INVOLUTIONS AND FREE PAIRS OF BICYCLIC UNITS IN INTEGRAL GROUP RINGS

J. Z. GONÇALVES AND D. S. PASSMAN

ABSTRACT. If $^*: G \to G$ is an involution on the finite group G, then * extends to an involution on the integral group ring $\mathbb{Z}[G]$. In this paper, we consider whether bicyclic units $u \in \mathbb{Z}[G]$ exist with the property that the group $\langle u, u^* \rangle$, generated by u and u^*, is free on the two generators. If this occurs, we say that (u, u^*) is a free bicyclic pair. It turns out that the existence of u depends strongly upon the structure of G and on the nature of the involution. One positive result here is that if G is a nonabelian group with all Sylow subgroups abelian, then for any involution *, $\mathbb{Z}[G]$ contains a free bicyclic pair.

1. Free Pairs of Bicyclic Units

Let R be a commutative ring with 1 and let $R[G]$ denote the group ring of G over R. For the most part, we will be concerned with integral group rings where $R = \mathbb{Z}$, or with group algebras where R is a field. Furthermore, we will mainly be interested in finite groups G, although some of our results do hold more generally.

If B is a finite subgroup of G, we let $\widehat{B} \in R[G]$ denote the sum of the elements of B in $R[G]$. Since $(1-b)\widehat{B} = \widehat{B}(1-b) = 0$ for any $b \in B$, we see that group ring elements of the form $(1-b)a\widehat{B}$, with $a \in G$, have square 0. Hence $1+(1-b)a\widehat{B}$ is a unit in the ring $R[G]$ with inverse $1-(1-b)a\widehat{B}$. When $B = \langle b \rangle$ is cyclic, elements of the form $u = 1 + (1-b)a\widehat{B}$ are known as bicyclic units. It is easy to see that $1+(1-b)a\widehat{B} = 1$ if and only if $b^a = a^{-1}ba \in B$ and hence if and only if $a \in \mathfrak{N}_G(B)$, the normalizer of B. In particular, if G is a Dedekind group, namely a group with all subgroups normal, then $R[G]$ has no nontrivial bicyclic units.

Now suppose that $^*: G \to G$ is an involution, that is an antiautomorphism of order 2. Then * extends to an involution of $R[G]$. In particular, if u is a unit of $R[G]$, then so is u^*, and we are interested in the nature of the subgroup $\langle u, u^* \rangle$ of the unit group that is generated by these two elements. If $^*: G \to G$ is the inverse map and if $R[G] = \mathbb{Z}[G]$, then it was shown in [6] that, for every nontrivial bicyclic unit u, the group $\langle u, u^* \rangle$ is free of rank 2. Certainly, it is of interest to see whether this property remains true for other involutions, and that is the theme of [2], where groups G with $|G : \mathfrak{Z}(G)| = 4$ are considered. In this paper, we study a wider class of examples. For convenience, we say that (u, u^*) is a free bicyclic pair if u is a bicyclic unit with $\langle u, u^* \rangle$ a free group on the two generators.

Section 1 is devoted to general tools. Following [6], we consider algebras over the complex numbers $\mathbb{C}$ and study when units $1+\alpha$ and $1+\beta$ with $\alpha^2 = \beta^2 = 0$ generate a free group of rank 2, that is when $(1+\alpha, 1+\beta)$ is a free pair. In some sense,

Research supported in part by the grant CNPq 303.756/82-5 and by Fapesp-Brazil, Proj. Tematico 00/07.291-0.

Research supported in part by NSA grant 144-LQ65.

this generalizes Sanov's theorem on linear groups, and the result depends upon the absolute value of the roots of the minimal polynomial satisfied by $\alpha\beta$. This, in turn, gives rise to numerous consequences. For example, we show in Corollary 1.10 that if $a \in G$ satisfies $\langle a^*a\rangle \neq \langle aa^*\rangle$, then $(1+\mu, 1+\mu^*)$ is a free bicyclic pair, where $b = (aa^*)^{-1} \in G$, $B = \langle b\rangle$ and $\mu = (1-b)a\widehat{B} \in \mathbb{Z}[G]$.

Section 2 considers a number of interesting examples. We start with finite symmetric and alternating groups. Then we study extra-special p-groups and show that, for certain involutions, free bicyclic pairs never exist. We also consider certain Frobenius groups and then use these results to show in Theorem 2.8 that if G is a finite nonabelian group with involution *, and if all Sylow subgroups of G are abelian, then $\mathbb{Z}[G]$ contains a free bicyclic pair (u, u^*). Finally, Section 3 considers a question of a somewhat different nature. Namely, in a group algebra $K[G]$, can every bicyclic unit $1 + (1-b)a\widehat{B}$, with the $(1-b)$ factor on the left, be written as $1 + \widehat{C}d(1-c)$, with the factor $(1-c)$ on the right. For fields K of characteristic different from 2, we show in Corollary 3.6 that if this occurs, then G must be nilpotent and presumably of small nilpotence class.

In the remainder of this section, let * denote an involution defined on the finite group G and naturally extended to the integral group ring $\mathbb{Z}[G]$. The results below actually hold for infinite groups, provided that certain elements, usually b, are assumed to have finite order.

Lemma 1.1. *The map $^*\colon G \to G$ is an involution if and only if * is equal to σ followed by the inverse map, where $\sigma\colon G \to G$ is an automorphism of order 1 or 2.*

Proof. Suppose * is an involution on G and let $\sigma\colon G \to G$ be equal to * followed by the inverse map. Then σ is easily seen to be an automorphism of G and, since σ commutes with inverse, we see that $\sigma^2 = 1$. The converse is clear. □

The following is a somewhat more efficient version of the argument of [6]. It appeared recently in [1] in a somewhat expanded form.

Lemma 1.2. *Let R be an algebra over the complex numbers $\mathbb{C}$ and let $\alpha, \beta \in R$ satisfy $\alpha^2 = \beta^2 = 0$. If either*

i. $\alpha\beta$ is transcendental over $\mathbb{C}$, or
ii. $\alpha\beta$ is algebraic over $\mathbb{C}$ having at least one eigenvalue ε with $|\varepsilon| \geq 4$,

then $(1+\alpha, 1+\beta)$ is a free pair.

Proof. It clearly suffices to assume that R is the $\mathbb{C}$-algebra generated by α and β. Let us first study the relatively free $\mathbb{C}$-algebra S generated by elements x and y, subject to the relations $x^2 = y^2 = 0$. Certainly, S is the span of all monomials in x and y, and any nonzero monomial must have the x and y factors alternating. In particular, if we set $z = xy$, then any nonzero monomial is of the form z^n, $z^n x$, yz^n or $yz^n x$ for some nonnegative integer n. It follows that if Z denotes the $\mathbb{C}$-linear span of all z^n, then Z is a commutative subalgebra with $S = Z + Zx + yZ + yZx$.

Now let $\mathbb{C}[t]$ be the ordinary polynomial ring over $\mathbb{C}$ in the variable t. Then there exists a homomorphism $\vartheta\colon S \to \mathbf{M}_2(\mathbb{C}[t])$ given by

$$\vartheta(x) = \begin{bmatrix} 0 & 0 \\ t & 0 \end{bmatrix}, \quad \vartheta(y) = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad \text{and} \quad \vartheta(z) = \vartheta(x)\vartheta(y) = \begin{bmatrix} 0 & 0 \\ 0 & t \end{bmatrix},$$

Since $\mathbb{C}[t]$ is a polynomial ring, it follows that $Z = \mathbb{C}[z]$ is also a polynomial ring.

We next observe that any nonzero ideal I of S meets Z nontrivially. Indeed, suppose $0 \neq s = s_1(z) + s_2(z)x + ys_3(z) + ys_4(z)x \in I$. If $s_1(z) \neq 0$, then $zsz = s_1(z)z^2$ is a nonzero element of $I \cap Z$. If $s_1(z) = 0$, then $I \cap Z$ contains $zsy = s_2(z)z^2$ and $xsz = s_3(z)z^2$. So, if either $s_2(z)$ or $s_3(z)$ is nonzero, then again $I \cap Z \neq 0$. It remains to assume that $s_1(z) = s_2(z) = s_3(z) = 0$. Then $s = ys_4(z)x$ and $0 \neq s_4(z)z^2 = xsy \in I \cap Z$, as required.

Since ϑ is clearly one-to-one on Z, it follows from the above that ϑ is one-to-one on S. Thus S is isomorphic to a subring of $\mathbf{M}_2(\mathbb{C}[t])$ and consequently S satisfies all polynomial identities of 2×2 matrix rings. Indeed, since R is a homomorphic image of S, we see that R also satisfies these identities. We now consider the two parts of this lemma separately.

(i) If $\alpha\beta \in R$ is transcendental over $\mathbb{C}$, then the map $S \to R$ given by $x \mapsto \alpha$, $y \mapsto \beta$ and $z \mapsto \alpha\beta$ is clearly one-to-one on Z. Hence it is one-to-one on S, so $R \cong S$ and R is relatively free. It follows that the homomorphism $\varphi\colon R \to \mathbf{M}_2(\mathbb{C})$ given by

$$\varphi(\alpha) = \begin{bmatrix} 0 & 0 \\ 2 & 0 \end{bmatrix} \quad \text{and} \quad \varphi(\beta) = \begin{bmatrix} 0 & 2 \\ 0 & 0 \end{bmatrix}$$

is well defined. Since

$$\varphi(1+\alpha) = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix} \quad \text{and} \quad \varphi(1+\beta) = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix},$$

Sanov's Theorem (see for example [9, Proposition 1.2]) implies that $\varphi(1+\alpha)$ and $\varphi(1+\beta)$ generate a free group on the two generators. Thus certainly $(1+\alpha, 1+\beta)$ is a free pair.

(ii) Now assume that $\alpha\beta$ is algebraic over $\mathbb{C}$ and let $m(\zeta)$ be its minimal polynomial. By assumption, ε is a root of $m(\zeta)$ and $|\varepsilon| \geq 4$. Note that, under the epimorphism $S \to R$ given by $x \mapsto \alpha$, $y \mapsto \beta$ and $z \mapsto \alpha\beta$, we see that the image of Z is finite dimensional over $\mathbb{C}$. Thus since $S = Z + Zx + yZ + yZx$, it follows that R, the image of S, is also finite dimensional over $\mathbb{C}$. In particular, R is an Artinian ring and its radical J is nilpotent. Furthermore, R/J is a finite direct sum of full matrix rings over $\mathbb{C}$, and we let $f(\zeta)$ be the product of the finitely many characteristic polynomials of the image of $\alpha\beta$ in each such ring. Then $f(\alpha\beta) \in J$, so $f(\alpha\beta)^k = 0$ for some integer k, and therefore $m(\zeta) \mid f(\zeta)^k$. If follows that ε is a root of $f(\zeta)$ and hence of one of the characteristic polynomials.

We have therefore shown that there exists an epimorphism $\psi\colon R \to \mathbf{M}_n(\mathbb{C})$ such that ε is an eigenvalue of $\psi(\alpha\beta)$. Since $\alpha^2 = 0$ and $\varepsilon \neq 0$, it follows that $n \neq 1$. On the other hand, R satisfies all polynomial identities of 2×2 matrix rings over $\mathbb{C}$, so the same is true of its homomorphic image $\mathbf{M}_n(\mathbb{C})$. Hence $n \leq 2$ and we conclude that $n = 2$. Again, since $\alpha^2 = \beta^2 = 0$, $\psi(\alpha\beta)$ must have at least one eigenvalue equal to 0. Thus the eigenvalues of $\alpha\beta$ are 0 and ε and, by conjugating if necessary, we can assume that

$$\psi(\alpha\beta) = \begin{bmatrix} 0 & 0 \\ 0 & \varepsilon \end{bmatrix}.$$

Since $\psi(\alpha)^2 = \psi(\beta)^2 = 0$ and $\psi(\alpha)\psi(\alpha\beta) = \psi(\alpha\beta)\psi(\beta) = 0$, it follows easily that

$$\psi(\alpha) = \begin{bmatrix} 0 & 0 \\ a & 0 \end{bmatrix} \quad \text{and} \quad \psi(\beta) = \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix}$$

for some $a, b \in \mathbb{C}$ with $ab = \varepsilon$. Finally, conjugating by a suitable diagonal matrix allows us to assume that $a = 2$. Then $b = \varepsilon/2$, so $|b| = |\varepsilon|/2 \geq 2$. Sanov's theorem

now implies that $\psi(1+\alpha)$ and $\psi(1+\beta)$ generate a free group of rank 2, and hence the same is true of $1+\alpha$ and $1+\beta$. □

Recall that the group algebra trace $\mathrm{tr}\colon \mathbb{C}[G] \to \mathbb{C}$ is the $\mathbb{C}$-linear map that reads off the identity coefficient of each element of $\mathbb{C}[G]$. As is well known, it satisfies $\mathrm{tr}\,\alpha\beta = \mathrm{tr}\,\beta\alpha$ for all $\alpha, \beta \in \mathbb{C}[G]$. If G is finite, then the trace is related to the character of the regular representation. Even when G is infinite, the trace contains information on the eigenvalues of algebraic elements. Because of this, we have

Lemma 1.3. *Let $\alpha, \beta \in \mathbb{C}[G]$ satisfy $\alpha^2 = \beta^2 = 0$. If $|\,\mathrm{tr}\,\alpha\beta| \geq 4$, then $(1+\alpha, 1+\beta)$ is a free pair.*

Proof. If $\alpha\beta$ is transcendental over $\mathbb{C}$, which can happen only when G is infinite, the result follows immediately from Lemma 1.2(i). Now suppose that $\alpha\beta$ is algebraic and let $m(\zeta) \in \mathbb{C}[\zeta]$ be its minimal polynomial. If $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n \in \mathbb{C}$ are the distinct roots of $m(\zeta)$, then [8, Theorem 2.3.8] implies that there exist nonnegative rational numbers $r_1, r_2, \ldots, r_n$ such that

$$r_1 + r_2 + \cdots + r_n = 1 \quad \text{and} \quad r_1\varepsilon_1 + r_2\varepsilon_2 + \cdots + r_n\varepsilon_n = \mathrm{tr}\,\alpha\beta.$$

In other words, $\mathrm{tr}\,\alpha\beta$ is a suitable weighted average of the roots. In particular, if ε is a root of largest absolute value then

$$|\varepsilon| = \sum_i r_i|\varepsilon| \geq \sum_i r_i|\varepsilon_i| \geq \Big|\sum_i r_i\varepsilon_i\Big| = |\,\mathrm{tr}\,\alpha\beta| \geq 4,$$

by assumption, so Lemma 1.2(ii) yields the result. □

Next, we prove the following two results together. While we will not have need for Lemma 1.4 in this paper, it is certainly of interest since $(1+\mu)^2 = 1 + 2\mu$.

Lemma 1.4. *Let $a, b \in G$, set $B = \langle b\rangle$ and let $\mu = (1-b)a\widehat{B} \in \mathbb{Z}[G]$. Suppose $BB^* = B^*B$ so that $C = BB^*$ is a *-stable subgroup of G. Furthermore, suppose that $a^{-1}ba \notin C$. If either*

i. $a^*ba \in C$, or
ii. $a^*a \in C$,

then $(1+2\mu, 1+2\mu^*)$ is a free pair.

Proposition 1.5. *Let $a, b \in G$, set $B = \langle b\rangle$ and let $\mu = (1-b)a\widehat{B} \in \mathbb{Z}[G]$. Suppose $BB^* = B^*B$ so that $C = BB^*$ is a *-stable subgroup of G. Furthermore, suppose that $|B \cap B^*| \geq 2$ and that $a^{-1}ba \notin C$.*

i. If $a^*ba \in C$, then $(1+\mu, 1+\mu^*)$ is a free pair.
ii. If $a^*a \in C$, then $(1+\mu, 1+\mu^*)$ is a free pair unless both $a^{-1}b^*ba \notin C$ and $|B \cap B^*| = 2$ or 3. In the exceptional case, $(1+2\mu, 1+2\mu^*)$ is a free pair.

Proof of Lemma 1.4 and Proposition 1.5. Since $\mathbb{Z}[G] \subseteq \mathbb{C}[G]$, we can work in the latter algebra. In view of Lemma 1.3, $(1+\mu, 1+\mu^*)$ is a free pair if $|\,\mathrm{tr}\,\mu^*\mu| \geq 4$, and $(1+2\mu, 1+2\mu^*)$ is a free pair if $|\,\mathrm{tr}\,2\mu^*2\mu| \geq 4$ or equivalently if $|\,\mathrm{tr}\,\mu^*\mu| \geq 1$. We now compute the trace.

Note that $\mu^* = \widehat{B}^* a^*(1-b^*)$ and that $\widehat{B}^* = \widehat{B^*}$. Furthermore, since $C = BB^*$ is a subgroup of G, we have $\widehat{B}\widehat{B}^* = |B \cap B^*|\widehat{C}$. Thus

$$\begin{aligned}\operatorname{tr} \mu^*\mu &= \operatorname{tr} \widehat{B}^* a^*(1-b^*)\cdot(1-b)a\widehat{B} \\ &= \operatorname{tr} \widehat{B}\widehat{B}^* a^*(1-b^*)(1-b)a \\ &= |B \cap B^*| \cdot \operatorname{tr} \widehat{C}(a^*a + a^*b^*ba - a^*ba - a^*b^*a).\end{aligned}$$

Since C is a subgroup of G, we have $\operatorname{tr} \widehat{C}g = 1$ if $g \in C$ and $\operatorname{tr} \widehat{C}g = 0$ if $g \in G \setminus C$. We consider parts (i) and (ii) separately.

(i) Here we suppose $a^*ba = c \in C$ so that $a^* = ca^{-1}b^{-1}$. Then $a^*b^*a = (a^*ba)^* \in C^* = C$, so $\operatorname{tr} \widehat{C}a^*ba = \operatorname{tr} \widehat{C}a^*b^*a = 1$. Furthermore, since $a^{-1}ba \notin C$, we have $a^*a = c(a^{-1}b^{-1}a) \notin C$. Also $a^*b^*a = c^* \in C$, so $a^*b^* = c^*a^{-1}$ and consequently $a^*b^*ba = c^*(a^{-1}ba) \notin C$. Thus $\operatorname{tr} \widehat{C}a^*a = \operatorname{tr} \widehat{C}a^*b^*ba = 0$ and $\operatorname{tr} \mu^*\mu = -2|B \cap B^*|$. In particular, $|\operatorname{tr} \mu^*\mu| \geq 2$, and $|B \cap B^*| \geq 2$ implies that $|\operatorname{tr} \mu^*\mu| \geq 4$, as required.

(ii) Now suppose that $a^*a = c \in C$ so that $a^* = ca^{-1}$. Since $a^{-1}ba \notin C$, we have $a^*ba = c(a^{-1}ba) \notin C$ and $a^*b^*a = (a^*ba)^* \notin C^* = C$. In other words, $\operatorname{tr} \widehat{C}a^*a = 1$, $\operatorname{tr} \widehat{C}a^*ba = \operatorname{tr} \widehat{C}a^*b^*a = 0$ and, of course, $\operatorname{tr} \widehat{C}a^*b^*ba = 0$ or 1. Thus $\operatorname{tr} \mu^*\mu = |B \cap B^*| \cdot m$, where $m = 1$ or 2. In particular, $|\operatorname{tr} \mu^*\mu| \geq 1$ and Lemma 1.4 is proved. Furthermore, for Proposition 1.5, we have $|\operatorname{tr} \mu^*\mu| \geq 4$ unless $m = 1$ and $|B \cap B^*| = 2$ or 3. Note that $m = 1$ implies that $c(a^{-1}b^*ba) = a^*b^*ba \notin C$, so $a^{-1}b^*ba \notin C$. In this exceptional case, we still have $|\operatorname{tr} \mu^*\mu| \geq 2$, so $(1+2\mu, 1+2\mu^*)$ is a free pair. □

With this, we can obtain the following key result.

Theorem 1.6. *Let $a, b \in G$, set $B = \langle b \rangle$ and let $\mu = (1-b)a\widehat{B} \in \mathbb{Z}[G]$. Suppose $B = B^*$ and that $a^{-1}ba \notin B$.*

i. If $a^*ba \in B$, then $(1+\mu, 1+\mu^*)$ is a free pair.
ii. If $a^*a \in B$, then $(1+\mu, 1+\mu^*)$ is a free pair unless $b^* = b$ and $|B| = 3$. In the exceptional case, $(1+2\mu, 1+2\mu^*)$ is a free pair.

Proof. Since $B = B^*$, we see that $C = BB^* = B^*B = B$ and that $a^{-1}ba \notin C$. Furthermore, $|B \cap B^*| = |B| \geq 2$ since $a^{-1}ba \notin B$. Parts (i) and (ii) now follow almost directly from Proposition 1.5(i) and (ii), respectively. Indeed, in the exceptional case of (ii), since $a^{-1}b^*ba \notin C$, we cannot have $b^* = b^{-1}$. Thus $B^* = B$ and $|B| = 2$ or 3 implies that $|B| = 3$ and $b^* = b$. □

As a first consequence, we have the main result of [6], namely

Corollary 1.7. *Let $^*\colon G \to G$ be the inverse map, let $a, b \in G$, set $B = \langle b \rangle$ and let $\mu = (1-b)a\widehat{B} \in \mathbb{Z}[G]$. If $a^{-1}ba \notin B$, then $(1+\mu, 1+\mu^*)$ is a free pair.*

Proof. Since * is the inverse map, we have $B^* = B$ and $a^*a = 1 \in B$. Furthermore, since $a^{-1}ba \notin B$, we have $|B \cap B^*| = |B| \geq 2$. The result now follows from part (ii) of the preceding theorem since if $|B| = 3$, then $b^* = b^{-1} \neq b$. □

Of course, this yields

Lemma 1.8. *Suppose * is σ followed by the inverse map, where σ is an automorphism of G. If $\mathfrak{C}_G(\sigma) = \{g \in G \mid g^\sigma = g\}$ is not a Dedekind group, then there exists a bicyclic unit $1+\mu \in \mathbb{Z}[G]$ such that $(1+\mu, 1+\mu^*)$ is a free pair.*

Proof. Since $H = \mathfrak{C}_G(\sigma)$ is not Dedekind, there exists $b \in H$ with $B = \langle b \rangle$ not normal in H. In particular, we can choose $a \in H$ with $a^{-1}ba \notin B$. Since * on H is the inverse map, Corollary 1.7 applied to H yields the result. □

Theorem 1.6 can also deal with inner automorphisms. Indeed, we have

Corollary 1.9. *Let $*$ be σ_b followed by the inverse map, where σ_b is the inner automorphism induced by $b \in G$. Set $B = \langle b \rangle$ and assume that $a \in G$ does not normalize B. If $\mu = (1-b)a\widehat{B} \in \mathbb{Z}[G]$, then $(1+\mu, 1+\mu^*)$ is a free pair.*

Proof. Certainly, $B = B^*$ and $|B| \geq 2$ since B is not normal. Furthermore, since σ_b has order 1 or 2, we know that $b^2 \in \mathfrak{Z}(G)$. Finally, $a^* = (a^{\sigma_b})^{-1} = b^{-1}a^{-1}b$, so $a^*ba = b^{-1}a^{-1}b^2a = b \in B$, using the fact that b^2 is central. The result now follows immediately from Theorem 1.6(i). □

Finally, we obtain a consequence of a somewhat different nature. It is surprisingly powerful.

Corollary 1.10. *Suppose $a \in G$ satisfies $\langle a^*a \rangle \neq \langle aa^* \rangle$ and set $b = (aa^*)^{-1}$. If $B = \langle b \rangle$ and $\mu = (1-b)a\widehat{B} \in \mathbb{Z}[G]$, then $(1+\mu, 1+\mu^*)$ is a free pair.*

Proof. Clearly $b^* = b$, so $B^* = B$. Furthermore, $a^{-1}b^{-1}a = a^{-1}(aa^*)a = a^*a \notin B$, so $a^{-1}ba \notin B$. Finally, $a^*ba = a^*(aa^*)^{-1}a = 1 \in B$, so Theorem 1.6(i) yields the result. □

As is to be expected, a lemma of the following sort can be used to construct free bicyclic pairs. Indeed, we have already used the obvious part (i), while part (ii) is just slightly less obvious.

Lemma 1.11. *Let G admit an involution * and assume that either*

i. G has a *-stable subgroup H such that $\mathbb{Z}[H]$ has a free bicyclic pair, or

ii. G has a *-stable normal subgroup N such that the group ring $\mathbb{Z}[G/N]$ contains a free bicyclic pair.

Then $\mathbb{Z}[G]$ has a free bicyclic pair (u, u^*).

Proof. We only consider (ii). For this, let $\theta\colon \mathbb{Z}[G] \to \mathbb{Z}[G/N]$ denote the natural epimorphism and let $v = 1 + (1-b)a\widehat{B} \in \mathbb{Z}[G/N]$ be given with $B = \langle b \rangle$ and with (v, v^*) a free pair. Choose $x, y \in G$ so that $\theta(x) = a$ and $\theta(y) = b$, and set $Y = \langle y \rangle$. Since $B \cong Y/(Y \cap N)$, it follows that $\theta(\widehat{Y}) = n\widehat{B}$ where $n = |Y \cap N|$. In particular, if $u = 1 + (1-y)x\widehat{Y}$, then $\theta(u) = 1 + n(1-b)a\widehat{B} = v^n$, and similarly $\theta(u^*) = (v^*)^n$. Since v and v^* generate a free group of rank 2, the same is true of v^n and $(v^*)^n$ and hence also of u and u^*. □

This motivates the following σ-generalization of a result of [7] on minimal nonabelian groups. We have opted to limit the group-theoretic work here by not offering a complete characterization below. For convenience, we say that G/N is a σ-stable homomorphic image of G if the automorphism σ stabilizes the normal subgroup N. In this case, σ determines an automorphism of G/N.

Lemma 1.12. *Let G be a finite nonabelian group that admits an automorphism σ of order 1 or 2, and suppose that every proper σ-stable subgroup or homomorphic image of G is abelian. Then we have either*

i. G is a p-group for some prime p, $|G'| = p$ and $|G : \mathfrak{Z}(G)| = p^2$, or

ii. G is the semidirect product $G = A \rtimes X$, where A is an elementary abelian q-group for some prime q, X is cyclic of prime order $p \neq q$, and $\mathfrak{Z}(G) = 1$.

Proof. Suppose $\sigma^2 = 1$ and assume that σ acts on an elementary abelian p-group V, viewed additively. If p is odd, then V is the direct sum of the eigenspaces $V = V_0 + V_1$, where $V_0 = \mathfrak{C}_V(\sigma)$ and $V_1 = \{v \in V \mid \sigma(v) = -v\}$. On the other hand, if $p = 2$, then σ has a Jordan decomposition consisting of blocks of size 1 or 2, and hence V is a direct sum of the corresponding σ-stable subgroups of order 2 or 4. In either case, it follows that V has a σ-stable subgroup of order p and a σ-stable homomorphic image of order p.

Now let the group G and σ be as given. If $\mathfrak{Z}(G) \neq 1$, then σ acts on $\Omega_1(\mathfrak{Z}(G))$, the set of elements of $\mathfrak{Z}(G)$ of order 1 or p, and hence there exists a σ-stable subgroup $Z \subseteq \mathfrak{Z}(G)$ of prime order p. By assumption, G/Z is abelian, and therefore G is nilpotent of class 2 with commutator subgroup $G' = Z$. Indeed, since all Sylow subgroups of G are characteristic, the minimal nature of G clearly implies that G is a p-group. Furthermore, σ acts on the Frattini quotient $G/\Phi(G)$, a nontrivial elementary abelian p-group, so we know that the latter has a σ-stable subgroup of index p. Thus G has a σ-stable subgroup H of index p and, by assumption, H is abelian. Finally, since $G = \langle H, g\rangle$ for some group element g and since $|G : \mathfrak{C}_G(g)| \leq |G'| = p$, we see that $H \cap \mathfrak{C}_G(g)$ has index at most p^2 in G. But $H \cap \mathfrak{C}_G(g)$ is clearly central in G, and consequently G has the structure described in (i).

We can now assume that $\mathfrak{Z}(G) = 1$ and hence that G is not nilpotent. We first show that G has a nonidentity normal abelian Sylow q-subgroup A. To start with, choose a nonidentity Sylow r-subgroup R having an odd number of conjugates. Indeed, if $|G|$ is even, we just take R to be a Sylow 2-subgroup, while if $|G|$ is odd, then we can choose any R since the index $|G : \mathfrak{N}_G(R)|$ divides $|G|$. Now σ permutes the conjugates of R and since $\sigma^2 = 1$, it follows that σ must stabilize at least one such conjugate. In particular, we can assume that σ stabilizes R. Of course, R is abelian since it is a proper subgroup of G and, if $R \lhd G$, we can take $A = R$. On the other hand, if R is not normal, then $\mathfrak{N}_G(R)$ is a proper σ-stable subgroup of G and hence $\mathfrak{N}_G(R)$ is abelian. In other words, R is in the center of its normalizer, so a result of Burnside (see [11, Theorem 6.2.9]) implies that G has a normal r-complement S. But $S \neq 1$ is a characteristic Hall subgroup of G, and S is abelian by the minimality of G. In this case, we can take A to be any nonidentity Sylow subgroup of S.

Obviously, A is characteristic and hence σ-stable. Thus G/A is abelian of order prime to q and, since $\mathfrak{Z}(G) = 1$, A cannot be central in the inverse images in G of all the Sylow subgroups of G/A. Since these inverse images are all characteristic in G, they are σ-stable, and the minimality of G implies that G must equal one of these. Thus $G = A \rtimes P$, where P is a nonidentity Sylow p-subgroup that acts nontrivially on A. Of course, $P \cong G/A$ is abelian and, since $\mathfrak{C}_P(A)$ is clearly central in G, we conclude that P acts faithfully on A. Thus G/A acts faithfully on A. Now σ acts on $\Omega_1(G/A)$, and hence it stabilizes a subgroup of G/A of order p. Since this subgroup corresponds to a nonabelian σ-stable subgroup of G, we conclude that $|G/A| = p$ and therefore that $P = X$ is cyclic of order p. Finally, since X acts faithfully on A, it acts faithfully on the Frattini quotient $A/\Phi(A)$ by [11, Theorem 7.3.12]. But then $G/\Phi(A)$ is nonabelian, so $\Phi(A) = 1$ by the minimality of G, and hence G has the structure described in (ii). □

Obviously much more can be said about the above groups. For example, if G is described as in (i), then Z must be the unique σ-stable subgroup of order p in $V = \Omega_1(\mathfrak{Z}(G))$. In particular, if p is odd, then V has order p and hence $\mathfrak{Z}(G)$ is cyclic. On the other hand, if $p = 2$, then σ can have at most one Jordan block in its action of V, and hence $\mathfrak{Z}(G)$ is either cyclic or the direct product of two cyclic subgroups. Of course, if $G = A \rtimes X$ is as in (ii) and if $|G|$ is odd, then A has no proper subgroup that is both X-stable and σ-stable.

2. Some Examples

In this section, we consider some examples of interest, and we start with the alternating and symmetric groups. Since the automorphisms of the latter groups are well understood, we have the following easy consequence of the preceding corollaries.

Example 2.1. *Let $G = \mathrm{Alt}_n$ or Sym_n and assume that G is nonabelian. If * is an involution of G extended to the integral group ring $\mathbb{Z}[G]$, then there exists a bicyclic unit $1 + \mu = 1 + (1 - b)a\widehat{B} \in \mathbb{Z}[G]$ with $(1 + \mu, 1 + \mu^*)$ a free pair.*

Proof. Since G is a nonabelian alternating or symmetric group, it is clearly not Dedekind. Now write * as in Lemma 1.1 as σ followed by the inverse map, where σ is an automorphism of order 1 or 2.

Suppose first that σ is the automorphism of G induced by conjugation by an element $g \in \mathrm{Sym}_n$ of order 1 or 2. Then g is a product of m disjoint transpositions, for some integer $m \geq 0$. If $m = 0$ apply Corollary 1.7 and if $m = 2$ apply Corollary 1.9 since $g \in \mathrm{Alt}_n \subseteq \mathrm{Sym}_n$. On the other hand, if $m \geq 3$, then $\mathfrak{C}_G(\sigma) = \mathfrak{C}_G(g)$ contains an isomorphic copy of $\mathrm{Sym}_m \supseteq \mathrm{Sym}_3$. Indeed, if $g = (r_1\, s_1)(r_2\, s_2) \cdots (r_m\, s_m)$, then we associate to each $\pi \in \mathrm{Sym}_m$ the even permutation $\psi(\pi) \in \mathfrak{C}_G(g)$ defined by $r_i \mapsto r_{\pi(i)}$, $s_i \mapsto s_{\pi(i)}$, and $t \mapsto t$ for all remaining points t. Hence $\mathfrak{C}_G(\sigma)$ is not Dedekind and Lemma 1.8 yields the result.

That leaves only $m = 1$ and if $G = \mathrm{Sym}_n$, then $g \in G$ and Corollary 1.9 applies. Thus $G = \mathrm{Alt}_n$ and, since G is nonabelian, we have $n \geq 4$. We can assume that g is the transposition $(1\,2)$ and let us set $a = (2\,3\,4) \in G$. Then $a^\sigma = a^g = (1\,3\,4)$, so $a^* = (4\,3\,1)$. We now see that $aa^* = (1\,4\,2)$ and $a^*a = (1\,2\,3)$ generate different cyclic subgroups, so Corollary 1.10 handles this case.

Finally, suppose σ is not conjugation by an element of order 1 or 2 in Sym_n. Then [11, Theorem 11.4.6] implies that $n = 6$ and, for convenience, let us write $A = \mathrm{Alt}_6$, $S = \mathrm{Sym}_6$, and $T = \mathrm{Aut}(S)$. It follows that $A \subseteq S \subseteq T$, with S embedded as inner automorphisms, and by [11, Theorem 11.4.8(3)], we have $|T : S| = 2$ and $T = \mathrm{Aut}(A)$. In particular, $T = \mathrm{Aut}(G)$.

By assumption, $\sigma \in T \setminus S$ and σ has order 2, so [5, Theorem 3.6] implies that there are precisely 36 possibilities for σ, forming one conjugacy class in T (see also the comments in [5] following Theorem 2.11). Furthermore, for any such σ, $\mathfrak{C}_S(\sigma)$ has order 20 and hence it must be the normalizer in S of a Sylow 5-subgroup. Since $G = S$ or A, it follows that $\mathfrak{C}_G(\sigma)$ contains the normalizer in A of a Sylow 5-subgroup, and such groups are isomorphic to the dihedral group of order 10. In particular, $\mathfrak{C}_G(\sigma)$ is not a Dedekind group, and Lemma 1.8 implies that $\mathbb{Z}[G]$ contains a free bicyclic pair (u, u^*). This completes the proof. □

A finite p-group P is said to be extra-special if $\mathfrak{Z}(P) = P'$ has order p. Here, of course, $Z = \mathfrak{Z}(P)$ is the center of P, and P' is the commutator subgroup. Such groups can be described as a finite direct product of nonabelian groups of order p^3

with their centers identified. Indeed, there are just two isomorphism classes of such groups for any fixed order p^{2n+1}. If p is odd, we can take all but one of the n direct factors to be nonabelian p-group of order p^3 and period p, while the last factor has either period p or p^2. When $p = 2$, we can take all but one of the n direct factors to be the dihedral group D_8 of order 8, while the last factor is either dihedral D_8 or quaternion Q_8.

It is easy to see that all such groups admit automorphisms σ of order 2 that invert P/Z, that is act like the inverse map on this abelian quotient group. In particular, such groups admit involutions * that act like the identity on P/Z. We now consider whether the integral group ring $\mathbb{Z}[P]$ has a bicyclic unit u with (u, u^*) being a free pair. As we will see, this can only occur when $p = 2$ and with some restrictions on P.

Example 2.2. *Let p be an odd prime and let P be an extra-special p-group with center Z. If * is an involution of P that is the identity on P/Z, then $\mathbb{Z}[P]$ has no free bicyclic pairs (u, u^*).*

Proof. Suppose $u = 1+\mu$ is a nonidentity bicyclic unit. Then $\mu = (1-b)a\widehat{B}$, where $B = \langle b\rangle$ and a does not normalize B. It follows that $|B| = p$ since every cyclic subgroup of P of order 1 or p^2 is normal. Thus $BZ \cong B \times Z$ is abelian of type (p, p), and we note that $C = BZ \triangleleft P$. Furthermore, since * acts trivially on P/Z, we see that $C^* = (BZ)^* = BZ = C$. Of course, $\mu^* = \widehat{B}^* a^*(1 - b^*)$, and there are two cases to consider according to whether $B = B^*$ or not.

Suppose first that $B \neq B^*$. Since $(BZ)^* = BZ$, we see that $B^* \subseteq BZ$ and hence $C = BZ = BB^* \cong B \times B^*$. In this case, we show that $\mu\mu^* = 0$. Indeed, since $\widehat{B}\widehat{B}^* = \widehat{B}\widehat{B^*} = \widehat{C}$ and $C \triangleleft P$, we have

$$\begin{aligned}\mu\mu^* &= (1 - b)a\widehat{B}\widehat{B}^* a^*(1 - b^*)\\ &= (1 - b)a\widehat{C}a^*(1 - b^*)\\ &= (1 - b)\widehat{C}aa^*(1 - b^*) = 0,\end{aligned}$$

using the fact that $\widehat{C}$ is central and $(1 - b)\widehat{C} = 0$. Now, for any integer i, we have $u^i = 1 + i\mu$ and $(u^*)^i = 1 + i\mu^*$, so $u^i(u^*)^i = (1 + i\mu)(1 + i\mu^*) = 1 + i(\mu + \mu^*)$. It follows, for any integers i, j, that $u^i(u^*)^i$ commutes with $u^j(u^*)^j$, and hence (u, u^*) is not a free pair.

Finally, suppose $B = B^*$. Since * acts trivially on P/Z and $B \cap Z = 1$, it follows that $b^* = b$ and that $a^* = at$ for some $t \in Z$. In this case, we claim that $\mu^*\mu = 0$ and, since the central element t factors out of this expression, we can assume that $t = 1$. Thus $\mu^* = \widehat{B}a(1 - b)$ and, since $b^a = a^{-1}ba = zb$ for some $z \in Z$, we have

$$\begin{aligned}\mu^*\mu &= \widehat{B}a(1 - b)(1 - b)a\widehat{B}\\ &= \widehat{B}a^2(1 - b)^a(1 - b)^a\widehat{B}\\ &= a^2\widehat{B}^{a^2}(1 - zb)(1 - zb)\widehat{B}.\end{aligned}$$

Now $b\widehat{B} = \widehat{B}$, so $(1 - zb)^2\widehat{B} = (1 - z)^2\widehat{B}$ and note that $(1 - z)$ is central. Also, since $p > 2$ and a does not normalize B, we see that a^2 does not normalize B. But $BZ \triangleleft P$, so $C = BZ = B^{a^2}B \cong B^{a^2} \times B$ and hence

$$\mu^*\mu = a^2\widehat{B}^{a^2}(1 - z)^2\widehat{B} = a^2(1 - z)^2\widehat{B^{a^2}}\,\widehat{B} = a^2(1 - z)^2\widehat{C} = 0,$$

using the fact that $z \in C$. As in the previous case, we can now show that $(u^*)^i u^i$ commutes with $(u^*)^j u^j$ for all integers i, j, and hence (u, u^*) is not a free pair. □

Now we turn to extra-special 2-groups P with the same sort of involution. Here, it is a simple matter, using Lemma 1.8, to show that if $|P| > 32$, then $\mathbb{Z}[P]$ has a bicyclic unit u with (u, u^*) a free pair. However, to handle the additional few groups of small order, we seem to require certain computations similar to those of the preceding example. Indeed, we start with

Lemma 2.3. *Let P be an extra-special 2-group with center Z and let * be an involution of P that is the identity on P/Z. Then $\mathbb{Z}[P]$ has a bicyclic unit u with (u, u^*) a free pair if and only if P has a noncentral element b of order 2 with $b = b^*$.*

Proof. We know that P has period 4 and that any cyclic subgroup of order 4 is normal. Thus nontrivial bicyclic units must be based on noncentral elements of order 2. Let $b \in P$ be such an element, set $B = \langle b \rangle$ and consider $\mu = (1-b)a\widehat{B} = (1-b)a(1+b)$ for some $a \notin \mathfrak{C}_P(b) = \mathfrak{N}_P(\langle b \rangle)$. Of course, $\mu^* = (1+b^*)a^*(1-b^*)$ and $Z = \{1, z\}$.

Suppose first that $b^* \neq b$. Then $b^* = bz$, so

$$\mu\mu^* = (1-b)a(1+b)(1+bz)a^*(1-bz).$$

Furthermore, since $(1+b)(1+bz) = \widehat{C}$, where C is the normal subgroup of order 4 generated by b and z, we have

$$\mu\mu^* = (1-b)a\widehat{C}a^*(1-bz) = (1-b)\widehat{C}aa^*(1-bz) = 0,$$

using the fact that $\widehat{C}$ is central and $b \in C$. As in the previous example, this implies that $(1+\mu, 1+\mu^*)$ is not a free pair.

On the other hand, suppose $b^* = b$. Then $a^* = at$ for some $t \in Z$ and $a^{-1}ba = bz$, so we have

$$\begin{aligned}\mu\mu^* &= (1-b)a(1+b)(1+b)a^*(1-b)\\ &= (1-b)a^2(1+b)^a(1+b)^a t(1-b) = (1-b)a^2(1+bz)^2 t(1-b).\end{aligned}$$

Furthermore, $(1+bz)^2 = 2(1+bz)$, $(1-b)^2 = 2(1-b)$ and a^2 is central, so

$$\operatorname{tr}\mu\mu^* = \operatorname{tr} 4a^2t(1-b)(1+bz) = \operatorname{tr} 4a^2t(1-b+bz-z).$$

Finally, $\operatorname{tr}\mu\mu^* = 4$ if $a^2t = 1$ and $\operatorname{tr}\mu\mu^* = -4$ if $a^2t = z$. Thus, in either case, Lemma 1.3 implies that $(1+\mu, 1+\mu^*)$ is a free pair. □

With this, we can quickly prove

Example 2.4. *Let P be an extra-special 2-group with center Z and let * be an involution of P that is the identity on P/Z. Then $\mathbb{Z}[P]$ has a bicyclic unit u with (u, u^*) a free pair unless $|P| = 8$ and * moves all noncentral elements of order 2.*

Proof. Write * equal to the automorphism σ followed by the inverse map. Since P/Z is elementary abelian, it follows that σ acts like the identity on this quotient. Furthermore, if we define $\lambda\colon P \to Z$ by $g^\sigma = g\lambda(g)$ for all $g \in P$, then it is easy to see that λ is a homomorphism. If C is the kernel of λ, then C has index at most $|Z| = 2$ in P, and $C = \mathfrak{C}_P(\sigma)$.

If C contains a noncentral element of P of order 2, then this element is fixed by the involution *, and hence it gives rise to a free pair (u, u^*) by the previous lemma. If this does not occur, then C has a unique element of order 2, so C is

cyclic or quaternion and hence $|C| \leq 8$ since P has period 4. Thus $|P| \leq 16$ and, since P is extra-special, we must have $|P| = 8$. In other words, $P \cong D_8$ or Q_8, and Lemma 2.3 yields the result. □

Of course, $\mathbb{Z}[Q_8]$ has no nontrivial bicyclic unit. Furthermore, if $P \cong D_8$, then the involution * moves all noncentral elements of order 2 if and only if * is conjugation by either element of order 4 followed by the inverse map. In particular, the latter involution is uniquely determined.

Next, we consider the groups that appear in Lemma 1.12(ii).

Example 2.5. *Let $G = A \rtimes X$ be a finite group, where A is a normal elementary abelian q-subgroup for some prime q and where $X = \langle x \rangle$ is cyclic of prime order $p \neq q$. Suppose $\mathfrak{Z}(G) = 1$ and that G admits an involution *. Then $\mathbb{Z}[G]$ has a free bicyclic pair (u, u^*) unless possibly when $|G|$ is odd, * is the inverse map on G/A, and there exists $1 \neq a \in A$ with $a^* = a$ and $\langle a \rangle \lhd G$.*

Proof. As usual, we write * as an automorphism σ followed by the inverse map. If σ is the identity, then free bicyclic pairs (u, u^*) exist by Corollary 1.7. Thus, we can assume that $\sigma \neq 1$. Since $\mathfrak{Z}(G) = 1$, it follows that X acts in a fixed-point-free manner on A and hence G is a Frobenius group. In particular, all elements of $G \setminus A$ have order p. Of course, A is characteristic in G, so σ acts on both A and G/A.

Suppose first that $p = 2$. Since there are an odd number of Sylow 2-subgroups of G, there exists a subgroup $X = \langle x \rangle$ of G of order 2 that is σ-stable. Clearly $x^\sigma = x$ and $x^* = x$. Furthermore, since x acts in a fixed-point-free manner on A, we must have $b^x = b^{-1}$ for all $b \in A$. Now σ acts nontrivially on G and $x^\sigma = x$, so σ must act nontrivially on A. Hence, since q is odd, there exists $1 \neq a \in A$ with $a^\sigma = a^{-1}$. Finally, the subgroup $H = \langle a \rangle \rtimes X$ is nonabelian and σ-stable, so it suffices to show that $\mathbb{Z}[H]$ contains a free bicyclic pair. But this is immediate from Corollary 1.9 since the action of σ on H is clearly equal to the inner automorphism of H induced by x.

We can now assume that $p > 2$ and, since σ acts on the cyclic group G/A of order p, there are two distinct possibilities. Namely, either σ is the identity on this quotient or it is the inverse map. We consider the latter case first, that is we assume σ is the inverse map and * is the identity on G/A. We first show that * cannot fix all elements of $G \setminus A$. Indeed, if this is the case, let $y \in G \setminus A$ and $a \in A$ be arbitrary. Then $y^* = y$ and $ay = (ay)^* = y^* a^* = ya^*$, so $y^{-1}ay = a^*$. Replacing y by $y^2 \notin A$, we also have $y^{-2}ay^2 = a^* = y^{-1}ay$, and thus y centralizes A, a contradiction. We can therefore choose $x \in G \setminus A$ with $x^* \neq x$ and hence $x^* = xc$ for some $1 \neq c \in A$. Note that $xx^* = x^2c$ and $x^*x = xcx$. In particular, if these two elements generate the same cyclic subgroup, then $(x^2c)^i = xcx$ for some exponent i. Viewing this equation modulo A, we see that $(x^2)^i \equiv x^2 \bmod A$, so $i \equiv 1 \bmod p$. But $x^2c \in G \setminus A$ has order p, so $xcx = (x^2c)^i = x^2c$ and consequently $cx = xc$. It follows that $c \in \mathfrak{Z}(G) = 1$, and this is a contradiction. Thus $\langle xx^* \rangle \neq \langle x^*x \rangle$ and Corollary 1.10 yields the result in this case.

It remains to assume that σ acts trivially on G/A so that * is the inverse map on this quotient, and here we consider the cases $q = 2$ and q odd separately. We suppose first that $q = 2$. Since $\sigma \neq 1$ and since G is generated by the elements of $G \setminus A$, there exists an element $x \in G \setminus A$ not fixed by σ. Thus $x^\sigma = xc$ for some $1 \neq c \in A$, and hence $x^* = (x^\sigma)^{-1} = c^{-1}x^{-1} = cx^{-1}$ since $c^2 = 1$. Now $x^*x = c$ and $xx^* = xcx^{-1}$ and these elements generate distinct cyclic groups since otherwise

$\langle c\rangle \triangleleft G$ and then $c \in \mathfrak{Z}(G)$ using the fact that $|\langle c\rangle| = q = 2$. Thus, again, the result follows from Corollary 1.10.

Finally, if q is odd, then G has an odd number of Sylow p-subgroups. Thus, we can assume that $X = \langle x\rangle$ is σ-stable and, since σ acts trivially on $G/A \cong X$, we have $x^\sigma = x$ and $x^* = x^{-1}$. Furthermore, since σ does not centralize G, it follows that σ does not centralize A, and hence we can choose $1 \neq a \in A$ with $a^\sigma = a^{-1}$. Thus $a^* = a$ and we let $r = xa \in G$. Note that $r^* = a^*x^* = ax^{-1}$, so $r^*r = a^2$ and $rr^* = xa^2x^{-1}$. If $\langle rr^*\rangle \neq \langle r^*r\rangle$, then Corollary 1.10 yields an appropriate free pair. On the other hand, if $\langle rr^*\rangle = \langle r^*r\rangle$, then $x\langle a^2\rangle x^{-1} = \langle rr^*\rangle = \langle r^*r\rangle = \langle a^2\rangle$, so $\langle a\rangle = \langle a^2\rangle \triangleleft G$. We have therefore shown that $\mathbb{Z}[G]$ has a free bicyclic pair unless possibly when $|G|$ is odd, * is the inverse map on G/A, and there exists $1 \neq a \in A$ with $a^* = a$ and $\langle a\rangle \triangleleft G$. □

It is easy to check, in the remaining case above, when A is cyclic and $*$ is the identity on A, that $|\operatorname{tr} \mu^*\mu| \leq 2$ for all bicyclic units $1 + \mu \in \mathbb{Z}[G]$. Thus, in order to handle this one special situation, we require an alternate approach to computing the eigenvalues of $\mu^*\mu$.

Part (i) below is a generalization of [3, Lemma 4.4] that allows A to be cyclic. As will be apparent, we do not need the full force of this result. Indeed, we only need part (ii) which follows fairly easily from the first paragraph of the proof of (i).

Lemma 2.6. *Let p and q be distinct odd primes, and let $\langle x\rangle$ be a cyclic group of order p acting faithfully and irreducibly on an elementary abelian q-group A. Choose $1 \neq a \in A$.*

i. If $p \geq 5$, then the $p-1$ nonidentity elements a^{1+x}, $a^{1+x^2}, \ldots, a^{1+x^{p-1}}$ cannot all be $\langle x\rangle$-conjugate.

ii. The element a^2 is not $\langle x\rangle$-conjugate to a^{1+x^j} for some $j = 1, 2, \ldots, p-1$.

Proof. (i) Note that $\mathfrak{C}_A(x) = 1$ and hence $1 + x + x^2 + \cdots + x^{p-1} = 0$ in its action on A. Note also that $a^{1+x^i} \neq 1$ since otherwise $a^{x^i} = a^{-1}$ and $\langle x\rangle = \langle x^{2i}\rangle$ centralizes a. Now suppose, by way of contradiction, that a^{1+x}, $a^{1+x^2}, \ldots, a^{1+x^{p-1}}$ are all $\langle x\rangle$-conjugate. Since $\mathfrak{C}_A(x) = 1$, it follows that these $p-1$ elements are all distinct and therefore if $b \in A$ is the pth element of this $\langle x\rangle$-conjugacy class, then $b\prod_{i=1}^{p-1} a^{1+x^i} \in \mathfrak{C}_A(x) = 1$. Thus, since $x + x^2 + \cdots + x^{p-1} = -1$, we conclude that $ba^{p-1}a^{-1} = 1$ and hence $b = a^{2-p}$. In particular, there exists a one-to-one function f from $\{1, 2, \ldots, p-1\}$ to itself such that

$$a^{(2-p)x^i} = b^{x^i} = a^{1+x^{f(i)}}$$

for all $1 \leq i \leq p-1$. Since $a^{\langle x\rangle} = A$, it follows that $(2-p)x^i = 1 + x^{f(i)}$ as operators on A.

Since $\langle x\rangle$ acts irreducibly on A, we can now view A as the additive group of $\mathrm{GF}(q^n)$. Furthermore, x can be taken to be an element of order p in this field acting by right multiplication on A, and x generates $\mathrm{GF}(q^n)$ over the prime subfield $\mathrm{GF}(q)$. The operator equations $(2-p)x^i = 1 + x^{f(i)}$ are now equations in the field.

For convenience, write $c = 2 - p \in \mathrm{GF}(q)$. Then $cx^i - 1 = x^{f(i)}$ has order p, so $x, x^2, \ldots, x^{p-1}$ are all roots of the polynomial equations $(c\zeta - 1)^p = 1$ and $\zeta^p = 1$ in $\mathrm{GF}(q)[\zeta]$. Hence they are all roots of $h(\zeta) = (c\zeta - 1)^p - 1 - c^p(\zeta^p - 1)$, a polynomial of degree at most $p-1$. It follows that $h(\zeta)$ must be a scalar multiple of $1 + \zeta + \zeta^2 + \cdots + \zeta^{p-1}$, and consequently all its coefficients are equal. Since

$p-1 \geq 4$, we can consider the degree 1, 2 and 3 coefficients and obtain

$$\binom{p}{1}c = -\binom{p}{2}c^2 = \binom{p}{3}c^3.$$

Note that $c \neq 0$ in $\mathrm{GF}(q)$ since $(cx-1)^p = 1$ and both p and q are odd.

Now $q \geq 3$ and $c \neq 0$, so the left-most equality in the displayed equation yields $p = -p(p-1)c/2$. In particular, since $p \neq 0$ in $\mathrm{GF}(q)$ and $c = 2-p$, we have $2 = (p-1)(-c) = (p-1)(p-2)$ and hence $p \equiv 3 \bmod q$ and $c \equiv -1 \bmod q$. It follows that $q \neq 3$, so $q \geq 5$ and the right-most equality in the displayed equation becomes $-3 = -p(p-1)/2 = -p(p-1)(p-2)/6 = -1$. In other words, $3 \equiv 1 \bmod q$ and we have the required contradiction.

(ii) If $p \geq 5$, then by the above, the elements a^{1+x^i} for $i = 1, 2, \ldots, p-1$ are in at least two distinct $\langle x \rangle$-conjugacy classes. Thus one of these elements is not in the class of a^2.

Finally, if $p = 3$, then $q \neq 3$ and $1 + x + x^2 = 0$ in its action on A. Thus $a^{1+x} = a^{-x^2}$ and $a^{1+x^2} = a^{-x}$. It follows that these two elements and a^{-1} form an $\langle x \rangle$-conjugacy class. If a^2 is in this class, then $a^2 = a^{-1}$ or $a^2 = a^{1+x}$ or $a^2 = a^{1+x^2}$, and none of these can occur since $a^3 \neq 1$ and since x does not centralize a. □

We briefly comment on the situation (i) above for the remaining small primes. If $p = 2$, then there is only one element of the form a^{1+x^i}, so the result is trivially false, and as we have seen, it is false for $p = 3$. Finally, if $q = 2$, $p = 2^n - 1$ is a Mersenne prime and $|A| = 2^n$, then all nonidentity elements of A are $\langle x \rangle$-conjugate, and in particular all a^{1+x^i} are $\langle x \rangle$-conjugate.

With this result in hand, we can now handle the missing case of Example 2.5. Specifically, we show

Example 2.7. *Let $G = A \rtimes X$ be a finite group of odd order, where A is a normal elementary abelian q-subgroup for some prime q and where $X = \langle x \rangle$ is cyclic of prime order $p \neq q$. If $\mathfrak{Z}(G) = 1$ and if G admits an involution * that is the identity on A, then $\mathbb{Z}[G]$ has a free bicyclic pair (u, u^*).*

Proof. As in Example 2.5, we write * as σ followed by the inverse map and, since $|G|$ is odd, we can assume that σ stabilizes X. Thus X is *-stable. Furthermore, since $p \neq q$ and $\mathfrak{Z}(G) = 1$, we see that X acts faithfully and completely reducibly on A. In particular, there exists a faithful irreducible submodule $A_1 \subseteq A$, and we set $G_1 = A_1 \rtimes X \subseteq G$. Obviously, G_1 is *-stable and $\mathfrak{Z}(G_1) = 1$, so we can replace G by G_1 and assume that X acts faithfully and irreducibly on A.

Now choose $1 \neq a \in A$ and, by part (ii) of the preceding lemma, we can can find a generator x of X so that a^2 is not $\langle x \rangle$-conjugate to a^{1+x}. In particular, a^2 and a^{1+x} are nonidentity elements belonging to different conjugacy classes of G. Now let $\mu = (1-x^{-1})a\widehat{X}$. Since $x\widehat{X} = \widehat{X}$, we have $x^{-1}a\widehat{X} = x^{-1}ax\widehat{X} = a^x\widehat{X}$ and hence $\mu = (a-a^x)\widehat{X}$. Furthermore, since * is the identity on A and since $X^* = X$, we have $\mu^* = \widehat{X}^*(a-a^x)^* = \widehat{X}(a-a^x)$ and $\mu^*\mu = \widehat{X}(a-a^x)^2\widehat{X}$.

Embed $\mathbb{Z}[G]$ in the complex group algebra $\mathbb{C}[G]$ and let $\mathfrak{X}$ be a nonlinear irreducible representation of $\mathbb{C}[G]$ with associated character χ. Then, by [3, Lemma 4.2], $\mathfrak{X}\colon \mathbb{C}[G] \to \mathbf{M}_p(\mathbb{C})$, and we can assume that $\mathfrak{X}(A)$ consists of diagonal matrices and

that $\mathfrak{X}(x)$ is the $p \times p$ permutation matrix

$$\mathfrak{X}(x) = \begin{bmatrix} & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \\ 1 & & & & \end{bmatrix}.$$

It follows that $\mathfrak{X}(\widehat{X}) = E$ is the $p \times p$ matrix having all entries equal to 1. Since E has rank 1, we see that

$$\mathfrak{X}(\mu^*\mu) = \mathfrak{X}(\widehat{X}) \cdot \mathfrak{X}(a - a^x)^2 \cdot \mathfrak{X}(\widehat{X}) = E \cdot \mathfrak{X}(a - a^x)^2 \cdot E$$

has rank 0 or 1. In particular, this matrix has $p - 1$ eigenvalues equal to 0 and one last eigenvalue, which we denote by $\varepsilon(\chi)$, that might also be 0. Clearly $\varepsilon(\chi) = \operatorname{Tr} \mathfrak{X}(\mu^*\mu)$, where Tr indicates the matrix trace.

Note that $E^2 = pE$ and that $\operatorname{Tr} ED = \operatorname{Tr} D$ if D is a diagonal matrix. Thus, since $\mathfrak{X}(A)$ is diagonal, we have

$$\begin{aligned} \varepsilon(\chi) &= \operatorname{Tr} E \cdot \mathfrak{X}(a - a^x)^2 \cdot E = \operatorname{Tr} E^2 \cdot \mathfrak{X}(a - a^x)^2 \\ &= p \operatorname{Tr} E \cdot \mathfrak{X}(a - a^x)^2 = p \operatorname{Tr} \mathfrak{X}(a - a^x)^2. \end{aligned}$$

Furthermore, by definition of the character χ, we have

$$\begin{aligned} \operatorname{Tr} \mathfrak{X}(a - a^x)^2 &= \operatorname{Tr} \mathfrak{X}(a^2) - 2 \operatorname{Tr} \mathfrak{X}(aa^x) + \operatorname{Tr}((a^2)^x) \\ &= \chi(a^2) - 2\,\chi(a^{1+x}) + \chi((a^2)^x) = 2\,\chi(a^2) - 2\,\chi(a^{1+x}) \end{aligned}$$

since a^2 and $(a^2)^x$ are conjugate group elements and hence have the same character values. In other words,

$$\varepsilon(\chi) = 2p\big(\chi(a^2) - \chi(a^{1+x})\big) = 2p\big(\chi(g) - \chi(h)\big),$$

where we set $g = a^2$ and $h = a^{1+x}$.

The goal now is to show that χ can be chosen with $|\chi(g) - \chi(h)|$ reasonably large. To this end, it is necessary to consider all irreducible complex characters ξ of G. Indeed, we use $\sum$ to denote a sum over all such irreducible characters, and we let $\sum'$ denote a sum over all nonlinear irreducible characters. We know that $g, h \in A = G'$, the commutator subgroup of G, so if ξ is a linear character of G, then $\xi(g) = \xi(h) = 1$ and $\xi(g) - \xi(h) = 0$. Furthermore, recall that $g = a^2$ and $h = a^{1+x}$ are not conjugate in G. Thus, since $\mathfrak{C}_G(g) = \mathfrak{C}_G(h) = A$, the Second Orthogonality Character Relation (see [4, Theorem 2.18]) yields

$$\begin{aligned} \sum{}' |\xi(g) - \xi(h)|^2 &= \sum |\xi(g) - \xi(h)|^2 = \sum \big(\xi(g) - \xi(h)\big)\big(\overline{\xi(g)} - \overline{\xi(h)}\big) \\ &= \sum \xi(g)\overline{\xi(g)} + \sum \xi(h)\overline{\xi(h)} - \sum \xi(g)\overline{\xi(h)} - \sum \xi(h)\overline{\xi(g)} \\ &= |\mathfrak{C}_G(g)| + |\mathfrak{C}_G(h)| - 0 - 0 = 2\,|A|. \end{aligned}$$

Since each nonlinear irreducible character of G corresponds to an $\langle x \rangle$-orbit of non-principal linear characters of A, the number of summands in $\sum'$ is precisely equal to $(|A| - 1)/p$. Thus, if χ determines the largest summand in $\sum'$, then we have

$$|\chi(g) - \chi(h)|^2 \geq 2p\,|A|/(|A| - 1) > 2p,$$

and hence

$$|\varepsilon(\chi)| = 2p\,|\chi(g) - \chi(h)| > 2p\sqrt{2p} = (2p)^{3/2}.$$

Finally, since G is finite, $\mu^*\mu$ is certainly algebraic over $\mathbb{C}$, and by the above, its minimal polynomial has at least one root having absolute value larger than $(2p)^{3/2} > 14$. Thus Lemma 1.2(ii) implies that $(1+\mu, 1+\mu^*)$ is a free pair. □

It would be nice to prove a * analog of Corollary 1.7, one that asserts that $\mathbb{Z}[G]$ always has a free bicyclic pair when G is a finite non-Dedekind group. But as we have seen in Examples 2.2 and 2.4, there are p-group counterexamples to this general assertion. Thus, perhaps the best we can do here is to assume that all Sylow subgroups of G are abelian, and indeed we have

Theorem 2.8. *Let G be a finite nonabelian group that admits an involution *. If all Sylow subgroups of G are abelian, then $\mathbb{Z}[G]$ contains a free bicyclic pair (u, u^*).*

Proof. Write * as σ followed by the inverse map, and proceed by induction on $|G|$. Note that the property of having only abelian Sylow subgroups is inherited by subgroups and factor groups. If G has a proper nonabelian σ-stable subgroup H or factor group G/N, then induction applies to this group of smaller order. Thus $\mathbb{Z}[H]$ or $\mathbb{Z}[G/N]$ has a free bicyclic pair, and hence so does $\mathbb{Z}[G]$ by Lemma 1.11.

We can therefore assume that all proper σ-stable subgroups H of G and factor groups G/N are abelian. Since G cannot be a nonabelian p-group, Lemma 1.12 implies that G is the semidirect product $G = A \rtimes X$, where A is an elementary abelian q-group for some prime q, X is a cyclic group of prime order $p \neq q$, and $\mathfrak{Z}(G) = 1$. But then, Example 2.5 implies that $\mathbb{Z}[G]$ has a free bicyclic pair unless $|G|$ is odd, * is the inverse map on G/A, and there exists $1 \neq a \in A$ with $a^* = a$ and $\langle a \rangle \triangleleft G$.

We consider this remaining possibility. Since $|G|$ is odd, there exists a Sylow p-subgroup of G that is σ-stable. In other words, we can assume that $X^\sigma = X$ and hence that $X^* = X$. With this, if $A_1 = \langle a \rangle$, then we see that $A_1 \rtimes X$ is a σ-stable subgroup of G, and it is nonabelian since $a \notin \mathfrak{Z}(G)$. The minimality of G now implies that $G = A_1 \rtimes X$ and hence that $A = A_1 = \langle a \rangle$. But $a^* = a$, so we conclude that * is the identity on A, and Example 2.7 yields the result. □

3. Left and Right Bicyclic Units

Because of the presence of the involution *, the types of bicyclic units that were considered in the previous sections are really right-left symmetric. By this, we mean that if $1+\mu = 1+(1-b)a\widehat{B}$ has $(1-b)$ as a left factor, then $1+\mu^* = 1+\widehat{B^*}a^*(1-b^*)$ has the factor $(1-b^*)$ on the right, and of course $(1+\mu^*)^* = 1+\mu$. On the other hand, there are papers like [1] that seem to consider both types of bicyclic units, and one wonders whether this is really necessary. In other words, is it possible that every left bicyclic unit $1+(1-b)a\widehat{B}$ is also a right bicyclic unit $1+\widehat{C}d(1-c)$, and vice versa. As we will see below, this is not always the case. Indeed, if this property occurs, then G is necessarily nilpotent and quite possibly G must have small nilpotence degree.

In this section, we work in group algebras $K[G]$ over a field K. We start with the following presumably well-known result.

Lemma 3.1. *Let C be a finite cyclic group and let $\theta\colon C \to \overline{C}$ be an epimorphism. If $\bar{c}$ is a generator of the cyclic group $\overline{C}$, then there exists a generator c of C with $\theta(c) = \bar{c}$.*

Proof. Write $C = \prod_p C_p$ as a direct product of its Sylow p-subgroups. Then each $C_p = \langle c_p \rangle$ is cyclic. Furthermore, $\overline{C} = \theta(C) = \prod_p \overline{C}_p$, where $\overline{C}_p = \theta(C_p)$. Of course, $\theta(c_p)$ is a generator of $\overline{C}_p$, and it is possible that some $\overline{C}_p$ are trivial.

Now let $\bar{c}$ be a generator of $\overline{C}$. Then $\bar{c} = \prod_p \bar{c}_p$, with each $\bar{c}_p$ a generator of $\overline{C}_p$. If $\theta(c_p) = 1$, then certainly $\bar{c}_p = \theta(c_p)^1$. On the other hand, if $\theta(c_p) \neq 1$, then we must have $\bar{c}_p = \theta(c_p)^{a_p}$ with $p \nmid a_p$. Thus $\bar{c}_p = \theta(c_p)^{a_p}$ with $p \nmid a_p$ in all cases. Finally, if $c = \prod_p c_p^{a_p}$, then c is certainly a generator of C, since $p \nmid a_p$, and $\theta(c) = \prod_p \theta(c_p)^{a_p} = \prod_p \bar{c}_p = \bar{c}$. □

With this, we offer a sufficient condition for a left bicyclic unit to also be a right bicyclic unit. Since the plus 1 part of the formula is the same in both the right and left expressions, we just consider the square 0 part.

Lemma 3.2. *Let $x, a \in G$, write $X = \langle x \rangle$, $A = \langle a \rangle$, and assume that*

$$X \triangleleft XX^a \triangleleft XX^aA.$$

If $Y = X^{a^{-1}}$, then there exists a generator y of Y with $(1-x)a\widehat{X} = \widehat{Y}a(1-y)$.

Proof. Set $H = XX^a$. Since $X \triangleleft H$ and H is normalized by A, it follows that $X^{a^i} \triangleleft H$ for all $a^i \in A$. Also, since $H = H^{a^{-1}}$, we have $H = YX = XY$, where $Y = X^{a^{-1}} = aXa^{-1}$. Note that $aX = Ya$, so $a\widehat{X} = \widehat{Y}a$. Furthermore, since $Y \triangleleft H$, we know that $\widehat{Y}$ is central in $K[H]$. Thus

$$(1-x)a\widehat{X} = (1-x)\widehat{Y}a = \widehat{Y}(1-x)a.$$

Now $H = XX^a$ and x^a generates X^a, so we see that the image of x^a generates the cyclic group H/X. But $H = XY$, so $H/X \cong Y/(X \cap Y)$, and it follows from the preceding lemma that there exists a generator y of Y that maps to the image of x^a. In other words, $x^a \in Xy$, so $x^a = x^j y$ for some $x^j \in X$. With this, we have

$$\widehat{Y}xa = \widehat{Y}a \cdot a^{-1}xa = a\widehat{X} \cdot x^j y = a\widehat{X} \cdot y = \widehat{Y}ay,$$

and hence

$$(1-x)a\widehat{X} = \widehat{Y}(a - xa) = \widehat{Y}(a - ay) = \widehat{Y}a(1-y),$$

as required. □

Since axa^{-1} generates $Y = aXa^{-1}$ in the above, it is tempting to think that we can take y to be $x^{a^{-1}}$. However, this is not the case in general. Indeed, consider the following example, where we take $H = XX^a$ to be an abelian direct product and where we use a mixture of additive and multiplicative notation.

Example 3.3. *Let X be cyclic of order n, let H be the direct sum $H = X + X^a$, and let the conjugation action of a be given by right multiplication by the matrix*

$$\begin{bmatrix} 0 & 1 \\ r & s \end{bmatrix}.$$

Here $r, s \in \mathbb{Z}/n\mathbb{Z}$ with r invertible in this ring. Then the generator y of the previous lemma is uniquely given by $(axa^{-1})^r$.

Proof. Note that x and x^a correspond to the row vectors $\begin{bmatrix} 1 & 0 \end{bmatrix}$ and $\begin{bmatrix} 0 & 1 \end{bmatrix}$, respectively. Furthermore, the action of a^{-1} is given by the matrix

$$\frac{1}{r}\begin{bmatrix} -s & 1 \\ r & 0 \end{bmatrix},$$

and therefore $axa^{-1} = x^{a^{-1}}$ corresponds to the row matrix $\begin{bmatrix}-s/r & 1/r\end{bmatrix}$. If $y = (x^{a^{-1}})^t$, we see that $x^a \in Xy$ if and only if $\begin{bmatrix}0 & 1\end{bmatrix}$ and $t\begin{bmatrix}-s/r & 1/r\end{bmatrix}$ have the same second coordinate. Obviously, this occurs precisely when $t \equiv r \bmod n$. □

Next we handle the necessary direction.

Lemma 3.4. *Let x, a, y, b be group elements, write $X = \langle x\rangle$ and $Y = \langle y\rangle$, and suppose that $(1-x)a\widehat{X} = \widehat{Y}b(1-y)$ in $K[G]$. If $\operatorname{char} K \neq 2$ and $A = \langle a\rangle$, then*

$$X \lhd XX^a \lhd XX^aA.$$

Furthermore, if a does not normalize X, then Y and b satisfy $Yb = Ya = aX$.

Proof. If a normalizes X, then the conclusion is clearly satisfied, so it suffices to assume that this is not the case. Since $(1-y)\widehat{Y} = 0$, we have $(1-y)(1-x)a\widehat{X} = 0$ and hence

$$a\widehat{X} + yxa\widehat{X} = xa\widehat{X} + ya\widehat{X}.$$

Note that the support of $a\widehat{X}$ is aX and all group elements occur with coefficient 1. Therefore all group elements of aX occur on the above left hand side with coefficient 1 or 2 and, since $\operatorname{char} K \neq 2$, they must occur on the right. But a does not normalize X, so $aX \neq xaX$, and we conclude that $aX = yaX$. Thus, $y^a = a^{-1}ya \in X$ and $o(y) \leq o(x)$. By symmetry, $o(x) \leq o(y)$, so the two elements have the same order. It follows that $a^{-1}Ya = X$, so we have $Y = X^{a^{-1}}$, $aX = Ya$, and $a\widehat{X} = \widehat{Y}a$. Thus $0 = (1-y)(1-x)a\widehat{X} = (1-y)(1-x)\widehat{Y}a$ and, since $(1-y)\widehat{Y} = 0$, we conclude that $(1-y)x\widehat{Y} = 0$. In other words, x normalizes Y and $X^{a^{-1}} = Y \lhd YX = X^{a^{-1}}X$. Conjugating by a then yields $X \lhd XX^a$.

Since $Y \lhd YX$, it follows that $\widehat{Y}$ is central in $K[YX]$. Therefore, using $a\widehat{X} = \widehat{Y}a$ again, we have

$$\widehat{Y}b(1-y) = (1-x)a\widehat{X} = (1-x)\widehat{Y}a = \widehat{Y}(1-x)a,$$

where the last equality follows because x commutes with $\widehat{Y}$. Thus

$$\widehat{Y}b + \widehat{Y}xa = \widehat{Y}by + \widehat{Y}a$$

and, since $\operatorname{char} K \neq 2$, the left and right-hand cosets of Y must match. But $Yxa = Ya$ implies that $x \in Y$, so $X = Y = X^{a^{-1}}$ and a normalizes X, a contradiction. Thus $Yb = Ya$ and $Yxa = Yby = Yay$. This yields, $aya^{-1} \in Yx \subseteq YX$ and, since we already have $axa^{-1} \in aXa^{-1} = Y$, we conclude that a^{-1} normalizes YX. Thus a normalizes $YX = (YX)^a = XX^a$, as required. □

By combining the previous two lemmas, we clearly obtain

Theorem 3.5. *Let $X = \langle x\rangle$ and $A = \langle a\rangle$ be cyclic subgroups of G and assume that $\operatorname{char} K \neq 2$. Then $(1-x)a\widehat{X} = \widehat{Y}b(1-y)$ in $K[G]$ for some $Y = \langle y\rangle \subseteq G$ and $b \in G$ if and only if*

$$X \lhd XX^a \lhd XX^aA.$$

Furthermore, if a does not normalize X, then Y and b satisfy $Yb = Ya = aX$.

As a consequence, we have

Corollary 3.6. *Let $\operatorname{char} K \neq 2$. If every element $(1-x)a\widehat{X} \in K[G]$ with $X = \langle x\rangle$ can be written as $\widehat{Y}b(1-y)$, for some $Y = \langle y\rangle \subseteq G$ and $b \in G$, then G is nilpotent.*

Proof. By the previous theorem, the hypothesis guarantees that all cyclic subgroups X of G are normalized by all their conjugates X^a. Thus, if X^G denotes the normal closure of X in G, then $X \lhd X^G \lhd G$, and every cyclic subgroup of G is subnormal. It follows that every subgroup of G is subnormal, so normalizers grow in G, and consequently G is nilpotent. □

We should point out that there are nonabelian groups that satisfy the group-theoretic conditions of Theorem 3.5, namely that $X \lhd XX^a \lhd XX^aA$, for all cyclic subgroups $X = \langle x \rangle$ and $A = \langle a \rangle$. Indeed, suppose G is any nilpotent group of class 2, so that $G' \subseteq \mathfrak{Z}(G)$. Then $x^{-1}a^{-1}xa = [x, a] = z \in \mathfrak{Z}(G)$, so $x^a = a^{-1}xa = xz$ commutes with x, and hence $X \lhd XX^a$. Furthermore, since a commutes with z, it follows easily that $x^{a^i} = xz^i$ for all integer exponents i, and therefore $XX^a = \langle x, z \rangle$ is normalized by A.

Conversely, we already know by Corollary 3.6 that if these group-theoretic conditions are satisfied for all X and a, then G must be nilpotent. In fact, it is possible that when G is a p-group with p sufficiently large, that the nilpotence class of G is forced to be reasonably small. For example, suppose for each X and $a \in G$, we have $X^a = X$ or $X^a \cap X = 1$, which of course occurs when G has period p. Then $X \lhd XX^a$ implies that $X^a \lhd (XX^a)^a = XX^a$, and hence either $XX^a = X$ or $XX^a \cong X \times X^a$. In particular, XX^a is always abelian, and thus x commutes with $a^{-1}x^{-1}a{\cdot}x = [a, x]$. In other words, G satisfies the Engel condition $[a, x, x] = 1$ for all $a, x \in G$, and a result of Levi (see [10, Theorem VI.8.c]) implies that G has nilpotence class at most 3. Indeed, if $p \neq 3$, then G has class at most 2.

More generally, if we just know that X and X^a are normal in XX^a, then the factor group $XX^a/(X \cap X^a)$ is abelian, so $[a, x, x] \in X \cap X^a$. Consequently, G satisfies the Engel condition $[a, x, x, x] = 1$ for all $a, x \in G$.

References

[1] A. del Rio and J. Z. Gonçalves, *Bicyclic units, Bass cyclic units and free groups*, J. Group Theory, **11** (2008), 247–265.

[2] A. Dooms, E. Jespers and M. Ruiz, *Free groups and subgroups of finite index in the unit group of an integral group ring*. Comm. Algebra, **35** (2007), 2879–2888.

[3] J. Z. Gonçalves and D. S. Passman, *Linear groups and group rings*, J. Algebra, **295** (2006), 94–118 (ibid. **307** (2007), 930–931).

[4] I. M. Isaacs, *Character Theory of Finite Groups*, Academic Press, New York, 1976.

[5] T. Y. Lam and D. B. Leep, *Combinatorial structure on the automorphism group of* S_6. Expositiones Math. **11** (1993), 289–308.

[6] Z. S. Marciniak and S. K. Sehgal, *Constructing free subgroups of integral group ring units*, Proc. AMS **125** (1997), 1005–1009.

[7] G. Miller and H. Moreno, *Non-abelian groups in which every subgroup is abelian*, Trans. AMS **4** (1903), 398–404.

[8] D. S. Passman, *The Algebraic Structure of Group Rings*, Wiley-Interscience, New York, 1977.

[9] ——— *Free subgroups in linear groups and group rings*, Contemp. Math, **456** (2008) 151–164.

[10] E. Schenkman, *Group Theory*, Van Nostrand, Princeton, 1965.

[11] W. R. Scott, *Group Theory*, Dover, New York, 1987.

Department of Mathematics, University of São Paulo, São Paulo, 05389-970, Brazil
E-mail address: jz.goncalves@usp.br

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