INTEGRAL GROUP ALGEBRAS AND CYCLOTOMIC POLYNOMIALS [1]

Kaoru MOTOSE

Recently, using cyclotomic polynomials, Z. Marciniak and S. K. Sehgal [3] obtained excellent results about units in integral group rings of cyclic groups. In this paper, we shall give some improvements and alternative proofs of their results.

Let $\mathbb{Z}G$ be the group algebra of a finite abelian group G over the ring $\mathbb{Z}$ of rational integers. It is well known that the units of *finite* order in $\mathbb{Z}G$ have the form $\pm g$ for some $g \in G$ (see [1], p. 262). We study the form of units of *infinite* order in $\mathbb{Z}G$ where $G = \langle \sigma \rangle$.

Let $\Phi_m(x)$ be cyclotomic polynomial of order m defined inductively by

$$X^m - 1 = \prod_{d|m} \Phi_d(x).$$

Z. Marciniak and S.K. Sehgal [3] construct many units of infinite order using cyclotomic polynomials. These units cover the alternative units, the Hoechsmann units [3] and Yamauchi's results [4].

In this paper, we study the Euclidean algorithm for cyclotomic polynomials in $\mathbb{Z}[x]$, and we have easy applications to some their results in [3]. The following are well known units. Units in 1, 2 are covered by cyclotomic polynomials.

1. The alternating units:

$$\Phi_{2k}(\sigma) = 1 - \sigma + \sigma^2 - \cdots + (-1)^k \sigma^k$$

where k is odd and $(2k, |G|) = 1$.

2. The Hoechsmann units (the constructible units) (see also K. Yamauchi [4]).

$$\frac{\sigma^{k\ell} - 1}{\sigma^k - 1} \cdot \frac{\sigma - 1}{\sigma^\ell - 1} = \frac{1 + \sigma^k + \sigma^{2k} + \cdots + \sigma^{(\ell-1)k}}{1 + \sigma + \sigma^2 + \cdots + \sigma^{\ell-1}}$$

where $k,\ \ell \geq 2,\ (k\ell, |G|) = 1$ and $(k, \ell) = 1$.

3. Bass cyclic units,

$$(1 + \sigma + \cdots + \sigma^{k-1})^m - \ell(1 + \sigma + \cdots + \sigma^{|G|-1})$$

where $k > 1$ and $k^m = 1 + \ell|G|$.

Since the group algebra $\mathbb{Z}G$ are isomorphic to $\mathbb{Z}[x]/(x^n - 1)\mathbb{Z}[x]$, our study on units in $\mathbb{Z}G$ is equivalent to find polynomials $f(x) \in \mathbb{Z}[x]$ satisfying

$$f(x)u(x) + (x^n - 1)v(x) = 1, \text{ where } u(x), v(x) \in \mathbb{Z}[x].$$

For relatively prime polynomials $f(x)$ and $g(x)$ over a field K, it is easy to compute polynomials $u(x), v(x) \in K[x]$ by Euclidean algorithm such that

$$f(x)u(x) + g(x)v(x) = 1.$$

[1]The detailed version of this paper will be submitted for publication elsewhere This paper was financially supported by Fund for the Promotion of International Scientific Research B-2, 2004, Aomori, Japan.

However, over $\mathbb{Z}[x]$, situation is different from this. Of course we can compute $u(x), v(x) \in \mathbb{Q}[x]$ by Euclidean algorithm for relatively prime polynomials $f(x), g(x) \in \mathbb{Z}[x]$. Thus we have

$$f(x)u_0(x) + g(x)v_0(x) = a$$

where $u_0(x), v_0(x) \in \mathbb{Z}[x]$ and $0 \neq a \in \mathbb{Z}$.

For example, we obtain for cyclotomic polynomials $\Phi_3(x) = x^2 + x + 1, \Phi_6(x) = x^2 - x + 1$,

$$\Phi_3(x)(1 - x) + \Phi_6(x)(x + 1) = 1 - x^3 + 1 + x^3 = 2$$

and we can easily show there is no polynomials $u(x), v(x) \in \mathbb{Z}[x]$ such that

$$\Phi_3(x)u(x) + \Phi_6(x)v(x) = 1.$$

In fact $1 = \Phi_6(\omega)v(\omega) = -2\omega v(\omega) = -2\bar{\omega}v(\bar{\omega})$ for two roots $\omega, \bar{\omega}$ of $\Phi_3(x)$. We have a contradiction such that $1 = 4 \cdot v(\omega)v(\bar{\omega})$ and $v(\omega)v(\bar{\omega})$ is an integer.

Thus it is natural to consider the next problem.

For given polynomials $f(x),\ g(x) \in \mathbb{Z}[x]$, does there exist polynomials $u(x),\ v(x) \in \mathbb{Z}[x]$ such that

$$f(x)u(x) + g(x)v(x) = 1\ ?$$

It is easy for $f(x) = x$ and $g(x) = x^n - 1$. But in general, it seems to be difficult for me because the ring $\mathbb{Z}[x]$ is not Euclidean though it is a unique factorization ring. In this paper, we shall answer to this problem in case $f(x)$ and $g(x)$ are cyclotomic polynomials for units in $\mathbb{Z}G$.

If $m \neq n$, then we have $\Phi_m(x)u(x) + \Phi_n(x)v(x) = 1$ in $\mathbb{Q}[x]$ since $\Phi_m(x), \Phi_n(x)$ are distinct irreducible polynomials in $\mathbb{Q}[x]$. Over $\mathbb{Z}[x]$, we can see the next theorem.

Theorem 1. *Assume $n > m \geq 1$. Then we have*

(1) *If m is not a devisor of n, then there exist $u(x), v(x) \in \mathbb{Z}[x]$ such that*

$$\Phi_m(x)u(x) + \Phi_n(x)v(x) = 1.$$

(2) *If m is a divisor of n, then we set $n = mk$ and k_0 is the product of all distinct prime divisors k. There exist $u(x), v(x) \in \mathbb{Z}[x]$ such that*

$$\Phi_m(x)u(x) + \Phi_n(x)v(x) = \Phi_{k_0}(1).$$

Proof. (1) If we set $n = mq + r,\ 0 \leq r < m$, then we have easily

$$x^n - 1 = (x^m - 1) \cdot (\frac{x^{mq} - 1}{x^m - 1} \cdot x^r) + x^r - 1.$$

Hence, we can use Euclidean algorithm in $\mathbb{Z}[x]$ and so

$$(x^n - 1)s(x) + (x^m - 1)t(x) = x^d - 1, \quad \text{for some } s(x), t(x) \in \mathbb{Z}[x]$$

where $d = (n, m)$. Thus we have

$$\frac{x^n - 1}{x^d - 1}s(x) + \frac{x^m - 1}{x^d - 1}t(x) = 1.$$

Therefore, we obtain the next equation excluding cases $m|n$

$$\Phi_n(x)u(x) + \Phi_m(x)v(x) = 1 \text{ for some } u(x), v(x) \in \mathbb{Z}[x].$$

(2) Since $x-1$ divides $\Phi_{k_0}(x)-\Phi_{k_0}(1)$ in $\mathbb{Z}[x]$, we have $x^{hm}-1$ and so $\Phi_m(x)$ divides $\Phi_{k_0}(x^{hm})-\Phi_{k_0}(1)$ where $h=\frac{k}{k_0}$. Let n_0 be the product of all distinct prime divisors n. We set $n_0=\ell k_0$ and

$$u(x)=\frac{\Phi_{k_0}(1)-\Phi_{k_0}(x^{hm})}{\Phi_m(x)} \text{ and } v(x)=\prod_{d|\ell,\ d<\ell}\Phi_{k_0 d}(x^{\frac{n}{n_0}}).$$

Then $u(x)$ and $v(x)\in\mathbb{Z}[x]$. Noting $\frac{n}{n_0}\ell=\frac{k}{k_0}m=hm$ and $(\ell,k_0)=1$, we have

$$\begin{aligned}\Phi_m(x)u(x)+\Phi_n(x)v(x) &= \Phi_m(x)u(x)+\Phi_{n_0}(x^{\frac{n}{n_0}})\prod_{d|\ell,\ d<\ell}\Phi_{k_0 d}(x^{\frac{n}{n_0}})\\ &= \Phi_{k_0}(1)-\Phi_{k_0}(x^{hm})+\Phi_{k_0}((x^{\frac{n}{n_0}})^{\ell})\\ &= \Phi_{k_0}(1).\end{aligned}$$

Let m be a natural number and let q be a power of a prime with $(q,m)=1$. Then we can see from Theorem 1 (2) that there exist $u(x),v(x)\in\mathbb{Z}[x]$ such that

$$\Phi_m(x)u(x)+\Phi_{mq}(x)v(x)=p.$$

However, the next proposition shows that p is the smallest positive integer satisfying the above equation.

Proposition 1. *There exist no $s(x),t(x)\in\mathbb{Z}[x]$ such that*

$$\Phi_m(x)s(x)+\Phi_{mq}(x)t(x)=1$$

for a natural number m and a power q of a prime p with $(q,m)=1$.

Proof. Let Δ be the set of roots of $\Phi_m(x)$. Using $\prod_{d|m}\Phi_{dq}(x)=\Phi_q(x^m)$, we have the next

$$\prod_{d|m}\Phi_{dq}(\eta)=\Phi_q(\eta^m)=\Phi_q(1)=p$$

where $\eta\in\Delta$. Thus

$$p^{|\Delta|}=\prod_{\eta\in\Delta}\prod_{d|m}\Phi_{dq}(\eta)=\prod_{d|m}\prod_{\eta\in\Delta}\Phi_{dq}(\eta).$$

We set $a_d=\prod_{\eta\in\Delta}\Phi_{dq}(\eta)$. Then a_d is an integer because a_d is a symmetric polynomial in $\mathbb{Z}[\eta\in\Delta]$ and so $a_d\in\mathbb{Z}[\text{coefficients of }\Phi_m(x)]$. Hence we have from the above equation.

$$p^{|\Delta|}=\prod_{d|m}|a_d| \text{ and } |a_d|=p^{\alpha(d)}$$

where $\alpha(d)$ is a nonnegative integer. Therefore we have

$$\varphi(m)=|\Delta|=\sum_{d|m}\alpha(d).$$

Using Möbius inversion formula, we obtain

$$\alpha(m)=\sum_{d|m}\varphi(d)\mu(\frac{m}{d}).$$

For a prime r,

$$\alpha(r^e) = \varphi(r^e) - \varphi(r^{e-1}) = \begin{cases} r^{e-2}(r-1)^2 & \text{for } e \geq 2, \\ r-2 & \text{for } e = 1. \end{cases}$$

Since $\varphi(i)$ is multiplicative, $\alpha(i)$ is also multiplicative. Thus if $\alpha(i) = 0$, then $i = 2j$ and j is odd.

On the other hand, it follows from the assumption that $\Phi_{mq}(\eta)t(\eta) = 1$ for $\eta \in \Delta$ and so $a_m = \prod_{\eta\in\Delta} \Phi_{mq}(\eta) = \pm 1$. Thus $|a_m| = 1$, and so $\alpha(m) = 0$. This implies $m = 2\ell$, ℓ is odd, and $q > 2$. Hence we have a contradiction for $\ell \geq 3$ by above arguments

$$1 = \Phi_{2\ell}(-x)s(-x) + \Phi_{2\ell q}(-x)t(-x) = \Phi_\ell(x)s(-x) + \Phi_{\ell q}(x)t(-x).$$

We have also a contradiction for $\ell = 1$ by $\Phi_2(-1) = 0$

$$1 = \Phi_2(-1)s(-1) + \Phi_{2q}(-1)t(-1) = pt(-1).$$

Remark 1. It follows from $\Phi_m(x^{p^s}) = \Phi_{mp^s}(x)\Phi_m(x^{p^{s-1}})$ for $(p, m) = 1$ that

$$\Phi_{mp^s}(x) \equiv \Phi_m(x)^{p^{s-1}(p-1)} \text{ or } \Phi_m(x)^{p^s} \bmod p.$$

We can see from Theorem 1 and the above that the ideal of $\mathbb{Z}[x]$ generated by $\Phi_m(x), \Phi_n(x)$ $(m < n)$ can be calculated as follows:

$$(\Phi_m(x), \Phi_n(x)) = \begin{cases} (p, \Phi_m(x)) & \text{if } m|n \text{ and } \frac{n}{m} \text{ is a power of a prime } p, \\ \mathbb{Z}[x] & \text{otherwise.} \end{cases}$$

The first part is an alternative proof of Proposition 1.

In the remainder of this paper, we consider our problem about $x^n - 1$ and $\Phi_m(x)$.

Theorem 2. *Let m_0 be the product of distinct prime divisors of m. If m_0 is not a divisor of n, then there exist $u(x), v(x) \in \mathbb{Z}[x]$ such that*

$$(x^n - 1)u(x) + \Phi_m(x)v(x) = \prod_{d|(m_0,n)} \Phi_{\frac{m_0}{d}}(1).$$

Proof. We may assume that $m = m_0$ from

$$\Phi_m(x) = \Phi_{m_0}(x^{\frac{m}{m_0}}) \text{ and } (x^{\frac{m}{m_0}})^n - 1 = (x^n - 1) \cdot \frac{(x^n)^{\frac{m}{m_0}} - 1}{x^n - 1}.$$

We assume d is a divisor of n. If d is not a divisor of m, there exist $u_d(x), v_d(x) \in \mathbb{Z}[x]$ from Theorem 1 (1) such that

$$\Phi_d(x)u_d(x) + \Phi_m(x)v_d(x) = 1.$$

If d is a divisor of m, there exist $u_d(x), v_d(x) \in \mathbb{Z}[x]$ from Theorem 1 (2) such that

$$\Phi_d(x)u_d(x) + \Phi_m(x)v_d(x) = \Phi_{\frac{m}{d}}(1).$$

Thus we have from $x^n - 1 = \prod_{d|n} \Phi_d(x)$,

$$(x^n - 1)u(x) + \Phi_m(x)v(x) = \prod_{d|(m,n)} \Phi_{\frac{m}{d}}(1).$$

Theorem 3 (Marciniak and Sehgal [3]). *Let m_0 be the product of distinct prime divisors of m. If $t = \frac{m_0}{(n,m_0)} > 1$ is not a prime, there exist integral polynomials $u(x),\ v(x) \in \mathbb{Z}[x]$ such that*

$$\Phi_m(x)u(x) + (x^n - 1)v(x) = 1.$$

Proof. We may assume $m = m_0$ from the same reason in Theorem 2.
If t is not a prime, we have $\Phi_{\frac{m}{d}}(1) = 1$ for all $d|(m,n)$ because $\frac{m}{d} = \frac{m}{(m,d)}$ is not a prime since $t = \frac{m}{(m,n)}$ is a divisor of $\frac{m}{(m,d)} = \frac{m}{d}$.

Remark 2. If t is a prime p, then we have

$$\Phi_m(x)u(x) + (x^n - 1)v(x) = \Phi_t(1) = p.$$

References

[1] C. W. Curtis and I. Reiner, Representation theory of finite groups and associative algebras, 1962, Interscience, New York.
[2] R. Lidl and H. Niederreiter, Finite fields, 1983, Addison Wesley.
[3] Z. Marciniak and S. K. Sehgal, Generic units in abelian group rings, J. Group Theory, to appear.
[4] K. Yamauchi, The construction of units of infinite order in the character ring of a finite group, Yokohama Math. J. **51** (2005), 89-97.

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