J. Math. Soc. Japan
Vol. 32, No. 4, 1980

On the units of the integral group ring of a dihedral group

By Takehiko MIYATA

(Received Nov. 20, 1978)
(Revised Jan. 20, 1979)

0. Introduction.

For G an arbitrary finite group, ZG denotes the integral group ring and $U(ZG)$ its group of units. We denote by ε the augmentation from ZG to Z and by $V(ZG)$ the subgroup of units u of ZG with $\varepsilon(u)=1$; clearly $U(ZG)=V(ZG)\times U(Z)$. In this paper we study $U(ZD_n)$ where D_n is a dihedral group of order $2n$. Throughout this paper we assume that n is an odd integer and all modules are finitely generated left modules. Main results in this paper are the following;

THEOREM A. *$V(ZD_n)$ is a semi-direct product of a torsion free normal subgroup with D_n.*

THEOREM B. *There are $\phi(n)/2$ conjugate classes in $V(ZD_n)$ of subgroups of $V(ZD_n)$ isomorphic to D_n if the order of the locally free class group $C(ZD_n)$ of ZD_n is odd. Here ϕ denotes Euler's totient function.*

By [3] $D(ZD_n)=0$ if $n<60$. Masley's results in [5] show that values of n satisfying the condition of Theorem B and less than 60 are 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 31, 33, 35, 39, 45, 51, 55 and 57. It seems to be an interesting problem to delete the condition on $C(ZD_n)$ in Theorem B.

Let D_n be generated by σ and τ with relations $\sigma^n=\tau^2=1$ and $\tau^{-1}\sigma\tau=\sigma^{-1}$. Set $S=ZD_n/(1+\sigma+\sigma^2+\cdots+\sigma^{n-1})$. The key point in proving Theorems A and B is that the order S behaves like a hereditary order as far as locally S-modules concern. For example the locally free class group of S is isomorphic to that of the center of S. For other applications of this property of S, see [6].

For $n=3$ complete results are obtained by Hughes and Pearson [4]. Further information on $V(ZD_3)$ and especially on the torsion free normal subgroup in Theorem A is found in the excellent survey article on the unit group of rings by Dennis [2].

Recently K. Sekiguchi (Tokyo Metropolitan University) has extended Theorem A to a metabelian group G such that the exponent of G/G' is 1, 2, 3, 4 or 6, where G' denotes the commutator subgroup of G.

1. Semi-direct products.

Let $\bar{\sigma}$ and $\bar{\tau}$ denote the images of σ and τ in S respectively and let us set $\omega=\bar{\sigma}+\bar{\sigma}^{-1}$. We consider a pull back diagram

$$\begin{array}{ccc} ZD_n & \longrightarrow & Z\langle\tau\rangle \\ \downarrow & & \downarrow \\ S & \longrightarrow & F_n\langle\tau\rangle \end{array}$$

where F_n is a finite ring Z/nZ. From this diagram we have an exact sequence (cf. [8], for example)

$$1 \longrightarrow U(ZD_n) \longrightarrow U(S) \longrightarrow U(F_n\langle\tau\rangle/\langle -1, \tau\rangle) \longrightarrow 1\,. \tag{1}$$

The exactness of the last map follows from the fact that the natural homomorphism $D(ZD_n) \longrightarrow D(S)$ is an injection ([3], [6]). By this sequence $U(ZD_n)$ will be viewed as a normal subgroup of $U(S)$. Since the center of S is $Z[\omega]$ and S acts on $Z[\bar{\sigma}]$ ($\cong S(1+\bar{\tau})$) as $Z[\omega]$-endomorphisms in a natural way, there is an injection from S to $\mathrm{End}_{Z[\omega]}(Z[\bar{\sigma}])$. Because $Z[\bar{\sigma}]$ is a free $Z[\omega]$-module with basis $(1, \bar{\sigma})$, we identify $\mathrm{End}_{Z[\omega]}(Z[\bar{\sigma}])$ with $M_2(Z[\omega])$, the ring of 2×2-matrices with entries in $Z[\omega]$. An arbitrary element $a+b\bar{\tau}+c\bar{\sigma}+d\bar{\tau}\bar{\sigma}$ of S (a, b, c, $d\in Z[\omega]$) is represented by the matrix

$$\begin{pmatrix} a+b & c+d \\ b\omega-c+d & a-b+c\omega \end{pmatrix}. \tag{2}$$

For the remainder of this paper $U(S)$ will be viewed as a subgroup of $GL_2(Z[\omega])$ by this representation. Let us set (2) equal to $\begin{pmatrix} x & y \\ z & u \end{pmatrix}$. Then we have

$$a(\omega^2-4)=x\omega^2-(z-y)\omega-2(x+y)\,. \tag{3}$$

Since ω and $\omega+2$ are units in $Z[\omega]$ (note that n is an odd integer), we obtain

LEMMA (1.1). *An element* $\begin{pmatrix} x & y \\ z & u \end{pmatrix}$ *of* $M_2(Z[\omega])$ *belongs to* S *if and only if* $x+y\equiv z+u \mod(\omega-2)$.

Let us set

$$H=\left\{\begin{pmatrix} x & y \\ z & u \end{pmatrix}\in GL_2(Z[\omega])\,\middle|\,\begin{pmatrix} x & y \\ z & u \end{pmatrix}\equiv\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod(\omega-2)\right\}.$$

Then, H is clearly a normal subgroup in $GL_2(Z[\omega])$ and $GL_2(Z[\omega])/H\cong GL_2(F_n)$. The formula (3) and the exact sequence (1) imply that H is contained in $V(ZD_n)$.

THEOREM (1.2). *$U(ZD_n)$ is the semi-direct product of H with $\pm D_n$.*

PROOF. By Lemma (1, 1) we have

$$U(S)/H=\left\{\begin{pmatrix} x & y \\ z & u \end{pmatrix}\in GL_2(F_n)\,\middle|\, x+y=z+u\right\}.$$

If $\begin{pmatrix} x & y \\ z & u \end{pmatrix}$ is an element of $U(S)/H$, then $\det\begin{pmatrix} x & y \\ z & u \end{pmatrix}=(x+y)(u-y)$. Hence the order of $U(S)/H$ is the number of triples (x, y, u) such that $x+y$ and $u-y$ are both units in F_n. Thus it is $n\phi(n)^2$. By the exact sequence (1) we have

$$[U(S): U(ZD_n)]=\phi(n)^2/4.$$

Since $[U(S): H]=[U(S): U(ZD_n)]\cdot[U(ZD_n): H]$, the order of $U(ZD_n)/H$ is $4n$. The natural homomorphism from $U(ZD_n)$ to $U(ZD_n)/H$ restricted to $\pm D_n$ is an isomorphism, because $H\cap(\pm D_n)=\{1\}$. This completes the proof.

Let $\Phi_m(X)$ be the m-th cyclotomic polynomial and $S_h=S/(\Phi_h(\bar{\sigma}))$ for h/n, $h>1$. Since S is the subring of $M_2(Z[\omega])$, S_h can be considered as a subring of $M_2(Z[\zeta_h+\zeta_h^{-1}])$ where $\zeta_h=\exp(2\pi i/h)$. Let us set $\omega_h=\zeta_h+\zeta_h^{-1}$.

PROPOSITION (1, 3). *H is torsion free.*

PROOF. Let $H_h=\left\{\begin{pmatrix} x & y \\ z & u \end{pmatrix}\in GL_2(Z[\omega_h])\,\middle|\, \begin{pmatrix} x & y \\ z & u \end{pmatrix}\equiv\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod(\omega_h-2)\right\}$ and let ψ_h be the natural homomorphism from H to H_h. It is easy to check that H_h is torsion free if h is a prime power. If $n=p^m$ where p is an odd prime, H is torsion free since the natural homomorphism

$$H\longrightarrow H_{p^m}\times H_{p^{m-1}}\times\cdots\times H_p$$

is an injection. Let $n=p_1^{m_1}p_2^{m_2}\cdots p_r^{m_r}$ $(p_1<p_2<\cdots<p_r)$ be the prime decomposition of n. We shall proceed the proof by the induction on r and $m_1+m_2+\cdots+m_r$. Let $A=\begin{pmatrix} 1+a & b \\ c & 1+d \end{pmatrix}$ $(a, b, c, d\in(\omega-2)Z[\omega])$ be an element of finite order of H. By the induction assumption we can assume that $\psi_h(A)=1$ for every $h\mid n$, $1<h<n$. Here a, b, c and d belong to an ideal $\bar{\sigma}^{-k/2}F(\bar{\sigma})Z[\omega]$, where $F(X)=(1+X+X^2+\cdots+X^{n-1})/\Phi_n(X)$ and k is the degree of $F(X)$. Since $F(X)$ is divisible by $(X^{n/p_i}-1)/(X-1)$ for $1\leqq i\leqq r$, $F(\zeta_n)$ is divisible by $\omega_{p_i}-2$ for $1\leqq i\leqq r$ and so by $\Omega=\prod_{1\leqq i\leqq r}(\omega_{p_i}-2)$. Since $a(\zeta_n)$, $b(\zeta_n)$, $c(\zeta_n)$ and $d(\zeta_n)$ are divisible by Ω, we see that

$$\psi_n(A)\equiv\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod\Omega.$$

Taking a suitable power of A we can assume that the order of A is a prime q. If q is odd, $\psi_n(A)$ is similar to $\begin{pmatrix} \zeta_q & 0 \\ 0 & \zeta_q^{-1} \end{pmatrix}$ over the complex numbers. Computing the trace of $\psi_n(A)$ in two different ways, we have $2\equiv\omega_q \bmod\Omega$. This

is a contradiction (note that $r \geqq 2$). If $q=2$, $\phi_n(A)$ is similar to $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ or to $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ over the complex numbers. This case also leads to a contradiction by a similar method. Therefore H has no element of finite order except an identity.

2. Conjugate classes.

Let G be a subgroup of $V(ZD_n)$ of order $2n$. Then, we have $ZG=ZD_n$ by [1]. Theorem (1, 2) implies that G is isomorphic to D_n. An isomorphism $f: D_n \longrightarrow G$ can be extended to an automorphism of ZD_n by linearlity. By Glauberman's theorem on class sums in group rings (cf. [7]), class sums of D_n in ZD_n coincide with class sums of G in ZD_n as sets and f preserves class sums (note that $f(V(ZD_n)) \subseteqq V(ZD_n)$, namely, f is a normalised automorphism). From the above remark we have $f(\sigma+\sigma^{-1})=\sigma^m+\sigma^{-m}$ where m is prime to n. Let g be the automorphism of ZD_n defined by $g(\sigma^m)=\sigma$ and $g(\tau)=\tau$. Changing f with $f \cdot g$ we can assume that f is the identity map on $Z[\sigma+\sigma^{-1}]$. Therefore f induces an automorphism on $V(ZD_n)/H$ too.

LEMMA (2, 1). *There exists an automorphism f_G of S such that* (i) $f_G(D_n)=G$, (ii) *f_G is the identity on $Z[\omega]$ and* (iii) $f_G(\tau)=\tau$ *in* $V(ZD_n)/H$.

PROOF. Let f_G be the automorphism constructed above. Set $\sigma'=f(\sigma)$. In $V(ZD_n)/H$ we have that $\sigma'=\sigma^k$ and $f(\tau)=\sigma^i\tau$. We choose an integer m such that $mk \equiv i \pmod{n}$. We define f_G by setting $f_G(\sigma)=f(\sigma)$ and $f_G(\tau)=\sigma'^{-m}f(\tau)$ and extend this map to an automorphism on S. Then f_G satisfies three conditions.

Let M be the S-module $Z[\bar{\sigma}] \cong S(1+\bar{\tau})$. N denotes an S-module $Z[\bar{\sigma}]$ on which S acts through f_G in Lemma (2, 1), that is, (i) $N \cong Z[\bar{\sigma}]$ as a $Z[\omega]$-module and (ii) $\alpha \cdot m = f_G(\alpha)m$ for $\alpha \in S$ and $m \in Z[\bar{\sigma}]$. By [6] M is a projective S-module. Since f_G induces an automorphism on $V(ZD_n)/H$ by Theorem (1, 1), it is easy to see that $F_n \otimes_{Z[\omega]} M \cong F_n \otimes_{Z[\omega]} N$ as $F_n \otimes_{Z[\omega]} S$-modules. This implies that M and N are locally isomorphic, since M and N are projective S-modules by [6].

We need the following result from [6].

LEMMA (2, 2). *There is a locally free ideal A of $Z[\omega]$ such that*

$$A \otimes_{Z[\omega]} M \cong AM \cong N$$

and $A \oplus A$ is a free $Z[\omega]$-module.

LEMMA (2, 3). *$U(S)$ is self-normalizing in $GL_2(Z[\omega])$.*

PROOF. By simple computations, the image of σ in $U(ZD_n)/H$ is conjugate to $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ in $GL_2(F_n)$. Since the normalizer G of the cyclic subgroup generated

by $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ is $\left\{\begin{pmatrix} x & y \\ 0 & u \end{pmatrix} \middle| xu \text{ is an unit in } F_n\right\}$, the order of G is $n\phi(n)^2$, which shows that G is conjugate to the image of $U(S)$ in $GL_2(F_n)$. This completes the proof.

Let C be the center of $GL_2(Z[\omega])$. Then, C is contained in $U(S)$ by Lemma (1, 1).

LEMMA (2, 4). *The normalizer of D_n in $GL_2(Z[\omega])$ is $D_n \cdot C$.*

PROOF. Let $X \in GL_2(Z[\omega])$ satisfy $XD_nX^{-1} \subseteqq D_n$. Then X belongs to $U(S)$ by Lemma (2, 3). By projecting σ to $U(S_h)$ for every $h \mid n$, $h>1$ it is easy to see that $X\sigma X^{-1}=\sigma$ or $X\sigma X^{-1}=\sigma^{-1}$. If $X\sigma X^{-1}=\sigma$, we have $X\tau X^{-1}=\sigma^i\tau$. Taking an integer j such that $2j \equiv i \pmod{n}$, we see that an inner automorphism of S induced by $X\sigma^{-j}$ is the identity on S. Hence $X\sigma^{-j} \in C$. If $X\sigma X^{-1}=\sigma^{-1}$, we can conclude that $X \in D_n \cdot C$ by a similar argument.

Finally we can prove,

THEOREM (2, 5). *There are $\phi(n)/2$ conjugate classes of subgroups in $V(ZD_n)$ isomorphic to D_n if the order of the locally free class group $C(ZD_n)$ is odd.*

PROOF. By [6], $C(Z[\omega]) \cong C(S) \cong C(ZD_n)$. Since $C(ZD_n)$ has no 2-torsion, M and N in Lemma (2, 2) are isomorphic. Therefore a subgroup G of $V(ZD_n)$ isomorphic to D_n is conjugate to D_n in $GL_2(Z[\omega])$. Hence G and D_n are conjugate in $U(S)$ by Lemma (2, 3). Let X and Y be elements of $U(S)$. Then, XD_nX^{-1} and YD_nY^{-1} are conjugate in $V(ZD_n)$ if and only if there exists $Z \in U(ZD_n)$ such that $Y^{-1}ZX$ belongs to the normalizer $D_n \cdot C$ of D_n in $U(S)$. This condition is the same as $Y^{-1}X \in U(ZD_n) \cdot C$ since $XU(ZD_n)X^{-1}=U(ZD_n)$. Hence the number of conjugate classes of subgroups of $V(ZD_n)$ isomorphic to D_n is

$$[U(S) : U(ZD_n) \cdot C] = \phi(n)/2 .$$

3. Remarks.

After the manuscript of this paper was completed the paper [9] by Fröhlich, Reiner and Ullom came to the author's attention. Theorem (4, 3) in [9] gives a proof of Theorem B when n is an odd prime but without the restriction on the order of $C(ZD_n)$ ($\cong C(Z[\zeta_n+\zeta_n^{-1}])$. Namely,

THEOREM B′. *When n is an odd prime, the number of conjugate classes in $V(ZD_n)$ of subgroups of $V(ZD_n)$ isomorphic to D_n is equal to*

$$(\phi(n)/2) \cdot |C(ZD_n)_2| ,$$

where $C(ZD_n)_2 = \{x \in C(ZD_n) \mid 2x=0\}$ and $|C(ZD_n)_2|$ is the order of $C(ZD_n)_2$.

We note the following simple lemma.

LEMMA. (3, 1). *Let f be an automorphism of ZD_n such that $f(D_n)=D_n$ and f is the identity on the center of ZD_n. Then, f is an inner automorphism of*

ZD_n.

This lemma shows that the number of conjugate classes in $V(ZD_n)$ of subgroups of $V(ZD_n)$ isomorphic to D_n is equal to the order of Outcent(ZD_n) (for the definition of Outcent(ZD_n), see [**9**]). This observation and Theorem (4, 3) in [**9**] imply Theorem B′.

It seems reasonable to conjecture that Theorem B′ holds for an arbitrary odd integer n.

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 rings, In: Ring Theory II, Marcel Dekker, 1977.
[3] S. Endo and T. Miyata, On the class groups of dihedral groups, (to appear).
[4] I. Hughes and K.R. Pearson, The group of units of the integral group ring ZS_3, Canad. Math. Bull., 15 (1972), 529-534.
[5] J.M. Masley, Solution of small class number problems for cyclotomic fields, Compositio Math., 33 (1976), 179-186.
[6] T. Miyata, A normal integral basis theorem for dihedral groups, (to appear).
[7] D.S. Passman, Isomorphic groups and group rings, Pacific J. Math., 15 (1965), 561-583.
[8] I. Reiner and S. Ullom, A Mayer-Vietoris sequences for class groups, J. Algebra, 31 (1974), 305-342.
[9] A. Fröhlich, I. Reiner and S. Ullom, Class groups and Picard groups of orders, Proc. London Math. Soc., (3) 29 (1974), 405-434.

Takehiko MIYATA
Department of Mathematics
Osaka City University
Sugimoto-cho, Sumiyoshi-ku
Osaka 558
Japan