Can. J. Math., Vol. XXXII, No. 6, 1980, pp. 1342–1352

FREE SUBGROUPS IN THE UNIT GROUPS OF INTEGRAL GROUP RINGS

B. HARTLEY AND P. F. PICKEL

1. Introduction. Let G be a group, $\mathbf{Z}G$ the group ring of G over the ring $\mathbf{Z}$ of integers, and $U(\mathbf{Z}G)$ the group of units of $\mathbf{Z}G$. One method of investigating $U(\mathbf{Z}G)$ is to choose some property of groups and try to determine the groups G such that $U(\mathbf{Z}G)$ enjoys that property. For example Sehgal and Zassenhaus [**9**] have given necessary and sufficient conditions for $U(\mathbf{Z}G)$ to be nilpotent (see also [**7**]), and the same authors have investigated when $U(\mathbf{Z}G)$ is an FC (finite-conjugate) group [**10**]. For a survey of related questions, see [**3**]. In this paper we consider when $U(\mathbf{Z}G)$ contains a free subgroup of rank 2. We conjecture that if this does not happen, then every finite subgroup of G is normal, from which various other conclusions then follow (see Lemma 4). As evidence, we prove:

THEOREM 1. *Let G be a soluble-by-finite group, and suppose that $U(\mathbf{Z}G)$ does not contain a free subgroup of rank* 2. *Then*

(i) *Every finite subgroup of G is normal in G.*

(ii) *The set of elements of finite order in G forms a subgroup T which is either abelian or the direct product of an elementary abelian* 2*-group and a quaternion group of order* 8.

In view of our ignorance about groups of units of group rings of torsion-free groups, a converse result cannot be expected at the present state of knowledge, without further hypotheses. In the finite case, however, a definitive result can be obtained, because of the well known fact that the units of $\mathbf{Z}G$ are trivial if G is a Hamiltonian 2-group [**5**].

THEOREM 2. *Let G be a finite group. Then exactly one of the following occurs:*

(i) *G is abelian (and so is $U(\mathbf{Z}G)$),*

(ii) *G is a Hamiltonian* 2*-group, and $U(\mathbf{Z}G) = \{\pm g : g \in G\}$,*

(iii) *$U(\mathbf{Z}G)$ contains a free subgroup of rank* 2.

Thus, for example, if G is finite then either $U(\mathbf{Z}G)$ has a derived group of order at most 2, and so is nilpotent of class at most 2, or $U(\mathbf{Z}G)$ contains a free subgroup of rank 2.

As a partial converse to Theorem 1 in the infinite case, we have

Received January 19, 1979.

https://doi.org/10.4153/CJM-1980-104-3 Published online by Cambridge University Press

THEOREM 3. *Let G be a group satisfying the conditions* (i) *and* (ii) *of Theorem* 1. *If G/T is right ordered, then $U(\mathbf{Z}G) = U(\mathbf{Z}T)G$. In particular, if G is furthermore soluble, so is $U(\mathbf{Z}G)$.*

The class of right ordered groups is quite large; for example it contains all infinite cyclic groups and is closed under extensions (and the more general operation corresponding to series of arbitrary order-type) and the operation "locally".

We are indebted to M. M. Parmenter for a number of useful conversations and for drawing our attention to the relevant literature.

Theorem 3 was proved for nilpotent groups by Sehgal and Zassenhaus [**9**], and our proof is based on theirs. We have learnt, since carrying out this work, that Theorem 2 and the soluble version of Theorem 1 are to be found in [**11**]. However our methods are somewhat different from those used there, and some of the intermediate results seem to have intrinsic interest.

2. The finite case. Although the finite case is a consequence of our general theorem, it turns out to be convenient to deal with it first.

The first lemma, which can obviously be applied to other suitable kinds of coefficient rings, is based on an idea of Berman [**1**].

LEMMA 1. *Let G be a finite group, e a central idempotent in $\mathbf{Q}G$. Then under the natural projection, $U(\mathbf{Z}G)$ maps onto a subgroup of finite index in $U(\mathbf{Z}Ge)$.*

Proof. We have $\mathbf{Q}G = \mathbf{Q}G(1-e) \oplus \mathbf{Q}Ge$. Choose an integer $t \geqq 1$ such that $te \in \mathbf{Z}G$. The ring $\mathbf{Z}Ge/t\cdot\mathbf{Z}Ge$ is finite, and so

$$H = \{\xi \in U(\mathbf{Z}Ge) : \xi \equiv e \bmod t\cdot\mathbf{Z}Ge\}$$

is a normal subgroup of finite index in $U(\mathbf{Z}Ge)$. Let $\xi \in H$ and consider the element

$$\beta = (1-e) + e\xi \in \mathbf{Q}G.$$

We have $\xi = e + te\gamma$ for some $\gamma \in \mathbf{Z}G$, whence $\beta = 1 + te\gamma \in \mathbf{Z}G$. Also, $\beta^{-1} = (1-e) + e\xi^{-1}$, and this belongs to $\mathbf{Z}G$ for the same reason. Hence $\beta \in U(\mathbf{Z}G)$, and so the image of $U(\mathbf{Z}G)$ in $\mathbf{Z}Ge$ contains H.

Proof of Theorem 2. If e is a centrally primitive idempotent in $\mathbf{Q}G$, then $\mathbf{Q}Ge \cong D_r$ for some division ring D and $r \geqq 1$. Suppose first that e can be chosen so that $r \geqq 2$, and let $\{e_{ij} : 1 \leqq i, j \leqq r\}$ be elements of $\mathbf{Q}Ge$ corresponding to the elementary matrices in D_r. There exists an integer $n \geqq 1$ such that $ne_{ij} \in \mathbf{Z}Ge$ for all i, j. Thus the image of $\mathbf{Z}Ge$ in D_r contains every $r \times r$ matrix over $\mathbf{Z}$ which is congruent to 1 mod n.

Hence $U(\mathbf{Z}Ge)$ contains a subgroup isomorphic to

$$\{x \in GL(r, \mathbf{Z}) : x \equiv 1 \bmod n\},$$

which is a subgroup of finite index in $GL(r, \mathbf{Z})$.

We now obtain from the lemma:

PROPOSITION 1. *Suppose* $\mathbf{Q}G$ *contains a centrally primitive idempotent* e *such that* $\mathbf{Q}Ge \cong D_r$, *where* D *is a division ring and* $r \geqq 2$. *Then there exist subgroups* $K \lhd H \leqq U(\mathbf{Z}G)$ *such that* H/K *is isomorphic to a subgroup of finite index in* $GL(r, \mathbf{Z})$. *In particular,* $U(\mathbf{Z}G)$ *contains a free subgroup of rank* 2.

If no idempotent exists as in Proposition 1, then every idempotent in QG is central, so if $H \leqq G$, then $|H|^{-1} \sum_{h \in H} h$ is central. It follows that $H \lhd G$. Therefore G is a Hamiltonian group, and so is either abelian, or has the form $G = A \times Q_8$, where A is an abelian group whose Sylow 2-subgroup is elementary [**8**]. It is well known that the units of $\mathbf{Z}G$ are trivial if A is a 2-group [**5**]. Therefore it remains to show that $U(\mathbf{Z}G)$ contains a free subgroup of rank 2 if A contains elements of odd order, and to do this, we may assume that $G = \langle a \rangle \times Q_8$, where a has odd prime order p. Proposition 1 actually handles certain values of p, but we give an argument which handles all values at once.

Let ζ be a primitive pth root of 1, and let H be the usual quaternion algebra over the rationals, with basis $1, i, j, k$, subject to the relations $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$. Then $\mathbf{Q}G$ contains a centrally primitive idempotent e such that

$$\mathbf{Q}Ge \cong \mathbf{Q}(\zeta) \otimes_Q H = \mathbf{Q}(\zeta) \oplus \mathbf{Q}(\zeta)i \oplus \mathbf{Q}(\zeta)j \oplus \mathbf{Q}(\zeta)k,$$

which may or may not be a division ring, depending on the value of p. Under this isomorphism, $\mathbf{Z}Ge$ corresponds to

$$R = \mathbf{Z}[\zeta] \oplus \mathbf{Z}[\zeta]i \oplus \mathbf{Z}[\zeta]j \oplus \mathbf{Z}[\zeta]k.$$

Now $1 + \zeta i$ is a unit in R. For $(1 + \zeta i)(1 - \zeta i) = 1 + \zeta^2$, and by putting $X = 1$ in the identity

$$X^p + 1 = \prod_{t=0}^{p-1} (X + \zeta^t) = (X + 1) \prod_{t=1}^{p-1} (X + \zeta^t)$$

we see that $1 + \zeta^2$ is a unit in $\mathbf{Z}[\zeta]$. For similar reasons, $1 + \zeta j$ is a unit in R. We shall show that there exists an integer $n > 0$ such that $(1 + \zeta i)^n$ and $(1 + \zeta j)^n$ generate a free group of rank 2. By Lemma 1, we can choose n so that these are images of units of $\mathbf{Z}G$, and we obtain the theorem.

We prove the required integer n exists by using an approach due to Tits [**12**]. Let K be the subfield of $H \otimes \mathbf{Q}(\zeta)$ generated by ζ and i. Then $H = K \oplus Kj$, and the right regular representation determines an embedding of $\langle 1 + \zeta i, 1 + \zeta j \rangle$ into $GL(2, K)$. Under this embedding we have

$$1 + \zeta i \to \xi = \begin{pmatrix} 1 + \zeta i & 0 \\ 0 & 1 - \zeta i \end{pmatrix}$$

and

$$1 + \zeta j \to \eta = \begin{pmatrix} 1 & \zeta \\ -\zeta & 1 \end{pmatrix}.$$

The eigenvalues of ξ are $1 + \zeta i$ and $1 - \zeta i$, with corresponding eigenspaces spanned by $(1, 0)$ and $(0, 1)$. We have, if bars denote complex conjugates,

$$\begin{aligned} |1 + \zeta i|^2 &= (1 + \zeta i)(1 - \bar{\zeta} i) \\ &= 2 + \zeta i - \bar{\zeta} i \end{aligned}$$

while

$$|1 - \zeta i|^2 = 2 - \zeta i + \bar{\zeta} i.$$

Since $\zeta \neq \bar{\zeta}$, we have $|1 + \zeta i| \neq |1 - \zeta i|$.

Similarly we find that the eigenvalues of η are also $1 + \zeta i$ and $1 - \zeta i$, with eigenspaces spanned this time by $(i, 1)$ and $(1, i)$ respectively. We can now use Proposition 3.12 of [**12**] to conclude that ξ^n and η^n freely generate a free group, for some $n > 0$, and hence deduce the theorem.

Remark. Another argument to show that $U(\mathbf{Z}G)$ contains a free group of rank 2 in the case when $\mathbf{Q}G$ has a matrix ring direct summand (and in particular when G is not Hamiltonian) can be given as follows. Write $\mathbf{Q}G = A \oplus B$, where A and B are two-sided ideals and $B \cong D_r$ for some division ring D and $r > 1$. In B, choose elements α and β corresponding to matrices which have the entry 1 in the $(1, 2)$ and $(2, 1)$ position respectively, and zeros elsewhere. Choose an integer $n > 0$ such that $n\alpha, n\beta \in \mathbf{Z}G$. Then $1 + n\alpha$ and $1 + n\beta$ are units in $\mathbf{Z}G$ (since $\alpha^2 = \beta^2 = 0$) and generate a group isomorphic to $\left\langle \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} \right\rangle$. This is well known to be free of rank 2 [**2**].

3. The infinite case. Let G be a group and $\langle a \rangle$ a finite cyclic subgroup of G. Suppose that x is an element of G which does not normalize $\langle a \rangle$. If a has order n and

$$(1) \quad \alpha = (1 - a)x(1 + a + \ldots + a^{n-1}),$$

then clearly $\alpha^2 = 0$. If $\alpha = 0$ then we clearly must have $x = axa^j$ for some j, which is impossible since x does not normalize $\langle a \rangle$. Hence $u = 1 + \alpha$ is a non-trivial unit of $\mathbf{Z}G$, and it is this which we shall exploit. We are grateful to P. Menal and E. Bernal for drawing our attention to these units, which simplified some of our original proofs and allowed the proof of Theorem 1 to be completed.

We first deal with some very special configurations.

LEMMA 2. *Let $G = H\langle a\rangle$ be the semidirect product of a finite elementary abelian 2-group H operated on by an element a of odd prime order p. Suppose that a operates faithfully and irreducibly on H. Let $1 \neq h \in H$, and define*

$$\alpha = (1 - a)h(1 + a + \ldots + a^{p-1})$$

and $u = 1 + \alpha$. Then $\langle u, u^h\rangle$ is freely generated by u and u^h.

Proof. Write $H = \langle h\rangle \times H_1$ and let $\mathbf{Z}v$ be an infinite cyclic group, written additively, generated by v. We make $\mathbf{Z}v$ into an H-module by defining $vh = -v$, and $vh_1 = v(h_1 \in H_1)$, and by inducing this to G, we obtain a $\mathbf{Z}G$-module V which is $\mathbf{Z}$-free of rank p.

Identifying v with $v \otimes 1$, we find that V has $\mathbf{Z}$-basis $v, va, \ldots, va^{p-1}$, and each element of H acts on V by changing the signs of certain of these basis elements.

Let

$$\xi = 1 + a + \ldots + a^{p-1} \quad \text{and} \quad w = v\xi = \sum_{i=0}^{p-1} va^i.$$

Then

$$\left(\sum_{i=0}^{p-1} \lambda_i va^i\right)\xi = \left(\sum_{i=0}^{p-1} \lambda_i\right)w.$$

We define the coefficient sum of an element

$$\sum_{i=0}^{p-1} \lambda_i va^i \in V$$

to be

$$\sum_{i=0}^{p-1} \lambda_i,$$

and now show that the coefficient sum of $wh(a - 1)h$ cannot exceed -4. Let S be the set of integers i such that $0 \leqq i \leqq p - 1$ and $va^ih = -va^i$. Then S is a proper subset of $\{0, 1, \ldots, p - 1\}$, otherwise, since V is clearly a faithful G-module, it would follow that h is central in G, which is not the case. Let S' be obtained by shifting the set S one step to the left modulo p, so that $S' \leqq \{0, 1, \ldots, p - 1\}$, and let $h' = aha^{-1}$. Then $va^ih' = -va^i$ if and only if $i \in S'$. Since $hah = hh'a$, we find that

$$va^ihah = \pm va^{i+1},$$

the minus sign being taken if and only if i belongs to

$$(S \cup S')\backslash(S \cap S') = T.$$

Since S is a proper subset of $\{0, 1, \ldots, p - 1\}$, we have $S \neq S'$, so $|T| \geqq 2$. It follows that the coefficient sum of $whah$ is at most $p - 4$, and that of $wh(a - 1)h = whah - w$ is at most -4, as claimed. Hence

$$wh\alpha = wh(1 - a)h\xi = \lambda w,$$

where λ is an integer and $\lambda \leqq -4$. Writing $y = wh$, we see that since $w\alpha = 0$, the element $u = 1 + \alpha$ leaves $\mathbf{Z}y \oplus \mathbf{Z}w$ invariant and operates on it via the matrix $\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$. Clearly $w\alpha^h = \lambda y$ and $y\alpha^h = 0$, so that u^h also leaves $\mathbf{Z}y \oplus \mathbf{Z}w$ invariant and operates on it via the matrix $\begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix}$. Since $|\lambda| \geqq 2$, these matrices generate freely a free group of rank 2 [**2**], and hence so do u and u^h.

LEMMA 3. *Let $G = \langle h \rangle \langle a \rangle$ be a dihedral group of order 8, where h has order 4 and a has order 2. Let*

$$\alpha = (1 - a)h(1 + a)$$

and $u = 1 + \alpha$. Then $\langle u, u^h \rangle$ is freely generated by u and u^h.

Proof. The map

$$h \rightarrow \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad a \rightarrow \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

determines a homomorphism of G into $GL(2, \mathbf{Z})$. Direct calculation reveals that

$$u \rightarrow \begin{pmatrix} 1 & -4 \\ 0 & 1 \end{pmatrix} \quad u^h \rightarrow \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix}.$$

These matrices freely generate a free group of rank 2 (see [**2**]).

LEMMA 4. *Let G be a group containing a locally finite normal subgroup T, and suppose that $U(\mathbf{Z}G)$ does not contain a free subgroup of rank 2. Then every subgroup of T is normal in G, and T is either abelian or a direct product of an elementary abelian 2-group and a quaternion group of order 8.*

Proof. The second part of the assertion follows from Theorem 2, and tells us in particular that every subgroup of T is normal in T.

Let H be any finite subgroup of T, and suppose H is not normal in G. Let $x \in G \backslash N_G(H)$ and

$$e = \frac{1}{|H|} \sum_{h \in H} h \in \mathbf{Q}G.$$

Define

$$f = e(1 - e^x).$$

The support of ee^x is clearly HH^x, which is not contained in H, so $e \neq ee^x$

and $f \neq 0$. We have $f^2 = f$ as e is central in $\mathbf{Q}T$; also

$$ff^x = e(1 - e^x)e^x(1 - e^{x^2}) = 0 = f^x f.$$

Let

$$\begin{aligned} e_{12} &= fx, \\ e_{21} &= x^{-1}f, \\ e_{11} &= e_{12}e_{21} = f, \\ e_{22} &= e_{21}e_{12} = f^x. \end{aligned}$$

Then it can be verified by direct calculation that $e_{ij}e_{kl} = \delta_{jk}e_{il}$, where δ_{jk} is the Kronecker symbol, for $1 \leqq i, j, k, l \leqq 2$. Since no e_{ij} is zero, it follows that

$$R = \sum_{i,j=1}^{2} \mathbf{Q}e_{ij} \cong \mathbf{Q}_2,$$

the ring of 2×2 matrices over $\mathbf{Q}$. Let

$$\epsilon = e_{11} + e_{22}, \quad \text{and } S = \mathbf{Q}(1 - \epsilon) \oplus R.$$

Choose an integer $n > 0$ such that $1 + ne_{12}$ and $1 + ne_{21}$ belong to $\mathbf{Z}G$. These elements are clearly units of $\mathbf{Z}G$ belonging to S, and under the projection onto R, they map to elements corresponding to the matrices

$$\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix}.$$

Hence $\langle 1 + ne_{12}, 1 + ne_{21} \rangle$ is free of rank 2.

Proof of Theorem 1. We have to consider a soluble-by-finite group G such that $U(\mathbf{Z}G)$ contains no free subgroup of rank 2. We shall prove that the set of elements of finite order of G is a subgroup, and the further conclusions needed then follow from Lemma 4.

Let T be the largest periodic normal subgroup of G, and let H be a soluble normal subgroup of finite index of G. Let M/H' be the torsion subgroup of H/H'. Since each finite set of elements of M lies in some finite extension of H', induction on the derived length of H allows us to assume that the set of elements of finite order of M is a subgroup. The same then holds for H, whence if $L = HT$, then L/T is torsion-free. Also, of course, $|G : L| < \infty$.

We now show that if a is an element of finite order in G, then

(1) $[L, a] \leqq T$.

Suppose this is not the case. Then we can choose a of order a power of a prime p, such that $[L, a] \nleqq T$ but $[L, a^p] \leqq T$. Let $x \rightarrow \bar{x}$ denote the natural homomorphism of G onto $\bar{G} = G/T$. The soluble group $\bar{L} = L/T$ contains a characteristic subgroup $\bar{N}$ which is nilpotent of class at most

https://doi.org/10.4153/CJM-1980-104-3 Published online by Cambridge University Press

two and satisfies $C_{\bar{L}}(\bar{N}) \leqq \bar{N}$ [**4**]. If $[\bar{N}, \bar{a}] = 1$, then since $\bar{a} \in C_{\bar{G}}(\bar{N}) \lhd \bar{G}$, we obtain

$$[\bar{L}, \bar{a}] \leqq C_{\bar{L}}(\bar{N}) \leqq \bar{N}.$$

Thus $\bar{a}$ stabilizes the series $\bar{L} \geqq \bar{N} \geqq 1$, and since $\bar{L}$ is torsion-free and $\bar{a}$ has finite order, this gives that $[\bar{L}, \bar{a}] = 1$. By assumption, this is not so, and therefore $[\bar{N}, \bar{a}] \neq 1$. Let $\bar{R}$ be a finitely generated $\bar{a}$-invariant subgroup of $\bar{N}$ such that $[\bar{R}, \bar{a}] \neq 1$. Then as above, $\bar{a}$ cannot stabilize the series $\bar{R} \geqq Z(\bar{R}) \geqq 1$ (where $Z(\ )$ denotes the centre), and so must act non-trivially on one of $\bar{R}/Z(\bar{R})$ and $Z(\bar{R})$. In this way, we obtain a-invariant subgroups $T \leqq V_1 \leqq U_1$ such that U_1/V_1 is free abelian of finite rank and a operates non-trivially on U_1/V_1, while a^p centralizes it.

Suppose now that $p \neq 2$, and write $X = U_1/V_1$. If a operates trivially on X/X^2, then a operates trivially on $X^{2^n}/X^{2^{n+1}}$ for all $n \geqq 0$, and hence stabilizes a finite series in the 2-group X/X^{2^n}. Therefore

$$[X, a] \leqq \bigcap_{n=0}^{\infty} X^{2^n} = 1,$$

which is not the case. We deduce that $[X, a] \nleqq X^2$, and by applying Maschke's Theorem, that there exists an a-invariant subgroup Y with $X^2 \leqq Y \leqq X$, such that a operates irreducibly on Y/X^2 and

$$C_{\langle a \rangle}(Y/X^2) = \langle a^p \rangle.$$

Write $Y = U/V_1$, $X^2 = V/V_1$. Choose $t \in U \backslash V$, let p^k be the order of a, and define

$$\alpha = (1 - a)t(1 + a + \ldots + a^{p^k-1})$$

and

$$u = 1 + \alpha.$$

Then $\alpha^2 = 0$, so u is a unit of $\mathbf{Z}G$. We have

$$V\langle a^p \rangle \lhd U\langle a \rangle$$

and

$$U\langle a \rangle / V\langle a^p \rangle \cong K\langle a^* \rangle,$$

where $K \cong U/V$ and a^* denotes the coset containing a. Thus a^* is an element of order p operating faithfully and irreducibly by conjugation on the elementary abelian 2-group K. The natural homomorphism of $U\langle a \rangle$ onto $K\langle a^* \rangle$, when extended to the group rings, maps α to $p^{k-1}\beta$, where

$$\beta = (1 - a^*)t^*(1 + a^* + \ldots + a^{*p-1})$$

and t^* denotes the image of t. Hence u is mapped to $(1 + \beta)^{p^{k-1}}$, and

u^t is mapped to $(1 + \beta)^{t^* p^{k-1}}$. By Lemma 2, these elements freely generate a free group of rank 2, and hence so do u and u^t. This contradiction establishes (1) when $p \neq 2$.

In the case $p = 2$ we can choose U_1/V_1 to be infinite cyclic. We then argue similarly to the above, mapping $U_1\langle a \rangle$ onto a dihedral group of order 8 and using Lemma 3, to obtain (1) in this case also.

By (1), we now have

$$|G/T : C_{G/T}(aT)| < \infty .$$

Hence, by Dietzmann's Lemma [**6**], aT lies in a finite normal subgroup of G/T. This clearly gives $a \in T$, and concludes the proof.

It remains to prove Theorem 3.

Proof of Theorem 3. Here G is a group in which the set of torsion elements forms a subgroup T which is either abelian or a direct product of an elementary abelian 2-group and a quaternion group of order 8. Furthermore, every subgroup of T is normal in G. It follows that every idempotent of $\mathbf{Q}T$ is central in $\mathbf{Q}G$. This can be seen by noting that if F is a finite subgroup of T and N is a normal subgroup of F such that F/N has a faithful irreducible representation over $\mathbf{Q}$, then the centre of F/N must be cyclic and so F/N is either cyclic or quaternion of order 8. In either case F/N has, up to isomorphism, a unique irreducible representation over $\mathbf{Q}$. So distinct primitive (central) idempotents in $\mathbf{Q}F$ correspond to irreducible representations whose kernels are distinct and hence not conjugate in G. Therefore distinct primitive idempotents in $\mathbf{Q}F$ cannot be G-conjugate.

We now use an argument based on a method of Sehgal and Zassenhaus [**9**]. Let X be a transversal to T in G, containing 1, and order X in the same way as G/T. Then every element of $\mathbf{Z}G$ is uniquely of the form

$$(2) \quad \alpha = \alpha_1 x_1 + \ldots + \alpha_n x_n \quad (0 \neq \alpha_i \in \mathbf{Z}T, x_i \in X, x_1 < x_2 < \ldots < x_n)$$

with $n \geqq 0$, and we have to show that if α is a unit, then $n = 1$. Suppose then that (2) represents a unit with $n > 1$. Let

$$\alpha^{-1} = \beta = \beta_1 y_1 + \ldots + \beta_m y_m \quad (0 \neq \beta_j \in \mathbf{Z}T,\ y_j \in X,\ y_1 < y_2 < \ldots < y_m).$$

Let $z_1 < z_2 < \ldots < z_k$ be elements of X representing the cosets $Tx_i y_j$. Then for $1 \leqq i \leqq n$, $1 \leqq j \leqq m$, we have

$$x_i y_j = t_{ij} z_{f(i,j)}$$

where $t_{ij} \in T$ and $1 \leqq f(i, j) \leqq k$.

Let E be the finite subgroup of T generated by the elements t_{ij} and the supports of the elements α_i and β_j. By the first paragraph, we can write

$$\mathbf{Q}E = A_1 \oplus \ldots \oplus A_l$$

https://doi.org/10.4153/CJM-1980-104-3 Published online by Cambridge University Press

where each A_i is a division algebra and a two-sided ideal of $\mathbf{Q}E$; also these ideals are invariant under conjugation by elements of G.

For each $\gamma \in \mathbf{Q}E$, define the carrier $\sigma(\gamma)$ of γ to be the set of integers i with $1 \leqq i \leqq l$, such that $\gamma A_i \neq 0$. Then $\gamma\gamma' = 0$ if and only if $\sigma(\gamma) \cap \sigma(\gamma') = \emptyset$. Also, if $g \in G$ and $t \in E$, we have $\sigma(\gamma^g) = \sigma(\gamma) = \sigma(\gamma t)$.

Since $n > 1$ we have $k > 1$, and so either $z_1 < 1$ or $z_k > 1$. We consider only the first possibility in detail, the second being dealt with by a similar argument or by applying the antiautomorphism $x \rightarrow x^{-1}$. Choose e such that $z_e = 1$. We prove by induction that $\alpha_i\beta_j = 0$ if $f(i, j) < e$. We have $x_iy_j \equiv z_1 \bmod T$ for some i and j, and the right ordering property shows that the only possibility is $i = 1$. Hence j is also uniquely determined; say $j = j_1$. Since $\alpha\beta = 1$, we have

(3) $\quad 1 = \sum \alpha_i\beta_j^{x_i^{-1}}t_{ij}z_{f(i,j)}.$

Equating the coefficient of z_1 to zero gives

$$\alpha_1\beta_{j_1}^{x_1^{-1}}t_{1,j_1} = 0.$$

Hence, by the above remarks, the carriers of α_1 and β_{j_1} are disjoint, and

(4) $\quad \alpha_1\beta_{j_1} = 0.$

Now consider values of i and j with $f(i, j) = d < e$, and suppose the claim has been established for values of i and j with $f(i, j) < d$. Equating the coefficient of z_d to zero in (3) gives

(5) $\quad 0 = \sum_{i,j} \alpha_i\beta_j^{x_i^{-1}}t_{ij}$

where the sum runs over values of i and j satisfying $f(i, j) = d$. We show that $\alpha_i\beta_j = 0$ for these values by downward induction on i. If it is known for all i greater than some i_0, we may assume that the sum (5) is restricted to $i \leqq i_0$. Let j_0 be the uniquely determined value of j such that $f(i_0, j_0) = d$. By the right ordering property, we have $f(i, j_0) < d$ if $i < i_0$, and so $\alpha_i\beta_j = 0$ if $i < i_0$. Hence

$$\sigma(\alpha_i) \cap \sigma(\beta_{j_0}) = \emptyset,$$

and so

$$\sigma(\alpha_i\beta_j^{x_i^{-1}}t_{ij}) \cap \sigma(\alpha_{i_0}\beta_{j_0}^{x_{i_0}}t_{i_0,j_0}) = \emptyset,$$

if $i < i_0$. Therefore we can write (5) as

$$0 = \delta + \epsilon$$

where

$$\delta = \alpha_{i_0}\beta_{j_0}^{x_{i_0}^{-1}}t_{i_0,j_0},$$

ϵ is the sum of the remaining terms, and $\sigma(\delta) \cap \sigma(\epsilon) = \emptyset$. Therefore $\delta = \epsilon = 0$, and hence $\alpha_{i_0}\beta_{j_0} = 0$. This completes the inductive proof that $\alpha_i\beta_j = 0$ if $f(i, j) < e$.

Now consider the coefficient of $z_e = 1$. We have

(6) $$1 = \sum_{i,j} \alpha_i \beta_j^{x_i^{-1}} t_{ij}$$

where the sum runs over values of i and j with $f(i, j) = e$. We claim that $\sigma(\alpha_i \beta_j^{x_i^{-1}} t_{ij})$ is a proper subset of $\{1, 2, \ldots, l\}$, for each term occurring. If $i = 1$ occurs, this is because α_1 is a zero divisor, by (4). If $\alpha_i \beta_j^{x_i^{-1}} t_{ij}$ is a term occurring with $i > 1$, then the right ordering property gives $f(1, j) < e$, whence $\alpha_1 \beta_j = 0$ and β_j is a zero divisor. It follows, since the carrier of each term in (6) is a proper subset of $\{1, 2, \ldots, l\}$, that at least two non-zero terms occur. Choosing the largest value of i which occurs and arguing as in the previous paragraph, we find that we can write

$$1 = \delta + \epsilon$$

where δ is the summand corresponding to the largest value of i, ϵ the sum of the rest, $\sigma(\delta) \cap \sigma(\epsilon) = \emptyset$, and $\delta, \epsilon \neq 0$. Hence both δ and ϵ are idempotents different from 1 lying in $\mathbf{Z}T$. Since this is impossible, we have a contradiction. This establishes Theorem 3.

References

1. S. D. Berman, *On the equation $x^m = 1$ in an integral group ring*, Ukrain. Mat. Z. *7* (1955), 253–261 (Russian).
2. J. L. Brenner, *Quelques groupes libres de matrices*, C.R. Acad. Sci. Paris *241* (1955), 1689–1691.
3. R. K. Dennis, *The structure of the unit group of group rings*, Proc. Ring Theory Conference, University of Oklahoma (Marcel Dekker, New York, 1976).
4. B. Hartley, *Finite groups of automorphisms of locally soluble groups*, J. Algebra *57* (1979), 242–257.
5. Graham Higman, *The units of group rings*, Proc. London. Math. Soc. *46* (1940), 231–248.
6. A. G. Kuros, *Theory of groups*, Vol. II, trans. K. A. Hirsch (Chelsea, New York, 1956).
7. C. Polcino Milies, *Integral group rings with nilpotent unit groups*, to appear.
8. E. Schenkman, *Group theory* (van Nostrand, Princeton, 1965).
9. S. K. Sehgal and H. Zassenhaus, *Integral group rings with nilpotent unit groups*, Comm. Algebra *5* (1977), 101–111.
10. ——— *Group rings whose units form an FC-group*, Math. Z. *153* (1977), 29–35.
11. S. K. Sehgal, *Topics in group rings* (Marcel Dekker, New York, 1978).
12. J. Tits, *Free subgroups in linear groups*, J. Algebra *20* (1972), 250–270.

University of Manchester,
Manchester, England;
Polytechnic Institute of New York,
Farmingdale, New York