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.