Sekiguchi, K.
Osaka J. Math.
18 (1981), 755–765

THE GROUP OF UNITS OF THE INTEGRAL GROUP RING OF A METACYCLIC GROUP

KATSUSUKE SEKIGUCHI

(Received February 6, 1980)

We denote by $U(\Lambda)$ the group of units of a ring Λ. Let G be a finite group and let $\boldsymbol{Z}G$ be its integral group ring. Define $V(\boldsymbol{Z}G)=\{u\in U(\boldsymbol{Z}G)\mid \varepsilon(u)=1\}$ where ε denotes the augmentation map of $\boldsymbol{Z}G$. In this paper we will study the following

Problem. *Is there a torsion-free normal subgroup F of $V(\boldsymbol{Z}G)$ such that $V(\boldsymbol{Z}G)=F\cdot G$?*

Denote by S_n the symmetric group on n symbols, by D_n the dihedral group of order $2n$ and by C_n the cyclic group of order n. The problem has been solved affirmatively in each of the following cases:

(1) G an abelian group (Higman [4]),

(2) $G=S_3$ (Dennis [2]),

(3) $G=D_n$, n odd (Miyata [5]) or

(4) G a metabelian group such that the exponent of G/G' is 1, 2, 3, 4 or 6 where G' is the commutator subgroup of G ([7]).

The purpose of this paper is to solve the problem for a class of metacyclic groups. Our main result is the following

Theorem. *Let $G=C_n\cdot C_q$ be the semidirect product of C_n by C_q such that $(n,q)=1$, q odd, and C_q acts faithfully on each Sylow subgroup of C_n. Then there exists a torsion-free normal subgroup F of $V(\boldsymbol{Z}G)$ such that $V(\boldsymbol{Z}G)=F\cdot G$.*

1. Lemmas

We begin with

Lemma 1.1. *Let r, k, n be non negative integers and h be a positive integer. Then*

(1) $\sum_{r=0}^{n}(r+1)\cdots(r+k)=(n+1)\cdots(n+k+1)/(k+1)$, *and*

(2) $$\sum_{r=0}^{n}r^h(r+1)\cdots(r+k)=\frac{n(n+1)\cdots(n+k+1)f(n,k,h)}{(k+2)\cdots(k+h+1)},$$

where $f(n,k,h)$ is a polynomial with respect to n, k and h whose coefficients are in $\boldsymbol{Z}$, and its degree with respect to n is $h-1$. (Notation: $deg_n f(n,k,h)=h-1$)

Proof. (1) is well known. (2) is also known for $h=1$. In fact, we have

$$\sum_{r=0}^{n} r(r+1)\cdots(r+k)=n(n+1)\cdots(n+k+1)/(k+2).$$

For $h\geqq 2$ (2), can be shown by induction on h.

For integers a, b such that $a>0$, $b\geqq 0$ and $a\geqq b$, we denote by $\binom{a}{b}$ the binomial coefficient. We extend this notation formally to the case where $0\leqq a<b$ as $\binom{a}{b}=0$ and set $\binom{0}{0}=1$. Let $\boldsymbol{N}=\{x\in\boldsymbol{Z}\,|\,x>0\}$ and $\bar{\boldsymbol{N}}=\boldsymbol{N}\cup\{0\}$.

For $(t, k_{t+1}, u_1, \cdots, u_t, w_1, \cdots, w_t)\in\boldsymbol{N}\times\bar{\boldsymbol{N}}^{2t+1}$, define

$$B_{t,k_{t+1},u_1,\cdots,w_t}=\sum_{k_t=0}^{k_{t+1}}\binom{k_t}{u_t}\binom{k_t}{w_t}\left(\sum_{k_{t-1}=0}^{k_t}\binom{k_{t-1}}{u_{t-1}}\binom{k_{t-1}}{w_{t-1}}\left(\cdots\left(\sum_{k_2=0}^{k_3}\binom{k_2}{u_2}\binom{k_2}{w_2}\left(\sum_{k_1=0}^{k_2}\binom{k_1}{u_1}\binom{k_1}{w_1}\right)\right)\cdots\right)\right).$$

For simplicity we write $B_t=B_{t,k_{t+1},u_1,\cdots,w_t}$.

Lemma 1.2. *Let s be a positive integer, and let u_i, w_j, $1\leqq i, j\leqq s$, be non negative integers.*

(1) *Suppose that there exists s_0, $1\leqq s_0\leqq s$, such that $u_i+w_i=0$ for any i, $1\leqq i\leqq s_0$, and $u_{s_0+1}+w_{s_0+1}\geqq 1$. Then*

$$B_t=\begin{cases}(k_{t+1}+1)\cdots(k_{t+1}+t)/t! & \text{if } t\leqq s_0\\ \dfrac{k_{t+1}(k_{t+1}+1)\cdots(k_{t+1}+t)f_{t+1}(k_{t+1})}{(\prod_{i=1}^{t}u_i!w_i!)s_0!(s_0+2)\cdots(\sum_{i=1}^{s_0+1}(u_i+w_i)+s_0+1)\cdots(t+1)\cdots(\sum_{i=1}^{t}(u_i+w_i)+t)} & \text{if } s_0+1\leqq t\leqq s\end{cases}$$

where $f_{t+1}(k_{t+1})$ is a polynomial with respect to k_{t+1} whose coefficients are in $\boldsymbol{Z}$, and $deg_{k_{t+1}} f_{t+1}(k_{t+1})=\sum_{i=1}^{t}(u_i+w_i)-1$.

(2) *Suppose that $u_1+w_1\geqq 1$. Then*

$$B_t=\left\{\frac{k_{t+1}(k_{t+1}+1)\cdots(k_{t+1}+t)f_{t+1}(k_{t+1})}{(\prod_{i=1}^{t}u_i!w_i!)2\cdots(\sum_{i=1}^{1}(u_i+w_i)+1)\cdots(t+1)\cdots(\sum_{i=1}^{t}(u_i+w_i)+t)}\right.\quad \text{for } 1\leqq t\leqq s$$

where $f_{t+1}(k_{t+1})$ is a polynomial with respect to k_{t+1} whose coefficients are in $\boldsymbol{Z}$, and $deg_{k_{t+1}} f_{t+1}(k_{t+1})=\sum_{i=1}^{t}(u_i+w_i)-1$.

Proof. (1) We use the induction on t. First, assume that $t\leqq s_0$. If $t=1$, the assertion is clearly valid. Suppose that the following equality holds:

$$B_t = (k_{t+1}+1) \cdots (k_{t+1}+t)/t!\,.$$

Since $B_{t+1}=\sum_{k_{t+1}=0}^{k_{t+2}} B_t$, $B_{t+1}=(k_{t+2}+1)\cdots(k_{t+2}+t+1)/(t+1)!$ by (1.1), as desired. In particular, $B_{s_0}=(k_{s_0+1}+1)\cdots(k_{s_0+1}+s_0)/s_0!$.

Next, we will consider the case where $t>s_0$.

Since $B_{s_0+1}=\sum_{k_{s_0+1}=0}^{k_{s_0+2}} \binom{k_{s_0+1}}{u_{s_0+1}}\binom{k_{s_0+1}}{w_{s_0+1}} B_{s_0}$, we have

$$B_{s_0+1} = \frac{1}{s_0!\,u_{s_0+1}!\,w_{s_0+1}!} \sum_{k_{s_0+1}=0}^{k_{s_0+2}} k_{s_0+1}(k_{s_0+1}+1) \cdots (k_{s_0+1}+s_0) g_{s_0+1}(k_{s_0+1})$$

for some $g_{s_0+1}(k_{s_0+1})$ with $\deg_{k_{s_0+1}} g_{s_0+1}(k_{s_0+1})=u_{s_0+1}+w_{s_0+1}-1$. Hence, by (1.1),

$$B_{s_0+1} = \frac{1}{s_0!\,u_{s_0+1}!\,w_{s_0+1}!} \cdot \frac{k_{s_0+2}(k_{s_0+2}+1) \cdots (k_{s_0+2}+s_0+1) f_{s_0+2}(k_{s_0+2})}{(s_0+2) \cdots (u_{s_0+1}+w_{s_0+1}+s_0+1)}$$

for some $f_{s_0+2}(k_{s_0+2})$ with $\deg_{k_{s_0+2}} f_{s_0+2}(k_{s_0+2})=u_{s_0+1}+w_{s_0+1}-1$. Suppose that the following equality holds:

$$B_t = \frac{k_{t+1}(k_{t+1}+1) \cdots (k_{t+1}+t) f_{t+1}(k_{t+1})}{(\prod_{i=1}^{t} u_i!\,w_i!) s_0!(s_0+2) \cdots (u_{s_0+1}+w_{s_0+1}+s_0+1) \cdots (t+1) \cdots (\sum_{i=1}^{t}(u_i+w_i)+t)}$$

for some $f_{t+1}(k_{t+1})$ with $\deg_{k_{t+1}} f_{t+1}(k_{t+1})=\sum_{i=1}^{t}(u_i+w_i)-1$. Then

$$B_{t+1} = \sum_{k_{t+1}=0}^{k_{t+2}} \binom{k_{t+1}}{u_{t+1}}\binom{k_{t+1}}{w_{t+1}} B_t =$$

$$\frac{1}{(\prod_{i=1}^{t+1} u_i!\,w_i!) s_0!(s_0+2) \cdots (\sum_{i=1}^{t}(u_i+w_i)+t)} \sum_{k_{t+1}=0}^{k_{t+2}} k_{t+1}(k_{t+1}+1) \cdots (k_{t+1}+t) g_{t+1}(k_{t+1})$$

for some $g_{t+1}(k_{t+1})$ with $\deg_{k_{t+1}} g_{t+1}(k_{t+1})=\sum_{i=1}^{t+1}(u_i+w_i)-1$. Hence

$$B_{t+1} = \frac{k_{t+2}(k_{t+2}+1) \cdots (k_{t+2}+t+1) f_{t+2}(k_{t+2})}{(\prod_{i=1}^{t+1} u_i!\,w_i!) s_0!(s_0+2) \cdots (t+2) \cdots (\sum_{i=1}^{t+1}(u_i+w_i)+t+1)}$$

for some $f_{t+2}(k_{t+2})$ with $\deg_{k_{t+2}} f_{t+2}(k_{t+2})=\sum_{i=1}^{t+1}(u_i+w_i)-1$, as desired.

(2) The proof can be done in the same way as in (1), hence we omit it.

Let q be an odd positive integer and let Γ be a commutative ring. Set $(q+1)/2=s$. For a non negative integer i, we define the subset L_i of $\boldsymbol{Z}\times\boldsymbol{Z}$ as follows:

$$L_i = \begin{cases} \left\{\begin{matrix}(1, 1+i), \cdots, (s-i, s), (s-i, s+1), \cdots, (s, s+i+1), \\ (s+1, s+i+1), \cdots\cdots\cdots, (q-i, q)\end{matrix}\right\} & \text{if } 1 \leqq i \leqq s-2, \\ \{(1, s), (1, s+1), \cdots\cdots\cdots, (s-1, q)\} & \text{if } i = s-1 \\ \{(1, i+2), (2, i+3), \cdots\cdots\cdots, (q-i-1, q)\} & \text{if } s \leqq i \leqq q-2, \\ \phi & \text{if } q-1 \leqq i \\ \{(k, h)\}_{1 \leqq k, h \leqq q} \setminus \bigcup_{i=1}^{q-2} L_i & \text{if } i = 0. \end{cases}$$

For each L_i, define $W_i(q, \Gamma) = \{(x_{k,h}) \in M_q(\Gamma) \mid x_{c,d} = 0 \text{ if } (c,d) \notin L_i\}$ and set $\bar{W}_k(q, \Gamma) = \bigcup_{i \geqq k} W_i(q, \Gamma)$.

Lemma 1.3. *Let i, j be positive integers. Suppose that $X_i \in W_i(q, \Gamma)$ and $Y_j \in W_j(q, \Gamma)$. Then $X_i Y_j \in W_{i+j}(q, \Gamma)$.*

Proof. When $i \geqq (q-1)/2$ or $j \geqq (q-1)/2$, the assertion can easily be verified. Hence we have only to consider the following cases:
Case 1. $i, j < (q-1)/2$ and $i+j < (q-1)/2$.
Case 2. $i, j < (q-1)/2$ and $i+j = (q-1)/2$.
Case 3. $i, j < (q-1)/2$ and $i+j > (q-1)/2$.

Case 1. Denote by $E_{k,h}$ a matrix unit (i.e. $E_{k,h}$ has an entry 1 at position (k,h) and zero elsewhere). Set $(q+1)/2 = s$ and write

$$\begin{aligned} X_i = {} & x_1 E_{1,1+i} + x_2 E_{2,2+i} + \cdots + x_{s-i} E_{s-i,s} + x_{s-i+1} E_{s-i,s+1} + \cdots \\ & \cdots + x_{s+1} E_{s,s+i+1} + x_{s+2} E_{s+1,s+i+1} + \cdots + x_{q-i+1} E_{q-i,q}, \end{aligned}$$

and

$$\begin{aligned} Y_j = {} & y_1 E_{1,1+j} + y_2 E_{2,2+j} + \cdots + y_{s-j} E_{s-j,s} + y_{s-j+1} E_{s-j,s+1} + \cdots \\ & \cdots + y_{s+1} E_{s,s+j+1} + y_{s+2} E_{s+1,s+j+1} + \cdots + y_{q-j+1} E_{q-j,q}, \text{ where } x_r, y_t \in \Gamma. \end{aligned}$$

Then

$$\begin{aligned} X_i Y_j = {} & x_1 y_{1+i} E_{1,1+i+j} + \cdots + x_{s-i-j} y_{s-j} E_{s-i-j,s} + x_{s-i-j} y_{s-j+1} E_{s-i-j,s+1} \\ & + \cdots + x_{s-i} y_{s+1} E_{s-i,s+j+1} + x_{s-i+1} y_{s+2} E_{s-i,s+j+1} + \cdots \\ & \cdots + x_{s+1} y_{s+i+2} E_{s,s+i+j+1} + x_{s+2} y_{s+i+2} E_{s+1,s+i+j+1} + \cdots \\ & \cdots + x_{q-i-j+1} y_{q-j+1} E_{q-i-j,q}. \end{aligned}$$

Therefore $X_i Y_j \in W_{i+j}(q, \Gamma)$.

The assertion in Case 2 and Case 3 can be proved in the same way as in Case 1, and therefore we omit them.

Let X be an arbitrary element in $M_q(\Gamma)$. Since $W_i(q, \Gamma) \cap W_j(q, \Gamma) = \{0\}$ for $i \neq j$, X can be expressed uniquely as follows:

$$X = X_0 + X_1 + \cdots + X_{q-2}, \text{ where } X_i \in W_i(q, \Gamma).$$

We call X_i the i-th component of X.

2. Proof of Theorem

Write $G=C_n\cdot C_q=\langle\sigma,\tau\,|\,\sigma^n=\tau^q=1,\ \tau\sigma\tau^{-1}=\sigma^r\rangle$. Consider the pullback diagram

$$\begin{array}{ccc} \boldsymbol{Z}G & \xrightarrow{h_2} & \boldsymbol{Z}[\tau] \\ {\scriptstyle h_1}\downarrow & & \downarrow{\scriptstyle g_2} \\ \boldsymbol{Z}G/(\Sigma) & \xrightarrow{g_1} & F_n[\tau]\,, \end{array}$$

where $\Sigma=\sum_{i=0}^{n-1}\sigma^i$ and $F_n=\boldsymbol{Z}/n\boldsymbol{Z}$.

Write $S=\boldsymbol{Z}[\sigma]/(\Sigma)$ and $\Lambda=\boldsymbol{Z}G/(\Sigma)$. Define the Λ-homomorphisms

$$f_k\colon S(1-h_1(\sigma))^k\to\Lambda,\quad 0\leqq k\leqq q-1\,,$$

by $s(1-h_1(\sigma))^k\to s\left\{1+\left(\dfrac{1-h_1(\sigma)}{1-h_1(\sigma)^r}\right)^k h_1(\tau)+\cdots+\left(\dfrac{1-h_1(\sigma)}{1-h_1(\sigma)^{r^{q-1}}}\right)^k h_1(\tau)^{q-1}\right\}$, $s\in S$, and set $f=f_0+\cdots+f_{q-1}\colon S\oplus\cdots\oplus S(1-h_1(\sigma))^{q-1}\to\Lambda$. Then f is a Λ-isomorphism ([3, Lemma 3.3]).

For a module M over a group H, we define $M^H=\{x\in M\,|\,hx=x \text{ for any } h\in H\}$. Set $R=S^{\langle\tau\rangle}$, $P_0=(1-h_1(\sigma))S$ and $P=P_0\cap R$. Then

$$\Lambda\cong\begin{pmatrix} R & \cdot & \cdot & \cdot & R \\ P & \cdot & & & \cdot \\ \cdot & \cdot & \cdot & & \cdot \\ \cdot & & \cdot & \cdot & \cdot \\ P & \cdot & \cdot & P & R \end{pmatrix}(\subseteqq M_q(R))$$

as R-algebras ([3, Proposition 3.4]). This isomorphism is the composite or the following two isomorphisms:

$$\varphi\colon\Lambda\to\mathrm{End}_\Lambda(\Lambda)^\circ,\quad\text{where }\ \varphi(u)(\lambda)=\lambda u,\ u,\lambda\in\Lambda\,,$$

and

$$\begin{aligned}\psi\colon \mathrm{End}_\Lambda(\Lambda)^\circ &\cong \mathrm{End}_\Lambda(S\oplus S(1-h_1(\sigma))\oplus\cdots\oplus S(1-h_1(\sigma))^{q-1})^\circ \\ &\cong\Big\{\bigoplus_{0\leqq i,j\leqq q-1}\mathrm{Hom}_\Lambda(S(1-h_1(\sigma))^i,\ S(1-h_1(\sigma))^j)\Big\}^\circ \\ &\cong\begin{pmatrix} R & \cdot & \cdot & \cdot & R \\ P & \cdot & & & \cdot \\ \cdot & \cdot & \cdot & & \cdot \\ \cdot & & \cdot & \cdot & \cdot \\ P & \cdot & \cdot & P & R \end{pmatrix}.\end{aligned}$$

Here, $\mathrm{End}_\Lambda(\Lambda)^\circ$ denotes the opposite ring of $\mathrm{End}_\Lambda(\Lambda)$.
Write

$$\Delta = \begin{pmatrix} R & \cdot & \cdot & \cdot & R \\ P & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & & \cdot \\ \cdot & & \cdot & \cdot & \cdot \\ P & \cdot & \cdot & P & R \end{pmatrix}.$$

For $x \in \Lambda$, we set $\psi \circ \varphi(x) = (b_{i,j}(x)) \in \Delta$.

We now determine $\bar{b}_{i,i}(h_1(\tau))$, $1 \leqq i \leqq q$, where $\bar{b}_{i,i}(h_1(\tau))$ is the image of $b_{i,i}(h_1(\tau))$ under the map $R \to R/P$. Set

$$x_k = 1 + \left(\frac{1-h_1(\sigma)}{1-h_1(\sigma)^r}\right)^k h_1(\tau) + \cdots + \left(\frac{1-h_1(\sigma)}{1-h_1(\sigma)^{r^{q-1}}}\right)^k h_1(\tau)^{q-1}.$$

Since g_1 is surjective and $\Lambda = Sx_0 + \cdots + Sx_{q-1}$, $F_n[\tau] = F_n g_1(x_0) + \cdots + F_n g_1(x_{q-1})$. Hence $g_1(x_i)$, $0 \leqq i \leqq q-1$, are linearly independent over F_n. Denote by π_k, $0 \leqq k \leqq q-1$, the projection from Λ to Sx_k. Then $\varphi(h_1(\tau)) \circ \pi_k$ is a Λ-homomorphism from Λ to Sx_k. If we put $\varphi(h_1(\tau))(x_k) = a_0 x_0 + \cdots + a_{q-1} x_{q-1}$, $a_i \in S$, $(\varphi(h_1(\tau)) \circ \pi_k)(x_k) = \pi_k(\varphi(h_1(\tau))(x_k)) = a_k x_k$. Hence $a_k \in R$ and so $g_1(a_k) = \bar{b}_{k+1,k+1}(h_1(\tau))$, by the definition of ψ. We have $g_1(\varphi(h_1(\tau))(x_k)) = g_1(x_k h_1(\tau)) = g_1(a_0) g_1(x_0) + \cdots\cdots \cdots\cdots + g_1(a_{q-1}) g_1(x_{q-1})$ in $F_n[\tau]$.
Write this equality explicitly as follows:

$$\begin{aligned} & r^{-(q-1)k} + \tau + r^{-k}\tau^2 + \cdots\cdots\cdots + r^{-(q-2)k}\tau^{q-1} \\ = {} & g_1(a_0)(1 + \tau + \tau^2 + \cdots\cdots\cdots + \tau^{q-1}) \\ + {} & \cdots\cdots \\ & \cdots\cdots\cdots \\ + {} & g_1(a_k)(1 + r^{-k}\tau + r^{-2k}\tau^2 + \cdots\cdots\cdots + r^{-(q-1)k}\tau^{q-1}) \\ & \cdots\cdots\cdots \\ + {} & g_1(a_{q-1})(1 + r^{-(q-1)}\tau + r^{-2(q-1)}\tau^2 + \cdots\cdots + r^{-(q-1)^2}\tau^{q-1}). \end{aligned}$$

Since $g_1(x_i)$, $0 \leqq i \leqq q-1$, are linearly independent over F_n, $(g_1(a_0), \cdots, g_1(a_{q-1}))$ is uniquely determined. If we set $g_1(a_k) = r^k$ and $g_1(a_j) = 0$ for every j, $j \neq k$, then this satisfies the equality. Thus we have $\bar{b}_{k+1,k+1}(h_1(\tau)) = g_1(a_k) = r^k$.

By a similar argument, we see that $\bar{b}_{i,i}(h_1(\sigma)) = 1$, $1 \leqq i \leqq q$.

Define a ring isomorphism $\Phi\colon F_n[\tau] \to F_n^q$ by $\tau \to (1, r, \cdots, r^{q-1})$, Further define $\Psi\colon \Delta \to F_n^q$ by $(b_{i,j}) \to (\bar{b}_{1,1}, \cdots, \bar{b}_{q,q})$. Then the following diagram is commutative:

$$
\begin{array}{ccc}
ZG & \xrightarrow{h_2} & Z[\tau] \\
{\scriptstyle h_1}\downarrow & & \downarrow{\scriptstyle g_2} \\
\Lambda & \xrightarrow{g_1} & F_n[\tau] \\
{\scriptstyle \psi\circ\varphi}\downarrow & & \downarrow{\scriptstyle \Phi} \\
\Delta & \xrightarrow{\Psi} & F_n^q .
\end{array}
\tag{2.1}
$$

Let ι be the involution of $Z[\tau]$ defined by $\iota(\tau^i)=\tau^{-i}$, $0\leqq i\leqq q-1$. Since q is odd, by virture of [6, Remark 2.7], $U(Z[\tau])=\pm\langle\tau\rangle\times V([Z[\tau]]^{\langle\iota\rangle})$ where $V([Z[\tau]]^{\langle\iota\rangle})=U([Z[\tau]]^{\langle\iota\rangle})\cap V(Z[\tau])$. Let $u\in V([Z[\tau]]^{\langle\iota\rangle})$. If we write $\Phi\circ g_2(u)=(u_1,\cdots,u_q)$, then, by the definition of Φ, $u_{(q+1)/2}=u_{(q+3)/2}$. The theorem of Higman ([4]) shows that $V([Z[\tau]]^{\langle\iota\rangle})$ is torsion-free. It is easy to see that $g_1(U(\Lambda))\supseteqq g_2(U(Z[\tau]))$ and $g_2(U(Z[\tau]))=\pm\langle\tau\rangle\times g_2(V([Z[\tau]]^{\langle\iota\rangle}))$. Define

$$F_1=\{(b_{i,j})\in U(\Delta)\,|\,\bar{b}_{(q+1)/2,(q+3)/2}=0\}\cap\Psi^{-1}(\Phi\circ g_2(V([Z[\tau]]^{\langle\iota\rangle}))) .$$

Then F_1 is contained in the subgroup $\{(d_{i,j})\in U(\Delta)\,|\,\bar{d}_{(q+1)/2,(q+3)/2}=0$ and $\bar{d}_{(q+1)/2,(q+1)/2}=\bar{d}_{(q+3)/2,(q+3)/2}\}$.

We now show that F_1 is a normal subgroup of $U(\Delta)$. Let $Y=(a_{i,j})\in U(\Delta)$. If we write $Y^{-1}=(c_{i,j})$, then $a_{(q+1)/2,(q+1)/2}\cdot c_{(q+1)/2,(q+1)/2}\equiv 1 \pmod P$, $a_{(q+3)/2,(q+3)/2}\cdot c_{(q+3)/2,(q+3)/2}\equiv 1 \pmod P$ and $a_{(q+1)/2,(q+1)/2}\cdot c_{(q+1)/2,(q+3)/2}+a_{(q+1)/2,(q+3)/2}\cdot c_{(q+3)/2,(q+3)/2}\equiv 0 \pmod P$. Let $X=(b_{i,j})\in F_1$ and write $YXY^{-1}=(z_{i,j})$. Then, by a direct calculation, $z_{i,i}\equiv b_{i,i} \pmod P$, $1\leqq i\leqq q$, and $z_{(q+1)/2,(q+3)/2}\equiv 0 \pmod P$. Hence F_1 is a normal subgroup of $U(\Delta)$. Define $F_2=\{(b_{i,j})\in F_1\,|\,\bar{b}_{i,i}=1,\ 1\leqq i\leqq q\}$.

Proposition 2.2. *F_2 is torsion-free.*

Proof. Step 1. Reduction to the case where n is a prime. By the same way as in [5, Proposition 1.3], we can show that $F_3=\{X\in F_2\,|\,X\equiv E \pmod P\}$ is torsion-free. Hence it suffices to show that every element in $F_2\backslash F_3$ is of infinite order.

Let $n=p_1^{e_1}\cdots p_t^{e_t}$ be the prime decomposition of n. Denote by Φ_m the m-th cyclotomic polynomial. Further, we denote by η_i, $1\leqq i\leqq t$, (resp. $\eta_{i,j}$, $1\leqq i\leqq t$, $1\leqq j\leqq e_i$) the natural maps $Z[\sigma]\to Z[\sigma]/(\prod_{j=1}^{e_i}\Phi_{p_i^j}(\sigma))$ (resp. $Z[\sigma]\to Z[\sigma]/(\Phi_{p_i^j}(\sigma))$). Write $Z[\sigma]/(\prod_{j=1}^{e_i}\Phi_{p_i^j}(\sigma))=S(p_i)$ and $Z[\sigma]/(\Phi_{p_i^j}(\sigma))=S(p_i,j)$. Set $S(p_i)^{\langle T\rangle}=R(p_i)$, $R(p_i)\cap(1-\eta_i(\sigma))S(p_i)=P(p_i)$, $S(p_i,j)^{\langle T\rangle}=R(p_i,j)$ and $R(p_i,j)\cap(1-\eta_{i,j}(\sigma))S(p_i,j)=P(p_i,j)$. Note that $R/P\cong F_n$. Consider the natural maps:

$$T_{p_k}\colon M_q(R)\to M_q(R(p_k)),\ 1\leqq k\leqq t .$$

If we take $(a_{i,j})\in F_2\backslash F_3$, then there exists $p_h\in\{p_1,\cdots,p_t\}$ such that $T_{p_h}((a_{i,j}))\not\equiv E$

(mod $P(p_h)$). For each $a_{i,j}$, $1\leqq i<j\leqq q$, we can take $m_{i,j}\in\{0,\cdots,n-1\}$ such that $a_{i,j}\equiv m_{i,j}$ (mod P). Write $m_{i,j}=p_h^{c_{i,j}}m'_{i,j}$, $p_h\nmid m'_{i,j}$, and set $c=Min\{c_{i,j}\,|\,1\leqq i<j\leqq q\}$. Further, let

$$\Psi_{p_h}\colon M_q(R(p_h))\to M_q(R(p_h,1))\oplus\cdots\oplus M_q(R(p_h,e_h))$$

be the natural injection, and let

$$\pi_d\colon M_q(R(p_h,1))\oplus\cdots\oplus M_q(R(p_h,e_h))\to M_q(R(p_h,d)),\ 1\leqq d\leqq e_h$$

be the projections.
Suppose that $1\leqq c$. Then $(\pi_d\circ\Psi_{p_h}\circ T_{p_h})((a_{i,j}))\equiv E$ (mod $P(p_h,d)$), $1\leqq d\leqq e_h$, and hence $(a_{i,j})$ is of infinite order.

Next, suppose that $c=0$. Then $(\pi_1\circ\Psi_{p_h}\circ T_{p_h})((a_{i,j}))\not\equiv E$ (mod $P(p_h,1)$), and hence, if we can show the assertion in the case where n is a prime, the proof is completed.

Step 2. The case where $n=p$ a prime.

Take an element B of F_2. Then $B\equiv X$ (mod P) for some X whose entries are in $\{0,\cdots,p-1\}$. By the definition of F_2, $X\in GL(q,\boldsymbol{Z})$. Write $B=X+P^eA$ where $A\in M_q(R)$ and $e\geqq 1$. Further, set $X=E+X_1+\cdots+X_{q-2}$ (resp. $X^{-1}=E+Y_1+\cdots+Y_{q-2}$) where X_i (resp. Y_i) is the i-th component of X (resp. Y). It is easy to see that $Y_1=-X_1$. We write $A^{(k)}=X^{-k}AX^k$. Then

$$\begin{aligned}B^p&=(X+P^eA)^p=X^p+\sum_{t=1}^{p}\Big(P^{te}\Big(\sum_{i_1+\cdots+i_{t+1}=p-t,\,i_1,\cdot,i_{t+1}\geqq 0}X^{i_1}AX^{i_2}\cdots X^{i_t}AX^{i_{t+1}}\Big)\Big)\\&=X^p+\sum_{t=1}^{p}\Big(P^{te}X^{p-t}\Big(\sum_{p-t\geqq k_t\geqq\cdots\geqq k_1\geqq 0}A^{(k_t)}\cdots A^{(k_1)}\Big)\Big)\\&=X^p+\sum_{t=1}^{p}\Big(P^{te}X^{p-t}\Big(\sum_{k_t=0}^{p-t}A^{(k_t)}\Big(\sum_{k_{t-1}=0}^{k_t}A^{(k_{t-1})}\Big(\cdots\Big(\sum_{k_2=0}^{k_3}A^{(k_2)}\Big(\sum_{k_1=0}^{k_2}A^{(k_1)}\Big)\Big)\cdots\Big)\,.\end{aligned}$$

Set $X^p=E+\tilde{X}_1+\cdots+\tilde{X}_{q-2}$ where $\tilde{X}_i$ is the i-th component of X^p. Then, by (1.3), $\tilde{X}_i=\sum_{t=1}^{i}\left(\binom{p}{t}\sum_{i_1+\cdots+i_t=i}X_{i_1}\cdots X_{i_t}\right)$, and hence $X^p\equiv E$ (mod p). Therefore $B^p\equiv E$ (mod P). Thus, if B is of finite order, B^p must be equal to E. Suppose that there exists $B=X+P^eA\in F_2$ such that $B^p=E$ and $B\neq E$. Set $S_i=\sum_{1\leqq h_1,\cdots,h_i\leqq q-2}Y_{h_1}\cdots Y_{h_i}$, $T_i=\sum_{1\leqq h_1,\cdots,h_i\leqq q-2}X_{h_1}\cdots X_{h_i}$ and $S_0=T_0=E$. Since $X^k=(E+X_1+\cdots+X_{q-2})^k=E+\binom{k}{1}T_1+\cdots+\binom{k}{k}T_k$ and $X^{-k}=(E+Y_1+\cdots+Y_{q-2})^k=E+\binom{k}{1}S_1+\cdots+\binom{k}{k}S_k$, $A^{(k)}=X^{-k}AX^k=\sum_{0\leqq u,w\leqq k}\binom{k}{u}\binom{k}{w}S_uAT_w$. Since $S_i, T_i\in\overline{W}_i(q,\boldsymbol{Z})$ by (1.3), $S_i=T_i=0$ for $i\geqq q-1$. Therefore we may write $A^{(k)}=\sum_{0\leqq u,w\leqq q-2}\binom{k}{u}\binom{k}{w}S_uAT_w$.

Hence, if we write (*) $\sum_{p-t\geqq k_t\geqq\cdots\geqq k_1\geqq 0} A^{(k_t)}\cdots A^{(k_1)}=\sum_{0\leqq u_i, w_j\leqq q-2} a_{u_tw_t\cdots u_1w_1}S_{u_t}AT_{w_t}\cdots S_{u_1}$ AT_{w_1}, then $a_{u_tw_t\cdots u_1w_1}=\sum_{k_t=0}^{p-t}\binom{k_t}{u_t}\binom{k_t}{w_t}\left(\sum_{k_{t-1}=0}^{k_t}\binom{k_{t-1}}{u_{t-1}}\binom{k_{t-1}}{w_{t-1}}\left(\cdots\left(\sum_{k_1=0}^{k_2}\binom{k_1}{u_1}\binom{k_1}{w_1}\right)\cdots\right)\right)$.

Set $(X+P^eA)^p=X^p+H$.

We now show that the 1-st component of H is divisible by pP^e. If we write $(p-1)/q=t_0$, $P^{t_0}=p$. Suppose that $t>t_0$, then $P^{et_0}=p^e\mid P^{te}$, and so for such t, $pP^e\mid P^{te}X^{p-t}(\sum_{p-t\geqq\cdots\geqq k_1\geqq 0} A^{(k_t)}\cdots A^{(k_1)})$. On the other hand, by (1.2), $a_{u_tw_t\cdots u_1w_1}$ is divisible by p if $\sum_{i=1}^{t}(u_i+w_i)+t<p$. Hence we have only to consider the case where $t\leqq t_0$ and $\sum_{i=1}^{t}(u_i+w_i)+t\geqq p$.

We show that the 0-th and 1-st components of $S_{u_t}AT_{w_t}\cdots S_{u_1}AT_{w_1}$ are 0, if $t\leqq t_0$ and $\sum_{i=1}^{t}(u_i+w_i)+t\geqq p$.

Case 1. $u_t+w_1\geqq q+1$. Suppose that $u_t\geqq(q+1)/2$. Write $S_{u_t}=(x(u_t)_{i,j})$ and $T_{w_1}=(x(w_1)_{i,j})$. Then $x(u_t)_{i,j}=0$ for $i\geqq q-u_t$ and $x(w_1)_{i,j}=0$ for $j\leqq w_1$ because $S_{u_t}\in\bar{W}_{u_t}(q,R)$ and $T_{w_1}\in\bar{W}_{w_1}(q,R)$. Hence, if we write $S_{u_t}AT_{w_t}\cdots S_{u_1}AT_{w_1}=(x_{i,j})$, $x_{i,j}=0$ whenever $i\geqq q-u_t$ or $j\leqq w_1$. Since $u_t+w_1\geqq q+1$, the 0-th and 1-st components of $(x_{i,j})$ are 0. The proof in the case $w_1\geqq(q+1)/2$ is similar to that in the case $u_t\geqq(q+1)/2$, so, we omit it.

Case 2. $u_t+w_1\leqq q$. Suppose that there exists $i\in\{1,\cdots,t-1\}$ such that $q-w_{i+1}\leqq u_i$. Then $T_{w_{i+1}}S_{u_i}=0$, and hence $S_{u_t}AT_{w_t}\cdots S_{u_1}AT_{w_1}=0$. Therefore we have only to consider the case where $q-w_{i+1}>u_i$ for each i, $1\leqq i\leqq t-1$. Further it is easy to see that $T_{w_{i+1}}S_{u_i}=0$ if $w_{i+1}+u_i=q-1$. Hence, we may assume that $q-2\geqq w_{i+1}+u_i$, $1\leqq i\leqq t-1$, But in this case

$$\sum_{i=1}^{t}(u_i+w_i)=u_t+w_1+\sum_{i=1}^{t-1}(w_{i+1}+u_i)\leqq q+(q-2)(t-1)\leqq t_0(q-2)+2\,.$$

On the other hand,

$$\sum_{i=1}^{t}(u_i+w_i)\geqq p-t=qt_0+1-t\,.$$

Therefore

$$qt_0+1-t\leqq\sum_{i=1}^{t}(u_i+w_i)\leqq t_0(q-2)+2\,.$$

This is impossible because $t\leqq t_0$ and $t_0\neq 1$.

Hence the 0-th and 1-st components of $S_{u_t}AT_{w_t}\cdots S_{u_1}AT_{w_1}$ are 0, and so the 1-st component of $X^{p-t}S_{u_t}AT_{w_t}\cdots S_{u_1}AT_{w_1}$ is 0.

Thus we conclude that the 1-st component of H is divisible by pP^e.

On the other hand, the 1-st component of X^p is pX_1. Since every entry in X_1 is in $\{0,\cdots,p-1\}$, X_1 must be equal to 0. Hence $Y_1=-X_1=0$. Therefore, if $i\geqq(q-1)/2$, $S_i=T_i=0$ because S_i, $T_i\in\bar{W}_i(q,R)$. Thus, if $S_{u_t}AT_{w_t}\cdots S_{u_1}AT_{w_1}\neq 0$, then we must have u_i $w_j\leqq(q-3)/2$ for all u_i, w_j $1\leqq i,j\leqq t$. Suppose that $t\leqq t_0$, then

$$\sum_{i=1}^{t}(u_i+w_i)+t\leqq t(q-2)\leqq t_0(q-2)\lneqq p\,.$$

Hence, for every $S_{u_t}AT_{w_t}\cdots S_{u_1}AT_{w_1}\neq 0$, its coefficient in (*) is divisible by p. Therefore H is divisible by pP^e. As $B^p=X^p+H=E$, $X^p\equiv E \pmod{pP^e}$. However $\tilde{X}_2$ is $pX_2+\binom{p}{2}X_1^2=pX_2$, and so X_2 must be equal to 0. Continuing this procedure, we get $X_i=0$ for any i, $1\leqq i\leqq q-2$. Therefore $X+P^eA\equiv E$ (mod P). This contradicts the fact that B is of finite order. Thus the proof is completed.

Proof of Theorem. Considering the property of the pullback diagram (2.1), we get $[(\psi\circ\varphi\circ h_1)(V(\boldsymbol{Z}G))\colon F_1]=nq$. Therefore, if we set $F=(\psi\circ\varphi\circ h_1)^{-1}(F_1)$, then $V(\boldsymbol{Z}G)\triangleright F$ and $[V(\boldsymbol{Z}G)\colon F]=nq$. Take an element u of F.

Suppose that $(\psi\circ\varphi\circ h_1)(u)=1$. The restriction of h_2 to $(\psi\circ\varphi\circ h_1)^{-1}(1)\cap U(\boldsymbol{Z}G)$ yields a group monomorphism $(\psi\circ\varphi\circ h_1)^{-1}(1)\cap U(\boldsymbol{Z}G)\rightarrow U(\boldsymbol{Z}[\tau])$. However, since $\Phi\circ g_2\circ h_2(u)=1$, $h_2(u)$ is of infinite order by [1, Theorem 3.1], hence so is u.

Suppose next that $1\neq(\psi\circ\varphi\circ h_1)(u)\in F_2$. Then it is of infinite order by (2.2), hence so is u.

Finally, suppose that $(\psi\circ\varphi\circ h_1)(u)\in F_1\backslash F_2$. Then, by the definition of F_1, there exists an element v of $V([\boldsymbol{Z}[\tau]]^{\langle\iota\rangle})$ such that $\Phi\circ g_2(v)=(\Psi\circ\psi\circ\varphi\circ h_1)(u)$. However v is of infinite order, hence so is u. This shows that F is torsion-free. Therefore we get $F\cap G=\{1\}$. Thus F is a torsion-free normal subgroup of $V(\boldsymbol{Z}G)$ such that $V(\boldsymbol{Z}G)=F\cdot G$. This completes the proof.

References

[1] J.A. Cohn and D. Livingstone: *On the structure of group algebras*, I, Canad. J. Math. **17** (1965), 583–593.

[2] R.K. Dennis: *The structure of the unit group of group rings*, Ring theory II, Marcel Dekker, 1977, 103–130.

[3] S. Endo, T. Miyata and K. Sekiguchi: *Picard groups and automorphism groups of integral group rings of metacyclic groups*, to appear.

[4] G. Higman: *The units of group rings*, Proc. London Math. Soc. **46** (1940), 231–248.

[5] T. Miyata: *On the units of the integral group ring of a dihedral group*, to appear in J. Math. Soc. Japan.

[6] ————: *A normal integral basis theorem for dihedral groups*, to appear in Tôhoku Math. J..

[7] K. Sekiguchi: *On the units of integral group rings,* to appear in Tokyo J. Math.

Department of Mathematics
Tokyo Metropolitan University
Fukazawa, Setagaya-ku
Tokyo 158, Japan