GAUSS SUMS ARE JUST CHARACTERS OF MULTIPLICATIVE GROUPS OF FINITE FIELDS [1]

Kaoru Motose

This paper is a summary of some papers [4,5,6] such that using special commutative group algebras, we could prove alternatively some reciprocity theorems, prime decompositions of Gauss sums and Lenstra's primality test.

1. Group Algebra Map(F, K)

Let $A = \mathrm{Map}(F, K)$ be the set of all mappings from a finite field $F = F_q$ of order q to a field K where q is a power of a prime p. 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 over K. If there is no chance of confusion we shall denote the product $f * g$ by the usual notation fg.

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

$$u_a(b) := \begin{cases} 1 & \text{if } b = a \\ 0 & \text{if } b \neq a. \end{cases}$$

Then we have the following equations.

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

Thus $\{u_a \mid a \in F\}$ forms a basis of the group algebra A of the additive group of F over K. We denote by $\widehat{F}$ the set of all characters of the multiplicative group $F^* = F \setminus \{0\}$, by $\chi^{[k]}$ k-th power of $\chi \in \widehat{F}$ with respect to the convolution product and by ϵ the trivial character. We set $\epsilon(0) = 1$ and $\chi(0) = 0$ for $\chi \neq \epsilon \in \widehat{F}$. Thus we have $\widehat{F} \subset A$. We set $J(f_1, f_2, \dots, f_n) = (f_1 f_2 \cdots f_n)(1)$ for $f_1, f_2, \dots, f_n \in A$ which is

[1] This paper is a summary of some papers [4,5,6] that was already published. This paper was financially supported by Fund for the Promotion of International Scientific Research B-2, 2004, Aomori, Japan.

usually called the Jacobi sum.

2. Gauss sums and Jacobi sums

It is easy to see that $\epsilon * \epsilon = q\epsilon$ and $\lambda * \epsilon = 0$ for nontrivial $\lambda \in \widehat{F}$. We have the following another relations which are important to our object.

Lemma 1. *Assume that $\lambda_1, \lambda_2, \ldots, \lambda_n$ are nontrivial elements in $\widehat{F}$ and $q-1 \neq 0$ in K. Then we have the next equations in each case.*

(1) *In case $\lambda_1\lambda_2 \ldots \lambda_n \neq \epsilon$, we have*

$$\lambda_1 * \lambda_2 * \cdots * \lambda_n = J(\lambda_1, \lambda_2, \ldots, \lambda_n)\lambda_1\lambda_2 \cdots \lambda_n.$$

(2) *In case $\lambda_1\lambda_2 \cdots \lambda_n = \epsilon$, we have*

$$\lambda_1 * \lambda_2 * \cdots * \lambda_n = \lambda_n(-1)J(\lambda_1, \lambda_2, \ldots, \lambda_{n-1})(qu_0 - \epsilon)$$

where $J(\lambda_1, \lambda_2, \ldots, \lambda_{n-1}) = 1$ if $n = 2$.

For $\chi \in \widehat{F}$, we can write $\chi = \Sigma_{a \in F_p}\chi(a)u_a$. On the other hand Gauss sums is defined by

$$g(\chi) = \sum_{a \in F} \chi(a)\zeta_p^{\mathrm{tr}(a)}$$

where $\zeta_p := e^{\frac{2\pi i}{p}}$, $q = p^r$ and $\mathrm{tr}(a) = a + a^p + \cdots + a^{p^{r-1}}$ for $a \in F$. Hence, in case $K = \boldsymbol{C}$ the complex number field, a map $\chi \mapsto g(\chi)$ ($u_a \mapsto \zeta_p^{\mathrm{tr}(a)}$) is the natural homomorphism from A to $\boldsymbol{C}$. Therefore, it is natural to think of χ as Gauss sum $g(\chi)$. It is easy to see $\widehat{F}$ forms a basis of A because $u_a = \frac{1}{q-1}\Sigma_{\chi \in \widehat{F}}\chi(a^{-1})\chi$ if $q-1 \neq 0$ in K.

3. Quadratic characters for odd primes

In this section, we shall have evaluation of the quadratic character $\eta \in A$ for an odd prime q. Using the character table and a permutation $b \mapsto b^{-1}$ on F^*, we can see easily the next proposition.

Proposition 2.

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

The next needs for evaluation of η. This follows from Proposition 2.

Lemma 3.

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

(2) $\eta = u_1^{\frac{(q^2-1)(q-1)}{16}} \prod_{k=1}^{\frac{q-1}{2}} (u_0 - u_1^k).$

(3) $\eta = (-1)^{\frac{q-1}{2}} v^{\frac{q(q^2-1)}{8}} \prod_{k=1}^{\frac{q-1}{2}} (v^k - v^{-k})$ *where* $v = u_{\frac{q+1}{2}}$.

We can see the evaluation of ordinary Gauss sum

$$g(\eta) = i^{\frac{(q-1)^2}{4}} \sqrt{q}$$

from Lemma 3 and the equation $\prod_{k=1}^{\frac{n-1}{2}} 2\sin(\frac{k\pi}{n}) = \sqrt{n}$ for an odd n.

4. Prime decompositions of Gauss sums

In this section, 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]).

Let m be a natural number, let p be a prime which does not divide m, let f be the order of $p \bmod m$, 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 $g_a = g(\chi^a) = \sum_{\alpha \in F} \chi^a(\alpha)\zeta_p^{\mathrm{tr}(\alpha)}$ 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]).

Theorem 4. $\mathrm{ord}_{\mathcal{P}}(g_a) = a^*$ *for* $0 < a < q$, *namely,* $\mathcal{P}^{a^*}$ *divides exactly* g_a.

Proof. Let ν be a natural homomorphism from $\mathrm{Map}(F, O)$ to $\mathrm{Map}(F, O/P)$ and let $\mathcal{J}$ be the ideal generated by P and $\{u_0 - u_\alpha | \alpha \in F\}$. 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 $\mathrm{Map}(F, O/P)$, and so $\chi^c \in \mathcal{J}$. [3, 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 $u_\beta \mapsto \zeta_p^{\mathrm{tr}(\beta)}$ induces the epimorphism ϕ :$\mathrm{Map}(F, O) \to \mathcal{O}$ 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 $g_a g_{q-1-a} = \chi^a(-1)q$ and $\mathrm{ord}_{\mathcal{P}}(p) = p-1$. This completes our proof.

Remark 5. [3, Proposition 3.3] shows that $\{\chi^a | a^* = k\}$ 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 $\chi^a \in \mathcal{J}^s$.

Loewy series of $\mathrm{Map}(F, O/P)$ are computed from this. (a^* is the maximum integer s with $\chi^a \in \mathcal{J}^s$)

5. Reciprocity theorems and Lenstra's primality test

The next lemma is essential in proving quadratic, cubic and biquadratic reciprocity theorems, and Lenstra's primality test.

Lemma 6. *Let ℓ be the order of $\chi \in \widehat{F}$, let n be a prime number with $(n,q) = 1$ and let e and s be natural numbers with $n^e \equiv s \bmod \ell$. Then*

$$\chi^{-es}(n) \equiv (jq)^{\frac{n^e-s}{\ell}} \chi^{[s]}(1) \mod n \quad \textit{where } j = \chi(-1)\chi^{[\ell-1]}(1).$$

Theorem 7 (Lenstra). *Let n be an odd integer and let r be a prime divisor of n. Let T be a finite set consisting of 2 and odd primes p satisfying $(n,p) = 1$ and $n^{p-1} \not\equiv 1 \bmod p^2$. We set $t = \prod_{p\in T} p$. Let S be the set of primes q satisfying $(n,q) = 1$ and $(q-1) \mid t$. We set $s = \prod_{q\in S} q$.*

We assume there exists an integer c such that $c^{\frac{n-1}{2}} \equiv -1 \bmod n$, and $(jq)^{\frac{n^{p-1}-1}{p}} \equiv \chi_q(n) \bmod n$ for every $p \in T$, $q \in S$ and $\chi_q \in \widehat{F}$ with order p. Then we have $r \equiv n^i \bmod s$ for some $i < t$.

References

1. K. Ireland and M. Rosen: A classical introduction to modern number theory, Springer GTM, 83 (1981).

2. H. W. Lenstra, Jr.: Primality testing algorithms, Springer Lecture Note, 901 (1980/1981).

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.

5. K. Motose: On commutative group algebras. II, Math. J. Okayama Univ. 36(1994), 23 – 27.

6. K. Motose: On commutative group algebras. III, Bull. Fac. Sci. Tech. Hirosaki Univ., 1(1999), 93 – 97.

Kaoru Motose
Department of Mathematical System Science,
Faculty of Science and Technology,
Hirosaki University, 036-8561, Japan
E-mail: skm@cc.hirosaki-u.ac.jp