FREE PAIRS OF SYMMETRIC ELEMENTS IN NORMAL SUBGROUPS OF DIVISION RINGS

JAIRO Z. GONÇALVES AND DONALD S. PASSMAN

ABSTRACT. Let D be a division ring with central subfield k of characteristic $\neq 2$, let * be a k-involution of D, and let $N \lhd D^\bullet$ be a normal subgroup of the multiplicative group $D^\bullet$ of D. We show that if G is a *-stable nonabelian subgroup of N that is either torsion-free polycyclic-by-finite but not abelian-by-finite, or finite of odd order, then N contains a pair (u, v) of elements such that $u^* = u$, $v^* = v$ and such that $\langle u, v\rangle$ is a noncyclic free group.

One aspect of the above proof requires that we extend a theorem of Bergman on invariant ideals in commutative group algebras. This new result is surely of interest in its own right. It appears in the Appendix and can be read independently of the remainder of the paper.

1. INTRODUCTION

Let D be a division ring with central subfield k of characteristic $\neq 2$, let $D^\bullet$ be its multiplicative group, and let * be a k-involution of D. In other words, * is a k-linear operator on D that is also an anti-automorphism of order 2. An element $u \in D^\bullet$ is said to be *symmetric* if $u^* = u$. Furthermore, if a pair (u, v) of symmetric elements of D generates a noncyclic free subgroup of $D^\bullet$, then we say that it is a *free symmetric pair*.

In [8], Lichtman posed the conjecture that the multiplicative group of a noncommutative division ring always contains a noncyclic free subgroup. In its support he proved [9]:

Theorem 1.1. *Let $N \lhd D^\bullet$ be a normal subgroup, and assume that $G \subseteq N$ with G a nonabelian nilpotent-by-finite group. Then N contains a noncyclic free subgroup.*

In the present work we obtain a more general and involutorial version of the above result, namely:

Theorem 1.2. *Let D be a division ring with central subfield k of characteristic $\neq 2$, and let * be a k-involution of D. Now suppose N is a normal subgroup of $D^\bullet$ that contains a nonabelian *-stable subgroup G that is either torsion-free polycyclic-by-finite but not abelian-by-finite, or is finite of odd order. Then N contains a free symmetric pair.*

Some very natural questions arise from the above statement. For example, in the first case, why do we require that G is not abelian-by-finite? Or in the second, why must the order of the finite group G be odd?

The first author's research was partially supported by FAPESP-Brazil, Proj. Temático 2015/009162-9 and by CNPq Grant 301.205/2015-9.

For the first question, our answer is just that we are not able to handle the case in which G is abelian-by-finite. In this situation the subalgebra kG is finite-dimensional over its center, which could be an algebraic number field, and the behavior of subgroups invariant under an involution is unknown to us in this context.

As for the second, we observe that in some cases where the order of the finite group G is even, N may not contain free symmetric pairs. For example, if G is the quaternion group of order 8 with the symplectic involution (the one with $\mathbf{i}^* = -\mathbf{i}$ and $\mathbf{j}^* = -\mathbf{j}$), then all symmetric elements of $D = \mathbb{Q}G$, the $\mathbb{Q}$-linear span of G, are central. In particular, there can be no free symmetric pairs here.

The outline of this paper is as follows. In the first section, we recall the notion of proto-specialization and some of its consequences. For example, it allows us to lift free groups from a division ring finite-dimensional over its center, to the group of units of a subring of the ring of fractions of a skew polynomial ring. Here we also present a criterion to produce free groups of matrices.

The next section studies when nonabelian torsion-free polycyclic-by-finite groups, that are not abelian-by-finite, have some special subgroups invariant under a given involution. We follow with a section dedicated to showing the existence of free symmetric pairs in division rings finite-dimensional over their centers. Finally, in the last section we prove our main theorem.

Because of its independent interest, we have placed our extension of Bergman's theorem in the appendix to this paper.

2. Proto-specializations

We start by recalling the concept of *proto-specialization*, introduced in [5]. Let D and $\overline{D}$ be division rings. By a *proto-specialization* from D to $\overline{D}$, we mean a homomorphism

$$\pi : T \to \overline{D}$$

from a subring T of D, such that $\pi(U(T)) = \overline{D}^\bullet$, where $U(T)$ denotes the group of units of T. We will sometimes write this proto-specialization as $\pi\colon D \to \overline{D}$ with the understanding that the true domain of π is a known subring of D. An immediate consequence of this definition is:

Lemma 2.1. *Suppose there exists a proto-specialization from D to $\overline{D}$. If $\overline{D}^\bullet$ contains a noncyclic free subgroup, then so does $D^\bullet$.*

Our goal is to find suitable proto-specializations from the field of fractions of a skew polynomial ring. The main tool for constructing such proto-specializations is:

Theorem 2.2. *Let Δ be a division ring with an automorphism τ and let $\Delta(Y;\tau)$ be the field of fractions of the skew polynomial ring $\Delta[Y;\tau]$. Assume that Δ contains a commutative subring R_0 having a prime ideal M_0, such that $\tau(R_0) = R_0$ and $\tau(M_0) = M_0$. Then there exists a proto-specialization from $\Delta(Y;\tau)$ to $\overline{S}(Y;\bar{\tau})$, where S is the localization of R_0 at the prime M_0, and $\overline{S} = S/M_0S$ is the quotient of this ring by the maximal ideal M_0S.*

Proof. See [5, Corollary 2.3]. □

Usually, we need a proto-specialization whose maximal ideal avoids finitely many elements of the domain. The result below helps in this task.

Proposition 2.3. *Let $f(x) \in \mathbb{Z}[x]$ be a nonconstant integral polynomial that is not the power of a linear polynomial, and let $\lambda_1, \lambda_2, \lambda_3, \dots$ be any increasing sequence of natural numbers. Then the set of prime factors of the members of the sequence $f(\lambda_1), f(\lambda_2), f(\lambda_3), \dots$ is infinite.*

Proof. This is a result of Siegel [15, pp. 204–205] or see [17, Theorem 7.2]. The special case where the λ_i are allowed to be all natural numbers is much easier, see [16, Lemma 1.5]. □

Finally, the next result gives the proto-specializations we are looking for. It is a corrected version of [5, Lemma 3.1] and contains additional information on involutions.

Proposition 2.4. *Let k be a prime field of characteristic $q \geq 0$ and let $G = A \rtimes \langle x \rangle$ be a semidirect product group, where $A \neq \langle 1 \rangle$ is a finitely generated free abelian group and $\langle x \rangle$ is infinite cyclic. Assume that x normalizes no nonidentity cyclic subgroup of A. If $D = k(G)$ is the field of fractions of the group algebra $k[G]$, then there exist infinitely many pairs (n, p), with infinitely many different p, such that $p \neq q$ is a prime, $K = k[\zeta]$ is the field extension of k generated by $\zeta \neq 1$, a p-th root of unity, and there exists a proto-specialization $\pi\colon D \to \overline{D} = K(X;\tau)$ where $\pi(A) = \langle \zeta \rangle$, $\pi(x) = X$ and $\zeta^X = \zeta^\tau = \zeta^n \neq \zeta$.*

Suppose further that * is an involution on G that stabilizes A and that k has characteristic $\neq 2$. Then we have:

i. *If either * is the identity on A, or $q = 0$ and * is the inverse map on A, then the kernel of the epimorphism $\pi\colon k[G] \to K[X, X^{-1}; \tau]$ is *-stable, so * can be defined on $K(X;\tau)$ in such a way that π intertwines the two involutions.*
ii. *Assume that $x^* = x^{-1}$, let R_0 be the subalgebra of *-symmetric elements of $k[A]$, and let $S_0 = \langle R_0, x, x^{-1} \rangle$, so that S_0 is a *-stable subalgebra of $k[G]$. If $D_0 \subseteq D$ is the field of fractions of S_0, then π determines a proto-specialization $\pi\colon D_0 \to \overline{D}_0 \subseteq \overline{D}$. Here $\pi(S_0) = K_0[X, X^{-1}; \tau_0]$ where $K_0 = k[\zeta]$ or $k[\zeta + \zeta^{-1}]$ and τ_0 acts nontrivially on K_0. Furthermore, the kernel of the epimorphism $\pi\colon S_0 \to K_0[X, X^{-1}; \tau_0]$ is *-stable, so * can be defined on $\overline{D}_0 = K_0(X;\tau_0)$ in such a way that π intertwines the two involutions.*

Proof. Let $a_1, a_2, \dots, a_r$ be a free generating set of A. Then x acts on A via the formulas

$$a_i^x = \prod_j a_j^{t_{ij}}$$

for suitable integers t_{ij} with $T = [t_{ij}] \in \mathrm{GL}_r(\mathbb{Z})$. Let $f(y) = \det(yI - T)$ be the characteristic polynomial of the matrix T. Then $f(y) \in \mathbb{Z}[y]$, $f(0) = \pm \det T = \pm 1$ since $T \in \mathrm{GL}_r(\mathbb{Z})$, $f(1) \neq 0$ and $f(-1) \neq 0$ since x normalizes no nonidentity cyclic subgroup of A, and $f(y)$ is not the power of a linear polynomial since the composition factors of x on $\mathbb{Q} \otimes A$ cannot all be linear.

Now $R = k[A]$ is isomorphic to the Laurent polynomial ring $k[a_1^{\pm}, a_2^{\pm}, \dots, a_r^{\pm}]$ and we will construct a homomorphism $\pi\colon R \to k[\zeta] = K$, where $\zeta \neq 1$ is an element of prime order p and where $\pi(a_i) = \zeta^{b_i}$. Here the $b_i \in \mathbb{Z}$, as well as the prime p, are to be determined. Of course, the exponents b_i need only be determined modulo p.

Next, we want to extend π to a homomorphism $\pi\colon k[A \rtimes \langle x \rangle] \to K[X, X^{-1}; \tau]$ by setting $\pi(x) = X$, and where $\zeta^X = \zeta^\tau = \zeta^n$ in the skew-Laurent polynomial

ring. Since the equation $x^{-1}a_i x = \prod_j a_j^{t_{ij}}$ maps to

$$\zeta^{nb_i} = X^{-1}\zeta^{b_i}X = \prod_j \zeta^{b_j t_{ij}}$$

we need

$$nb_i \equiv \sum_j t_{ij}b_j \mod p$$

for all i. Of course this is equivalent to the column vector

$$\beta = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_r \end{bmatrix}$$

being an eigenvector for $T \bmod p$ with eigenvalue n, that is $n\beta \equiv T\beta \bmod p$.

Furthermore, we have to ensure that the map $\zeta \to \zeta^n$ actually determines a field automorphism of $K = k[\zeta]$. In characteristic 0, since $k = \mathbb{Q}$ and the cyclotomic polynomial for p-th roots of unity is irreducible, it is clear that any integer n not divisible by p will work. On the other hand, when the characteristic is $q > 0$, then $k = \mathrm{GF}(q)$ and any q^s determines a field automorphism of K. Thus in this situation, we insist that $n = q^s$ for some $s = 1, 2, 3, \ldots$. In either case, we have an infinite number of possible choices for n.

We now apply Proposition 2.3 to the polynomial $f(y) \in \mathbb{Z}[y]$ and the sequence $\lambda_1, \lambda_2, \lambda_3, \ldots$ of natural numbers. Here $\lambda_i = i$ if $q = 0$ and $\lambda_i = q^i$ if $q > 0$. We conclude that the set of prime factors of the sequence $f(\lambda_1), f(\lambda_2), f(\lambda_3), \ldots$ is infinite. Note that $f(1), f(-1) \in \mathbb{Z}$ are nonzero so $f(1)$ and $f(-1)$ have only finitely many prime factors. By avoiding these, we obtain infinitely many pairs (n, p), with infinitely many primes p and with n appropriate, such that $f(n) \equiv 0 \bmod p$, $f(1) \not\equiv 0 \bmod p$ and $f(-1) \not\equiv 0 \bmod p$. Note that p does not divide n since otherwise $f(n) \equiv f(0) = \pm 1 \bmod p$.

Since $f(n) \equiv 0 \bmod p$, we see that n is an eigenvalue for the matrix $T \bmod p$ and hence there is a corresponding nonzero eigenvector β. As above, this allows us to construct the homomorphism $\pi\colon k[G] \to K[X, X^{-1}; \tau] \subseteq K(X; \tau)$. Since n is appropriate, we see that $\tau : \zeta \to \zeta^n$ determines a field automorphism of K. Furthermore, $n \not\equiv 1 \bmod p$ since otherwise $f(n) \equiv f(1) \bmod p$ and $p \mid f(1)$ contrary to our assumption. Thus τ is nontrivial on K. In addition, since β is nonzero modulo p, it follows that $\pi(A) = \langle \zeta \rangle$ and thus the image of $k[G]$ is $K[X, X^{-1}; \tau]$.

Now let P be the kernel of π in $k[G]$. Since the powers of $\pi(x) = X$ are linearly independent over the field $\pi(k[A]) = K$, it follows that $P = (P \cap k[A]) \cdot k[G]$. In addition, since $D = k(G)$ is the field of fractions of $k[G]$, it follows from [5, Corollary 2.3] that π extends to a proto-specialization $\pi\colon D \to \overline{D} = K(X; \tau)$.

Finally, suppose G admits an involution * that stabilizes A and, for each i, let $g_i(t) \in k[t]$ be the minimal monic polynomial of ζ^{b_i} over k, so that $g_i(t)$ is an irreducible divisor of $t^p - 1$. We note that $P \cap k[A]$ is generated by the elements $g_i(a_i)$ for $i = 1, 2, \ldots, r$ and the elements $a_i^{b_j} - a_j^{b_i}$ for all i, j. Here of course, $b_1, b_2, \ldots, b_r$ are the entries of β lifted to $\mathbb{Z}$. If * is the identity on A, then certainly $P \cap k[A]$ is *-stable. Furthermore, if * is the inverse map on A and if $q = 0$, then $g_i(t) = 1 + t + \cdots + t^{p-1}$ or $g_i(t) = t - 1$, so $g_i(t)$ and $g_i(t^{-1})$ are identical up to a factor of ± 1 and a power of t. With this, it is easy to check that $P \cap k[A]$ is again

a *-stable ideal of $k[A]$. Hence P is also *-stable, and thus * defines an involution on $k[G]/P = K[X, X^{-1}; \tau]$ and then on the field of fractions $K(X; \tau)$. Of course, π now intertwines these two involutions and (i) is satisfied.

For (ii), observe that since $R = k[A]$ is commutative, * acts as an automorphism of order 1 or 2. In particular, its set R_0 of *-fixed, that is *-symmetric, elements is a k-subalgebra, and R_0 is Noetherian by [14, Corollary 26.13(ii)] since k has characteristic different from 2. Furthermore, if $\alpha \in R_0$, then $x^{-1}\alpha x = x^*\alpha x$ is also *-symmetric. Thus x normalizes R_0 and hence $S_0 = \langle R_0, x, x^{-1}\rangle \subseteq k[G]$ is a skew Laurent polynomial ring over R_0 in the variables x and x^{-1}. It remains to find the image $\pi(S_0)$ and properties of the kernel $P_0 = \ker \pi \cap S_0$. Since X acts nontrivially on $\langle\zeta\rangle$, it is clear that p is odd.

For convenience, write $A_0 = \{a \in A \mid a^* = a\}$, $A_1 = \{a \in A \mid a^* = a^{-1}\}$ and $A_2 = \{a^2 \mid a \in A\}$, so that these are subgroups of A. Since $\pi(A) = \langle\zeta\rangle$ and p is odd, we have $\pi(A_2) = \langle\zeta\rangle$. Furthermore, since the square of every element of A is a product of a *-fixed element and a *-inverted element of A, it follows that $A_2 \subseteq A_0A_1$ so either $\pi(A_0) = \langle\zeta\rangle$ or $\pi(A_1) = \langle\zeta\rangle$. In particular, there exists a suitable element $a \in A_0$ or A_1 with $\pi(a) = \zeta$. Then $a + a^* \in R_0$ and $\pi(a + a^*) = 2\zeta$ or $\zeta + \zeta^{-1}$. But $|k[\zeta] : k[\zeta + \zeta^{-1}]| \leq 2$, so it follows that $\pi(R_0) = K_0 \subseteq K$ where $K_0 = k[\zeta]$ or $k[\zeta + \zeta^{-1}]$.

If X acts trivially on K_0, then $|K : K_0| = 2$ and $n^2 \equiv 1 \bmod p$. Thus $n \equiv \pm 1 \bmod p$, a contradiction since p divides $f(n)$ but not $f(1)$ or $f(-1)$. Finally, as above, we see that $P_0 = (P_0 \cap R_0)\cdot S_0$ and $P_0 \cap R_0$ is *-stable since * acts like the identity on R_0. Thus P_0 is also *-stable and therefore * can be defined on S_0/P_0 and on its field of fractions $\overline{D}_0 = K_0(X; \tau_0)$ in such a way that π intertwines the two involutions.

As usual π now determines a proto-specialization from the division ring $D_0 = R_0(x)$ by first localizing the commutative ring R_0 at its maximal ideal $P_0 \cap R_0$ to get R_0'. Then, since R_0' is Noetherian, we can localize the skew polynomial ring $R_0'[x]$ at the multiplicatively closed set $\mathcal{M}$ of its monic polynomials. In this way, we obtain the necessary *-stable subalgebra of D_0 that maps onto $\overline{D}_0$. □

It is clear from the proof of (i) above that the assumption $q = 0$ can be replaced by the weaker hypothesis that ζ and ζ^{-1} are Galois conjugate aver k. Indeed, in this case, ζ^{b_i} and ζ^{-b_i} are also Galois conjugate, so $g_i(t)$ and $g_i(t^{-1})$ are identical up to a factor of a power of t and a nonzero scalar, and this is all that is required.

The next two lemmas are tools, using valuations, to produce free groups.

Lemma 2.5. *Let $\mathbb{Q}$ be the field of rationals, and let $n > 1$ be an integer. Then there exist infinitely may primes l such that, if $\mathbb{Q}_l$ denotes the field of l-adic rationals with ν_l its l-adic valuation, then for any n-th root of unity $\varepsilon \in \mathbb{Q}_l$, there exist infinitely many integers $m \in \mathbb{Z}$ such that $\nu_l(m - \varepsilon) > 0$, while $\nu_l(m - \delta) = 0$ for all remaining n-th roots of unity $\delta \in \mathbb{Q}_l$.*

Proof. See [6, Lemma 2.2]. □

Lemma 2.6. *Let ν be a non-Archimedean valuation defined on a field F, let $m \geq 2$ be an integer, and let $u, v \in F^{m\times m}$ be invertible $m \times m$ matrices. Assume that:*

i. *u is a diagonal matrix and its diagonal has a unique entry with maximal ν-value and a unique entry with minimal ν-value.*
ii. *All the entries of v and v^{-1} have zero ν-value and, in particular, are not 0.*

Then the pair $(u, v^{-1}uv)$ generates a noncyclic free group.

Proof. See [4, Proposition 2.4]. □

3. Subgroups invariant under an involution

Let G be a group, and assume that * is an involution acting on G, namely * is an anti-automorphism of order 2. Recall that any such map * is the commuting product of a group automorphism σ of order 1 or 2 with the inverse map. We call σ the automorphism *associated* to * and we fix this notation throughout.

We first consider the behavior of a rather special finite nonabelian group under an involution.

Theorem 3.1. *Let G be a finite nonabelian group of odd order admitting an involution *, and assume that G is contained in the multiplicative group of a division ring. Then G has a *-stable nonabelian subgroup $H = X \rtimes Y$, where $X \lhd H$ is a subgroup of prime order p, and Y is a cyclic q-group for some prime $q \neq p$. Furthermore, $X = \langle x \rangle$, with $x^* = x$ or x^{-1}, and $Y = \langle y \rangle$ with $y^* = y^{-1}$.*

Proof. Since G is contained in the multiplicative group of a division ring, it follows that G has no abelian subgroup of type (p, p). Thus by [13, Proposition 9.5], since $|G|$ is odd, all Sylow p-subgroups of G are cyclic. In particular, G is a Z-group and hence (see [13, Lemma 12.9]) its commutator subgroup G' is cyclic. If G' is central in G, then G is nilpotent and hence abelian, since all Sylow subgroups of G are abelian. But this is not the case, so G' has a Sylow p-subgroup X_0 that is not central in G. Of course G' is cyclic, so X_0 is characteristic in G' and hence normal in G. Furthermore X_0 is *-stable.

Now, X_0 is not central, so there exists a Sylow q-subgroup Y_0 of G that does not centralize X_0. Since the subgroup X_0Y_0 is nonabelian, it cannot be a p-group and hence $p \neq q$. This implies (see [13, Proposition 9.3]) that Y_0 acts nontrivially on $X = \Omega_1(X_0)$, the unique subgroup of X_0 of order p. Note that X is characteristic in G and hence *-stable. Since $\operatorname{Aut} X$ has a unique element of order 2, it follows that $X = \langle x \rangle$ with $x^* = x$ or x^{-1}.

Now * permutes the Sylow q-subgroups of G and there are an odd number of these, since $|G|$ is odd. Thus * stabilizes some Sylow q-subgroup Y of G. If Y centralizes X, then $Y \subseteq \mathbb{C}_G(X) \lhd G$ and hence $Y_0 \subseteq \mathbb{C}_G(X)$, a contradiction. Thus Y acts nontrivially on X and we set $H = XY = X \rtimes Y$. Clearly H is nonabelian.

Since Y is *-stable, we have $Y = \langle y \rangle$ with $y^* = y$ or y^{-1}. We claim that $y^* = y^{-1}$. Indeed, suppose that $y^* = y$ and note that $y^{-1}xy = x^a$ implies that $y^{-1}x^*y = (x^*)^a$. Now applying * to $y^{-1}xy = x^a$ yields $y^*x^*(y^*)^{-1} = (x^*)^a$ so $yx^*y^{-1} = (x^*)^a = y^{-1}x^*y$. Thus y^2 commutes with $x^* = x$ or x^{-1}, and hence y commutes with x since q is odd, a contradiction.

On the other hand, both possibilities for x^* exist, since the map $x \mapsto x^{-1}, y \mapsto y$ determines an automorphism of H of order 2 and this automorphism followed by the inverse map yields an involution *. □

Now we move on to consider nilpotent groups with an involution. Our goal is to reduce such groups to *-stable Heisenberg subgroups. This will be achieved in Theorem 3.5.

Lemma 3.2. *Let G be a nilpotent group with an involution * and suppose $C \lhd G$ with G/C a nonidentity torsion-free abelian group. Then there exists $x \in G \setminus C$ with $x^* = x$ or x^{-1}.*

Proof. Suppose first that G is abelian and choose $x \in G \setminus C$. Set $y = xx^*$ and $z = x(x^*)^{-1}$. Then $y^* = y$ and $z^* = z^{-1}$. Thus the result will follow unless both y and z are contained in C. In this latter case $x^2 = yz \in C$ and this contradicts the fact that G/C is torsion free.

Now suppose that G is nilpotent. We proceed by induction on the nilpotence class of G. If G has class 1, then it is abelian and the result follows from the above. So assume G is nonabelian and let $G = G_0 \supseteq G_1 \supseteq G_2 \cdots \supseteq G_{n+1} = 1$ be the lower central series of G with $G_n \neq 1$. Since G/C is abelian, we see that $C \supseteq G' = G_1$. Note that all G_i are characteristic in G and hence *-stable.

By induction, the result holds in G/G_n with subgroup C/G_n. Thus there exists $y \in G \setminus C$ with $y^* \equiv y$ or y^{-1} modulo G_n. Set $H = \langle G_n, y\rangle$ so that H is *-stable. Also G_n is central in G, so H is abelian. Furthermore, since the powers of y are all in different cosets of C, and since $H \cap C \supseteq G_n$, it follows that $H \cap C = G_n$ and hence $H/G_n = H/(H \cap C)$ embeds in the torsion-free abelian group G/C.

By the abelian group result of the first paragraph, applied to the group H and subgroup $H \cap C$, there exists $x \in H \setminus (H \cap C)$ with $x^* = x$ or x^{-1}. Since $x \in G \setminus C$, the lemma is proved. □

Lemma 3.3. *Let G be a nilpotent group and let A be a torsion-free normal abelian subgroup. Then $G/\mathbb{C}_G(A)$ is torsion-free.*

Proof. If $x \in G$, then the nilpotence of G implies that x satisfies a polynomial of the form $(x-1)^r$ in its action on A, when A is viewed additively. On the other hand, if $x^s \in \mathbb{C}_G(A)$, then x satisfies the polynomial $x^s - 1$ in its action. Since A is torsion-free abelian, it follows that x satisfies the greatest common divisor of the two polynomials in $\mathbb{Q}[x]$, so x satisfies $x - 1$, and hence $x \in \mathbb{C}_G(A)$. □

Lemma 3.4. *Let G be a nonabelian torsion-free nilpotent group with involution *. Then G has a *-stable class 2 subgroup.*

Proof. Let $1 = Z_0 \subseteq Z_1 \subseteq \cdots \subseteq Z_m = G$ be the upper central series of G. These are characteristic subgroups and hence *-stable. Note that Z_1 is the center of G and hence is abelian, while $Z_m = G$ is nonabelian. Thus we can choose t maximal so that $A = Z_t$ is abelian. Then $H = Z_{t+1}$ is nonabelian and H/A is abelian.

Let $C = \mathbb{C}_H(A)$ so that $H \supseteq C \supseteq A$. If C is nonabelian, then $C' \subseteq A \subseteq \mathbb{Z}(C)$ so C is a *-stable class 2 group and we are done. Thus we can assume that C is abelian and hence we have $H > C$. The previous lemma implies that H/C is torsion-free abelian.

By Lemma 3.2, we can now choose $y \in H \setminus C$ with $y^* = y$ or y^{-1}. With this, we let $R = \{a \in A \mid a(y-1) = 0\} = \mathbb{C}_A(y)$. Since A and $\langle y\rangle$ are *-stable, so is R. Next, let $S = \{a \in A \mid a(y-1)^2 = 0\}$ so that $S/R = \mathbb{C}_{A/R}(y)$. Again S is *-stable and hence so is $W = \langle S, y\rangle$.

We claim that W has class 2. First, R is central in W and S/R is central in W/R, so $W/R = \langle S/R, y\rangle$ is abelian. Thus $W' \subseteq R \subseteq \mathbb{Z}(W)$ and W has class at most 2.

It remains to show that W is nonabelian. To this end, since G is nilpotent, we know that $A(y-1)^n = 0$ for some integer n, and we can assume that n is

minimal with this property. Since $y \notin C$ does not centralize A, $n \neq 1$, and hence $n \geq 2$. Now, observe that $A(y-1)^{n-2} \subseteq S$ and, by the minimality of n, we see that $A(y-1)^{n-2}$ is not contained in R. Thus $S > R$, so y does not centralize S and W is indeed nonabelian. Therefore W is the required *-stable class 2 subgroup of G. □

Let us recall that the group

$$H = \langle x, y \,|\, (x,y) = x^{-1}y^{-1}xy = z \neq 1, (x,z) = (y,z) = 1 \rangle$$

is called the *Heisenberg group*. We are now in position to prove:

Theorem 3.5. *Let G be a nonabelian torsion-free nilpotent group with involution *. Then G has a *-stable Heisenberg subgroup with $x^* = x$ or x^{-1}, $y^* = y$ or y^{-1}. Of course $z^* = z$ or z^{-1}.*

Proof. By the previous lemma, we can assume that G has class 2, and we set $Z = \mathbb{Z}(G)$. Choose $g \in G \setminus Z$ and set $A = \langle Z, g \rangle$. Then A is a normal torsion-free abelian subgroup of G, and so Lemma 3.3 implies that $G/\mathbb{C}_G(A)$ is torsion-free. Since $G > \mathbb{C}_G(A)$, Lemma 3.2 implies that there exists $x \in G \setminus \mathbb{C}_G(A)$ with $x^* = x$ or x^{-1}.

Since $x \notin Z$, we can repeat this process. In other words, $B = \langle Z, x \rangle$ is a normal torsion-free abelian subgroup of G, $G/\mathbb{C}_G(B)$ is nonidentity torsion-free abelian, and there exists $y \in G \setminus \mathbb{C}_G(B)$ with $y^* = y$ or y^{-1}. Set $z = (x,y)$ so that $1 \neq z \in Z$.

We claim that $H = \langle x, y, z \rangle$ is a Heisenberg group. First, x has infinite order modulo $\mathbb{C}_G(A) \supseteq Z$, so $\langle x, z \rangle$ is a free abelian group of rank 2 normalized by y. Also y has infinite order modulo $\mathbb{C}_G(B) \supseteq \langle x, z \rangle$, so H is the semidirect product of $\langle x, z \rangle$ by $\langle y \rangle$. Thus H is indeed a Heisenberg group with $\mathbb{Z}(H) = \langle z \rangle$. □

We now look for subgroups invariant under an involution * when G is a torsion-free polycyclic-by-finite group that is not abelian-by-finite.

Recall that a group is said to be *poly-Z* if it is poly-{infinite cyclic}. The following arguments are essentially due to Lorenz [10, Theorem 2.3] except that we deal with characteristic subgroups and elements that are fixed or inverted by *.

Suppose A is a finitely-generated free abelian normal subgroup of G. If $x \in G$, then conjugation by x is an automorphism of A, which can be viewed as an integral matrix acting on the rational vector space $V = \mathbb{Q} \otimes A$. The eigenvalues of x are the eigenvalues of its corresponding matrix. Specifically, these are the complex roots of the characteristic polynomial of the matrix.

Lemma 3.6. *Let G be a finitely generated group.*

i. *For each integer $n \geq 1$, G has only finitely many subgroups of index n.*
ii. *Any subgroup of finite index in G contains a characteristic subgroup of G of finite index.*

Proof. See [14, Lemma 19.2]. □

If G is a polycyclic-by-finite group, then as is well known, so are all subgroups and factor groups. In particular, all subgroups and factor groups are finitely generated.

Lemma 3.7. *If G is polycyclic-by-finite, then G has a characteristic poly-Z subgroup of finite index. Hence G has a characteristic torsion-free subgroup of finite index.*

Proof. We know that G has a poly-Z subgroup of finite index. Hence, by Lemma 3.6 and the fact (see [12, Lemma 10.2.4]) that subgroups of poly-Z groups are poly Z, G has a characteristic poly-Z subgroup of finite index. Of course, any such poly-Z subgroup is torsion free. □

Lemma 3.8. *Let G be a polycyclic-by-finite group and assume that every characteristic nilpotent subgroup of G is abelian-by-finite. Then G has characteristic subgroups $A \subseteq L$ where A is torsion-free abelian, L has finite index in G, and L/A is torsion-free abelian. Furthermore, if all the eigenvalues of the action of an element $x \in L$ on A are all roots of unity, then $x \in A$. In particular, A is self-centralizing in L.*

Proof. By Malcev's theorem, see [12, Theorem 12.1.5], G has a subgroup H of finite index whose commutator subgroup H' is nilpotent. In view of Lemmas 3.6 and 3.7, we can assume that H is characteristic in G and also poly-Z. Let F be the Fitting subgroup of H so that $F = \mathrm{Fit}(H)$ is the unique maximal normal nilpotent subgroup of H. Then F is characteristic in H and, in this situation, $F \supseteq H'$. By hypothesis, F is abelian-by-finite and hence F has a characteristic abelian subgroup A of finite index. Then H/A is finite-by-abelian since H/F is abelian. Now, by Lemma 3.7, H/A has a characteristic torsion-free subgroup L/A of finite index and note that $L \cap F = A$ since F/A is finite. If $W = \mathrm{Fit}(L)$, then W is a characteristic nilpotent subgroup of H. Hence $W \subseteq F$, so $W \subseteq F \cap L = A$ and $\mathrm{Fit}(L) = A$.

Finally, suppose $x \in L$ has only roots of unity as eigenvalues in its action on A. Then for some integer $n \geq 1$, all the eigenvalues of $y = x^n$ are equal 1. Thus conjugation by y satisfies the characteristic equation $(y-1)^m = 0$ and it follows that the group $B = \langle A, y \rangle$ is nilpotent. But L/A is abelian, so $B \lhd L$ and hence $B \subseteq \mathrm{Fit}(L) = A$. In other words, $y = x^n \in A$ and since L/A is torsion free, we see that $x \in A$, as required. Of course, if x centralizes A then all its eigenvalues are equal to 1, and hence $x \in A$. □

We continue with the hypotheses and notation of the preceding lemma. Furthermore, σ will be the automorphism of G associated with *.

Lemma 3.9. *There exist characteristic subgroups $B \subseteq M$ with $B \subseteq A$ and A/B finite, $M \subseteq L$ with L/M finite and M/B torsion-free. Furthermore*

i. *If $x \in M$ with $x^\sigma \equiv x \pmod{B}$, then there exists $y \in L$ with $y \equiv x \pmod{A}$ and $y^\sigma = y$.*
ii. *If $x \in M$ with $x^\sigma \equiv x^{-1} \pmod{B}$, then there exists $y \in L$ with $y \equiv x \pmod{A}$ and $y^\sigma = y^{-1}$.*

Proof. Let $B = A^2 = \{a^2 \mid a \in A\}$. Then B is certainly characteristic in A and A/B is finite. Now note that L/B is finite-by-abelian since L/A is abelian. By Lemmas 3.6 and 3.7, L/B has a characteristic torsion-free subgroup M/B of finite index. Thus M is characteristic in G, L/M is finite and $M \cap A = B$, since M/B is torsion-free and A/B is finite. Of course $M/B = M/(M \cap A)$ embeds in the abelian group L/A.

(i.) Now let $x \in M$ with $x^\sigma \equiv x \pmod{B}$. Since $B = A^2$, we have $x^\sigma = xa^2$ for some $a \in A$. Now, $\sigma^2 = 1$, so

$$x = (x^\sigma)^\sigma = (xa^2)^\sigma = xa^2(a^2)^\sigma.$$

Thus $1 = a^2(a^2)^\sigma = (aa^\sigma)^2$ and, since A is torsion-free, we have $aa^\sigma = 1$. Finally, set $y = xa \equiv x \pmod{A}$. Then

$$y^\sigma = (xa)^\sigma = x^\sigma a^\sigma = xa^2a^\sigma = xa = y$$

as required.

(ii.) On the other hand, suppose $x \in M$ with $x^\sigma \equiv x^{-1} \pmod{B}$. Again $x^\sigma = x^{-1}a^2$ for some $a \in A$ and since $\sigma^2 = 1$, we have

$$x = (x^\sigma)^\sigma = (x^{-1}a^2)^\sigma = (a^{-2}x)(a^2)^\sigma.$$

Thus $1 = (x^{-1}a^{-2}x)(a^2)^\sigma = (x^{-1}a^{-1}xa^\sigma)^2$ and since A is torsion-free, we have $x^{-1}a^{-1}xa^\sigma = 1$, so $x^{-1}ax = a^\sigma$ and $x^{-1}a = a^\sigma x^{-1}$. Finally, set $y = xa^{-\sigma} \equiv x \pmod{A}$. Then

$$y^\sigma = x^\sigma a^{-1} = (x^{-1}a^2)a^{-1} = x^{-1}a = a^\sigma x^{-1} = y^{-1}$$

and the lemma is proved. □

Lemma 3.10. *Assume that G is not abelian-by-finite. Then L/A, M/B, A and B are all infinite abelian.*

Proof. Since L and M have finite index in G, neither is abelian. Thus $A \neq 1$ and $B \neq 1$ and, being torsion-free, these groups are infinite abelian. Also L and M cannot be abelian-by-finite, so L/A and M/B are infinite abelian. □

Finally we obtain our main result on polycyclic-by-finite groups that admit an involution.

Theorem 3.11. *Let G be a polycyclic-by-finite group that admits an involution *. Assume that every characteristic nilpotent subgroup of G is abelian-by-finite, but G is not abelian-by-finite. Then G has a *-stable subgroup $H = A \rtimes X$, where A is a *-stable finitely generated free abelian group of rank ≥ 2, and where $X = \langle x \rangle$ is a *-stable infinite cyclic group that acts faithfully on A by conjugation. In addition, we have one of the following:*

i. *$x^* = x$ or x^{-1}, and X and all its subgroups of finite index act irreducibly on the rational module $\mathbb{Q} \otimes A$. Furthermore, if $x^* = x^{-1}$, then * on A is either the identity map or the inverse map.*
ii. *$x^* = x$, and $A = A_1 \oplus A_2$ is the direct product of the X-stable subgroups A_1 and $A_1^\sigma = A_2$. Furthermore for each subgroup X_0 of finite index in X, the rational X_0-modules $\mathbb{Q} \otimes A_1$ and $\mathbb{Q} \otimes A_2$ are irreducible and not isomorphic.*

Proof. We use the notation of the preceding three lemmas and obtain a number of immediate consequences. First, by Lemma 3.8, G has nonidentity characteristic subgroups $A \subseteq L$, where A and L/A are infinite torsion-free abelian groups and hence free abelian of finite rank. Next, G has characteristic subgroups $B \subseteq M$ with M/B infinite abelian. As usual, let σ be the automorphism of G associated with *. Then σ acts on M/B and $\sigma^2 = 1$, so there exists an element $z \in M \setminus B$ with $z^\sigma \equiv z^{\pm 1} \bmod B$. Hence, by Lemma 3.9, there exists an element $x \in L$ having infinite order modulo A and with $x^\sigma = x$ or x^{-1}. Thus $X = \langle x \rangle$ is infinite cyclic and acts faithfully on A. Indeed, by Lemma 3.8, the eigenvalues of x in its action on the additive finite-dimensional vector space $V = \mathbb{Q} \otimes A$ cannot all be roots of unity. In particular, A has rank ≥ 2. We split the argument into two cases.

(i) Let us suppose first that $x^\sigma = x$ and note that for all $n \geq 1$, x^n is also fixed by σ and x^n has infinite order modulo A. Thus we are free below to replace x by x^n and deal with the same structure.

Now let $\chi(t)$ be the characteristic polynomial of the conjugation action of x on V and let ε be an eigenvalue of x that is not a root of unity. Consider the algebraic number field $\mathbb{Q}[\varepsilon]$. If x is replaced by x^m and ε by ε^m, then $\mathbb{Q}[\varepsilon^m] \subseteq \mathbb{Q}[\varepsilon]$. Thus, we can now choose m so that the field generated by ε^m is minimal. When we do this, then $\mathbb{Q}[\varepsilon^n] = \mathbb{Q}[\varepsilon]$ for all $n \geq 1$.

We continue considering x and ε as above. Let $f(t)$ be the irreducible factor of the characteristic polynomial $\chi(t)$ with $f(\varepsilon) = 0$, and note that $\mathbb{Q}[t]/(f(t)) \cong \mathbb{Q}[\varepsilon]$. Now, let $W \subseteq V$ be the subspace of vectors in V annihilated by $f(x)$. In other words $W = \{w \in V \mid w^{f(x)} = 0\}$. Then W is a nonzero $\mathbb{Q}$-subspace of V, and W is σ-stable, since σ commutes with x.

Next, at least one of $W_+ = \{w \in W \mid w^\sigma = +w\}$ or $W_- = \{w \in W \mid w^\sigma = -w\}$ is a nonzero subspace of W, and call this one U. Since x commutes with σ, x also acts on U. Indeed, $U^{f(x)} = 0$, so x acts like its image in $\mathbb{Q}[t]/(f(t)) = \mathbb{Q}[\varepsilon]$. In other words, U is a vector space over the field $\mathbb{Q}[\varepsilon]$, and therefore it has a 1-dimensional subspace U_0. Note that x acts on $C = U_0 \cap A$ and that $\mathbb{Q} \otimes C = U_0$. Since $\mathbb{Q} \otimes C$ is 1-dimensional over $\mathbb{Q}[\varepsilon]$ and since $\mathbb{Q}[\varepsilon^n] = \mathbb{Q}[\varepsilon]$, it follows that C is rationally irreducible over $\langle x^n \rangle$ for all $n \geq 1$. Furthermore, since σ acts like $+1$ or -1 on U, it is clear that U_0 and C are σ-stable and hence *-stable. Thus G has a *-stable subgroup $H = C \rtimes X$ satisfying condition (i) above.

(ii) Suppose now that $x^\sigma = x^{-1}$ so $x^* = x$. Again we are free to replace x by any x^m and obtain a similar structure. As above, we let ε be an eigenvalue of x that is not a root of unity, and by suitably replacing x by x^m and ε by ε^m, we can assume that $\mathbb{Q}[\varepsilon^n] = \mathbb{Q}[\varepsilon]$ for all $n \geq 1$.

Let $f(t)$ be the irreducible factor of the characteristic polynomial $\chi(t)$ of x with $f(\varepsilon) = 0$ and let $W \subseteq V$ be the set of all $w \in V$ with $w^{f(x)} = 0$. Then W is a nonzero subspace of V, and W is a vector space over the field $\mathbb{Q}[\varepsilon]$. Since $x^\sigma = x^{-1}$, there is no reason to believe that W is σ-stable. Nevertheless, we can still choose $U_1 \subseteq W$ to be a 1-dimensional $\mathbb{Q}[\varepsilon]$-subspace of W, and set $C_1 = U_1 \cap A$. Then $\mathbb{Q} \otimes C_1 = U_1$ is 1-dimensional over $\mathbb{Q}[\varepsilon]$, and since $\mathbb{Q}[\varepsilon^n] = \mathbb{Q}[\varepsilon]$, it follows that C_1 is rationally irreducible as an $\langle x^n \rangle$-module for all $n \geq 1$.

Let $U_2 = U_1^\sigma$. Since X normalizes U_1, it follows that $X^\sigma = X$ normalizes U_2. Indeed, if $u_1 \in U_1$, then

$$(u_1^\sigma)^x = (u_1^\sigma)^{(x^{-1})^\sigma} = (u_1^{x^{-1}})^\sigma$$

so x acts on U_2 as x^{-1} does on U_1, namely with eigenvalue ε^{-1}. Note that both U_1 and U_2 are rationally irreducible X-modules, so it follows that either $U_1 = U_2$ or $U_1 \cap U_2 = 0$. In the former case, U_1 and hence C_1 are σ-stable. So again, $H = C_1 \rtimes X$ is a subgroup of G satisfying (i) above. Thus we can assume that $U_1 \cap U_2 = 0$.

Now let $C_2 = U_2 \cap A = U_1^\sigma \cap A = C_1^\sigma$ and set $U = U_1 \oplus U_2$ and $C = C_1 \oplus C_2$. Then clearly

$$\mathbb{Q} \otimes C = \mathbb{Q} \otimes C_1 \oplus \mathbb{Q} \otimes C_2 = U_1 \oplus U_2 = U.$$

Furthermore, C is σ-stable, σ permutes C_1 and C_2, and each of these subgroups is a rationally irreducible $\langle x^n \rangle$-module for all $n \geq 1$. If the corresponding modules U_1

and U_2 are never isomorphic, then $H = C \rtimes X$ is a $*$-stable subgroup of G satisfying condition (ii) above.

It remains to consider the possibility that for some $n \geq 1$, U_1 and U_2 are isomorphic $\langle x^n \rangle$-modules. As usual, we can replace x by x^n and assume that U_1 and U_2 are isomorphic X-modules. Since $f(t)$ is the minimal polynomial for the action of x on U_1, the isomorphism assumption implies that it is also the minimal polynomial for the action of x on U_2. Thus $f(\varepsilon^{-1}) = 0$ and therefore ε and ε^{-1} are Galois conjugate. In other words, there exists a field automorphism τ of $\mathbb{Q}[\varepsilon]$ with $\varepsilon^\tau = \varepsilon^{-1}$, and clearly $\tau^2 = 1$. Furthermore, since $U_1 = v\mathbb{Q}[\varepsilon]$ is a 1-dimensional $\mathbb{Q}[\varepsilon]$-vector space, we can extend τ to act on U_1 by $(v\alpha)^\tau = v\alpha^\tau$ for all $\alpha \in \mathbb{Q}[\varepsilon]$. Note that for all $u_1 = v\alpha \in U_1$, we have

$$(u_1^x)^\tau = (v\alpha\varepsilon)^\tau = v\alpha^\tau\varepsilon^\tau = (v\alpha)^\tau\varepsilon^{-1} = (u_1^\tau)^{x^{-1}}.$$

Now define the additive map $\theta\colon U_1 \to U = U_1 \oplus U_1^\sigma$ by $\theta(u_1) = u_1 \oplus (u_1^\tau)^\sigma$. Then

$$\begin{aligned}\theta(u_1^x) &= u_1^x \oplus (u_1^x)^{\tau\sigma} = u_1^x \oplus (u_1^\tau)^{x^{-1}\sigma} \\ &= u_1^x \oplus (u_1^\tau)^{\sigma x} = \theta(u_1)^x,\end{aligned}$$

so θ is an X-module homomorphism, which is clearly an isomorphism into U. Furthermore, since $\sigma^2 = 1$ and $\tau^2 = 1$, we have

$$\begin{aligned}\theta(u_1^\tau) &= u_1^\tau \oplus (u_1^\tau)^{\tau\sigma} = u_1^\tau \oplus u_1^\sigma \\ &= (u_1 \oplus u_1^{\tau\sigma})^\sigma = \theta(u_1)^\sigma.\end{aligned}$$

Thus $\theta(U_1)$ is a σ-stable rational X-module that is X-isomorphic to U_1. Hence if we set $E = \theta(U_1) \cap A$, then $H = E \rtimes X$ is a *-stable subgroup of G that satisfies (i) above. This completes the proof. □

Lorenz's goal in [10] was to show that a certain group G contained a free subsemigroup on two generators. Unfortunately, we cannot just quote that result directly because we need to know that the element $1 \neq a \in A$ can be chosen arbitrarily and we also need to know exact expressions for the free generators. Thus it is necessary for us to cite parts of the proof of [10, Theorem 2.3]. The following lemma gives us precisely what we need.

Lemma 3.12. *Let $G = A \rtimes X$ be a semidirect product group, where A is a finitely generated free abelian group and where $X = \langle x \rangle$ is infinite cyclic. Assume that $A = A_1 \oplus A_2 \oplus \cdots \oplus A_n$, where each A_i is X-stable and where each subgroup X_0 of finite index in X acts irreducibly and nontrivially on the rational module $\mathbb{Q} \otimes A_i$. Now let $1 \neq a \in A$ be arbitrary. Then by replacing x by a suitable power if necessary, the elements x and ax generate a free subsemigroup of G.*

Proof. As usual we are free to replace x by any nonidentity power and obtain the same structure. We assume first that $n = 1$ so that $A = A_1$.

Let $f(\zeta) \in \mathbb{Q}[\zeta]$ be the minimal polynomial for the conjugation action of x on A. Since $\mathbb{Q} \otimes A$ is a rationally irreducible X-module, it is clear that $f(\zeta)$ is irreducible. If the complex roots of $f(\zeta)$ are all roots of unity, then some nonidentity power of x has fixed points on A and then acts trivially on the irreducible module, a contradiction. It then follows as in Step 2 of the proof of [10, Theorem 2.3], that by replacing x by a suitable power if necessary, we can assume that $f(\zeta)$ has at least one complex root ε with $|\varepsilon| > 2$.

Now x acts on $\mathbb{Q}\otimes A$ as does the image ε of ζ in $\mathbb{Q}[\zeta]/(f(\zeta)) \simeq \mathbb{Q}[\varepsilon]$. Furthermore, $Q \otimes A$ is a vector space over the field $\mathbb{Q}[\varepsilon]$ and since this module is irreducible, we see that $\mathbb{Q} \otimes A$ is 1-dimensional over $\mathbb{Q}[\varepsilon]$. Thus since $1 \neq a \in A$, we have, in additive notation, $\mathbb{Q} \otimes A = a\mathbb{Q}[\varepsilon]$. It follows, again in additive notation, that x acts on a via multiplication by ε and then Step 2 of the proof of [10, Theorem 2.3] shows that the subsemigroup of G generated by x and ax is indeed free of rank 2.

Finally suppose n is arbitrary and write $a = a_1 \oplus a_2 \oplus \cdots \oplus a_n$ in terms of its components. Since $a \neq 1$, at least one of these components is also a nonidentity element, say a_n. If we set $B = A_1 \oplus \cdots \oplus A_{n-1}$, then $B \lhd G$ and $\overline{G} = G/B$ is isomorphic to $A_n \rtimes X$. By the $n = 1$ case, replacing x by a suitable power if necessary, we know that $\bar{x}$ and $\overline{ax} = \bar{a}\bar{x} = \bar{a}_n\bar{x}$ generate a free subsemigroup of $\overline{G}$. Thus x and ax generate a free subsemigroup of G, as required. □

We will apply Lorenz's free subsemigroup result above by using the following surprisingly easy computations.

Lemma 3.13. *Let D be a division ring with involution * and prime subfield k. Furthermore, let G be a subgroup of N, a *-stable normal subgroup of $D^\bullet$. Suppose $a, x \in G$ with $a^* = a$, $x^* = x$, and such that x and ax generate a free subsemigroup of G. If the group algebra $k[G]$ is naturally embedded in D, then N contains a free symmetric pair.*

Proof. Since x and ax generate a free subsemigroup of G, the same is clearly true of x and $x(ax) = xax$, and then of $x(xax) = x^2ax$ and $(xax)x = xax^2$. Thus since $k[G]$ embeds in D, we see that $k\langle x^2ax, xax^2\rangle$ is a free subalgebra of D with the two free generators x^2ax and xax^2. It now follows from Magnus' theorem (see [11, Theorem 5.6]) that $u = 1 + x^2ax$ and $v = 1 + xax^2$ generate a free subgroup of $D^\bullet$ of rank 2.

Now notice that $x^{-1}ux = v$ and $xvx^{-1} = u$. Thus since $x, x^{-1} \in N \lhd D^\bullet$, it follows that the commutators

$$u^{-1}v = u^{-1}(x^{-1}ux) = (u^{-1}x^{-1}u)x$$

and

$$v^{-1}u = v^{-1}(xvx^{-1}) = (v^{-1}xv)x^{-1}$$

both belong to N.

Furthermore, since $a^* = a$ and $x^* = x$, we see that $u^* = v$ and $v^* = u$. Thus $N^* = N$ implies that

$$\alpha = (u^{-1}v)(u^{-1}v)^* = u^{-1}vuv^{-1}$$

and

$$\beta = (v^{-1}u)(v^{-1}u)^* = v^{-1}uvu^{-1}$$

are *-symmetric elements of $N \cap \langle u, v\rangle$. Next, notice that α and β do not commute since

$$\alpha\beta = u^{-1}vuv^{-1}{\cdot}v^{-1}uvu^{-1}$$

and

$$\beta\alpha = v^{-1}uvu^{-1}{\cdot}u^{-1}vuv^{-1}$$

are distinct reduced words in the free group $\langle u, v\rangle$.

Finally, we note that $\langle \alpha, \beta\rangle$ is a subgroup of the free group $\langle u, v\rangle$, so $\langle \alpha, \beta\rangle$ is also free. Indeed, since α and β do not commute, α and β are free generators of the

nonabelian free group $\langle \alpha, \beta \rangle$ of rank 2. Thus (α, β) is the required free symmetric pair contained in N. □

4. The finite dimensional case

Let $B = \{e_1, \ldots, e_n\}$ be a basis for an algebra $\mathfrak{A}$ over a field F. Then every $a \in \mathfrak{A}$ can be written uniquely as $\sum_{i=1}^{n} \alpha_i e_i$ with $\alpha_i \in F$, and we call the α_i the *B-coefficients* of a. If all such B-coefficients are nonzero, then we say that a has *full support* with respect to B. We start with an example of interest. Note that the elements α or β below, but of course not both, are allowed to equal 1.

Lemma 4.1. *Let $\mathfrak{A} = k(X)$ be the rational function field in the indeterminate X over the field k of characteristic $\neq 2$. Let $n \geq 1$ be a fixed integer and set $y = X^n$ and $F = k(y) = k(X^n)$. Then $\mathfrak{A}$ is a finite-dimensional algebra over F with basis $B = \{1, X, \ldots, X^{n-1}\}$. Now let α and β be distinct nonnegative powers of y, with $\alpha \neq \beta^{n+1} y$ and $\beta \neq \alpha^{n+1} y$, and set $w = (1 - \alpha X)(1 - \beta X)^{-1} \in \mathfrak{A}$.*

i. *The elements w, w^2, w^{-1} and w^{-2} all have full support with respect to B.*
ii. *Let $\alpha = y^a$, $\beta = y^b$ and $c = \max\{a, b\}$. Then all the B-coefficients of w and w^{-1} in $k(y)$ have numerator and denominator degrees at most $cn + 1$. Furthermore, the B-coefficients of w^2 and w^{-2} in $k(y)$ have numerator and denominator degrees at most $2(cn + 1)$.*
iii. *If * is the k-involution defined on $\mathfrak{A}$ by $X^* = X^{-1}$, then * inverts y, α and β. It follows that $w^* = (\beta\alpha^{-1})w$, so w^*, $(w^*)^{-1}$, ww^* and $(ww^*)^{-1}$ all have full support with respect to B.*

Proof. The comments on F and the basis B are clear. Furthermore, since $n \geq 1$ and since α and β are distinct powers of y, we have $\alpha, \beta, y \in F$, $\alpha \neq \beta$ and $\alpha\beta^{n-1} y \neq 1$. There is of course nothing to prove when $n = 1$, so we can assume that $n \geq 2$.

(i) Now $X^n = y$ and

$$(1 - \beta X)(1 + \beta X + \cdots + \beta^{n-1} X^{n-1}) = 1 - \beta^n X^n = 1 - \beta^n y,$$

so we have

$$\begin{aligned} w &= (1 - \beta^n y)^{-1}(1 - \alpha X)(1 + \beta X + \cdots + \beta^{n-1} X^{n-1}) \\ &= (1 - \beta^n y)^{-1}[1 + \beta X + \cdots + \beta^{n-1} X^{n-1} \\ &\qquad - \alpha X - \alpha\beta X^2 - \cdots - \alpha\beta^{n-2} X^{n-1} - \alpha\beta^{n-1} y] \\ &= \frac{\beta - \alpha}{1 - \beta^n y} \left[\frac{1 - \alpha\beta^{n-1} y}{\beta - \alpha} + X + \beta X^2 + \cdots + \beta^{n-2} X^{n-1} \right]. \end{aligned}$$

This describes $w \in \mathfrak{A}$ in terms of the B-basis and shows that it has full support.

For convenience, set

$$\delta = \frac{\beta - \alpha}{1 - \beta^n y} \qquad \text{and} \qquad \gamma = \frac{1 - \alpha\beta^{n-1} y}{\beta - \alpha},$$

both nonzero elements of F. Then we can write

$$\frac{w}{\delta} = \gamma + X + \beta X^2 + \cdots + \beta^{n-2} X^{n-1}$$

and hence

$$\frac{w^2}{\delta^2} = \gamma^2 + 2\gamma \sum_{i=1}^{n-1} \beta^{i-1} X^i + \sum_{i,j=1}^{n-1} \beta^{i+j-2} X^{i+j}.$$

We describe this element in terms of the basis B. First, if d_0 denotes the coefficient of X^0, then $d_0 = \gamma^2 + (n-1)\beta^{n-2}y$ and

$$\begin{aligned}(\beta-\alpha)^2 d_0 &= (\beta-\alpha)^2(\gamma^2 + (n-1)\beta^{n-2}y)\\ &= (1-\alpha\beta^{n-1}y)^2 + (n-1)(\beta-\alpha)^2\beta^{n-2}y.\end{aligned}$$

It follows that $d_0 \neq 0$ since X divides y so the constant term of the above polynomial is equal to 1.

Next, if d_r denotes the coefficient of X^r of the element w^2/δ^2, for $1 \leq r \leq n-1$, then

$$d_r = 2\gamma\beta^{r-1} + (r-1)\beta^{r-2} + (n-r-1)\beta^{n+r-2}y$$

and hence

$$\begin{aligned}(\beta-\alpha)d_r &= (\beta-\alpha)[2\gamma\beta^{r-1} + (r-1)\beta^{r-2} + (n-r-1)\beta^{n+r-2}y]\\ &= 2(1-\alpha\beta^{n-1}y)\beta^{r-1} + (r-1)(\beta-\alpha)\beta^{r-2}\\ &\qquad + (n-r-1)(\beta-\alpha)\beta^{n+r-2}y.\end{aligned}$$

Thus $(\beta-\alpha)d_r$ is a polynomial in y and hence in X. For convenience, write $e_r = (\beta-\alpha)d_r/\beta^{r-2}$ so that

$$e_r = 2(1-\alpha\beta^{n-1}y)\beta + (r-1)(\beta-\alpha) + (n-r-1)(\beta-\alpha)\beta^n y,$$

again a polynomial in y.

Now suppose by way of contradiction that $d_r = 0$, so $e_r = 0$. Since $\alpha \neq \beta$ and $\alpha \neq \beta^{n+1}y$, by assumption, it follows that the coefficient of α in e_r is $1 - r = 0$. Furthermore, since $\beta \neq \alpha$, the coefficient of β in e_r is $2 + (r-1) = 0$. Thus $2 = 0$ in k, which contradicts the assumption that k has characteristic different from 2.

Consequently $d_r \neq 0$ for all r and we conclude that w^2 has full support with respect to B. Finally, by interchanging α and β, we see that w^{-1} and w^{-2} also have full support with respect to B.

(ii) Since

$$(1-\beta^n y)w = (1-\alpha\beta^{n-1}y) + (\beta-\alpha)[X + \beta X^2 + \cdots + \beta^{n-2}X^{n-1}]$$

we see that each B-coefficient of w is a ratio of polynomials in y each of degree at most $nc+1$. Furthermore, the term $\alpha\beta^{n-1}y$ has degree strictly larger than all other terms on the right-hand side. Thus, when we square both sides and take into account the additional factor of $y = X^n$ when $[X + \beta X^2 + \cdots + \beta^{n-2}X^{n-1}]$ is squared, we see that each B-coefficient of w^2 is a ratio of polynomials in y each of degree at most $2(nc+1)$. Again, interchanging α and β yields the corresponding facts for w^{-1} and w^{-2}.

(iii) Since α, β and y are powers of X, it follows that * inverts each of these. Thus

$$\frac{\alpha}{\beta}\, w^* = \frac{\alpha}{\beta}\frac{(1-\alpha^{-1}X^{-1})}{(1-\beta^{-1}X^{-1})} = \frac{\alpha X - 1}{\beta X - 1} = w.$$

Since β/α is a nonzero element of the field F, the observations concerning the elements w^*, $(w^*)^{-1}$, ww^* and $(ww^*)^{-1}$ are immediate consequences of (i). □

Next, we need

Lemma 4.2. *Let k be a prime field of characteristic $q \geq 0$ and let $K = k[\zeta]$ be the extension field generated by a nonidentity root of unity ζ. If the positive integer m is given, then there exists an irreducible polynomial $f(y) \in K[y]$ of degree $\geq m$*

such that $f(y)$ divides the polynomial $1-\zeta y^t \in K[y]$ for some positive integer t not divisible by q.

Proof. Suppose first that k has characteristic 0 so that $k=\mathbb{Q}$, and let ζ have multiplicative order rp^s for some prime power $p^s>1$ and p'-integer r. For any integer $a\geq 1$ let μ be a complex primitive p^a-th root of unity. Since $|k[\mu]:k| = p^{a-1}(p-1)$, we can choose $a>s$ so that $|K[\mu]:K|\geq m$. Now let η generate the cyclic group $\langle \mu,\zeta\rangle$ so that η has multiplicative order rp^a. Since $K[\mu]=K[\eta]$, the minimal polynomial $f(y)\in K[y]$ of η over K is irreducible of degree $|K[\mu]:K|\geq m$. Furthermore, $\zeta\in\langle\eta\rangle$, so that $\zeta^{-1}=\eta^t$ for some positive integer t. Thus η satisfies $1-\zeta y^t\in K[y]$ and hence this polynomial is divisible by $f(y)$.

Now let k have characteristic $q>0$ so that $k=\mathrm{GF}(q)$ and $K=k[\zeta]=\mathrm{GF}(q^a)$ for some $a\geq 1$. Consider the field $F=\mathrm{GF}(q^{ma})$ with $|F:K|=m$, and let η generate the cyclic group $F^\bullet$. Then $F=K[\eta]$, so $f(y)\in K[y]$, the minimal polynomial of η over K, is irreducible of degree m. Furthermore, since $\zeta\in\langle\eta\rangle$, we see that $\zeta^{-1}=\eta^t$ for some positive integer t dividing $|F^\bullet|$ and hence not divisible by q. Again, we see that η satisfies $1-\zeta y^t\in K[y]$ and hence this polynomial is divisible by $f(y)$. □

In addition, we need the following quaternion freeness result.

Proposition 4.3. *Let $k\subseteq K=k[\omega]$ be fields of characteristic $\neq 2$ with $\omega^2\neq 0,\pm 1$, and let τ be a k-automorphism of K with $\omega^\tau=-\omega$. Define $D=K(X;\tau)$ to be the field of fractions of the skew polynomial ring $K[X;\tau]$ and let * be a k-involution of D that satisfies one of the following:*

i. *$X^*=X^{-1}$, $\omega^*=\omega$, or*
ii. *$X^*=X$, $\omega^*=-\omega$.*

If $N\lhd D^\bullet$ is a normal subgroup of $D^\bullet$ such that $X\in N$ and $N^*=N$, then N contains a free symmetric pair.

Proof. Observe that $y=X^2$ centralizes $K=k[\omega]$ and that $K[y]$ is the polynomial ring over K in the indeterminate y. If $F=K(y)$ is its field of fractions, then D is a free left and right F-module with basis $B=\{1,X\}$. Using this basis, the left regular representation θ of D_F embeds D in the 2×2 matrix ring over F. Let ν be the valuation of F determined by the irreducible polynomial $1-\omega y$.

We now define $\mathbf{i}=X$, $\mathbf{j}=\omega y$ and $\mathbf{k}=\mathbf{ij}=X\omega y$, and we let F_0 be the subfield of D given by $F_0=k(\omega^2,y)$. Then $\mathbf{ji}=-\mathbf{ij}$ and it follows that $F_0[\mathbf{i},\mathbf{j}]$ is a quaternion algebra $\mathfrak{A}$ over F_0. Since $\mathbf{i}=X\in N$, we see that the commutator

$$\begin{aligned} u &= (1+\mathbf{j})\mathbf{i}(1+\mathbf{j})^{-1}\mathbf{i}^{-1}\\ &= (1+\mathbf{j})(1-\mathbf{j})^{-1} = (1+\omega y)(1-\omega y)^{-1}\in F\end{aligned}$$

belongs to the normal subgroup N. Furthermore, set $v=1-\mathbf{i}=1-X$. We consider the two cases separately.

(i) Here $X^*=X^{-1}$, $y^*=y^{-1}$ and $\omega^*=\omega$. Thus $u^*=(1+\omega y^{-1})(1-\omega y^{-1})^{-1}\in F$, so $\theta(uu^*)$ is diagonal with entries

$$(1+\omega y)(1-\omega y)^{-1}(1+\omega y^{-1})(1-\omega y^{-1})^{-1}$$

and

$$(1-\omega y)(1+\omega y)^{-1}(1-\omega y^{-1})(1+\omega y^{-1})^{-1}.$$

Since the fields have characteristic $\neq 2$ and since $\omega^2 \neq 0, \pm 1$, these entries have ν-values -1 and 1, respectively. Furthermore, $v^* = 1 - X^{-1} = (y - X)y^{-1}$, so

$$v^*v = (y - X)(1 - X)y^{-1} = (2y - (1 + y)X)y^{-1}$$

and we conclude easily that all four entries of $\theta(v^*v)$ have ν-values 0. Furthermore,

$$(v^*v)^{-1} = -(2y + (1 + y)X)(y - 1)^{-2}$$

so again all four entries of $\theta((v^*v)^{-1})$ have ν-values 0. Thus, by Lemma 2.6, $(uu^*, (uu^*)^{v^*v})$ is a free pair in $N = N^*$. Conjugating by v^{-1}, we see that $((uu^*)^{v^{-1}}, (uu^*)^{v^*}) = (w_1, w_2)$ is also a free pair in N. But, $w_1^* = w_2$ and $w_2^* = w_1$, so (w_1w_2, w_2w_1) is the free symmetric pair we require.

(ii) Here $X^* = X$, $y^* = y$ and $\omega^* = -\omega$. Thus $\mathbf{j}^* = -\mathbf{j}$ and this implies that $u^* = u^{-1}$ so u is unitary with respect to *. Note that $u \in F$ acts in a diagonal manner on B with diagonal entries $(1 + \omega y)(1 - \omega y)^{-1}$ and $(1 - \omega y)(1 + \omega y)^{-1}$. Thus, these entries have ν-values -1 and 1, respectively. Next observe that $v^2 = (1 + y) - 2X$ has full support with respect to B. Moreover, since $1 + y$ is prime to $1 - \omega y$ and since the characteristic is not 2, it follows easily that the entries of the matrix $\theta(v^2)$ all have ν-value 0. Furthermore, we have $v^{-1} = (1 + X)(1 - y)^{-1}$ so we conclude that all entries of $\theta(v^{-2})$ also have ν-value 0. Of course, $\mathbf{i}^* = \mathbf{i}$ implies that $v^* = v$. Thus, by Lemma 2.6, we conclude that (u, u^{v^2}) is a free pair in N. Finally, conjugating by v^{-1} implies that $(u^{v^{-1}}, u^v) = (w_1, w_2)$ is also a free pair in N, and this time * sends each group element to the inverse of the other. Since (w_1, w_2^{-1}) is a free pair in N, the free symmetric pair we are looking for is $(w_1w_2^{-1}, w_2^{-1}w_1)$. □

We now come to the key result of this section.

Proposition 4.4. *Let k be the prime subfield of the field K of characteristic $q \geq 0$ with $q \neq 2$, and let $\tau \neq 1$ be a k-automorphism of K. Moreover, let ζ be a nonidentity root of unity in K, assume that $K = k[\zeta]$ and that $|K : k| \geq 5$. Define $D = K(X; \tau)$ to be the field of fractions of the skew polynomial ring $K[X; \tau]$, and let * be a k-involution of D that satisfies one of the following:*

i. *$X^* = X^{-1}$ and $\zeta^* = \zeta^{-1}$, or*
ii. *$X^* = X^{-1}$ and $\zeta^* = \zeta$.*

If $N \lhd D^\bullet$ is a *-stable normal subgroup of $D^\bullet$ such that $X \in N$, then N contains a free symmetric pair.

Proof. Since $K = k[\zeta]$ and since τ necessarily acts on the finite cyclic group $\langle \zeta \rangle$, it is clear that τ has finite order in its action on K. Say $\tau \neq 1$ has order $n \geq 2$, so $y = X^n$ commutes with K. Thus $K[y]$ is a polynomial ring in the indeterminate y and its field of fractions $F = K(y)$ is contained in D. Indeed, D is a free left and right F-module with basis $B = \{1, X, X^2, \ldots, X^{n-1}\}$. Thus the left regular representation θ of D_F embeds D in the $n \times n$ matrix ring over F, and we use Lemma 2.6 to construct free pairs in D.

By Lemma 4.2, we can choose an irreducible polynomial $f(y) \in K[y]$ of degree $> 5n$ so that $f(y)$ divides $1 - \zeta y^t$ for some positive integer t not divisible by q. In particular, $f(y)$ is prime to y. Furthermore, $f(y)^2$ does not divide $1 - \zeta y^t$ since $f(y)$ is prime to the derivative $-t\zeta y^{t-1}$. Of course, $f(y)$ divides no polynomial that is prime to $1 - \zeta y^t$. This all translates to information concerning the valuation ν of F determined by $f(y)$.

Now let $w = (1-y^2X)(1-X)^{-1} \in k(X) \subseteq D$ be as in Lemma 4.1. In the notation of that lemma, we have $\alpha = y^a = y^2$ and $\beta = y^b = y^0 = 1$, so $c = \max\{a, b\} = 2$. Then, by Lemma 4.1(ii), since $k(y) \subseteq F$, we see that w^2 has full support with respect to B. Indeed, all B-coefficients of w^2 are nonzero in $k(y)$ and have numerator and denominator degrees at most $2(cn + 1) \leq 5n$. Furthermore, by Lemma 4.1(iii), modulo some factors of y, the same is true for the element $ww^* = w^*w$.

Recall that ν is the valuation of $F = K(y)$ determined by $f(y)$. Since the degree of this polynomial is larger than $5n$ and since $f(y)$ is prime to y, it follows that all B-coefficients of w^*w have ν-value 0. Furthermore, since $k(y)$ is central in D and since $\nu(y) = 0$, it follows easily that all entries of the $n \times n$ matrix $\theta(w^*w)$, associated with w^*w, have ν-value 0.

Note that $\zeta^\tau \in \langle\zeta\rangle$ implies that we know how * acts on ζ^τ. We now consider the two possibilities for *.

(i) Here $\zeta^* = \zeta^{-1}$. Let

$$u = X^{-1}(1 - \zeta y^t)X(1 - \zeta y^t)^{-1} = (1 - \zeta^\tau y^t)(1 - \zeta y^t)^{-1}$$

be the commutator of $X \in N$ with $(1 - \zeta y^t)^{-1} \in D^\bullet$. Since $N \lhd D^\bullet$, it follows that $u \in N$. Next, notice that

$$\begin{aligned} u^* &= (1 - \zeta^{-1}y^{-t})^{-1}X^{-1}(1 - \zeta^{-1}y^{-t})X = (1 - \zeta^{-1}y^{-t})^{-1}(1 - \zeta^{-\tau}y^{-t}) \\ &= \zeta\zeta^{-\tau}(1 - \zeta^\tau y^t)(1 - \zeta y^t)^{-1} \end{aligned}$$

is also in N and hence so is the product

$$uu^* = \zeta\zeta^{-\tau}(1 - \zeta^\tau y^t)^2(1 - \zeta y^t)^{-2}.$$

Note that $d = uu^* \in F$, so this element acts in a diagonal manner on the basis B. Indeed, using $\eta X^i = X^i(X^{-i}\eta X^i) = X^i\eta^{\tau^i}$ for any $\eta \in F$, we see that the diagonal entries of $\theta(d)$ are precisely the elements

$$\zeta^{\tau^i}\zeta^{-\tau^{i+1}}(1 - \zeta^{\tau^{i+1}}y^t)^2(1 - \zeta^{\tau^i}y^t)^{-2}$$

for $i = 0, 1, \ldots, n - 1$.

Now it is clear that the polynomials $1 - \zeta^{\tau^i}y^t$ and $1 - \zeta y^t$ are coprime unless $\zeta^{\tau^i} = \zeta$. Moreover, since $K = k[\zeta]$ and τ has order n in its action on K, we see that $\zeta^{\tau^i} = \zeta$ if and only if $i \equiv 0 \bmod n$. It therefore follows that almost all of the diagonal entries of $\theta(d)$ have ν-value 0. Indeed, there are just two exceptions. First when $i = 0$, this entry has ν-value -2. Next, when $i = n-1$, this entry has ν-value 2. In other words, $\theta(d)$ is a diagonal matrix with a unique diagonal entry having largest ν-value and a unique diagonal entry having smallest ν-value. Since θ is an embedding, we conclude from Lemma 2.6 that (d, d^{w^*w}) is a free pair in N.

Finally, conjugating by w^{-1}, we see that $(d^{w^{-1}}, d^{w^*})$ is also a free pair in N, but this time the two group elements are interchanged by * since $d^* = d$. The free pair we are looking for is therefore $(d^{w^{-1}}d^{w^*}, d^{w^*}d^{w^{-1}})$.

(ii) Here $\zeta^* = \zeta$. The argument in this case is similar. Take

$$u = X^{-1}(1 - \zeta y^t)X(1 - \zeta y^t)^{-1} = (1 - \zeta^\tau y^t)(1 - \zeta y^t)^{-1}$$

so $u \in N$. Next notice that

$$\begin{aligned} u^* &= (1 - \zeta y^{-t})^{-1}X^{-1}(1 - \zeta y^{-t})X = (1 - \zeta y^{-t})^{-1}(1 - \zeta^\tau y^{-t}) \\ &= \zeta^{-1}\zeta^\tau(1 - \zeta^{-\tau}y^t)(1 - \zeta^{-1}y^t)^{-1} \end{aligned}$$

is also in N and hence so is

$$uu^* = \zeta^{-1}\zeta^{\tau}[(1-\zeta^{\tau}y^t)(1-\zeta^{-\tau}y^t)]\cdot[(1-\zeta y^t)(1-\zeta^{-1}y^t)]^{-1}$$

which is a symmetric element.

Again $d = uu^* \in F$ acts in a diagonal manner on the basis B. This time, the diagonal entries of $\theta(d)$ are precisely the elements

$$\zeta^{-\tau^i}\zeta^{\tau^{i+1}}[(1-\zeta^{\tau^{i+1}}y^t)(1-\zeta^{-\tau^{i+1}}y^t)]\cdot[(1-\zeta^{\tau^i}y^t)(1-\zeta^{-\tau^i}y^t)]^{-1}$$

for $i = 0, 1, \ldots, n-1$.

As above, the polynomial $1-\zeta^{\tau^i}y^t$ is prime to $1-\zeta y^t$ unless $\zeta^{\tau^i} = \zeta$ and hence $i \equiv 0 \bmod n$. Similarly, $1-\zeta^{-\tau^i}y^t$ is prime to $1-\zeta y^t$ unless $\zeta^{-\tau^i} = \zeta$ or equivalently $\zeta^{\tau^i} = \zeta^{-1}$. Let us suppose first that there are no powers τ^i with $\zeta^{\tau^i} = \zeta^{-1}$. In this case, it now follows that almost all diagonal entries of $\theta(d)$ have ν-value 0. Again there are just two exceptions. First when $i = 0$, this entry has ν-value -1. Next, when $i = n-1$, this entry has ν-value 1. In other words, $\theta(d)$ is a diagonal matrix with a unique diagonal entry having largest ν-value and a unique diagonal entry having smallest ν-value. Since θ is an embedding, we conclude from Lemma 2.6 that (d, d^{w^*w}) is a free pair in N. The result now follows as in the end of (i).

On the other hand, suppose there exists $\tau_0 = \tau^i$ with $\zeta^{\tau_0} = \zeta^{-1}$ and set $\omega_0 = \zeta - \zeta^{-1}$. If $\omega_0^2 = 0$ or ± 1, then $|k[\omega_0] : k| \leq 2$ so $|k[\zeta] : k| \leq 4$ contrary to our assumption. Thus $\omega_0^2 \neq 0, \pm 1$ and $\omega_0^{\tau_0} = -\omega_0$. Furthermore, if $X_0 = X^i$, then X_0 acts like τ_0 on $K_0 = k[\omega_0] \subseteq K$. Note that $D_0 = K_0(X_0; \tau_0) \subseteq D$, $X_0^* = X_0^{-1}$ and $\omega_0^* = \omega_0$. Thus, by Proposition 4.3(i), $N_0 = N \cap D_0$ contains a free symmetric pair, and case (ii) is proved. □

5. Proof of Theorem 1.2

We start with the following useful observation.

Proposition 5.1. *Let G and H be groups with involution *, and let $\pi : G \to H$ be a homomorphism such that $\pi(x^*) = \pi(x)^*$, for all $x \in G$. Then:*

i. *If $x \in G$ is such that $(\pi(x), \pi(x)^*)$ is a free pair, then (x, x^*) is a free pair.*
ii. *If the elements $x, y \in G$ are such that $(\pi(x), \pi(y))$ is a free symmetric pair, then (xx^*, yy^*) is a free symmetric pair.*

Proof. See [3, Proposition 19]. □

We now begin the proof of Theorem 1.2. Since there are so many special cases to deal with, we have split the proof into three main sections: where G is nilpotent-by-finite, polycyclic-by-finite, or finite of odd order.

Proof of Theorem 1.2 - The nilpotent-by-finite group case. Here we assume that G is a torsion-free finitely-generated group that is nilpotent-by-finite but not abelian-by-finite. Then, by Lemma 3.6, G has a characteristic torsion-free nilpotent subgroup of finite index. In particular, this subgroup is *-stable and not abelian. Furthermore, by applying Theorem 3.5 to this subgroup, we see that G has a Heisenberg subgroup $H = \langle x, y\rangle$ with infinite cyclic center $\langle\lambda\rangle$ and with $xy = \lambda yx$. In addition, $x^* = x^{\pm 1}$ and $y^* = y^{\pm 1}$. At this point, it would be nice to quote [7, Theorem 1.3] directly. Unfortunately, we cannot do this. Rather, we have to revert to aspects of its proof that appear at that end of the paper.

To start with, let $k = \mathbb{F}_p$ be the prime field of characteristic $p \geq 0$, with $p \neq 2$, and let $\mathbb{H}_p$ denote the quaternion algebra $\mathbb{F}_p(a,b)\langle \mathbf{i}, \mathbf{j}\rangle$, where $\mathbb{F}_p(a,b)$ is a purely transcendental extension of k of transcendence degree 2, $\mathbf{i}^2 = a$, $\mathbf{j}^2 = b$ and $\mathbf{ij} = -\mathbf{ji}$. The first goal is to construct a suitable specialization $\psi\colon D \to \mathbb{H}_p$ and this is where the proof of [7, Theorem 1.3] comes into play.

If λ is transcendental over k, then by [7, Lemma 3.3(ii)], kH, the k-linear span of H in D, is naturally isomorphic to the group algebra $k[H]$. With this, and using $\mathbb{F}_p = k$, we can certainly define a homomorphism $\psi\colon kH \to \mathbb{H}_p$ by taking $\psi(x) = \mathbf{i}$ and $\psi(y) = \mathbf{j}$. Since the images of the group elements in $\langle x\rangle\langle y\rangle$ are $\mathbb{F}_p$-linearly independent, it follows that the kernel P of ψ is the principal ideal generated by the central element $\pi = 1+\lambda$. Furthermore, since $\bigcap_{m=0}^{\infty} \pi^m \cdot k\langle\lambda\rangle = 0$, it follows from freeness that $\bigcap_{m=0}^{\infty} \pi^m \cdot kH = 0$. Thus, by [7, Lemma 3.2], we see that $M = kH \setminus P$ is a multiplicatively closed right divisor set in kH. In particular, $R = (kH)M^{-1}$ is a subring of D, and then ψ clearly extends to a homomorphism from R to $\mathbb{H}_p$.

On the other hand, suppose that λ is algebraic over k. Then k cannot be a finite field since λ has infinite multiplicative order in D. Thus k must be the field of rationals $\mathbb{Q}$. Furthermore, by the proof of [7, Theorem 1.3(ii)], there exists an integer $n \geq 0$, a prime $p > 2$ and a specialization $\psi\colon D \to \mathbb{H}_p$ with $\psi(x^{2^n}) = \mathbf{i}$ and $\psi(y) = \mathbf{j}$. Note that x^{2^n} is an element of G that is either fixed or inverted by *. Furthermore, $x^{2^n} y = \lambda^{2^n} y x^{2^n}$ so $\langle x^{2^n}, y\rangle$ is also a suitable Heisenberg subgroup of G. Thus, replacing x^{2^n} by x, we can assume that $p > 2$ and ψ exist with $\psi(x) = \mathbf{i}$ and $\psi(y) = \mathbf{j}$.

Now let $u = 1+x+x^*$ and $v = 1+y+y^*$. Then $\psi(u) = 1+\mathbf{i}+\mathbf{i}^{\pm 1} = 1+\alpha\mathbf{i}$ where $\alpha = 2$ or $1 + a^{-1}$, depending on whether $x^* = x$ or x^{-1}. Similarly, $\psi(v) = 1 + \beta\mathbf{j}$ where $\beta = 2$ or $1 + b^{-1}$. Since $x, y \in G \subseteq N \lhd D^\bullet$, it follows that $s = uy^{-1}u^{-1}y$ and $t = vx^{-1}v^{-1}x$ both belong to N. Furthermore,

$$\psi(s) = (1+\alpha\mathbf{i})\mathbf{j}^{-1}(1+\alpha\mathbf{i})^{-1}\mathbf{j} = (1+\alpha\mathbf{i})(1-\alpha\mathbf{i})^{-1} = (1+\alpha\mathbf{i})^2(1-a\alpha^2)^{-1}$$

and similarly $\psi(t) = (1+\beta\mathbf{j})^2(1-b\beta^2)^{-1}$. Next notice that u and v are symmetric, so $s^* = y^*u^{-1}(y^*)^{-1}u \in N$, $\psi(s^*) = \psi(s)$, $t^* \in N$ and $\psi(t^*) = \psi(t)$. In particular, we have $ss^*, tt^* \in N$.

Finally, by [2, Proposition 16], it follows that $\psi(ss^*) = (1+\alpha\mathbf{i})^4(1-a\alpha^2)^{-2}$ and $\psi(tt^*) = (1+\beta\mathbf{j})^4(1-b\beta^2)^{-2}$ generate a free subgroup in $\mathbb{H}_p$. Thus the same is true for the pair (ss^*, tt^*) in N. □

Proof of Theorem 1.2 - The polycyclic-by-finite group case. Here we assume that G is polycyclic-by-finite, but not abelian-by-finite. If G has a characteristic subgroup H that is nilpotent-by-finite, but not abelian-by-finite, then H is *-stable and the preceding special case applied to H yields the result.

Thus we can assume that every characteristic subgroup of G that is nilpotent-by-finite is necessarily abelian-by-finite, and therefore Theorem 3.11 applies to G. In particular, G has a *-stable subgroup $G_0 = A \rtimes X_0$, where A is a *-stable finitely-generated free abelian group, and where $X_0 = \langle x\rangle$ is infinite cyclic, acts faithfully on A and normalizes no nonidentity cyclic subgroup of A. Furthermore, G_0 satisfies conditions (i) or (ii) of that theorem. Of course, it now suffices to assume that $G = G_0 = A \rtimes X_0$.

Let $\theta\colon G \to D^\bullet$ be the natural embedding of G into the multiplicative group of D, and let σ be the automorphism of G associated to *. Then θ is certainly a σ-homomorphism that can be extended to an algebra homomorphism $\theta\colon k[G] \to D$, where k is the prime subfield of D and $k[G]$ is the group algebra of G over k. Let $I = \ker\theta$ so that I is a σ-stable prime ideal of $k[G]$, and suppose by way of contradiction that $I \neq 0$. Then a standard shortest length argument given below shows that $I \cap k[A] \neq 0$.

Indeed, let α be a nonzero element of I with support in the minimal number of cosets of A. Say $\alpha = \sum_i x^i\alpha_i$ with $\alpha_i \in k[A]$, and multiply α by a suitable x^j so that $\alpha_0 \neq 0$. If $a \in A$, then $a\alpha - \alpha a \in I$, and since A is abelian,

$$a\alpha - \alpha a = \sum_{i\neq 0} x^i(a^{x^i} - a)\alpha_i$$

has a smaller number of cosets of A in its support since the x^0-term has been deleted. Thus, by minimality, $a\alpha - \alpha a = 0$ and in particular $(a^{x^i} - a)\alpha_i = 0$ for all i. But $k[A]$ is a domain and X_0 acts faithfully on A, so for each $i \neq 0$ we can choose $a \in A$ with $a^{x^i} \neq a$ and conclude that $\alpha_i = 0$. Thus $\alpha = \alpha_0 \in I \cap k[A]$ and this intersection is not 0.

Next observe that $I \cap k[A] \neq 0$ is X_0-stable and also σ-stable. In particular, if G satisfies condition (i) of Theorem 3.11, then Bergman's theorem, namely Theorem 6.4 with $n = 1$, implies that $k[A]/(I\cap k[A])$ is finite dimensional over k. On the other hand, if G satisfies (ii) of Theorem 3.11, then $\langle\sigma\rangle = S_2$ naturally permutes the factors A_1 and A_2, and hence Theorem 6.4, this time with $n = 2$, again implies that $k[A]/(I\cap k[A])$ is finite dimensional over k. Since $k[A]/(I\cap k[A])$ is a commutative domain, it follows in both cases that $k[A]/(I\cap k[A])$ is a finite degree field extension of k. Furthermore X_0 acts on this field, so Galois theory implies that X_0 acts like a finite group on the quotient $k[A]/(I\cap k[A])$. Hence since A embeds in this image, we see that X_0 acts like a finite group on A, contrary to the assumption that X_0 acts faithfully on A. We conclude therefore that $I = 0$ and hence that $k[G]$ embeds faithfully in D.

Now by Proposition 2.4 we can find numerous proto-specializations π from $k(G) \subseteq D$ to a division ring $\overline{D} = k[\zeta](X;\tau)$, where ζ is a primitive p-th root of unity, $\zeta^\tau = \zeta^n$, $n \not\equiv 1 \pmod p$, $\pi(x) = X$ and $\pi(A) = \langle\zeta\rangle$. Since there are infinitely many choices for p, we can assume that $|k[\zeta] : k| \geq 10$.

Suppose first that $x^* = x^{-1}$, so by Theorem 3.11(i), * acts like the identity map or the inverse map on A. If either * is the identity on A or $q = 0$ and * is the inverse on A, then Proposition 2.4(i) yields a proto-specialization $\pi\colon k(G) \to \overline{D} = K(X;\tau)$ where $K = k[\zeta]$, $\zeta^p = 1$ and τ is nontrivial on K. Furthermore, * can be defined on $\overline{D}$ in such a way that π intertwines the two involutions. Since $x^* = x^{-1}$, we have $X^* = X^{-1}$ and Proposition 4.4(i)(ii) implies that $\pi(N)$ contains a free symmetric pair. By Proposition 5.1, applied to N and $\pi(N)$, the same is true for N.

On the other hand, if $q > 0$ and * is the inverse map on A, then by Proposition 2.4(ii), $k[G]$ has a *-stable subring S_0, with division ring of fractions $D_0 \subseteq D$ and with a proto-specialization $\pi\colon D_0 \to \overline{D}_0 = K_0(X;\tau_0)$. Here $\zeta^p = 1$ and $K_0 = k[\zeta]$ or $k[\zeta + \zeta^{-1}]$. Clearly $|K_0 : k| \geq 5$ and, since $q > 0$, K_0 is a finite field and both ζ and $\zeta + \zeta^{-1}$ are roots of unity. Furthermore, $K_0(X;\tau_0)$ inherits the involution * from S_0 and again Proposition 4.4(i)(ii) implies that $\pi(N\cap D_0)$ contains

a free symmetric pair. By Proposition 5.1, applied to $N \cap D_0$ and $\pi(N \cap D_0)$, the same is true for $N \cap D_0 \subseteq N$.

It remains to consider the case where $x^* = x$ and we observe first that * cannot acts like the inverse map on A. Indeed, if this were the case, take any $c \in A$ and let $x^{-1}cx = d \in A$. Applying * yields $xc^{-1}x^{-1} = d^{-1}$ and then taking inverses gives us $xcx^{-1} = d$. Thus x and x^{-1} act the same on A and hence x^2 centralizes A, contrary to our assumptions. Finally, since * does not act like the inverse map on A, it follows that there exists $b \in A$ with $a = bb^* \neq 1$ and hence there exists $1 \neq a \in A$ with $a^* = a$. By Lemma 3.12, replacing x by a suitable power if necessary, we see that x and ax generate a free subsemigroup of G. Thus since $a^* = a$, $x^* = x$, $k[G] \subseteq D$ and $G \subseteq N \lhd D^\bullet$, we conclude from Lemma 3.13 that N contains a free symmetric pair. This completes the proof. □

Proof of Theorem 1.2 - The finite group case. We now assume that $G \subseteq N \lhd D^\bullet$, with G nonabelian of finite odd order, and let k be the prime subfield of D. If k is a finite field, then kG, the k-linear span of G in D, is a finite noncommutative division ring, certainly a contradiction. Thus we must have $k = \mathbb{Q}$, the field of rationals. By Theorem 3.1, G has a *-stable nonabelian subgroup $H = X \rtimes Y$ with suitable properties, and we can now assume that $G = H$. Note that $X = \langle x \rangle$ has prime order p and $x^* = x$ or x^{-1}. Furthermore, $Y = \langle y \rangle$ is a cyclic q-group with prime $q \neq p$ and $y^* = y^{-1}$. Since every subgroup of Y is characteristic, we can also assume that Y is chosen minimal with G being nonabelian. In particular, it follows that y^q centralizes X. We note that $y^q \neq 1$ by [13, Theorem 18.1(ii)].

Let $\mathbb{Q}G$ be the $\mathbb{Q}$-linear span of G in D. Then $F = \mathbb{Q}\langle x, y^q \rangle$ is an algebriac number field and y acts nontrivially on this field. A standard shortest length argument then shows that $B = \{1, y, \ldots, y^{q-1}\}$ is a right and left F-basis for $\mathbb{Q}G$. In particular the left regular representation θ for $(\mathbb{Q}G)_F$ embeds $\mathbb{Q}G$ into the ring of $q \times q$ matrices over F, and hence over any larger field.

For any rational number m with $m \neq 0, \pm 1$, set

$$f(m, y) = \frac{1 - my}{1 - m^{-1}y}.$$

Then

$$(1 - m^{-1}y) \sum_{i=0}^{q-1} m^{-i}y^i = 1 - m^{-q}y^q$$

is a nonzero element in the field F, and therefore

$$\begin{aligned} f(m, y) &= \frac{1 - my}{1 - m^{-q}y^q} \sum_{i=0}^{q-1} m^{-i}y^i \\ &= \frac{1}{1 - m^{-q}y^q} \left[(1 - m^{-q+2}y^q) + (1 - m^2) \sum_{i=1}^{q-1} m^{-i}y^i\right] \end{aligned}$$

has full support with respect to B.

In particular, if we set

$$v = \frac{1 - my}{1 - my^{-1}} = -m^{-1}y \, \frac{1 - my}{1 - m^{-1}y} = -m^{-1}y \, f(m, y),$$

then v also has full support. Indeed, a closer look at the above expressions shows that all coefficients of v are nonzero products of

$$m, \quad y^q, \quad m^2-1, \quad m^q-y^q, \quad m^{q-2}-y^q$$

and their inverses. Furthermore, $f(m^{-1},y)$ has full support and therefore so does v^{-1}, with the same factors as above and with additionally

$$m^q-y^{-q}, \quad m^{q-2}-y^{-q}.$$

Since v and v^{-1} commute with the elements of B, it now follows that all entries of the matrices $\theta(v)$ and $\theta(v^{-1})$ are nonzero products of the above factors and some additional factors of y^q. Note that $y^* = y^{-1}$ implies that $v^* = v^{-1}$.

Next observe that $x \in F$, so $\theta(x)$ is the diagonal matrix

$$\theta(x) = \operatorname{diag}(x, x^y, x^{y^2}, \ldots, x^{y^{q-1}}).$$

Now form the commutator

$$u = (m-x)^{-1}y^{-1}(m-x)y = (m-x)^{-1}(m-x^y).$$

Then $y \in N \triangleleft D^\bullet$ implies that $u \in N$. Furthermore, $u \in F$ so $\theta(u)$ is also a diagonal matrix, this time with diagonal entries

$$(m-x^{y^{i+1}})/(m-x^{y^i})$$

for $i = 0, 1, \ldots, q-1$.

Let

$$n = |G|\cdot 2(q-2) = |\langle x, y^q\rangle|\cdot 2q(q-2)$$

and let $L = F[\zeta]$ where ζ is a primitive n-th root of unity. Then $x \in \langle\zeta\rangle$ and by Lemma 2.5 there exists an integer $m \in \mathbb{Z}$ and a prime $l \in \mathbb{Z}$ such that $L \subseteq \mathbb{Q}_l$, the field of l-adic rationals with corresponding valuation ν_l, and with $\nu_l(m-x) > 0$ and $\nu_l(m-\lambda) = 0$ for all $\lambda \in \langle\zeta\rangle$ with $\lambda \neq x$. We fix this value of m. Since $\nu_l(\zeta) = 0$, we have $\nu_l(x) = \nu_l(y^q) = 0$. Also $\nu_l(m-x) > 0$ implies that $\nu_l(m) = 0$. Thus $l \nmid m$ and in particular $m \neq 0$. Furthermore, $x \neq \pm 1$ in F and $2 \mid n$, so $\nu_l(m-1) = 0$ and $\nu_l(m+1) = 0$. Thus $m \neq \pm 1$ and $\nu_l(m^2-1) = 0$.

Next, since $(q-2) \mid n$ and $q > 2$, we see that

$$m^{q-2} - y^q = \prod_\lambda (m-\lambda)$$

as λ runs through the $q-2$ elements of $\langle\zeta\rangle$ with $\lambda^{q-2} = y^q$. Of course, none of these λ's can equal x since $1 \neq y^q$ is not contained in $\langle x\rangle = X$. Thus $\nu_l(m^{q-2}-y^q) = 0$ and similarly $\nu_l(m^{q-2}-y^{-q}) = 0$. Furthermore, since n has an extra factor of q, the same argument shows that $\nu_l(m^q - y^{\pm q}) = 0$. We conclude that all entries of the matrices $\theta(v)$ and $\theta(v^{-1})$ have ν_l-values 0.

Since y acts like an element of order q on $\langle x\rangle$, we see that one diagonal entry of $\theta(u)$ has positive ν_l-value, one has negative ν_l-value and the remaining diagonal entries all have ν_l-value 0. We consider the two possibilities for x^* separately. Suppose first that $x^* = x$. Then $u^* = u$ and Lemma 2.6 implies that $\theta(u)$ and $\theta(u^v)$ generate a free group of rank 2. Thus (u, u^v) is a free pair in N. Indeed, this is a symmetric pair since $u^* = u$ and $v^* = v^{-1}$.

On the other hand, if $x^* = x^{-1}$, then $y^* = y^{-1}$ implies that

$$u^* = (m-x^{-1})^{-1}(m-x^{-y})$$

and therefore $\theta(u^*)$ is diagonal with entries

$$(m - x^{-y^{i+1}})/(m - x^{-y^i})$$

for $i = 0, 1, \ldots, q-1$. Now notice that x^{-y^i} cannot equal x since otherwise y^i would have order 2 in its action on X, surely a contradiction. Thus all diagonal entries of $\theta(u^*)$ have ν_l-value 0. Since N is *-stable, we conclude that $uu^* \in N$ and $\theta(uu^*) = \theta(u)\theta(u^*)$ is a diagonal matrix with one diagonal entry having positive ν_l-value, one diagonal entry having negative ν_l-value and with all the remaining diagonal entries having ν_l-value 0. It now follows from Lemma 2.6 that $\theta(uu^*)$ and $\theta((uu^*)^v)$ generate a free group of rank 2. Hence, the same is true for the symmetric pair $(uu^*, (uu^*)^v)$ in N and the theorem is proved. □

6. Appendix. Bergman's Theorem

The goal of this section is to obtain the extension of Bergman's theorem [1, Theorem 1] (see also [12, Corollary 9.3.9]) that was used in the proof of Theorem 1.2. For convenience, we recall several lemmas and appropriate notation from [12, Section 9.3].

Lemma 6.1. *Let A be a finitely generated abelian group and let $\mathcal{F} = \{F_\alpha \mid \alpha \in I\}$ be a collection of finite nonempty subsets of A. Let $\mathcal{W} = \mathcal{W}(\mathcal{F})$ be the set of all subgroups $W \subseteq A$ with the property that $W \cap F_\alpha \neq \emptyset$ for all α. Then every member of $\mathcal{W}$ contains a minimal member of $\mathcal{W}$, and $\mathcal{W}$ has only finitely many minimal members.*

Proof. See [12, Lemma 9.3.4]. □

Again, let A be a finitely generated abelian group and let $I \neq K[A]$ be an ideal of the group algebra $K[A]$. Then a *log subgroup* for I is a subgroup of A that occurs intrinsically in each nonzero element of I in the following well-defined manner. Namely, $W \subseteq A$ is a log subgroup for I if and only if, for all $0 \neq \alpha \in I$, there exist two distinct group elements x, y in the support of α with $xy^{-1} \in W$. This strange name, used in [12], is based on the title of [1] where these subgroups were introduced. Several observations are now in order. First, if $I = 0$, then the conditions on W are vacuous and hence all subgroups of A are log subgroups for $I = 0$. Second, since $I \neq K[A]$, all nonzero elements of this ideal have at least two elements in their support and hence A is always a log subgroup for I. Finally, if W is a log subgroup for I, then so are all larger subgroups. Hence the subgroups of interest here are the minimal log subgroups, namely the *minilogs*.

Lemma 6.2. *Let A be a finitely generated abelian group and let $I \neq K[A]$ be an ideal of $K[A]$. Then any log subgroup for I contains a minilog subgroup and I has only finitely many such minilog subgroups. Furthermore, if τ is any automorphism of A that stabilizes I, then τ permutes the minilogs for I.*

Proof. For each nonzero $\alpha \in I$, set $F_\alpha = \{xy^{-1} \mid x, y \in \operatorname{Supp} \alpha,\ x \neq y\}$. Also set $F_0 = \{1\}$ and $\mathcal{F} = \{F_\alpha \mid \alpha \in I\}$. Then, in the notation of the preceding lemma, $\mathcal{W}(\mathcal{F})$ is the collection of all log subgroups for I. Since the τ part of the above is obvious, Lemma 6.1 yields the result. □

Bergman's key observation is as follows.

Lemma 6.3. *Let A be a finitely generated abelian group and let $I \neq K[A]$ be an ideal of the group algebra $K[A]$. If B is a torsion-free subgroup of A with $K[B] \cap I = 0$, then there exists a minilog subgroup W for I with $B \cap W = \langle 1 \rangle$.*

Proof. See [12, Lemma 9.3.5]. Note that if $B \cap W = \langle 1 \rangle$ for some log subgroup, then this intersection also holds for any minilog subgroup contained in W. □

We now offer our extension of Bergman's theorem. Of course, the $n = 1$ case below is the original result, and we include a simple argument that does not use pure minilog subgroups or the rank formalism of [12, Section 9.3]. Furthermore, as we saw, only the $n = 1$ and $n = 2$ cases are needed for our work. But the remaining n values are no more difficult to handle. The presence of the symmetric group S_n below, rather than an arbitrary transitive permutation group, seems to be needed for the inductive argument.

Theorem 6.4. *Let $A = A_1 \oplus A_2 \oplus \cdots \oplus A_n$ be the direct product of n finitely generated free abelian groups and let the group $\mathfrak{B} = \langle \mathfrak{A}, S_n \rangle$ act as automorphisms on A. Here, the symmetric group S_n permutes the factors $\{A_1, A_2, \ldots, A_n\}$ via its natural action on the subscripts, while $\mathfrak{A}$ stabilizes each A_i. Furthermore, assume that for every subgroup $\mathfrak{A}_0$ of finite index in $\mathfrak{A}$, the rational $\mathfrak{A}_0$-modules $\mathbb{Q}A_i$ are irreducible and pairwise nonisomorphic. If I is a nonzero $\mathfrak{B}$-stable prime ideal of the group algebra $K[A]$, then $\dim_K K[A]/I$ is finite.*

Proof. Of course, if $I = K[A]$, then $K[A]/I = 0$ is certainly finite dimensional over K. Thus we can assume that I is proper.

We use the above notation. Suppose $W \subseteq A$ is a minilog subgroup for the ideal I. Then $W \neq \langle 1 \rangle$ since $I \neq 0$. Furthermore, by Lemma 6.2, there are only finitely many such minilog subgroups and they are permuted by $\mathfrak{A} \subseteq \mathfrak{B}$. In particular, $\mathfrak{A}$ has a subgroup $\mathfrak{A}_0$ of finite index that stabilizes W. Now consider the additive inclusion $0 \neq \mathbb{Q}W \subseteq \mathbb{Q}A_1 \oplus \mathbb{Q}A_2 \oplus \cdots \oplus \mathbb{Q}A_n$ of rational $\mathfrak{A}_0$-modules. Since the summands $\mathbb{Q}A_i$ are irreducible and pairwise nonisomorphic by assumption, it follows that $\mathbb{Q}W$ must be a direct sum of several of these $\mathbb{Q}A_i$. In particular, $\mathbb{Q}W \supseteq \mathbb{Q}A_j \supseteq A_j$ for some j, and hence W contains a subgroup of finite index in some A_j.

We proceed by induction on n. Suppose $n = 1$ and $I \neq 0$ is a proper ideal of $K[A]$. As we saw above, any minilog subgroup W of I contains a subgroup of finite index in $A_j = A$. In particular, if a is any free generator of A, then $\langle a \rangle$ cannot be disjoint from W. Thus the preceding lemma implies that $I \cap K[\langle a \rangle] \neq 0$ and therefore the image of a in $K[A]/I$ is algebraic over K. Hence $K[A]/I$ is algebraic and therefore finite dimensional over K.

We can now assume that $n \geq 2$ and that the result holds for all smaller direct products. Suppose $I \cap K[\widetilde{A}] \neq 0$ where $\widetilde{A}$ is a properly smaller direct product of the A_i's, say $\widetilde{A} = A_1 \oplus A_2 \oplus \cdots \oplus A_{n-1}$. Then $\widetilde{\mathfrak{B}} = \langle \mathfrak{A}, S_{n-1} \rangle \subseteq \mathfrak{B}$ acts on $\widetilde{A}$ and $\widetilde{I} = I \cap K[\widetilde{A}]$ is a nonzero $\widetilde{\mathfrak{B}}$-stable prime ideal. By induction, $K[\widetilde{A}]/\widetilde{I}$ is finite dimensional over K, and in particular, the image of $K[A_1]$ in $K[A]/I$ is finite dimensional. It now follows from the transitive action of S_n that the images of all $K[A_i]$ in $K[A]/I$ are finite dimensional, and thus clearly so is $K[A]/I$. We can therefore assume that $K[\widetilde{A}_i] \cap I = 0$ for every $i = 1, 2, \ldots, n$, where $\widetilde{A}_i = \oplus_{j \neq i} A_j$.

Next, observe that the transitive action of S_n implies that all A_i have the same rank r. If $r \leq 1$, then each A_i is cyclic and hence has finite automorphism group. In

particular, $\mathfrak{A}$ has a subgroup $\mathfrak{A}_0$ of finite index that centralizes all A_i. It then follows that all the rational $\mathfrak{A}_0$-modules $\mathbb{Q}A_i$ are isomorphic, contrary to the hypothesis. Thus we must have $r \geq 2$. For convenience, let $^-\colon K[A] \to K[A]/I$ denote the natural homomorphism.

We are now ready to prove the theorem and recall that $K[A]/I$ is a commutative domain. For each i, let a_i be a fixed free generator of A_i. For convenience, we isolate two of these and so we write $b = a_{n-1}$ and $c = a_n$. Consider the subgroup $\langle a_1, a_2, \ldots, a_{n-1}, a_n\rangle$ of A and observe that this subgroup cannot be disjoint from any minilog subgroup W of I. Indeed, as was shown in the second paragraph of this proof, W must contain a subgroup of finite index in some A_j, and then certainly $\langle a_j\rangle \cap W \neq \langle 1\rangle$. It then follows from Lemma 6.3 that $K[\langle a_1, a_2, \ldots, a_{n-1}, a_n\rangle]\cap I \neq 0$ and this gives us relations in the image.

Let us denote by F the field of fractions of the image $K[\langle \bar{a}_1, \bar{a}_2, \ldots, \bar{a}_{n-2}\rangle] \subseteq K[A]/I$. Then the field generated by F and $\bar{b} = \bar{a}_{n-1}$ is the rational function field $F(\bar{b})$ since $^-$ is a monomorphism on $K[A_1 \oplus A_2 \oplus \cdots \oplus A_{n-1}]$. Furthermore, a nonzero element in the intersection $K[\langle a_1, a_2, \ldots, a_{n-2}, b, c\rangle] \cap I$ must have support in at least two distinct cosets of $\langle a_1, a_2, \ldots, a_{n-2}, b\rangle$ since otherwise the coset generator could be cancelled yielding a nonzero element in $K[\langle a_1, a_2, \ldots, a_{n-2}, b\rangle] \cap I$. Thus the relations we obtain from the nonzero intersection $K[\langle a_1, a_2, \ldots, a_{n-2}, b, c\rangle] \cap I$ involve at least two distinct powers of $\bar{c}$ and therefore show that $\bar{c}$ is algebraic over $F(\bar{b})$. Similarly $\bar{b}$ is algebraic over $F(\bar{c})$.

Next, since $r \geq 2$, we can replace $b = a_{n-1}$ by a second free generator of A_{n-1}, namely b', and deduce as above that $\overline{b'}$ is algebraic over $F(\bar{c})$ and hence over $F(\bar{b})[\bar{c}]$. But an algebraic extension of an algebraic extension is algebraic, so we conclude that $\overline{b'}$ is algebraic over $F(\bar{b})$, contrary to the fact that $^-$ is a monomorphism on $K[A_1 \oplus A_2 \oplus \cdots \oplus A_{n-1}]$. This contradiction clearly yields the result. □

The same proof also yields the following generalization of the above.

Theorem 6.5. *Let $A = A_1 \oplus A_2 \oplus \cdots \oplus A_n$ be the direct product of n finitely generated free abelian groups and let the groups $\mathfrak{B} \supseteq \mathfrak{A}$ act as automorphisms on A. Here, $\mathfrak{B}$ permutes the factors $\{A_1, A_2, \ldots, A_n\}$ and is n-fold transitive, while $\mathfrak{A}$ stabilizes each A_i. Furthermore, assume that for every subgroup $\mathfrak{A}_0$ of finite index in $\mathfrak{A}$, the rational $\mathfrak{A}_0$-modules $\mathbb{Q}A_i$ are irreducible and pairwise nonisomorphic. If I is a nonzero $\mathfrak{B}$-stable prime ideal of the group algebra $K[A]$, then we conclude that $\dim_K K[A]/I$ is finite.*

Finally, we thank Pedro Russo for his careful proofreading of this manuscript and for finding a number of small mathematical errors. We also thank the referee for his many suggestions.

References

[1] Bergman, G. M. *The logarithmic limit-set of an algebraic variety*, Trans. AMS **157** (1971), 459–469.

[2] Goncalves, J. Z., Mandel, and Shirvani, M. *Free products of units in algebras I: quaternion algebras.* J. Algebra **314** (1999), 301–316.

[3] ——— *Free products of units in algebras II. Crossed products.* J. Algebra **233** (2000), 567–593.

[4] ——— *Free symmetric and unitary pairs in central simple algebras with involution.* In Groups, Rings and Algebras, Madison 2005. Contemp. Math. **420**, AMS, Providence, 2006, 121–139.

[5] Goncalves, J. Z. *Constructing free groups in a normal subgroup of the multiplicative group of division rings.* J. Group Theory **18**, 5 (2015), 829–843.
[6] Goncalves, J. Z. and Passman, D. S. *Unitary units in group algebras.* Israel J. Math. **125** (2001), 131–155.
[7] ——— *Explicit free groups in division rings.* Proc. AMS **143**, 2 (2015), 459–468.
[8] Lichtman, A. I. *On the subgroups of the multiplicative group of a skewfields.* Proc. AMS **63** (1977), 15–16.
[9] ——— *Free subgroups of normal subgroups of the multiplicative group of skew fields.* Proc. AMS **7**, 2 (1978), 174–178.
[10] Lorenz, M. *Group rings and division rings.* Methods in Ring Theory, NATO ASI Ser C **233**, Reidel, Dordrecht (1984), 265–280.
[11] Magnus, W., Karras, A. and Solitar, D. *Combinatorial Group Theory: Presentations of Groups in Terms of Generators and Relations.* Second edition, Dover, New York, 1976.
[12] Passman, D. S. *The Algebraic Structure of Group Rings.* Dover, New York, 2011.
[13] ——— *Permutation Groups.* Dover, New York, 2012.
[14] ——— *Infinite Crossed Products.* Dover, New York, 2013.
[15] Siegel, C. *Approximation algebraisher Zahlen.* Math. Z. **10**, (1921), 173–273.
[16] Sury, B. *Polynomials with integer values.* Resonance **6**, 8 (2001), 46–60.
[17] Shorey, T. and Tejdeman, R. *Exponential Diophantine Equations.* Cambridge University Press, Cambridge, 1986.

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

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