J. Korean Math. Soc.
Vol. 20, No. 1, 1983

THE UNIT GROUP OF THE INTEGRAL GROUP RING $\mathbf{Z}D_n$

SEUNG AHN PARK

1. Introduction

The purpose of this paper is to determine the structure of the unit group $U(\mathbf{Z}D_n)$ of the integral group ring $\mathbf{Z}D_n$, where

$$D_n=\langle x,\ y\,|\,x^n=y^2=1,\ \ x^y=x^{-1}\rangle$$

is the dihedral group of order $2n$, $n\geq 3$.

In order to generalize our result we will consider the unit group $U(\mathbf{Z}D)$ of the integral group ring $\mathbf{Z}D$, where the group $D=CY$ is the semidirect product of subgroups C and Y satisfying the following conditions:

(i) C is a finite abelian normal subgroup and $Y=\langle y\,|\,y^2=1\rangle$,
(ii) y inverts every element of C, and
(iii) C has at most one involution.

Note that every element u of $\mathbf{Z}D$ can be uniquely expressed as $u=\alpha+\beta y$ where $\alpha,\beta\in\mathbf{Z}C\subset\mathbf{Z}D$. For each element $\alpha=\sum_{x\in C}a_x x$ of $\mathbf{Z}C$, we set

$$\bar{\alpha}=\sum_{x\in C}a_x x^{-1},\qquad \mathrm{tr}\,\alpha=a_1.$$

The unit group $U(\mathbf{Z}D)$ of the integral group ring $\mathbf{Z}D$ is given by the following theorem.

THEOREM 1. *Let $D=CY$ be the semidirect product of subgroups C and Y satisfying the following conditions*:

(i) *C is an abelian normal subgroup of order n and $Y=\langle y\,|\,y^2=1\rangle$,*
(ii) *y inverts every element of C, and*
(iii) *C has at most one involution.*

Let

$$r=r(D)=\frac{1}{2}(n+1+n_2-2\sum_{d\,|\,n}n_d)$$

where n_d is the number of cyclic subgroups of C of order d.

Then we have

(1) *There exists a system of units $\{\xi_1,\cdots,\xi_r\}$ in $U(\mathbf{Z}C)$ such that*

Received March 1, 1983
*) This research is supported by KOSEF Research Grant.

for each i, $\bar{\xi}_i=\xi_i$ and $\mathrm{tr}\xi_i$ is a positive odd integer, and

$$U(\mathbf{Z}C)=\pm C\times\langle\xi_1,\cdots,\xi_r\rangle$$

where $\langle\xi_1,\cdots\xi_r\rangle$ is a free abelian group of rank r.

(2) *For each i there exists a unit $u_i=\alpha_i+\beta_i y$ in $U(\mathbf{Z}D)$ such that*

$$\alpha_i\bar{\alpha}_i-\beta_i\bar{\beta}_i=\xi_i.$$

Moreover, the unit group $U(\mathbf{Z}D)$ is the semidirect product of subgroups $U_0\langle y\rangle$ and U_1, that is,

$$U(\mathbf{Z}D)=(U_0\langle y\rangle)\,U_1$$

$$U_0\langle y\rangle\lhd U(\mathbf{Z}D),\quad U_0\langle y\rangle\cap U_1=\{1\},$$

where

$$U_0=\{\alpha+\beta y\in\mathbf{Z}D\mid\alpha\bar{\alpha}-\beta\bar{\beta}=1\},\qquad U_1=\langle u_1,\cdots,u_r\rangle$$

and U_1 is a free abelian group of rank r.

The dihedral group $D_n=\langle x, y\mid x^n=y^2=1, x^y=x^{-1}\rangle$ is the semidirect product of subgroups $\langle x\rangle$ and $\langle y\rangle$ satisfying the conditions (i)$-$(iii) in Theorem 1. Thus the unit group $U(\mathbf{Z}D_n)$ of the integral group ring $\mathbf{Z}D_n$ is given by the following theorem, which is the corollary to Theorem 1.

THEOREM 2. *Let*

$$D_n=\langle x, y\mid x^n=y^2=1, x^y=x^{-1}\rangle$$

be the dihedral group of order $2n$, $n\geq 3$, and let

$$r=r(D_n)=\frac{1}{2}\{n+1+n_2-2\tau(n)\}$$

where n_2 is 0 or 1 according as n is odd or even and $\tau(n)$ is the number of all positive divisors of n.

Then the assertions (1) *and* (2) *of* Theorem 1 *hold for $C=\langle x\rangle$ and $D=D_n$.*

It is easy to see that

$$r(D_n)=0 \text{ if and only if } n=3, 4, \text{ or } 6$$

and

$$r(D_n)=1 \text{ if and only if } n=5, 8, \text{ or } 12.$$

In fact the unit groups $U(\mathbf{Z}D_3)$, $U(\mathbf{Z}D_4)$ and $U(\mathbf{Z}D_6)$ have been determined in [2], [5], and [6], respectively. Using Theorem 2, we will explicitly determine the unit groups $U(\mathbf{Z}D_5)$, $U(\mathbf{Z}D_8)$ and $U(\mathbf{Z}D_{12})$ in [4].

The proof of Theorem 1 will be given in section 3.

The terminology and notation in this paper are standard, and they are taken from [3].

By an *involution* we mean an element of order 2 in a group. For elements g, h of a group we set $g^h=h^{-1}gh$, and we say that h *inverts* g if $g^h=g^{-1}$.

2. Necessary lemmas

Let G be a group and let $\mathbf{Z}G$ be the integral group ring of G. For each automorphism σ of G the map $\sigma : \mathbf{Z}G \to \mathbf{Z}G$ defined by

$$\sigma(\sum a_x x) = \sum a_x \sigma(x)$$

is a ring-automorphism of $\mathbf{Z}G$. Thus this defines an action of the automorphism group $\mathrm{Aut}(G)$ on the group ring $\mathbf{Z}G$. More, for any $\sigma \in \mathrm{Aut}(G)$ and any unit α of $\mathbf{Z}G$, the element $\sigma(\alpha)$ is a unit of $\mathbf{Z}G$. Hence the automorphism group $\mathrm{Aut}(G)$ acts on the unit group $U(\mathbf{Z}G)$ of $\mathbf{Z}G$ via this action.

In general, for any homomorphism ρ of a group G into a group H the map $\rho : \mathbf{Z}G \to \mathbf{Z}H$ defined by

$$\rho(\sum a_x x) = \sum a_x \rho(x)$$

is a ring-homomorphism of $\mathbf{Z}G$ into $\mathbf{Z}H$. Moreover, if α is a unit of $\mathbf{Z}G$ then $\rho(\alpha)$ is a unit of $\mathbf{Z}H$. Indeed $\rho(\alpha)$ is a unit of $\mathbf{Z}H$ if and only if it is a unit of $\mathbf{Z}\rho(G)$.

Let C be a finite abelian group. For each element $\alpha = \sum_{x \in C} a_x x$ of $\mathbf{Z}C$ we set

$$\bar{\alpha} = \sum_{x \in C} a_x x^{-1}.$$

Since the map $x \to x^{-1}$ is an automorphism of C, the map $\alpha \to \bar{\alpha}$ is a ring-automorphism of $\mathbf{Z}C$. And α is a unit of $\mathbf{Z}C$ if and only if $\bar{\alpha}$ is a unit of $\mathbf{Z}C$.

Define a map $\mathrm{T} : \mathbf{Z}C \to \mathbf{Z}$ by

$$\mathrm{T}(\sum_{x \in C} a_x x) = \sum_{x \in C} a_x .$$

Then it is easy to prove the following lemma.

(2.1) *The map* $\mathrm{T} : \mathbf{Z}C \to \mathbf{Z}$ *is a ring-homomorphism, and for all* $\alpha \in \mathbf{Z}C$ *we have* $\mathrm{T}(\bar{\alpha}) = \mathrm{T}(\alpha)$.

Moreover, if α *is a unit of* $\mathbf{Z}C$ *then*

$$\mathrm{T}(\alpha) = \mathrm{T}(\alpha^{-1}) = \pm 1.$$

Let $\mathrm{tr} : \mathbf{Z}C \to \mathbf{Z}$ be the *trace* map given by

$$\mathrm{tr}(\sum_{x \in C} a_x x) = a_1.$$

and define an inner product in $\mathbf{Z}C$ by

$$(\alpha, \beta) = \sum_{x \in C} a_x b_x$$

where $\alpha = \sum a_x x$ and $\beta = \sum b_x x$. Then it is easy to see that the following holds (*cf.* [3, p. 33]).

(2. 2) *The map* $\mathrm{tr} : \mathbf{Z}C \to \mathbf{Z}$ *is a* $\mathbf{Z}$*-homomorphism, and for all* $\alpha, \beta \in \mathbf{Z}C$ *we have*

(1) $(\alpha, \beta) = \mathrm{tr}\,\alpha\bar{\beta} = \mathrm{tr}\,\bar{\beta}\alpha$.

(2) $(\alpha, \alpha) = 1$ *if and only if* $\alpha \in \pm C$, *where*

$$\pm C = \{\pm x \mid x \in C\} \subset \mathbf{Z}C.$$

(3) *If* $\alpha = \sum a_x x$, *then for each* $x \in C$

$$\mathrm{tr}(x^{-1}\alpha) = a_x .$$

3. Proof of Theorem

In this section we will prove Theorem 1 by a series of propositions.

Let $D = CY$ be the semidirect product of subgroups C and Y, where C *is an abelian group of order* n *and* $Y = \langle y \mid y^2 = 1 \rangle$, *and* y *inverts every element of* C.

Let

$$r = \frac{1}{2}(n + 1 + n_2 - 2\sum_{d \mid n} n_d)$$

where n_d is the number of cyclic subgroups of C of order d. It is clear that every element u of $\mathbf{Z}D$ can be uniquely expressed as $u = \alpha + \beta y$, where $\alpha, \beta \in \mathbf{Z}C \subset \mathbf{Z}D$. Since y inverts every element of C, we have

$$y\alpha = \bar{\alpha} y$$

for all $\alpha \in \mathbf{Z}C$. Define a map $\mathrm{N} : \mathbf{Z}D \to \mathbf{Z}C$ by

$$\mathrm{N}(\alpha + \beta y) = (\alpha + \beta y)(\bar{\alpha} - \beta y) = \alpha\bar{\alpha} - \beta\bar{\beta}.$$

(3. 1) *The map* $\mathrm{N} : \mathbf{Z}D \to \mathbf{Z}C$ *has the following properties.*

(1) $\mathrm{N}(-u) = \mathrm{N}(u)$ *and* $\overline{\mathrm{N}(u)} = \mathrm{N}(u)$ *for all* $u \in \mathbf{Z}D$.

(2) $\mathrm{N}(uv) = \mathrm{N}(u)\mathrm{N}(v)$ *for all* $u, v \in \mathbf{Z}D$.

Moreover, $\mathrm{N}(x) = 1$ *for all* $x \in C$ *and* $\mathrm{N}(y) = -1$.

(3) *An element* u *of* $\mathbf{Z}D$ *is a unit of* $\mathbf{Z}D$ *if and only if* $\mathrm{N}(u)$ *is a unit of* $\mathbf{Z}C$. *In particular,* $\mathrm{N} : U(\mathbf{Z}D) \to U(\mathbf{Z}C)$ *is a homomorphism of the unit group* $U(\mathbf{Z}D)$ *into the unit group* $U(\mathbf{Z}C)$.

Proof. It is easy to prove (1) and (2).

Let u be a unit of $\mathbf{Z}D$ with inverse v. Then

$$\mathrm{N}(u)\mathrm{N}(v) = \mathrm{N}(uv) = \mathrm{N}(1) = 1$$

by (2), and so $\mathrm{N}(u)$ is a unit of $\mathbf{Z}C$.

Conversely, suppose that $u = \alpha + \beta y$ is an element of $\mathbf{Z}C$ such that $\mathrm{N}(u)$ is a unit of $\mathbf{Z}C$. Since $\mathrm{N}(u) = u \cdot (\bar{\alpha} - \beta y)$, the element u is a unit of $\mathbf{Z}D$ such that

$$u^{-1} = \mathrm{N}(u)^{-1}(\bar{\alpha} - \beta y).$$

Hence the assertion (3) holds.

(3. 2) *For any unit α of $\mathbf{Z}C$, there exists $x\in C$ such that $\bar{\alpha}=x^2\alpha$.*

Proof. Set $\beta=\alpha^{-1}\bar{\alpha}$. Then $\beta\bar{\beta}=1$, and so $(\beta,\beta)=\mathrm{tr}\,\beta\bar{\beta}=1$. This implies that $\beta\in\pm C$, by (2. 2). Moreover, we have

$$\mathrm{T}(\beta)=\mathrm{T}(\alpha^{-1})\mathrm{T}(\bar{\alpha})=\mathrm{T}(\alpha)^2=1$$

by (2. 1). Therefore, there exists $g\in C$ such that $\beta=g$ and $\bar{\alpha}=g\alpha$. Now it suffices to show that $g=x^2$ for some $x\in C$. Let $C^2=\{x^2\,|\,x\in C\}$.

If C is of odd order, then $C=C^2$. Hence $g=x^2$ for some $x\in C$.

Assume that C is of even order. Suppose that $g\notin C^2$ and let $\alpha=\sum a_x x$. Since $\bar{\alpha}=g\alpha$, we have $a_x=a_{(gx)^{-1}}$ for all $x\in C$. On the other hand, $x\neq(gx)^{-1}$ for all $x\in C$, since $g\notin C^2$. Hence it follows that $\mathrm{T}(\alpha)$ is even. But this contradicts to the fact that $\mathrm{T}(\alpha)=\pm 1$. Therefore, $g\in C^2$ and $g=x^2$ for some $x\in C$.

(3. 3) *Let $E=\{t\in C\,|\,t^2=1\}$. Then for any unit α of $\mathbf{Z}C$ with $\bar{\alpha}=\alpha$ there exists an element $t\in E$ such that $\mathrm{tr}(t\alpha)$ is odd.*

Proof. Note that for any $x\in C$ we have

$$x=x^{-1} \text{ if and only if } x\in E.$$

Thus there is a subset P of C such that C is a disjoint union $C=E\cup P\cup P^{-1}$. Since $\bar{\alpha}=\alpha$, the unit α can be expressed as a sum

$$\alpha=\sum_{t\in E} a_t t+\sum_{x\in P} a_x(x+x^{-1}).$$

Now it follows that

$$1\equiv\mathrm{T}(\alpha)=\sum_{t\in E} a_t \pmod 2.$$

If C is of odd order, then $E=\{1\}$. Hence $\mathrm{tr}\,\alpha=a_1$ is odd. If C is of even order, then E is an elementary abelian 2-group of order ≥ 2. Hence there exists an element $t\in E$ such that a_t is odd. Thus $\mathrm{tr}(t\alpha)=a_t$ is odd.

(3. 4) *There exists a system of units $\{\xi_1,\cdots,\xi_r\}$ in $U(\mathbf{Z}C)$ which satisfies the following conditions.*

(i) *For each i, $\bar{\xi}_i=\xi_i$ and $\mathrm{tr}\xi_i$ is a positive odd integer, and*

(ii) *$U(\mathbf{Z}C)=\pm C\times\langle\xi_1,\cdots,\xi_r\rangle$, where $\langle\xi_1,\cdots,\xi_r\rangle$ is a free abelian group of rank r.*

Proof. It is well-known that

$$U(\mathbf{Z}C)=\pm C\times F$$

where $F=\langle\alpha_1,\cdots,\alpha_r\rangle$ is a free abelian group of rank r [1]. By (3. 2), for each α_i there exists $x_i\in C$ such that $\bar{\alpha}_i=x_i^2\alpha_i$. Set $\beta_i=x_i\alpha_i$. Then it is easy to see that

$$\bar{\beta}_i=\beta_i \text{ and } U(\mathbf{Z}C)=\pm C\times\langle\beta_1,\cdots,\beta_r\rangle$$

where $\langle\beta_1,\cdots,\beta_r\rangle$ is a free abelian group of rank r.

By (3.3), for each β_i there exists $t_i \in E$ such that $\mathrm{tr}(t_i\beta_i)$ is odd. Set

$$\xi_i = t_i\beta_i \text{ or } \xi_i = -t_i\beta_i$$

according as $\mathrm{tr}(t_i\beta_i) > 0$ or $\mathrm{tr}(t_i\beta_i) < 0$. Then it is clear that $\{\xi_1, \cdots, \xi_r\}$ satisfies the conditions (i) and (ii).

(3.5) *Assume that C is of odd order. Then*

$$\mathrm{N}(U(\mathbf{Z}D)) = \pm\langle \xi_1, \cdots, \xi_r \rangle.$$

Proof. Note that $x = x^{-1}$ if and only if $x = 1$. Thus there is a subset P of C such that C is a disjoint union $C = \{1\} \cup P \cup P^{-1}$. Let $V = \{\gamma \in U(\mathbf{Z}C) \mid \bar{\gamma} = \gamma\}$. Then V is a subgroup of $U(\mathbf{Z}C)$ and

$$V = \pm\langle \xi_1, \cdots, \xi_r \rangle.$$

Moreover, it follows from (3.1) that $\mathrm{N}(U(\mathbf{Z}D)) \subseteq V$.

In order to prove that $V \subseteq \mathrm{N}(U(\mathbf{Z}D))$, let γ be any element of V. Then γ can be expressed as a sum

$$\gamma = c_1 1 + \sum_{x \in P} c_x (x + x^{-1}).$$

Since $\mathrm{T}(\gamma) = \pm 1$ by (2.1), it follows that $\mathrm{tr}\gamma = c_1$ is odd. Set

$$u = 1 + \alpha + \alpha y, \quad \alpha = \frac{c_1 - 1}{2} + \sum_{x \in P} c_x x.$$

Then

$$\mathrm{N}(u) = (1+\alpha)(1+\bar{\alpha}) = 1 + \alpha + \bar{\alpha} = \gamma.$$

Hence we have $V \subseteq \mathrm{N}(U(\mathbf{Z}D))$.

(3.6) *Assume that C is of even order and let I be the set of all involutions in C. Then*

$$\mathrm{N}(U(\mathbf{Z}D)) = \{\gamma \in U(\mathbf{Z}C) \mid \bar{\gamma} = \gamma \text{ and } \mathrm{tr}(t\gamma) \text{ is even for all } t \in I\}$$

and

$$\mathrm{N}(U(\mathbf{Z}D)) \cap I = \phi.$$

Furthermore, if C has exactly one involution then

$$\mathrm{N}(U(\mathbf{Z}D)) = \pm\langle \xi_1, \cdots, \xi_r \rangle.$$

Proof. Let $E = \{x \in C \mid x^2 = 1\}$. Then $E = \{1\} \cup I$ and there is a subset P of C such that C is a disjoint union $C = E \cup P \cup P^{-1}$.

Let $V = \{\gamma \in U(\mathbf{Z}C) \mid \bar{\gamma} = \gamma\}$. Then V is a subgroup of $U(\mathbf{Z}C)$ and

$$V = \pm E \times \langle \xi_1, \cdots, \xi_r \rangle.$$

Let

$$W = \{\gamma \in V \mid \mathrm{tr}(t\gamma) \text{ is even for all } t \in I\}.$$

First we will show that for any element α of $\mathbf{Z}C$ and for any $t \in I$, $\mathrm{tr}(t\alpha\bar{\alpha})$ *is even.*

Let $\alpha = \sum a_x x$. Then $t\alpha = \sum a_{tx} x$. Hence, by (2.2), we have

$$\mathrm{tr}(t\alpha\bar{\alpha}) = (t\alpha,\ \alpha) = \sum_{x\in C} a_{tx}a_x.$$

Let A be a transversal of a subgroup $\langle t\rangle$ in C. Then

$$\mathrm{tr}(t\alpha\bar{\alpha}) = 2\sum_{x\in A} a_{tx}a_x$$

and so $\mathrm{tr}(t\alpha\bar{\alpha})$ is even.

Suppose that $u=\alpha+\beta y$ is an element of $U(\mathbf{Z}D)$. Then $\mathrm{N}(u)$ is an element of V, by (3.1). Moreover, for any $t\in I$

$$\mathrm{tr}(t\mathrm{N}(u)) = \mathrm{tr}(t\alpha\bar{\alpha}) - \mathrm{tr}(t\beta\bar{\beta}) \equiv 0 \pmod 2$$

by the above result. This implies that $\mathrm{N}(u)\in W$. Therefore, we have $\mathrm{N}(U(\mathbf{Z}D))\subseteq W$.

Conversely, suppose that γ is any element of W. Then γ can be expressed as a sum

$$\gamma = c_1 1 + 2\sum_{t\in I} c_t t + \sum_{x\in P} c_x(x+x^{-1}).$$

Since $\mathrm{T}(\gamma)=\pm 1$, it follows that $\mathrm{tr}\gamma = c_1$ is odd. Set

$$u = 1+\alpha+\alpha y,\quad \alpha = \frac{c_1-1}{2} + \sum_{t\in I} c_t t + \sum_{x\in P} c_x x.$$

Then $\mathrm{N}(u)=\gamma$, which implies that u is an element of $U(\mathbf{Z}D)$ such that $\mathrm{N}(u)=\gamma$. Hence $W\subseteq \mathrm{N}(U(\mathbf{Z}D))$.

Therefore, we have $\mathrm{N}(U(\mathbf{Z}D)) = W$. By definition of W, it is clear that $\mathrm{N}(U(\mathbf{Z}D)) \cap I = \phi$.

Now assume that C has exactly one involution, say s. Then $E=\{1, s\}$ and $V = \pm\{1, s\}\times\langle \xi_1, \cdots, \xi_r\rangle$. Thus each ξ_i can be expressed as a sum

$$\xi_i = d_1 + d_s + \sum_{x\in P} d_x(x+x^{-1}).$$

Since d_1 is odd by (3.4) and $\mathrm{T}(\xi_i)=\pm 1$, it follows that $\mathrm{tr}(s\xi_i)=d_s$ is even. This implies that $\xi_i\in W=\mathrm{N}(U(\mathbf{Z}D))$. Furthermore, W is a subgroup of V such that $s\notin W$. Hence we have

$$\mathrm{N}(U(\mathbf{Z}D)) = W = \pm\langle \xi_1, \cdots, \xi_r\rangle.$$

(3.7) *Theorem* 1 *holds.*

Proof. The assertion (1) follows from (3.4).

By assumption C has at most one involution. Thus either C is of odd order, or C is of even order and it has exactly one involution. Therefore, from (3.1), (3.5) and (3.6) it follows that $\mathrm{N} : U(\mathbf{Z}D) \to U(\mathbf{Z}C)$ is a group-homomorphism with

$$ker\ \mathrm{N} = U_0 = \{\alpha+\beta y\in \mathbf{Z}D \mid \alpha\bar{\alpha} = \beta\bar{\beta} = 1\}$$

and

$$im\ \mathrm{N} = \mathrm{N}(U(\mathbf{Z}D)) = \pm\langle \xi_1, \cdots, \xi_r\rangle.$$

By (3.1) the inverse image of $\{1, -1\}$ is $U_0\langle y\rangle$ and it is a normal subgroup of $U(\mathbf{Z}D)$. Moreover, for each i there exists $u_i \in U(\mathbf{Z}D)$ such that $\mathrm{N}(u_i)=\xi_i$. Set

$$U_1=\langle u_1, \cdots, u_r\rangle.$$

Then U_1 is isomorphic to $\langle \xi_1, \cdots, \xi_r\rangle$ and it is a free abelian group of rank r. Now it is easy to prove that $U(\mathbf{Z}D)$ is the semidirect product of subgroups $U_0\langle y\rangle$ and U_1.

This completes the proof of Theorem 1.

References

1. Ayoub, R.G. and Ayoub, C., *On the group ring of a finite abelian group*, Bull. Austral. Math. Soc. **1** (1969), 245-261
2. Hughes, I. and Pearson, K.R., *The groups of units of the integral group ring* $\mathbf{Z}S_3$, Canada Math. Bull. **15** (1972), 529-534
3. Passman, D.S., *The algebraic structure of group rings*, Interscience, New York, 1977
4. Park, S.A., *The unit group of the integral group ring* $\mathbf{Z}D_n$ II, to appear
5. Polcino, M.C., *The units of the integral group ring* $\mathbf{Z}D_4$, Bol. Soc. Brasil Mat. **4** (1972), 85-92
6. Shin, J.S., *The unit group of the integral group ring* $\mathbf{Z}D_6$, to appear

Sogang University
Seoul 121, Korea