22. *A Note on Jacobi Sums. II*

By Akihiko GYOJA[*)] and Takashi ONO[**)]

(Communicated by Shokichi IYANAGA, M. J. A., April 12, 1993)

This is a continuation of [1] which will be referred to as (I). In this paper, we follow notation and conventions of (I) with one exception; our definition of the Jacobi sum (1,1) is that of Weil [2] which differs from that in (I) only by a factor ± 1.

§ 1. Statement of results. For a prime $l \neq 2$, let $k = k_l = \boldsymbol{Q}(\zeta)$, $\zeta = e^{2\pi i/l}$, the l th cyclotomic field. For a prime ideal $\mathfrak{p}$ of k with $\mathfrak{p} \nmid l$, let $\chi_{\mathfrak{p}}(x) = (x/\mathfrak{p})_l$, the l th power residue symbol in k. Following [2], we put

(1.1) $$J(\mathfrak{p}) = J_{l+1}(\mathfrak{p}) = -\sum \chi_{\mathfrak{p}}(x_1) \cdots \chi_{\mathfrak{p}}(x_{l+1}),$$

where $x_1 + \cdots + x_{l+1} = -1$ and $x_i \in \boldsymbol{Z}[\zeta]/\mathfrak{p}$. Note that

(1.2) $$J(\mathfrak{p}) = g(\mathfrak{p})^l,$$

where $g(\mathfrak{p})$ is the Gauss sum. As usual, we denote by p, q, f, g the integers such that $N\mathfrak{p} = q = p^f$, $l - 1 = fg$.

Consider three subgroups of the Galois group $G(k/\boldsymbol{Q})$:

(1.3) $$G(J(\mathfrak{p})) = \{\sigma \in G(k/\boldsymbol{Q})\,;\, J(\mathfrak{p})^\sigma = J(\mathfrak{p})\},$$

(1.4) $$G^*(J(\mathfrak{p})) = \{\sigma \in G(k/\boldsymbol{Q})\,;\, (J(\mathfrak{p}))^\sigma = (J(\mathfrak{p}))\},$$

(1.5) $$Z(\mathfrak{p}) = \{\sigma \in G(k/\boldsymbol{Q})\,;\, \mathfrak{p}^\sigma = \mathfrak{p}\},$$

where (1.5) is the decomposition group of $\mathfrak{p}$ whose order is f. One sees easily that

(1.6) $$Z(\mathfrak{p}) \subset G(J(\mathfrak{p})) \subset G^*(J(\mathfrak{p})).$$

As in (I) we are interested in the subfield $\boldsymbol{Q}(J(\mathfrak{p}))$ of k, i.e., the fixed field of the group $G(J(\mathfrak{p}))$. We prove the following

Theorem 1. *If f is even, then $G(J(\mathfrak{p})) = G(k/\boldsymbol{Q})$. In other words, $J(\mathfrak{p}) \in \boldsymbol{Q}$.*

Theorem 2. *If f is odd, then $G^*(J(\mathfrak{p})) = G(J(\mathfrak{p})) = Z(\mathfrak{p})$. Especially, $\boldsymbol{Q}(J(\mathfrak{p}))$ is the decomposition field of $\mathfrak{p}$.*

Remark. In case $f = 1$, we proved a general result without appealing to Stickelberger's theorem (see (I)). This paper is logically independent of (I).

§ 2. Proof of Theorem 1. Denote by k^+ the maximal real subfield of $k = k_l$. Call σ_t, $l \nmid t$, the element of $G(k/\boldsymbol{Q})$ defined by $\zeta^{\sigma_t} = \zeta^t$. Hence σ_{-1} is the generator of $G(k/k^+)$, i.e., the restriction of the complex conjugation. If f is even, then $\sigma_{-1} \in Z(\mathfrak{p})$, for $G(k/\boldsymbol{Q})$ is cyclic. Hence $\sigma_{-1} \in G(J(\mathfrak{p}))$ by (1.6); so $J(\mathfrak{p}) \in k^+$ and, by (1.2), $J(\mathfrak{p})^2 = |J(\mathfrak{p})|^2 = q^l = p^{fl}$, or $J(\mathfrak{p}) = \pm p^{1/2fl} \in \boldsymbol{Q}$. Q.E.D.

Remark. Actually we have

(2.1) $$J(\mathfrak{p}) \in k^+ \Leftrightarrow f \text{ is even} \Leftrightarrow J(\mathfrak{p}) \in \boldsymbol{Q}.$$

---

*) Department of Fundamental Sciences, Faculty of Integrated Human Studies, Kyoto University.

**) Department of Mathematics, The Johns Hopkins University.

For (2.1), we have only to verify "$J(\mathfrak{p}) \in k^+ \Rightarrow f$: even." So suppose f is odd. If $J(\mathfrak{p})$ were real, then $J(\mathfrak{p})^2 = |J(\mathfrak{p})|^2 = p^{fl} = p^{1+2h}$; so $J(\mathfrak{p}) = \pm \sqrt{p}\, p^h$. Hence $\boldsymbol{Q}(J(\mathfrak{p})) = \boldsymbol{Q}(\sqrt{p})$. Since only quadratic field in k is $\boldsymbol{Q}(\sqrt{l^*})$, $l^* = (-1)^{1/2(l-1)} l$, we must have $\boldsymbol{Q}(\sqrt{p}) = Q(\sqrt{l^*})$ which contradicts $l \neq p$.

§ 3. Proof of Theorem 2. For an integer $m \geqq 1$ and $x \in \boldsymbol{Z}/m\boldsymbol{Z}$, we shall denote by $\mathrm{res}_m(x)$ the remainder of the division of x by m. Applying the prime decomposition of $J(\mathfrak{p})$ due to Stickelberger (see [2] formula (5), (8), pp. 489-490), we obtain

(3.1) $$(J(\mathfrak{p})) = \mathfrak{p}^{\omega},\ \omega \in \boldsymbol{Z}[G(k/\boldsymbol{Q})],\ \text{where}$$

(3.2) $$\omega = \sum_{t \in F_l^\times} \mathrm{res}_l\,(t)\, \sigma_{t^*}, \quad t^* = -t^{-1}.$$

For $s \in F_l^\times$, we have

(3.3) $$\sigma_s\, \omega = \sum_t \mathrm{res}_l\,(t)\, \sigma_{st^*} = \sum_t \mathrm{res}_l(st)\sigma_{t^*}.$$

Hence, we have

(3.4) $$\sigma_s \in G^*(J(\mathfrak{p})) \Leftrightarrow \mathfrak{p}^{\sigma_s\omega} = \mathfrak{p}^{\omega}.$$

Since $(F_l^\times)^g \xrightarrow{\sim} Z(\mathfrak{p})$ by the map $t \mapsto \sigma_t$, it follows from (3.2) that

(3.5) $$\mathfrak{p}^{\omega} = \prod_{t \in F_l^\times/(F_l^\times)^g} (\mathfrak{p}^{\sigma_{t^*}})^{R(t)} \text{ with}$$

$$R(t) = \sum_{u \in (F_l^\times)^g} \mathrm{res}_l(tu).$$

We see from (3.3)-(3.5) that

(3.6) $$\sigma_s \in G^*(J(\mathfrak{p})) \Leftrightarrow \sum_u \mathrm{res}_l(stu) = \sum_u \mathrm{res}_l(tu),\ t \in F_l^\times.$$

Note that, in (3.6), we may consider s, t as elements of $F_l^\times/(F_l^\times)^g$ and σ_s as an element of $G^*(J(\mathfrak{p}))/Z(\mathfrak{p})$, for $J(\mathfrak{p}^\sigma) = J(\mathfrak{p})^\sigma$ for all $\sigma \in G(k/\boldsymbol{Q})$. Now, let w be a generator of the cyclic group $F_l^\times$. Passing to the additive group $\Gamma = \boldsymbol{Z}/g\boldsymbol{Z}$ by the correspondence $t = w^x$, $s = w^\xi$, x, $\xi \in \Gamma$, we can write the equality in (3.6) as

(3.7) $$S(x+\xi) = S(x) \quad \text{for all } x \in \Gamma,$$

with

(3.8) $$S(x) = \sum_{i=0}^{f-1} \mathrm{res}_l\,(w^{ig+x}).$$

We denote by P the subgroup of Γ defined by

(3.9) $$P = \{\xi \in \Gamma\ ;\ S(x+\xi) = S(x) \quad \text{for all } x \in \Gamma\}.$$

In view of (3.6), we have an isomorphism:

(3.10) $$P \simeq G^*(J(\mathfrak{p}))/Z(\mathfrak{p}).$$

By (1.6) and Theorem 1, we have $P \simeq G(k/Q)/Z(\mathfrak{p})$ if f is even; hence $P = \Gamma$, in this case.

We are now ready to prove Theorem 2. Let X be the totality of $\chi \in \mathrm{Hom}(F_l^\times, C^\times)$ such that $\chi^g = 1$. We shall naturally identify X with $\mathrm{Hom}(F_l^\times/(F_l^\times)^g, C^\times)$. Note that the matrix $(S(x-y))_{x,y\in\Gamma}$ is diagonalized by $(e^{2\pi i(xy)/g})_{x,y}$ and the set of its eigenvalues is

$$E = \{\sum_{x\in\Gamma} S(x)e^{2\pi i\xi x/g}\ ;\ \xi \in \Gamma\} = \{\sum_{x \in F_l^\times} \mathrm{res}_l(x)\chi(x)\ ;\ \chi \in X\}.$$

The members of E are $\sum_{x=1}^{l} \chi(x)x$, which are the values $L(1, \bar{\chi})$ of the Dirichlet L-functions up to some non-zero constants if $\chi(-1) = -1$, and so non-zero in these cases. Here $\bar{\chi}$ denotes the complex conjugate. (See [3] for properties of Dirichlet L-functions used here.) Since the order f of $(F_l^{\times})^g$ is odd by the assumption, -1 does not belong to $(F_l^{\times})^g$ and defines an element of $F_l^{\times}/(F_l^{\times})^g$ of order 2. Hence there are exactly $g/2$ elements $\chi \in X$ such that $\chi(-1) = -1$, and so the corresponding $g/2$ elements of E are non-zero. Moreover, the element of E corresponding to $\chi = 1$ is positive; hence E has at least $(g/2) + 1$ non-zero elements. In other words, we have rank $(S(x + \xi))_{x,\xi \in \Gamma} \geq (g/2) + 1$. If $P \neq \{0\}$, then this rank is at most $g/2$. Hence $P = \{0\}$, and the assertion of the theorem follows from (1.6) and (3.10).

Acknowledgement. This work was done during the first author's stay in The Johns Hopkins University. He would like to express his hearty thanks to the warm hospitality of the staff of JHU.

References

[1] Kida, M., and Ono, T.: A note on Jacobi sums. Proc. Japan Acad., **69**A, 32–34 (1993).

[2] Weil, A.: Jacobi sums as "Grössencharactere." Trans. Am. Math. Soc., **73** VI, 487–495 (1952).

[3] Borevich, Z. I., and Shafarevich, I. R.: Number Theory. Academic Press, New York (1966).