

## CENTRAL UNITS OF THE INTEGRAL GROUP RING $\mathbb{Z}A_5$

YUANLIN LI AND M. M. PARMENTER

(Communicated by Ronald M. Solomon)

ABSTRACT. There are very few cases known of nonabelian groups  $G$  where the group of central units of  $\mathbb{Z}G$ , denoted  $Z(U(\mathbb{Z}G))$ , is nontrivial and where the structure of  $Z(U(\mathbb{Z}G))$ , including a complete set of generators, has been determined. In this note, we show that the central units of augmentation 1 in the integral group ring  $\mathbb{Z}A_5$  form an infinite cyclic group  $\langle u \rangle$ , and we explicitly find the generator  $u$ .

### 1. INTRODUCTION

Let  $\mathbb{Z}G$  denote the integral group ring of a group  $G$ ,  $U(\mathbb{Z}G)$  the group of units of such a group ring and  $V(\mathbb{Z}G)$  the subgroup of units of augmentation 1. We will use the term trivial units to describe the subgroup  $\pm G$  of  $U(\mathbb{Z}G)$ .

For any group it is possible to define the important families of bicyclic and Bass cyclic units in  $V(\mathbb{Z}G)$  (see [6] for the definitions). It turns out that for many finite groups, these families, taken together, generate a subgroup of finite index in  $V(\mathbb{Z}G)$  ([4], [6]). The problem of finding the full structure of  $V(\mathbb{Z}G)$ , including a complete set of generators, seems to be more difficult and has been settled for only a small number of special cases (see [6] for an excellent survey).

Even less is known about  $Z(U(\mathbb{Z}G))$ , the group of central units of  $\mathbb{Z}G$ . When  $G$  is finite, Ritter and Sehgal ([3], [6]) proved the following theorem giving necessary and sufficient conditions for  $Z(U(\mathbb{Z}G))$  to be trivial.

**Theorem 1.** *Let  $G$  be a finite group. All central units of  $\mathbb{Z}G$  are trivial if and only if for every  $x \in G$  and every natural number  $j$  relatively prime to  $|G|$ ,  $x^j$  is conjugate to  $x$  or  $x^{-1}$ .*

Also, when  $G$  is finite Ritter and Sehgal [5] constructed a finite set of generators for a subgroup of finite index in  $Z(U(\mathbb{Z}G))$ , while Jespers, Parmenter and Sehgal [1] found a different set of generators which works for finitely generated nilpotent groups (and some others as well). In the latter case, the generators were constructed from Bass cyclic units in  $\mathbb{Z}G$  and the construction depended on the existence of a very well behaved finite normal series in  $G$ . In general, however, there is no simple procedure known for constructing examples of central units in  $\mathbb{Z}G$  (even when Theorem 1 guarantees their existence). Also there are very few cases of nonabelian groups where  $Z(U(\mathbb{Z}G))$  is nontrivial and where a complete set of generators has been obtained for  $Z(U(\mathbb{Z}G))$ .

---

Received by the editors July 22, 1995.

1991 *Mathematics Subject Classification.* Primary 16U60, 20C05.

The second author was supported in part by NSERC grant A8775.

In this paper we make some progress on these questions. Since  $A_5$ , the alternating group on 5 letters, is a simple group, the procedure in [1] cannot be used to construct central units in  $\mathbb{Z}A_5$ . However, if  $\alpha = (12345)$  then  $\alpha$  and  $\alpha^{-1}$  are conjugate to each other but not to  $\alpha^2 = \alpha^7$ , so Theorem 1 says that  $Z(U(\mathbb{Z}A_5))$  is nontrivial. We will show that  $Z(U(\mathbb{Z}A_5)) = \pm\langle u \rangle$  where  $\langle u \rangle$  is an infinite cyclic group. More significantly, we will explicitly find the generator  $u$ , thus obtaining a complete description of  $Z(U(\mathbb{Z}A_5))$ .

The work described here will form part of the first author's doctoral dissertation.

## 2. MAIN RESULTS

Recall that whenever  $R$  is a commutative ring with 1, the centre of  $RG$  is a free  $R$ -module with basis consisting of the finite conjugacy class sums in  $RG$ .  $A_5$  has 5 distinct conjugacy classes, and we will denote the corresponding class sums by  $C_0, C_1, C_2, C_3, C_4$  where  $C_0 = 1, C_1$  is the sum of elements conjugate to  $(12345)$ ,  $C_2$  is the sum of elements conjugate to  $(13524)$ ,  $C_3$  is the sum of all 3-cycles and  $C_4$  is the sum of all elements which are the product of 2 disjoint transpositions. We will need to use the following identities:

$$\begin{aligned}
C_1^2 &= 12 + 5C_1 + C_2 + 3C_3, \\
C_1C_2 &= C_1 + C_2 + 3C_3 + 4C_4, \\
C_1C_3 &= 5C_1 + 5C_2 + 3C_3 + 4C_4, \\
C_1C_4 &= 5C_2 + 3C_3 + 4C_4, \\
C_2^2 &= 12 + C_1 + 5C_2 + 3C_3, \\
C_2C_3 &= 5C_1 + 5C_2 + 3C_3 + 4C_4, \\
C_2C_4 &= 5C_1 + 3C_3 + 4C_4, \\
C_3^2 &= 20 + 5C_1 + 5C_2 + 7C_3 + 8C_4, \\
C_3C_4 &= 5C_1 + 5C_2 + 6C_3 + 4C_4, \\
C_4^2 &= 15 + 5C_1 + 5C_2 + 3C_3 + 2C_4.
\end{aligned}$$

Suppose  $u \in Z(V(\mathbb{Z}A_5))$ . Let  $u = \sum a_i C_i$  and  $u^{-1} = \sum b_i C_i$  where  $a_i, b_i \in \mathbb{Z}$ ,  $0 \leq i \leq 4$ . Since  $uu^{-1} = 1$ , the identities just stated can be used to give 5 equations, one for each  $C_i$  (some of the details will be omitted here as they are routine). The augmentation map tells us that  $a_0 + 12a_1 + 12a_2 + 20a_3 + 15a_4 = 1$  and similarly for the  $b_i$ . Substituting for  $a_0$  and  $b_0$ , we see that the equation arising from  $C_0$  can be ignored as it is a linear combination of the rest. The other 4 equations are:

$$\begin{aligned}
(1 - 19a_1 - 11a_2 - 15a_3 - 15a_4)b_1 + (-11a_1 + a_2 + 5a_3 + 5a_4)b_2 \\
+ (-15a_1 + 5a_2 + 5a_3 + 5a_4)b_3 + (-15a_1 + 5a_2 + 5a_3 + 5a_4)b_4 = -a_1,
\end{aligned}$$

$$\begin{aligned}
(a_1 - 11a_2 + 5a_3 + 5a_4)b_1 + (1 - 11a_1 - 19a_2 - 15a_3 - 15a_4)b_2 \\
+ (5a_1 - 15a_2 + 5a_3 + 5a_4)b_3 + (5a_1 - 15a_2 + 5a_3 + 5a_4)b_4 = -a_2,
\end{aligned}$$

$$\begin{aligned}
(3a_1 + 3a_2 - 9a_3 + 3a_4)b_1 + (3a_1 + 3a_2 - 9a_3 + 3a_4)b_2 \\
+ (1 - 9a_1 - 9a_2 - 33a_3 - 9a_4)b_3 + (3a_1 + 3a_2 - 9a_3 + 3a_4)b_4 = -a_3,
\end{aligned}$$

$$\begin{aligned}
(4a_2 + 4a_3 - 8a_4)b_1 + (4a_1 + 4a_3 - 8a_4)b_2 + (4a_1 + 4a_2 + 8a_3 - 16a_4)b_3 \\
+ (1 - 8a_1 - 8a_2 - 16a_3 - 28a_4)b_4 = -a_4.
\end{aligned}$$

Adding these together, we obtain

$$(1 - 15(a_1 + a_2 + a_3 + a_4))(b_1 + b_2 + b_3 + b_4) = -(a_1 + a_2 + a_3 + a_4).$$

Since we are dealing with integers, this means that  $a_1 + a_2 + a_3 + a_4 = 0$  and  $b_1 + b_2 + b_3 + b_4 = 0$ . Substituting for  $a_1$  and  $b_1$ , and ignoring the first equation which is then a linear combination of the others, we are reduced to

$$(1 + 4a_2 - 8a_3 - 8a_4)b_2 + (-8a_2 - 4a_3 - 4a_4)b_3 \\ + (-8a_2 - 4a_3 - 4a_4)b_4 + a_2 = 0,$$

$$(1 - 12a_3)b_3 + a_3 = 0,$$

$$(-8a_2 - 4a_3 - 4a_4)b_2 + (-4a_2 - 12a_4)b_3 \\ + (1 - 4a_2 - 12a_3 - 12a_4)b_4 + a_4 = 0.$$

It follows from the second equation that  $1 - 12a_3$  divides  $a_3$ , forcing  $a_3 = 0$  and  $b_3 = 0$ . We are now reduced to

$$(1 + 4a_2 - 8a_4)b_2 + (-8a_2 - 4a_4)b_4 = -a_2, \\ (-8a_2 - 4a_4)b_2 + (1 - 4a_2 - 12a_4)b_4 = -a_4.$$

The determinant of the  $2 \times 2$  matrix arising here is

$$D = 1 - 20(4a_2^2 + 4a_2a_4 - 4a_4^2 + a_4) = -20(2a_2 + a_4)^2 + (10a_4 - 1)^2.$$

We note that  $D \neq 0$  and also

$$b_2 = \frac{(2a_2 + a_4)^2 - (5a_4^2 + a_2)}{D}, \\ b_4 = \frac{10a_4^2 - a_4 - 2(2a_2 + a_4)^2}{D}.$$

Since  $2b_2 + b_4 = \frac{-2a_2 - a_4}{D}$  is an integer, we have that  $D|(2a_2 + a_4)$ . The equation for  $b_4$  then says that  $D|a_4(10a_4 - 1)$ . We conclude from the equation for  $D$  that  $\gcd(D, a_4) = 1$ , so  $D|(10a_4 - 1)$ . Setting  $2a_2 + a_4 = Du$  and  $10a_4 - 1 = Dv$ , we obtain  $D = D^2(v^2 - 20u^2)$ . Since  $D \neq 0$  and  $D \neq -1$ , it follows that  $D = 1$ .

We then have that  $(10a_4 - 1)^2 - 20(2a_2 + a_4)^2 = 1$ , and this can be rewritten as  $(2a_2 + a_4)^2 = (5a_4 - 1)a_4$ . It follows that  $a_4$  is an even number and that both  $a_4$  and  $5a_4 - 1$  are  $\pm$  (perfect squares). Let  $a_4 = \pm 4Y^2$  and  $5a_4 - 1 = \pm X^2$ . If  $a_4 > 0$ , we get  $X^2 - 20Y^2 = -1$ . Since the left hand side is 0 or 1 (mod 4), this equation has no solution.

If  $a_4 \leq 0$ , we have the Pell's equation  $X^2 - 20Y^2 = 1$ . Working back through the identities which have been developed, we have proved

**Proposition 2.**  $Z(U(\mathbb{Z}A_5)) = \{\pm u | u = (1 + 12Y^2)C_0 + (\pm XY + 2Y^2)C_1 + (\mp XY + 2Y^2)C_2 - 4Y^2C_4 \text{ where } X, Y \text{ range through all solutions of the Pell's equation } X^2 - 20Y^2 = 1\}$ .

Note that if  $X, Y$  is any solution of the above Pell's equation, then the solution  $-X, Y$  gives the same units, so we may assume  $X$  and  $Y$  are nonnegative. Also, if  $X, Y$  is a particular solution of the equation, then the 2 units obtained from this

solution are inverse to each other – i.e., if

$$u = (1 + 12Y^2)C_0 + (XY + 2Y^2)C_1 + (-XY + 2Y^2)C_2 - 4Y^2C_4,$$

then  $u^{-1} = (1 + 12Y^2)C_0 + (-XY + 2Y^2)C_1 + (XY + 2Y^2)C_2 - 4Y^2C_4$ .

For example, the solution  $X = 9, Y = 2$  gives the inverse pair  $v = 49 + 26C_1 - 10C_2 - 16C_4$ ,  $v^{-1} = 49 - 10C_1 + 26C_2 - 16C_4$ . In fact, our main theorem shows that this particular  $v$  is more than just an isolated example.

**Theorem 3.**  $Z(U(\mathbb{Z}A_5)) = \pm\langle v \rangle$  where  $v$  is as defined above.

A careful discussion of solutions to Pell's equation can be found in [2], but for our purposes the crucial result is

**Lemma 4** ([2], Theorem 7.26). *Consider the Pell's equation  $x^2 - dy^2 = 1$  where  $d$  is a positive integer which is not a perfect square. Let  $X_1, Y_1$  be the least positive solution to the equation. Then all positive solutions are given by  $X_n, Y_n$  for  $n = 1, 2, 3, \dots$ , where  $X_n$  and  $Y_n$  are the integers defined by  $X_n + Y_n\sqrt{d} = (X_1 + Y_1\sqrt{d})^n$ .*

*Proof of Theorem 3.* By Proposition 2 and the subsequent remark, we are considering nonnegative solutions to the equation  $X^2 - 20Y^2 = 1$ . When  $Y = 0$  we get  $u = 1$ , while there is no solution when  $X = 0$ , so we may assume  $X, Y > 0$ .

All positive solutions are given by  $X_n, Y_n$  as stated in Lemma 4. For each such  $n$ , define

$$u_n = 1 + 12Y_n^2 + (X_nY_n + 2Y_n^2)C_1 + (-X_nY_n + 2Y_n^2)C_2 - 4Y_n^2C_4.$$

It is easy to see that  $X = 9, Y = 2$  is the least positive solution of  $X^2 - 20Y^2 = 1$ , so  $u_1 = v$ .

Using our earlier remarks on inverses, we will be finished if we can show that  $u_n = u_1^n$  for all  $n \geq 1$ . This we will do by induction, the case  $n = 1$  being obvious. Assume the result is true when  $n = k$  for some  $k \geq 1$ . Since  $u_1^{k+1}$  is a central unit, Proposition 2 tells us that we only need prove that the identity coefficient of  $u_1^{k+1}$  equals  $1 + 12Y_{k+1}^2$  and that the coefficient of  $C_1$  in  $u_1^{k+1}$  equals  $X_{k+1}Y_{k+1} + 2Y_{k+1}^2$ .

The identity coefficient of  $u_1^{k+1} = u_1u_k$  is

$$\begin{aligned} & 49(1 + 12Y_k^2) + 12(26)(X_kY_k + 2Y_k^2) + 12(-10)(-X_kY_k + 2Y_k^2) + 15(-16)(-4Y_k^2) \\ &= 49 + 432X_kY_k + 1932Y_k^2. \end{aligned}$$

On the other hand, Lemma 4 says that  $1 + 12Y_{k+1}^2 = 1 + 12(9Y_k + 2X_k)^2 = 1 + 12(81Y_k^2 + 36X_kY_k + 4(20Y_k^2 + 1)) = 49 + 432X_kY_k + 1932Y_k^2$ , as desired.

The coefficient of  $C_1$  in  $u_1^{k+1}$  equals

$$\begin{aligned} & 49(X_kY_k + 2Y_k^2) + 26(1 + 12Y_k^2) + 5(26)(X_kY_k + 2Y_k^2) + 26(-X_kY_k + 2Y_k^2) \\ & \quad + (-10)(X_kY_k + 2Y_k^2) + (-10)(-X_kY_k + 2Y_k^2) + 5(-10)(-4Y_k^2) \\ & \quad + 5(-16)(-X_kY_k + 2Y_k^2) + 5(-16)(-4Y_k^2) \\ &= 26 + 233X_kY_k + 1042Y_k^2. \end{aligned}$$

Lemma 4 says that  $X_{k+1}Y_{k+1} + 2Y_{k+1}^2 = (9X_k + 40Y_k)(2X_k + 9Y_k) + 2(2X_k + 9Y_k)^2 = 26(20Y_k^2 + 1) + 233X_kY_k + 522Y_k^2 = 26 + 233X_kY_k + 1042Y_k^2$ , and this completes the proof.  $\square$

## REFERENCES

1. E. Jespers, M.M. Parmenter and S.K. Sehgal, Central units of integral group rings of nilpotent groups. Proc. Amer. Math. Soc. 124 (1996), 1007–1012.
2. Ivan Niven and H.S. Zuckerman, *An Introduction to the Theory of Numbers* (4th edition), Wiley, 1980. MR **81g**:10001
3. J. Ritter and S.K. Sehgal, Integral group rings with trivial central units, Proc. Amer. Math. Soc. 108 (1990), 327–329. MR **90d**:16009
4. J. Ritter and S.K. Sehgal, Construction of units in integral group rings of finite nilpotent groups, Trans. Amer. Math. Soc. 324(2) (1991), 603–621. MR **91h**:20008
5. J. Ritter and S.K. Sehgal, Units of group rings of solvable and Frobenius groups over large rings of cyclotomic integers, Journal of Algebra 158 (1993), 116–129. MR **95d**:16045
6. S.K. Sehgal, *Units in Integral Group Rings*, Longman, 1993. MR **94m**:16039

DEPARTMENT OF MATHEMATICS AND STATISTICS, MEMORIAL UNIVERSITY OF NEWFOUNDLAND,  
ST. JOHN'S, NEWFOUNDLAND, CANADA A1C 5S7

*E-mail address:* yuanlin@fermat.math.mun.ca

*E-mail address:* mparmen@plato.ucs.mun.ca