On commutative Group Algebras. III

K. Motose

Bull. Fac. Sci. Techn. Hirosaki Univ. 1(1999), 93-97

この論文は符号暗号理論との関係で, この科研費申請中に書かれたものである。

June 2003 本瀬香

Bull. Fac. Sci. Tech. Hirosaki Univ. **1**, 93—97 (1999)

On Commutative Group Algebras. III

Dedicated to Professor Yukio Tsushima on his 60th birthday

Kaoru MOTOSE

(Received September 17, 1998)

In this paper, using commutative group algebras, we shall give some reciprocity theorems and Lenstra's primality test.

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

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

for $f, g \in A$ and $c \in F_q$. This product together with the usual sum and the scalar product gives the structure of a commutative group algebra of the additive group of F_q over C. If there is no chance of confusion, we shall denote the product $f * g$ by the usual notation fg.

Let $u = u_a$ be the characteristic function of $a \in F_q$, 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 equation.

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

Thus $\{u_a \mid a \in F_q\}$ forms a basis of the group algebra A.

We denote by $\widehat{F_q}$ the set of all characters of the multiplicative group $F_q^* = F_q - \{0\}$, by $\chi^{[k]}$ kth power of $\chi \in \widehat{F_q}$ with respect to the convolution product and by ε the trivial character. We set $\varepsilon(0) = 1$ and $\chi(0) = 0$ for $\chi \neq \varepsilon$.

The next is our key Lemma.

Lemma. *Let $\ell > 1$ be the order of $\chi \in \widehat{F_q}$, 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*

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

Proof. We have the next equation

$$\chi^{[n^e]} = \Big(\sum_{a \in F_q} \chi(a)\, u_a\Big)^{n^e} \equiv \sum_{a \in F_q} \chi^{n^e}(a)\, u_{n^e a}$$
$$= \chi^{-n^e}(n^e) \sum_{a \in F_q} \chi^{n^e}(n^e a)\, u_{n^e a} = \chi^{-en^e}(n)\chi^{n^e}$$

$$= \chi^{-es}(n)\chi^{s} \bmod n.$$

On the other hand, using $\chi * u_0 = \chi$ and $\chi * \varepsilon = 0$, we have the next by [3, Lemma 2 (2)].

$$\chi^{[n^e]} = (\chi^{[\ell]})^{[\frac{n^e-s}{\ell}]} * \chi^{[s]} = (j(qu_0 - \varepsilon))^{[\frac{n^e-s}{\ell}]} * \chi^{[s]} = (jq)^{\frac{n^e-s}{\ell}}\chi^{[s]}$$

where $j = \chi(-1)\chi^{[\ell-1]}(1)$. Thus we obtain

$$\chi^{-es}(n) \equiv (jq)^{\frac{n^e-s}{\ell}}\chi^{[s]}(1) \bmod n.$$

The next is a specialization of Lemma.

Corollary. *Let $\ell > 1$ be the order of $\chi \in \widehat{F}_q$, let p be a prime number with $(p, q) = 1$ and $p \equiv 1 \bmod \ell$. Then*

$$\chi^{-1}(p) \equiv (jq)^{\frac{p-1}{\ell}} \bmod p \text{ where } j = \chi(-1)\chi^{[\ell-1]}(1).$$

Theorem 1 (Quadratic reciprocity). *Let p and q be distinct odd primes in Z. Then*

$$\chi_q(p) = \chi_p(q)(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

where $\chi_q \in \widehat{F}_q$ and $\chi_p \in \widehat{F}_p$ are of the order 2.

Proof. It follow from Corollary that

$$\chi_q(p) \equiv (\chi_q(-1)q)^{\frac{p-1}{2}} \bmod p.$$

Using the next equation, we have the assertion.

$$\chi_q(-1) = (-1)^{\frac{q-1}{2}} \text{ and } q^{\frac{p-1}{2}} \equiv \chi_p(q) \bmod p.$$

Proposition 1. Let O be the principal ideal ring of all integers in a quadratic field, let π be prime in O and let χ_π be a character of order $\ell > 2$ of a finite field $O/\pi O$ with $N(\pi)$ elements such that

$$\chi_\pi(\alpha) \equiv \alpha^{\frac{N(\pi)-1}{\ell}} \bmod \pi$$

where N means the norm. Then we have

(1) If $\pi = q$ is rational and $q \equiv -1 \bmod \ell$, then $\chi_q(a) = 1$ for rational integers a.

(2) If π is complex, then $\chi_\pi^{[2]}(1)$ and π are associates.

Proof. (1): It is easy see that $\chi_q(a)$ is real and so $\chi_q(a) = \pm 1$. Thus we have the assertion from the next.

$$\chi_q(a) \equiv a^{\frac{q^2-1}{\ell}} = (a^{q-1})^{\frac{q+1}{\ell}} \equiv 1 \bmod q.$$

(2): Since $N(\pi) = q$ is prime and $N(\chi_\pi^{[2]}(1)) = q$, we have $\chi_\pi^{[2]}(1)$ is prime.
We can see the next from $\sum_{a\in F_q} a^k = 0$ for $k < q-1$.

$$\chi_\pi^{[2]}(1) = \sum_{a\in F} \chi_\pi(a)\chi_\pi(1-a) \equiv \sum_{a\in F} a^{\frac{q-1}{\ell}}(1-a)^{\frac{q-1}{\ell}} \equiv 0 \bmod \pi.$$

Thus we have the assertion.

Theorem 2 (Cubic reciprocity). *Let π and λ be primary primes in $Z[\omega]$ with $N\pi$, $N\lambda \neq 3$ and $N\pi \neq N\lambda$, where ω is the primitive 3rd root of 1, and N means the norm. Then we have*

$$\chi_\pi(\lambda) = \chi_\lambda(\pi)$$

where χ_π and χ_λ are the cubic residue characters modulo π and modulo λ, respectively.

Proof. In virtue of Proposition 1, we may assume π is complex and we have $j = \chi_\pi(-1)\chi_\pi^{[2]}(1)$ and π are associates. We set $N(\pi) = q \equiv 1 \bmod 3$. We can see from the next by [3, Lemma 2] that $j \equiv 2 \bmod 3$ and j is primary.

$$j(qu_0 - \varepsilon) = \chi_\pi^{[3]} \equiv \sum_{a\in F_q^*} u_{3a} = \varepsilon - u_0 \bmod 3.$$

Hence we have $j = \pi$.

In case $\lambda = p$ is rational, namely, $\lambda = p \equiv 2 \bmod 3$, setting $n = p$, $\ell = 3$, $e = 2$, and $s = 1$ in Lemma, we have $\chi_\pi^{-2}(p) \equiv (\pi q)^{\frac{p^2-1}{3}} \bmod p$ and so

$$\chi_\pi(p) = \chi_p(\pi q) = \chi_p(\pi)\chi_p(q) = \chi_p(\pi).$$

In case λ is complex, namely, $N(\lambda) = p \equiv 1 \bmod 3$, using Corollary, we have

$$\chi_\pi^{-1}(p) \equiv (\pi q)^{\frac{p-1}{3}} \bmod p.$$

Hence we obtain

$$\chi_\pi^{-1}(p) = \chi_\lambda(\pi)\chi_\lambda(q), \text{ similarly, } \chi_\lambda^{-1}(q) = \chi_\pi(p)\chi_\pi(\lambda).$$

Thus we have

$$\chi_\lambda(\pi) = \chi_\pi^{-1}(p)\chi_\lambda^{-1}(q) = \chi_\pi^{-1}(p)\chi_\pi(p)\chi_\pi(\lambda) = \chi_\pi(\lambda).$$

Theorem 3 (Biquadratic reciprocity). *Let π and λ be relatively prime and primary primes in $Z[i]$ where $i = \sqrt{-1}$. Then*

$$\chi_\pi(\lambda) = \chi_\lambda(\pi)(-1)^{\frac{N(\pi)-1}{4}\frac{N(\lambda)-1}{4}}$$

where χ_π and χ_λ are the biquadratic residue characters modulo π and modulo λ, respectively.

Proof. In virtue of Proposition 1, we may assume π is complex and we have $\chi_\pi^{[2]}(1)$ and

π are associates. We set $N(\pi) = q \equiv 1 \bmod 4$, $\eta = \chi_\pi^2$ and $j = \chi_\pi(-1)\,\chi_\pi^{[3]}(1)$.

We obtain the next from [3, Lemma 2].

$$j(qu_0 - \varepsilon) = \chi_\pi^{[4]} = (\chi_\pi * \chi_\pi)^{[2]} = (\chi_\pi^{[2]}(1)\,\eta)^{[2]}$$
$$= \chi_\pi^{[2]}(1)^2\,\eta(-1)\,(qu_0 - \varepsilon) = \chi_\pi^{[2]}(1)^2(qu_0 - \varepsilon).$$

Thus $j = \chi_\pi^{[2]}(1)^2$ and π^2 are associates. On the other hand, We obtain

$$\chi_\pi^{[2]} = (\sum_{a \in F_q} \chi_\pi(a)\,u_a)^2 \equiv \eta(2)\,(\sum_{a \in F_q} \eta(2a)\,u_{2a}) = \eta(2)\,\eta \bmod 2.$$

Using the above equation, we have

$$j(qu_0 - \varepsilon) = \chi_\pi^{[4]} \equiv (\eta(2)\,\eta)^{[2]} = \eta^{[2]} = qu_0 - \varepsilon \bmod 4.$$

Thus $j \equiv 1 \bmod 4$, namely, j is primary. Since j and π^2 are associates, we have $j = \pi^2$.

In case λ is complex, namely, $N(\lambda) = p \equiv 1 \bmod 4$, then using Corollary, we have $\chi_\pi^{-1}(p) \equiv (\pi^2 q)^{\frac{p-1}{4}} \bmod p$ and so

$$\chi_\pi(p) = \chi_\lambda^{-1}(\pi^2 q) = \chi_\lambda^{-1}(\pi^3 \bar{\pi}) = \chi_\lambda(\pi)\,\chi_{\bar{\lambda}}(\pi) = \chi_\mathfrak{p}(\pi).$$

In case λ is rational, namely, $\lambda = p \equiv 3 \bmod 4$, then setting $n = p$, $\ell = 4$, $e = 1$ and $s = 3$ in Lemma, we have from $\pi^p \equiv \bar{\pi} \bmod p$ that

$$\chi_\pi(-p) = \chi_\pi(-1)\,\chi_\pi^{-3}(p) \equiv \chi_\pi(-1)\,(\pi^2 q)^{\frac{p-3}{4}}\,\chi_\pi^{[3]}(1)$$
$$\equiv (\pi^3 \bar{\pi})^{\frac{p-3}{4}}\,\pi^2 \equiv (\pi^3 \pi^p)^{\frac{p-3}{4}}\,\pi^2 = \pi^{\frac{p^2-1}{4}} \equiv \chi_\mathfrak{p}(\pi) \bmod p.$$

From here on we proceed exactly as in [1, pp. 126-127] to the desired conclusion.

In the remainder of this paper, we shall state Lenstra's primality test (see [2]).

Proposition 2. *Assume n is prime.*

(1) *There exists c with $c^{\frac{n-1}{2}} \equiv -1 \bmod n$.*

(2) *Let $\chi_q \in \widehat{F_q}$ be of order p where $p \mid q-1$ and $(pq, n) = 1$. Then we have*

$$(jq)^{\frac{n^{p-1}-1}{p}} \equiv \chi_q(n) \bmod n \text{ where } j = \chi_q(-1)\,\chi_q^{[p-1]}(1).$$

Proof.

(1) It is easy to see the assertion for a primitive root c of n.

(2) We set $s = 1$, $e = p - 1$, $\ell = p$ in Lemma. Then $es \equiv -1 \bmod \ell$ and

$$(jq)^{\frac{n^{p-1}-1}{p}} = (jq)^{\frac{n^s-s}{\ell}} \equiv \chi_q^{-es}(n) = \chi_q(n) \bmod n.$$

Theorem 4 (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 $t = \Pi_{p \in T} p$. Let S be the set of primes q satisfying $(n, q) = 1$ and $(q-1) \mid t$. We set $s = \Pi_{q \in S} q$. We assume there exists an integer c such that $c^{\frac{n-1}{2}} \equiv -1 \bmod n$, and $(jq)^{\frac{n^{p-1}-1}{p}} \equiv \chi_q(n) \bmod n$, where $j = \chi_q(-1)\chi_q^{[p-1]}(1)$, for every $p \in T$, $q \in S$ and $\chi_q \in \widehat{F_q}$ with order p. Then we have $r \equiv n^i \bmod s$ for some $i < t$.

Proof. We set $n^{p-1} - 1 = p^k \ell$ with $(\ell, p) = 1$. In case $p \neq 2$, $k = 1$ by the assumption. In case $p = 2$, we can see 2^k is a divisor of $r - 1$ since $(c^\ell)^{2^{k-1}} \equiv -1 \bmod r$. In each case, p^k is a divisor of $r^{p-1} - 1$. There exists an integer x with $\ell x \equiv 1 \bmod p$. We set $b = \ell x$ and $a = mx$, where $m = \frac{r^{p-1}-1}{p^k}$. Then we have $\frac{r^{p-1}-1}{p} b = \frac{n^{p-1}-1}{p} a$ with $b \equiv 1 \bmod p$.

Thus we have for $\chi_q \in \widehat{F_q}$ with order p.

$$\chi_q(r) = \chi_q(r)^b \equiv (jq)^{\frac{r^{p-1}-1}{p} b} = (jq)^{\frac{n^{p-1}-1}{p} a} \equiv \chi_q(n)^a \bmod r.$$

By virtue of Chinese remainder theorem, there exists i with $i \equiv a \bmod p$ for every p and a. Thus $\chi_q(r) = \chi_q(n)^i = \chi_q(n^i)$ for every character χ_q of F_q. Hence $r \equiv n^i \bmod q$ for every $q \in S$ and $r \equiv n^i \bmod s$.

References

[1] K. Ireland and M. Rosen : A classical introduction to modern number theory, Springer GTM, 84 (1982).

[2] H. W. Lenstra, Jr. : Primality testing algorithms, Springer Lecture Note, **901** (1981).

[3] K. Motose : Commutative group algebras, Sci. Rep. Hirosaki Univ., **40** (1993), 127-131.

[4] K. Motose : Commutative group algebras. II, Math. J. Okayama Univ. **36** (1994), 23-27.

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