STICKELBERGER RELATIONS AND LOEWY SERIES OF A GROUP ALGEBRA $\mathbf{Map}(\mathbb{F}_\mathbf{q}, \mathbb{F}_\mathbf{q})$

KAORU MOTOSE

Abstract. In this note, we present a proof of the Stickelberger relation (see [1]) using Loewy series of a group algebra $\mathrm{Map}(\mathbb{F}_q, \mathbb{F}_q)$ of the additive group of a finite field $\mathbb{F}_q$. This relation is essential in a proof of the Eisenstein reciprocity law. We also present partial solutions to the Feit-Thompson conjecture for primes 3 and 5 by a special case of this law.

Key Words : Gaussian sum, Power residue symbol, Feit-Thompson conjecture.

2000 *Mathematics Subject Classification* : Primary 11A15; Secondary 20D05.

§1. Loewy series of group algebras $\mathbf{Map}(\mathbb{F}_{\boldsymbol{q}}, \mathbb{F}_{\boldsymbol{q}})$

Let $\mathbb{F} = \mathbb{F}_q$ be the finite field of order $q = p^f$, where p is a prime, and let $A = \mathrm{Map}(\mathbb{F}, K)$ be the set of mappings from $\mathbb{F}$ to a subring K of a field. We define a convolution product $*$ in A as follows,

$$(f * g)(\alpha) := \sum_{\alpha+\beta=\gamma} f(\alpha)g(\beta) \text{ for } f,\ g \in A \text{ and } \alpha, \beta, \gamma \in \mathbb{F}.$$

We say a character by a group homomorphism from the multiplicative group $\mathbb{F}^*$ to K. Let X be the set of characters. We define the trivial character ϵ by $\epsilon(\alpha) = 1$ for all $\alpha \in \mathbb{F}^*$. It is convenient to set $\epsilon(0) = 1$ and $\chi(0) = 0$ for $\chi \neq \epsilon$. In virtue of this definition, we can see X is contained in A. In case K is a field, X is a group by the usual product, namely, $(\lambda\mu)(\alpha) := \lambda(\alpha)\mu(\alpha)$. This group isomorphic to the group $\mathbb{F}^*$. Let u_α be the characteristic function of $\alpha \in \mathbb{F}_q$, namely,

$$u_\alpha(\beta) := \begin{cases} 1 & \beta = \alpha, \\ 0 & \beta \neq \alpha. \end{cases}$$

This definition shows $u_\alpha * u_\beta = u_{\alpha+\beta}$ and so the set $\{u_\alpha \mid \alpha \in \mathbb{F}\}$ is the additive group of $\mathbb{F}$. Moreover A is a group algebra of the additive group of $\mathbb{F}$ over K. It is easy to see that $\{u_\alpha \mid \alpha \in \mathbb{F}_q\}$ are linearly independent over K and

$$f = \sum_{\alpha \in \mathbb{F}_q} f(\alpha)u_\alpha \text{ for } f \in \mathrm{Map}(\mathbb{F}_q, K).$$

§1, §2 in this note is the detailed proof of Theorem 1 in the published paper [3]. The detailed version of **§3** in this note will be submitted for publication elsewhere.

Thus $\{u_\alpha \mid \alpha \in \mathbb{F}_q\}$ is a basis of A. In case $q-1 \neq 0$ in K, the set $\{u_0\} \cup X$ is also a basis of A because orthogonal relations shows

$$(q-1)u_\alpha = \sum_{\eta \in X} \eta(\alpha^{-1})\eta \text{ for } \alpha \neq 0 \text{ and } \chi = \sum_{\alpha \in \mathbb{F}} \chi(\alpha) u_\alpha.$$

In the remainder of this paper, we assume $K = \mathbb{F}_q$. We define Jacobi sums as follows

$$J_\alpha(\lambda, \mu) = \sum_{\beta+\gamma=\alpha} \lambda(\beta)\mu(\gamma) \text{ for } \lambda,\ \mu \in X \text{ and } \alpha, \beta, \gamma \in \mathbb{F}$$

and we set $J(\lambda, \mu) = J_1(\lambda, \mu)$.

Lemma 1. *We set $\lambda,\ \mu \in X$ and $\alpha \in \mathbb{F}$.*

(1) $J_\alpha(\epsilon, \epsilon) = 0$.
(2) $J_0(\lambda, \mu) = 0$ *for* $\lambda\mu \neq \epsilon$.
(3) $J_\alpha(\lambda, \mu) = \lambda\mu(\alpha) J(\lambda, \mu)$ *for* $\alpha \neq 0$.
(4) $J(\lambda, \lambda^{-1}) = J_0(\lambda, \lambda^{-1}) = -\lambda(-1)$ *for* $\lambda \neq \epsilon$.
(5) $J(\lambda, \mu)$ *is contained in the prime field* $\mathbb{F}_p$.
(6) $\lambda * \mu = J(\lambda, \mu)\lambda\mu$.

Proof. (1) $J_\alpha(\epsilon, \epsilon) = p^f = 0$.
(2) $J_0(\lambda, \mu) = \sum_{\beta \in \mathbb{F}^*} \lambda(\beta)\mu(-\beta) = \mu(-1) \sum_{\beta \in \mathbb{F}^*} \lambda\mu(\beta) = 0$.
(3) $J_\alpha(\lambda, \mu) = \lambda\mu(\alpha) \sum_{\beta+\gamma=\alpha} \lambda(\beta\alpha^{-1})\mu(\gamma\alpha^{-1}) = \lambda\mu(\alpha) J(\lambda, \mu)$.
(4) Using (3), we have

$$\begin{aligned} J_0(\lambda, \lambda^{-1}) - J(\lambda, \lambda^{-1}) &= J_0(\lambda, \lambda^{-1}) + (q-1)J(\lambda, \lambda^{-1}) = \sum_{\alpha \in \mathbb{F}} J_\alpha(\lambda, \lambda^{-1}) \\ &= (\sum_{\beta \in \mathbb{F}} \lambda(\beta))(\sum_{\gamma \in \mathbb{F}} \lambda^{-1}(\gamma)) = 0. \end{aligned}$$

Thus we have

$$\begin{aligned} J(\lambda, \lambda^{-1}) &= J_0(\lambda, \lambda^{-1}) = \sum_{\beta \in \mathbb{F}} \lambda(-\beta)\lambda^{-1}(\beta) = \sum_{\beta \in \mathbb{F}} \lambda(-\beta)\lambda^{-1}(\beta) \\ &= \lambda(-1) \cdot \sum_{\beta \in \mathbb{F}^*} \epsilon(\beta) = \lambda(-1)(q-1) = -\lambda(-1). \end{aligned}$$

(5) The assertion follows from the equation

$$J(\lambda, \mu)^p = \sum_{\beta \in \mathbb{F}} \lambda(\beta)^p \mu(1-\beta)^p = \sum_{\beta \in \mathbb{F}} \lambda(\beta^p)\mu(1-\beta^p) \sum_{\gamma \in \mathbb{F}} \lambda(\gamma)\mu(1-\gamma) = J(\lambda, \mu).$$

(6) We have $J_0(\lambda, \mu)u_0 - J(\lambda, \mu)\lambda\mu(0)u_0 = 0$ from (2) and (4). Thus using (3), we obtain our result.

$$\begin{aligned} \lambda * \mu &= \left(\sum_{\beta \in \mathbb{F}} \lambda(\beta) u_\beta\right)\left(\sum_{\gamma \in \mathbb{F}} \mu(\gamma) u_\gamma\right) = \sum_{\beta, \gamma \in \mathbb{F}} \lambda(\beta)\mu(\gamma) u_{\beta+\gamma} = \sum_{\alpha \in \mathbb{F}} J_\alpha(\lambda, \mu) u_\alpha \\ &= J(\lambda, \mu)\lambda\mu + J_0(\lambda, \mu)u_0 - J(\lambda, \mu)\lambda\mu(0)u_0 = J(\lambda, \mu)\lambda\mu. \end{aligned}$$

Lemma 2. *Let η be a generator of $\mathbb{F}^*$ and $\phi : \eta^k \to \eta^{-k}$ be a generator of X. We set integers $0 < s, t, m < n = q-1$ with $t = p^e$ and $tm \equiv s \bmod n$. Then $J(\phi^s,\ \phi^t) = -m-1$.*

Proof. Let L be a permutation on $B = \{1,\ \ldots,\ n-1\}$ such that $\eta^{L(k)} = 1-\eta^k$ and set $\theta = \eta^t$. Then the order of θ is n. We can easily verify the next equation from the formula of a geometric series.

$$\theta^{-\ell k} \cdot (1-\theta^k)^{-1} = \theta^{-k} + \theta^{-2k} + \cdots + \theta^{-\ell k} + (1-\theta^k)^{-1} \text{ for } k \in B.$$

The next equation follows from the above formula and t is a power of a prime p.

$$\begin{aligned}
J(\phi^s, \phi^t) &= \sum_{k=0}^{n-1} \phi^s(\eta^k)\phi^t(1-\eta^k) = \sum_{k=1}^{n-1} \phi(\eta^{ks} \cdot \eta^{L(k)t}) \\
&= \sum_{k=1}^{n-1} \eta^{-ks}\eta^{-L(k)t} = \sum_{k=1}^{n-1} \eta^{-tmk}(1-\eta^{kt})^{-1} \\
&= \sum_{k=1}^{n-1} \theta^{-mk}(1-\theta^k)^{-1} = \sum_{k=1}^{n-1} \left(\left(\sum_{\ell=1}^{m} \theta^{-\ell k} \right) + \eta^{-L(k)} \right) \\
&= \sum_{\ell=1}^{m} \left(\sum_{k=1}^{n-1} \theta^{-\ell k} \right) + \sum_{k=1}^{n-1} \eta^{-L(k)} = \sum_{\ell=1}^{m} (-1) + \sum_{k=1}^{n-1} \eta^k \\
&= -m-1
\end{aligned}$$

Proposition 3. *$\mu_0^{[p-1]} * \mu_1^{[p-1]} * \cdots * \mu_{f-1}^{[p-1]} = \gamma\epsilon \neq 0$ where $\mu_k = \phi^{p^k}$, $\gamma \in \mathbb{F}$ and $\chi^{[\ell]}$ is the ℓth power by the product $*$.*

Proof. In virtue of Lemma 1 (6), the above product is equal to $\gamma\phi^{q-1} = \gamma\epsilon$ with $\gamma = \prod_{s,t} J(\phi^s, \phi^t)$ where $t = p^k$ for $k = 0, \cdots, f-1$ and $s = (\ell+1)t - 1$ for $\ell = 0, \ldots, p-2$ ($(k,\ell) \neq (0,0)$). Thus it remains only to prove $J(\phi^s, \phi^t) \neq 0$. In fact, setting $0 < m = q - q/t + \ell < n = q-1$, It is easily seen that $tm \equiv s \mod n$ and $m \equiv \ell \bmod p$. It follows from Lemma 2 that $J(\phi^s, \phi^t) = -m-1 = -\ell-1 \neq 0$ since $0 < \ell+1 < p$.

§2. Stickelberger relations

Let m be a natural number. let p be a prime do not divide m, and let f be the order of $p \bmod m$. Moreover let D_m be the ring of algebraic integers in $\mathbb{Q}(\zeta_m)$ and let P be a prime ideal containing p, where $\zeta_m = e^{\frac{2\pi i}{m}}$. Then it is well known that q is the order of a finite field $\mathbb{F} = D_m/P$. We consider Gaussian sums $g(\chi^a) = \sum_{a\in\mathbb{F}} \chi^a(\alpha)\zeta_p^{\mathrm{tr}(\alpha)}$ where χ is a generator of X and $\mathrm{tr}(\alpha)$ is the trace of α. Let $\wp$ be the ideal generated by P and $\{1-\zeta_p^k | 0 < k < p\}$ in the ring of algebraic integers D_{mp} of $\mathbb{Q}(\zeta_{mp})$. It is easy to see $\wp$ is a prime ideal generated by P and $1-\zeta_p$. We set $a^* = b_0 + b_1 + \cdots + b_{f-1}$ for a positive integer $a = b_0 + b_1 p + \cdots + b_{f-1}p^{f-1}$.

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

Proof. Let ν be a natural homomorphism:

$$\mathrm{Map}(\mathbb{F}, D_m) \to \mathrm{Map}(\mathbb{F}, D_m/P), \text{ where } D_m/P = \mathbb{F},$$

and $\Re$ be the ideal generated by P and $\{u_0 - u_\alpha | \alpha \in \mathbb{F}\}$. Since $\nu(\theta)^{[p]} = 0$ for $\epsilon \neq \theta \in X$, We obtain that $\nu(\theta)$ is contained in $\nu(\Re)$, the radical of the group algebra $\mathrm{Map}(\mathbb{F}, D_m/P)$ and so $\theta \in \Re$. By Proposition 3 together with this implies that $\gamma\chi^a \in \Re^{a^*}$ for the product of Jacobi sums $\gamma \in D_m \setminus P$. The character $u_\beta \to \zeta_p^{\mathrm{tr}(\beta)}$ induces the epimorphism

$$\phi : \mathrm{Map}(\mathbb{F}, D_m) \to D_{mp}$$

with $\phi(\Re) = \wp$ and $\phi(\gamma\chi^a) = \gamma g(\chi^a)$. Thus we have $\mathrm{ord}_{\wp}(g(\chi^a)) \geqq a^*$. On the other hand, using $\mathrm{ord}_{\wp}(p) = p - 1$ and $g(\chi^a)g(\chi^{q-1-a}) = g(\chi^a)g(\overline{\chi^a}) = \chi^a(-1)q = \chi^a(-1)p^f$, we have the next

$$\mathrm{ord}_{\wp}(g(\chi^a)) + \mathrm{ord}_{\wp}(g(\chi^{q-1-a})) = f(p-1) = a^* + (q-1-a)^*$$

This completes our proof.

From this theorem we have Stickelberger relation and Eisenstein reciprocity law by the same method in [1]. Let σ_t be an automoripism of $\mathbb{Q}(\zeta)$ for $0 < t < m$ and $(m, t) = 1$ such that $\sigma_t(\zeta_m) = \zeta_m^t$.

Theorem 5 (the Stickelberger relation)**.** $g(\chi)^m D_m = \prod_{\sigma_t} \sigma_t(P^t)$ *where* t *runs over* $0 < t < m$ *and* $(t, m) = 1$.

We set $\zeta_\ell = e^{\frac{2\pi i}{\ell}}$ for odd prime ℓ, $\theta_a = \left(\frac{-}{a}\right)_\ell$ is the ℓth power residue symbol and D_ℓ is the ring of algebraic integers in $\mathbb{Q}(\zeta_\ell)$. A non zero and non unit element $\alpha \in D_\ell$ is called primary if α is prime to ℓ and $\alpha \equiv c \bmod (1 - \zeta_\ell)^2$ for some $c \in \mathbb{Z}$.

Theorem 6 (the Eisenstein reciprocity law)**.** *Let* ℓ *be an odd prime,* $a \in \mathbb{Z}$ *and let* $\alpha \in D_\ell$ *be primary. Each pair of* ℓ, a *and* α *is coprime. Then* $\theta_a(\alpha) = \theta_\alpha(a)$.

§3. Partial solutions to the Feit Thompson conjecture for primes 3 and 5

We set $p < q$ are odd primes, and

$$F = \frac{q^p - 1}{q - 1} \text{ and } T = \frac{p^q - 1}{p - 1}.$$

Feit Thompson conjectured that F never divides T. If it would be proved, their odd paper would be greatly simplified (see [4]).

Lemma 7. *We set* $\chi_\eta = \left(\frac{-}{\eta}\right)_p$ *pth power residue symbol,* $\zeta = e^{\frac{2\pi i}{p}}$ *and* $c(q-1) \equiv 1 \bmod p$. *Then* $\eta = \zeta^c(\zeta - q)$ *is primary in the algebraic integer ring of* $\mathbb{Q}(\zeta)$.

(1) $\chi_\eta(1-\zeta)^{2(q-1)} = \chi_{q-1}(\zeta)^{q+1}$. *In particular,* $\chi_\eta(1-\zeta) = 1$ *if* p *divides* $q+1$.
(2) *if* F *divides* T, *then* $\chi_\eta(p) = 1$ *and* $\chi_\eta(1-\zeta) = \chi_\eta(u)$ *where* $u = \prod_{k=1}^{p-1} \frac{1-\zeta^k}{1-\zeta}$.
In particular, if p *divides* $q+1$, *then* $\chi_\eta(u) = 1$ *by* (1).

Using this lemma, we obtain

Corollary 8. *F never divides T in either case of the next conditions.*
(1) $p = 3$ *and* $q \not\equiv -1 \bmod 9$.
(2) $p = 5$ *and* $q + 1 = 5\ell$ *with* $(\ell, 5) = 1$.

References

[1] K. Ireland and M. Rosen. A classical introduction to modern number theory. Springer, 2nd ed., 1990.
[2] K. Motose. On Loewy series of group algebras of some solvable groups. J. Alg., 130 (1990), 261-272.
[3] K. Motose. On commutative group algebras. II, Math. J. Okayama Univ., 36 (1994), 23-27.
[4] K. Motose. Notes to the Feit-Thompson conjecture. Proc. Japan, Acad., ser A, 85(2009), 16-17.

Emeritus Professor of Hirosaki University
Toriage 5-13-5, Hirosaki, 036-8171, Japan
E-mail address: moka.mocha_no_kaori@snow.ocn.ne.jp