BULL. AUSTRAL. MATH. SOC. 16A26
VOL. 7 (1972), 169-182.

On the units of a modular group ring

K.R. Pearson

It is shown that a finite group G is a normal subgroup of the group of units of the group ring of G over the ring of integers modulo n if and only if G is abelian or $n = 2$ and G is isomorphic to the symmetric group on 3 letters.

Let R be a ring with identity 1, G a finite group and let RG denote the corresponding group ring. If α is a unit in R and if $g \in G$ then αg is a unit in RG, and is called a *trivial* unit. In particular $\{1g \mid g \in G\}$ is always a subgroup of the group $(RG)^*$ of units of RG; by a slight abuse of notation this set will also be denoted by G. We consider the following conditions.

I Every unit in RG is trivial.

II Every unit of finite order in RG is trivial.

III Every conjugate in $(RG)^*$ of an element of G is trivial; or equivalently, G is a normal subgroup of $(RG)^*$.

It is clear that, in general, I $\Rightarrow$ II $\Rightarrow$ III.

For the case $R = Z$, the ring of rational integers, these conditions have been examined by Higman [8] and Berman [2]. Higman showed that I holds if and only if G is either abelian of exponent dividing 4 or 6 or hamiltonian of order a power of 2. Berman showed that II holds if and only if G is either abelian or hamiltonian of order a power of 2. In addition, although it is not stated explicitly, his proof shows that (still when $R = Z$) II and III are equivalent.

If R has characteristic zero, it is clear that any one of these

Received 12 April 1972.

three conditions implies the corresponding condition for the case $R = Z$. Hence the results of Higman and Berman give some information about the general case when R has characteristic zero.

In this case we consider the conditions when $R = Z_n$, the ring of rational integers modulo n. The results then give some information about the case where R has finite characteristic. Because Z_nG is a finite ring it is clear that, when $R = Z_n$, I and II are equivalent. We prove the following results.

THEOREM 1. *Let G be a finite group. G is a normal subgroup of $(Z_nG)^*$ if and only if G is abelian or $n = 2$ and $G \simeq S_3$, the symmetric group on 3 letters.*

THEOREM 2. *Let G be a finite nontrivial group. Every unit in Z_nG is trivial if and only if $n = 2$ and $|G| \leq 3$ or $n = 3$ and $|G| = 2$.*

A result related to Theorem 1 has been proved in [4] by Eldridge. He has proved that if G is a locally finite p-group and H is a subgroup of G, then H is normal in $(Z_pG)^*$ if and only if H is central in G.

§1 contains some preliminary results which are perhaps of independent interest. Theorem 1 is proved in §§2-4, while Theorem 2 is proved in §5.

1. The behaviour of unit groups under ring homomorphisms

Let R be a ring with identity and let $\phi : R \to S$ be a surjective ring homomorphism. It is easy to see that ϕ maps the group R^* of units of R into the group S^* of units of S. That $R^*\phi$ is not always the whole of S^* may be seen by considering, for example, the canonical homomorphism from Z to Z/nZ. It is of interest to know conditions under which $\phi : R^* \to S^*$ is surjective. When the kernel of ϕ is contained in the Jacobson radical of R this is known to be the case (see (2.1) of [6] or Lemma 1 of [5]). The following result shows that it is also the case when R is artinian (irrespective of the kernel of ϕ).

THEOREM 3. *Let R be a ring with identity such that R/J is artinian, where J is the Jacobson radical of R. If $\phi : R \to S$ is a*

https://doi.org/10.1017/S0004972700044956 Published online by Cambridge University Press

surjective ring homomorphism then ϕ *induces a surjective group homomorphism* $\phi : R^* \to S^*$, *where* R^* *and* S^* *denote the group of units of* R *and* S *respectively.*

Proof. We must show that ϕ is onto. Let K denote the kernel of ϕ.

Suppose firstly that $J = 0$. Then R is an internal direct sum

$$R = R_1 \dot{+} \ldots \dot{+} R_t ,$$

where each R_i is a simple artinian ring. By renumbering if necessary we can assume that

$$K = R_{u+1} \dot{+} \ldots \dot{+} R_t .$$

Suppose $x \in R$ is such that $x\phi \in S^*$; then there is an element y in R such that $xy-1 \in K$ and $yx-1 \in K$. Let

$$1 = e_1 + \ldots + e_t ,$$

where $e_i \in R_i$. Then if

$$z = xe_1 + \ldots + xe_u + e_{u+1} + \ldots + e_t ,$$

$$w = ye_1 + \ldots + ye_u + e_{u+1} + \ldots + e_t ,$$

$zw = 1 = wz$ and $z-x \in K$. Thus $z \in R^*$ and $z\phi = x\phi$.

Now consider the general case. Suppose $x \in R$ is such that $x\phi \in S^*$. Then $x+K \in (R/K)^*$ and so $x+(J+K) \in [R/(J+K)]^*$. Since $J \subseteq J+K$ there is a natural homomorphism $\psi : R/J \to R/(J+K)$. Because R/J is semisimple it follows from the above that there exists $x_1 \in R$ such that $x_1+J \in (R/J)^*$ and $x_1 + (J+K) = x + (J+K)$. By Lemma 1 of [5], there exists $y \in R^*$ such that $x_1 + J = y + J$. Hence there exists $k \in K$, $j \in J$ such that

$$x + k = y + j = y\left(1+y^{-1}j\right) .$$

But $y^{-1}j \in J$, so $1+y^{-1}j \in R^*$ and hence $z = y+j \in R^*$. Also $z\phi = x\phi$ since $z-x \in K$.

COROLLARY 4. *Let R be an artinian ring with identity and let G be a finite group such that $G \triangleleft (RG)^*$. If $P \triangleleft G$ then $(G/P) \triangleleft [R(G/P)]^*$.*

Proof. Since RG is artinian ([8], Appendix 2, Proposition 6) we can apply the theorem to the homomorphism $\phi : RG \to R(G/P)$ which extends the identity on R, and the canonical homomorphism from G to G/P.

COROLLARY 5. *If $G \triangleleft \left(Z_nG\right)^*$ and m divides n then $G \triangleleft \left(Z_mG\right)^*$.*

If R is a finite ring

$$\delta(R) = |R^*|/|R| ,$$

the proportion of invertible elements in R, has been considered in [6]. If $\phi : R \to S$ is a surjective ring homomorphism, it is shown in (3.2) of [6] that $\delta(R) = \delta(S)$ if the kernel of ϕ equals the Jacobson radical of R.

PROPOSITION 6. *Let R be a finite ring and let $\phi : R \to S$ be a surjective ring homomorphism with kernel K. Then $\delta(R) = \delta(S)$ if and only if K is contained in the Jacobson radical of R.*

Proof. ϕ induces a surjective group homomorphism from R^* to S^* whose kernel is $R^* \cap (1+K)$. It is thus easy to see that $\delta(R) = \delta(S)$ if and only if $1+K \subseteq R^*$, which in turn is the case if and only if K is a quasi-regular ideal.

2. Outline the proof of Theorem 1

If G is abelian, it is clear that $G \triangleleft \left(Z_nG\right)^*$. That $S_3 \triangleleft \left(Z_2S_3\right)^*$ is shown in the following lemma. This completes the sufficiency part of Theorem 1.

LEMMA 7. $S_3 \triangleleft \left(Z_2S_3\right)^*$.

Proof. If $S_3 = \langle a, b \mid a^2 = b^3 = 1, ba = ab^2 \rangle$ then $\theta : S_3 \to Z_2 \oplus M_2\left(Z_2\right)$ given by

$$a\theta = \left(1, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right) , \quad b\theta = \left(1, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\right)$$

https://doi.org/10.1017/S0004972700044956 Published online by Cambridge University Press

defines a group homomorphism, and so can be extended to a ring homomorphism $\theta : Z_2S_3 \to Z_2 \oplus M_2(Z_2)$. θ is onto and its kernel is $J = \{0, \gamma\}$ where $\gamma = 1 + b + b^2 + a + ab + ab^2$. $\gamma^2 = 0$ and J is the radical of Z_2S_3 . By Theorem 3, θ induces a surjective homomorphism from $(Z_2S_3)^*$ onto $GL(2, Z_2)$ whose kernel is $1 + J$. Since $|GL(2, Z_2)| = 6$ and since θ is one-to-one when restricted to S_3 it follows that $(Z_2S_3)^* = S_3(1+J)$. Because γ is in the centre of Z_2S_3 , we see that $(Z_2S_3)^* = S_3 \times (1+J)$ and $S_3 \triangleleft (Z_2S_3)^*$.

The necessity part of Theorem 1 remains. Suppose that $G \triangleleft (Z_nG)^*$ and that G is not abelian. In §§3, 4 we consider the case where n is a prime and show that $n = 2$ and $G \simeq S_3$. In view of Corollary 5 above it follows that $G \simeq S_3$ and $n = 2^k$ for some $k \geq 1$. If $k \geq 2$ and $y = 2^{k-1}$ then $(1+ya)^2 = 1$ so that $1 + ya$ is a unit of order 2 in Z_nS_3 . But

$$(1+ya)b(1+ya) = b + yab + yab^2 \notin S_3 .$$

Hence $k = 1$. This will complete the necessity part.

3.

LEMMA 8. *If p is a prime, if p does not divide $|G|$ and if $G \triangleleft (Z_pG)^*$, then G is abelian.*

Proof. For suppose, if possible, that G is not abelian. Since $R = Z_pG$ is semisimple, there exists a central idempotent e in R such that $Re \simeq M_n(GF(p^k))$ for some $n \geq 2$ and $k \geq 1$. Since $G \triangleleft R^*$ it follows that $Ge \triangleleft (Re)^* \simeq GL(n, p^k)$. Let $\theta : (Re)^* \to GL(n, p^k)$ be an isomorphism. Now p divides $|SL(n, p^k)|$ ([1], Theorem 4.11) so that $SL(n, p^k)\theta^{-1}$ is not contained in Ge . Since the centre of $GL(n, p^k)$ is

https://doi.org/10.1017/S0004972700044956 Published online by Cambridge University Press

contained in the centre of $M_n(\mathrm{GF}(p^k))$ ([1], Theorem 4.8), $Ge \subseteq$ centre $(Re)^*$ would mean $Ge \subseteq$ centre (Re) and then Re would be commutative since it is spanned by Ge over Z_pe. Thus it follows from [1], Theorem 4.9, that $n = 2$, $k = 1$ and $p = 2$ or 3.

If $p = 2$, we get $|Ge| = 3$ since $\mathrm{GL}(2, 2) \simeq S_3$. But then Re has dimension at most 3 over Z_pe and so cannot be isomorphic to $M_2(Z_2)$.

Thus $p = 3$. Now the only normal subgroup of $\mathrm{GL}(2, 3)$ which has order not divisible by 3 and which is not contained in the centre of $\mathrm{GL}(2, 3)$ is isomorphic to the quaternion group H of order 8. Thus $Ge \simeq H$. Since Ge is a homomorphic image of G it follows from Corollary 4 that $H \triangleleft (Z_3H)^*$. Let

$$H = \langle i, j \mid i^2 = j^2 = t,\ t^2 = 1,\ ji = tij \rangle .$$

Then in Z_3H, if $x = (i+j+ij)(1-t)$ we have $x^2 = 0$ and therefore $1 + x$ is a unit with inverse $1 - x$. But

$$(1+x)i(1-x) = 1 - j - ij - t + ti + tj + tij \notin S .$$

Thus we have a contradiction.

LEMMA 9. *If p is a prime ≥ 3, if p divides $|G|$ and if $G \triangleleft (Z_pG)^*$, then G is abelian.*

Proof. Let H be a p-Sylow subgroup of G. We first show that H is in the centre of G. For let $g \in G$, $h \in H$ and let h have order p^m with $m \geq 1$. Since $(1-h)^{p^m} = 1 - h^{p^m} = 0$, $1 - h$ is nilpotent and hence so is $(1-h)^2$. Thus $1 - (1-h)^2 = 2h - h^2$ is a unit in Z_pG. Hence there exists $g' \in G$ such that $(2h-h^2)g = g'(2h-h^2)$, or

$$2hg - h^2g = 2g'h - g'h^2 .$$

Since $h \neq e$, hg and h^2g are distinct. Thus we get two possibilities, namely

(i) $g'h^2 = h^2g$ and $g'h = hg$, in which case $gh = hg$; or

(ii) $2 = -1$ (that is, $p = 3$), $g'h = h^2g$ and $g'h^2 = hg$, in which case $g^{-1}hg = h^{-1}$.

Suppose, if possible, that $gh \neq hg$; then $p = 3$, $g \neq e$, $g \neq h^{-1}$ and $ghg^{-1} = h^{-1}$. Since $ghg^{-1} = h^{-1}$, it is easy to see that $(1-h)g$ is nilpotent, and so $\alpha = 1 + (1-h)g$ is a unit. Hence there exists $h' \in G$ such that $\alpha h = h'\alpha$, which gives

$$h + gh - hgh = h' + h'g - h'hg .$$

Since h, gh and hgh are distinct, we have $h'hg = hgh = g$ and $h' = h^{-1}$. Then $h + gh = h^{-1} + h^{-1}g$. Since $h \neq h^{-1}$ we get $h^{-1} = gh$, whence $g = h^{-2}$ and we have a contradiction.

We can now show that G is abelian. For suppose, if possible, that $x, y \in G$ and $xy \neq yx$. If $h \neq 1$ is an element of H then h is in the centre of G and $\beta = 1 + (1-h)x$ is a unit. Thus there exists $z \in G$ such that $\beta y = z\beta$, and so

$$y + xy - hxy = z + zx - hzx .$$

Since $xy \neq yx$, $y \neq e$ and $x \neq h^{-1}$ so that y, xy and hxy are distinct. Thus $hxy = hzx$ and $z = xyx^{-1}$. Now $y + xy = xyx^{-1} + xy$, which means $y = xyx^{-1}$ or $xy = yx$.

4. $n = 2$ and $|G|$ is even

We are left with $G \triangleleft (Z_2G)^*$ and $|G|$ even. We show that either G is abelian or $G \simeq S_3$.

In what follows we will often have a situation similar to the following. Suppose

$$x_1 + \ldots + x_n = y_1 + \ldots + y_n ,$$

where $x_i, y_i \in Z_2G$ and $x_1, \ldots, x_n$ are distinct. Then the y_i must be a permutation of the x_j and so this leads to $n!$ possible cases.

https://doi.org/10.1017/S0004972700044956 Published online by Cambridge University Press

LEMMA 10. *If* $h \in G$ *has order* 2^m *with* $m \geq 2$ *then* h *is in the centre of* G .

Proof. Let $g \in G$. Since $1 + (1+h)h$ is a unit, there exists $z \in G$ with $(1+h+h^2)g = z(1+h+h^2)$. This gives $ghg^{-1} = h^s$ where $s = \pm 1$. Thus $(1+h)g$ is nilpotent and so there exists $w \in G$ with

$$[1+(1+h)g]g = w[1+(1+h)g] .$$

If $gh \neq hg$ then $ghg^{-1} = h^{-1}$ and this leads to a contradiction.

LEMMA 11. *If any two elements of order* 2 *in* G *commute then* G *is abelian.*

Proof. Let $b \in G$ have order 2 . We show that b is in the centre of G . For let $g \in G$. If for $x \in G$, b^x denotes xbx^{-1} then, for all $t \geq 1$,

$$((1+b)g)^t = (1+b)\left(1+b^g\right) \ldots \left(1+b^{g^{t-1}}\right)g^t .$$

There exists an integer n such that $g^n = 1$ and so

$$((1+b)g)^{n+1} = (1+b)\left(1+b^g\right) \ldots \left(1+b^{g^{n-1}}\right)(1+b)g^{n+1} = 0 ,$$

since $b, b^g, \ldots, b^{g^{n-1}}$ all commute and $(1+b)^2 = 0$. Thus $\alpha = 1 + (1+b)g$ is a unit and there exists $h \in G$ with $\alpha g = h\alpha$. Consideration of the six cases gives $gb = bg$.

Suppose $x, y \in G$ and $xy \neq yx$. Then let $b \in G$ have order 2 . Since $\beta = 1 + (1+b)x$ is a unit, there exists $z \in G$ with $\beta y = z\beta$ and this yields $yx = bxy$. Now $y^{x^2} = y$ and $y^x \neq y$ so that $y^{x^n} = y$ if and only if n is even. Thus x has even order, say $2^s t$ where t is odd and $s \geq 1$. Then if $z = x^t$, z has order 2^s and $yz = b^t x^t y = bzy$. Now if $s \geq 2$ this contradicts Lemma 10 while if $s = 1$ this contradicts the paragraph above. Hence G is abelian.

LEMMA 12. *If* $x, y \in G$ *both have order* 2 *and if* $xy \neq yx$ *then*

https://doi.org/10.1017/S0004972700044956 Published online by Cambridge University Press

xy has order 3 .

Proof. Let $xy = b$ and let b have order m . Then $\langle b, x\rangle$ is a dihedral group of degree m and $m \geq 3$. Now $\big((1+x)b(1+x)\big)^2 = 0$ and so $\beta = 1 + (1+x)b(1+x)$ is a unit. Thus there exists $g \in G$ such that $\beta b = g\beta$. Since $g \in \langle b, x\rangle$ and g has the same order as b , it follows from a knowledge of the dihedral group that $g = b^j$ for some j . From $\beta b = b^j\beta$ we get $xb^2 + x = xb^{-1-j} + xb^{1-j}$. If $b^{1-j} = 1$ we get $b^4 = 1$, which contradicts Lemma 10, and so $b^{1-j} = b^2$. If we substitute this in $\beta b = b^j\beta$ we get $b^3 = 1$ and $m = 3$.

LEMMA 13. *Let $a \in G$ have order* 2 *and suppose there exists $b \in G$ of order* 2 *such that $ab \neq ba$. If $c \in G$ has order* 2 *then $ac \neq ca$.*

Proof. For suppose $ac = ca$; then $(a+c)^2 = 0$ and there exists $d \in G$ such that

$$(1+a+c)ab = d(1+a+c) ,$$

and this leads to a contradiction.

COROLLARY 14. *Let $a, b \in G$ both have order* 2 *with $ab \neq ba$. If $c, d \in G$ both have order* 2 *then $cd \neq dc$.*

Proof. By the lemma, $ac \neq ca$. Then from the lemma with a, b, c replaced by c, a, d respectively we get $cd \neq dc$.

LEMMA 15. *If G is not abelian then $|G|$ is not divisible by* 4 .

Proof. If 4 divides $|G|$ then G contains a subgroup of order 4 . This cannot be cyclic, by Lemma 10, so contains two commuting elements of order 2 . It then follows from Corollary 14 and Lemma 11 that G is abelian.

LEMMA 16. *Suppose G is not abelian. Then G contains two elements a, b of order* 2 *such that $ab \neq ba$. The only elements of order* 2 *in G are a, b , and aba and, if K is the subgroup generated by these elements of order* 2 , *then $K = \{1, a, b, aba, ab, ba\}$ and $K \simeq S_3$.*

Proof. The existence of a and b is given by Lemma 11. We know from Lemma 12 that ab has order 3 and hence aba has order 2 . Suppose that c is an element of order 2 which is distinct from a, b and aba , and let $d = ab$, $f = ac$ and let H be the subgroup generated by d and f ; we know that d and f have order 3 . Also $df = (aba)c$, $d^2f = bc$, $df^2 = a(bc)a$, $d^2f^2 = b(aca)$ all have order 3 . Thus, for all i, j ,

$$f^jd^if^j = d^{-1}f^{-j}d^{-i} . \tag{1}$$

It now follows as on page 321 of [7] that any element of H can be written as d^i, d^ifd^j, $d^if^{-1}d^j$ or $d^ifd^jf^{-1}d^k$. It can then be verified by using (1) that H has exponent 3 . Hence H is abelian, by Lemma 8, and $df = fd$. If $x = 1 + (1+d)(1+f+f^2)$ then $x^3 = 1$ and $bxb = x^2$, which gives $xbx^{-1} = bx$ and means that $x \in G$. Since f, df and df^2 are distinct, x must then equal one of them, and this yields $f = d$ or d^2 , which in turn yields $c = b$ or aba and is a contradiction.

It is routine to verify that K is as stated and is isomorphic to S_3 .

In what follows we assume G is nonabelian. Let N be the radical of $S = Z_2G$, let $\phi : S \to S/N = \bar{S}$ be the canonical map, let

$$\bar{S} = \bar{S}(e_1\phi) + \dots + \bar{S}(e_t\phi) ,$$

where the $e_i\phi$ are central primitive orthogonal idempotents in $\bar{S}$ and let

$$\bar{S}(e_i\phi) \simeq M_{n_i}\left(\mathrm{GF}\left(2^{k_i}\right)\right) .$$

LEMMA 17.

(i) At least one $n_i \geq 2$.

(ii) If $n_i \geq 2$ *then* $n_i = 2$, $k_i = 1$ *and*

$$(G\phi)(e_i\phi) = \left(\bar{S}(e_i\phi)\right)^* \simeq \mathrm{GL}(2, 2) .$$

Proof. *(i)* We know from Theorem 3 that $\phi : S^* \to \bar{S}^*$ is onto and has kernel $1 + N$. If $g \in G \cap (1+N)$ then $1+g \in N$ and so

https://doi.org/10.1017/S0004972700044956 Published online by Cambridge University Press

$(1+g)^{2^k} = 1 + g^{2^k} = 0$ for some k ; hence g has order 2 by Lemma 16. But $1+a \notin N$, since otherwise $(1+a)b = b+ab \in N$, and this is impossible because $(b+ab)^3 = (b+ab)^2 \neq 0$. Similarly $1+b \notin N$ and $1+aba \notin N$. Thus $G \cap (1+N) = \{1\}$ and $G\phi \simeq G$. Hence $\bar{S}$ is not commutative, so at least one $n_i \geq 2$.

(ii) Suppose $n_i \geq 2$. Now $(G\phi)(e_i\phi) \triangleleft (\bar{S}(e_i\phi))^*$ and, since $\bar{S}(e_i\phi)$ is spanned by $(G\phi)(e_i\phi)$ over Z_2 , $(G\phi)(e_i\phi)$ is not contained in the centre of $(\bar{S}(e_i\phi))^*$. If $n_i \geq 3$ or if $n_i = 2$ and $k_i > 1$ it follows from Theorem 4.9 of [1] that $(G\phi)(e_i\phi)$ contains a subgroup H with $H \simeq \mathrm{SL}\left(n_i, 2^{k_i}\right)$ but in this case $4 \mid \left|\mathrm{SL}\left(n_i, 2^{k_i}\right)\right|$ ([1], Theorem 4.11), and this contradicts Lemma 15. Thus $n_i = 2$ and $k_i = 1$. Since $S(e_i\phi)$ is spanned by $(G\phi)(e_i\phi)$ over Z_2 and has dimension 4 , it follows that $(G\phi)(e_i\phi) = (\bar{S}(e_i\phi))^*$, since otherwise $|(G\phi)(e_i\phi)| \leq 3$.

LEMMA 18. *G is an internal direct product $G = K \otimes L$ for some abelian group L of odd order.*

Proof. Let $\psi_i : \bar{S} \to \bar{S}(e_i\phi)$ be given by $\bar{s}\psi_i = \bar{s}(e_i\phi)$, and let L_i be the kernel of $\phi\psi_i$.

Suppose $n_i = 2$. Since $G\phi\psi_i \simeq S_3$ and 4 does not divide $|G|$, $|L_i|$ must be odd. Hence $L_i \cap K = \{1\}$ or $\langle ab \rangle$.

Suppose that $L_i \cap K = \langle ab \rangle$ for all i such that $n_i = 2$. Then if $n_i = 2$,

$$b\phi\psi_i = (a\cdot ab)\phi\psi_i = (a\cdot 1)\phi\psi_i = (1\cdot a)\phi\psi_i = (aba)\phi\psi_i .$$

Also, if $n_j = 1$, then, since $S\phi\psi_j$ is commutative,

$$b\phi\psi_j = (a\cdot ab)\phi\psi_j = (aba)\phi\psi_j .$$

Thus $b\phi\psi_i = aba\phi\psi_i$ for all i , which means that $b\phi = aba\phi$ and contradicts the fact that ϕ is one-to-one on G (see the proof of *(i)*, Lemma 17).

Thus for some i, $n_i = 2$ and $L_i \cap K = \{1\}$. Since L_i and K are both normal in G, and since

$$|G| = |L_i|\,|(\bar{S}(e_i\phi))^*| = |L_i|\,|K| ,$$

we must have $G = K \otimes L_i$. Further, it follows from Lemma 8 that L_i is abelian.

LEMMA 19. $G = K$.

Proof. Since L is abelian and of odd order, Z_2L is isomorphic to a direct sum of fields $F_1 \oplus \ldots \oplus F_t$. Then

$$Z_2G = (Z_2L)K \simeq \left(\bigoplus_{i=1}^{t} F_i\right)(K) \simeq \bigoplus_{i=1}^{t} \left(F_iS_3\right) = M ,$$

say. Now if N_i the radical of F_iS_3, then, as in Lemma 7, $F_iS_3/N_i \simeq F_i \oplus M_2(F_i)$. Thus if J is the radical of M, then

$$M/J \simeq \bigoplus_{i=1}^{t} \left(F_i \oplus M_2(F_i)\right) .$$

It now follows from Lemma 17 that $F_i \simeq Z_2$ for all i. But then Z_2L is isomorphic to t copies of Z_2 and $|L| = 1$.

5. Proof of Theorem 2

Suppose that every unit in Z_nG is trivial. It follows from Theorem 1 that either G is abelian or else $n = 2$ and $G \simeq S_3$. In the latter case, if γ is the sum of all the elements of G then $\gamma^2 = 0$ so $(1+\gamma)(1-\gamma) = 1$ and $1 + \gamma$ is a non-trivial unit. Thus G is abelian.

We next notice that if m divides n then every unit in Z_mG is trivial. For let $\theta : Z_nG \to Z_mG$ be the homomorphism extending the canonical homomorphism from Z_n to Z_m and the identity on G. Then if

https://doi.org/10.1017/S0004972700044956 Published online by Cambridge University Press

β is a unit in Z_mG, it follows from Theorem 3 that there is a unit α in Z_nG such that $\alpha\theta = \beta$. Since α is trivial, β must be also.

Let p be a prime dividing n. Notice that p^2 does not divide n, for otherwise, if γ is the sum of all the elements of G then $[(n/p)\gamma]^2 = 0$ and so $1 + (n/p)\gamma$ is a non-trivial unit.

Let H be a subgroup of G of order k; then Z_pH has only trivial units.

If p divides k and if γ is the sum of all the elements in H then $\gamma^p = 0$ in Z_pH so that $1 + \gamma$ is a unit. Because it is non-trivial if $k > 2$, we must have $p = k = 2$.

If $p \neq k$ and if k is a prime we know from Theorem 4.7 of [3] that

$$Z_pH \simeq Z_p \oplus \{[(k-1)/\mu] \text{ copies of } GF(p^\mu)\}$$

where μ is the order of p modulo k. Thus Z_pH has

$$(p-1)(p^\mu-1)^{[(k-1)/\mu]}$$

units. But Z_pH has only $(p-1)k$ trivial units. Since μ divides $k - 1$ by Fermat's Theorem and k divides $p^\mu - 1$, we must have $\mu = k - 1$ and $p^{k-1} = k$. This latter equation means that either $p = 2$ and $k = 3$, or $p = 3$ and $k = 2$.

Firstly consider what happens if $p = 3$; then G must be a 2-group. But, again using Theorem 4.7 of [3], $Z_3C_4 \simeq 2Z_3 \oplus GF(9)$ has 32 units and only 8 trivial units, while $Z_3(C_2 \times C_2) \simeq 4Z_3$ has 16 units and only 8 trivial units. Thus G must be of order 2. Also, in Z_6C_2, $(3+3x)^2 = 0$ so $1 + (3+3x)$ is a non-trivial unit; thus $n = 3$.

The only remaining possibility is that $n = 2$. But, again using Theorem 4.7 of [3], $Z_2C_9 \simeq Z_2 \oplus GF(4) \oplus GF(64)$ has 189 units and only 9 trivial ones while $Z_2(C_3 \times C_3) \simeq Z_2 \oplus 4GF(4)$ has 243 units but only

https://doi.org/10.1017/S0004972700044956 Published online by Cambridge University Press

9 trivial units. Thus G must be cyclic of order 2 or 3 .

Conversely, it is easily checked that if $n = 2$ and $|G| \leq 3$ or if $n = 3$ and $|G| = 2$ then $Z_n G$ has only trivial units.

References

[1] E. Artin, *Geometric algebra* (Interscience, New York, London, 1957).

[2] С.Д. Берман [S.D. Berman], "Об уравнении $x^m = 1$ в целочисленном групповом кольце" [On the equation $x^m = 1$ in an integral group ring], *Ukrain. Mat. Ž.* **7** (1955), 253-261.

[3] Charles Allen Cable, "On the decomposition of a group ring", (PhD dissertation, Pennsylvania State University, University Park, Pennsylvania, 1969).

[4] Klaus E. Eldridge, "On normal subgroups in modular group algebras", (unpublished).

[5] Klaus E. Eldridge and Irwin Fischer, "D.C.C. rings with a cyclic group of units", *Duke Math. J.* **34** (1967), 243-248.

[6] H.K. Farahat, "The multiplicative groups of a ring", *Math. Z.* **87** (1965), 378-384.

[7] Marshall Hall, Jr, *The theory of groups* (The Macmillan Company, New York, 1959).

[8] Graham Higman, "The units of group-rings", *Proc. London Math. Soc.* (2) **46** (1940), 231-248.

[9] J. Lambek, *Lectures on rings and modules* (Blaisdell, Waltham, Massachusetts; 1966).

Department of Mathematics,
La Trobe University,
Bundoora,
Victoria.