# EMBEDDING FREE PRODUCTS IN THE UNIT GROUP OF AN INTEGRAL GROUP RING

J. Z. GONÇALVES AND D. S. PASSMAN

ABSTRACT. Let $G$ be a finite group and let $p$ be a prime. We show that the unit group of the integral group ring $\mathbb{Z}[G]$ contains the free product $Z_p{*}Z$ if and only if $G$ has a noncentral element of order $p$. Moreover, when this occurs, then the $Z_p$-part of the free product can be taken to be a suitable noncentral subgroup of $G$ of order $p$.

## 1. INTRODUCTION

Let $\mathbb{Z}[G]$ be the integral group ring of the group $G$, and let $U(\mathbb{Z}[G])$ be its group of units. When $G$ is finite, Hartley and Pickel [3] showed that $U(\mathbb{Z}[G])$ contains the free product $Z{*}Z$ unless $G$ is abelian or a Hamiltonian 2-group. Furthermore, Marciniak and Sehgal [4] proved that if $\mathbb{Z}[G]$ contains a bicyclic unit $u$, then $\langle u, u^* \rangle \cong Z{*}Z$. Continuing in this spirit of finding concrete generators for free products in $U(\mathbb{Z}[G])$, we offer the following result.

**Theorem 1.1.** *Let $G$ be a finite group. Then $U(\mathbb{Z}[G])$ contains the free product $Z_p{*}Z$ for some prime $p$, if and only if $G$ has a noncentral element of order $p$. Moreover, when this occurs, there exists $u \in U(\mathbb{Z}[G])$ and a noncentral element $y$ of $G$ of order $p$ such that $\langle y, u \rangle = \langle y \rangle {*} \langle u \rangle \cong Z_p{*}Z$.*

There is also an extension of the above $p = 2$ result to the case of torsion groups. Specifically, we obtain

**Corollary 1.2.** *Let $G$ be a torsion group. Then $U(\mathbb{Z}[G])$ contains the free product $Z_2{*}Z$, if and only if $G$ has a noncentral element of order 2. Moreover, when this occurs, there exists $u \in U(\mathbb{Z}[G])$ and a noncentral element $y$ of $G$ of order 2 such that $\langle y, u \rangle = \langle y \rangle {*} \langle u \rangle \cong Z_2{*}Z$.*

The necessity parts of the above follow quite easily from known results. Indeed, we have

**Lemma 1.3.** *Let $G$ be an arbitrary group, let $p$ be a prime, and assume that all elements of $G$ of order $p$ are central. Then any unit $u$ of $\mathbb{Z}[G]$ with $u^p = 1$ satisfies $u = \pm g$ for some $g \in G$ with $g^p = 1$. Hence $u$ is central in $\mathbb{Z}[G]$.*

*Proof.* Write $u = \sum_{x \in G} a_x x$ with $a_x \in \mathbb{Z}$. Then, by [8, Lemma I.1.5], we have $1 = u^p = \sum_{x \in G} a_x^p \, x^p + v + pw$ for suitable $v \in [\, \mathbb{Z}[G], \mathbb{Z}[G] \,]$ and $w \in \mathbb{Z}[G]$. Thus, by considering the coefficient of the identity element, [8, Lemma I.1.5] implies that $1 \equiv \sum{}' a_x^p \mod p$, where the sum $\sum'$ is over all $x \in G$ with $x^p = 1$. In particular,

2000 *Mathematics Subject Classification.* 16S34, 16U60.

The first author research was supported in part by CNPq Grant 303.756/82-5 and Fapesp-Brazil, Proj. Tematico 00/07.291-0.

it follows that there exists $g \in G$ with $a_g \neq 0$ and $g^p = 1$. Note that either $g = 1$ or $g$ has order $p$, and hence $g$ is central by assumption. Thus $(ug^{-1})^p = 1$ and, since $ug^{-1}$ has a nonzero identity coefficient, we conclude from [8, Corollary II.1.3] that $ug^{-1} = \pm 1$ and hence that $u = \pm g$ is central. □

Of course, the possibility that $u = -g$ in the above situation can only occur when $p = 2$.

## 2. Group-theoretic considerations

Our proof of the sufficiency part of Theorem 1.1 proceeds by induction on $|G|$. If $G$ has a proper subgroup $H$ having a noncentral element of order $p$, then the result for $H$ obviously yields the result for $G$. Thus it is necessary to understand those groups $G$ having no such proper subgroup. Specifically, we say that $G$ is *$p$-critical* provided that:

(1) $G$ has a noncentral element of order $p$;
(2) for all proper subgroups $H$ of $G$, the elements of $H$ of order $p$ are central in $H$.

We begin by studying $p$-groups.

**Lemma 2.1.** *If $P$ is a finite $p$-critical $p$-group, then $P'$ is central of order $p$ and $P$ is the semidirect product $P = B \rtimes A$ of the abelian group $B$ by $A = \langle a \rangle$, a cyclic group of order $p$. Furthermore, either $B = \langle b \rangle$ is cyclic of order $p^{n+1} \geq p^2$ with $b^a = b^{1+p^n}$, or $B = \langle b \rangle \times \langle z \rangle$, with $z$ central of order $p$ and $b^a = bz$.*

*Proof.* Let $a$ be a noncentral element of order $p$ and choose $b \in P$ with $ab \neq ba$. Then $\langle a, b \rangle$ cannot be a proper subgroup of $P$, so $a$ and $b$ generate $P$. Since $P$ is not cyclic, $a$ is contained in a maximal subgroup $H$ of $P$, and we know that $H \lhd P$. Thus $H$ contains all conjugates of $a$, and by (2), these are all central in $H$. In particular, $C = \langle a^g \mid g \in P \rangle$ is a normal elementary abelian subgroup of $P$. If $z = b^a b^{-1} = a^{-1}bab^{-1} = a^{-1}a^{b^{-1}}$, then $z \in C$ and hence $z$ is a commutator of order $p$. We claim that $z$ is central in $P$. To see this, let $g \in P$ be arbitrary and let $L$ be a maximal subgroup of $P$ containing $g$. Then $L \lhd P$ and $P/L$ is cyclic of order $p$, so $z \in P' \subseteq L$. By (2), $z$ is central in $L$, and hence $z$ commutes with $g$. Thus $Z = \langle z \rangle$ is indeed central in $P$. Note that $aZ$ and $bZ$ commute in $P/Z$ so, since $P = \langle a, b \rangle$, we see that $P/Z$ is abelian. Hence $P' = Z$ is central of order $p$.

Set $A = \langle a \rangle$ and $B = \langle b, z \rangle$, so that $A$ is cyclic of order $p$ and $B$ is abelian. Furthermore, $B \lhd P$ since $B \supseteq P'$, and thus $P = BA$ since $P$ is generated by $a$ and $b$. Obviously, $A \not\subseteq B$, so $A \cap B = 1$ and $P = B \rtimes A$. If $B = \langle b \rangle$ is cyclic of order $p^{n+1}$, then $Z = \langle b^{p^n} \rangle$. Hence $p^{n+1} = |B| \geq p^2$, and by replacing $a$ by another generator of $A$, if necessary, we have $b^a = b^{1+p^n}$. On the other hand, if $B$ is not cyclic, then $B = \langle b \rangle \times \langle z \rangle$ since $z$ has order $p$, and $b^a = bz$ by definition of $z$. □

It is easy to see that the groups given above are $p$-critical. For this, note that $P = \langle a, b \rangle$ has two generators, so the Burnside Basis Theorem implies that the Frattini quotient $P/\Phi(P)$ is elementary abelian of order $p^2$. Furthermore, since $b^p$ and $z$ are central elements contained in $\Phi(P)$, we conclude that $\Phi(P) = \langle b^p, z \rangle$ is central in $P$. Finally, let $M$ be any maximal subgroup of $P$. Then $P > M \supseteq \Phi(P)$, $[P : M] = p$ and $[P : \Phi(P)] = p^2$. Thus $[M : \Phi(P)] = p$ and, since $\Phi(P)$ is central, we see that $M$ is abelian. In particular, all elements of $M$ of order $p$ are central in $M$. Next, we need

**Lemma 2.2.** *If $G$ is an arbitrary $p$-critical finite group, then either $G$ has a normal $p$-complement or $G = P \rtimes Q$, where $P$ is an elementary abelian $p$-group, $Q = \langle b \rangle$ is a cyclic $q$-group for some prime $q \neq p$, and $Q$ acts irreducibly on $P$ as a group of order $q$ (that is, $[Q : \mathbb{C}_Q(P)] = q$).*

*Proof.* Let $p$ be odd and assume that $G$ does not have a normal $p$-complement. By Frobenius' Theorem [1, Theorem 7.4.5], there exists a $p$-subgroup $D$ of $G$ such that $\mathbb{N}_G(D)/\mathbb{C}_G(D)$ is not a p-group. In particular, there exists a cyclic $q$-group $Q \subseteq \mathbb{N}_G(D)$, for some prime $q \neq p$, such that $Q/\mathbb{C}_Q(D)$ has order $q$. In other words, $Q$ acts like a group of order $q$ on $D$. Now $D$ is properly smaller than $G$, so $\Omega_1(D)$ is central in $D$. In particular, $E = \Omega_1(D)$ is an elementary abelian p-group and, since $p > 2$, [1, Theorem 5.3.10] implies that $Q$ acts nontrivially on $E$. By Maschke's Theorem, there exists a $Q$-stable subgroup $P$ of $E$ such that $Q$ acts irreducibly and nontrivially on $P$. Since $H = \langle P, Q \rangle = P \rtimes Q$ is a subgroup of $G$ having noncentral elements of order $p$, we conclude that $G = H = P \rtimes Q$, as required.

Now let $p = 2$ and suppose first that all elements of $G$ of order 2 commute with each other. If $W$ is the group they generate, then $W$ is a normal elementary abelian 2-subgroup of $G$. Since $W$ is not central in $G$, there exists a cyclic group $Q$ of minimal order such that $Q$ does not centralize $W$. By minimality, $Q$ has prime power order, say $q^n$, and its unique subgroup of index $q$ acts trivially on $W$. Note that $WQ$ is a subgroup of $G$ with noncentral elements of order 2, so condition (2) implies that $G = WQ$. If $Q$ is a 2-group, then $G$ is a 2-group and hence $G$ has a normal 2-complement. Otherwise, we can proceed as above and conclude that $G = P \rtimes Q$, where $Q$ acts irreducibly on $P = W$. Finally, suppose that there exist two elements $x, y \in G$ of order 2 which do not commute. Then (2) implies that $G = \langle x, y \rangle$ and, as is well known, $\langle x, y \rangle$ is a dihedral group. Since such groups have normal 2-complements, the result follows. □

We can now put these lemmas together to obtain

**Proposition 2.3.** *Let $G$ be a finite group and let $p$ be prime. If $G$ is $p$-critical, then $G$ has one of the following structures:*

*i. $G$ is the group $B \rtimes A$ of Lemma 2.1;*
*ii. $G$ is the group $P \rtimes Q$ of Lemma 2.2;*
*iii. $G = Q \rtimes P$, where $Q$ is a $q$-group for some prime $q \neq p$, $P$ is a cyclic group of order $p$, $P$ acts faithfully and irreducibly on the Frattini quotient $Q/\Phi(Q)$, and $P$ centralizes $\Phi(Q)$.*

*Proof.* If a Sylow $p$-subgroup of $G$ has a noncentral element of order $p$, then $G$ must be a $p$-group and we can apply Lemma 2.1. Thus we can assume that all elements of $G$ of order $p$ are central in any Sylow $p$-subgroup that contains them. By Lemma 2.2, we can assume that $G$ has a normal $p$-complement $N \neq 1$. Thus $G = N \rtimes P_0$, where $P_0$ is a Sylow $p$-subgroup of $G$. Let $P$ be a subgroup of $P_0$ of order $p$ that is not central in $G$. Since $P$ is central in $P_0$, it follows that $P$ does not centralize $N$. In particular, $N \rtimes P$ has a noncentral element of order $p$, so $G = N \rtimes P$ and $P_0 = P$.

Since $N$ is a $p'$-group, there is a full set $Q_1, \ldots, Q_k$ of Sylow subgroups of $N$ such that each is normalized by $P$. Then $N = \langle Q_1, \ldots, Q_k \rangle$ and, since $P$ does not centralize $N$, it follows that $P$ does not centralize some $Q_i$. By (2), we can assume that $G = Q \rtimes P$, where $Q$ is a $q$-group for some prime $q \neq p$. Furthermore,

$P$ must centralize $\Phi(Q)$, and by Burnside's Theorem [1, Theorem 5.1.4], $P$ acts nontrivially on the Frattini quotient $Q/\Phi(Q)$. Finally, Maschke's Theorem and (2) clearly imply that $P$ acts faithfully and irreducibly on $Q/\Phi(Q)$. □

## 3. Module-theoretic considerations

Let us restate Proposition 2.3 in the simplified form we require.

**Lemma 3.1.** *Let $G$ be a $p$-critical finite group and let $y \in G$ be a noncentral element of order $p$. Then $G$ has a homomorphic image $\overline{G}$ such that:*

*i. the image $\overline{y}$ of $y$ is a noncentral element of $\overline{G}$;*
*ii. $\overline{G} = \overline{A} \rtimes \overline{X}$, where $\overline{A}$ is abelian and $\overline{X}$ has prime order.*

*Proof.* If $G$ is a $p$-group, then we take $\overline{G} = G$. If $G$ is the group $P \rtimes Q$ of Lemma 2.2, then $\mathbb{C}_Q(P)$ is central in $G$ and we take $\overline{G} = G/\mathbb{C}_Q(P) = \overline{P} \rtimes \overline{Q}$, where $\overline{P} \cong P$ and $\overline{Q} = Q/\mathbb{C}_Q(P)$ has prime order $q$. Finally, if $G = Q \rtimes P$ is the group of Proposition 2.3(iii), then we take $\overline{G} = G/\Phi(Q) = \overline{Q} \rtimes \overline{P}$, where $\overline{P} \cong P$ has order $p$ and $\overline{Q} = Q/\Phi(Q)$ is elementary abelian. □

Next, we need a result on the irreducible representations of the rational group algebra $\mathbb{Q}[G]$ for those finite groups satisfying condition (ii) above.

**Lemma 3.2.** *Let $G = A \rtimes X$ be a finite group with $A$ abelian and with $X$ cyclic of prime order. If $\theta$ is an irreducible representation of $\mathbb{Q}[G]$, then $\theta(\mathbb{Q}[G])$ is a full matrix ring over a (commutative) field extension of $\mathbb{Q}$.*

*Proof.* Let $1 = \sum_i e_i$ be the decomposition of 1 as a sum of primitive idempotents of $\mathbb{Q}[A]$. Since $\theta(1) = 1$, we have $\theta(e_i) \neq 0$ for some $i$. Let $\theta(\mathbb{Q}[G]) = S$ and set $e = e_i$. Then, either $e$ is fixed by the action of $X$ on $\mathbb{Q}[A]$ or $e$ has $q = |X|$ conjugates. We consider the two cases separately.

Suppose first that $e$ is fixed under the action of $X$. Then $e$ is a central idempotent of $\mathbb{Q}[G]$, so $\theta(e) \neq 0$ implies that $\theta(e) = 1$. In particular, by restriction, we obtain a ring epimorphism $\theta\colon e\mathbb{Q}[G] \to S$. Note that $e\mathbb{Q}[G] = (e\mathbb{Q}[A])X = FX$ is a skew group ring with identity element $e$ and with $F = e\mathbb{Q}[A]$, a field extension of $\mathbb{Q}$. Here, the conjugation action of $X$ on $e\mathbb{Q}[A]$ gives rise to the field automorphisms of $F$. If $X$ acts trivially on $F$, then $FX$ is commutative, so $S = \theta(\mathbb{Q}[G]) = \theta(FX)$ is commutative and hence $S$ is the ring of $1 \times 1$ matrices over a field. We can therefore assume that $X$ acts nontrivially on $F$ and hence faithfully, since $X$ has prime order $q$. The usual shortest length argument (or see [6, Corollary 12.6]) implies that $FX$ is simple and hence that $S \cong FX$.

Let now $h = (e/q)\sum_{x \in X} x$ so that $h$ is an idempotent in $FX$. Furthermore, by [6, Lemma 26.10], $h(FX)h = hF^X \cong F^X$, where $F^X$ is the fixed field of $F$ under the action of $X$. Since $FX$ is a finite-dimensional simple algebra, we therefore conclude that $S \cong FX \cong \mathbf{M}_m(F^X)$, where the latter is the ring of $m \times m$ matrices over $F^X$ for some $m \geq 1$. By dimension considerations, it is easy to see that $m = q$.

Finally, suppose that $e$ has $q = |X|$ conjugates under the action of $X$, and say these conjugates are $e = e_1, e_2, \ldots, e_q$. In this case, $e' = \sum_{i=1}^{q} e_i$ is a central idempotent of $\mathbb{Q}[G]$. Since $ee' = e$ and $\theta(e) \neq 0$, it follows that $\theta(e') \neq 0$ and hence that $\theta(e') = 1$. Again, by restriction, we have a ring epimorphism $\theta\colon e'\mathbb{Q}[G] \to S$. Furthermore, by [5, Lemma 6.1.7], we have $e\mathbb{Q}[G]e = e\mathbb{Q}[A] \cong F$, a field extension of $\mathbb{Q}$, and $e'\mathbb{Q}[G] \cong \mathbf{M}_q(F)$. In particular, $e'\mathbb{Q}[G]$ is a simple ring with identity $e'$, so $S \cong e'\mathbb{Q}[G] \cong \mathbf{M}_q(F)$, as required. □

We can now offer the

*Proof of Theorem 1.1.* If all elements of $G$ of order $p$ are central, then Lemma 1.3 implies that all units of $\mathbb{Z}[G]$ of order $p$ are central in the integral group ring. In particular, $U(\mathbb{Z}[G])$ cannot contain the free product $Z_p{*}Z$.

Conversely, suppose that $G$ is a finite group having a noncentral element of order $p$. We show by induction on $|G|$ that $U(\mathbb{Z}[G])$ contains the free product $Z_p{*}Z$ with the $Z_p$-part being a subgroup of $G$. If $G$ has a proper subgroup $H$ having a noncentral element of order $p$, then the result is clear. Thus we may assume that $G$ has no such proper subgroup $H$ and therefore, by definition, $G$ is $p$-critical.

Now let $y \in G$ be any noncentral element of order $p$ and let $\overline{G}$ be the homomorphic image of $G$ given by Lemma 3.1. Since $\overline{y}$ is not central in $\overline{G}$ and since $\mathbb{Q}[\overline{G}]$ is semisimple, there exists an irreducible representation $\overline{\theta}$ of $\mathbb{Q}[\overline{G}]$ such that $\overline{\theta}(\overline{y})$ is not central in $S = \overline{\theta}(\mathbb{Q}[\overline{G}])$. Furthermore, by Lemmas 3.1(ii) and 3.2, we know that $S = \mathbf{M}_m(F)$ is a full matrix ring over some field $F \supseteq \mathbb{Q}$. Next, via the natural epimorphism $\mathbb{Q}[G] \to \mathbb{Q}[\overline{G}]$, $\overline{\theta}$ gives rise to an irreducible representation $\theta$ of $\mathbb{Q}[G]$. Indeed, $\theta(\mathbb{Q}[G]) = \overline{\theta}(\mathbb{Q}[\overline{G}]) = S = \mathbf{M}_m(F)$ and $\theta(y) = \overline{\theta}(\overline{y})$ is a noncentral element of $S$ of order $p$. In particular, the intersection of the cyclic group generated by $\theta(y)$ with the scalar matrices of $S$ is precisely the identity matrix.

By [7, Corollary 1.4] (or see [2]), there exists a transvection $1+\tau \in \mathrm{GL}_n(F)$ such that $\langle \theta(y), 1+\tau\rangle \cong \langle\theta(y)\rangle{*}\langle 1+\tau\rangle \cong Z_p{*}Z$. Furthermore, by definition, we have $\tau^2 = 0$ and hence, since $S = \theta(\mathbb{Q}[G])$ is a direct summand of $\mathbb{Q}[G]$, there exists an element $\alpha \in \mathbb{Q}[G]$ with $\alpha^2 = 0$ and $\theta(\alpha) = \tau$. Note that $v = 1+\alpha$ is a unit in $\mathbb{Q}[G]$ with inverse $1-\alpha$, and that $\theta(v) = 1+\tau$. Thus, since $\theta$ maps $\langle y, v\rangle$ onto $\langle\theta(y), 1+\tau\rangle \cong \langle\theta(y)\rangle{*}\langle 1+\tau\rangle \cong Z_p{*}Z$, it follows that $\langle y, v\rangle \cong \langle y\rangle{*}\langle v\rangle \cong Z_p{*}Z$. Now $\alpha \in \mathbb{Q}[G]$, so there exists a positive integer $n$ with $n\alpha \in \mathbb{Z}[G]$. Set $u = 1+n\alpha$ and observe that $v^n = (1+\alpha)^n = 1+n\alpha = u$ since $\alpha^2 = 0$. Furthermore, $u$ is a unit in $\mathbb{Z}[G]$ since $u^{-1} = 1-n\alpha \in \mathbb{Z}[G]$. Finally, since $\langle y, u\rangle = \langle y, v^n\rangle \subseteq \langle y, v\rangle \cong \langle y\rangle{*}\langle v\rangle$, it is clear that $\langle y, u\rangle \cong \langle y\rangle{*}\langle u\rangle \cong Z_p{*}Z$, as required. □

We close this paper with the

*Proof of Corollary 1.2.* As above, if all elements of $G$ of order 2 are central, then the same is true of $U(\mathbb{Z}[G])$, and hence this unit group cannot contain $Z_2{*}Z$. Conversely, suppose that $G$ has a noncentral element of order 2. We will show below that $G$ has a finite subgroup $H$ having a noncentral element of order 2. Since $U(\mathbb{Z}[H]) \subseteq U(\mathbb{Z}[G])$, the result will then follow from Theorem 1.1 applied to $H$.

We proceed as in the $p = 2$ part of the proof of Lemma 2.2. Thus, suppose first that all elements of $G$ of order 2 commute with each other. If $W$ is the group they generate, then $W$ is a normal elementary abelian 2-subgroup of $G$ and, in particular, $W$ is a locally finite group. Since $W$ is not central in $G$, there exists a cyclic subgroup $T$ such that $W$ is not central in $WT$. But $G$ is torsion, so $T$ is finite and hence $|WT : W| < \infty$. It follows that $WT$ is also locally finite and consequently it contains a finite subgroup $H$ having a noncentral element of order 2. On the other hand, if there exist two elements $x, y \in G$ of order 2 which do not commute, then the dihedral group $\langle x, y\rangle$ has noncentral elements of order 2. Since $G$ is torsion, this dihedral group must have finite order, and the result follows. □

## References

[1] D. Gorenstein, *Finite groups*, Harper & Row, New York, 1968.

[2] J. Z. Gonçalves and A. Mandel, *Free groups generated by transvections*, preprint.
[3] B. Hartley and P. F. Pickel, *Free subgroups in the unit groups of integral group rings*, Canad. J. Math. **32** (1980), 1342–1352.
[4] Z. S. Marciniak and S. K. Sehgal, *Constructing free subgroups of integral group ring units*, Proc. AMS **125** (1997), 1005–1009.
[5] D. S. Passman, *The algebraic structure of group rings*, Wiley-Interscience, New York, 1977.
[6] ———— *Infinite crossed products*, Academic Press, Boston, 1989.
[7] ———— *Free products in linear groups*, Proc. AMS, to appear.
[8] S. K. Sehgal, *Topics in group rings*, Marcel Dekker, New York, 1978.

Department of Mathematics, University of São Paulo, São Paulo 05389, Brazil
*E-mail address*: jzg@ime.usp.br

Department of Mathematics, University of Wisconsin, Madison, Wisconsin 53706
*E-mail address*: passman@math.wisc.edu