *A. Tamagawa* for explaining an argument concerning the topic discussed in the present paper. This discussion is one main motivation of the study of the present paper. The author also would like to thank the *referee* for some helpful comments. This research was supported by JSPS KAKENHI Grant Number 21K03162 and by the Research Institute for Mathematical Sciences, an International Joint Usage/Research Center located in Kyoto University.

References

[1] N. Aoki: Abelian fields generated by a Jacobi sum. *Comment. Math. Univ. St. Paul.* **45** (1996), no. **1**, 1–21.

[2] A. Gyoja and T. Ono: A note on Jacobi sums. II. *Proc. Japan Acad. Ser. A Math. Sci.* **69** (1993), no. **4**, 91–93.

[3] M. Kida and T. Ono: A note on Jacobi sums. *Proc. Japan Acad. Ser. A Math. Sci.* **69** (1993), no. **2**, 32–34.

[4] J. Neukirch: *Algebraic number theory.* Grundlehren der Mathematischen Wissenschaften, **322**. Springer-Verlag, Berlin, 1999.

[5] T. Ono: A note on Jacobi sums. III. *Proc. Japan Acad. Ser. A Math. Sci.* **69** (1993), no. **7**, 272–274.

[6] A. Weil: Jacobi sums as "Grössencharaktere". *Trans. Amer. Math. Soc.* **73**, (1952). 487–495.

Yuichiro Hoshi
Research Institute for Mathematical Sciences
Kyoto University
Kyoto, 606-8502, Japan
e-mail address: yuichiro@kurims.kyoto-u.ac.jp

(*Received November 24, 2021*)
(*Accepted March 29, 2022*)