Canad. Math. Bull. Vol. **33** (2), 1990

DETERMINING UNITS IN SOME INTEGRAL GROUP RINGS

BY

E. G. GOODAIRE, E. JESPERS, AND M. M. PARMENTER

In this brief note, we will show how in principle to find all units in the integral group ring $\mathbf{Z}G$, whenever G is a finite group such that $G/Z(G) \cong C_2 \times C_2$, and G/G' and $Z(G)$ each have exponent 2, 3, 4 or 6. Special cases include the dihedral group of order 8, whose units were previously computed by Polcino Milies [5], and the group $G = \langle a, b \mid a^4 = 1 = b^4,\ [b,a] = a^{-2}\rangle$ discussed by Ritter and Sehgal [6]. Other examples of noncommutative integral group rings whose units have been computed include $\mathbf{Z}S_3$ ([2], [4]), and $\mathbf{Z}A_4$ ([1]), but in general very little progress has been made in this direction. For basic information on units in group rings, the reader is referred to Sehgal [7].

Before beginning, we would like to confess that we are slightly embarassed by the simplicity of what follows. However, we feel the results are interesting because very few noncommutative group rings have had their units completely determined. The ideas behind the computations originate in work on units of loop rings [3], and some of the arguments here can also be applied to that area, but we have elected to work solely with group rings in this paper.

First we list a few simple properties of the groups we are interested in.

LEMMA 1. *Let G be a finite group such that $G/Z(G) \cong C_2 \times C_2$.* (1) $G' = \{1, e\}$ *where $e \in Z(G)$.* (2) *If $g, h \in G$, then $hg = gh$ or $hg = egh$.* (3) *If $g, h \notin Z(G)$, then $hg = gh$ if and only if $gh \in Z(G)$.* (4) *The mapping $* : G \longrightarrow G$, defined by $g^* = g$ if $g \in Z(G)$, and $g^* = eg$ if $g \notin Z(G)$, is an involution.*

PROOF. To prove Part 1, note that if $G/Z(G) = \langle \bar{a}, \bar{b}\rangle$, then $[b,a] = bab^{-1}a^{-1} = babb^{-2}a^{-1} = baba^{-1}b^{-2}$ since $b^{-2} \in Z(G)$. Hence $[b,a] = b(aba^{-1}b^{-1})b^{-1} = aba^{-1}b^{-1} = [a,b]$ since $[a,b] \in Z(G)$. Similar arguments show that all other commutators equal either 1 or $[a,b]$.

Part 2 follows immediately from Part 1, while Part 3 is obvious.

To prove part 4, we note first that $*$ is certainly bijective. Let $a, b \in G$. If $a, b \in Z(G)$, then $ab \in Z(G)$, so $(ab)^* = ab = ba = b^*a^*$. If $a \in Z(G)$, $b \notin Z(G)$ (or conversely), then $ab \notin Z(G)$, so $(ab)^* = eab = (eb)a = b^*a^*$. Finally, assume $a \notin Z(G)$, $b \notin Z(G)$. Then $b^*a^* = (eb)(ea) = ba$. If $ab \in Z(G)$, then $(ab)^* = ab = ba$ by Part 3, so $(ab)^* = b^*a^*$. If $ab \notin Z(G)$, then $(ab)^* = eab = ba$ by Parts 2 and 3, so

Received by the editors November 17, 1988 and, in revised form, March 20, 1989.

AMS 1980 Subject Classification: 16A26.

This research was supported in part by the Natural Sciences and Engineering Research Council, Grants No. A9087, OGP0036631 and A8775.

again $(ab)^* = b^*a^*$. Hence, in every case we have $(ab)^* = b^*a^*$, so $*$ is an involution. $\square$

Note that if $*$ is extended $\mathbf{Z}$-linearly to $\mathbf{Z}G$, then it is still an involution on $\mathbf{Z}G$. In fact, we have more.

LEMMA 2. *Let G and $*$ be as defined in Lemma 1. If $\alpha \in \mathbf{Z}G$, then $\alpha\alpha^* = \alpha^*\alpha$ is in the centre of $\mathbf{Z}G$.*

PROOF. Let g, h be any two elements in the support of α.

If $g, h \in Z(G)$, then gh is obtained in the expansion of $\alpha\alpha^*$ and $hg = gh$ is obtained in $\alpha^*\alpha$, with the same coefficient. Note that gh and hg are in $Z(G)$.

If $g \in Z(G)$ and $h \notin Z(G)$, then $g(eh)$ and hg are both obtained when expanding $\alpha\alpha^*$ and they have the same coefficient. Note that $g(eh) + hg = egh + gh$ is in the centre of $\mathbf{Z}G$. Also $(eh)g$ and gh are obtained in $\alpha^*\alpha$. They have the same coefficient as the terms hg and $g(eh)$ in $\alpha\alpha^*$, and $gh = hg$, $(eh)g = g(eh)$. Hence these products make the same (central) contribution to $\alpha\alpha^*$ and to $\alpha^*\alpha$.

The last case is where $g \notin Z(G)$ and $h \notin Z(G)$. If $gh \in Z(G)$, then $g(eh)$ is obtained in $\alpha\alpha^*$ while $(eh)g$ is obtained in $\alpha^*\alpha$ with the same coefficient, and Lemma 1 yields $(eh)g = e(gh) = g(eh)$.

Finally, assume $g \notin Z(G)$, $h \notin Z(G)$ and $gh \notin Z(G)$. Again, $g(eh)$ and $h(eg)$ are obtained in $\alpha\alpha^*$ and they have the same coefficients. Further Lemma 1 tells us that $g(eh) + h(eg) = hg + e(hg)$ is central. Also $(eh)g$ and $(eg)h$ are in $\alpha^*\alpha$, with the same coefficients as above. But $(eh)g = h(eg)$ and $(eg)h = g(eh)$, so the result is proved. $\square$

Now let us see how to compute units. For this we assume that G is a finite group such that $G/Z(G) \cong C_2 \times C_2$, and G/G' has exponent 2, 3, 4 or 6.

Let u be a unit in $\mathbf{Z}G$; we may assume it has augmentation 1. By Higman's result $\mathbf{Z}(G/G')$ has only trivial units [7], so $u = g + (1-e)a$ for some $g \in G$, $a \in \mathbf{Z}G$. Hence $u = g(1 + (1-e)g^{-1}a)$ and thus we may assume $g = 1$.

We note the following.

LEMMA 3. *Let G satisfy the two conditions listed above and let $*$ be as in Lemma 2. If $u = 1 + (1-e)\alpha$, then $uu^* = u^*u$ is in $\mathbf{Z}(Z(G))$. Hence u is a unit in $\mathbf{Z}G$ if and only if uu^* is a unit in $\mathbf{Z}(Z(G))$.*

PROOF. We know from Lemma 2 that $uu^* = u^*u$ is in $Z(\mathbf{Z}G)$. Let $u = 1 + (1-e)(\sum \alpha_g g)$. Then $u^* = 1 + (1-e)(\sum_{g\in Z(G)} \alpha_g g + \sum_{g\notin Z(G)} \alpha_g eg) = 1 + (1-e)(\sum_{g\in Z(G)} \alpha_g g - \sum_{g\notin Z(G)} \alpha_g g)$. Thus $uu^* = 1 + 2(1-e)(\sum_{g\in Z(G)} \alpha_g g) + (1-e)^2(\sum_{g\in Z(G)} \alpha_g g)^2 - (1-e)^2(\sum_{g\notin Z(G)} \alpha_g g)^2$. The first three terms in this sum are in $\mathbf{Z}(Z(G))$. In the final term, note that $gh \notin Z(G)$ if and only if $gh = ehg$ by Lemma 1 and $(1-e)ehg = -(1-e)hg$. Hence non-central products cancel. $\square$

https://doi.org/10.4153/CMB-1990-038-8 Published online by Cambridge University Press

We are now able to give a procedure to compute all units in some integral group rings.

PROPOSITION 4. *Let G be a finite group such that $G/Z(G) \cong C_2 \times C_2$, G/G' and $Z(G)$ both have exponent* 2, 3, 4 *or* 6. *Then* (1) *all units of $\mathbf{Z}G$ are (up to $\pm G$) of the form $u = 1 + (1-e)\alpha$, with $u^*u = uu^* = 1$;* (2) *this yields a set of quadratic diophantine equations for the coefficients of u, and thus the latter are "determined".*

PROOF. Let u be unit in $\mathbf{Z}G$. As before we may assume that u is of the form $1 + (1-e)\alpha$. Lemma 3 tells us that $uu^* = u^*u$ is in $\mathbf{Z}(Z(G))$, and Higman's result now guarantees that all such units are trivial. Observing that, in the proof of Lemma 3, every non-identity group element of uu^* had an even coefficient, we conclude that $uu^* = u^*u = 1$. This will yield a set of quadratic diophantine equations for the coefficients of u which are equivalent to $u = 1 + (1-e)\alpha$ being a unit, and the units of $\mathbf{Z}G$ are therefore determined. □

We give two examples illustrating how this procedure works. In the first, we classify the units in an interesting group of order 16 studied by Ritter and Sehgal [6], while in the second we classify again the well-known ([5]) units of the integral group ring $\mathbf{Z}D_4$.

EXAMPLE 1. Let $G = \langle a, b \mid a^4 = b^4 = 1,\ [b,a] = a^{-2}\rangle$. Here $G = \{a^i b^j \mid 0 \le i \le 3,\ 0 \le j \le 3\}$, $G' = \{1, a^2\}$ and $Z(G) = \{1, a^2, b^2, a^2b^2\}$. Note that $e = a^2$.

Any unit of the type $1 + (1-e)x$ can be written as

$$u = 1 + (1-e)(\alpha_1 + \alpha_2 b^2 + \alpha_3 a + \alpha_4 ab^2 + \alpha_5 b + \alpha_6 b^3 + \alpha_7 ab + \alpha_8 ab^3).$$

Hence

$$u^* = 1 + (1-e)(\alpha_1 + \alpha_2 b^2 - \alpha_3 a - \alpha_4 ab^2 - \alpha_5 b - \alpha_6 b^3 - \alpha_7 ab - \alpha_8 ab^3).$$

So

$$\begin{aligned} uu^* &= 1 + 2(1-e)(\alpha_1 + \alpha_2 b^2) + (1-e)^2(\alpha_1^2 + 2\alpha_1\alpha_2 b^2 + \alpha_2^2 - \alpha_3^2 e \\ &\quad - 2\alpha_3\alpha_4 e b^2 - \alpha_4^2 e - \alpha_5^2 b^2 - \alpha_6^2 b^2 - 2\alpha_5\alpha_6 - \alpha_7^2 b^2 - \alpha_8^2 b^2 \\ &\quad - 2\alpha_7\alpha_8) \\ &= 1 + 2(1-e)(\alpha_1 + \alpha_2 b^2) + 2(1-e)(\alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_4^2 - 2\alpha_5\alpha_6 \\ &\quad - 2\alpha_7\alpha_8) + 2(1-e)b^2(2\alpha_1\alpha_2 + 2\alpha_3\alpha_4 - \alpha_5^2 - \alpha_6^2 - \alpha_7^2 - \alpha_8^2). \end{aligned}$$

Since $uu^* = 1$, we conclude that u is a unit if and only if:

$$\begin{aligned} &\alpha_1 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_4^2 - 2\alpha_5\alpha_6 - 2\alpha_7\alpha_8 = 0, \text{ and} \\ &\alpha_2 + 2\alpha_1\alpha_2 + 2\alpha_3\alpha_4 - \alpha_5^2 - \alpha_6^2 - \alpha_7^2 - \alpha_8^2 = 0. \end{aligned}$$

Subtracting the second condition from the first, we obtain

$$\alpha_1 - \alpha_2 + (\alpha_1 - \alpha_2)^2 + (\alpha_3 - \alpha_4)^2 + (\alpha_5 - \alpha_6)^2 + (\alpha_7 - \alpha_8)^2 = 0.$$

https://doi.org/10.4153/CMB-1990-038-8 Published online by Cambridge University Press

There are two sets of solutions to this diophantine equation, namely

1. $\alpha_1 = \alpha_2, \alpha_3 = \alpha_4, \alpha_5 = \alpha_6, \alpha_7 = \alpha_8$;
2. $\alpha_1 = \alpha_2 - 1, \alpha_3 = \alpha_4, \alpha_5 = \alpha_6, \alpha_7 = \alpha_8$.

In case 1, $u = 1 + (1-e)(1+b^2)(\alpha_1 + \alpha_3 a + \alpha_5 b + \alpha_7 ab)$ and our conditions reduce to

$$(1+2\alpha_1)^2 + (2\alpha_3)^2 - (2\alpha_5)^2 - (2\alpha_7)^2 = 1 + 2\alpha_1.$$

In case 2, $u = e + (1-e)(1+b^2)(\alpha_1 + \alpha_3 a + \alpha_5 b + \alpha_7 ab) = ev$, where v is a unit as in case 1.

EXAMPLE 2. Let $D_4 = \langle a, b \mid a^4 = b^2 = 1,\ a^b = a^{-1}\rangle$, the dihedral group of order 8. Here $G = \{a^i b^j \mid 0 \leq i \leq 3,\ 0 \leq j \leq 1\}$, $D_4' = \{1, a^2\}$, $Z(D_4) = \{1, a^2\}$ and $e = a^2$. Any unit of the type $1 + (1-e)x$ can be written as

$$u = 1 + (1-e)(\alpha_1 + \alpha_2 a + \alpha_3 b + \alpha_4 ab).$$

So

$$uu^* = 1 + 2(1-e)(\alpha_1 + \alpha_1^2 + \alpha_2^2 - \alpha_3^2 - \alpha_4^2).$$

Again since $uu^* = 1$, we obtain that u is a unit if and only if:

$$(1+2\alpha_1)^2 + (2\alpha_2)^2 - (2\alpha_3)^2 - (2\alpha_4)^2 = 1.$$

We close with a few remarks. As mentioned in [6], 2-groups create the main problem in computing units. In [6], Ritter and Sehgal give a concrete generating set for a subgroup of finite index of the unit group of integral group rings $\mathbf{Z}G$, where G belongs to a wide class of finite groups. The restrictions on this class are on the Sylow 2-subgroups, and the group mentioned in Example 1 is not in the class.

However, this note provides a method of computing all units of the integral group rings $\mathbf{Z}G$, where G is in the class $\mathcal{G}$ of all finite groups G satisfying the conditions mentioned in Proposition 4. One easily verifies that if a group G is a direct product $H \times A$, where A is an abelian group, then G is in $\mathcal{G}$ if and only if H is in $\mathcal{G}$ and $Z(G) \times A$ has exponent 2, 3, 4 or 6. Further, one can verify that any group G in $\mathcal{G}$ can be written in the form $H \times A$, where A is an abelian group and H cannot be written as such a direct product. One could call the latter an indecomposable group in the class $\mathcal{G}$.

A somewhat tedious but straightforward argument shows that there are very few such indecomposable groups. The quaternion group Q and the dihedral group D_4 are the two examples of order 8, while there are four of order 16, namely

$$\langle a, b, c \mid a^4 = [a, b] = [a, c] = 1,\ a^2 = b^2 = c^2 = [b, c]\rangle,$$
$$\langle a, b \mid a^4 = b^4 = 1,\ [b, a] = a^{-2}\rangle,$$
$$\langle a, b \mid a^4 = b^4 = (ab)^2 = [a^2, b] = 1\rangle \text{ and}$$
$$\langle a, b \mid a^8 = (ab)^2 = 1,\ b^2 = a^2\rangle.$$

There are three examples of order 32, namely

$$\langle a,b,c \mid a^4 = b^4 = (ab)^2 = [a^2,b] = [a,c] = [b,c] = 1,\ c^2 = [a,b]\rangle,$$
$$\langle a,b \mid a^4 = b^4 = [a^2,b] = [a,b^2] = [a,b]^2 = 1\rangle \text{ and}$$
$$\langle a,b \mid a^8 = [a^2,b] = [a,b^2] = 1,\ a^4 = b^4 = [a,b]\rangle.$$

Finally, there is one indecomposable group of order 64, namely

$$\langle a,b,c \mid a^4 = b^4 = [a^2,b] = [a,b^2] = [a,b]^2 = [a,c] = [b,c] = 1,\ c^2 = [a,b]\rangle.$$

Acknowledgement. The authors would like to thank the referee for several valuable comments and suggestions.

References

1. P. J. Allen and C. Hobby, *A characterization of units in* $\mathbf{Z}[A_4]$, J. Algebra **66**, (1980) 534–543.
2. P. J. Allen and C. Hobby, *A note on the unit group of* $\mathbf{Z}S_3$, Proc. A.M.S. **99** (1) (1987), 9–14.
3. E. G. Goodaire and M. M. Parmenter, *Units in alternative loop rings*, Israel J. Math. **53** (2) (1986), 209–216.
4. I. Hughes and K. R. Pearson, *The group of units of the integral group ring* $\mathbf{Z}S_3$, Canad. Math. Bull. **15** (1972), 529–534.
5. C. S. Polcino Milies, *The group of units of the integral group ring* $\mathbf{Z}D_4$, Boletim Soc. Bras. Mat. **4** (2) (1973), 85–92.
6. J. Ritter and S. K. Sehgal, *Construction of units in integral group rings of finite nilpotent groups*, Trans. Amer. Math. Soc. to appear 1990.
7. S. K. Sehgal, Topics in Group Rings, *Marcel Dekker, New York*, 1978.

Memorial University of Newfoundland,
St. John's, Canada
A1C 5S7