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

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

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

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

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

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

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

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

One sees easily that

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

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

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

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