Contemporary Mathematics

Free Subgroups in Linear Groups and Group Rings

D. S. Passman

Abstract. This paper is an extension of the talk I gave at the International Conference on Non-Commutative Rings, Group Rings, Diagram Algebras and Applications at the University of Madras in December 2006. It discusses certain techniques used to prove the existence of free subgroups in linear groups and in the unit group of integral group rings of finite groups. Its main focus is recent joint work with Jairo Gonçalves on non-abelian free groups generated by Bass cyclic units. Additional concrete examples are also offered.

1. The Ping-Pong Lemma

The goal here is to discuss joint work with Jairo Gonçalves [**GP**] on the existence of free subgroups in unit groups of matrix rings and group rings. The subject starts with the famous ping-pong lemma of F. Klein and reaches its high point with the theorem of J. Tits [**T**] on free subgroups of linear groups. There are interesting group rings results due to B. Hartley and P. F. Pickel [**HP**], as well as to Z. S. Marciniak and S. K. Sehgal [**MS**]. Indeed, Sehgal's group ring books [**S1, S2**] are mostly concerned with the structure of the unit group of $\mathbb{Z}[G]$. Our work generalizes aspects of Tits' machinery and these new results are then applied to obtain concrete pairs of units that generate free groups in the integral group rings of certain critical groups. The hard part here is to verify the so-called idempotent conditions. While this is mostly a survey paper, a few new interesting examples are offered at the end.

In order to construct non-abelian free subgroups of a group G, we are faced with the problem of proving that a certain subgroup of G is in fact a free product. Specifically, if G_1 and G_2 are nonidentity subgroups of G, we would like to know whether the subgroup $\langle G_1, G_2\rangle$ they generate is naturally isomorphic to the free product $G_1 * G_2$. In other words, we have to decide whether or not every element of $\langle G_1, G_2\rangle$ is uniquely writable as a finite alternating product of elements of $G_1^{\#}$, the nonidentity elements of G_1, and of $G_2^{\#}$. To do this, one can use the following elementary, but surprisingly powerful, "ping-pong lemma" of F. Klein.

2000 *Mathematics Subject Classification.* 16S34, 16U60, 20E06, 20H20.

Research supported in part by NSA grant 144-LQ65. The author would like to thank Professors S. K. Jain, P. Kanwar and S. Parvathi for organizing this wonderful conference and for their kindness and hospitality.

LEMMA 1.1. *Let G be a group with nonidentity subgroups G_1 and G_2, and suppose that G acts on a set P having distinct nonempty subsets P_1 and P_2. If $G_1^\# P_1 \subseteq P_2$, $G_2^\# P_2 \subseteq P_1$, and if $|G_2| > 2$, then $\langle G_1, G_2\rangle$ is naturally isomorphic to the free product $G_1 * G_2$.*

PROOF. It suffices to show that $1 \in G$ cannot be written as a nonempty alternating product of elements coming from $G_1^\#$ and $G_2^\#$. Suppose by way of contradiction that such a product $1 = h_1h_2\cdots h_n$ exists with $n \geq 2$. If the product starts and ends in $G_1^\#$, that is if $h_1, h_n \in G_1^\#$, then by conjugating this expression by a nonidentity element of G_2, we obtain a similar expression, but this time starting and ending in $G_2^\#$. Next, if $h_1 \in G_1^\#$ and $h_n \in G_2^\#$, then since $|G_2| > 2$, we can conjugate this expression by an element of $G_2^\#$, different from h_n^{-1}, to obtain a similar product but starting and ending in $G_2^\#$. Since the same argument handles the $h_1 \in G_2^\#$, $h_n \in G_1^\#$ situation, we can therefore replace any such expression by one with $h_1, h_n \in G_2^\#$. But then, the alternating nature of the action of $G_1^\#$ and $G_2^\#$ on P_1 and P_2 yields $1P_2 = P_2$ and $h_1h_2\cdots h_nP_2 \subseteq P_1$, and hence $P_2 \subseteq P_1$. Furthermore, by conjugating the expression for 1 by a nonidentity element of G_1, we obtain a similar expression but now starting and ending in $G_1^\#$. This time, the alternating nature of the action yields $1P_1 = P_1$ and $h_1h_2\cdots h_nP_1 \subseteq P_2$, so we obtain the reverse inclusion $P_1 \subseteq P_2$. Hence $P_1 = P_2$, contradiction. □

Note that the assumption above that one of the subgroups has order > 2 is definitely necessary. Indeed, if $|G_1| = |G_2| = 2$, then $G = \langle G_1, G_2\rangle$ acts on the set $\{1, 2\}$ with both $G_1^\#$ and $G_2^\#$ interchanging the subsets $P_1 = \{1\}$ and $P_2 = \{2\}$. Obviously, G can be any finite or infinite dihedral group, including the Klein fours group, while $G_1 * G_2$ is clearly the infinite dihedral group.

To see how the ping-pong lemma might apply, we offer a proof from [**H**] of the following well-known result attributed to I. N. Sanov concerning free subgroups of the complex special linear group $\mathrm{SL}_2(\mathbb{C})$.

PROPOSITION 1.2. *Let $G = \mathrm{SL}_2(\mathbb{C})$ and suppose*

$$g_1 = \begin{bmatrix} 1 & a_1 \\ 0 & 1 \end{bmatrix} \quad \textit{and} \quad g_2 = \begin{bmatrix} 1 & 0 \\ a_2 & 1 \end{bmatrix}$$

are two unipotent elements in this group. If $|a_1|, |a_2| \geq 2$, then g_1 and g_2 generate a free subgroup of G of rank 2.

PROOF. Note that $G_1 = \langle g_1\rangle$ is infinite cyclic, and so is $G_2 = \langle g_2\rangle$. Thus it suffices to show that $\langle G_1, G_2\rangle = G_1 * G_2$. To this end, observe that G acts on $P = \mathbb{C}^2$, the 2-dimensional space of column vectors $v(r, s) = \begin{bmatrix} r & s \end{bmatrix}^{\mathrm{T}}$, and we define P_1 to be the subset of P consisting of those matrices $v(r, s)$ with $|r| < |s|$, and P_2 to be the subset of P consisting of those matrices with $|r| > |s|$. Now if $v(r, s) \in P_1$ and if $t \in G_1^\#$, then $t = g_1^n$ for some nonzero integer n and $t{\cdot}v(r, s) = v(r + na_1s, s)$. Since $|na_1| \geq 2$ and $|s| > |r|$, we have

$$|r + na_1s| \geq |na_1|{\cdot}|s| - |r| \geq 2|s| - |r| > |s|.$$

Thus $G_1^\# P_1 \subseteq P_2$ and similarly $G_2^\# P_2 \subseteq P_1$. Lemma 1.1 now yields the result. □

We remark that some assumption on the size of a_1 and a_2 is required here, since if $a_1 = a_2 = 1$, then

$$g_1^{-1} g_2 g_1^{-1} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

has order 4 and hence $\langle g_1, g_2 \rangle$ cannot be free.

Surely the high point of this subject is the following wonderful theorem of J. Tits [**T**] on linear groups, known as the "Tits' alternative".

Theorem 1.3. *Let F be a field of characteristic 0 and let G be a subgroup of $\mathrm{GL}_n(F)$. Then G is either solvable-by-finite or it has a non-abelian free subgroup.*

The result is not quite true in characteristic $p > 0$. Indeed, if F is the algebraic closure of $\mathrm{GF}(p)$, then the general linear group $G = \mathrm{GL}_n(F)$ is close to being infinite simple, so it is not solvable-by-finite, and it is locally finite, so it does not have a nontrivial free subgroup. Indeed, the locally finite condition is the only real difference here, since the modular version of the Tits' alternative is given by

Theorem 1.4. *Let F be a field of characteristic $p > 0$ and let G be a subgroup of $\mathrm{GL}_n(F)$. Then G is either solvable-by-(locally finite) or it has a non-abelian free subgroup.*

The proof of these results is difficult and uses a good deal of algebraic geometry. But someplace in the middle of the argument is a proposition that depends upon the ping-pong lemma, and we describe it below.

Let F be a field with a real-valued absolute value or norm $|\ |$. Then this norm determines a metric on F and we assume that F is locally compact in the associated topology. In particular, F is complete. If the absolute value is Archimedean, then F is just the field of real numbers or complex numbers with the usual norm. On the other hand, if $|\ |$ is non-Archimedean, then F has a valuation subring R with unique maximal ideal M, and local compactness is equivalent to R/M being finite. For simplicity, one can just think of F as being the field of complex numbers, but we will state the results in full generality.

Suppose V is a finite dimensional F-vector space and let S be a nonsingular, diagonalizable linear operator on V. Then V is a direct sum of the eigenspaces of S, and we say that $V = X_+ \oplus X_0 \oplus X_-$ is an "S-decomposition" of V if there exist real numbers $s > t > 0$ with $X_+ \neq 0$ spanned by the eigenspaces of S corresponding to the eigenvalues of absolute value $\geq s$, $X_- \neq 0$ spanned by the eigenspaces of S corresponding to the eigenvalues of absolute value $\leq t$, and with X_0 the span of the remaining eigenspaces.

If m is a sufficiently large positive integer, then the eigenvalues of S^m in X_+ will surely dominate those in $X_0 \oplus X_-$. Hence X_+ will be an "attractor" for S^m. By this we mean that image vectors $S^m(v)$ will tend to have large components in X_+ and hence be close to X_+. Of course, this is not quite true. First, we must start with vectors having nonzero components in X_+ or equivalently, we must avoid vectors in $X_0 \oplus X_-$. This explains the assumptions in the following theorem that the eight intersections are trivial. Secondly, the component of $S^m(v)$ in $X_0 \oplus X_-$ may turn out be large just because we started with a vector v having a large component there. Thus, we need to work in projective space P, or perhaps in the unit sphere of V, to control the total size of all components. With this, we have

Theorem 1.5. *Let V be a finite-dimensional F-vector space and let $S, T\colon V \to V$ be two nonsingular operators on V. Suppose S and T are both diagonalizable and that $V = X_+ \oplus X_0 \oplus X_-$ and $V = Y_+ \oplus Y_0 \oplus Y_-$ are the S- and T-decompositions of V, respectively. If the eight intersections $X_\pm \cap (Y_0 \oplus Y_\pm)$ and $Y_\pm \cap (X_0 \oplus X_\pm)$ are trivial, then for all sufficiently large positive integers m, n, we have $\langle S^m, T^n\rangle = \langle S^m\rangle * \langle T^n\rangle$.*

It is easy to see that the triviality of the eight intersections above implies that the dimensions of X_+, X_-, Y_+ and Y_- are all equal. In the original proposition of [**T**], all these dimensions were assumed to be 1. The more general formulation was proved in [**GP**] and is also based on the ping-pong lemma. Specifically, one shows that for suitably large integers m, n, one can find subsets P_1 and P_2 of V with $\langle S^m\rangle^\# P_1 \subseteq P_2$ and $\langle T^n\rangle^\# P_2 \subseteq P_1$. Indeed, there exist neighborhoods of $\overline{X}_+$, $\overline{X}_-$, $\overline{Y}_+$ and $\overline{Y}_-$, the images of these subspaces in P, with $P_1 = \mathfrak{N}(\overline{Y}_+) \cup \mathfrak{N}(\overline{Y}_-)$ and $P_2 = \mathfrak{N}(\overline{X}_+) \cup \mathfrak{N}(\overline{X}_-)$.

Of course, the operators in Sanov's theorem are not diagonalizable. Rather, they are "generalized transvections". Specifically, they are of the form $S = 1 + a\sigma$, where $a \in F$ and $\sigma^2 = 0$. Observe that if $a \in F$ has sufficiently large absolute value, then the image of σ, $\sigma(V) = \operatorname{im}\sigma$, will be an attractor for S provided that we avoid vectors in $\ker\sigma$, the kernel of σ. Thus, we should be able to apply the ping-pong lemma to operators of this sort. However, since $S^m = 1 + ma\sigma$, we also require an assumption on the absolute value to guarantee that if $|a|$ is large, then so is $|ma|$ for all nonzero integers m. This explains the hypothesis below that $|1\mathbb{Z} \setminus 0| \geq 1$, and essentially means that we cannot allow p-adic norms. Furthermore, the assumption that $\operatorname{char} F \neq 2$ eliminates the possibility that S and T both have order 2.

Theorem 1.6. *Let F be a locally compact field, let V be a finite-dimensional F-vector space, and let $S, T\colon V \to V$ be linear operators. Specifically, suppose that $S = 1 + a\sigma$ and $T = 1 + b\tau$ are both generalized transvections, so that $\sigma, \tau\colon V \to V$ are nonzero operators of square 0. Assume that $|1\mathbb{Z} \setminus 0| \geq 1$, $\operatorname{char} F \neq 2$, and write $I = \sigma(V) = \operatorname{im}\sigma$, $K = \ker\sigma$, $J = \tau(V) = \operatorname{im}\tau$, and $L = \ker\tau$. If the intersections $I \cap L$ and $J \cap K$ are both trivial, then for all $a, b \in F$ with $|a|$ and $|b|$ sufficiently large, we have $\langle S, T\rangle = \langle S\rangle * \langle T\rangle$.*

As is to be expected, we also have the mixed case.

Theorem 1.7. *Let V be a finite-dimensional F-vector space and let $S, T\colon V \to V$ be two nonsingular operators. Suppose S is diagonalizable with S-decomposition of V given by $V = X_+ \oplus X_0 \oplus X_-$. Furthermore, suppose $T = 1 + a\tau$ is a generalized transvection, where $\tau\colon V \to V$ is a nonzero operator of square 0 with $I = \tau(V) = \operatorname{im}\tau$ and $K = \ker\tau$. Assume also that $|1\mathbb{Z} \setminus 0| \geq 1$. If the four intersections $X_\pm \cap K$ and $I \cap (X_0 \oplus X_\pm)$ are trivial, then for all sufficiently large integers n and all $a \in F$ of sufficiently large absolute value, we have $\langle S^n, T\rangle = \langle S^n\rangle * \langle T\rangle$.*

Finally, there are results to guarantee that $\langle G, T\rangle = G * \langle T\rangle$ when G is a finite subgroup of $\mathrm{GL}(V)$ and T is a suitable linear operator on V. The first, essentially proved in [**P**], considers the case of generalized transvections.

Theorem 1.8. *Let F be a locally compact field, let V be a finite-dimensional F-vector space, and let G be a nonidentity finite subgroup of the general linear group $\mathrm{GL}(V)$. Assume that $|G| \geq 3$ when $\operatorname{char} F = 2$. Furthermore, let $\tau\colon V \to V$ be a nonzero linear transformation of square 0, and write $K = \ker\tau$ and $I = \operatorname{im}\tau =$*

$\tau(V)$. If $gI \cap K = 0$ for all $g \in G^{\#}$ and if $|1\mathbb{Z} \setminus 0| \geq 1$, then for all $a \in F$ of sufficiently large absolute value, we have $\langle G, T\rangle \cong G * \langle T\rangle$ where $T = 1 + a\tau$.

The second, proved in [**GP**], is the analogous result for diagonalizable operators.

Theorem 1.9. *Let F be a locally compact field, let V be a finite-dimensional F-vector space, and let $G \neq 1$ be a finite subgroup of $\mathrm{GL}(V)$. Furthermore, suppose $T\colon V \to V$ is a nonsingular, diagonalizable linear transformation and let $V = X_+ \oplus X_0 \oplus X_-$ be a T-decomposition of V. Assume that, for all $g \in G^{\#}$, gX_+ and gX_- are disjoint from both $X_0 \oplus X_-$ and $X_+ \oplus X_0$. Then, for all sufficiently large integers n, $\langle G, T^n\rangle \cong G * \langle T^n\rangle$.*

2. Bass Cyclic Units

The previous theorems on free products in linear groups can be applied to yield analogous results in integral group rings. The difficult part of these applications is the verification of the four or eight conditions on the triviality of certain subspace intersections. In the remainder of this paper, we consider several applications to the study of Bass cyclic units. As will be apparent, the existence of these units is based on the well-known observation that if $\varepsilon \neq 1$ is a complex dth root of unity and if the integer $k \geq 1$ is prime to d, then $(\varepsilon^k - 1)/(\varepsilon - 1) = 1 + \varepsilon + \cdots + \varepsilon^{k-1}$ is a unit in $\mathbb{Z}[\varepsilon]$. Indeed, if $\delta = \varepsilon^k$, then $\varepsilon = \delta^\ell$ for some integer $\ell \geq 1$ and then $(\varepsilon - 1)/(\varepsilon^k - 1) = (\delta^\ell - 1)/(\delta - 1) = 1 + \delta + \cdots + \delta^{\ell-1} \in \mathbb{Z}[\varepsilon]$. We now introduce the necessary notation.

Let G be a group and let x be an elements of G of finite order d. We work in the integral group ring $\mathbb{Z}[X] \subseteq \mathbb{Z}[G]$, where X is the cyclic group generated by x. To start with, let $\hat{x} = \hat{X} = \sum_{i=0}^{d-1} x^i$ denote the sum of the elements of X. As is well known, $x^j\hat{X} = \hat{X}x^j = \hat{X}$ for all integers j. Now define

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

where $1 \leq k$, $\gcd(k,d) = 1$, and where m is a multiple of the Euler function $\varphi(d)$. The latter two conditions imply that $k^m \equiv 1 \bmod d$ and hence $u_{k,m}(x) \in \mathbb{Z}[X]$. Recall that the augmentation map of $\mathbb{Z}[X]$ is the homomorphism $\mathbb{Z}[X] \to \mathbb{Z}$ determined by $x \mapsto 1$. Then each $u_{k,m}(x)$ has augmentation 1, and indeed we can write $u_{k,m}(x) = (1 + x + \cdots + x^{k-1})^m + c\hat{x}$ where c is the unique integer such that this element has the 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 2.1. *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* $k\ell \equiv 1 \bmod d$.

Proof. For parts (i), (ii) and (iii), we use the identities $x^j\hat{x} = \hat{x}x^j = \hat{x}$ and $x^d = 1$ to easily show that the right and left sides of each equation differ by an integer multiple of $\hat{x}$, say $c\hat{x}$. Furthermore, since both sides have augmentation 1, their difference has augmentation 0. But the augmentation of $c\hat{x}$ 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 $r \equiv 1 \bmod d$. Finally, if $k\ell \equiv 1 \bmod d$, then (iii) implies that $u_{k,m}(x)\cdot u_{\ell,m}(x^k) = 1$, as required. □

In view of (iv) above, each $u_{k,m}(x)$ is a unit in $\mathbb{Z}[G]$ and, following [**S2**], 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 we need $d \ge 5$. Finally, it follows from (ii) that $u_{k,m}(x)^a = u_{k,ma}(x)$ for all integers $a \ge 1$.

As we will see, linear group results apply to the integral group ring $\mathbb{Z}[G]$ via the complex representation theory of G. Specifically, $\mathbb{Z}[G]$ is contained in the complex group algebra $\mathbb{C}[G]$, and the irreducible representations of the latter algebra are homomorphisms θ from $\mathbb{C}[G]$ onto suitable full matrix rings $\mathrm{M}_n(\mathbb{C})$. In particular, if u and v are units in $\mathbb{Z}[G]$ and if their images $\theta(u)$ and $\theta(v)$ in $\mathrm{M}_n(\mathbb{C})$ generate a free group of rank 2, then certainly $\langle u, v\rangle$ is also free of rank 2.

Since we wish to study Bass cyclic units, it is necessary to understand the possible images of $u_{k,m}(x)$ in $\mathrm{M}_n(\mathbb{C})$. To start with, since $x \in G$ is an element of order d, its image $\bar{x} = \theta(x)$ satisfies the separable polynomial equation $\zeta^d = 1$ and hence $\bar{x}$ is diagonalizable with eigenvalues that are dth roots of unity. It follows that $\theta(u_{k,m}(x)) = u_{k,m}(\bar{x})$ is also diagonalizable with eigenvalues equal to $u_{k,m}(\varepsilon)$, as ε runs through the eigenvalues of $\bar{x}$. This clearly leads to two questions of interest. First, for which dth roots of unity ε is $|u_{k,m}(\varepsilon)|$ maximal, and for which dth roots of unity ε is $|u_{k,m}(\varepsilon)|$ minimal. Second, if ε_1 and ε_2 are dth roots of unity, when is $|u_{k,m}(\varepsilon_1)| = |u_{k,m}(\varepsilon_2)|$. We consider both of these below.

Note that, if ε is a dth root of unity and if $\varepsilon^a \ne 1$, then

$$(*) \qquad 1 + (\varepsilon^a) + (\varepsilon^a)^2 + \cdots + (\varepsilon^a)^{k-1} = \frac{\varepsilon^{ak} - 1}{\varepsilon^a - 1}.$$

Hence, since $|\varepsilon^{a/2}| = 1$, we have

$$(**) \qquad |1 + (\varepsilon^a) + (\varepsilon^a)^2 + \cdots + (\varepsilon^a)^{k-1}| = \left|\frac{\varepsilon^{ak/2} - \varepsilon^{-ak/2}}{\varepsilon^{a/2} - \varepsilon^{-a/2}}\right|.$$

Lemma 2.2. *Let $\varepsilon = e^{2\pi i/d}$ be a primitive complex dth root of unity and let a be an integer. Assume that $2 \le k \le d-2$ and that* $\gcd(k,d) = 1$.

i. $u_{k,m}(1) = 1$ *and if* $\varepsilon^a \ne 1$ *then*

$$|u_{k,m}(\varepsilon^a)| = \left|\frac{\varepsilon^{ak/2} - \varepsilon^{-ak/2}}{\varepsilon^{a/2} - \varepsilon^{-a/2}}\right|^m = \left|\frac{\sin(k\pi a/d)}{\sin(\pi a/d)}\right|^m.$$

ii. *The largest absolute value $|u_{k,m}(\varepsilon^a)|$ occurs when $a \equiv \pm 1 \bmod d$.*

iii. *The smallest absolute value $|u_{k,m}(\varepsilon^a)|$ occurs when $ak \equiv \pm 1 \bmod d$.*

Proof. (i) Since $\hat{x}$ evaluated at 1 equals d, we have $u_{k,m}(1) = k^m + (1-k^m) = 1$. On the other hand, if $\varepsilon^a \ne 1$, then $\hat{x}$ evaluated at ε^a is 0, so

$$u_{k,m}(\varepsilon^a) = (1 + (\varepsilon^a) + (\varepsilon^a)^2 + \cdots + (\varepsilon^a)^{k-1})^m = \left(\frac{\varepsilon^{ak} - 1}{\varepsilon^a - 1}\right)^m,$$

by equation $(*)$. Hence, $(**)$ yields

$$|u_{k,m}(\varepsilon^a)| = \left|\frac{\varepsilon^{ak/2} - \varepsilon^{-ak/2}}{\varepsilon^{a/2} - \varepsilon^{-a/2}}\right|^m .$$

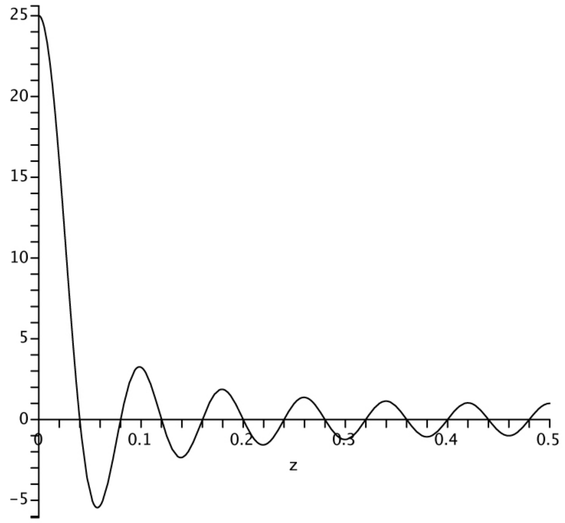
Note that the numerator and denominator here are twice the imaginary parts of $\varepsilon^{ak/2}$ and $\varepsilon^{a/2}$ respectively, so

$$|u_{k,m}(\varepsilon^a)| = \left|\frac{\sin(k\pi a/d)}{\sin(\pi a/d)}\right|^m .$$

(ii) Let us first assume that $\varepsilon^a \neq 1$. Then from the above formula, it is clear that $|u_{k,m}(\varepsilon^a)| = |u_{(d-k),m}(\varepsilon^a)|$. In particular, by replacing k by $d-k$ if necessary, it suffices to assume that $2 \leq k \leq d/2$. Furthermore, since $|u_{k,m}(\varepsilon^a)| = |u_{k,m}(\varepsilon^{-a})|$, it suffices to restrict our attention to the possibilities $a = 1, 2, \ldots, \lfloor d/2 \rfloor$. At this point, we consider the real-valued function

$$f(z) = \frac{\sin k\pi z}{\sin \pi z}$$

and observe that $|u_{k,m}(\varepsilon^a)| = |f(a/d)|^m$ with $m > 0$. Furthermore, each a/d is contained in the closed interval $[r, 1/2]$ with $r = 1/d \leq 1/2k$. A computer plot of the function with $k = 25$ is given below.



As one can see, the function decreases precipitously from $f(0) = k$ to $f(1/k) = 0$ and then stays relatively small throughout the remaining interval $[1/k, 1/2]$. Indeed, using a bit of calculus, one can show that this is a general phenomenon. It then follows that the maximum value of $|f(z)|$ in the interval $[r, 1/2]$ occurs at $r = 1/d$, so $a = 1$, and that this value is > 1. Taking into account the ± symmetry, we see that the maximum value of $|u_{k,m}(\varepsilon^a)|$ with $\varepsilon^a \neq 1$ occurs precisely when $a \equiv \pm 1 \bmod d$. Indeed, since this value is larger than 1 and since $u_{k,m}(1) = 1$, we see that $|u_{k,m}(\varepsilon^{\pm 1})|$ is the maximum value of $|u_{k,m}(\varepsilon^a)|$ over all dth roots of unity.

(iii) The smallest value of $|u_{k,m}(\varepsilon^a)|$ occurs precisely when $|u_{k,m}(\varepsilon^a)^{-1}|$ takes on its largest value. Thus, since $u_{k,m}(x)^{-1} = u_{\ell,m}(x^k)$ with $k\ell \equiv 1 \bmod d$, we see that $|u_{k,m}(\varepsilon^a)|$ is minimal when $|u_{\ell,m}(\varepsilon^{ak})|$ is maximal. Since $2 \le \ell \le d-2$, we conclude from the above that this occurs precisely when $ak \equiv \pm 1 \bmod d$. □

Finally, we discuss the remaining values of $|u_{k,m}(\varepsilon^a)|$, at least when d is a prime power. For this, we first need

Lemma 2.3. *Let p be a prime and set $d = p^n$.*

i. *Suppose $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_r$ and $\delta_1, \delta_2, \ldots, \delta_r$ are complex dth roots of unity that satisfy $\varepsilon_1 + \varepsilon_2 + \cdots + \varepsilon_r = \delta_1 + \delta_2 + \cdots + \delta_r$. If $r \le p-1$ then, by relabeling the δ's if necessary, we have $\varepsilon_i = \delta_i$ for all i.*
ii. *Assume that $p \ge 5$, let ε be a primitive complex dth root of unity, and suppose that $k \not\equiv 0, \pm 1 \bmod p$. If*
$$|1 + (\varepsilon^a) + (\varepsilon^a)^2 + \cdots + (\varepsilon^a)^{k-1}| = |1 + (\varepsilon^b) + (\varepsilon^b)^2 + \cdots + (\varepsilon^b)^{k-1}|,$$
then $a \equiv \pm b \bmod d$.

Proof. (i) Let tr denote the Galois trace in the field of p^nth roots of unity divided by p^{n-1}. Then $\operatorname{tr} 1 = p-1$, $\operatorname{tr}\varepsilon = -1$ if ε is a primitive pth root of unity, and $\operatorname{tr}\varepsilon = 0$ if ε is a primitive p^ath root of unity with $2 \le a \le n$. We first show that some δ_i must equal ε_1. For this, by multiplying through by ε_1^{-1} if necessary, it suffices to assume that $\varepsilon_1 = 1$. Since $r \le p-1$, the trace of the left hand side of the equation is $\ge (p-1) - (p-2) > 0$ and thus there must exist some δ_i with $\operatorname{tr}\delta_i > 0$. In other words, $\delta_i = 1 = \varepsilon_1$, and the result follows by induction on r.

(ii) Since p is odd, each dth root of unity is a square. Thus, to avoid fractional exponents, we replace a by $2a$ and b by $2b$. Suppose first that ε^{2a} and ε^{2b} are not equal to 1. Then, by equation $(**)$ and the fact that $(\varepsilon^{ak} - \varepsilon^{-ak})/(\varepsilon^a - \varepsilon^{-a})$ is real, the equality
$$|1 + (\varepsilon^{2a}) + (\varepsilon^{2a})^2 + \cdots + (\varepsilon^{2a})^{k-1}| = |1 + (\varepsilon^{2b}) + (\varepsilon^{2b})^2 + \cdots + (\varepsilon^{2b})^{k-1}|$$
implies that
$$\frac{\varepsilon^{ak} - \varepsilon^{-ak}}{\varepsilon^a - \varepsilon^{-a}} = \kappa \cdot \frac{\varepsilon^{bk} - \varepsilon^{-bk}}{\varepsilon^b - \varepsilon^{-b}}$$
where $\kappa = \pm 1$.

For convenience, let $\Re(\vartheta) = \vartheta + \bar{\vartheta}$ denote twice the real part of ϑ. Then cross multiplying the above displayed equation yields
$$\Re\big(\varepsilon^{ak+b} - \varepsilon^{ak-b}\big) = \kappa \cdot \Re\big(\varepsilon^{bk+a} - \varepsilon^{bk-a}\big) = \Re\big(\varepsilon^{bk+\kappa a} - \varepsilon^{bk-\kappa a}\big),$$
where the last equality holds because $\kappa = \pm 1$. Thus
$$\Re\big(\varepsilon^{ak+b} + \varepsilon^{bk-\kappa a}\big) = \Re\big(\varepsilon^{bk+\kappa a} + \varepsilon^{ak-b}\big)$$
and note that both sides are sums of four p^nth roots of unity. Since $p \ge 5$, we conclude from part (i) that the right-hand and left-hand exponents must match modulo d. But certainly $ak + b \not\equiv \pm(ak - b) \bmod d$, so we obtain
$$ak + b \equiv \pm(bk + \kappa a) \bmod d$$
$$ak - b \equiv \pm(bk - \kappa a) \bmod d.$$
If the two ± signs above disagree, then adding the equations yields $2ak \equiv \pm 2\kappa a$ and hence, since $k \not\equiv \pm 1 \bmod p$, we have $2a \equiv 0 \bmod d$, a contradiction. Thus the signs must agree and this time adding yields $2ak \equiv \pm 2bk$ so, since $k \not\equiv 0 \bmod p$, we have $2a \equiv \pm 2b \bmod d$, as required.

Finally, if $\varepsilon^{2a} = 1$, then the triangle inequality and $k \geq 2$ imply that $\varepsilon^{2b} = 1$. Hence again $2a \equiv \pm 2b \bmod d$. □

Obviously, part (ii) above can be made more precise by merely listing the possible exponent matchings that can occur.

LEMMA 2.4. *Let $p \geq 5$ be a prime, set $d = p^n$, and let ε be a primitive complex dth root of unity. Assume that $k \not\equiv 0, \pm 1 \bmod p$.*

i. $|u_{k,m}(\varepsilon^a)| = |u_{k,m}(\varepsilon^b)|$ *if and only if* $a \equiv \pm b \bmod d$.
ii. $u_{k,m}(\varepsilon^a) = u_{k,m}(\varepsilon^b)$ *if and only if either* $a \equiv b \bmod d$ *or* $a \equiv -b \bmod d$ *and d divides ma.*

PROOF. (i) Since p is odd, each element of $\langle \varepsilon \rangle$ is a square. Thus, we can again replace a by $2a$ and b by $2b$. Suppose first that ε^{2a} and ε^{2b} are both not 1. Then $\hat{x}$ evaluated at these roots is 0, so

$$u_{k,m}(\varepsilon^{2a}) = (1 + (\varepsilon^{2a}) + (\varepsilon^{2a})^2 + \cdots + (\varepsilon^{2a})^{k-1})^m$$

and similarly for $u_{k,m}(\varepsilon^{2b})$. In particular, if $|u_{k,m}(\varepsilon^{2a})| = |u_{k,m}(\varepsilon^{2b})|$, then

$$|1 + (\varepsilon^{2a}) + (\varepsilon^{2a})^2 + \cdots + (\varepsilon^{2a})^{k-1}| = |1 + (\varepsilon^{2b}) + (\varepsilon^{2b})^2 + \cdots + (\varepsilon^{2b})^{k-1}|,$$

and Lemma 2.3(ii) implies that $2a \equiv \pm 2b \bmod d$.

It remains to show that if one of ε^{2a} or ε^{2b} is equal to 1, then so is the other. To this end, let $\varepsilon^{2b} = 1$, and suppose, by way of contradiction, that $\varepsilon^{2a} \neq 1$. Then $|u_{k,m}(\varepsilon^{2a})| = |u_{k,m}(\varepsilon^{2b})| = 1$, so the above and equation $(**)$ yield

$$\frac{\varepsilon^{ak} - \varepsilon^{-ak}}{\varepsilon^{a} - \varepsilon^{-a}} = \kappa = \pm 1.$$

Thus, as in the proof of Lemma 2.3,

$$\varepsilon^{ak} - \varepsilon^{-ak} = \kappa(\varepsilon^{a} - \varepsilon^{-a}) = \varepsilon^{\kappa a} - \varepsilon^{-\kappa a}.$$

In particular, we have $\varepsilon^{ak} + \varepsilon^{-\kappa a} = \varepsilon^{-ak} + \varepsilon^{\kappa a}$ and this contradicts the preceding lemma since $ak \not\equiv -ak \bmod d$ and $ak \not\equiv \kappa a \bmod d$.

(ii) If $u_{k,m}(\varepsilon^a) = u_{k,m}(\varepsilon^b)$, then these two complex numbers have the same absolute value. Thus, part (i) implies that $b \equiv \pm a \bmod d$, and we need only consider the possibility that $b \equiv -a \bmod d$ with $a \not\equiv 0$. In this situation, equation $(*)$ yields

$$u_{k,m}(\varepsilon^a) = \left(\frac{\varepsilon^{ak} - 1}{\varepsilon^{a} - 1}\right)^m = \left(\frac{\varepsilon^{ak}}{\varepsilon^{a}}\right)^m \left(\frac{\varepsilon^{-ak} - 1}{\varepsilon^{-a} - 1}\right)^m = \varepsilon^{(k-1)am} u_{k,m}(\varepsilon^b).$$

Thus $u_{k,m}(\varepsilon^a) = u_{k,m}(\varepsilon^b)$ if and only if $\varepsilon^{(k-1)am} = 1$. Indeed, since $k-1$ is prime to d, this occurs if and only if d divides am. □

Note that $p^{n-1}(p-1) = \varphi(p^n)$ divides m, by assumption. Thus we need only one additional factor of p in m to guarantee that all $u_{k,m}(\varepsilon^a)$ are real.

3. The Idempotent Conditions

As we indicated at the beginning, the goal of this talk is to discuss the work of [**GP**]. So far, we have restricted our attention to describing some of the machinery developed in that paper. Now we are ready to show how that machinery can be used to prove the main result of [**GP**], namely

Theorem 3.1. *If G is a finite nonabelian group of order prime to 6, then there exist two elements $x, y \in G$ of prime power order and two Bass cyclic units $u_{k,m}(x)$ and $u_{r,s}(y)$ such that $\langle u_{k,m}(x), u_{r,s}(y)\rangle$ is a nonabelian free subgroup of the unit group of the integral group ring $\mathbb{Z}[G]$.*

Note that some assumption on the primes dividing $|G|$ is required in the above because, as we have observed, there are no nontrivial Bass cyclic units based on group elements of order 2 or 3. For example, suppose $G = A \rtimes X$, where X is cyclic of order $p = 2$ or 3 and where X acts in a fixed-point-free manner on the normal abelian subgroup A. Then G is a Frobenius group, so all elements of $G \setminus A$ have order $p = 2$ or 3. Thus the only Bass cyclic units of the integral group ring $\mathbb{Z}[G]$ come from elements of A and these all commute. In particular, we cannot find two Bass cyclic units that generate a nonabelian free group.

As is to be expected, the proof of Theorem 3.1 proceeds by induction on $|G|$, and hence we can clearly assume that all proper subgroups of G are abelian. Furthermore, if $\overline{G}$ is a proper homomorphic image of G that is nonabelian, then by induction, there exist elements $\bar{x}, \bar{y} \in \overline{G}$ of prime power order such that $u_{k,m}(\bar{x})$ and $u_{r,s}(\bar{y})$ generate a nonabelian free group. It is then fairly easy to see that there exist elements $x, y \in G$ of prime power order and suitable integers m' and s' such that $u_{k,m'}(x)$ and $u_{r,s'}(y)$ map to powers of $u_{k,m}(\bar{x})$ and $u_{r,s}(\bar{y})$, respectively, under the natural homomorphism $\mathbb{Z}[G] \to \mathbb{Z}[\overline{G}]$. Thus $\langle u_{k,m'}(x), u_{r,s'}(y)\rangle$ is clearly a free subgroup of the unit group of $\mathbb{Z}[G]$. This allows us to also assume that all proper homomorphic images of G are abelian, and hence that G is a "minimal nonabelian group". But these groups have been classified. Indeed, it follows from [**MM**] that G is the semi-direct product $G = A \rtimes X$, where $X = \langle x\rangle$ is cyclic of prime order p. Furthermore, either A is a cyclic p-group, or A is abelian of type (p, p), or A is an elementary abelian q-group for some prime $q \neq p$. In the latter situation, X acts faithfully and irreducibly on A.

The representation theory of such groups G is fairly easy to understand and hence it affords an effective mechanism for completing the proof. To this end, we note that if G is as above and if the irreducible representation $\theta\colon \mathbb{C}[G] \to \mathrm{M}_n(\mathbb{C})$ has degree $n > 1$, then $n = p$ and θ is determined by a "linear character", or group homomorphism, $\mu\colon A \to \mathbb{C}^\bullet$. Specifically, $\theta = \mu^G$ is the "induced representation" given by

$$\theta(a) = \mathrm{diag}(\mu(a), \mu^x(a), \ldots, \mu^{x^{p-1}}(a))$$

for all $a \in A$, where these diagonal entries satisfy $\mu^{x^i}(a) = \mu(x^i a x^{-i})$. Furthermore, $\theta(x)$ is the permutation matrix

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

We can then use $\theta = \mu^G$, along with Theorem 1.5, to find suitable integers k, m, r, s and a suitable element $a \in A$, so that the Bass cyclic units $u_{k,m}(x)$ and $u_{r,s}(a^{-1}xa)$, or $u_{k,m}(x)$ and $u_{r,s}(a)$, generate a free group of rank 2 in the unit group of $\mathbb{Z}[G]$. The work is reasonably concrete, but tedious and by no means obvious. It is especially difficult when $G = A \rtimes X$ is a Frobenius group, and thus we will not proceed further with this proof. Instead, we will discuss a similar, but somewhat easier, situation.

Now, in order to apply Theorem 1.5, it is necessary to verify that the eight intersections $X_\pm \cap (Y_0 \oplus Y_\pm)$ and $Y_\pm \cap (X_0 \oplus X_\pm)$ are all trivial. We do this by studying the idempotents that correspond to the S- and T-decompositions of V. For simplicity, if $V = X_+ \oplus X_0 \oplus X_-$ is an S-decomposition of V, we say that the projections $e_+ \colon V \to X_+$ and $e_- \colon V \to X_-$ are the S-idempotents in $\mathrm{GL}(V)$.

Lemma 3.2. *Let V be a finite-dimensional F-vector space and let $S, T \colon V \to V$ be two nonsingular operators on V. Suppose S and T are both diagonalizable and that $V = X_+ \oplus X_0 \oplus X_-$ and $V = Y_+ \oplus Y_0 \oplus Y_-$ are S- and T-decompositions of V, respectively, with $r = \dim X_\pm = \dim Y_\pm$. Furthermore, let e_+, e_- and f_+, f_- be the corresponding S- and T-idempotents, respectively. Then the eight intersections $X_\pm \cap (Y_0 \oplus Y_\pm)$ and $Y_\pm \cap (X_0 \oplus X_\pm)$ are trivial, if and only if the eight products $e_\pm f_\pm$ and $f_\pm e_\pm$ all have rank r.*

Proof. We consider the intersection $X_+ \cap (Y_0 \oplus Y_-)$. Since $\ker f_+ = Y_0 \oplus Y_-$, we see that $X_+ \cap (Y_0 \oplus Y_-) = 0$ if and only if the restricted linear transformation $f_+ \colon X_+ \to Y_+$ is one-to-one. But $\dim X_+ = \dim Y_+$, so the map is one-to-one if and only if it is onto. Since $X_+ = e_+V$, the image of $f_+ \colon X_+ \to Y_+$ is $f_+X_+ = f_+e_+V \subseteq Y_+$, and hence the map is onto if and only if $\operatorname{rank} f_+e_+ = \dim Y_+ = r$. □

We call the eight rank formulas, namely $\operatorname{rank} e_\pm f_\pm = r$ and $\operatorname{rank} f_\pm e_\pm = r$, the "idempotent conditions". Obviously, there are analogous idempotent conditions for Theorems 1.6 and 1.7. Since $\operatorname{rank} e_\pm = \operatorname{rank} f_\pm = r$, the conditions for Theorem 1.5 are equivalent to showing that the eight products $e_\pm f_\pm$ and $f_\pm e_\pm$ all have rank at least r. In particular, when $r = 1$, this reduces to showing that $e_\pm f_\pm \neq 0$ and $f_\pm e_\pm \neq 0$. On the other hand, when dealing with Bass cyclic units, we usually have $r = 2$ or larger, and then the rank computations become much more difficult. Fortunately, there is a trick that is sometimes helpful in dealing with the $r = 2$ situation. Indeed, we will use it to prove Theorem 3.4 below.

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 $\overline{vc} = \overline{v}\,\bar{c}$ 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 $\bar{t}\,\overline{v} = \overline{tv}$. Then $\bar{t}$ is also a $\mathbb{C}$-linear transformation and $^-$ defines an automorphism of $\mathrm{End}_{\mathbb{C}}(V)$ of order 2 with $\overline{tc} = \bar{t}\,\bar{c}$.

Lemma 3.3. *Suppose $V = V' \otimes_{\mathbb{R}} \mathbb{C}$ is as above. Let $e, \bar{e}$ be orthogonal idempotent linear transformations on V and let $f, \overline{f}$ also be orthogonal idempotent linear transformations on V. Assume that the transformation $t = (e + \bar{e})(f + \overline{f})$ has rank ≤ 1. Then for every $v \in V$, there exists some $c \in \mathbb{C}$ with $|c| = 1$ such that $e\overline{f}\overline{v} = efvc$.*

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 $(e + \bar{e})\overline{f}\overline{v} = t(\overline{f}\overline{v}) \in L$. Furthermore, the definition of $^-$ on $\mathrm{End}_{\mathbb{C}}(V)$ implies that if $w = t(fv)$, then $\overline{w} = \bar{t}(\overline{f}\overline{v}) = t(\overline{f}\overline{v})$. 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 $(e+\bar{e})\overline{f}\bar{v} = (e+\bar{e})fvc$, and multiplying on the left by e yields the result. $\square$

As an application, we consider certain Bass cyclic units $u_{s,m}(x)$ in the integral group ring of the symmetric group $G = \mathrm{Sym}_n$. As will be apparent, the first parameter s plays an almost nonexistent role in these examples. This differs significantly from the proof of Theorem 3.1, where a delicate choice of parameter is required. Recall that the action of G on $\{1, 2, \dots, n\}$ gives rise to a real permutation module V' with natural $\mathbb{R}$-basis denoted by $\{[1], [2], \dots, [n]\}$. The latter set is then also a $\mathbb{C}$-basis for $V = V' \otimes_{\mathbb{R}} \mathbb{C}$, and these basis vectors are fixed by complex conjugation.

Now suppose $x = (x_1\, x_2\, \dots\, x_d)$ is a d-cycle in G. Then x acts on V by cyclically permuting the basis vectors $\{[x_1], [x_2], \dots, [x_d]\}$ 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. 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 σ is a nonidentity dth root of unity, then V_σ, the σ-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 $e_\sigma = (1/d)\sum_{i=0}^{d-1} x^i \sigma^{-i}$ as σ runs through the dth roots of unity. Since $xe_\sigma = \sigma e_\sigma$, it follows that the σ-eigenspace of x in V is given by $e_\sigma V = V_\sigma$. Thus each e_σ, with $\sigma \neq 1$, has rank 1 in its action on V, while e_1 has rank $(n-d)+1$. With all of this, we can now prove

Theorem 3.4. *Let $p \geq 5$ be a prime and let $d = p^w$ be a power of p. Suppose x and y are two d-cycles in $G = \mathrm{Sym}_n$ of the form*

$$x = (1\, 2\, \dots\, k\, x_{k+1}\, x_{k+2}\, \dots\, x_d) \quad \text{and} \quad y = (1\, 2\, \dots\, k\, y_{k+1}\, y_{k+2}\, \dots\, y_d),$$

where $\{x_{k+1}, x_{k+2}, \dots, x_d\}$ and $\{y_{k+1}, y_{k+2}, \dots, y_d\}$ are disjoint subsets of the set $\{k+1, k+2, \dots, n\}$ of remaining numbers, and where $k \not\equiv 0, \pm 1 \bmod p$. Then, for all parameters s and s', there exist m and m', so that the Bass cyclic units $u_{s,m}(x)$ and $u_{s',m'}(y)$ 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 $\{[1], [2]. \dots, [n]\}$ 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 σ occurring once on the diagonal and with the remaining $(n-d)+1$ diagonal entries equal to 1. Furthermore, the projection of V onto the σ-eigenspace

V_σ is precisely the idempotent $e_\sigma = (1/d)\sum_{i=0}^{d-1} x^i\sigma^{-i}$. In particular, each e_σ, with $\sigma \neq 1$, has rank 1 and, since $x = \bar{x}$, it follows that $\bar{e}_\sigma = e_{\bar{\sigma}}$.

Set $q = \varphi(d)$. If s is any acceptable parameter, that is if $2 \leq s \leq d-2$, then $S = u_{s,q}(x) \in \mathrm{GL}(V)$, and clearly when x is diagonal, then so is S. Indeed, the eigenvalues of S are precisely the numbers $u_{s,q}(\sigma)$ as σ 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 $u_{s,q}(\sigma)$ is the direct sum of all V_τ with $u_{s,q}(\sigma) = u_{s,q}(\tau)$.

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 Lemma 2.2 and the above, that $X_+ = V_{\sigma_+} \oplus V_{\bar{\sigma}_+}$ for a suitable dth root of unity $\sigma_+ \neq 1$, and hence $\dim X_+ = 2$. In particular, the projection map $e_+\colon V \to X_+$ is given by $e_+ = e_{\sigma_+} + e_{\bar{\sigma}_+} = e_{\sigma_+} + \bar{e}_{\sigma_+}$. Similarly, $\dim X_- = 2$, $X_- = V_{\sigma_-} \oplus V_{\bar{\sigma}_-}$ for a suitable dth root of unity $\sigma_- \neq 1$, and $e_- = e_{\sigma_-} + e_{\bar{\sigma}_-} = e_{\sigma_-} + \bar{e}_{\sigma_-}$.

Obviously, the above properties of x apply equally well to y, but of course with a change of notation. Thus, for a suitable integer s', we let $T = u_{s',q}(y) \in \mathrm{GL}(V)$, 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 τ, we set $f_\tau = (1/d)\sum_{i=0}^{d-1} y^i\tau^{-i}$. Then it follows, as for the element x, that $\dim Y_+ = \dim Y_- = 2$ and that $f_+ = f_{\tau_+} + \bar{f}_{\tau_+}$ and $f_- = f_{\tau_-} + \bar{f}_{\tau_-}$ for suitable nonidentity dth roots of unity τ_+ and τ_-.

We now use Theorem 1.5 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, $\operatorname{rank} e_\pm f_\pm = 2$ and $\operatorname{rank} f_\pm e_\pm = 2$, are satisfied and, by symmetry, we need only consider the products $e_\pm f_\pm$. Furthermore, in view of our previous observations, it suffices to show that if σ and τ are any nonidentity complex dth roots of unity, then $t = (e_\sigma + \bar{e}_\sigma)(f_\tau + \bar{f}_\tau)$ has rank ≥ 2. Suppose, by way of contradiction, that $\operatorname{rank} t \leq 1$. Then, by Lemma 3.3 and the fact that the vector $[1]$ is fixed under $^-$, there exists a complex number c of absolute value 1 with $e_\sigma\bar{f}_\tau[1] = e_\sigma f_\tau[1]c$. In particular, if we write

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

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

Now if $0 \leq i \leq k-1$, then the cycle structure of the permutations x and y imply that $x^i[1] = y^i[1] = [i+1]$. Hence, it follows easily from the disjointness of the remaining entries that

$$a_1 = \sum_{i=0}^{k-1}(\sigma\tau)^i \quad \text{and} \quad b_1 = \sum_{i=0}^{k-1}(\sigma\tau^{-1})^i.$$

But we are given $k \not\equiv 0, \pm 1 \bmod p$, so Lemma 2.3(ii) and the equality $|a_1| = |b_1|$ imply that $\sigma\tau = \sigma\tau^{-1}$ or $\sigma\tau = (\sigma\tau^{-1})^{-1} = \sigma^{-1}\tau$. This is, of course, a contradiction since $\sigma^2 \neq 1$ and $\tau^2 \neq 1$. Thus the idempotent conditions are satisfied and we conclude from Theorem 1.5 that, for suitable 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 $|u_{s,q}(\sigma_+)|$ and $|u_{s',q}(\tau_+)|$ are both larger than 1, and therefore both S and T have infinite multiplicative order.

Finally, Lemma 2.1(ii) implies that $\big(u_{s,q}(x)\big)^z = u_{s,m}(x)$ and $\big(u_{s',q}(y)\big)^{z'} = u_{s',m'}(y)$, where $m = qz$ and $m' = qz'$. Thus, the Bass cyclic units $u_{s,m}(x)$ and $u_{s',m'}(y)$ 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 $\langle u_{s,m}(x), u_{s',m'}(y)\rangle$ is also a nonabelian free group, and the theorem is proved. □

Obviously, these techniques can be used to obtain many additional concrete examples of a similar nature. However, we will not pursue this now, but rather leave it for possible later considerations.

References

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

[H] P. de la Harpe, *Topics in Geometric Group Theory*, Chicago Lectures in Mathematics, Univ. of Chicago Press, Chicago, 2000.

[HP] B. Hartley and P. F. Pickel, *Free subgroups in the unit groups of integral group rings*, Canad. J. Math. **32** (1980), 1342–1352.

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

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

[P] D. S. Passman, *Free products in linear groups*, Proc. AMS **132** (2004), 37–46.

[S1] S. K. Sehgal, *Topics in group rings*, Dekker, New York, 1978.

[S2] S. K. Sehgal, *Units in Integral Group Rings*, Longman Scientific, Harlow, 1993.

[T] J. Tits, *Free subgroups in linear groups*, J. Algebra **20** (1972), 250–270.

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