Math. J. Okayama Univ. 36(1994), 23–27

ON COMMUTATIVE GROUP ALGEBRAS. II

To the memory of Professor Hisao Tominaga

KAORU MOTOSE

In this paper, using commutative group algebras, we shall give an alternative proof of theorem about the prime decomposition of the Gauss sum which was essentially used in the proof of Stickelberger relation (see [1,2]). Moreover, in commutative group algebras, we shall obtain a formula for the evaluation of the quadratic Gauss sum.

Let $A = \boldsymbol{C}^F$ be the set of all mappings from a finite field $F = F_q$ of order q to the complex number field $\boldsymbol{C}$. Then we define the convolution product in A by the following

$$(f * g)(c) = \sum_{\substack{a,b \in F \\ a+b=c}} f(a)g(b)$$

for $f, g \in A$ and $c \in F$. This product together with the usual sum and the scalar product gives the structure of a commutative algebra. When there is no danger of confusion, we shall write fg instead of $f * g$.

Let $u = u_a$ be the characteristic function of $a \in F$, namely, u_a is defined by the following

$$u_a(a) = 1 \quad \text{and} \quad u_a(b) = 0 \quad \text{if } b \neq a.$$

Then we have the following equation.

$$u_a u_b = u_{a+b} \quad \text{and} \quad f = \sum_{a \in F} f(a)u_a \quad \text{for } f \in A.$$

Thus $\{u_a \mid a \in F\}$ forms a basis of the group algebra A of the additive group of F over $\boldsymbol{C}$.

We denote by $\widehat{F^*} = \mathrm{Hom}(F^*, \boldsymbol{C}^*)$ the set of all group homomorphisms from F^* to $\boldsymbol{C}^*$, by $\chi^{[n]}$ nth power of $\chi \in \widehat{F^*}$ with respect to the convolution product and by ϵ the trivial homomorphism from F^* to $\boldsymbol{C}^*$. We set $\epsilon(0) = 1$ and $\chi(0) = 0$ for $\chi \neq \epsilon \in \widehat{F^*}$.

1. The Stickelberger relation. Let m be a natural number, let p be a prime do not divide m, let f be the order of p mod m, and $q = p^f$.

Moreover let O be the ring of algebraic integers in $\boldsymbol{Q}(\zeta_{q-1})$ and let P be a prime ideal containing p, where ζ_{q-1} is a primitive $q-1$th root of 1. Then it is well known that q is the order of a finite field $F = O/P$.

We consider the Gauss sum $g_a = \sum_{\alpha \in F} \chi^a(\alpha)\zeta_p^{\mathrm{tr}(\alpha)}$ where χ is a generator of $\widehat{F^*}$ and $\mathrm{tr}(\alpha)$ is the trace of α. Let $\mathcal{P}$ be the ideal generated by P and $\{1-\zeta_p^k \mid 0 < k < p\}$ in the ring of algebraic integers $\mathcal{O}$ of $\boldsymbol{Q}(\zeta_{(q-1)p})$. It is easy to see $\mathcal{P}$ is the prime ideal generated by P and $1-\zeta_p$. We set $a^* = b_0 + b_1 + \cdots + b_{f-1}$ for a positive integer $a = b_0 + b_1 p + \cdots + b_{f-1}p^{f-1}$ where $0 < a < q$ and $0 \leq b_k < p$.

The next follows essentially from [3, Proposition 3.2] and this was used essentially for the Stickelberger relation (see [1,2]).

Theorem 1. $\mathrm{ord}_{\mathcal{P}}(g_a) = a^*$ *for* $0 < a < q$, *namely,* $\mathcal{P}^{a^*}$ *divides exactly* g_a.

Proof. Let ν be a natural homomorphism from O^F to $(O/P)^F$ and let $\mathcal{J}$ be the ideal generated by P and $\{u_0 - u_\alpha \mid \alpha \in F\}$. Since $\nu(\chi^c)^{[p]} = 0$ for $\chi^c \neq 1$, we obtain that $\nu(\chi^c)$ is contained in $\nu(\mathcal{J})$, the radical of the group algebra $(O/P)^F$, and so $\chi^c \in \mathcal{J}$. [2, Proposition 3.2] together with this implies that $\gamma\chi^a \in \mathcal{J}^{a^*}$ for the Jacobi sum $\gamma \in O \setminus P$. The character $u_\beta \to \zeta_p^{\mathrm{tr}(\beta)}$ induces the epimorphism $\phi: O^F \to \mathcal{O}$ with $\phi(\mathcal{J}) = \mathcal{P}$ and $\phi(\gamma\chi^a) = \gamma g_a$. Thus we have $\mathrm{ord}_{\mathcal{P}}(g_a) \geq a^*$. On the other hand, $\mathrm{ord}_{\mathcal{P}}(g_a) + \mathrm{ord}_{\mathcal{P}}(g_{q-1-a}) = f(p-1) = a^* + (q-1-a)^*$ follows from $\chi^a * \bar{\chi}^a = \chi^a(-1)(qu_0 - \epsilon)$ (see [4]) and $\mathrm{ord}_{\mathcal{P}}(p) = p-1$. This completes our proof.

Remark. [3, Proposition 3.3] shows that $\{\chi^a \mid a^* = k\}$ forms a basis of $\nu(\mathcal{J})^k/\nu(\mathcal{J})^{k+1}$ and so $\mathrm{ord}_{\mathcal{J}}(\chi^a) = a^*$, namely, a^* is the maximum integer s such that $\chi^a \in \mathcal{J}^s$.

2. Quadratic characters. In the remainder of this paper, we shall consider the quadratic character. The next is necessary for Theorem 4.

Proposition 2. *Let* η *be the element of order* 2 *in* $\widehat{F_q^*}$.

(1) $\det[u_{ab^{-1}}]_{a,b} = (\epsilon - u_0) * \prod_{\chi \neq \epsilon}^* \chi$ *where* $\prod^*$ *means the product of all nontrivial multiplicative characters with respect to the convolution product.*

(2) $\det[u_{ab}]_{a,b} = (-1)^{(q^2-1)/8} q^{(q-3)/2}\eta$ *where* q *is odd.*

Proof. (1) The matrix equation

$$[\chi(a)]_{\chi,a}[u_{ab^{-1}}]_{a,b}[\theta(b^{-1})]_{b,\theta} = \operatorname{diag}[(q-1)\sum_a \chi(a)u_a]$$

follows from the equation

$$\sum_{a,b}\chi(a)u_{ab^{-1}}\theta(b^{-1}) = \sum_b \Big(\sum_a \chi(ab^{-1})u_{ab^{-1}}\Big)\chi(b)\theta(b^{-1})$$
$$= \Big(\sum_b \chi(b)\theta(b^{-1})\Big)\sum_a \chi(a)u_a = \delta_{\chi,\theta}(q-1)\sum_a \chi(a)u_a$$

where $\chi, \theta \in \widehat{F_q^*}$ and a, b run over F_q^*. We obtain the formula (1) from the orthogonality relations.

(2) It is easy to see

$$\det[u_{ab^{-1}}]_{a,b} = (-1)^{\frac{q-3}{2}}\det[u_{ab}]_{a,b}$$

because the permutation $b \to b^{-1}$ on F_q^* is the product of cyclic permutations (b, b^{-1}), namely, $b \to b^{-1} = \prod_{b^2\neq 1}(b, b^{-1})$. The next equations show the formula (2). These follow from $\chi * \bar{\chi} = \chi(-1)(qu_0 - \epsilon)$ (see [4]).

$$(\epsilon - u_0) * \prod_{\chi\neq\epsilon}^{*}\chi = (\epsilon - u_0) * \eta * \prod_{\chi^2\neq\epsilon}^{*}\chi * \bar{\chi}$$
$$= -\eta * (qu_0 - \epsilon)^{\frac{q-3}{2}}\prod_{k=1}^{\frac{q-3}{2}}(-1)^k = -q^{\frac{q-3}{2}}(-1)^{\frac{(q-3)(q-1)}{8}}\eta.$$

3. Quadratic characters for odd primes. In the remainder of this paper, we assume q is an odd prime. First, We shall prove that

Lemma 3.

$$\prod_{n=1}^{q-1}(u_0 - u_1^n) = qu_0 - \epsilon.$$

Proof. Let $\sigma_1, \sigma_2, \ldots, \sigma_{q-1}$ be the elementary symmetric functions of $u_1, u_2 \ldots, u_{q-1}$, let $s_t = \sum_{a\in F_q^*} u_a^t$ and let $B = \sum_{k=0}^{q-1}(-1)^k\sigma_k$ where $\sigma_0 = u_0$. Then $\sigma_{q-1} = u_0$, $s_t = s_1 = \epsilon - u_0$ for all $1 \leq t < q$,

$$\prod_{n=1}^{q-1}(u_0 - u_1^n) = B, \quad \text{and} \quad B\epsilon = 0 \quad \text{from} \quad u_a\epsilon = \epsilon.$$

These equations together with Newton's formula

$$\sum_{k=0}^{q-2}(-1)^k s_{q-1-k}\sigma_k + (-1)^{q-1}(q-1)\sigma_{q-1} = 0$$

imply our formula.

The next is useful to the evaluation of the Gauss sum and to suggestions of the Stickelberger relation.

Theorem 4. *Let η be the element of order 2 in $\widehat{F_q^*}$. Then we have*
(1) $\eta = u_1^{(q^2-1)(q-1)/16}\prod_{n=1}^{(q-1)/2}(u_0 - u_1^n)$,
(2) $\eta = (-1)^{(q-1)/2}\prod_{n=1}^{(q-1)/2}(v^n - v^{-n})$, *where* $v = u_{(q+1)/2}$.

Proof. (2) follows from (1) and $v^2 = u_1$ as in the following.

$$\begin{aligned}\eta &= v^{\frac{(q^2-1)(q-1)}{8}}\prod_{n=1}^{\frac{q-1}{2}}(-v^n)(v^n - v^{-n})\\ &= (-1)^{\frac{q-1}{2}}v^{\frac{q^2-1}{8}}v^{\frac{(q^2-1)(q-1)}{8}}\prod_{n=1}^{\frac{q-1}{2}}(v^n - v^{-n})\\ &= (-1)^{\frac{q-1}{2}}\prod_{n=1}^{\frac{q-1}{2}}(v^n - v^{-n})\end{aligned}$$

(1) It is easy to see our assertion for $q = 3$. We set $q > 3$ and $u = u_1$. Then our result follows from the next equations in virtue of Proposition 2(2), Lemma 3 and $3(q^2-1)(q-1) \equiv (q^2-1)(q-3) \bmod 16q$.

$$\begin{aligned}&i^{\frac{q^2-1}{4}}q^{\frac{q-3}{2}}\eta\\ &= \prod_{q-1\geq m>n\geq 1}(u^m - u^n) = \prod_{m=1}^{q-2}\prod_{n=1}^{m}(-u^n)(u_0 - u^{m-n+1})\\ &= (-1)^{\frac{(q-1)(q-2)}{2}}u^{\frac{q(q-1)(q-2)}{6}}\prod_{m=1}^{q-2}\prod_{n=1}^{m}(u_0 - u^{m-n+1})\\ &= (-1)^{\frac{q-1}{2}}\prod_{m=1}^{\frac{q-3}{2}}\Big\{\prod_{n=1}^{m}(u_0 - u^n)\prod_{n=1}^{q-m-1}(u_0 - u^n)\Big\}\cdot\prod_{n=1}^{\frac{q-1}{2}}(u_0 - u^n)\\ &= (-1)^{\frac{q-1}{2}}\prod_{m=1}^{\frac{q-3}{2}}\Big\{\prod_{n=1}^{m}(-u^n)(u_0 - u^{q-n})\prod_{n=1}^{q-m-1}(u_0 - u^n)\Big\}\cdot\prod_{n=1}^{\frac{q-1}{2}}(u_0 - u^n)\\ &= i^{\frac{q^2-1}{4}}u^{\frac{(q^2-1)(q-1)}{16}}\Big\{\prod_{n=1}^{q-1}(u_0 - u^n)\Big\}^{\frac{q-3}{2}}\cdot\prod_{n=1}^{\frac{q-1}{2}}(u_0 - u^n)\\ &= i^{\frac{q^2-1}{4}}q^{\frac{q-3}{2}}u^{\frac{(q^2-1)(q-1)}{16}}\cdot\prod_{n=1}^{\frac{q-1}{2}}(u_0 - u^n).\end{aligned}$$

4. The quadratic Gauss sums for odd primes. In this section, using the last theorem, we shall determine the quadratic Gauss sums for odd primes q. First we need the following

Lemma 5. $\prod_{k=1}^{(n-1)/2} 2\sin(k\pi/n) = \sqrt{n}$, *where* n *is odd.*

Proof. Setting $x = 1$ in the equation

$$x^{n-1} + \cdots + x + 1 = \prod_{k=1}^{n-1}(x - \sigma^{2k}), \quad \text{where } \sigma = e^{\frac{\pi i}{n}},$$

we have our assertion from the next

$$n = \prod_{k=1}^{n-1}(-\sigma^k)(\sigma^k - \sigma^{-k}) = (-1)^{n-1}\sigma^{\frac{n(n-1)}{2}} i^{n-1} \prod_{k=1}^{n-1} 2\sin\left(\frac{k\pi}{n}\right).$$

We set $\rho = \epsilon^{\pi i/q}$ and $g = \sum_{k=1}^{q-1} \eta(k)\rho^{2k}$. Then considering the linear representation $u_a \to \rho^{2a}$ $(v \to -\rho)$ of G, Theorem 4(2) together with Lemma 5 implies

$$g = (-1)^{\frac{(q-1)(q+5)}{8}} i^{\frac{q-1}{2}} \prod_{k=1}^{\frac{q-1}{2}} 2\sin\left(\frac{k\pi}{q}\right) = i^{\frac{(q-1)^2}{4}}\sqrt{q}$$

since $(q+7)/2 \equiv (q-1)/2 \bmod 4$.

References

[1] K. Ireland and M. Rosen: A Classical Introduction to Modern Number Theory, Springer, GTM 84, 1982.

[2] C. Moreno: Algebraic Curves over Finite Fields, Cambridge Univ. Press, 1991

[3] K. Motose: On Loewy series of group algebras of some solvable groups, J. Algebra **130** (1990), 261–272.

[4] K. Motose: On commutative group algebras, Sci. Rep. Hirosaki Univ. **40** (1993), 127–131.

Department of Mathematics
Hirosaki University
Hirosaki 036, Japan

(*Received March 30, 1994*)