BULL. AUSTRAL. MATH. SOC. 16A26
VOL. 8 (1973), 435-442.

On the units of a modular group ring II

K.R. Pearson

Let R be a ring of nonzero characteristic and let G be a finite group with subgroup H. It is shown that H is a normal subgroup of the group of units of the group ring RG if and only if H is contained in the centre of G or R is the field with 2 elements, G is the symmetric group on 3 letters and H is normal in G.

Let R be a ring of nonzero characteristic and with identity 1, let G be a finite group with a subgroup H. We examine when $\{1h \mid h \in H\}$, which we again denote by H, is a normal subgroup of the group $(RG)^*$ of units of the group ring RG, and prove the following theorem. (Z_n denotes the ring of rational integers modulo n and S_3 and A_3 denote the symmetric and alternating groups on 3 letters.)

THEOREM. *Let R be a ring of nonzero characteristic and let G be a finite group with a subgroup H. Then H is a normal subgroup of the group of units of the group ring RG if and only if H is contained in the centre of G or $R \simeq Z_2$, $G \simeq S_3$ and $H \simeq S_3$ or A_3.*

This extends Theorem 1 of [4] in two directions. In the first place R was restricted there to Z_n; the present theorem now gives a complete characterization of those group rings RG with R of nonzero characteristic which satisfy the Condition III stated in [4]. Secondly, in [4] only the case $H = G$ was considered. Although Theorem 1 of [4] is a special

Received 30 January 1973.

https://doi.org/10.1017/S0004972700042726 Published online by Cambridge University Press

case of the present theorem, the proof given here makes essential use of it and does not subsume it.

The removal of the restriction $H = G$ was suggested by Eldridge [2] where it is 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 contained in the centre of G.

1. Outline of the proof

If H is contained in the centre of G then H is contained in the centre of RG and clearly $H \triangleleft (RG)^*$. Also it is shown in Lemma 7 of [4] that $S_3 \triangleleft (Z_2S_3)^*$, and it follows easily from this result that $A_3 \triangleleft (Z_2S_3)^*$. This takes care of the sufficiency part of the theorem.

We now consider the necessity part, and first show that it is sufficient to prove the theorem in the case where $R \simeq Z_p$ for some prime p. To do this let us assume the result when $R \simeq Z_p$ and consider an arbitrary ring R of nonzero characteristic n with $H \triangleleft (RG)^*$. If R_0 is the prime subring of R then $H \triangleleft (R_0G)^*$. Also if p is a prime dividing n the natural homomorphism from Z_n to Z_p extends to a homomorphism from Z_nG to Z_pG. Since Z_nG is finite, it follows from Theorem 3 of [4] that $H \triangleleft (Z_pG)^*$. Thus either H is contained in the centre of G or $p = 2$, $G \simeq S_3$ and $H \simeq S_3$ or A_3. This means that either H is contained in the centre of G, and we are finished, or $n = 2^k$ and we can take $A_3 \subseteq H \subseteq G = S_3$. The following lemma gives the required result.

LEMMA 1. *Let R be a ring of characteristic 2^k with $k \geq 1$. If $A_3 \subseteq H \subseteq G = S_3$ and $H \triangleleft (RG)^*$ then $R \simeq Z_2$.*

Proof. Let $S_3 = \langle a, b \mid a^2 = b^3 = 1, ba = ab^2 \rangle$. Suppose, if possible, that $k > 1$. Then if $x = 2^{k-1}$ we have $x^2 = 0 = 2x$ and so

$(1+xa)^2 = 1$. But

$$(1+xa)b(1+xa) = b + xab + xab^2 ,$$

which is not in H . Hence $k = 1$. If $\theta = (1+a)(b+b^2)$, then $\theta^2 = 0$. Thus if $y \in R$, $1 + y\theta$ is its own inverse. But

$$(1+y\theta)b(1+y\theta) = (1+y^2)b + y^2b^2 + (y^2+y)(ab+ab^2) ,$$

which is in H only if $y = 0$ or 1 . Therefore $R \simeq Z_2$ as required.

Accordingly in what follows we always assume that $H \triangleleft (Z_pG)^*$. We show that either H is contained in the centre of G or $p = 2$, $G \simeq S_3$ and $H \simeq S_3$ or A_3 . Because $(Z_pH)^*$ is a subgroup of $(Z_pG)^*$ we know that $H \triangleleft (Z_pH)^*$ and can apply Theorem 1 of [4] to see that either H is abelian or $p = 2$ and $H \simeq S_3$. When p does not divide $|G|$ the result is proved in §2. When p divides $|G|$ the result is proved in §3 and §4 for the cases $p \geq 3$ and $p = 2$ respectively.

One simple fact we use frequently is that H is normal in any subgroup of $(Z_pG)^*$. In particular H is normal in G and, if L is any subgroup of G containing H , $H \triangleleft (Z_pL)^*$.

2. The semisimple case

LEMMA 2. *If p does not divide $|G|$ then H is contained in the centre of G .*

Proof. Suppose, if possible, that H is not contained in the centre of G . Z_pG is semisimple and there must exist a central idempotent e in Z_pG such that He is not contained in the centre of $(Z_pG)e$ and $(Z_pG)e \simeq M_n(\mathrm{GF}(p^k))$ for some $n \geq 2$, $k \geq 1$. Let $\theta : [(Z_pG)e]^* \to \mathrm{GL}(n, p^k)$ be an isomorphism. Now $He \triangleleft [(Z_pG)e]^*$ and $p \nmid |He|$. But p divides $|\mathrm{SL}(n, p^k)|$ ([1], Theorem 4.11) and therefore $\mathrm{SL}(n, p^k)$ is not contained in $(He)\theta$. Nor can $(He)\theta$ be contained in

https://doi.org/10.1017/S0004972700042726 Published online by Cambridge University Press

the centre of $\mathrm{GL}(n, p^k)$, for otherwise $(He)\theta$ would be in the centre of $M_n(\mathrm{GF}(p^k))$, by [1], Theorem 4.8, and then He would be in the centre of $(Z_pG)e$. It follows from Theorem 4.9 of [1] that $n = 2$, $k = 1$ and $p = 2$ or 3 .

If $p = 2$ then $(He)\theta \subseteq \mathrm{GL}(2, 2) \simeq S_3$. Since $2 \nmid |Ge|$, Ge must be abelian and He is in the centre of Ge and therefore of $(Z_pG)e$, which is a contradiction.

Thus $p = 3$. But 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 of order 8 . But $H \lhd (Z_pH)^*$ and $p \nmid |H|$ so that H (and therefore He) must be abelian ([4], Theorem 1), and we again have a contradiction.

3. p divides $|G|$ and $p \geq 3$

Here H is abelian ([4], Theorem 1).

LEMMA 3. *If p divides $|G|$ and $p \geq 3$ then H is contained in the centre of G .*

Proof. Firstly if $k \in G$ has order a power of p we show that k is in the centralizer of H . For let $h \in H$. Since H is abelian we may assume that $k \notin H$. Because $(1+k)^{p^n} = 1 + k^{p^n}$ for all n , $1 + k$ is nilpotent and $1 + (1+k)$ is a unit. Thus there exists $h' \in H$ with $(2+k)h = h'(2+k)$. We can equate the terms in H to get $h' = h$ and then $kh = hk$ as required.

Now suppose that $p \nmid |H|$. If $g \in G$ we can write $g = g^sg^t$ where $g_1 = g^s$ has order a power of p and $g_2 = g^t$ has order relatively prime to p . Then $L = H\langle g_2\rangle$ is a subgroup of G and p does not divide its order. Since $H \lhd (Z_pL)^*$ it follows from Lemma 2 that g_2 centralizes H . Thus g centralizes H .

Accordingly we may assume that p divides $|H|$. In this case there exists $x \in H$ of order p. If $g \in G$, $h \in H$ and $n \geq 1$, then

$$[(1-x)g]^n = (1-x)\left(1-gxg^{-1}\right) \ldots \left(1-g^{n-1}xg^{1-n}\right)g^n .$$

Since $H \triangleleft G$ and H is abelian it follows that $(1-x)g$ is nilpotent. Thus there exists $h' \in H$ such that $[1+(1-x)g]h = h'[1+(1-x)g]$. Again we can assume that $g \notin H$. A comparison of the terms in H gives $h' = h$ and then, since $p \geq 3$, the other terms yield $gh = hg$.

4. $p = 2$ and $|G|$ even

Here either H is abelian or $H \simeq S_3$ ([4], Theorem 1).

LEMMA 4. *Suppose $p = 2$ and $|G|$ is even. If $x \in G$ has order 2^s with $s \geq 2$ then x is in the centralizer of H.*

Proof. If $x \in H$ then H must be abelian (as S_3 has no element of order 4) and so x centralizes H. Thus we can assume that $x \notin H$. Since $\left(x+x^{-1}\right)^{2^s} = 0$, $1 + x + x^{-1}$ is a unit. Then if $h \in H$ there exists $h' \in H$ with $\left(1+x+x^{-1}\right)h = h'\left(1+x+x^{-1}\right)$. If we compare the terms in H we have $h' = h$ and the other terms then give $h^{-1}xh = x^{\pm 1}$. But then h is in the normalizer of $\langle x \rangle$ and so $(1+x)h$ is nilpotent which means that there exists $h'' \in H$ with $[1+(1+x)h]h = h''[1+(1+x)h]$. If we compare the terms outside of H we get $h'' = xhx^{-1}$ and so $h + h^2 = xhx^{-1} + xhx^{-1}h$. Now either $h = h^2$ or $h = xhx^{-1}$ or $h = xhx^{-1}h$, and we get $xh = hx$ in each case.

LEMMA 5. *If $p = 2$, $|G|$ is even and $H \simeq S_3$, then $G = H$.*

Proof. We first show that if z centralizes H then $z = 1$. For then $H\langle z \rangle = H \times \langle z \rangle$ so that $Z_2(H\langle z \rangle)$ is isomorphic to the group ring of H over the ring $Z_2\langle z \rangle$. Then, by Lemma 1, $z = 1$.

Now let $g \in G$. We can write $g = g_1g_2$ where g_1 has odd order and g_2 has order 2^s $(s \geq 0)$. We let $H = \left\{a^ib^j \mid 0 \leq i \leq 1, 0 \leq j \leq 2\right\}$ with $a^2 = 1 = b^3$ and $ba = ab^2$. It

https://doi.org/10.1017/S0004972700042726 Published online by Cambridge University Press

is easy to see that $\langle b\rangle \triangleleft (Z_2G)^*$ and so $\langle b\rangle \triangleleft [Z_2(\langle b\rangle\langle g_1\rangle)]^*$ and it follows from Lemma 2 that $g_1b = bg_1$. Also $g_1ag_1^{-1} \in H$ and has order 2 so that $g_1ag_1^{-1} = ab^j$ for some j and then $\left(b^{-j}g_1\right)a = a\left(b^{-j}g_1\right)$. This means that $b^{-j}g_1$ centralizes H and hence $g_1 \in H$. If $s \geq 2$, g_2 centralizes H (Lemma 4) which is a contradiction. Accordingly we can assume that g_2 has order 2. If $x = g_2ag_2 = g_2ag_2^{-1}$ then x has order 2 and $g_2xg_2 = a$. If $x = a$, g_2 centralizes a. If $x \neq a$ and if w is the element of order 2 in H distinct from x and a then $g_2wg_2^{-1}$ must equal w and g_2 centralizes w. Since g_2 does not centralize H we must have $g_2b \neq bg_2$ and so $g_2b = b^2g_2$. Then if c is an element of order 2 in H which g_2 centralizes, $(1+c+g_2)^2 = 1$ yet

$$(1+c+g_2)b(1+c+g_2) = b + cb + cb^2 + g_2b + g_2b^2$$

which is not in H unless $g_2 \in H$. Thus $g \in H$ as required.

LEMMA 6. *If $p = 2$, $|G|$ is even and H is abelian, then either H is contained in the centre of G or $H \cong A_3$ and $G \cong S_3$.*

Proof. Suppose $g \in G\backslash H$ and $h \in H$. We can write $g = g_1g_2$ and $h = h_1h_2$ where g_1 and h_1 have odd order and g_2 and h_2 have order a power of 2. Because H is abelian, $(1+h_2)g$ is nilpotent and so there exists $h' \in H$ with

$$[1+(1+h_2)g]h_2 = h'[1+(1+h_2)g] .$$

A comparison of the terms in H yields $h' = h_2$ and gives $gh_2 + h_2gh_2 = h_2g + h_2^2g$, from which we get $h_2g = gh_2$. If K is the product of all the Sylow subgroups of H of odd order then K is a characteristic subgroup of H and so $K \triangleleft (Z_2G)^*$. Since $L = K\langle g_1\rangle$ has odd order and $K \triangleleft (Z_2L)^*$ it follows from Lemma 2 that g_1 and h_1 commute. Thus it follows from Lemma 4 that g and h commute unless g_2 has order 2 and $g_2h_1 \neq h_1g_2$.

Accordingly we examine what happens if there exist $x \in H$ of odd order and $z \in G\backslash H$ of order 2 with $xz \neq zx$. If $\gamma = (1+z)x(1+z)$ then $\gamma^2 = 0$ so that $\delta = 1 + \gamma$ is a unit of order 2, which means that $\delta x \delta$ is in H again. Because H is abelian and normal in G we have $zx^iz.x^j = x^j.zx^iz$ for all i and j. A calculation then yields

$$\delta x \delta = x + x^3 + zxzx^2 + zx^3z + xzx^2z + xzx^2 + zx^2 + zx^3 + x^2zx + x^2z + x^3z .$$

The terms not in H must cancel out and this gives $x^3 = 1$ and $xz = zx^2$. (Note that $x^2z = zx^2$ is impossible as x has odd order.)

We now assume that the centralizer of H is not the whole of G. It follows from the above that there exist $b \in H$ of order 3 and $a \in G\backslash H$ of order 2 with $ba = ab^2$.

We first show that $H = \langle b \rangle$. For suppose that $b_1 \in H\backslash\langle b \rangle$. If $ab_1 \neq b_1a$ then $ab_1 = b_1^2a$ and $b_1^3 = 1$. But then if $\theta = (1+a)b(1+a)$, $\theta^2 = 0$ and $(1+\theta)b_1(1+\theta)$ is again in H, which leads to a contradiction. Hence $ab_1 = b_1a$. Now if $\psi = (1+a)(b+b^2)$, $\psi^2 = 0$ and so $(1+b_1\psi)^2 = 1$. Thus there exists $h' \in H$ with $(1+b_1\psi)b = h'(1+b_1\psi)$. The terms not in H give $h' = b^{-1}$ and then the terms in $\langle b \rangle$ give a contradiction.

Suppose now that $g \in G$ is not in the centralizer of H. As before we can write $g = g_1g_2$ where g_1 has odd order and g_2 has order 2, and we have shown that $b_2g = b^2g_2$. Suppose if possible that $ag_2 \notin H$. If $\lambda = (1+a)bg_2(1+a)$ then $\lambda^2 = 0$, and so there exists $c \in H$ with $(1+\lambda)b = c(1+\lambda)$. If we compare the terms in H we get $c = b$ and then the other terms show that $g_2a = bag_2$. Since $g_2a = (ag_2)^{-1}$ is also not in H we can interchange g_2 and a and get $ag_2 = bg_2a$, which yields $b^2 = 1$ and is a contradiction. Thus $ag_2 \in H$ and $g_2 \in aH$. Now g_1 commutes with g_2 (each is a power of g), g_1 commutes with b and $a \in g_2\langle b\rangle$ so that g_1 commutes with a . Also $g_1a = g\left(g_2^{-1}a\right) \in gH \neq H$. Suppose if possible that $g_1 \notin H$. If $\eta = (1+a)\left(b+b^2\right)$ then $\eta g_1 = g_1\eta$ and $\left(g_1\eta\right)^2 = 0$, so there exists $d \in H$ with $\left(1+g_1\eta\right)b = d\left(1+g_1\eta\right)$. A comparison of the terms in H gives $d = b$ and then the other terms yield $b = 1$ which is a contradiction. Hence $g_1 \in H$ and $g \in g_2H = aH$. If H_1 denotes the centralizer of H we see that $aH_1 \subseteq aH$. Thus $H_1 = H$ and $G = H \cup aH$ as required.

References

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

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

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

[4] K.R. Pearson, "On the units of a modular group ring", *Bull. Austral. Math. Soc.* 7 (1972), 169-182.

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