J. Korean Math. Soc.
Vol. 20, No. 2, 1983

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

SEUNG AHN PARK

1. Introduction

Let

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

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

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

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. The structure of the unit group $U(\mathbf{Z}D_n)$ of the integral group ring $\mathbf{Z}D_n$ has been determined in [1]. Note 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 this paper we will explicitly determine three unit groups $U(\mathbf{Z}D_5)$, $U(\mathbf{Z}D_8)$ and $U(\mathbf{Z}D_{12})$, by using the results of [1]. In fact we will prove the following two theorems.

THEOREM 1. *Let* $C_n=\langle x \mid x^n=1\rangle$. *Then*

(1) $U(\mathbf{Z}C_5)=\pm C_5\times\langle\xi\rangle$,

$$\xi=1-(x+x^{-1})$$

(2) $U(\mathbf{Z}C_8)=\pm C_8\times\langle\xi\rangle$,

$$\xi=1+(x+x^{-1})-(x^3+x^{-3})-2x^4$$

(3) $U(\mathbf{Z}C_{12})=\pm C_{12}\times\langle\xi\rangle$,

$$\xi=3+2(x+x^{-1})+(x^2+x^{-2})-(x^4+x^{-4})-2(x^5+x^{-5})-2x^6$$

Received May 10, 1983
This rcsearch is supported by KOSEF Research Grant

THEOREM 2. *Let* $D_n=\langle x, y \mid x^n=y^2=1,\ x^y=x^{-1}\rangle$, *and assume that* $n=5$, 8, *or* 12. *Then* $U(\mathbf{Z}D_n)$ *is the semidirect product of a normal subgroup* $U_0\langle y\rangle$ *and a subgroup* U_1, *that is,*

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

where

$$U_0=\{\alpha+\beta y \mid \alpha, \beta\in\mathbf{Z}\langle x\rangle,\ \alpha\bar{\alpha}-\beta\bar{\beta}=1\},\quad U_1=\langle u\rangle$$

and U_1 *is an infinite cyclic group.*

More precisely, we have

(1) $U(\mathbf{Z}D_6)=(U_0\langle y\rangle)\langle u\rangle,\ u=1-x-xy$

(2) $U(\mathbf{Z}D_8)=(U_0\langle y\rangle)\langle u\rangle,\ u=1+x-x^3-x^4+(x-x^3-x^4)y$

(3) $U(\mathbf{Z}D_{12})=(U_0\langle y\rangle)\langle u\rangle,$

$$u=2+2x+x^2-x^4-2x^5-x^6+(1+2x+x^2-x^4-2x^5-x^6)\,y$$

The terminology and notation in this paper are exactly same as those introduced in [1].

Let $C_n=\langle x \mid x^n=1\rangle$ be the cyclic group of order n. For each integer j the map $\sigma_j : C_n\to C_n$ defined by $\sigma_j(x^i)=x^{ij}$ is an endomorphism of C_n with $\sigma_j(C_n)=\langle x^j\rangle$. The induced map $\sigma_j : \mathbf{Z}C_n\to\mathbf{Z}C_n$ given by

$$\sigma_j(\textstyle\sum a_i x^i)=\sum a_i x^{ij}$$

is a ring-endomorphism of $\mathbf{Z}C_n$ with $\sigma_j(\mathbf{Z}C_n)=\mathbf{Z}\langle x^j\rangle$, and if α is a unit of $\mathbf{Z}C_n$ then $\sigma_j(\alpha)$ is a unit of $\mathbf{Z}\langle x^j\rangle$. An endomorphism σ_j is an automorphism of C_n if and only if $(j, n)=1$. Clearly, σ_{-1} is an automorphism of C_n.

As stated in [1], the automorphism group $\mathrm{Aut}(C_n)$ of C_n acts on the unit group $U(\mathbf{Z}C_n)$ of the integral group ring $\mathbf{Z}C_n$. A unit α in $U(\mathbf{Z}C_n)$ is said to be $\mathrm{Aut}(C_n)$-*invariant* if $\sigma(\alpha)=\alpha$ for all $\sigma\in\mathrm{Aut}(C_n)$. Note that

$$\sigma_{-1}(\alpha)=\bar{\alpha},\quad T(\sigma(\alpha))=T(\alpha),\quad \mathrm{tr}\,\sigma(\alpha)=\mathrm{tr}\,\alpha$$

for all $\alpha\in U(\mathbf{Z}C_n)$ and $\sigma\in\mathrm{Aut}(C_n)$.

2. Proof of Theorem

In this section we will prove Theorem 1 and Theorem 2 by a series of propositions.

(2.1) *Let* $C_n=\langle x \mid x^n=1\rangle$ *and let* $r=r(D_n)$. *Set*

$$W=\{\alpha\in U(\mathbf{Z}C_n) \mid \bar{\alpha}=\alpha \text{ and } \mathrm{tr}\alpha \text{ is odd}\}.$$

Then there exists a system of units $\xi_1, \cdots, \xi_r$ *in* $U(\mathbf{Z}C_n)$ *such that*

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

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

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

(iii) $W=\pm\langle\xi_1, \cdots, \xi_r\rangle$, *and* W *is* $\mathrm{Aut}(C_n)$*-invariant.*

Proof. This follows from the proofs of (3.4), (3.5), (3.6) in [1].

(2.2) *Let* $C_n=\langle x\mid x^n=1\rangle$ *and assume that*

$$n=p^e q^f, \quad e\geq 1, \quad f\geq 0$$

where p *and* q *are distinct primes. Let* S *be the set of all* $\mathrm{Aut}(C_n)$*-intariant units in* $U(\mathbf{Z}C_n)$. *Then*

$$S=\pm\{1\} \text{ or } S=\pm\{1,\ x^{\frac{n}{2}}\}$$

according as n *is odd or even.*

Proof. Let α be an $\mathrm{Aut}(C_n)$-invariant unit in $U(\mathbf{Z}C_n)$. Then α^{-1} is $\mathrm{Aut}(C_n)$-invariant, and we have $\sigma_{-1}(\alpha)=\bar{\alpha}=\alpha$ and $T(\alpha)=T(\alpha^{-1})=\varepsilon$ where $\varepsilon=1$ or -1.

We will prove the assertion by induction on e and f.

Step 1 : *Let* $e=1$, $f=0$. *Thus* $n=p$.

Since $\mathrm{Aut}\langle x\rangle$ acts transitively on the set $\langle x\rangle-\{1\}$, the units α and α^{-1} are of the form

$$\alpha=a+b\sum_{i=1}^{p-1}x^i, \quad \alpha^{-1}=a'+b'\sum_{i=1}^{p-1}x^i$$

where $a, b, a', b'\in\mathbf{Z}$. Now we have

$$1=\mathrm{tr}\alpha^{-1}\alpha=(\alpha^{-1}, \alpha)=aa'+(p-1)bb'$$

and

$$a+(p-1)b=\varepsilon=a'+(p-1)b'.$$

From these two equations it follows that $\varepsilon(b+b')=pbb'$. Hence $b'=b$, and so if p is odd then $b=0$ and if $p=2$ then $b=0$ or ε.

Therefore, the assertion holds for $e=1$, $f=0$.

Step 2 : *Let* $e=f=1$. *Thus* $n=pq$.

The generator x of $\langle x\rangle$ can be expressed as a product $x=yz$, where y is of order p and z is of order q. Thus

$$\langle x\rangle=\langle y\rangle\times\langle z\rangle, \quad \mathrm{Aut}\langle x\rangle\cong\mathrm{Aut}\langle y\rangle\times\mathrm{Aut}\langle z\rangle.$$

Since $\mathrm{Aut}\langle x\rangle$ acts transitively on the four sets

$$\{1\},\ \langle y\rangle-1,\ \langle z\rangle-1,\ \langle x\rangle-\{\langle y\rangle\cup\langle z\rangle\},$$

the units α and α^{-1} are of the form

$$\alpha=a+b\sum_{i=1}^{p-1}y^i+c\sum_{j=1}^{q-1}z^j+d\sum_{i=1}^{p-1}\sum_{j=1}^{q-1}y^iz^j,$$

$$\alpha^{-1}=a'+b'\sum_{i=1}^{p-1}y^i+c'\sum_{j=1}^{q-1}z^j+d'\sum_{i=1}^{p-1}\sum_{j=1}^{q-1}y^iz^j.$$

Hence we have

$$\begin{aligned}1&=\mathrm{tr}\,\alpha^{-1}\alpha=(\alpha^{-1},\alpha)\\&=aa'+(p-1)bb'+(q-1)cc'+(p-1)(q-1)dd'.\end{aligned}\tag{i}$$

On the other hand,

$$\sigma_p(\alpha)=a+(p-1)b+\{c+(p-1)d\}\sum_{i=1}^{q-1}z^j\in U(\mathbf{Z}\langle z\rangle)$$

and

$$\sigma_q(\alpha)=a+(q-1)c+\{b+(q-1)d\}\sum_{i=1}^{p-1}y^i\in U(\mathbf{Z}\langle y\rangle).$$

Moreover, $\mathrm{Aut}\langle x\rangle$ induces $\mathrm{Aut}\langle z\rangle$ and $\mathrm{Aut}\langle y\rangle$. Hence $\sigma_p(\alpha)$ is $\mathrm{Aut}\langle z\rangle$-invariant and $\sigma_q(\alpha)$ is $\mathrm{Aut}\langle y\rangle$-invariant. Similar results for $\sigma_p(\alpha^{-1})$ and $\sigma_q(\alpha^{-1})$ can be obtained. Thus we can apply Step 1 to these four units.

Now we may assume that $p<q$. Thus q is odd and so we have

$$\begin{aligned}&a+(p-1)b=\varepsilon=a'+(p-1)b'\\&c+(p-1)d=0=c'+(p-1)d'\end{aligned}\tag{ii}$$

From (i) and (ii) it follows that

$$\varepsilon(b+b')=pbb'+p(q-1)dd'\tag{iii}$$

Furthermore, one of the following holds:

$$b+(q-1)d=0=b'+(q-1)d'\tag{iv}$$

or

$$p=2\quad\text{and}\quad b+(q-1)d=\varepsilon=b'+(q-1)d'\tag{v}$$

If (iv) holds, then $\varepsilon(d+d')=-pqdd'$, from which we obtain $\alpha=\varepsilon=\pm1$. If (v) holds, then $\varepsilon(d+d')=2qdd'$, from which we obtain $\alpha=\varepsilon y=\pm x^{\frac{n}{2}}$.

Hence the assertion holds for $e=f=1$.

Step 3 : Let $n=p^e q^f$, where $e\geq 2$ and $f\geq 0$.

And assume that the assertion holds for all divisor n' of n with $1<n'<n$. Set $m=p^{e-1}\geq p$ and $l=q^f\geq 1$. The generator x of $\langle x\rangle$ can be expressed as a product $x=yz$, where y is of order p^e and z is of order q^f. Thus

$$\langle x\rangle=\langle y\rangle\times\langle z\rangle,\quad \mathrm{Aut}\langle x\rangle\cong\mathrm{Aut}\langle y\rangle\times\mathrm{Aut}\langle z\rangle.$$

For each z^j. the set

$$(\langle y\rangle-\langle y^p\rangle)z^j=\{y^k z^j\mid (k,p)=1\}$$

is contained in an $\mathrm{Aut}\langle x\rangle$-orbit. Hence the unit α can be written as a sum

$$\alpha=\sum_{j=0}^{l-1}\alpha_j z^j+\sum_{j=0}^{l-1}\sum_{(k,p)=1}a_j y^k z^j$$

where $\alpha_j\in\mathbf{Z}\langle y^p\rangle$ and $a_j\in\mathbf{Z}$. It follows that

$$\sigma_m(\alpha)=\sum_{j=0}^{l-1}T(\alpha_j)z^j+\sum_{j=0}^{l-1}\sum_{k=1}^{p-1}m\,a_j\,y^{mk}z^j$$

and it is a unit in $U(\mathbf{Z}\langle x^m\rangle)$. Clearly, $\mathrm{Aut}\langle x\rangle$ induces $\mathrm{Aut}\langle x^m\rangle$. Therefore, the unit $\sigma_m(\alpha)$ is $\mathrm{Aut}\langle x^m\rangle$-invariant and, by induction hypothesis, we have $a_j=0$ for all j. This implies that

$$\alpha=\sum_{j=0}^{l-1}\alpha_j z^j\in U(\mathbf{Z}\langle x^p\rangle).$$

Since $\mathrm{Aut}\langle x\rangle$ induces $\mathrm{Aut}\langle x^p\rangle$, the unit α is an $\mathrm{Aut}\langle x^p\rangle$-invariant unit in $U(\mathbf{Z}\langle x^p\rangle)$. Hence, by induction hypothesis, the assertion holds.

(2.3) *Let $C_n=\langle x\mid x^n=1\rangle$ and assume that*

$$n=p^e q^f,\quad e\geq 1,\quad f\geq 0$$

where p and q are distinct primes. Let H be a transversal of the subgroup $\{1,\sigma_{-1}\}$ in $\mathrm{Aut}(C_n)$.

Then for any $\alpha\in U(\mathbf{Z}C_n)$ such that $\bar{\alpha}=\alpha$ and $\mathrm{tr}\,\alpha$ is odd, we have

$$\prod_{\sigma\in H}\sigma(\alpha)=\pm 1.$$

Furthermore, if $|H|$ is even then $\prod_{\sigma\in H}\sigma(\alpha)=1$.

Proof. Set $G=\mathrm{Aut}(C_n)$ and

$$W=\{\alpha\in U(\mathbf{Z}C_n)\mid\bar{\alpha}=\alpha\text{ and }\mathrm{tr}\,\alpha\text{ is odd}\}.$$

Let α be any element of W and let $\beta=\prod_{\sigma\in H}\sigma(\alpha)$. Then W is G-invariant by (2.1), and so $\beta\in W$. Since $G=H\cup H\sigma_{-1}$ and $\sigma_{-1}(\alpha)=\bar{\alpha}=\alpha$, we have

$$\beta^2 = \prod_{\sigma\in G} \sigma(\alpha).$$

Hence β^2 is G–invariant. By (2. 2) this implies that $\beta^2 \in S$, where $S=\pm\{1\}$ or $S=\pm\{1, x^{\frac{n}{2}}\}$ according as n is odd or even. Therefore, it follows that $\beta \in W$ and $\beta^4=1$. By (2. 1) this yields that $\beta=\pm 1$.

If $|H|$ is even, then we have $T(\beta)=T(\alpha)^{|H|}=1$ and so $\beta=1$.

(2. 4) *Let* $C_n=\langle x \mid x^n=1\rangle$.

If $n=3, 4,$ *or* 6, *then* $U(\mathbf{Z}C_n)=\pm C_n$.

If $n=5, 8,$ *or* 12, *then there exists a fundamental unit* ξ *in* $U(\mathbf{Z}C_n)$ *such that*

(i) $\bar{\xi}=\xi$ *and* tr ξ *is a positive odd integer, and*

(ii) $U(\mathbf{Z}C_n)=\pm C_n \times \langle\xi\rangle$, *where* $\langle\xi\rangle$ *is an infinite cyclic group.*

Furthermore, if $n=5$ *then* $\sigma_2(\xi)=\xi^{-1}$, *and if* $n=8$ *or* 12 *then* $\sigma_5(\xi)=\xi^{-1}$.

Proof. The assertions follow from (2. 1), (2. 2) and (2. 3).

Note that we have

$$\mathrm{Aut}(C_5)=\langle\sigma_2\rangle=\{1, \sigma_2\} \cup \{1, \sigma_2\}\sigma_{-1},$$

$$\mathrm{Aut}(C_8)=\langle\sigma_{-1}\rangle\times\langle\sigma_5\rangle,\ \ \mathrm{Aut}(C_{12})=\langle\sigma_{-1}\rangle\times\langle\sigma_5\rangle.$$

(2. 5) Theorem 1 *holds.*

Proof. By (2. 4) it suffices to find a fundamental unit ξ of $U(\mathbf{Z}C_n)$ for $n=5, 8, 12$. We will use (2. 4) repeatedly.

(1) Since $\bar{\xi}=\xi$ and $\sigma_2(\xi)=\xi^{-1}$, the units ξ and ξ^{-1} can be expressed as

$$\xi=a_0+a_1(x+x^{-1})+a_2(x^2+x^{-2}),$$

$$\xi^{-1}=a_0+a_2(x+x^{-1})+a_1(x^2+x^{-2}).$$

Hence the following hold.

$$a_0{}^2+4a_1a_2=1,\ \ T(\xi)=a_0+2(a_1+a_2)=\pm 1,$$

$$(a_1+a_2)(a_0+a_1)=-a_2{}^2,\ \ (a_1+a_2)(a_0+a_2)=-a_1{}^2.$$

Assume that $\mathrm{tr}\,\xi=a_0=1$. Then it is easy to see that $\xi=\beta$ or $\xi=\beta^{-1}$, where

$$\beta=1-(x+x^{-1}),\ \ \beta^{-1}=1-(x^2+x^{-2}).$$

Suppose that $\mathrm{tr} \geq 3$. Then the following hold.

$$a_0 \geq 3,\ \ a_1a_1>0,\ \ a_1a_2<0,$$

$$a_1+a_2<0,\ \ a_0+a_1>0,\ \ a_0+a_2>0.$$

Hence, by induction on $m\geq 1$, we can show that ξ^m is of the form

$$\xi^m=b_0+b_1(x+x^{-1})+b_2(x^2+x^{-2})$$

where

$$b_0\geq 3,\ \ a_1b_1>0,\ \ a_1b_2<0.$$

In particular we have

$$\mathrm{tr}\,\xi^m\geq 3,\ \ \mathrm{tr}\,\xi^{-m}=\mathrm{tr}\,\sigma_2(\xi^m)=\mathrm{tr}\,\xi^m\geq 3$$

for all $m\geq 1$. This implies that $\beta\notin\langle\xi\rangle$, which is a contradiction.

Therefore, we have $\mathrm{tr}\,\xi=1$ and we may take β as ξ.

(2) The fundamental unit ξ can be expressed as a sum

$$\xi=a_0+a_1(x+x^{-1})+a_2(x^2+x^{-2})+a_3(x^3+x^{-3})+a_4x^4.$$

Note that

$$\sigma_2(\xi)=a_0+a_4+(a_1+a_3)(x^2+x^{-2})+2a_2x^4$$

and it is a unit in $U(\mathbf{Z}\langle x^2\rangle)$, where $U(\mathbf{Z}\langle x^2\rangle)=\pm\langle x^2\rangle$.
Hence we have $a_1+a_2=0$, $a_2=0$, and it follows that

$$\xi=a_0+a_1(x+x^{-1})-a_1(x^3+x^{-3})+a_4x^4,$$

$$\xi^{-1}=\sigma_5(\xi)=a_0-a_1(x+x^{-1})+a_1(x^3+x^{-3})+a_4x^4.$$

Thus the following hold.

$$T(\xi)=a_0+a_4=\pm 1,\ \ a_0a_4+2a_1^2=0.$$

Assume that $\mathrm{tr}\,\xi=1$. Then it is easy to see that $\xi=\beta$ or $\xi=\beta^{-1}$, where

$$\beta=1+(x+x^{-1})-(x^3+x^{-3})-2x^4,$$

$$\beta^{-1}=1-(x+x^{-1})+(x^3+x^{-3})-2x^4.$$

Now suppose that $\mathrm{tr}\,\xi\geq 3$. Then, by induction on $m\geq 1$, we can show that ξ^m is of the form

$$\xi^m=b_0+b_1(x+x^{-1})-b_1(x^3+x^{-3})+b_4x^4$$

where

$$b_0\geq 3,\ \ a_1b_1>0,\ \ b_4<0.$$

In particular, we have

$$\mathrm{tr}\,\xi^m\geq 3,\ \ \mathrm{tr}\,\xi^{-m}=\mathrm{tr}\,\sigma_5(\xi^m)=\mathrm{tr}\,\xi^m\geq 3$$

for all $m\geq 1$. This implies that $\beta\notin\langle\xi\rangle$, which is a contradiction.

Therefore, we have $\mathrm{tr}\,\xi=1$ and we may take β as ξ.

(3) The fundamental unit ξ can be expressed as

$$\xi = a_0 + a_6 x^6 + \sum_{i=1}^{5} a_i (x^i + x^{-i}).$$

Since $\sigma_2(\xi)$ is in $U(\mathbf{Z}\langle x^2\rangle) = \pm\langle x^2\rangle$, we have $a_1 + a_5 = 0$, $a_2 + a_4 = 0$, $a_3 = 0$. Moreover, $\xi^{-1} = \sigma_5(\xi)$. Hence the following hold.

$$T(\xi) = a_0 + a_6 = \pm 1,$$

$$a_0 a_2 - a_2 a_6 - a_1{}^2 - a_2{}^2 = 0, \quad a_0 a_6 + 2a_1{}^2 - 2a_2{}^2 = 0.$$

Assume that $\mathrm{tr}\,\xi = 1$. Then $\xi = 1$, which is not the case. Now assume that $\mathrm{tr}\,\xi = 3$. Then it is easy to see that $\xi = \beta$ or $\xi = \beta^{-1}$, where

$$\beta = 3 + 2(x + x^{-1}) + (x^2 + x^{-2}) - (x^4 + x^{-4}) - 2(x^5 + x^{-5}) - 2x^6$$

and

$$\beta^{-1} = \sigma_5(\beta) = 3 - 2(x + x^{-1}) + (x^2 + x^{-2}) - (x^4 + x^{-4}) + 2(x^5 + x^{-5}) - 2x^6$$

Suppose that $\mathrm{tr}\,\xi \geq 5$. Then, by induction on $m \geq 1$, we can show that

$$\xi^m = b_0 + b_1(x + x^{-1}) + b_2(x^2 + x^{-2}) - b_2(x^4 + x^{-4}) - b_1(x^5 + x^{-5}) + b_6 x^6$$

where

$$b_0 \geq 5, \quad a_1 b_1 > a_2 b_2, \quad b_2 > 0, \quad b_6 < 0.$$

In particular, we have $\mathrm{tr}\,\xi^m = \mathrm{tr}\,\xi^{-m} \geq 5$ for all $m \geq 1$. This implies that $\beta \notin \langle \xi \rangle$, which is a contradiction.

Therefore, we have $\mathrm{tr}\,\xi = 3$ and we may take β as ξ.

(2.6) Theorem 2 *holds.*

Proof. This follows from Theorem 2, proofs of (3.5) and (3.6) in [1] and Theorem 1.

Reference

1. Park, S. A., *The unit group of the integral group ring* $\mathbf{Z}D_n$, Journal of K.M.S. **20** (1983),

Sogang University
Seoul 121, Korea