LINEAR GROUPS AND GROUP RINGS

J. Z. GONÇALVES AND D. S. PASSMAN

Abstract. This paper consists of two parts. The first is concerned with free products in linear groups and uses the usual "ping pong" lemma and attractors to prove the results. What is new here is that we allow certain subspaces of V associated with the semisimple and generalized transvection operators to have dimensions larger than 1. The second part is concerned with applications of this machinery to integral groups rings $\mathbb{Z}[G]$ of finite groups. We show, for example, that if G is nonabelian of order prime to 6, then $\mathbb{Z}[G]$ contains two Bass cyclic units that generate a nonabelian free group.

1. Linear operators and attractors

Let F be a field and let $|\ |\colon F \to \mathbb{R}^+ = \{r \in \mathbb{R}\colon r \geq 0\}$ be an absolute value defined on F. Here $\mathbb{R}$ is the field of real numbers and, by definition, we have

$$|ab| = |a|\cdot|b|$$
$$|a+b| \leq |a| + |b|$$
$$|a| = 0 \iff a = 0$$

for all $a, b \in F$. In particular, $|1| = 1 = |-1|$. Indeed, $|a| = 1$ if a is any root of unity in F. See [J, Chapter 9] or [B, Chapter VI] for additional basic properties.

If we define $\delta\colon F \times F \to \mathbb{R}^+$ by $\delta(a,b) = |a-b|$, then F clearly becomes a metric space using δ as a metric. We assume throughout that F is locally compact in this topology, so that each $a \in F$ has a neighborhood with compact closure. As a consequence of the product formula $|ab| = |a|\cdot|b|$, it follows that every closed, bounded subset of F is compact. Furthermore, $|\ |\colon F \to \mathbb{R}^+$ is a continuous function and F is complete, in that every Cauchy sequence has a limit.

If $|\ |$ is archimedean, then Ostrowski's Theorem [J, page 552] implies that $F = \mathbb{R}$ or $\mathbb{C}$, the field of complex numbers, and that $|\ |$ is the ordinary absolute value defined on $\mathbb{C}$. In particular, $|\ |$ is the identity function on $|F| = \mathbb{R}^+ \subseteq F$, where $|F|$ is the set of absolute values taken on by elements of F. Thus, if $0 \neq a \in F$, then $a/|a|$ is an element of F having absolute value 1.

On the other hand, if $|\ |$ is non-archimedean, then we know that

$$|a+b| \leq \max\{|a|, |b|\}$$

for all $a, b \in F$. Indeed, if $|a| \neq |b|$, then $|a+b| = \max\{|a|, |b|\}$. In this situation, $\mathfrak{O} = \{a \in F\colon |a| \leq 1\}$ is a subring of F, the valuation ring associated with $|\ |$, and $\mathfrak{O}$ has the unique maximal ideal $\mathfrak{m} = \{a \in F\colon |a| < 1\}$. Since F is locally compact, $\mathfrak{O}$ is compact and hence the residue class field $\mathfrak{O}/\mathfrak{m}$ is finite, since the

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

The first author's reasearch was supported in part by CNPq grant 303.756/82-5 and Fapesp-Brazil, Proj. Tematico 00/07.291-0. The second author's research was supported in part by NSA grant 144-LQ65.

cosets of $\mathfrak{m}$ yield an open cover of $\mathfrak{O}$. Furthermore, for any real number $0 < r < 1$, $\mathfrak{m}_r = \{a \in F \colon |a| < r\}$ is an open ideal of $\mathfrak{O}$ and we see again that $\mathfrak{O}/\mathfrak{m}_r$ is finite. It follows that there are only finitely many different values for $|F|$ between r and 1. In particular, $|F|$ takes on a unique largest value < 1, and with this, we see that the valuation is discrete.

Conversely, if the residue class field is finite and if $|\ |$ is a complete discrete valuation, then [B, Proposition VI.5.2] implies that F is locally compact. Furthermore, by [B, Theorem VI.9.1], this occurs if and only if F is either a finite algebraic extension of a p-adic field or the field of formal Laurent series over a finite field.

Now let $V = F^n$ be the vector space of n-tuples of F. If $v = (a_1, a_2, \ldots, a_n) \in V$, we define the norm of v by

$$\|v\| = \max\{|a_i| \colon i = 1, 2, \ldots, n\}.$$

Then, it is easy to see that

$$\begin{aligned} \|av\| &= |a| \cdot \|v\| \\ \|v + w\| &\leq \|v\| + \|w\| \\ \|v\| = 0 &\iff v = 0 \end{aligned}$$

for all $a \in F$ and $v, w \in V$. Thus, V becomes a metric space using the metric $\delta(v, w) = \|v - w\|$ and, since F is locally compact, so is V. Again, as a consequence of the product formula $\|av\| = |a| \cdot \|v\|$, it follows that every closed, bounded subset of V is compact. In particular, the unit sphere in V given by $\mathbf{S} = \{v \in V \colon \|v\| = 1\}$ is compact since $\|\ \| \colon V \to \mathbb{R}^+$ is continuous. Note that $\|V\| = |F|$ so that for each $0 \neq v \in V$ there exists $a \in F$ with $\|v\| = |a|$. In particular, v/a has norm 1 and hence $Fv \cap \mathbf{S} \neq \emptyset$.

We say that $X \subseteq V$ is a projective subset of V if X contains a nonzero vector and if it is closed under multiplication by $F^\bullet = F \setminus 0$, that is $F^\bullet X \subseteq X$. Thus, except for the possible presence or absence of the zero vector, these projective subsets correspond in a one-to-one manner to the nonempty subsets of $\mathcal{P}(V)$, the projective space of V. Because of this, we say that projective subsets X and Y are disjoint if $X \cap Y \subseteq \{0\}$. Furthermore, we define the distance between them by

$$d(X, Y) = \inf\{\|x - y\| \colon x \in X \cap \mathbf{S},\ y \in Y \cap \mathbf{S}\}.$$

If $0 \neq v, w \in V$, we set

$$d(v, w) = d(Fv, Fw) = \inf\{\|av - bw\| \colon a, b \in F,\ \|av\| = 1 = \|bw\|\}.$$

As we observed, field elements a and b do indeed exist with $\|av\| = 1 = \|bw\|$. Finally, we define

$$d(Y, v) = d(v, Y) = d(Fv, Y) = \inf\{d(v, y) \colon y \in Y\}.$$

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

i. If X and Y are nonzero subspaces of V, then there exist $x_0 \in X \cap \mathbf{S}$ and $y_0 \in Y \cap \mathbf{S}$ with $d(X, Y) = \|x_0 - y_0\|$. In particular, if X and Y are disjoint, then $d(X, Y) > 0$.

ii. The distance function d defines a metric on the projective space $\mathcal{P}(V)$. With respect to this metric, $\mathcal{P}(V)$ has diameter ≤ 2. It has diameter ≤ 1 if $|\ |$ is a non-archimedean absolute value.

iii. If $0 \neq v, w \in V$, then $d(v, w) \leq 2 \cdot \|v - w\|/\|v\|$. If $|\ |$ is non-archimedean, then $d(v, w) \leq \|v - w\|/\|v\|$.

Proof. (i) This is clear since $X \cap \mathbf{S}$ and $Y \cap \mathbf{S}$ are compact, and since the map $(X \cap \mathbf{S}) \times (Y \cap \mathbf{S}) \to \mathbb{R}^+$ given by $(x, y) \mapsto \|x - y\|$ is continuous.

(ii) Let u, v, w be nonzero vectors in V. By (i), there exist $a, b, b', c' \in F$ such that $\|au\| = \|bv\| = \|b'v\| = \|c'w\| = 1$, $d(u, v) = \|au - bv\|$ and $d(v, w) = \|b'v - c'w\|$. Then $|b| = |b'|$ and therefore $(b/b')(b'v - c'w)$ has the same norm as $b'v - c'w$. In other words, if we set $c = (b/b')c' \in F$, then $\|cw\| = 1$, $d(v, w) = \|bv - cw\|$ and

$$d(u, v) + d(v, w) = \|au - bv\| + \|bv - cw\| \geq \|au - cw\| \geq d(u, w).$$

Furthermore, if u and v correspond to distinct points in $\mathcal{P}(V)$, then $Fu \neq Fv$ and hence $Fu \cap Fv = 0$. It now follows from (i) that $d(u, v) > 0$. Finally, for any $0 \neq u, v \in V$, we have, as above, $d(u, v) = \|au - bv\| \leq \|au\| + \|bv\| = 2$ so $\mathcal{P}(V)$ has diameter at most 2. In the non-archimedean case, $d(u, v) = \|au - bv\| \leq \max\{\|au\|, \|bv\|\} = 1$.

(iii) We first assume that $|\ |$ is archimedean. Then $|F| \subseteq F$, so that $v/\|v\|$ and $w/\|w\|$ both have norm 1. Now note that

$$u = \frac{v}{\|v\|} - \frac{w}{\|w\|} = \frac{v - w}{\|v\|} - \frac{w}{\|w\|} \cdot \frac{\|v\| - \|w\|}{\|v\|} = u' - u''.$$

Since $\|u'\| = \|v - w\|/\|v\|$ and $\|u''\| = \big|\|v\| - \|w\|\big|/\|v\| \leq \|v - w\|/\|v\|$, it follows that

$$d(v, w) \leq \|u\| \leq \|u'\| + \|u''\| \leq \frac{2 \cdot \|v - w\|}{\|v\|},$$

as required. Finally, suppose that $|\ |$ is non-archimedean. If $\|v\| \neq \|w\|$, then (ii) yields

$$d(v, w) \leq 1 \leq \max\{\|v\|, \|w\|\}/\|v\| = \|v - w\|/\|v\|.$$

On the other hand, if $\|v\| = \|w\|$, choose $a \in F$ with $|a|$ equal to this common norm. Then

$$d(v, w) \leq \|v/a - w/a\| = \|v - w\|/|a| = \|v - w\|/\|v\|$$

and the lemma is proved. □

It is clear from the above that if X and Z are projective subsets of V and if $0 \neq y \in V$, then

$$d(X, Z) = \inf\{d(x, z) \colon 0 \neq x \in X,\ 0 \neq z \in Z\}$$
$$d(X, Z) \leq d(X, y) + d(y, Z).$$

As usual, if $\sigma \colon V \to W$ is a linear transformation to another normed vector space W, then we can define

$$\|\sigma\| = \sup\{\|\sigma(v)\| \colon v \in \mathbf{S}\}.$$

Since the unit sphere $\mathbf{S}$ is compact, $\|\sigma\| = \|\sigma(v_0)\|$ for some $v_0 \in \mathbf{S}$. Furthermore, $\|\sigma(v)\| \leq \|\sigma\| \cdot \|v\|$ for all $v \in V$. Of course, if $\sigma \neq 0$, then $\|\sigma\| \neq 0$.

Now, let $T \colon V \to V$ be a linear operator and let I be a subspace of V determined by T. Then I is an attractor for T if, for certain subspaces Y of V, T maps vectors close to Y to vectors that are close to I. More precise versions are given below. For convenience, if X is any projective subset of V and if $\varepsilon > 0$, we define the (closed) ε-neighborhood of X by $\overline{\mathfrak{N}}_\varepsilon(X) = \{0 \neq v \in V \colon d(v, X) \leq \varepsilon\}$.

We first consider operators T that can be viewed as generalized transvections. Specifically, let $\tau \colon V \to V$ be a nonzero operator of square 0 and set $I = \operatorname{im} \tau = \tau(V)$. If $T = 1 + a\tau$ with $a \in F$ and $|a|$ large, then the $a\tau$ term should dominate T,

and hence I should be an attractor for T. Indeed, the following is a slight variant of an argument given in [P].

Proposition 1.2. *Let $T = 1 + a\tau$ be an operator on the normed F-vector space V, where $a \in F$ and $\tau\colon V \to V$ is nonzero and has square 0. Set $I = \operatorname{im}\tau = \tau(V)$, and let $K = \ker\tau$. Suppose X is a subspace of V with $V = X \oplus K$, let κ be a positive real number $\leq d(X,K)/2$, and let $\varepsilon > 0$. If $\overline{X} = \overline{\mathfrak{N}}_\kappa(X)$ and $\bar{I} = \overline{\mathfrak{N}}_\varepsilon(I)$, then $T(\overline{X}) \subseteq \bar{I}$ for all suitably large $|a|$.*

Proof. It is clear that both $\overline{X}$ and $\bar{I}$ are projective subsets of V. Furthermore, if $0 \neq u \in \overline{X}$ is arbitrary, then by definition of κ and $\overline{X}$, we have

$$\kappa + d(u,K) \geq d(X,u) + d(u,K) \geq d(X,K) \geq 2\kappa,$$

so $d(u,K) \geq \kappa$. In particular, $d(\overline{X},K) \geq \kappa$ and $\overline{X}$ is disjoint from K. Since $\mathcal{P}(V)$ has diameter ≤ 2, we also have $\kappa \leq 1$.

Let $v \in \overline{X}$ and write $v = x + y \in V = X \oplus K$, with $x \in X$ and $y \in K$. Since $\overline{X} \cap K = \emptyset$, we have $x \neq 0$. Indeed, we claim that $\|x\| \geq (\kappa/2)\cdot\|v\|$. For this, if $y = 0$, then $x = v$ so $\|x\| \geq (\kappa/2)\cdot\|v\|$, since $\kappa \leq 1$. On the other hand, if $y \neq 0$, then Lemma 1.1(iii) yields

$$\kappa \leq d(\overline{X},K) \leq d(v,K) \leq d(v,y) \leq 2\cdot\|v-y\|/\|v\| = 2\cdot\|x\|/\|v\|.$$

So again we obtain $\|x\| \geq (\kappa/2)\cdot\|v\|$, as required.

Now $I \cong V/K \cong X$ and $X \cap K = 0$, so the restriction of τ to X yields an isomorphism $\sigma\colon X \to I$. Let $\sigma^{-1}\colon I \to X$ be the inverse of σ and set $s = \|\sigma^{-1}\|$. If $z = \tau(x) = \sigma(x)$, then $x = \sigma^{-1}(z)$ and hence $\|x\| \leq \|\sigma^{-1}\|\cdot\|z\| = s\cdot\|\tau(x)\|$. Thus, we conclude that $\|\tau(x)\| \geq s^{-1}\cdot\|x\| \geq (\kappa/2s)\cdot\|v\|$.

Finally, note that $T = 1 + a\tau$, so $T(v) = v + a\tau(x+y) = v + a\tau(x)$. Since, $T(v)$ and $a\tau(x)$ are nonzero, and since $a\tau(x) \in I$, Lemma 1.1(iii) yields

$$d(T(v),I) \leq d(T(v),a\tau(x)) \leq \|T(v) - a\tau(x)\|/\|a\tau(x)\| = \|v\|/\|a\tau(x)\|.$$

But $\|a\tau(x)\| = |a|\cdot\|\tau(x)\| \geq |a|\cdot(k/2s)\cdot\|v\|$, so

$$d(T(v),I) \leq \|v\|/\|a\tau(x)\| \leq 2s/(\kappa\cdot|a|).$$

In particular, if $|a| \geq 2s/(\kappa\varepsilon)$, then $d(T(v),I) \leq \varepsilon$ and we conclude that $T(v) \in \bar{I}$. Note that this lower bound $2s/(\kappa\varepsilon)$ depends upon τ, X and κ, but not upon the choice of $v \in \overline{X}$. □

Next, suppose that $T\colon V \to V$ is diagonalizable, that is, T is semisimple with all eigenvalues in F. If I is the subspace of V spanned by the eigenvectors corresponding to those eigenvalues of maximal absolute value, then it is reasonable that I should be an attractor for all T^n, with n a sufficiently large positive integer. For this, it is convenient to first isolate the following facts.

Lemma 1.3. *Let $T\colon V \to V$ be diagonalizable, and let n be a positive integer.*

i. If all eigenvalues of T have absolute value $\leq r$, then there exists a real constant $k > 0$ such that $\|T^n(v)\| \leq kr^n\cdot\|v\|$ for all $v \in V$.

ii. If all eigenvalues of T have absolute value $\geq s$, then there exists a real constant $k' > 0$ with $\|T^n(v)\| \geq k's^n\cdot\|v\|$ for all $v \in V$.

Proof. Let $\{v_1, v_2, \ldots, v_m\}$ be a basis for V consisting of eigenvectors of T, with v_i corresponding to the eigenvalue λ_i. Then each $v \in V$ can be written uniquely as

$v = \sum_{i=1}^{m} \pi_i(v)v_i$, where $\pi_i\colon V \to F$ is a nonzero linear functional. Now define a new norm $\| \ \|'$ on V by $\|v\|' = \max\{|\pi_i(v)|\colon 1 \le i \le m\}$.

Assume that each λ_i satisfies $r \ge |\lambda_i| \ge s$. Since $T^n(v) = \sum_{i=1}^{m} \lambda_i^n \pi_i(v)\cdot v_i$, we see that

$$\begin{aligned}\|T^n(v)\|' &= \max\{|\lambda_i^n \pi_i(v)|\colon 1 \le i \le m\} \\ &\le r^n \cdot \max\{|\pi_i(v)|\colon 1 \le i \le m\} = r^n \cdot \|v\|'.\end{aligned}$$

Similarly, $\|T^n(v)\|' \ge s^n \cdot \|v\|'$.

Finally, note that the two norms $\| \ \|$ and $\| \ \|'$ are equivalent. In other words, there are positive constants a and b with $a\cdot\|v\|' \ge \|v\| \ge b\cdot\|v\|'$ for all $v \in V$. Thus

$$\|T^n(v)\| \le a\cdot\|T^n(v)\|' \le ar^n\cdot\|v\|' \le (a/b)r^n\cdot\|v\|,$$

and similarly

$$\|T^n(v)\| \ge b\cdot\|T^n(v)\|' \ge bs^n\cdot\|v\|' \ge (b/a)s^n\cdot\|v\|.$$

The result follows with $k = a/b$ and $k' = b/a$. □

With this, we can now prove the following generalization of [T, Lemma 3.9].

Proposition 1.4. *Let $T\colon V \to V$ be a diagonalizable, nonsingular operator on the normed F-vector space V. Let I be the subspace of V spanned by the eigenspaces of T corresponding to the eigenvalues of absolute value $\ge r > 0$, and let $0 \ne K \subseteq V$ be spanned by the remaining eigenspaces. Suppose X is a subspace of V disjoint from K, let κ be a positive real number $\le d(X,K)/2$, and let $\varepsilon > 0$. If we set $\overline{X} = \overline{\mathfrak{N}}_\kappa(X)$ and $\bar{I} = \overline{\mathfrak{N}}_\varepsilon(I)$, then we have $T^n(\overline{X}) \subseteq \bar{I}$ for all suitably large positive integers n.*

Proof. Since T is diagonalizable, we have $V = I \oplus K$, and it is clear that both $\overline{X}$ and $\bar{I}$ are projective subsets of V. Furthermore, if $0 \ne u \in \overline{X}$ is arbitrary, then by definition of κ and $\overline{X}$, we have

$$\kappa + d(u,K) \ge d(X,u) + d(u,K) \ge d(X,K) \ge 2\kappa,$$

so $d(u,K) \ge \kappa$. Hence $d(\overline{X},K) \ge \kappa$.

Let $v \in \overline{X}$ and write $v = z + y \in V = I \oplus K$, with $z \in I$ and $y \in K$. If $y = 0$, then $v \in I$, so $T^n(v) \in I$, for all n, and there is nothing to prove. Thus, we can suppose that $y \ne 0$. By Lemma 1.1(iii), we have

$$\kappa \le d(\overline{X},K) \le d(v,K) \le d(v,y) \le 2\cdot\|v-y\|/\|v\| = 2\cdot\|z\|/\|v\|,$$

so $\|z\| \ge (\kappa/2)\cdot\|v\|$ and $z \ne 0$. On the other hand, if $\pi\colon V \to K$ is the natural projection with kernel I, then $y = \pi(v)$, so $\|y\| \le h\cdot\|v\|$, where we set $h = \|\pi\|$.

By the definition of r, part (ii) of the previous lemma implies that $\|T^n(z)\| \ge k'r^n\|z\|$ for some positive constant k'. Also, if s is the maximum absolute value of all the eigenvalues of the restriction of T to K, then $s < r$ and part (i) of the previous lemma implies that $\|T^n(y)\| \le ks^n\|y\|$ for some positive constant k.

Finally, since $T^n(v), T^n(z) \ne 0$ and $T^n(z) \in I$, Lemma 1.1(iii) yields

$$\begin{aligned}d(T^n(v),I) \le d(T^n(v),T^n(z)) &\le 2\cdot\|T^n(v-z)\|/\|T^n(z)\| \\ &= 2\cdot\|T^n(y)\|/\|T^n(z)\|.\end{aligned}$$

Furthermore, by the above, we have $\|T^n(y)\| \le ks^n \cdot \|y\| \le khs^n \cdot \|v\|$ and $\|T^n(z)\| \ge k'r^n \cdot \|z\| \ge k'r^n(\kappa/2)\cdot\|v\|$. Thus

$$d(T^n(v), I) \le \frac{2\cdot\|T^n(y)\|}{\|T^n(z)\|} \le \frac{4kh}{k'\kappa}\cdot(s/r)^n.$$

But $0 < (s/r) < 1$ and $(4kh)/(k'\kappa)$ is a positive constant, so it is clear that if n is sufficiently large, then this upper bound for $d(T^n(v), I)$ can be made to be $\le \varepsilon$. In other words, $T^n(v) \in \bar{I}$ for all sufficiently large n, where the bound on n depends on T, X and κ, but not on the particular choice of $v \in \overline{X}$. □

As a consequence of the above, essentially replacing T by T^{-1}, we obtain

Proposition 1.5. *Let $T\colon V \to V$ be a diagonalizable, nonsingular operator on the normed F-vector space V. Let I be the subspace of V spanned by the eigenspaces of T corresponding to the eigenvalues of absolute value $\le r$, and let $0 \ne K \subseteq V$ be spanned by the remaining eigenspaces. Suppose X is a subspace of V disjoint from K, let κ be a positive real number $\le d(X, K)/2$, and let $\varepsilon > 0$. If we set $\overline{X} = \overline{\mathfrak{N}}_\kappa(X)$ and $\bar{I} = \overline{\mathfrak{N}}_\varepsilon(I)$, then we have $T^{-n}(\overline{X}) \subseteq \bar{I}$ for all suitably large positive integers n.*

2. Free products in linear groups

Our goal now is to obtain applications of the attractor results to the existence of free products as is done, for example, in [T, §3]. Since, most of the arguments here tend to be similiar, our proofs are somewhat skimpy. We first need

Lemma 2.1. *Let $T\colon V \to V$ be a nonsingular linear transformation, and let X and Y be projective subsets of V. Then*

$$d(T(X), T(Y)) \le 2\, d(X, Y)\cdot\|T\|\cdot\|T^{-1}\|.$$

In particular, if $0 \ne x \in V$, then

$$d(T(x), T(Y)) \le 2\, d(x, Y)\cdot\|T\|\cdot\|T^{-1}\|.$$

Proof. Let $x \in X \cap \mathbf{S}$ and $y \in Y \cap \mathbf{S}$, where $\mathbf{S}$ denotes the unit sphere of V. Then

$$d(T(X), T(Y)) \le d(T(x), T(y)) \le 2\,\|T(x - y)\|/\|T(x)\|,$$

by Lemma 1.1(iii). Now $\|T(x - y)\| \le \|T\|\cdot\|x - y\|$, and $x = T^{-1}(T(x))$ implies that $1 = \|x\| \le \|T^{-1}\|\cdot\|T(x)\|$. Thus

$$d(T(X), T(Y)) \le 2\,\|x - y\|\cdot\|T\|\cdot\|T^{-1}\|,$$

and the result follows since $d(X, Y) = \inf\{\|x - y\| \colon x \in X \cap \mathbf{S},\ y \in Y \cap \mathbf{S}\}$. □

As is to be expected, the proof of the existence of free products ultimately depends upon the "ping-pong" lemma of F. Klein (see [H, Lemma II.24]). For convenience, we state and quickly prove this elementary, but powerful, result. Here, we use $G^\#$ to denote the nonidentity elements of a group G.

Lemma 2.2. *Let Γ be a group generated by the nonidentity subgroups G and H, and suppose that Γ acts on a set X having nonempty subsets P and Q with $Q \ne P$. If $G^\# Q \subseteq P$, $H^\# P \subseteq Q$, and $|H| > 2$, then Γ is naturally isomorphic to the free product $G * H$.*

Proof. It suffices to show that $1 \in \Gamma$ cannot be written as a nonempty alternating product of elements coming from $G^\#$ and $H^\#$. Suppose by way of contradiction that such a product $1 = \gamma_1\gamma_2\cdots\gamma_n$ exists with $n \geq 1$. If the product starts and ends in $G^\#$, that is if $\gamma_1, \gamma_n \in G^\#$, then by conjugating this expression by a nonidentity element of H, we obtain a similar expression, but this time starting and ending in $H^\#$. Next, if $\gamma_1 \in G^\#$ and $\gamma_n \in H^\#$, then since $|H| > 2$, we can conjugate the expression by an element of $H^\#$, different from γ_n^{-1}, to obtain a similar product but starting and ending in $H^\#$. Since the same argument handles the $\gamma_1 \in H^\#$, $\gamma_n \in G^\#$ situation, we can therefore replace any such expression by one with $\gamma_1, \gamma_n \in H^\#$. But then, the alternating nature of the action of $G^\#$ and $H^\#$ on P and Q yields $1P = P$ and $\gamma_1\gamma_2\cdots\gamma_nP \subseteq Q$, and hence $P \subseteq Q$. Furthermore, by conjugating the expression for 1 by a nonidentity element of G, we obtain a similar expression but now starting and ending in $G^\#$. This time, the alternating nature of the action yields $1Q = Q$ and $\gamma_1\gamma_2\cdots\gamma_nQ \subseteq P$, so we obtain the reverse inclusion $Q \subseteq P$. Hence $P = Q$, contradiction. □

The following is essentially [P, Theorem 1.1]. Suppose $T\colon V \to V$ is given by $T = 1 + a\tau$, where $0 \neq a \in F$ and $\tau\colon V \to V$ is a nonzero operator of square 0. Since $T^n = 1 + na\tau$, we see that T has infinite order if $\operatorname{char} F = 0$ and it has prime order p if $\operatorname{char} F = p > 0$. Thus the condition below that either $|G| \geq 3$ or $\operatorname{char} F \neq 2$ guarantees that one of the two generating subgroups in $\langle G, T\rangle$ has order at least 3. Furthermore, note that $|na| = |n|\,|a|$. Hence, in order to apply Proposition 1.2 to T^n, we need to know that $|na|$ is at least as large as $|a|$, when $n \neq 0$ in F. Specifically, we use $1\mathbb{Z}$ to denote the set of integer multiples of 1 in F, so that $1\mathbb{Z} = \mathbb{Z}$ if $\operatorname{char} F = 0$ and $1\mathbb{Z} = \mathrm{GF}(p)$ if $\operatorname{char} F = p > 0$. In the latter case, it is clear that $|1\mathbb{Z} \setminus 0| = 1$, but in the former situation, a number of possibilities exist. Thus, the hypothesis below that $|1\mathbb{Z} \setminus 0| \geq 1$ comes into play only in the characteristic 0 situation. This hypothesis is needed, since the condition fails, for example, in p-adic fields. Indeed, in view of [B, Theorem VI.9.1] it fails precisely when F is a finite algebraic extension of a p-adic field.

Theorem 2.3. *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, in fact, 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 $T = 1 + a\tau$.*

Proof. Let 2κ be the minimum of the finitely many distances $d(gI, K)$ for all $g \in G^\#$. Then $\kappa > 0$, by assumption and Lemma 1.1(i), and we set $P = \bigcup_{g\in G^\#} \overline{\mathfrak{N}}_\kappa(gI)$. Next, let $r = \max\{2{\cdot}\|g\|{\cdot}\|g^{-1}\|\colon g \in G^\#\}$, set $\varepsilon = \kappa/r$, and define $Q = \overline{\mathfrak{N}}_\varepsilon(I)$.

We claim that $G^\#Q \subseteq P$. To this end, let $g \in G^\#$ and $v \in Q$. Then $v \in \overline{\mathfrak{N}}_\varepsilon(I)$, so $d(v, I) \leq \varepsilon$. Therefore, by Lemma 2.1, we have $d(gv, gI) \leq 2{\cdot}\|g\|{\cdot}\|g^{-1}\|{\cdot}\varepsilon \leq r\varepsilon = \kappa$, so $gv \in \overline{\mathfrak{N}}_\kappa(gI) \subseteq P$, as required. Note also that $I \subseteq Q$, but that $I \cap P = \emptyset$ by the definition of κ and the fact that $I \subseteq K$. Thus $P \neq Q$.

Finally, by Propositions 1.2, we know that I is an attractor for T. Specifically, by applying this result to each of the finitely many subspaces gI, with $g \in G^\#$, we see that there exists a positive real number s so that if $|a| \geq s$, then $T{\cdot}\overline{\mathfrak{N}}_\kappa(gI) \subseteq \overline{\mathfrak{N}}_\varepsilon(I) = Q$. Thus since $T^n = (1 + a\tau)^n = 1 + na\tau$ and $|na| \geq |a|$ for all $n \in \mathbb{Z}$ with

$1 \cdot n \neq 0$, we have $\langle T \rangle^{\#} P \subseteq Q$. Since at least one of the groups G or $\langle T \rangle$ has order ≥ 3, we conclude from Lemma 2.2 that $\langle G, T \rangle = G * \langle T \rangle$. □

The next result is the semisimple analog of the above. To avoid repetition, if $T\colon V \to V$ is any nonsingular, diagonalizable operator, then we say that $V = X_+ \oplus X_0 \oplus X_-$ is a T-decomposition of V if there exist real numbers $r > s > 0$ with $X_+ \neq 0$ spanned by the eigenspaces of T corresponding to the eigenvalues of absolute value $\geq r$, $X_- \neq 0$ spanned by the eigenspaces of T corresponding to the eigenvalues of absolute value $\leq s$, and with X_0 the span of the remaining eigenspaces. Note that the hypothesis below implies that $X_+ \neq X_-$ and that $\dim_F X_+ = \dim_F X_-$. In particular, T must have infinite multiplicative order since all its eigenvalues cannot be roots of unity, which all have absolute value 1.

Theorem 2.4. *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, $\langle G, T^n \rangle \cong G * \langle T^n \rangle$.*

Proof. Let 2κ be the minimum of the finitely many distances $d(gX_+, X_0 \oplus X_-)$, $d(gX_-, X_0 \oplus X_-)$, $d(gX_+, X_+ \oplus X_0)$ and $d(gX_-, X_+ \oplus X_0)$ for all $g \in G^{\#}$. Then $\kappa > 0$, by assumption and Lemma 1.1(i), and we set

$$P = \bigcup_{g \in G^{\#}} \overline{\mathfrak{N}}_\kappa(gX_+) \cup \bigcup_{g \in G^{\#}} \overline{\mathfrak{N}}_\kappa(gX_-).$$

Next, let $t = \max\{2 \cdot \|g\| \cdot \|g^{-1}\| \colon g \in G^{\#}\}$, set $\varepsilon = \kappa/t$, and define

$$Q = \overline{\mathfrak{N}}_\varepsilon(X_+) \cup \overline{\mathfrak{N}}_\varepsilon(X_-).$$

We claim that $G^{\#} Q \subseteq P$. To this end, let $g \in G^{\#}$ and $v \in Q$. Then $v \in \overline{\mathfrak{N}}_\varepsilon(X_\pm)$ for some choice of $\pm$, so $d(v, X_\pm) \leq \varepsilon$. Therefore, by Lemma 2.1, we have $d(gv, gX_\pm) \leq 2 \cdot \|g\| \cdot \|g^{-1}\| \cdot \varepsilon \leq t\varepsilon = \kappa$, so $gv \in \overline{\mathfrak{N}}_\kappa(gX_\pm) \subseteq P$, as required. Note also that $X_+ \subseteq Q$, but that $X_+ \cap P = \emptyset$ by the definition of κ, so $P \neq Q$.

Finally, by Propositions 1.4 and 1.5, we know that X_+ is an attractor for T and that X_- is an attractor for T^{-1}. Specifically, by applying those results to each of the finitely many subspaces gX_+ and gX_-, with $g \in G^{\#}$, we see that there exists a positive integer n_0 so that if $n \geq n_0$, then $T^n \cdot \overline{\mathfrak{N}}_\kappa(gX_\pm) \subseteq \overline{\mathfrak{N}}_\varepsilon(X_+) \subseteq Q$ and $T^{-n} \cdot \overline{\mathfrak{N}}_\kappa(gX_\pm) \subseteq \overline{\mathfrak{N}}_\varepsilon(X_-) \subseteq Q$, for all $g \in G^{\#}$. It follows that if $n \geq n_0$, then $\langle T^n \rangle^{\#} P \subseteq Q$. Thus, since T has infinite multiplicative order, Lemma 2.2 implies that $\langle G, T^n \rangle = G * \langle T^n \rangle$. □

The remaining theorems in this section are concerned with groups generated by two operators S and T that are either both diagonalizable, both generalized transvections, or one of each. As above, in the case of generalized transvections, we need to assume that $|1\mathbb{Z} \setminus 0| \geq 1$. Furthermore, when both S and T are generalized transvections, we suppose that $\mathrm{char}\, F \neq 2$ to avoid the possibility that both operators have order 2. It is easy to see that the hypotheses below imply that the various subspaces I, J, $X_\pm$ and $Y_\pm$ must all have the same dimension.

Theorem 2.5. *Let V be a finite-dimensional F-vector space and let $S, T\colon V \to V$ be two nonsingular operators. Suppose S and T are both diagonalizable with*

$V = X_+ \oplus X_0 \oplus X_-$ and $V = Y_+ \oplus Y_0 \oplus Y_-$ being 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 $\langle S^m, T^n \rangle = \langle S^m \rangle * \langle T^n \rangle$.

Proof. Let 2κ be the smallest value of the eight distances $d(X_\pm, Y_0 \oplus Y_\pm)$ and $d(Y_\pm, X_0 \oplus X_\pm)$, so that $\kappa > 0$ by assumption and Lemma 1.1(i). Define $P = \overline{\mathfrak{N}}_\kappa(X_+) \cup \overline{\mathfrak{N}}_\kappa(X_-)$ and $Q = \overline{\mathfrak{N}}_\kappa(Y_+) \cup \overline{\mathfrak{N}}_\kappa(Y_-)$. Since X_+ is an attractor for S and X_- is an attractor for S^{-1}, it follows from Propositions 1.4 and 1.5 that $\langle S^m \rangle^\# Q \subseteq P$ for all sufficiently large positive integers m. Similarly, $\langle T^n \rangle^\# P \subseteq Q$ for all sufficiently large n. Since $X_+ \subseteq P$ and $X_+ \cap Q = \emptyset$, we see that $P \neq Q$, and hence the result follows from Lemma 2.2. □

The above generalizes [T, Proposition 3.2], but also follows from it. Namely, if k is the common dimension of $X_\pm$ and $Y_\pm$, then we can let $G = \langle S, T \rangle$ act on the exterior power $W = \wedge^k V$. Since S and T are diagonalizable on W and since $\wedge^k X_\pm$ and $\wedge^k Y_\pm$ reduce to points in the projective space $\mathcal{P}(W)$, we can conclude from [T, Proposition 3.2] that the image of G is a free product and hence so is G. On the other hand, if either S or T is a generalized transvection, then its structure as an operator on $\wedge^k V$ becomes quite different in nature, and therefore this exterior power trick no longer applies.

Theorem 2.6. *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 two nonsingular operators. Specifically, $S = 1 + a\sigma$ and $T = 1 + b\tau$ are both generalized transvections, where $\sigma, \tau \colon V \to V$ are nonzero operators of square 0. Assume that $|1\mathbb{Z} \setminus 0| \geq 1$ and $\operatorname{char} F \neq 2$. 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 $\langle S, T \rangle = \langle S \rangle * \langle T \rangle$.*

Proof. Let 2κ be the smaller of the distances $d(I, L)$ and $d(J, K)$, so that $\kappa > 0$ by assumption and Lemma 1.1(i). Define $P = \overline{\mathfrak{N}}_\kappa(I)$ and $Q = \overline{\mathfrak{N}}_\kappa(J)$. Since I is an attractor for S and $|1\mathbb{Z} \setminus 0| \geq 1$, it follows from Proposition 1.2 that $\langle S \rangle^\# Q \subseteq P$ for all $a \in F$ with sufficiently large absolute value. Similarly, $\langle T \rangle^\# P \subseteq Q$ for all $b \in F$ with sufficiently large absolute value. Since $I \subseteq K$, we have $I \subseteq P$ and $I \cap Q = \emptyset$. Thus $P \neq Q$ and, since S and T have order at least 3, the result follows from Lemma 2.2. □

Finally, we consider the mixed case.

Theorem 2.7. *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 an S-decomposition 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 $\langle S^n, T \rangle = \langle S^n \rangle * \langle T \rangle$.*

Proof. Let 2κ be the smallest of the four distances $d(I, X_0 \oplus X_\pm)$ and $d(X_\pm, K)$, so that $\kappa > 0$ by assumption and Lemma 1.1(i). Define $P = \overline{\mathfrak{N}}_\kappa(X_+) \cup \overline{\mathfrak{N}}_\kappa(X_-)$ and $Q = \overline{\mathfrak{N}}_\kappa(I)$. Since X_+ is an attractor for S and X_- is an attractor for S^{-1}, it follows from Propositions 1.4 and 1.5 that $\langle S^n \rangle^\# Q \subseteq P$ for all sufficiently large positive integers n. Similarly, since I is an attractor for T, Proposition 1.2 and

the hypothesis imply that $\langle T\rangle^{\#}P \subseteq Q$ for all $a \in F$ with sufficiently large absolute value. Finally, $I \subseteq Q$ and $I \cap P = \emptyset$, so $P \neq Q$, and Lemma 2.2 yields the result. □

3. Bass cyclic units

The goal of the remainder of this paper is to apply linear group results, and in particular Theorem 2.5, to the unit group of an integral group ring. We first introduce some 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 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, $u_{k,m}(x) = (1 + x + \cdots + x^{k-1})^m + c\hat{x}$ 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 3.1. *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, as in [S, 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 $1 \leq k \leq d-1$. 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 $2 \leq k \leq d-2$ and hence $d \geq 5$. Finally, it follows from (ii) that $u_{k,m}(x)^a = u_{k,ma}(x)$ for all integers $a \geq 1$.

Lemma 3.2. *Let $\theta\colon \mathbb{Z}[G] \to \mathbb{Z}[H]$ be the group ring homomorphism determined by the group epimorphism $\theta\colon G \to H$, and let y be an element of H of order d. If $u_{k,m}(y)$ 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 y, and a Bass cyclic unit $u_{k,m'}(x)$ of $\mathbb{Z}[G]$ such that $u_{k,m'}(x)$ maps to a positive integer power of $u_{k,m}(y)$.

Proof. If y is a π-element, then there exists a π-element $x \in G$ with $\theta(x) = y$. 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 m divides $\varphi(d')$. Nevertheless, there certainly exists a positive integer a so that $\varphi(d')$ divides $m' = ma$. Then $u_{k,m'}(x)$ is a Bass cyclic unit and, since $\theta(\hat{x})$ is an integer multiple of $\hat{y}$, it follows from part (ii) of the preceding lemma that $\theta(u_{k,m'}(x))$ and $u_{k,m}(y)^a$ agree up to an integer multiple of $\hat{y}$, say $c\hat{y}$. But both of these terms have augmentation 1, so we conclude that $c = 0$, as required. □

We will apply Theorem 2.5 to matrix images of these units, so it is necessary to understand their eigenvalues. For this, we first isolate the following simple fact using a bit of calculus.

Lemma 3.3. *Let r and k be real numbers with $2 \le k$ and $0 < r \le 1/(2k)$. Then the real-valued function*

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

defined on the interval $[r, 1/2]$ takes on its maximum at $z = r$. Moreover, $f(r) > 1$.

Proof. We first study the function $f(z)$ in the open interval $(0, 1/k)$. Note that both numerator and denominator are positive here, so the absolute value is unnecessary. Furthermore, if $z \in [1/(2k), 1/k)$ then the numerator of $f(z)$ is decreasing and the denominator is increasing, so $f(z)$ is certainly strictly decreasing. On the other hand, if $z \in (0, 1/(2k))$, then all the trigonometric functions involved are positive and it is easy to see that the derivative $\partial f(z)/\partial z$ is a positive multiple of $k \tan \pi z - \tan k\pi z < 0$. Thus $f(z)$ is also decreasing in $(0, 1/(2k))$, and we conclude that $f(z)$ is strictly decreasing to 0 in $(0, 1/k)$. Since r is in this interval, we see that $f(r) > f(z)$ for all $z \in (r, 1/k)$.

It remains to compare $f(r)$ with the values $f(z)$ for $z \in [1/k, 1/2]$. To do this, we use the inequalities $y \ge \sin y \ge y - y^3/6 = y(1 - y^2/6)$ which hold for all $y \ge 0$. To start with

$$\sin k\pi r \ge k\pi r \cdot [1 - (k\pi r)^2/6] \ge k\pi r \cdot [1 - \pi^2/24]$$

since $kr \le 1/2$. Thus, $\sin \pi r \le \pi r$ yields

$$f(r) = \frac{\sin k\pi r}{\sin \pi r} \ge \frac{k\pi r \cdot [1 - \pi^2/24]}{\pi r} = k \cdot [1 - \pi^2/24].$$

Indeed, using $k \ge 2$, we have $f(r) \ge 2[1 - \pi^2/24] > 1.177 > 1$.

On the other hand, if $z \in [1/k, 1/2]$, then $|\sin k\pi z| \le 1$ and

$$\sin \pi z \ge \sin \pi/k \ge (\pi/k) \cdot [1 - (\pi/k)^2/6] \ge (\pi/k) \cdot [1 - \pi^2/24],$$

using $k \ge 2$. Thus, since $\pi \cdot [1 - \pi^2/24]^2 > 1.089 > 1$, we have

$$f(z) = \left| \frac{\sin k\pi z}{\sin \pi z} \right| \le \frac{k}{\pi \cdot [1 - \pi^2/24]} < k \cdot [1 - \pi^2/24] \le f(r),$$

and the lemma is proved. □

It is instructive to look at a computer plot of the function $f(z)$ in the interval $[0, 1/2]$ for large values of k. One sees that the decreasing aspect of $f(z)$ from $f(0) = k$ to $f(1/k) = 0$ is quite precipitous. On the other hand, the values of $f(z)$ in the interval $[1/k, 1/2]$ stay relatively small.

Lemma 3.4. *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 is equal to 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 and

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

Hence, since $|\varepsilon^{a/2}| = 1$, this 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 $\varepsilon^a \ne 1$. 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 $2 \le k \le d/2$. Furthermore, since $|u_{k,m}(\varepsilon^a)| = |u_{k,m}(\varepsilon^{-a})|$, it suffices to restrict our attention to the possibilities $a = 1, 2, \ldots, \lfloor d/2 \rfloor$. For this, consider the real-valued function

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

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 $r = 1/d$. Since $rk = k/d \le 1/2$, the preceding lemma now implies that the maximum value of $f(z)$ on this interval occurs at $z = r = 1/d$ and that this largest value is > 1. Thus $a = 1$ and $f(1/d) > 1$. Taking into account the $\pm$ symmetry, we see that the maximum value of $|u_{k,m}(\varepsilon^a)|$ with $\varepsilon^a \ne 1$ 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 complex 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 $|u_{\ell,m}(\varepsilon^{ka})|$ is maximal. Since $2 \le \ell \le d-2$, we conclude from the above that this occurs precisely when $ak \equiv \pm 1 \bmod d$, as required. □

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

Lemma 3.5. *Let p be a prime.*

i. Suppose $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_r$ and $\delta_1, \delta_2, \dots, \delta_r$ are complex p^nth 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. Set $d = p^n$, suppose $2 \le k \le d-2$, and let ε be a primitive complex dth root of unity. If $p \ge 5$ and $|u_{k,m}(\varepsilon^a)| = |u_{k,m}(\varepsilon^b)|$, 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 d 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 1. Then, by Lemma 3.4(i) and the fact that $(\varepsilon^{ak} - \varepsilon^{-ak})/(\varepsilon^a - \varepsilon^{-a})$ is real, the equality $|u_{k,m}(\varepsilon^{2a})| = |u_{k,m}(\varepsilon^{2b})|$ 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 of course holds only for $\kappa = \pm 1$. Thus

$$\Re\big(\varepsilon^{ak+b} + \varepsilon^{bk-\kappa a}\big) = \Re\big(\varepsilon^{bk+\kappa a} + \varepsilon^{ak-b}\big)$$

and, since both sides are sums of four p^nth roots of unity and 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 $\pm$ signs above disagree, then adding the equations yields $2ak \equiv \pm 2\kappa a$ and hence $k \equiv \pm 1 \bmod d$, a contradiction. Thus the signs must agree and this time adding yields $2ak \equiv \pm 2bk$ so $2a \equiv \pm 2b \bmod d$, as required.

When $\varepsilon^{2b} = 1$, the argument is of course simpler. Suppose, by way of contradiction that $\varepsilon^{2a} \ne 1$. Then $|u_{k,m}(\varepsilon^{2a})| = |u_{k,m}(\varepsilon^{2b})| = 1$ yields

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

so $\varepsilon^{ka} - \varepsilon^{-ka} = \kappa(\varepsilon^a - \varepsilon^{-a}) = \varepsilon^{\kappa a} - \varepsilon^{-\kappa a}$. Thus $\varepsilon^{ka} + \varepsilon^{-\kappa a} = \varepsilon^{-ka} + \varepsilon^{\kappa a}$ and this is a contradiction since $ka \not\equiv -ka \bmod d$ and $ka \not\equiv \kappa a \bmod d$. □

4. Free subgroups of the unit group

In this section, we prove our main group ring result which asserts that if G is a nonabelian group of order prime to 6, then $\mathbb{Z}[G]$ has two Bass cyclic units that generate a nonabelian free subgroup of the unit group. For this, it is first convenient to restate Theorem 2.5 in a more usable form, based on the projection maps to the plus and minus components of the S- and T-decompositions of V. Here, all the assumptions of the first two sections apply. In particular, F is an absolute-valued field that is locally compact in the metric topology. As will be apparent, the reformulation below includes a slight change in notation.

Corollary 4.1. *Let V be a finite-dimensional F-vector space and let S and T be two nonsingular operators on V. Suppose S and T are both diagonalizable with $V = S_+ \oplus S_0 \oplus S_-$ and $V = T_+ \oplus T_0 \oplus T_-$ being S- and T-decompositions of V, respectively. Assume that $\dim S_+ = \dim S_- = r = \dim T_+ = \dim T_-$ and consider the four projections $\sigma_+ \colon V \to S_+$, $\sigma_- \colon V \to S_-$, $\tau_+ \colon V \to T_+$, and $\tau_- \colon V \to T_-$. If the idempotent conditions $\operatorname{rank} \sigma_i\tau_j = r = \operatorname{rank} \tau_j\sigma_i$ hold for all $i, j \in \{+, -\}$, then $\langle S^m, T^n\rangle = \langle S^m\rangle * \langle T^n\rangle$ for all sufficiently large positive integers m and n.*

Proof. Since $\operatorname{rank} \sigma_+\tau_+ = r = \operatorname{rank} \tau_+$, we have $V\sigma_+\tau_+ = V\tau_+$. Thus the map $\tau_+ \colon V\sigma_+ \to V\tau_+$ is onto and consequently also one-to-one. In other words, $V\sigma_+$ is disjoint from $\ker \tau_+ = V(1 - \tau_+)$, and we see that $S_+ \cap (T_0 \oplus T_-) = 0$. Similarly, the seven remaining idempotent conditions yield the seven remaining intersection conditions of Theorem 2.5, and hence the result follows. □

Obviously, Theorems 2.6 and 2.7 have similar interpretations based on suitable projections, but these maps are not canonically defined. For integral group ring applications, we will of course apply Corollary 4.1 with $F = \mathbb{C}$, the field of complex numbers. We now begin the proof of our main result by considering a number of special cases. The following lemma is well-known. We use it to fix notation for much of the remainder of this paper.

Lemma 4.2. *Let $G = A \rtimes X$, where A is a normal abelian subgroup of G and where $X = \langle x\rangle$ is cyclic of prime order p. Let $\mathfrak{X} \colon \mathbb{C}[G] \to \mathrm{M}_n(\mathbb{C})$ be a complex irreducible representation of G of degree $n > 1$, with associated character $\chi \colon G \to \mathbb{C}$, and let μ be an irreducible constituent of the restriction of χ to A. Then we have*

i. $n = p$ and we can assume that

$$\mathfrak{X}(a) = \operatorname{diag}(\mu(a), \mu^x(a), \ldots, \mu^{x^{p-1}}(a))$$

for all $a \in A$. Here $\mu^{x^i}(a) = \mu(x^i a x^{-i})$ and these p linear characters are all distinct. Furthermore, $\mathfrak{X}(x)$ is then the permutation matrix

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

ii. Let $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_p$ be all the complex pth roots of unity, define

$$P = \frac{1}{\sqrt{p}} \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \varepsilon_1 & \varepsilon_2 & \cdots & \varepsilon_p \\ \vdots & \vdots & & \vdots \\ \varepsilon_1^{p-1} & \varepsilon_2^{p-1} & \cdots & \varepsilon_p^{p-1} \end{bmatrix}$$

and let $Q = P^*$, where $*$ denotes transpose conjugate. Then P is a unitary matrix, $Q = P^{-1}$ and $Q\mathfrak{X}(x)P = D = \operatorname{diag}(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_p)$.

iii. If $A = \langle a \rangle$ is cyclic, then $\mu(a), \mu^x(a), \ldots, \mu^{x^{p-1}}(a)$ are all distinct and not equal to 1. In addition, if p is odd, then no two of these elements can be complex conjugates of each other.

Proof. Part (i) follows from Clifford's Theorem [I, Theorem 6.5] and a result of Ito [I, Theorem 6.15]. Note that if two of the characters μ^{x^i} and μ^{x^j} are equal, then all of these conjugate characters are identical and hence $\mathfrak{X}(A)$ is central in the matrix ring. But then $\mathfrak{X}(G)$ is abelian, contradicting the assumption that $n > 1$. Thus the various μ^{x^i} must be distinct. Part (ii) is an immediate consequence of the simple computation $\mathfrak{X}(x)P = PD$ along with the fact that P is clearly unitary. Finally, for (iii), since $A = \langle a \rangle$, we see that the linear characters of A are determined by their value on a. In particular, by (i), it follows that $\mu(a), \mu^x(a), \ldots, \mu^{x^{p-1}}(a)$ are all distinct. Furthermore, if some $\mu^{x^i}(a) = 1$, then $\mu^{x^i} = 1_A$ and hence $\mu^{x^k} = 1_A$ for all k, certainly a contradiction. Finally, if $\mu^{x^i}(a)$ and $\mu^{x^j}(a)$ are complex conjugates for some $i \not\equiv j \bmod p$, then x^{j-i} sends μ^{x^i} to its complex conjugate character, and hence $x^{2(j-i)}$ fixes μ^{x^i}. By (i), this can only occur when $p = 2$. □

Our first special cases, considered below, are fairly easy to handle.

Lemma 4.3. *Let $G = A \rtimes X$ be a nonabelian group, where $A \lhd G$ and $X = \langle x \rangle$ is cyclic of prime order $p \geq 5$. Assume that either A is cyclic of prime power order or A is abelian of type (p, p). Then, for some $a \in A$, 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. If A is cyclic, we take $a \in A$ to be a generator of the group. By assumption, a has order q^k for some prime q. Since $|\operatorname{Aut}(A)| = (q-1)q^{k-1}$ and since G is nonabelian, it follows that either $q = p$ or p divides $q - 1$. In either case, we have $q \geq 5$. On the other hand, if A is abelian of type (p, p), then we can take $a \in A$ to be any element that is not central in G. Now choose any two Bass cyclic units $u_{k,t}(a)$ and $u_{r,s}(x)$ with $k \not\equiv \pm 1$ modulo the order of a and with $r \not\equiv \pm 1 \bmod p$. Since a and x both have odd order ≥ 5, one possibility here is that $k = r = 2$.

Since G is nonabelian, there exists a nonlinear irreducible representation $\mathfrak{X}$ of $\mathbb{C}[G] \supseteq \mathbb{Z}[G]$ with associated character $\chi\colon G \to \mathbb{C}$. Say $\mathfrak{X}\colon \mathbb{C}[G] \to \mathrm{M}_u(\mathbb{C})$ for some $u > 1$. By the preceding lemma, we have $u = p$, and we can assume that $\mathfrak{X}(a) = \operatorname{diag}(\alpha_1, \alpha_2, \ldots, \alpha_p)$ for suitable $\alpha_i \in \mathbb{C}$. Indeed, if A is cyclic, then $\alpha_1, \alpha_2, \ldots, \alpha_p$ are distinct q^kth roots of unity and no two of these are complex conjugates of each other. On the other hand, if A is abelian of type (p, p), then we know that $\chi(a) = 0$ and therefore $\{\alpha_1, \alpha_2, \ldots, \alpha_p\}$ are all the complex pth roots of unity.

Note that

$$S = \mathfrak{X}(u_{k,t}(a)) = \operatorname{diag}(u_{k,t}(\alpha_1), u_{k,t}(\alpha_2), \ldots, u_{k,t}(\alpha_p)).$$

In particular, if A is cyclic, then by Lemma 3.5(ii) the eigenvalues of S have distinct absolute values, and hence we can choose an S-decomposition of the space $V = \mathbb{C}^p$ with $\dim S_+ = \dim S_- = 2$. Similarly, by Lemma 3.4(ii)(iii), this holds for any noncentral $a \in A$ if A is abelian of type (p, p). Thus we have $V = S_+ \oplus S_0 \oplus S_-$ and we denote by σ_+ and σ_- the projections of V into S_+ and S_-, respectively. Certainly, there exist distinct subscripts i, j, i', j' satisfying $\sigma_+ = e_{i,i} + e_{j,j}$ and $\sigma_- = e_{i',i'} + e_{j',j'}$.

Next, by Lemma 4.2(ii), there exists a suitably described unitary matrix P with $P^{-1}\mathfrak{X}(x)P = D = \mathrm{diag}(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_p)$, where $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_p$ are the p distinct complex pth roots of unity, written in any order we choose. Thus, if $T = \mathfrak{X}(u_{r,s}(x))$, then $P^{-1}TP = \mathrm{diag}(u_{r,s}(\varepsilon_1), u_{r,s}(\varepsilon_2), \ldots, u_{r,s}(\varepsilon_p))$. In other words, we know the eigenvalues of T and, by Lemma 3.4(ii)(iii), precisely two of these have the largest absolute value and precisely two have the smallest absolute value. These therefore give rise to a T-decomposition $V = T_+ \oplus T_0 \oplus T_-$ of V with $\dim T_+ = \dim T_- = 2$. Indeed, by ordering the eigenvalues of $\mathfrak{X}(x)$ appropriately, we can assume that ε_1 and ε_2 yield the largest absolute value, while ε_3 and ε_4 yield the smallest. It then follows that the corresponding projections τ_+ and τ_- satisfy $\tau_+ = P(e_{1,1}+e_{2,2})P^{-1}$ and $\tau_- = P(e_{3,3} + e_{4,4})P^{-1}$.

It remains to verify the eight idempotent conditions of Corollary 4.1. For this, we will just consider $\sigma_+\tau_-$ and $\tau_-\sigma_+$, since the six additional products follow in the same manner. To start with, note that $\sigma_+\tau_- = (e_{i,i} + e_{j,j})\cdot P(e_{3,3} + e_{4,4})P^{-1}$, so $\sigma_+\tau_-$ and $(e_{i,i} + e_{j,j})P(e_{3,3} + e_{4,4})$ have the same rank. Furthermore, the latter matrix has only four nonzero entries and these form the 2×2 submatrix

$$\frac{1}{\sqrt{p}} \cdot \begin{bmatrix} \varepsilon_3^{i-1} & \varepsilon_4^{i-1} \\ \varepsilon_3^{j-1} & \varepsilon_4^{j-1} \end{bmatrix}$$

which has a nonzero determinant. Thus we conclude that $\mathrm{rank}\, \sigma_+\tau_- = 2$. On the other hand, since P is a unitary matrix, it is clear that both σ_+ and τ_- are Hermetian. It follows that $\tau_-\sigma_+ = (\sigma_+\tau_-)^*$, and therefore $\mathrm{rank}\, \tau_-\sigma_+ = \mathrm{rank}\, \sigma_+\tau_- = 2$.

It follows from Corollary 4.1 that there exist positive integers m and n such that $\langle S^m, T^n\rangle = \langle S^m\rangle * \langle T^n\rangle$ is a free group of rank 2. Thus, since $S = \mathfrak{X}(u_{k,t}(a))$ and $T = \mathfrak{X}(u_{r,s}(x))$, we conclude that $u_{k,t}(a)^m$ and $u_{r,s}(x)^n$ generate a nonabelian free subgroup of the unit group of $\mathbb{Z}[G]$. But $u_{k,t}(a)^m = u_{k,tm}(a)$ and $u_{r,s}(x)^n = u_{r,sn}(x)$ by Lemma 3.1(ii), so the result follows. □

When $G = A \rtimes X$ with A an elementary abelian q-group of order $> q$, then the above proof cannot apply since the eigenvalues of $\mathfrak{X}(a)$ for any $a \in A$ are difficult to control. Thus we are forced to take a different approach, and for this we need

Lemma 4.4. *Let $\langle x\rangle$ be a group of prime order p acting faithfully and irreducibly on an elementary abelian q-group A. Here $p \geq 5$, $q \geq 3$ is a prime different from p, and $|A| > q$. If $1 \neq a \in A$, then the $p-1$ elements a^{1+x}, $a^{1+x^2}, \ldots, a^{1+x^{p-1}}$ cannot all be $\langle x\rangle$-conjugate.*

Proof. Note that $\mathbb{C}_A(x) = 1$ and hence $1+x+x^2+\cdots+x^{p-1} = 0$ in its action on A. Let $1 \neq a \in A$ and suppose, by way of contradiction, that a^{1+x}, $a^{1+x^2}, \ldots, a^{1+x^{p-1}}$ are all $\langle x\rangle$-conjugate. Since $a^{\langle x\rangle} = A$, it follows that these $p-1$ elements are all distinct and therefore if $b \in A$ is the pth element of this $\langle x\rangle$-conjugacy class, then $b\prod_{i=1}^{p-1} a^{1+x^i} \in \mathbb{C}_A(x) = 1$. Thus, since $x + x^2 + \cdots + x^{p-1} = -1$, we conclude

that $ba^{p-1}a^{-1} = 1$ and hence $b = a^{2-p}$. It follows that there exists a one-to-one function f from $\{1, 2, \ldots, p-1\}$ to itself such that

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

for all $1 \le i \le p-1$. In particular, since $a^{\langle x \rangle} = A$, we see that $(2-p)x^i = 1 + x^{f(i)}$ as operators on A.

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

Next, we multiply the equation $(2-p)x^i = 1 + x^{f(i)}$ by x^{-i}, and then setting $j \equiv -i \bmod p$, we get

$$(2-p) = x^j + x^{g(j)},$$

where $g(j) = f(i) - i \not\equiv 0 \bmod p$. Thus g is also a one-to-one function from $\{1, 2, \ldots, p-1\}$ to itself, and by summing the above displayed equation over all such j, we obtain $(2-p)(p-1) \equiv (-1) + (-1) = -2 \bmod q$. Thus $p^2 \equiv 3p \bmod q$ and hence $p \equiv 3 \bmod q$ since $p \ne q$. In particular, $q \ne 3$ and $2 - p \equiv -1 \bmod q$, so we have $1 + x^j = -x^{g(j)}$ for all $j = 1, 2, \ldots, p-1$. Since p is odd and $x^p = 1$, this yields $(1 + x^j)^p = -1$.

In other words, $x, x^2, \ldots, x^{p-1} \in \mathrm{GF}(q^n)$ are all roots of the polynomial equations $(1+\zeta)^p = -1$ and $\zeta^p = 1$ in $\mathrm{GF}(q)[\zeta]$. Hence, they are roots of $2+(1+\zeta)^p-\zeta^p$, a polynomial of degree $p-1$. It follows that this polynomial must be a scalar multiple of $1 + \zeta + \zeta^2 + \cdots + \zeta^{p-1}$ and, by considering the constant term, we see that this scalar is 3. We conclude that $\binom{p}{k} \equiv 3 \bmod q$ for $k = 1, 2, \ldots, p-1$. However, since $p \equiv 3 \bmod q$ and $p, q \ge 5$, we see that $\binom{p}{3} \equiv 1 \not\equiv 3 \bmod q$, and this is the required contradiction. □

We briefly comment on the above situation for the missing small primes. If $p = 2$, then $|A| = q$, so this case does not occur. If $p = 3$, then $1 + x + x^2 = 0$, so $a^{1+x} = a^{-x^2}$ and $a^{1+x^2} = a^{-x}$. Hence, these elements are always $\langle x \rangle$-conjugate. Finally, if $q = 2$, then the preceding proof yields $(1 + \zeta)^p = 1 + \zeta + \cdots + \zeta^{p-1} + \zeta^p$ in the polynomial ring $\mathrm{GF}(2)[\zeta]$. Thus $(1 + \zeta)^{p+1} = 1 + \zeta^{p+1}$ and it follows easily that p must be a Mersenne prime. Conversely, if $p = 2^n - 1$ is such a prime, then $|A| = 2^n$ and all nonidentity elements of A are $\langle x \rangle$-conjugate.

At this point, it is convenient to isolate certain matrix computations. We assume in that following that $G = A \rtimes X$, $\mathfrak{X}$, χ, P and $Q = P^*$ are as in Lemma 4.2.

Lemma 4.5. *Let $i \ne i'$ be subscripts with $\varepsilon_{i'} = \bar{\varepsilon}_i$, and let $j \ne j'$ be subscripts with $\varepsilon_{j'} = \bar{\varepsilon}_j$ Furthermore, let $a \in A$ be an element of order prime to p, and assume that the matrix*

$$M = (e_{i,i} + e_{i',i'}) \cdot Q\mathfrak{X}(a)P \cdot (e_{j,j} + e_{j',j'})$$

does not have rank 2.

i. If $i = j$ or j', then $\chi\big(aa^{x^d}\big) = \chi\big(aa^x\big)$ for all $d = 1, 2, \ldots, p-1$.

ii. If $i \ne j$ and $i \ne j'$, then $\chi\big(aa^{x^d}\big) = \chi\big(aa^{x^{td}}\big)$ for all $d = 1, 2, \ldots, p-1$, where $t \not\equiv \pm 1 \bmod p$ satisfies $\varepsilon_j/\bar{\varepsilon}_i = (\varepsilon_j/\varepsilon_i)^t$.

Proof. Let a have order q so that, by assumption, q is prime to p, and write $\mathfrak{X}(a) = \mathrm{diag}(\alpha_0, \alpha_1, \ldots, \alpha_{p-1})$, where each α_d is a qth root of unity and where we view the subscripts modulo p. Observe that $\mathfrak{X}(x)^{-1}\mathfrak{X}(a)\mathfrak{X}(x) = \mathrm{diag}(\alpha_{p-1}, \alpha_0, \ldots, \alpha_{p-2})$ and thus $\mathfrak{X}(x)^{-d}\mathfrak{X}(a)\mathfrak{X}(x)^d = \mathrm{diag}(\alpha_{0-d}, \alpha_{1-d}, \ldots, \alpha_{p-1-d})$. It follows that

$$\mathfrak{X}(aa^{x^d}) = \mathrm{diag}(\alpha_0\alpha_{0-d}, \alpha_1\alpha_{1-d}, \ldots, \alpha_{p-1}\alpha_{p-1-d})$$

and therefore $\chi\big(aa^{x^d}\big) = \sum_{r=0}^{p-1} \alpha_r\alpha_{r-d}$.

Next, if ρ is any pth root of unity, we set $\mathrm{Tr}(\rho, a) = \sum_{r=0}^{p-1} \rho^r\alpha_r$. Then

$$\begin{aligned}\mathrm{Tr}(\rho, a)\mathrm{Tr}(\rho^{-1}, a) &= \sum_{r=0}^{p-1} \rho^r\alpha_r \cdot \sum_{s=0}^{p-1} \rho^{-s}\alpha_s \\ &= \sum_{d=0}^{p-1} \rho^d \cdot \sum_{r=0}^{p-1} \alpha_r\alpha_{r-d} = \sum_{d=0}^{p-1} \rho^d \cdot \chi\big(aa^{x^d}\big).\end{aligned}$$

Now note that the (i, j)th entry of $Q\mathfrak{X}(a)P$ is equal to

$$\frac{1}{p}\sum_{r=0}^{p-1} \bar{\varepsilon}_i^r\alpha_r\varepsilon_j^r = \frac{1}{p}\mathrm{Tr}(\varepsilon_j/\varepsilon_i, a),$$

since $Q = P^*$. In particular, since $\varepsilon_{i'} = \bar{\varepsilon}_i$ and $\varepsilon_{j'} = \bar{\varepsilon}_j$, we see that the 2×2 submatrix of M corresponding to rows i and i' and columns j and j' is given by

$$M_{2\times 2} = \frac{1}{p} \cdot \begin{bmatrix} \mathrm{Tr}(\varepsilon_j/\varepsilon_i, a) & \mathrm{Tr}(\bar{\varepsilon}_j/\varepsilon_i, a) \\ \\ \mathrm{Tr}(\varepsilon_j/\bar{\varepsilon}_i, a) & \mathrm{Tr}(\bar{\varepsilon}_j/\bar{\varepsilon}_i, a) \end{bmatrix}.$$

Setting $\sigma = \varepsilon_j/\varepsilon_i$ and $\tau = \varepsilon_j/\bar{\varepsilon}_i$, we see that $\sigma \neq \tau, \bar{\tau}$ and

$$M_{2\times 2} = \frac{1}{p} \cdot \begin{bmatrix} \mathrm{Tr}(\sigma, a) & \mathrm{Tr}(\bar{\tau}, a) \\ \\ \mathrm{Tr}(\tau, a) & \mathrm{Tr}(\bar{\sigma}, a) \end{bmatrix}.$$

Since $\mathrm{rank}\, M \neq 2$, by assumption, it follows that $\det M_{2\times 2} = 0$ and therefore $\mathrm{Tr}(\sigma, a) \cdot \mathrm{Tr}(\bar{\sigma}, a) = \mathrm{Tr}(\tau, a) \cdot \mathrm{Tr}(\bar{\tau}, a)$. In other words, we have

$$(*) \qquad \sum_{d=0}^{p-1} \sigma^d \cdot \chi\big(aa^{x^d}\big) = \sum_{d=0}^{p-1} \tau^d \cdot \chi\big(aa^{x^d}\big).$$

Now a is an element of order q, so each $\chi\big(aa^{x^d}\big)$ is contained in $\mathbb{Q}[\delta]$, where δ is a primitive complex qth root of unity. In particular, $(*)$ is a polynomial equation satisfied by a primitive pth root of unity over $\mathbb{Q}[\delta]$ and, since $\gcd(p, q) = 1$, we know that any such equation is a multiple of $1 + \zeta + \cdots + \zeta^{p-1}$.

Suppose first that $i = j$. Then $\varepsilon_i = \varepsilon_j$, so $\sigma = 1$ and τ is a primitive pth root of unity. Since $(*)$ is a polynomial equation in τ of degree $\leq p - 1$, we conclude from the above remarks that all coefficients of the powers of τ must be equal. In particular, $\chi\big(aa^{x^d}\big) = \chi\big(aa^x\big)$ for all $d = 1, 2, \ldots, p - 1$. Similarly, if $i = j'$, then $\tau = 1$ and the same argument applies.

On the other hand, if $i \neq j$ and $i \neq j'$, then both σ and τ are primitive pth roots of unity, and we can write $\tau = \sigma^t$ for some $t \in \{1, 2, \ldots, p-1\}$. Indeed, since $\tau \neq \sigma$

and $\tau \neq \bar{\sigma}$, we have $t \neq 1$ or $p-1$. Viewing the exponents modulo p, equation $(*)$ now becomes

$$\sum_{d=0}^{p-1} \sigma^d \cdot \chi\big(aa^{x^d}\big) = \sum_{d=0}^{p-1} \sigma^{dt} \cdot \chi\big(aa^{x^d}\big),$$

and since the $d = 0$ coefficients match, we see that $\chi\big(aa^{x^d}\big) = \chi\big(aa^{x^{dt}}\big)$ for all d. Of course, $\varepsilon_j/\bar{\varepsilon}_i = \tau = \sigma^t = (\varepsilon_j/\varepsilon_i)^t$, so the result follows. □

With Lemmas 4.4 and 4.5 in hand, we can now deal with the Frobenius case. Unlike the proof of Lemma 4.3, where the first parameters k and r are essentially arbitrary, here our proof requires that k be selected in a rather careful manner.

Lemma 4.6. *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 and with $|A| > q$. 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. Write $G = A \rtimes X$ and let $1 \neq a \in A$. Since $|A| > q$, Lemma 4.4, implies that the elements $a^{1+x}, a^{1+x^2}, \ldots, a^{1+x^{p-1}}$ cannot be all X-conjugate to a^{1+x}. In other words, there exists $t \in \{1, 2, \ldots, p-1\}$ with a^{1+x} not X-conjugate to a^{1+x^t}. Since $(a^{1+x})^{x^{-1}} = a^{1+x^{-1}}$, it is clear that $t \neq 1$ or $p-1$. Thus $2 \leq t \leq p-2$, and we set

$$k \equiv (t-1)/(t+1) \bmod p.$$

Certainly, $k \not\equiv 0 \bmod p$ and, since $t \equiv (1-k)/(1+k) \bmod p$, it is clear that $k \not\equiv \pm 1 \bmod p$. Thus we can assume that $2 \leq k \leq p-2$. For any suitable integer m, for example $m = \varphi(p) = p-1$, we can now consider the Bass cyclic units $u_{k,m}(x)$ and $u_{k,m}(a^{-1}xa) = a^{-1}u_{k,m}(x)a$.

Since G acts on A as X does, it follows that a^{1+x} and a^{1+x^t} are not G-conjugate. Thus there exists an irreducible representation $\mathfrak{X}$ of $\mathbb{C}[G]$, with corresponding character χ, such that $\chi(a^{1+x}) \neq \chi(a^{1+x^t})$. Taking complex conjugates, we see that $\chi(a^{-(1+x)}) \neq \chi(a^{-(1+x^t)})$. Now X acts faithfully and irreducibly on A, so G is nonabelian and clearly $A = G'$, the commutator subgroup of G. It follows that $\chi(1) \neq 1$ and therefore Lemma 4.2 applies. In particular, $\chi(1) = p$ and we can assume that $\mathfrak{X}(x)$ and $\mathfrak{X}(a)$ are as described in that lemma. Furthermore, let ε be the primitive complex pth root of unity whose angle with the real axis is $2\pi/p$, and then use $\varepsilon_\ell = \varepsilon^\ell$ in the matrix P, for all $\ell = 1, 2, \ldots, p$.

Now Lemma 4.2(ii) implies that $P^{-1}\mathfrak{X}(x)P = D = \operatorname{diag}(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_p)$ and hence $T = \mathfrak{X}(u_{k,m}(x))$ satisfies $P^{-1}TP = \operatorname{diag}(u_{k,m}(\varepsilon_1), u_{k,m}(\varepsilon_2), \ldots, u_{k,m}(\varepsilon_p))$. In other words, we know the eigenvalues of T and, since $2 \leq k \leq p-2$, Lemma 3.4(ii)(iii) implies that there are precisely two of these that have largest absolute value, namely $u_{k,m}(\varepsilon_i)$ and $u_{k,m}(\varepsilon_{i'})$ with $i = 1$, $i' = p-1$, and $\varepsilon_{i'} = \bar{\varepsilon}_i$. Furthermore, there are precisely two of these that have smallest absolute value, namely $u_{k,m}(\varepsilon_j)$ and $u_{k,m}(\varepsilon_{j'})$ with $j \equiv k^{-1} \bmod p$, $j' \equiv -k^{-1} \bmod p$, and $\varepsilon_{j'} = \bar{\varepsilon}_j$. These therefore give rise to a T-decomposition $\mathbb{C}^p = V = T_+ \oplus T_0 \oplus T_-$ with $\dim T_+ = \dim T_- = 2$. Since $Q = P^{-1}$, the corresponding projections $\tau_+ \colon V \to T_+$ and $\tau_- \colon V \to T_-$ satisfy $\tau_+ = P(e_{i,i} + e_{i',i'})Q$ and $\tau_- = P(e_{j,j} + e_{j',j'})Q$.

Next, let $S = \mathfrak{X}(u_{k,m}(a^{-1}xa)) = \mathfrak{X}(a)^{-1}\mathfrak{X}(u_{k,m}(x))\mathfrak{X}(a)$. Since S is conjugate to T, it is clear that there is an S-decomposition $V = S_+ \oplus S_0 \oplus S_-$ with $\dim S_+ =$

$\dim S_- = 2$. Furthermore, the corresponding projections σ_+ and σ_- satisfy

$$\sigma_+ = \mathfrak{X}(a)^{-1}\tau_+\mathfrak{X}(a) = \mathfrak{X}(a)^{-1}P(e_{i,i} + e_{i',i'})Q\mathfrak{X}(a), \text{ and}$$
$$\sigma_- = \mathfrak{X}(a)^{-1}\tau_-\mathfrak{X}(a) = \mathfrak{X}(a)^{-1}P(e_{j,j} + e_{j',j'})Q\mathfrak{X}(a).$$

Our goal now is to apply Corollary 4.1 to S and T, and for this we need to verify the eight idempotent conditions, namely that the eight possible products all have rank 2. However, since P and $\mathfrak{X}(a)$ are unitary matrices and since $e_{i,i} + e_{i',i'}$ and $e_{j,j} + e_{j'.j'}$ are Hermetian, we see that $\sigma_\pm$ and $\tau_\pm$ are also Hermetian. In particular, $(\tau_\pm\sigma_\pm)^* = \sigma_\pm^*\tau_\pm^* = \sigma_\pm\tau_\pm$, so $\operatorname{rank}\tau_\pm\sigma_\pm = \operatorname{rank}\sigma_\pm\tau_\pm$. It follows that we need only check that the four products $\sigma_\pm\tau_\pm$ each have rank 2.

Next, since P, Q, $\mathfrak{X}(a)$ and $\mathfrak{X}(a)^{-1}$ are nonsingular matrices, we see that

$$\operatorname{rank}\sigma_\pm\tau_\pm = \operatorname{rank}(e_{r,r} + e_{r',r'})\cdot Q\mathfrak{X}(a)P\cdot(e_{s,s} + e_{s',s'}),$$

where $r = i$ or j and $s = i$ or j. Two of these cases are quite simple. Namely, if $r = s$, then Lemma 4.5(i) asserts that if these matrices do not have rank 2, then $\chi(a^{1+x}) = \chi(a^{1+x^d})$ for all $d = 1, 2, \ldots, p-1$, and this is a contradiction since we know that $\chi(a^{1+x}) \neq \chi(a^{1+x^t})$. Thus, only two cases remain. But observe that

$$[(e_{j,j} + e_{j',j'})\cdot Q\mathfrak{X}(a)P\cdot(e_{i,i} + e_{i',i'})]^*$$
$$= (e_{i,i} + e_{i',i'})\cdot Q\mathfrak{X}(a^{-1})P\cdot(e_{j,j} + e_{j',j'}),$$

and we know that both $\chi(a^{1+x}) \neq \chi(a^{1+x^t})$ and $\chi(a^{-(1+x)}) \neq \chi(a^{-(1+x^t)})$.

Thus, we need only consider the rank of

$$M = (e_{i,i} + e_{i',i'})\cdot Q\mathfrak{X}(a)P\cdot(e_{j,j} + e_{j',j'}),$$

since the other argument will be similar. Now if $\operatorname{rank} M \neq 2$, and if u is defined by $\varepsilon_j/\bar{\varepsilon}_i = (\varepsilon_j/\varepsilon_i)^u$, then Lemma 4.5(ii) asserts that $\chi(a^{1+x}) = \chi(a^{1+x^u})$. But, working with exponents modulo p, we have $\varepsilon_j/\bar{\varepsilon}_i = \varepsilon^{k^{-1}+1}$ and $\varepsilon_j/\varepsilon_i = \varepsilon^{k^{-1}-1}$, so $u(k^{-1} - 1) \equiv k^{-1} + 1 \bmod p$ and therefore $u \equiv (1 + k)/(1 - k) \equiv t \bmod p$. This is, of course, a contradiction by our choice of the parameters t and k.

It follows that all the idempotent conditions are verified and we conclude from Corollary 4.1 that, for some positive integer n, we have $\langle S^n, T^n\rangle = \langle S^n\rangle * \langle T^n\rangle$ is a free group of rank 2. Since $\mathfrak{X}(u_{k,m}(a^{-1}xa)^n) = S^n$ and $\mathfrak{X}(u_{k,m}(x)^n) = T^n$, Lemma 3.1(ii) implies that $u_{k,mn}(x^a) = u_{k,m}(x^a)^n$ and $u_{k,mn}(x) = u_{k,m}(x)^n$ generate a nonabelian free subgroup of the unit group of $\mathbb{Z}[G]$. □

We can now quickly prove our main result.

Theorem 4.7. *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 $\mathbb{Z}[G]$.*

Proof. We proceed by induction on $|G|$. Certainly, we can assume that all proper subgroups of G are abelian. Furthermore, suppose $\overline{G}$ is a proper homomorphic image of G that is nonabelian and, by induction, let $\bar{x}, \bar{y} \in \overline{G}$ be elements of prime power order such that $u_{k,m}(\bar{x})$ and $u_{r,s}(\bar{y})$ generate a nonabelian free group. By Lemma 3.2, there exist elements $x, y \in G$ of prime power order 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 the required free group of units in $\mathbb{Z}[G]$. Thus, we can now also assume that all proper homomorphic images

of G are abelian. It therefore follows from [M] that $G = A \rtimes X$, where X is cyclic of prime order p. Furthermore, either A is cyclic, 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 result now follows from the special cases already obtained in Lemmas 4.3 and 4.6. □

Note that some assumption on the primes dividing $|G|$ is required in the above because, as we have seen, there are no Bass cyclic units for 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.

References

[B] N. Bourbaki, *Elements of Mathematics, Commutative Algebra*, Hermann, Paris, 1972.

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

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

[J] N. Jacobson, *Basic Algebra II*, Freeman, San Francisco, 1980.

[M] 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.

[S] 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 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