INVOLUTIONS AND FREE PAIRS OF BASS CYCLIC UNITS IN INTEGRAL GROUP RINGS

J. Z. GONÇALVES AND D. S. PASSMAN

Abstract. Let $\mathbb{Z}G$ be the integral group ring of the finite nonabelian group G over the ring of integers $\mathbb{Z}$, and let * be an involution of $\mathbb{Z}G$ that extends one of G. If x and y are elements of G, we investigate when pairs of the form $(u_{k,m}(x), u_{k,m}(x^*))$, or $(u_{k,m}(x), u_{k,m}(y))$, formed respectively by Bass cyclic and $*$-symmetric Bass cyclic units, generate a free noncyclic subgroup of the unit group of $\mathbb{Z}G$.

1. Bass Cyclic Units

Let $\mathbb{Z}G$ be the integral group ring of the group G over the ring of integers $\mathbb{Z}$, and let $U(\mathbb{Z}G)$ be its group of units. Suppose that * is an involution of $\mathbb{Z}G$ that extends the involution * of G. If u is a unit of $\mathbb{Z}G$, then u^* is also a unit, and we say that u is $*$-*symmetric* if $u^* = u$. In this paper, we are interested in the nature of subgroups of $U(\mathbb{Z}G)$ of the form $\langle u, u^*\rangle$ or $\langle v, w\rangle$, where v and w are $*$-symmetric units. Indeed, if v and w are any two units, then we say that (v, w) is a *free pair* if $\langle v, w\rangle$ is a free group on the two generators.

If B is a finite subgroup of G, we denote by $\widehat{B} \in \mathbb{Z}G$ the sum of elements of B in $\mathbb{Z}G$. Since $(1-b)\widehat{B} = \widehat{B}(1-b) = 0$ for any $b \in B$, it follows that elements of the form $(1-b)a\widehat{B}$, with $a \in G$, have square 0. The expression $u = 1 + (1-b)a\widehat{B}$ is therefore a unit of $\mathbb{Z}G$, and if $B = \langle b\rangle$ is cyclic, then u is called a *bicyclic unit*. It is clear that $u \neq 1$ if and only if $a \in G$ does not normalize $B = \langle b\rangle$.

In reference [3], it was shown that if G is a nonabelian finite group admitting an involution *, and if all Sylow subgroups of G are abelian, then $\mathbb{Z}G$ contains a free bicyclic pair (u, u^*). We can ask how general is this occurrence, and if it extends to other types of units. Recall that for large families of finite groups, see for example [5], the subgroup of $U(\mathbb{Z}G)$ generated by the bicyclic and Bass cyclic units has finite index in $U(\mathbb{Z}G)$. Thus we are led to ask if this latter result from [3] remains true if we replace bicyclic units by Bass cyclic units, as defined below.

Let x be an element of G of order $o(x) = d$ and write $\widehat{x}$ for $\widehat{\langle x\rangle}$. Then $x^j\widehat{x} = \widehat{x}x^j = \widehat{x}$ for all integers j, and we define

$$u_{k,m}(x) = (1 + x + \cdots + x^{k-1})^m + \frac{1-k^m}{d}\widehat{x},$$

where $1 \leq k$, $\gcd(k, d) = 1$, and where m is multiple of $\phi(d)$, the Euler ϕ-function evaluated at d. The latter two conditions imply that $k^m \equiv 1 \bmod d$ and hence that $u_{k,m}(x) \in \mathbb{Z}[G]$.

The first author's research was supported in part by CNPq grant 300.128/2008-8 and Fapesp-Brazil, Proj. Tematico 2009/52665-0. The second author's research was supported in part by NSA grant H98230-10-1-0217.

Recall that the augmentation map of $\mathbb{Z}[G]$ is the homomorphism $\mathbb{Z}[G] \to \mathbb{Z}$ determined by $g \mapsto 1$ for all $g \in G$. Then each $u_{k,m}(x)$ has augmentation 1, and indeed, $u_{k,m}(x) = (1+x+\cdots+x^{k-1})^m + c\widehat{x}$ where c is the unique integer such that this element has augmentation 1. We can, of course, view $u_{k,m}(x)$ as a polynomial function on x subject to $x^d = 1$. In particular, we can evaluate this function on any y satisfying $y^d = 1$. For example, we can take $y = x^j$ for any integer j, or $y = \varepsilon$ where ε is any complex dth root of unity.

Lemma 1.1. *With the above notation, we have*

i. $u_{(k+d),m}(x) = u_{k,m}(x)$.
ii. $u_{k,m}(x) \cdot u_{k,n}(x) = u_{k,(m+n)}(x)$.
iii. $u_{k,m}(x) \cdot u_{\ell,m}(x^k) = u_{kl,m}(x)$.
iv. $u_{1,m}(x) = 1$ *and* $u_{k,m}(x)^{-1} = u_{\ell,m}(x^k)$ *where* $k\ell \equiv 1 \bmod d$.
v. $u_{k,m}(x^{-1}) = u_{k,m}(x)$ *if* $(k-1)m$ *is divisible by* $o(x) = d$.

Proof. For parts (i), (ii) and (iii), we use the identities $x^j\widehat{x} = \widehat{x}x^j = \widehat{x}$ and $x^d = 1$ to easily show that the right and left sides of each equation differ by an integer multiple of $\widehat{x}$, say $c\widehat{x}$. Furthermore, since both sides have augmentation 1, their difference has augmentation 0. But the augmentation of $c\widehat{x}$ is equal to cd, so it follows that $c = 0$ and hence both sides of each equation are equal. For part (iv), it is clear that $u_{1,m}(x) = 1$ and hence, by part (i), $u_{r,m}(x) = 1$ for any positive integer $r \equiv 1 \bmod d$. In particular, if $k\ell \equiv 1 \bmod d$, then (iii) implies that $u_{k,m}(x) \cdot u_{\ell,m}(x^k) = 1$, as required. Finally, note that

$$(1 + x^{-1} + \cdots + x^{-(k-1)})^m \cdot x^{(k-1)m} = (1 + x + \cdots + x^{k-1})^m,$$

so $x^{(k-1)m} = 1$ implies that $u_{k,m}(x^{-1}) = u_{k,m}(x)$, and (v) is proved. □

In view of (iv) above, each $u_{k,m}(x)$ is a unit in $\mathbb{Z}[G]$ and, as in [5, Chapter 2], these elements are called *Bass cyclic units*. Furthermore, in view of (i), $u_{k,m}(x)$ is determined by k modulo d and hence we can assume that $1 \le k \le d-1$. When the first parameter is equal to 1, then $u_{1,m}(x) = 1$, and when this parameter is equal to $d-1$, then it is easy to see that $u_{d-1,m}(x) = x^{(d-1)m}$. Because of this, we usually take $2 \le k \le d-2$, and hence $d \ge 5$ and $d \ne 6$. Note that there are $\phi(d) - 2$ choices for k so, since $\phi(d) \ge \sqrt{d}/2$, it is easy to check that suitable values for k always exist. Of course, when d is odd, we can take $k = 2$. Finally, it follows from (ii) that $u_{k,m}(x)^a = u_{k,ma}(x)$ for all integers $a \ge 1$.

Lemma 1.2. *Let* $\theta\colon \mathbb{Z}[G] \to \mathbb{Z}[H]$ *be the group ring epimorphism determined by the group epimorphism* $\theta\colon G \to H$*, and let* h *be an element of* H *of order* d*. If* $u_{k,m}(h)$ *is a Bass cyclic unit of* $\mathbb{Z}[H]$*, then there exists an element* $x \in G$*, whose order has the same prime factors as those of* h*, and a Bass cyclic unit* $u_{k,m'}(x)$ *of* $\mathbb{Z}[G]$*, such that* $u_{k,m'}(x)$ *maps via* θ *to a positive integer power of* $u_{k,m}(h)$*.*

Proof. If h is a π-element, then there exists a π-element $x \in G$ with $\theta(x) = h$. In particular, we now know that k is prime to d', the order of x. On the other hand, we may have $d' > d$ so it is not necessarily true that $\phi(d')$ divides m. Nevertheless, there certainly exists a positive integer a so that $\phi(d')$ divides $m' = ma$. Then $u_{k,m'}(x)$ is a Bass cyclic unit and, since $\theta(\widehat{x})$ is an integer multiple of $\widehat{h}$, it follows from part (ii) of the preceding lemma that $\theta(u_{k,m'}(x))$ and $u_{k,m}(h)^a$ agree up to an integer multiple of $\widehat{h}$, say $c\widehat{h}$. But both of these terms have augmentation 1, so we conclude that $c = 0$, as required. □

Recall that the *support* of a group ring element $\alpha = \sum_g a_g g \in \mathbb{Z}G$ is the set $\operatorname{supp}\alpha$ of group elements g with coefficients $a_g \neq 0$. Furthermore, the *support group* of α is the subgroup of G generated by $\operatorname{supp}\alpha$. For Bass cyclic units, we have

Lemma 1.3. *If $o(x) = d \geq 5$ and $2 \leq k \leq d-2$, then $\langle x\rangle$ is the support group of the unit $u_{k,m}(x)$.*

Proof. Let $\varepsilon = e^{2\pi i/d}$ be this particular complex dth root of unity and let p be a prime divisor of d. If $a = 1$ and $b = 1 + d/p$, then $b \not\equiv \pm a \bmod d$ since $d \geq 5$. Hence, by [2, Lemma 3.4(ii)], we have $|u_{k,m}(\varepsilon^a)| \neq |u_{k,m}(\varepsilon^b)|$, and this implies that $\operatorname{supp} u_{k,m}(x) \not\subseteq \langle x^p\rangle$. Indeed, if $\operatorname{supp} u_{k,m}(x) \subseteq \langle x^p\rangle$, then $u_{k,m}(x)$ is a polynomial in x^p, modulo $(x^d - 1)$, and since $ap \equiv bp \bmod d$, this would imply that $u_{k,m}(\varepsilon^a) = u_{k,m}(\varepsilon^b)$, certainly a contradiction. Finally, since $\operatorname{supp} u_{k,m}(x) \subseteq \langle x\rangle$ and $\operatorname{supp} u_{k,m}(x) \not\subseteq \langle x^p\rangle$ for any prime p that divides d, the result follows. □

As usual, an *involution* * on a ring R or a group G is an anti-automorphism of order 1 or 2. For example, if R is the full $n \times n$ matrix ring over a commutative ring, then the transpose map is an involution on R. Furthermore, for any group G, it is clear that the inverse map $^{-1}$ is a suitable involution. Note that if * is any involution of G, then * extends naturally to an involution of $\mathbb{Z}G$. The main result of this paper is

Theorem 1.4. *Let G be a finite nonabelian group of order prime to 6 and suppose * is an involution on $\mathbb{Z}G$ that extends one of G. Then, for some prime p and appropriate parameters k and m, we have either*

i. *there exist two p-elements x and y such that the pair of $*$-symmetric Bass cyclic units $(u_{k,m}(x), u_{k,m}(y))$ is free, or*
ii. *there exists a p-element x such that the pair $(u_{k,m}(x), u_{k,m}(x^*))$ is free.*

This will be proved in the next section. As we mentioned earlier, if $x \in G$ has order $d = 1, 2, 3, 4$ or 6, then any Bass cyclic unit $u_{k,m}(x)$ is trivial, that is of the form x^j. Thus, when dealing with these units, we are usually forced to avoid the primes 2 and 3. This explains the hypothesis above that $|G|$ is prime to 6.

On the other hand, in Section 3, we consider symmetric groups $G = \operatorname{Sym}_n$, and of course these groups have order divisible by 6. We show, for example

Proposition 1.5. *Let $G = \operatorname{Sym}_n$, where n is an odd integer and $n \geq 5$. If the involution * on G is not the inverse map, then G has a suitable d-cycle x with $(u_{k,m}(x), u_{k,m}(x^*))$ being a free pair.*

2. Involutions

The goal of this section is to prove the main theorem. We start by considering the lifting of $*$-symmetric elements in groups of odd order. Recall that if * is an involution of the group G, then * is the commuting product of an automorphism σ of G with the inverse map $^{-1}$. Of course, σ is * followed by the inverse map, and $\sigma^2 = 1$. In particular, if $G = \langle g\rangle$ is cyclic of odd prime power order, then either $\sigma = 1$ and $g^* = g^{-1}$, or σ is the inverse map and $g^* = g$.

Lemma 2.1. *Let G be a finite group of odd order with an involution *, and let $N \lhd G$ with $N^* = N$. Then * determines an involution * on $G/N = H$ in such a way that the natural epimorphism $\theta\colon G \to H$ is a $*$-map. Furthermore, let p be*

a prime and let h be a p-element of H with $h^* = h^{-1}$ (or h). Then there exists a p-element x in G with $x^* = x^{-1}$ (or x) and with $\theta(x) = h$.

Proof. The first part is clear. Now write * as the automorphism σ followed by the inverse map. Then $h^* = h$ (or h^{-1}) implies that h is fixed by * (or σ). Choose $g \in G$ with $\theta(g) = h$. Then the coset Ng is the complete inverse image of h in G, and hence Ng is stablized by * (or σ). But $|Ng| = |N|$ is odd, while * (or σ) acts on this set as a permutation of order 1 or 2. Thus there exists $y \in Ng$ with $y^* = y$ (or $\sigma(y) = y$), and hence with $y^* = y$ (or $y^* = y^{-1}$). Furthermore, * acts in the same manner on all elements of the cyclic group $\langle y \rangle$ and hence on any p-element $x \in \langle y \rangle$ that maps to h. □

Part (ii) below is a $*$-version of Lemma 1.2 with essentially the same proof.

Lemma 2.2. *Let G be a group of odd order with an involution *, and let p be a prime.*

i. *If x is a p-element of G and if $\langle x \rangle$ is $*$-stable, then some power of any Bass cyclic unit $u_{k,m}(x)$ is $*$-symmetric.*
ii. *Suppose N is a $*$-stable normal subgroup of G and set $H = G/N$. If h is a p-element of H and if $u_{k,m}(h)$ is a $*$-symmetric Bass cyclic unit in $\mathbb{Z}H$, then there exists a p-element $x \in G$ and a $*$-symmetric Bass cyclic unit $u_{k,m'}(x)$, such that $u_{k,m'}(x)$ maps to a positive power of $u_{k,m}(h)$ under the natural epimorphism $\theta\colon \mathbb{Z}G \to \mathbb{Z}H$.*

Proof. (i) Since x is a p-element and $\langle x \rangle$ is $*$-stable, it follows that $x^* = x$ or x^{-1}. Now choose an integer a so that $o(x)$ divides $m' = ma$. Then $u_{k,m}(x)^a = u_{k,m'}(x)$ is $*$-symmetric since $u_{k,m'}(x)^* = u_{k,m'}(x^{\pm 1}) = u_{k,m'}(x)$ by Lemma 1.1(v).

(ii) Since $u_{k,m}(h) = u_{k,m}(h)^* = u_{k,m}(h^*)$, it follows from Lemma 1.3 that $\langle h \rangle$, the support group of $u_{k,m}(h)$, is $*$-stable. Thus $h^* = h$ or h^{-1} and, by the previous lemma, there exists a p-element $x \in G$ with $x^* = x$ or x^{-1}, and with $\theta(x) = h$. By (i) above, we can choose $m' = ma$ so that $u_{k,m'}(x)$ is a $*$-symmetric Bass cyclic unit, and clearly θ maps $u_{k,m'}(x)$ to $u_{k,m}(h)^a$. □

Our next step is to sharpen [3, Lemma 1.12] under the assumption that G has odd order. For this, we use the following well-known fact which is a consequence of properties of regular p-groups. We offer a quick elementary proof for the convenience of the reader.

Lemma 2.3. *Let G be a p-group with p odd, and assume that its commutator subgroup G' is central and has period p. Then the p-power map $x \mapsto x^p$ is a homomorphism from G into its center $\mathfrak{Z}(G)$.*

Proof. If $x, y \in G$, then $yxy^{-1} = xt$ for some $t \in G'$. Thus since t is central in G and $t^p = 1$, we have $yx^iy^{-1} = (xt)^i = x^it^i$ and $yx^py^{-1} = x^p$. In particular, x^p commutes with all $y \in G$, so $x^p \in \mathfrak{Z}(G)$. Next, by induction on $i \geq 1$, we have $(xy)^i = x^iy^it^{i(i-1)/2}$. Indeed, this holds for $i = 1$, and if it holds for i, then $yx^i = x^iyt^i$ implies that $(xy)^{i+1} = (xy)(x^iy^it^{i(i-1)/2}) = x^{i+1}y^{i+1}t^j$, where $j = i + i(i-1)/2 = (i+1)i/2$, and the induction step is proved. When $i = p$, we conclude that $(xy)^p = x^py^p$ since p being odd implies that p divides $p(p-1)/2$. □

With this, we have

Lemma 2.4. *Let G be a finite nonabelian group of odd order 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 G is the semidirect product $G = A \rtimes X$, where $X = \langle x \rangle$ is cyclic of prime order p, and where A and X are σ-stable. Furthermore, we have either*

i. *A is a cyclic p-group, or*
ii. *$A = Z \times Y$ is an abelian group of type (p, p), where $Z = \mathfrak{Z}(G)$ and Y is a σ-stable subgroup of order p, or*
iii. *$A = A_1 \times A_2$ is an elementary abelian q-group for some prime $q \neq p$. Here $A_1 = \{a \in A \mid \sigma(a) = a\}$ and $A_2 = \{a \in A \mid \sigma(a) = a^{-1}\}$. Furthermore, $\mathfrak{Z}(G) = 1$, and X acts faithfully and irreducibly on A. Finally, if $\sigma(x) = x$, then $A_1 = 1$ or $A_2 = 1$, while if $\sigma(x) = x^{-1}$, then $A_1 \neq 1$ and $A_2 \neq 1$.*

Proof. By [3, Lemma 1.12], we know that either G is a p-group with $|G'| = p$ and $|G/\mathfrak{Z}(G)| = p^2$, or $G = A \rtimes X$ where $X = \langle x \rangle$ is cyclic of prime order p and A is an elementary abelian q-group for some prime $q \neq p$. Furthermore, in the latter case, $\mathfrak{Z}(G) = 1$, and X acts faithfully and irreducibly on A.

We consider these two possibilities in turn. First note that if σ acts on an elementary abelian q-group V with $q \neq 2$, then since σ satisfies the separable polynomial $\zeta^2 - 1 = (\zeta - 1)(\zeta + 1)$ in $\mathrm{GF}(q)[\zeta]$, we conclude that $V = V_1 \times V_2$, where $V_1 = \{v \in V \mid \sigma(v) = v\}$ and $V_2 = \{v \in V \mid \sigma(v) = v^{-1}\}$. It follows that σ acts in a completely reducible manner on V and that all σ-composition factors are cyclic of order q.

Now suppose G is a p-group with p odd, $|G'| = p$ and $|G : \mathfrak{Z}(G)| = p^2$. If V is the subgroup of $\mathfrak{Z}(G)$ consisting of all elements of order 1 or p, then $G' \subseteq V$ and V is σ-stable. In particular, $V = G' \times J$, where J is a σ-stable complement. Since G/J is certainly a nonabelian σ-stable homomorphic image of G, it follows that $J = 1$ and hence $Z = \mathfrak{Z}(G)$ is cyclic. Let Z_1 be the unique maximal subgroup of Z.

By the previous lemma, the p-power map $\theta\colon G \to Z$ given by $\theta(g) = g^p$ is a homomorphism that clearly commutes with σ. It follows that the kernel K of θ is a σ-stable normal subgroup of G, and of course K consists of all elements of G of order 1 or p. Furthermore, since $\theta(Z) = Z_1$, we see that $\theta(G) = Z$ or Z_1.

Suppose first that $\theta(G) = Z$. Then $|K| = p^2$ and $K \cap Z = G'$, so $K = G' \times X$, where X is a σ-stable subgroup of G of order p. Note that σ acts on the (p, p) group G/Z and that $XZ/Z = KZ/Z$ is a σ-stable subgroup of order p. Thus there exists a σ-stable complement A/Z, where A is a subgroup of G of index p. Since $X \not\subseteq A$, we see that $K \cap A = G'$ has order p, and this group is the kernel of the restriction $\theta\colon A \to Z$. Thus $\theta(A) = Z$, so A is cyclic, $G = A \rtimes X$ and therefore G satisfies (i).

On the other hand, if $\theta(G) = Z_1 = \theta(Z)$, then $|K| = p^3 = |G : Z_1|$ and $G = ZK$. It follows that K is a nonabelian σ-stable subgroup of G, and hence $G = K$ has order p^3. By considering the action of σ on G/Z, we see that G has two σ-stable subgroups A and B of order p^2, each containing Z. Of course, both A and B are abelian of type (p, p), $AB = G$ and $A \cap B = Z$. Furthermore, by considering the action of σ on B, we see that $B = Z \times X$, where X is a σ-stable subgroup of order p. Thus $G = AX = A \rtimes X$, and G satisfies (ii).

Finally, suppose $G = A \rtimes X$, where A is an elementary abelian q-group, $|X| = p$, and where X acts faithfully and irreducibly on A. Since A is the unique Sylow q-subgroup of G, it is characteristic in G and hence σ-stable. Thus $A = A_1 \times A_2$

as described in (iii). Next note that X is a Sylow p-subgroup of G and that σ permutes $\mathrm{Syl}_p(G)$, the set of all such Sylow p-subgroups. But $|\mathrm{Syl}_p(G)|$ is odd since q is odd, and hence σ stabilizes some member of $\mathrm{Syl}_p(G)$. We can therefore assume that σ stabilizes $X = \langle x \rangle$, and hence that $\sigma(x) = x$ or x^{-1}.

In the former case, the action on A given by σ and via conjugation by x commute, and hence both A_1 and A_2 are X-stable. But X acts irreducibly on A, so either $A_1 = 1$ or $A_2 = 1$. On the other hand, if $\sigma(x) = x^{-1}$, then the dihedral group $X\langle\sigma\rangle$ of order $2p$ acts faithfully on A. Thus since σ is not central in $X\langle\sigma\rangle$, the action of σ cannot be central in $\mathrm{Aut}(A)$. It follows that $\sigma \neq 1$ or $^{-1}$ on A, and hence both A_1 and A_2 must be nontrivial. Thus G satisfies (iii), and the proof is complete. □

At this point, we need two results from [2], where all the serious computations have already been done. Unfortunately, these two results are not stated in the generality we require. Thus, we restate them below and briefly comment in each proof on the changes we have made. To start with, we have

Lemma 2.5. *Let $G = A \rtimes X$ be a nonabelian semidirect product, where $A \lhd G$ and $X = \langle x \rangle$ is cyclic of prime order $p \geq 5$. Assume that either $A = \langle a \rangle$ is cyclic of prime power order, or A is abelian of type (p, p) and $a \in A \setminus \mathfrak{Z}(G)$. Then, for any $k \not\equiv \pm 1 \bmod o(a)$ with $\gcd(k, o(a)) = 1$ and any $r \not\equiv \pm 1, 0 \bmod p$, there exist Bass cyclic units $u_{k,t}(a)$ and $u_{r,s}(x)$ that generate a nonabelian free subgroup of the unit group of the integral group ring $\mathbb{Z}[G]$.*

Proof. This is essentially [2, Lemma 4.3], but with the choices of $a \in A$ and the parameters r and k carefully spelled out, as in the first paragraph of its proof. □

Unlike the previous result, the next one uses a careful choice of the parameter k.

Lemma 2.6. *Let $X = \langle x \rangle$ be a cyclic group of prime order p that acts faithfully and irreducibly on an elementary abelian q-group A, with q a prime different from p. If $p \geq 5$ and $q \geq 3$, then for any $1 \neq a \in A$, there exist suitable Bass cyclic units $u_{k,m}(x)$ and $u_{k,m}(a^{-1}xa)$ that generate a nonabelian free subgroup of the unit group of $\mathbb{Z}[A \rtimes X]$.*

Proof. This is [2, Lemma 4.6], but without the hypothesis that $|A| > q$. As it turns out, that assumption only shows up in [2, Lemma 4.4], and it is not really needed there. Indeed, the latter result has now been improved in [3, Lemma 2.6(i)] to allow for the possibility that $|A| = q$. □

With these two lemmas in hand, we can now offer the

Proof of Theorem 1.4. Suppose we can find two group elements $x_1, x_2 \in G$ such that $\langle u_{k,m_1}(x_1), u_{k,m_2}(x_2) \rangle$ is a free group on the two generators. Then any positive power of the first unit and any positive power of the second will also generate a free subgroup of $U(\mathbb{Z}G)$. In particular, if $m = \mathrm{lcm}(m_1, m_2)$, then $(u_{k,m}(x_1), u_{k,m}(x_2))$ is a free pair. In other words, in this proof, we do not have to concern ourselves with the equality of the second parameters.

As usual, write * as the automorphism σ followed by the inverse map. Then any $*$-stable subgroup or homomorphic image of G is σ-stable, and vice-versa. We proceed by induction on $|G|$. If G has a nonabelian σ-stable proper subgroup, then the result clearly follows. On the other hand, suppose $\mathbb{Z}H$ is a nonabelian proper σ-stable homomorphic image of $\mathbb{Z}G$. Then, by induction, we have either a free pair

$(u_{k,m}(h), u_{k,m}(h^*))$ or a free $*$-symmetric pair $(u_{k,m}(h_1), u_{k,m}(h_2))$ of Bass cyclic units, where h, h_1 and h_2 are p-elements of H.

In the first case, Lemma 1.2 implies that there exists a p-element $g \in G$ and parameter m' such that $u_{k,m'}(g)$ maps to a power of $u_{k,m}(h)$. Then $u_{k,m'}(g^*)$ maps to a power of $u_{k,m}(h^*)$, and we see that $(u_{k,m'}(g), u_{k,m'}(g^*))$ is a free pair in $\mathbb{Z}G$. In the second case, Lemma 2.2(ii) yields p-elements $g_1, g_2 \in G$ and parameters m_1, m_2 such that $u_{k,m_i}(g_i)$ is $*$-symmetric and maps to a power of $u_{k,m}(h_i)$ for $i = 1, 2$. Thus, $(u_{k,m_1}(g_1), u_{k,m_2}(g_2))$ is a free pair of $*$-symmetric Bass cyclic units in $\mathbb{Z}G$, and the result follows by induction.

We can now assume that all proper σ-stable subgroups and homomorphic images of G are abelian, so Lemma 2.4 comes into play. In particular, $G = A \rtimes X$, where $X = \langle x \rangle$ is cyclic of prime order p, and where A and X are σ-stable.

Suppose first that G satisfies (i) or (ii) of Lemma 2.4, so that G is a p-group. Furthermore, either $A = \langle a \rangle$ is cyclic or we can choose a to generate the $*$-stable subgroup Y of A. In either case, $a \in A \setminus \mathfrak{Z}(G)$ and, if $2 \leq k \leq p-2$, then Lemma 2.5 implies that there exist suitable parameters m, m' so that $(u_{k,m}(x), u_{k,m'}(a))$ is a free pair. Furthermore, by Lemma 2.2(i), suitable powers of these two units form a free pair of $*$-symmetric Bass cyclic units.

Finally, suppose G satisfies Lemma 2.4(iii). Then $\mathfrak{Z}(G) = 1$, $A = A_1 \times A_2$ is an elementary abelian q-group for some prime $q \neq p$, and X acts faithfully and irreducibly on A. If $A_1 \neq 1$, we can choose $1 \neq a \in A_1$ so that, by definition, $\sigma(a) = a$ and hence $a^* = a^{-1}$. It follows that $\langle x \rangle$ and $\langle a^{-1}xa \rangle$ are distinct $*$-stable subgroups of G of order p, and Lemma 2.6 implies that there exist parameters k, m so that $u_{k,m}(x)$ and $u_{k,m}(a^{-1}xa)$ form a free pair. Indeed, by Lemma 2.2(i), suitable powers of these units yield a free pair of $*$-symmetric Bass cyclic units.

On the other hand, if $A_1 = 1$, then $\sigma(a) = a^{-1}$ for all $a \in A$ and $\sigma(x) = x$. Hence $a^* = a$ and $x^* = x^{-1}$. Now take any $1 \neq a \in A$ and note that $a^2 \neq 1$. Thus, by Lemma 2.6 again, there exist parameters k, m such that $(u_{k,m}(x), u_{k,m}(a^2xa^{-2}))$ is a free pair. Furthermore, by taking powers if necessary, we can assume that $p = o(x)$ divides m. Next, by conjugating both of these units by a, we see that $a^{-1}u_{k,m}(x)a = u_{k,m}(a^{-1}xa)$ and $a^{-1}u_{k,m}(a^2xa^{-2})a = u_{k,m}(axa^{-1})$ also form a free pair. In particular, if we set $y = a^{-1}x^{-1}a$, then $y^* = (a^{-1}x^{-1}a)^* = axa^{-1}$, and we deduce that $(u_{k,m}(y^{-1}), u_{k,m}(y^*))$ is a free pair. But $p = o(y)$ divides m, so $u_{k,m}(y^{-1}) = u_{k,m}(y)$ by Lemma 1.1(v), and therefore $(u_{k,m}(y), u_{k,m}(y^*))$ is a free pair. This completes the proof. □

3. Symmetric Groups

Results like those in Lemmas 2.5 and 2.6 follow from [2, Corollary 4.1] once the so-called idempotent conditions are verified. But these conditions can become more difficult to deal with as the dimensions of V_+ and V_- increase. Indeed, even the 2-dimensional case is surprisingly nontrivial in general, but there is a trick from [4] that can sometimes be used.

Let V' be a (right) vector space over the real numbers $\mathbb{R}$ and let $V = V' \otimes_{\mathbb{R}} \mathbb{C}$ be the extended complex vector space. Clearly, complex conjugation $^-$ can be defined on V by setting $^-\colon v' \otimes c \mapsto v' \otimes \bar{c}$, and it is easy to see that $\overline{vc} = \bar{v}\,\bar{c}$ for all $v \in V$ and $c \in \mathbb{C}$. Of course, $^-$ is additive and has order 2 as an operator. If $t\colon V \to V$ is a $\mathbb{C}$-linear transformation, we define $\bar{t}\colon V \to V$ so that $\bar{t}\,\bar{v} = \overline{tv}$. Then $\bar{t}$ is also

a $\mathbb{C}$-linear transformation and $^-$ defines an automorphism of $\mathrm{End}_{\mathbb{C}}(V)$ of order 2 with $\overline{tc} = \bar{t}\,\bar{c}$. The following is [4, Lemma 3.3].

Lemma 3.1. *Suppose $V = V' \otimes_{\mathbb{R}} \mathbb{C}$ is as above. Let $e, \bar{e}$ be orthogonal idempotent linear transformations on V and let $f, \bar{f}$ also be orthogonal idempotent linear transformations on V. Assume that the transformation $t = (e+\bar{e})(f+\bar{f})$ has rank ≤ 1. Then for every $v \in V$, there exists some $c \in \mathbb{C}$ with $|c| = 1$ such that $e\bar{f}\bar{v} = efvc$.*

Proof. By the rank assumption, there exists a line $L \subseteq V$ with $tV \subseteq L$. Let $v \in V$. Then $(e+\bar{e})fv = t(fv) \in L$ and $(e+\bar{e})\bar{f}\bar{v} = t(\bar{f}\bar{v}) \in L$. Furthermore, the definition of $^-$ on $\mathrm{End}_{\mathbb{C}}(V)$ implies that if $w = t(fv)$, then $\overline{w} = \bar{t}(\bar{f}\bar{v}) = t(\bar{f}\bar{v})$. Now, if either w or $\overline{w}$ is 0, then both are 0 and $\overline{w} = wc$ with $c = 1$. Otherwise, both w and $\overline{w}$ are nonzero elements of the line L, and therefore $\overline{w} = wc$ for some $c \in \mathbb{C}$. By applying $^-$, we get $w = \overline{w}\,\bar{c} = wc\bar{c}$, so $c\bar{c} = 1$ and $|c| = 1$. We therefore have $\overline{w} = wc$ with $|c| = 1$ in all cases. Thus $(e+\bar{e})\bar{f}\bar{v} = (e+\bar{e})fvc$, and multiplying on the left by e yields the result. □

As an application, we consider certain Bass cyclic units $u_{k,m}(x)$ in the integral group ring of the symmetric group $G = \mathrm{Sym}_n$. As will be apparent, the first parameter k plays an almost nonexistent role in these examples. This differs significantly from the proof of Theorem 1.4, where a delicate choice of parameter is required in at least one lemma. Recall that the action of G on $\{1, 2, \ldots, n\}$ gives rise to a real permutation module V' with natural $\mathbb{R}$-basis denoted by $\{[1], [2], \ldots, [n]\}$. The latter set is then also a $\mathbb{C}$-basis for $V = V' \otimes_{\mathbb{R}} \mathbb{C}$, and these basis vectors are fixed under complex conjugation.

Now suppose $x = (z_1\ z_2\ \ldots\ z_d)$ is a d-cycle in G. Then x acts on V by cyclically permuting the basis vectors $\{[z_1], [z_2], \ldots, [z_d]\}$ and by fixing the remaining members. In particular, the matrix of x, in its action on V, is similar to $\mathrm{diag}(P, I)$, where P is the $d \times d$ permutation matrix

$$P = \begin{bmatrix} & & & & 1 \\ 1 & & & & \\ & 1 & & & \\ & & \ddots & & \\ & & & 1 & \end{bmatrix}$$

and I is the $(n-d) \times (n-d)$ identity matrix. Furthermore, if * denotes the transpose conjugate map on the ring of $n \times n$ matrices over $\mathbb{C}$, then it is easy to see that $x^* = x^{-1}$.

Note that the minimal polynomial of P is $\zeta^d - 1$, so P is similar to a $d \times d$ diagonal matrix whose diagonal entries run through all the complex dth roots of unity. It follows that the matrix of x is similar to a diagonal matrix where each nonidentity dth root of unity occurs precisely once on the diagonal and where the remaining $(n-d)+1$ entries are equal to 1. In particular, if μ is a nonidentity dth root of unity, then V_μ, the μ-eigenspace of x, has dimension 1.

If $X = \langle x \rangle$ then, by restriction, V is naturally a $\mathbb{C}[X]$-module. Since X is cyclic, the primitive idempotents of $\mathbb{C}[X]$ are all of the form $e_\mu = (1/d)\sum_{i=0}^{d-1} x^i \mu^{-i}$ as μ runs through the dth roots of unity. Since $xe_\mu = \mu e_\mu$, it follows that the μ-eigenspace of x in V is given by $e_\mu V = V_\mu$. Thus each e_μ, with $\mu \neq 1$, has rank 1 in its action on V, while e_1 has rank $(n-d)+1$. Furthermore, the transpose conjugate of e_μ satisfies $e_\mu^* = (1/d)\sum_{i=0}^{d-1} x^{-i}\mu^i = e_\mu$. In other words, these idempotent

matrices are all Hermitian symmetric. With all of this, we can use a variant of the argument of [4, Theorem 3.4] to prove

Theorem 3.2. *Let $d \geq 5$ and $d \neq 6$, and suppose that x and y are the two d-cycles in $G = \mathrm{Sym}_n$ given by*

$$x = (1\ 2\ 3\ 4\ 5\ 6\ \ldots\ d) \quad \text{and} \quad y = (2\ 3\ 1\ 4\ 5\ 6\ \ldots\ d).$$

Then, for all parameters k and k' relatively prime to d, with $2 \leq k, k' \leq d-2$, there exists a parameter m so that the Bass cyclic units $u_{k,m}(x)$ and $u_{k',m}(y)$ generate a nonabelian free subgroup of the unit group of $\mathbb{Z}[G]$.

Proof. Since $G = \mathrm{Sym}_n$ acts faithfully on V, it is convenient to think of G as a subgroup of $\mathrm{GL}(V)$. From the nature of the action of G on the $\mathbb{R}$-basis $\{[1], [2]. \ldots, [n]\}$ of V', it is then clear that $g = \bar{g}$ for every $g \in G$. Of course, when we take $\mathbb{C}$-linear combinations of elements of G in $\mathrm{End}_{\mathbb{C}}(V)$, we are actually looking at homomorphic images of the corresponding elements in the group algebra $\mathbb{C}[G]$.

As we observed, the matrix $x \in \mathrm{GL}(V)$ is diagonalizable with each nonidentity dth root of unity μ occurring once on the diagonal and with the remaining $(n-d)+1$ diagonal entries equal to 1. Furthermore, the projection of V onto the μ-eigenspace V_μ is precisely the idempotent $e_\mu = (1/d)\sum_{i=0}^{d-1} x^i \mu^{-i}$. In particular, each e_μ, with $\mu \neq 1$, has rank 1 and, since $x = \bar{x}$, it follows that $\bar{e}_\mu = e_{\bar{\mu}}$.

Set $q = \phi(d)$. If k is any acceptable parameter, that is if $2 \leq k \leq d-2$ and $\gcd(k, d) = 1$, then $S = u_{k,q}(x) \in \mathrm{GL}(V)$, and clearly when x is diagonal, then so is S. Indeed, the eigenvalues of S are precisely the numbers $u_{k,q}(\mu)$ as μ runs through the eigenvalues of x. Furthermore, the eigenspaces of S and of x are identical with the understanding that some merging can occur. In other words, the S-eigenspace for the eigenvalue $u_{k,q}(\mu)$ is the direct sum of all V_η with $u_{k,q}(\mu) = u_{k,q}(\eta)$.

Let $V = V_+ \oplus V_0 \oplus V_-$ denote the S-decomposition of V, where X_+ corresponds to all eigenvalues of maximum absolute value and where X_- corresponds to all eigenvalues of minimum absolute value. Then it follows, from [2, Lemma 3.4(ii)] and the above, that $X_+ = V_{\mu_+} \oplus V_{\bar{\mu}_+}$ for a suitable primitive dth root of unity μ_+, and hence $\dim X_+ = 2$. In particular, the projection map $e_+ \colon V \to X_+$ is given by $e_+ = e_{\mu_+} + e_{\bar{\mu}_+} = e_{\mu_+} + \bar{e}_{\mu_+}$. Similarly, by [2, Lemma 3.4(iii)], $\dim X_- = 2$, $X_- = V_{\mu_-} \oplus V_{\bar{\mu}_-}$ for a suitable primitive dth root of unity μ_-, and $e_- = e_{\mu_-} + e_{\bar{\mu}_-} = e_{\mu_-} + \bar{e}_{\mu_-}$.

Obviously, the above properties of x apply equally well to y, but of course with a change of notation. Thus, for a suitable integer k', we let $T = u_{k',q}(y) \in \mathrm{GL}(V)$, and we let $V = Y_+ \oplus Y_0 \oplus Y_-$ denote the T-decomposition of V. Here Y_+ corresponds to all eigenvalues of T of maximum absolute value and Y_- corresponds to all eigenvalues of T of minimum absolute value. Furthermore, we let $f_+ \colon V \to Y_+$ and $f_- \colon V \to Y_-$ be the corresponding projections. Next, for each complex dth root of unity η, we set $f_\eta = (1/d)\sum_{i=0}^{d-1} y^i \eta^{-i}$. Then it follows, as for the element x, that $\dim Y_+ = \dim Y_- = 2$ and that $f_+ = f_{\eta_+} + \bar{f}_{\eta_+}$ and $f_- = f_{\eta_-} + \bar{f}_{\eta_-}$ for suitable primitive dth roots of unity η_+ and η_-.

We now use [2, Corollary 4.1] to prove that there exist positive exponents z and z' so that $\langle S^z, T^{z'} \rangle = \langle S^z \rangle * \langle T^{z'} \rangle$ is free of rank 2. For this, it suffices to show that the eight idempotent conditions, $\mathrm{rank}\, e_\pm f_\pm = 2$ and $\mathrm{rank}\, f_\pm e_\pm = 2$, are satisfied and, by symmetry, we need only consider the products $e_\pm f_\pm$. Indeed, if * is the transpose conjugate map, then $e_\pm^* = e_\pm$ and $f_\pm^* = f_\pm$, so $\mathrm{rank}\, f_\pm e_\pm = \mathrm{rank}\, (f_\pm e_\pm)^* = \mathrm{rank}\, e_\pm f_\pm$. Thus, in view of our previous observations, it suffices to show that if μ

and η are any primitive complex dth roots of unity, then $t = (e_\mu + \bar{e}_\mu)(f_\eta + \bar{f}_\eta)$ has rank ≥ 2.

Suppose, by way of contradiction, that $\operatorname{rank} t \leq 1$. Then, by Lemma 3.1 and the fact that the vector $[1]$ is fixed under $^-$, there exists a complex number c of absolute value 1 with $e_\mu \bar{f}_\eta[1] = e_\mu f_\eta[1]c$. In particular, if we write

$$d^2 e_\mu \bar{f}_\eta[1] = \sum_{j=1}^{n} a_j[j] \quad \text{and} \quad d^2 e_\mu f_\eta[1] = \sum_{j=1}^{n} b_j[j],$$

then we must have $|a_1| = |b_1|$.

Note that

$$d^2 e_\mu f_\eta[1] = \sum_{i=0}^{d-1} x^i \mu^{-i} \cdot \sum_{j=0}^{d-1} y^j \eta^{-j} \cdot [1]$$

and hence b_1, the coefficient of $[1]$ in this vector, is given by

$$\begin{aligned} b_1 &= 1 + \mu^{-(d-1)}\eta^{-(d-2)} + \mu^{-(d-2)}\eta^{-(d-1)} + \sum_{j=1}^{d-3} \mu^{j+2}\eta^{-j} \\ &= 1 + \mu\eta^2 + \mu^2\eta + \mu^2 \sum_{j=1}^{d-3} (\mu\eta^{-1})^j. \end{aligned}$$

In particular, if $\mu = \eta$, we have

$$b_1 = 1 + \mu\eta^2 + \mu^2\eta + (d-3)\mu^2 = 1 + 2\mu^3 + (d-3)\mu^2.$$

On the other hand, if $\mu \neq \eta$, then $\sum_{j=0}^{d-1} (\mu\eta^{-1})^j = 0$, so

$$\begin{aligned} b_1 &= 1 + \mu\eta^2 + \mu^2\eta - \mu^2 \left(1 + (\mu\eta^{-1})^{d-2} + (\mu\eta^{-1})^{d-1}\right) \\ &= 1 + \mu\eta^2 + \mu^2\eta - \mu^2(1 + \mu^{-2}\eta^2 + \mu^{-1}\eta) \\ &= 1 + \mu\eta^2 + \mu^2\eta - (\mu^2 + \eta^2 + \mu\eta) \\ &= (1-\mu)(1-\eta)(1+\mu+\eta). \end{aligned}$$

Furthermore, by replacing η by $\bar{\eta}$ in the above, we obtain analogous formulas for the coefficient a_1.

Now in verifying the idempotent condition, we are comparing the sets of eigenvalues $\{\mu, \bar{\mu}\}$ and $\{\eta, \bar{\eta}\}$. In particular, since $\eta \neq \bar{\eta}$, it suffices to assume the notation chosen so that $\mu \neq \eta$. Thus, b_1 is given by the second formula above. On the other hand, there are two possibilities for a_1. If $\mu \neq \bar{\eta}$, then

$$a_1 = (1-\mu)(1-\bar{\eta})(1+\mu+\bar{\eta}),$$

so $|a_1| = |b_1|$ yields

$$|1 + \mu + \bar{\eta}| = |1 + \mu + \eta|.$$

Thus

$$(1 + \mu + \bar{\eta})(1 + \bar{\mu} + \eta) = (1 + \mu + \eta)(1 + \bar{\mu} + \bar{\eta})$$

and hence $\mu\eta + \bar{\mu}\bar{\eta} = \mu\bar{\eta} + \bar{\mu}\eta$. Of course, this says that the two dth roots of unity $\mu\eta$ and $\mu\bar{\eta}$ have the same real part, so they are either equal or are complex conjugates. But this implies that either $\eta = \bar{\eta}$ or $\mu = \bar{\mu}$, certainly a contradiction.

On the other hand, if $\mu = \bar{\eta}$, then $a_1 = 1 + 2\mu^3 + (d-3)\mu^2$ and $|a_1| > (d-3) - 3 = d - 6$. Furthermore,

$$b_1 = 1 + \mu\eta^2 + \mu^2\eta - (\mu^2 + \eta^2 + \mu\eta) = \mu + \bar{\mu} - \mu^2 - \bar{\mu}^2,$$

so $|b_1| < 4$. In particular, if $|a_1| = |b_1|$, then $4 > d - 6$ and hence $d < 10$. Since, by assumption, $d \geq 5$ and $d \neq 6$, we need only verify numerically that $|a_1| \neq |b_1|$ for $d = 5, 7, 8$ and 9, and this is quite easy for the latter three using a computer algebra system like Maple or Magma. On the other hand, $|a_1| \neq |b_1|$ fails when $d = 5$, and indeed computer computations show that some $(e_\mu + \bar{e}_\mu)(f_\eta + \bar{f}_\eta)$ have rank 1.

We now know that for $d \geq 7$ the idempotent conditions are satisfied, so we conclude from [2, Corollary 4.1] that, for suitable positive integers z and z', $\langle S^z, T^{z'} \rangle = \langle S^z \rangle * \langle T^{z'} \rangle$ is indeed free of rank 2. Note that that $|u_{k,q}(\mu_+)|$ and $|u_{k',q}(\eta_+)|$ are both larger than 1, and therefore both S and T have infinite multiplicative order.

Finally, Lemma 1.1(ii) implies that $\big(u_{k,q}(x)\big)^z = u_{k,m}(x)$ and $\big(u_{k',q}(y)\big)^{z'} = u_{k',m'}(y)$, where $m = qz$ and $m' = qz'$. Thus, the Bass cyclic units $u_{k,m}(x)$ and $u_{k',m'}(y)$ in the integral group ring $\mathbb{Z}[G]$ map to S^z and $T^{z'}$, respectively, under the homomorphism $\mathbb{Z}[G] \subseteq \mathbb{C}[G] \to \mathrm{End}_{\mathbb{C}}(V)$. It therefore follows from the above that $\langle u_{k,m}(x), u_{k',m'}(y) \rangle$ is also a nonabelian free group. Furthermore, by taking suitable powers if necessary, we can assume that $m' = m$, and the theorem is proved for $d \geq 7$.

To handle the missing $d = 5$ case, we use a different, somewhat larger, representation for $H = \mathrm{Alt}_5$. This is described for example in [1]. Note that

$$H = \mathrm{gp}\langle a, b \mid a^2 = b^3 = (ab)^5 = 1 \rangle$$

and that $\mathbb{C}[H]$ has an irreducible representation of degree 5 given by

$$a = (1\ 2)(3\ 4) \mapsto \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ -1 & -1 & -1 & -1 & -1 \end{bmatrix}$$

$$b = (1\ 3\ 5) \mapsto \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ -1 & -1 & -1 & -1 & -1 \end{bmatrix}.$$

Furthermore, under this representation, we have

$$x = ab = (1\ 2\ 3\ 4\ 5) \mapsto \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

$$y = bab = (2\ 3\ 1\ 4\ 5) \mapsto \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ -1 & -1 & -1 & -1 & -1 \end{bmatrix}.$$

Since the latter two matrices are both similar to the permutation matrix P, the preceding argument can also apply to this situation. Indeed, in this case, we discover, using Maple or Magma, that the eight matrices $(e_\mu + \bar{e}_\mu)(f_\eta + \bar{f}_\eta)$ and $(f_\eta + \bar{f}_\eta)(e_\mu + \bar{e}_\mu)$ all have rank 2. With this, the result also holds for $d = 5$. $\square$

We need one more example using the same proof.

Lemma 3.3. *Let $G = \mathrm{Sym}_n$ with $n \geq d = 5$, and let x and y be the two d-cycles given by*

$$x = (1\ 2\ 3\ 4\ 5) \quad \text{and} \quad y = (2\ 1\ 3\ 4\ 5).$$

If k and k' are each either 2 or 3, then there exists a parameter m so that the Bass cyclic units $u_{k,m}(x)$ and $u_{k',m}(y)$ generate a nonabelian free subgroup of the unit group of $\mathbb{Z}[G]$.

Proof. Since $x, y \in \mathrm{Alt}_5$, we can use the irreducible representation of $\mathrm{Alt}_5 = \langle a, b\rangle$ as described in the preceding proof. Then $x = ab$ and $y = (ab^2a)b(ab^2a)$, so

$$x = (1\ 2\ 3\ 4\ 5) \mapsto \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

$$y = (2\ 1\ 3\ 4\ 5) \mapsto \begin{bmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ -1 & -1 & -1 & -1 & -1 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Since the latter two matrices are both similar to the permutation matrix P, the same argument as above can also apply to this situation. Indeed, here we discover, using Maple or Magma, that the eight matrices $(e_\mu + \bar{e}_\mu)(f_\eta + \bar{f}_\eta)$ and $(f_\eta + \bar{f}_\eta)(e_\mu + \bar{e}_\mu)$ all have rank 2, and therefore the result follows. □

As is well known, all automorphisms of $G = \mathrm{Sym}_n$ are inner except when $n = 6$. In particular, if σ is an automorphism of order 2, and $n \neq 6$, then σ is conjugation by an element $g \in G$ of order 2, and of course g is a product of disjoint transpositions. As a consequence of the above, we have

Corollary 3.4. *Let $g \in G = \mathrm{Sym}_n$ be a product of $c \geq 1$ disjoint transpositions and let * be the involution on G that is conjugation by g followed by the inverse map. Assume that either $c \geq 2$ and $n \geq d = 2c + 1$, or $c = 1$ and $n \geq d = 5$. Then there exists a d-cycle $x \in G$ such that $(u_{k,m}(x), u_{k,m}(x^*))$ is a free pair in $\mathbb{Z}G$. Here k is any suitable first parameter, and m depends upon k.*

Proof. First let $c \geq 2$, so $n \geq d = 2c + 1$, and assume that the points $\{1, 2, \ldots, n\}$ are labeled so that

$$g = (2\ 3) \prod_{i=0}^{c-2} (4{+}i\ \ d{-}i).$$

If we set $x = (1\ 2\ 3\ 4\ 5\ 6\ \ldots\ d)$, then it is easy to check that $x^g = g^{-1}xg = (1\ 3\ 2\ d\ d{-}1\ d{-}2\ \ldots\ 4)$ and therefore that $x^* = (x^g)^{-1} = (2\ 3\ 1\ 4\ 5\ 6\ \ldots\ d) = y$. Theorem 3.2 now yields the result in this case. Finally, let $c = 1$ and assume the points are labeled so that $g = (1\ 2)$. If $x = (1\ 2\ 3\ 4\ 5)$, then $x^g = y = (2\ 1\ 3\ 4\ 5)$ and the preceding lemma implies that $(u_{k,m}(x), u_{k,m}(y))$ is a free pair. Furthermore, by taking powers, if necessary, we can assume that $d = 5$ divides m. Then $u_{k,m}(y) = u_{k,m}(y^{-1}) = u_{k,m}(x^*)$, and hence $(u_{k,m}(x), u_{k,m}(x^*))$ is a free pair, as required. □

Note that Proposition 1.5 follows immediately from this result. Furthermore, if $c = 0$, then * is the inverse map on G. In this case, x commutes with $x^* = x^{-1}$, so $u_{k,m}(x)$ commutes with $u_{k,m}(x^*)$, and certainly $(u_{k,m}(x), u_{k,m}(x^*))$ cannot be a free pair.

References

[1] R. Abbott, S. Linton, R. Parker, P. Walsh, R. Wilson, et al, *Atlas of Finite Group Representations*, available online at http://brauer.maths.qmul.ac.uk/Atlas/.

[2] J. Z. Gonçalves and D. S. Passman, *Linear groups and group rings*, J. Algebra **295** (2006), 94–118.

[3] ——— *Involutions and free pairs of bicyclic units in integral group rings*, to appear in J. Group Theory.

[4] D. S. Passman, *Free subgroups in linear groups and group rings*, Contemporary Math. **456** (2008), 151–164.

[5] S. K. Sehgal, *Units in Integral Group Rings*, Longman Scientific, Harlow, 1993.

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

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