9. *A Note on Jacobi Sums*

By Masanari KIDA and Takashi ONO

Department of Mathematics, The Johns Hopkins University, U.S.A

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

Introduction. Let p be an odd prime, $\boldsymbol{F}_p$ be the finite field with p elements and χ be a character of order l of the multiplicative group $\boldsymbol{F}_p^\times$. Consider a Jacobi sum

$$J = \sum_{x \in \boldsymbol{F}_p} \chi(x)\chi(1-x), \quad \chi(0) = 0.$$

Obviously J is an integer in the lth cyclotomic fieid k_l. By machine computation, the older author observed that $\boldsymbol{Q}(J) = k_l$ for small p and l. In this paper, we shall prove a theorem which explains (more than enough) the observation.

§1. The group $G(\mathfrak{p})$**.** For a positive integer m, let ζ_m be a primitive mth root of 1, $k_m = \boldsymbol{Q}(\zeta_m)$ and $\mathfrak{o}_m = \boldsymbol{Z}[\zeta_m]$. For a prime ideal $\mathfrak{p}$ of $\mathfrak{o}_m$ such that $\mathfrak{p} \nmid m$, let $\chi_\mathfrak{p}(x) = (x/\mathfrak{p})_m$, the mth power residue symbol, $x \in \mathfrak{o}_m$, $\mathfrak{p} \nmid x$, i.e., $\chi_\mathfrak{p}(x \bmod \mathfrak{p})$ is the unique mth root of 1 such that

$$\chi_\mathfrak{p}(x \bmod \mathfrak{p}) \equiv x^{\frac{q-1}{m}}, \quad (\bmod\ \mathfrak{p}), \tag{1}$$

where $q = p^f = N\mathfrak{p}$ is the cardinality of $\mathfrak{o}_m/\mathfrak{p}$. One sees that $\chi_\mathfrak{p}$ is a character of $(\mathfrak{o}_m/\mathfrak{p})^\times$ of order m. We put $\chi_\mathfrak{p}(0) = 0$. As a nontrivial additive character of $\mathfrak{o}_m/\mathfrak{p} = \boldsymbol{F}_q$, we adopt the function $\psi_\mathfrak{p}(x) = \zeta_p T(x)$, where T is the trace map from $\boldsymbol{F}_q$ to $\boldsymbol{F}_p$.

Consider the Gauss sum

$$g(\mathfrak{p}) = \sum_{x \in \mathfrak{o}_m/\mathfrak{p}} \chi_\mathfrak{p}(x)\psi_\mathfrak{p}(x) \in \mathfrak{o}_{mp}. \tag{2}$$

Note that $k_{mp} = k_m k_p$, $k_m \cap k_p = \boldsymbol{Q}$; hence we can identify two Galois groups $G(k_m/\boldsymbol{Q})$ and $G(k_{mp}/k_p)$. For an integer t with $(t, m) = 1$, we denote by σ_t the element of $G(k_m/\boldsymbol{Q}) = G(k_{mp}/k_p)$ such that $\zeta_m^{\sigma_t} = \zeta_m^t$. We denote by μ_n the group of nth roots of 1. For a number field K, we denote by $\mu(K)$ group of roots of 1 in K. For the cyclotomic field $k_m = \boldsymbol{Q}(\mu_m)$, we know that $\mu(k_m) = \mu_m$ or μ_{2m} according as m is even or odd.

Consider the group

$$G(\mathfrak{p}) = \{\sigma_t \in G(k_m/\boldsymbol{Q})\ ;\ g(\mathfrak{p})^{1-\sigma_t} \in \mu(k_m)\}. \tag{3}$$

For $u \in \boldsymbol{F}_p$, put

$$A_u = \sum_{T(x)=u} \chi_\mathfrak{p}(x). \tag{4}$$

One sees easily that

$$A_u = \chi_\mathfrak{p}(u)A_1, \quad \text{for } u \neq 0. \tag{5}$$

From (2), (4), (5), we have

$$g(\mathfrak{p}) = \sum_{u \in \boldsymbol{F}_p} A_u \zeta_p^u = A_0 + A_1 \sum_{u \neq 0} \chi_\mathfrak{p}(u)\zeta_p^u. \tag{6}$$

Since $1 = -\sum_{u \neq 0} \zeta_p^u$, (6) implies that

$$g(\mathfrak{p}) = \sum_{u \neq 0} (\chi_{\mathfrak{p}}(u) A_1 - A_0)\, \zeta_p^u. \tag{7}$$

Since $\{\zeta_p^u\}_{u \neq 0}$ is linearly independent over k_m, it follows from (3), (7) that

$$G(\mathfrak{p}) = \{\sigma_t \in G(k_m/\boldsymbol{Q})\ ;\ (\chi_{\mathfrak{p}}(u)A_1 - A_0)^{\sigma_t} = \alpha_t(\chi_{\mathfrak{p}}(u)A_1 - A_0),\ \alpha_t \in \mu(k_m) \text{ for all } u \in \boldsymbol{F}_p^{\times}\}. \tag{8}$$

If, in particular, $f = 1$, i.e., $q = p$, then $A_1 = 1$, $A_0 = 0$, and the condition (8) boils down to

$$\chi_{\mathfrak{p}}(u)^{\sigma_t} = \alpha_t\, \chi_{\mathfrak{p}}(u), \text{ for all } u \in \boldsymbol{F}_p^{\times}. \tag{9}$$

Putting $u = 1$ in (9), we get $\alpha_t = 1$, hence $\chi_{\mathfrak{p}}(u)^{\sigma_t} = \chi_{\mathfrak{p}}(u)^t = \chi_{\mathfrak{p}}(u)$ for all $u \in \boldsymbol{F}_p^{\times}$, i.e., $\sigma_t = 1$. Therefore we conclude that

$$G(\mathfrak{p}) = \{1\} \quad \text{if } f = 1. \tag{10}$$

§2. The Jacobi sum $J_n(\mathfrak{p})$. Notation being as in §1, assume that $m > 1$; hence $\chi_{\mathfrak{p}}$ is nontrivial. From (1) one sees that

$$\chi_{\mathfrak{p}^\sigma}(x^\sigma) = \chi_{\mathfrak{p}}(x)^\sigma, \quad \text{for all } \sigma \in G(k_m/\boldsymbol{Q}). \tag{11}$$

For a natural number n such that $(n, m) = 1$, we put

$$J_n(\mathfrak{p}) = g(\mathfrak{p})^n / g(\mathfrak{p})^{\sigma_n} = g(\mathfrak{p})^{n - \sigma_n}. \tag{12}$$

Notice that $J_n(\mathfrak{p})$ is a special case of the Jacobi sum of n variables

$$J_{(a_1,\dots,a_n)}(\mathfrak{p}) = \sum_{\substack{x_1+\dots+x_n=1 \\ x_i \in \mathfrak{o}_m/\mathfrak{p}}} \chi_{\mathfrak{p}}^{a_1}(x_1) \dots \chi_{\mathfrak{p}}^{a_n}(x_n), \tag{13}$$

where $a_i \in \boldsymbol{Z}$; the relation (12) is a consequence of

$$g_{a_1}(\mathfrak{p}) \cdots g_{a_n}(\mathfrak{p}) = J_{(a_1,\dots,a_n)}(\mathfrak{p})\, g_{a_1+\dots+a_n}(\mathfrak{p}), \tag{14}$$

which holds whenever a_i, $1 \leqq i \leqq n$, and $a_1 + \dots + a_n$ are all $\not\equiv 0 \pmod{m}$.[1] Needless to say, we have set in (14),

$$g_t(\mathfrak{p}) = \sum_{x \in \mathfrak{o}_m/\mathfrak{p}} \chi_{\mathfrak{p}}^t(x)\, \psi_{\mathfrak{p}}(x), \quad t \in \boldsymbol{Z}. \tag{15}$$

From (13) we see that $J_n(\mathfrak{p}) = J_{(1,\dots,1)}(\mathfrak{p})$ is in $\mathfrak{o}_m$. We are interested in the subfield $\boldsymbol{Q}(J_n(\mathfrak{p}))$ of k_m.

Proposition 1. *$\boldsymbol{Q}(J_n(p))$ is contained in the decomposition field of* $\mathfrak{p}$.

Proof. From (11), (13), it follows that $J_n(\mathfrak{p}^\sigma) = J_n(\mathfrak{p})^\sigma$ for any $\sigma \in G(k_m/\boldsymbol{Q})$. In particular, we have $J_n(\mathfrak{p}) = J_n(\mathfrak{p})^\sigma$ if $\mathfrak{p} = \mathfrak{p}^\sigma$. Q.E.D.

Proposition 2. *If $p \neq 2$ and $n \not\equiv 1 \pmod{p}$, then $\boldsymbol{Q}(J_n(\mathfrak{p}))$ contains the fixed field of the group $G(\mathfrak{p})$ defined by* (3).

Proof. Let $\sigma = \sigma_t$ be an element of $G(k_m/\boldsymbol{Q})$ such that $J_n(p)^\sigma = J_n(\mathfrak{p})$. Then we have $(g(\mathfrak{p})^{n-\sigma_n})^{\sigma_t} = g(\mathfrak{p})^{n-\sigma_n}$, so $g_t(\mathfrak{p})^{n-\sigma_n} = g(\mathfrak{p})^{n-\sigma_n}$, or

$$\alpha_t^n = \alpha_t^{\sigma_n} \quad \text{with } \alpha_t = g_t(p)/g(\mathfrak{p}). \tag{16}$$

Since $G(k_m/\boldsymbol{Q})$ is of order $\varphi(m)$, (16) implies that

$$\alpha_t^{n\varphi(m)} - \alpha_t = \alpha_t(\alpha_t^{n\varphi(m)-1} - 1) = 0. \tag{17}$$

Since $\alpha_t \neq 0$, (17) implies that $\alpha_t \in \mu(k_{mp})$. Hence we have $\alpha_t = \pm \zeta_m^i \zeta_p^j$, $i, j \in \boldsymbol{Z}$. In view of (16), we have $(\pm 1)^n \zeta_m^{ni} \zeta_p^{nj} = \pm \zeta_m^{ni} \zeta_p^j$, or $\zeta_p^{2nj} = \zeta_p^{2j}$. Since $p \neq 2$ and $n \not\equiv 1 \pmod{p}$, we have $j \equiv 0 \pmod{p}$, so $\alpha_t = \pm \zeta_m^i \in \mu(k_m)$; in other words, we have $g(\mathfrak{p})^{1-\sigma_t} \in \mu(k_m)$, i.e., $\sigma_t \in G(\mathfrak{p})$. Q.E.D.

---

[1] As for basic facts on Gauss sums and Jacobi sums, see, e.g., a beautifully written textbook [1].

The following Theorem follows from (10) and Propositions; it justifies the observation more than enough.

Theorem. *Let k_m, $m > 1$, be the mth cyclotomic field, p an odd prime, $p \nmid m$, n a positive integer such that $(n, m) = 1$ and $n \not\equiv 1 \pmod{p}$. Let $\mathfrak{p}$ be a prime ideal in k_m such that $\mathfrak{p} \mid p$. Let $J_n(\mathfrak{p})$ be the Jacobi sum defined by* (12) (*or by* (13) *with $a_i = 1$, $1 \leqq i \leqq n$). Then $k_m = \boldsymbol{Q}(J_n(\mathfrak{p}))$ if and only if p splits completely in k_m*, i.e., $p \equiv 1 \pmod{m}$.

Remark. Notation being as in Theorem, consider the group

(18) $$G(J_n(\mathfrak{p})) = \{\sigma \in G(k_m/\boldsymbol{Q})\ ;\ J_n(\mathfrak{p})^\sigma = J_n(\mathfrak{p})\}.$$

Proposition 1 means that

(19) $$G(J_n(\mathfrak{p})) \supseteqq Z(\mathfrak{p}),$$

where $Z(\mathfrak{p})$ is the decomposition group of $\mathfrak{p}$. On the other hand, Theorem means that

(20) $$G(J_n(\mathfrak{p})) = \{1\} \Leftrightarrow Z(\mathfrak{p}) = \{1\}.$$

Therefore we do not have yet a complete knowledge about the field $\boldsymbol{Q}(J_n(\mathfrak{p}))$ when $Z(\mathfrak{p}) \neq \{1\}$, i.e., when $f > 1$. Here is an illustrative example. Let $m = 5$. Hence $\varphi(m) = 4$ and only possible $f > 1$ are $f = 2$ and $f = 4$. If $f = 4$, then $Z(\mathfrak{p}) = G(J_n(\mathfrak{p})) = G(k_5/\boldsymbol{Q})$, no problem. If $f = 2$, the decomposition field of $\mathfrak{p}$ is $k_5{}^+$, the maximal real subfield of k_5. Since $J_n(\mathfrak{p})$ is contained in the decomposition field of $\mathfrak{p}$ by (19), we have $J_n(\mathfrak{p}) \in \boldsymbol{R}$. Now, since $J_n(\mathfrak{p})^2 = |J_n(\mathfrak{p})|^2 = (N\mathfrak{p})^{n-1} = p^{2(n-1)}$, we have $J_n(\mathfrak{p}) = \pm p^{n-1} \in \boldsymbol{Q}$; hence $G(J_n(\mathfrak{p})) = G(k_5/\boldsymbol{Q}) \neq Z(\mathfrak{p})$. Let $n = 6$ (with $m = 5$, still). Then $J_6(\mathfrak{p}) = g(\mathfrak{p})^{6-\sigma_6} = g(\mathfrak{p})^{6-\sigma_1} = g(\mathfrak{p})^5$. Hence $g(\mathfrak{p})^5 \in \boldsymbol{Q}$, but the decomposition field of $\mathfrak{p}$ is $k_5^+ \neq \boldsymbol{Q}$.[2)]

Reference

[1] Ireland, K., and Rosen, M.: A Classical Introduction to Modern Number Theory. 2nd ed., Springer-Verlag (1990).

2) This provides us with counterexample to Exercise 10, p.226 in [1].