FREE GROUPS IN NORMAL SUBGROUPS OF THE MULTIPLICATIVE GROUP OF A DIVISION RING

JAIRO Z. GONÇALVES AND DONALD S. PASSMAN

ABSTRACT. Let D be a division ring with center Z and multiplicative group $D \setminus \{0\} = D^\bullet$, and let N be a normal subgroup of $D^\bullet$. We investigate various conditions under which N must contain a free noncyclic subgroup. In one instance, assuming that the transcendence degree of Z over its prime field is infinite, and that N contains a nonabelian solvable subgroup, we use a construction method due to Chiba to exhibit free generators of the free subgroup.

1. INTRODUCTION

Let D be a non-commutative division ring with center Z and multiplicative group $D^\bullet = D \setminus \{0\}$. Not much is known about the structure of $D^\bullet$, and the first clue as to how bad its behavior can be is the conjecture of Lichtman [15], which asserts

Conjecture 1.1. *$D^\bullet$ contains a noncyclic free subgroup.*

Perhaps the best general result in this regard is due to Chiba [1]. He showed that if D is noncommutative and if $Z = \mathfrak{Z}(D)$ is uncountable, then $D^\bullet$ contains a noncyclic free subgroup. Analogous to the above, but much more difficult is

Conjecture 1.2. *Let N be a non-central normal subgroup of $D^\bullet$. Then N contains a noncyclic free subgroup.*

Conjecture 1.2 was proved by the first author in [3] when D is finite dimensional over Z , and by Lichtman in various other instances, see for example papers [16], [17] and [18].

The goal of the present work is to give more support to Conjecture 1.2 and, at the same time, to exhibit the generators of the free subgroup in N. For example, in section 3, we offer a new proof of a result of Lichtman showing that Conjecture 1.2 is true when N contains a nonabelian nilpotent subgroup. Next, in section 4, we prove the validity of the conjecture when N contains a nonabelian finite subgroup. Finally, if $\mathrm{tr.deg}(Z/P)$, the transcendence degree of Z over its prime field P, is infinite, then in section 5 we prove that Conjecture 1.2 is true when N contains a nonabelian solvable subgroup. The interested reader can find more on the history and development of this subject in [14].

2. CROSSED PRODUCT RESULTS

We start by discussing certain preliminary results concerning crossed products and rings related to crossed products.

The first author was supported by Grant CNPq 301.320/2011-0, and Fapesp-Brazil, Proj. Tematico 2009/52665-0.

The first lemma uses the notation of [6]. Let K be a cyclic Galois extension of the field F, with Galois group $\langle\sigma\rangle$ of order n, let x be a symbol and let $0 \neq b \in F$. Then we denote by $A = (K, \langle\sigma\rangle, x, b)$ the cyclic algebra of degree n and center F, generated by K and x, with relations $x^{-1}\alpha x = \sigma(\alpha)$ for all $\alpha \in K$ and $x^n = b$. Specifically, every element u of A is uniquely writable as a sum $u = \sum_{i=0}^{n-1} \alpha_i x^i$ with $\alpha_i \in K$. Recall that this element u is said to have *full support* if all the coefficients α_i are nonzero. The following is [6, Proposition 9].

Lemma 2.1. *Let $A = (K, \langle\sigma\rangle, x, b)$ be a cyclic algebra of degree n with center F and let $\alpha, \beta \in F$ be distinct nonzero elements of F with $\alpha^n \neq b^{-1}$ and $\beta^n \neq b^{-1}$. Then*

$$u = \frac{1 - \alpha x}{1 - \beta x}$$

is a unit in A. Furthermore, u and u^{-1} have full support and this support lies in $P(\alpha, \beta, b)$, the subfield of F generated by α, β, b, and the prime subfield P.

Of course, cyclic algebras are examples of certain more general rings called crossed products and indeed of crossed products over a field. Specifically, let K be a field and let G be a multiplicative group that acts on K as field automorphisms. Then we let $A = K*G$ be an associative ring in which every element u is a finite sum $u = \sum_g \alpha_g \bar{g}$, where $\alpha_g \in K$ and $\bar{g}$ is a copy of $g \in G$ in A. Addition is obvious and multiplication is determined by $\bar{g}^{-1}\alpha\bar{g} = \sigma_g(\alpha)$ for all $\alpha \in K$, where σ_g is the field automorphism associated with $g \in G$. Furthermore, for $g, h \in G$, we have $\bar{g}\bar{h} = \kappa_{g,h}\overline{gh}$ for some $0 \neq \kappa_{g,h} \in K$. It is easy to determine the conditions on the various $\kappa_{g,h}$ and σ_g that are equivalent to the associativity of A. For example, since K is commutative, the map $g \mapsto \sigma_g$ must be a group homomorphism. If all $\kappa_{g,h} = 1$, then A is indeed associative and $K*G$ is called a skew group ring. If all $\sigma_g = 1$, then K is central and $K*G$ is called a twisted group ring. When all parameters are equal to 1, then $K*G = K[G]$ is the ordinary group ring. In all cases, one can assume that $\bar{1} = 1$ is the identity element of A. The following result is well known, so we just sketch the proof.

Lemma 2.2. *Let $K*G$ be a crossed product of G over the field K and assume that G acts faithfully on K. Then $K*G$ is a simple ring with center $F = K^G$, the fixed subfield of K under the action of G. If, in addition, $K*G$ is an Ore ring with ring of fractions S, then F is also the center of S.*

Proof. We first show that $K = K\bar{1}$ is self-centralizing in $K*G$. To this end, let $u = \sum_g \alpha_g \bar{g}$ be in the centralizer of K. Then, for all $\beta \in K$, we have $u\beta = \beta u$ and uniqueness of coefficient implies that $\alpha_g\beta = \alpha_g\sigma_{g^{-1}}(\beta)$. In particular, if g is in the support of u, then $\alpha_g \neq 0$, so $\sigma_{g^{-1}}$ is the identity automorphism. Faithfulness now implies that $g = 1$, and with this it is clear that $\mathfrak{C}_{K*G}(K) = K$ and that $\mathfrak{Z}(K*G) = F = K^G$. Finally, let I be a nonzero ideal of $K*G$ and choose $0 \neq v \in I$ to have minimal support size. Since I is an ideal, we can multiply v by some $\bar{h}$ with $h \in G$ to guarantee that 1 is in the support of v. Now, for all $\beta \in K$, we see that $v\beta - \beta v \in I$ and these elements all have smaller support than v since the identity term drops out. Thus, by minimality, $v\beta - \beta v = 0$ and v is contained in $\mathfrak{C}_{K*G}(K) = K$. Therefore v is invertible, and $v \in I$ implies that $I = K*G$.

Finally, suppose $R = K*G$ is an Ore ring with ring of fractions S. Then certainly $F \subseteq \mathfrak{Z}(S)$. On the other hand, if $s \in \mathfrak{Z}(S)$, let $J = \{r \in R \mid sr \in R\}$. Then J

is clearly a 2-sided ideal of R since s is central, and $J \neq 0$ since s is a fraction. Thus, since R is simple, we have $J = R$ and $1 \in J$. It follow that $s \in R$ and hence $s \in \mathfrak{Z}(R) = F$. □

In particular, this explains why F is the center of the cyclic algebra $A = (K, \langle\sigma\rangle, x, b)$. An interesting example of a twisted group ring of the fours group $\mathbb{Z}_2 \times \mathbb{Z}_2$ is a generalized quaternion algebra which we denote by $\mathbb{H}_p$. Specifically, let F_0 be a field of characteristic $p \neq 2$ and let $F = F_0(a, b)$ be the rational function field over F_0 in the variables a and b. Then $\mathbb{H}_p$ is the four-dimensional F-algebra with basis $1, \mathbf{i}, \mathbf{j}, \mathbf{k}$ subject to the relations $\mathbf{i}^2 = a$, $\mathbf{j}^2 = b$, $\mathbf{ij} = -\mathbf{ji} = \mathbf{k}$. We will sometimes denote this algebra by the symbol $\frac{(a,b)}{F}$.

Lemma 2.3. *Let R be a ring with units u and v, and suppose there exists a homomorphism $\psi\colon R \to \mathbb{H}_p$, for some $\mathbb{H}_p$ with $p \neq 2$. If $\psi(u) = (1+\mathbf{i})/(1-\mathbf{i})$ and $\psi(v) = (1+\mathbf{j})/(1-\mathbf{j})$, then the group $\langle u, v\rangle$ is free of rank 2.*

Proof. We know that $1 \pm \mathbf{i}$ and $1 \pm j$ are units in $\mathbb{H}_p$ and that $\langle 1+\mathbf{i}, 1+\mathbf{j}\rangle$ is free of rank 2 by [5, Proposition 16]. Thus $H = \langle (1+\mathbf{i})^2, (1+\mathbf{j})^2\rangle$ is also free of rank 2. Since noncyclic free groups have trivial center, it follows that the group generated by H and $F^\bullet$ is their direct product, and hence $(1+\mathbf{i})/(1-\mathbf{i}) = (1+\mathbf{i})^2/(1-a)$ and $(1+\mathbf{j})/(1-\mathbf{j}) = (1+\mathbf{j})^2/(1-b)$ generate a free group of rank 2. Since $\psi(u) = (1+\mathbf{i})/(1-\mathbf{i})$ and $\psi(v) = (1+\mathbf{j})/(1-\mathbf{j})$, the same is clearly true of the group $\langle u, v\rangle$. □

Next we consider one more method for constructing free subgroups of units. Let K be a field admitting an automorphism σ and let $K[T;\sigma]$ denote the skew polynomial ring over K in the variable T. By definition, $\alpha T = T\sigma(\alpha)$ for all $\alpha \in K$. Since this ring is a Noetherian domain, it is an Ore domain with division ring of fractions $K(T;\sigma)$.

Proposition 2.4. *Let K, σ and $K[T;\sigma]$ be as above, and let Z be a subfield of the fixed field of σ. Suppose there exists $a \in K$ such that the field $Z(a, \sigma(a), \sigma^2(a), \ldots)$ is not finitely generated over Z. Setting $A = aT$ and $B = \sigma(a)T$ in $K[T;\sigma]$, we have*

i. *The Z-subalgebra of $K[T;\sigma]$ generated by A and B is free on those two generators.*
ii. *The elements $1 + A$ and $1 + B$ in $K(T;\sigma)^\bullet$ generate a free group of rank 2.*
iii. *If N is a normal subgroup of $K(T;\sigma)^\bullet$ containing the element T, then N contains a noncyclic free subgroup.*

Proof. (i) Set $a_i = \sigma^i(a)$ for $i = 0, 1, 2, \ldots$, and suppose by way of contradiction that $Z[A, B]$ is not free on the generators A and B. Since $K[T;\sigma]$ is graded by the powers of T, and since A and B are homogeneous of degree 1, it follows that there exists a Z-linear dependence relation among the monomials in A and B, with all such monomials having the same degree n. Furthermore, we can assume that $n \geq 1$ is minimal with this property, and that the number of terms appearing in this relation is minimal for n.

Let us write the relation as

$$\sum_I \alpha_I B^{i_1} A^{j_1} B^{i_2} A^{j_2} \cdots ,$$

where $I = (i_1, j_1, i_2, j_2, \ldots)$, at least one of i_1 or j_1 is positive, and $0 \neq \alpha_I \in Z$. Furthermore, since the monomials all have degree n, we have $i_1+j_1+i_2+j_2+\cdots = n$. If all i_1 are positive, then we can cancel a factor of B on the left and obtain a relation of degree $n-1$, contradicting the minimality of n. Similarly, if all i_1 are 0, then we can cancel a factor of A, again a contradiction. Thus some, but not all i_1 are zero.

Now write $A = aT = a_0T$ and $B = \sigma(a)T = a_1T$. Using $a_iT = Ta_{i+1}$ in the dependence relation and shifting all factors of T to the left, we obtain, after canceling the factor of T^n, an algebraic relation over Z in $a_0, a_1, \ldots, a_{n+1}$. Furthermore, a_{n+1} occurs precisely when we shift T^{n-1} past $B = a_1T$ and these correspond to the terms that have a left-most factor of B. In other words, the linear dependence relation becomes an expression of the form

$$a_{n+1}f(a_0, a_1, \ldots, a_n) + g(a_0, a_1, \ldots, a_n) = 0,$$

where f and g are suitable polynomials over Z.

Notice that $a_{n+1}f(a_0, a_1, \ldots, a_n)$ corresponds to the sum of those terms in the relation with $i_1 > 0$ and $g(a_0, a_1, \ldots, a_n)$ corresponds to the sum of those terms with $i_1 = 0$. Thus, the minimality of the number of terms in this relation implies that $a_{n+1}f(a_0, a_1, \ldots, a_n) \neq 0$. It follows that $a_{n+1} \in Z(a_0, a_1, \ldots, a_n)$ and, by applying σ^m to this expression, we get $a_{m+n+1} \in Z(a_m, a_{m+1}, \ldots, a_{m+n})$. By induction, $Z(a_0, a_1, a_2, \ldots) = Z(a_0, a_1, \ldots, a_n)$, and this field is finitely generated, a contradiction.

(ii) We follow the argument of Magnus in [19, Theorem 5.6], but we work in the natural Laurent power series ring extension L of $K[T;\sigma]$, obtained from the power series ring $K[[T;\sigma]]$ by adjoining T^{-1}. Notice that this larger ring is also graded by the powers of T, and this grading extends the total degree grading in $Z[A, B]$. Furthermore, since $K[T;\sigma]$ is an Ore domain and L is a division ring, it follows that if $r \in K[T;\sigma]$ and if $r^{-1} \in K[[T;\sigma]]$, then $r^{-1} \in K(T;\sigma)$. Now $A = aT$ and $B = \sigma(a)T$, so it follows that $1 + A$ and $1 + B$ are invertible in $K[[T;\sigma]]$. Hence these inverses are the same as those in $K(T;\sigma)$. To prove that $\langle 1+A, 1+B\rangle$ is free of rank 2, it suffices to show that if

$$W = (1 + A)^{i_1}(1 + B)^{j_1}(1 + A)^{i_2}(1 + B)^{j_2} \cdots (1 + A)^{i_n}(1 + B)^{j_n}$$

is a nonempty reduced word in the units $1 + A$ and $1 + B$, then $W \neq 1$.

Suppose first that $\operatorname{char} K = 0$. Then

$$(1 + A)^{i_m} = 1 + i_mA + A^2*$$

for all integers i_m positive or negative, and where $*$ indicates a power series in A. There is, of course, a similar expression for $(1 + B)^{j_m}$. Since A and B generate a free Z-algebra, it follows that the monomial $ABAB\cdots AB = (AB)^n$ can occur in only one way in the support of W. Indeed, since the number of adjacencies of A and B in $(AB)^n$ is the same as the number of adjacencies of $1 + A$ and $1 + B$ in W, we can only obtain the monomial $(AB)^n$ in the support of W by not using the 1 summands in the above expressions for $(1 + A)^{i_m}$ and $(1 + B)^{j_m}$. With this, it is clear that the monomial $(AB)^n$ occurs in the support of W with coefficient $i_1j_1i_2j_2\cdots i_nj_n \neq 0$, and thus $W \neq 1$, as required.

Finally suppose $\operatorname{char} K = p > 0$ and write each exponent of $1 + A$ and $1 + B$ in W as a power of p times a p'-factor. Say $i_m = p^{\lambda_m}\mu_m$ and $j_m = p^{\lambda'_m}\mu'_m$. Now note that

$$(1 + A)^{p^{\lambda_m}\mu_m} = (1 + A^{p^{\lambda_m}})^{\mu_m} = 1 + \mu_mA^{p^{\lambda_m}} + A^{2p^{\lambda_m}}*$$

for all $\lambda_m \geq 0$ and all integers μ_m. Of course, $*$ again indicates a power series in A, and there is a similar expression for $(1+B)^{p^{\lambda'_m}\mu'_m}$. Since $Z[A,B]$ is free on the two generators, it follows as above that the monomial $A^{p^{\lambda_1}}B^{p^{\lambda'_1}}A^{p^{\lambda_2}}B^{p^{\lambda'_2}}\cdots A^{p^{\lambda_n}}B^{p^{\lambda'_n}}$ can occur in only one way in the support of W. Indeed, it occurs with coefficient $\mu_1\mu'_1\mu_2\mu'_2\cdots\mu_n\mu'_n \neq 0$, and again $W \neq 1$.

(iii) Now we work in $K(T;\sigma)$. Since conjugation by T acts like σ on K, we see that $T^{-1}AT = B$ and hence $T^{-1}(1+A)T = 1+B$. Thus $[T, 1+A] = (1+B)^{-1}(1+A)$ and $[T,(1+A)^{-1}] = (1+B)(1+A)^{-1}$. Since $1+A$ and $1+B$ generate a free group of rank 2, the same is therefore true of $(1+B)^{-1}(1+A)$ and $(1+B)(1+A)^{-1}$. Thus $[T,1+A]$ and $[T,(1+A)^{-1}]$ generate a noncyclic free group, and this group is contained in $N \lhd K(T;\sigma)^\bullet$ since $T \in N$ by assumption. □

3. When N contains a nonabelian nilpotent subgroup

Let $N \lhd D^\bullet$, so that N is a normal subgroup of $D^\bullet$, the multiplicative group of the division ring D. In [16, Theorem 2], Lichtman proved the existence of a free subgroup in N under the assumption that N contains a nonabelian nilpotent-by-finite group. We offer another proof of this result below, explicitly exhibiting the free generators when N contains a nonabelian torsion-free nilpotent subgroup. As usual, we write $[x,y] = x^{-1}y^{-1}xy$ for the group commutator.

Theorem 3.1. *Let D be a division ring with center Z and prime subfield P. Denote the characteristic of Z by $p \geq 0$, and let $N \lhd D^\bullet$. If N contains a nonabelian nilpotent-by-finite subgroup, then N contains a noncyclic free subgroup. In the special case where N contains a nonabelian torsion-free nilpotent subgroup H, we can choose $x, y \in H$ so that $[x,y] = x^{-1}y^{-1}xy = \lambda \neq 1$, and such that λ commutes with both x and y. Since λ has infinite order, we have the following three possibilities.*

i. *λ is transcendental over P and $p \neq 2$. In this case $[x,(1+y)]$ and $[y,(1+x)]$ generate a noncyclic free subgroup of N.*
ii. *λ is transcendental over P and $p = 2$. In this case, if $u = [x,(1+y)]$ and $v = x^2+xy+y^2$, then u and $u^v = v^{-1}uv$ generate a free subgroup of N of rank 2.*
iii. *$p = 0$ and λ is algebraic over $\mathbb{Q}$. Here we can find a nonnegative integer n such that if $u = [y,(1+x^{2^n})]$ and $v = [x^{2^n},(1+y)]$, then u and v generate a noncyclic free subgroup of N.*

Proof. Let G be the nonabelian nilpotent-by-finite group contained in N and let H be the normal nilpotent subgroup of G of finite index.

Suppose first that H is abelian and denote by $P(H)$ the subfield of D generated by P and H. Then the finite group G/H acts as automorphisms on $P(H)$, and the division subring $D_0 = P(G)$ generated by P and G is easily seen to be finite dimensional over the central subfield $P(H)^{G/H}$. In this situation, the normal subgroup $N_0 = N \cap D_0^\bullet$ of $D_0^\bullet$ is non-central since it contains G. By [3, Theorem 2.1], N_0 contains a noncyclic free subgroup and hence the same is true for N.

Thus we can assume that H is nilpotent, but not abelian. In this case, by choosing $x \in \mathfrak{Z}_2(H) \setminus \mathfrak{Z}(H)$ and $y \in H \setminus \mathfrak{C}_H(x)$, we have $[x,y] = \lambda \neq 1$, and $\lambda \in \mathfrak{Z}(H)$ so $[x,\lambda] = 1 = [y,\lambda]$. If λ is an mth root of unity for some $m > 1$, then x^m, y^m and λ are central in $\langle x,y\rangle$, so the latter group is nonabelian and center-by-finite. In particular, it is abelian-by-finite, and the result of the previous paragraph guarantees that N contains a noncyclic free group in this case.

In other words, it suffices to assume that $G = \langle x, y\rangle$ with λ having infinite order. Notice that the structure of G is essentially symmetric in x and y. From $x^{y^i} = x\lambda^i$, for all integers i, we see that the group $\langle y\rangle$ is infinite cyclic and acts faithfully on the field $P(\lambda, x)$, where P is the prime subfield of D. Now there is a natural homomorphism from the skew group ring $P(\lambda, x)*\langle y\rangle$ to D and, since the skew group ring is simple by Lemma 2.2, it follows that $P(\lambda, x)*\langle y\rangle$ embeds in D. In particular, the powers of y are linearly independent over $P(\lambda, x)$. Similarly, the powers of x are linearly independent over $P(\lambda, y)$ and hence over $P(\lambda)$. It follows that the elements x^iy^j are linearly independent over $P(\lambda)$, so the subring of D generated by $P(\lambda), x, x^{-1}, y$ and y^{-1} is naturally isomorphic to a twisted group ring over $P(\lambda)$ of the group $G/\langle\lambda\rangle \cong \mathbb{Z} \times \mathbb{Z}$.

Suppose that λ is transcendental over P. Then $P(\lambda)$ contains the group ring $P[\langle\lambda\rangle]$ and the subring of D generated by P and G is naturally isomorphic to $P[G]$. By the Hilbert Basis Theorem, $P[G]$ is a Noetherian domain and hence, by Goldie's theorem, $P[G]$ is an Ore domain. It follows that $P(G)$, the division subring of D generated by P and G, is the Ore ring of fractions of $P[G]$.

If $p = \operatorname{char} P \neq 2$, we construct a subring R of $P(G)$ as follows. First note that $I = (1 + \lambda)P[G]$ is a strongly prime ideal of the group ring with

$$\psi\colon P[G] \to P[G]/I \cong \mathbb{H}_p = \tfrac{(\overline{x}^2, \overline{y}^2)}{P(\overline{x}^2, \overline{y}^2)}$$

since x^2 and y^2 become central in the quotient. Furthermore, $M = P[G] \setminus I$ is a multiplicatively closed right and left divisor set of $P[G]$ by [11, Lemma 3.2]. Thus we can form $R = M^{-1}P[G] \subseteq P(G)$ and extend the homomorphism $\psi\colon R \to \mathbb{H}_p$. Notice that $u = (1 + x)/(1 + \lambda x)$ and $v = (1 + y)/(1 + \lambda^{-1}y)$ are units of R with $\psi(u) = (1 + \mathbf{i})/(1 - \mathbf{i})$ and $\psi(v) = (1 + \mathbf{j})/(1 - \mathbf{j})$. Thus, by Lemma 2.3, $\langle u, v\rangle$ is free of rank 2. Since $[x, 1 + y] = v$ and $[y, 1 + x] = u$ are elements of $N \lhd D^\bullet$, part (i) of the result now follows.

Part (ii), namely when λ is transcendental over P but $p = 2$, is an immediate consequence of [6, Theorem 27(ii)]. Indeed, by that result, in suitably translated notation, if $u = (1 + y)/(1 + \lambda^{-1}y)$ and $v = x^2 + xy + y^2$, then u and u^v generate a free group of rank 2. This case now follows since the commutator $[x, 1 + y] = u$ is contained in N.

Finally assume that λ is algebraic over P. In particular, since λ has infinite multiplicative order, it follows that $\operatorname{char} P = 0$ and hence that $P = \mathbb{Q}$ is the field of rationals. This situation has been studied in [11], where almost all the work involves constructing a suitable subring S of D. Indeed, by the proof of [11, Theorem1.3(ii)], there exists an integer $n \geq 0$ and a subring S of $P(G)$ that contains $z = x^{2^n}$, y and λ^{2^n}. Furthermore, $1+z$, $1+\lambda^{2^n}z$, $1+y$ and $1+\lambda^{-2^n}y$ are units of S, and there exists a homomorphism $\psi\colon S \to \mathbb{H}_p$, for some $p > 2$, with $\psi(z) = \mathbf{i}$, $\psi(y) = \mathbf{j}$ and $\psi(\lambda^{2^n}) = -1$. Thus, by Lemma 2.3, $u = (1 + z)/(1 + \lambda^{2^n}z)$ and $v = (1 + y)/(1 + \lambda^{-2^n}y)$ generate a free group of rank 2 in $S^\bullet$. Since $u = [y, 1 + z] = [y, 1 + x^{2^n}]$ and $v = [z, 1 + y] = [x^{2^n}, 1 + y]$ both belong to the normal subgroup $N \lhd D^\bullet$, part (iii) is clearly proved. □

We remark that the abelian-by-finite group $G = \langle x, y\rangle$, with $[x, y] = \lambda$ central of finite order $m > 1$, can be studied in a concrete manner using the techniques of the next section. However, we will not pursue this further.

4. When N contains a nonabelian finite subgroup

Note that, in a previous paper [10], we showed how to construct a free group from a finite nonabelian group of units in an algebra over a nonabsolute field. Here we extend this result by constructing the free subgroup inside a normal subgroup of $D^\bullet$.

Theorem 4.1. *Let D be a division ring and let $N \lhd D^\bullet$. If N contains a finite nonabelian subgroup G, then $\operatorname{char} D = 0$ and we can choose $x, y \in G$ so that y normalizes the cyclic group $\langle x \rangle$ and acts on it like an automorphism of prime order. Furthermore, there exists an integer $m \in \mathbb{Z}$ such that if $u = [y, m - x]$ and if $v = (2 + x)/(2 - x)$, then u and u^v generate a free subgroup of N of rank 2.*

To prove this, we require the following two lemmas that consider certain valuations defined on a field. The first is [4, Proposition 2.4].

Lemma 4.2. *Let ν be a nonarchimedean valuation defined on the 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.*

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

The next lemma is the characteristic 0 version of [9, Lemma 2.2].

Lemma 4.3. *Let $\mathbb{Q}$ be the field of rationals, and let $n > 1$ be an integer. Then there exists infinitely many primes p such that, if $\mathbb{Q}_p$ denotes the field of p-adic rationals with ν_p its p-adic valuation, then for any $\varepsilon \in \mathbb{Q}_p$ an n-th root of 1, there exist infinitely many integers $m \in \mathbb{Z}$ such that $\nu_p(m - \varepsilon) > 0$ while $\nu(m - \delta) = 0$ for all remaining $\delta \in \mathbb{Q}_p$ with $\delta^n = 1$.*

With these in hand, we can now offer the

Proof of Theorem 4.1. If P is the prime subfield of D, then the linear span PG of G over P is a finite-dimensional noncommutative division ring. Thus P must have characteristic 0, and in particular $P = \mathbb{Q}$.

Next, since G is finite, we can assume that G has minimal order as a nonabelian subgroup of N. It follows that all proper subgroups of G are abelian, so G is solvable by [20] and G properly contains its commutator subgroup G'. Choose $H \supseteq G'$ to be a maximal subgroup of G. Then $H \lhd G$ since $H \supseteq G'$, and H is abelian since it is a proper subgroup of G. Furthermore, $H = \langle x \rangle$ is cyclic, being a finite abelian subgroup of $D^\bullet$, and G/H has prime order q, since H is maximal. Now H cannot be central in G, since G is nonabelian, so $G = \langle x, y \rangle$ has the appropriate structure, and $h_0 = y^q \in H$. Let y act on the field $P(x) = P(H)$ as the automorphism σ of order q.

Now there is a natural homomorphism from the cyclic algebra $P(H)*(G/H) = (P(x), \langle\sigma\rangle, y, h_0)$ to D and, since G/H acts faithfully on $P(H)$, Lemma 2.2 implies that this homomorphism is an embedding. In particular, the elements $1, y, \ldots, y^{q-1}$ are linearly independent over the field $F = P(x)$, and we let $B = \sum_{i=0}^{q-1} Fy^i$ denote the corresponding cyclic algebra contained in D. Of course, B is a left F-vector space with basis $\{1, y, \ldots, y^{q-1}\}$, and B acts as F-linear transformations on B via the right regular representation. In this way, and using this basis, we obtain a monomorphism $\theta\colon B \to F^{q\times q}$.

Using $\alpha = -1/2$ and $\beta = 1/2$ in Lemma 2.1, we see that $v = (2+y)/(2-y)$ is a unit of B, with v and v^{-1} having full support. It follows that all entries of the matrices $\theta(v)$ and $\theta(v^{-1})$ are nonzero. Furthermore, by writing each such entry as a/b, a ratio of algebraic integers, and by considering the Galois norm $F \to \mathbb{Q}$ applied to these numerators and denominators, it follows that there exists a finite set $\mathcal{P}$ of rational primes, such that if $p \notin \mathcal{P}$ and if ν_p is a p-adic valuation, then all entries of $\theta(v)$ and $\theta(v^{-1})$ have ν_p-value 0.

For the sake of clarity, let us write ε for the nth root of unity x in F, so that $F = P(\varepsilon)$. Then it is easy to see that $\theta(x)$ is a diagonal matrix with diagonal entries $\varepsilon, \sigma^{-1}(\varepsilon), \ldots, \sigma^{-(q-1)}(\varepsilon)$, in that order. Since these are q distinct nth roots of unity in F, Lemma 4.3 implies that there exists an integer m and a prime $p \notin \mathcal{P}$ such that $F \subseteq \mathbb{Q}_p$, $\nu_p(m-\varepsilon) > 0$ and $\nu_p(m-\sigma^i(\varepsilon)) = 0$ for $i = 1, 2, \ldots, q-1$. Here, of course, ν_p is the p-adic valuation associated with $\mathbb{Q}_p$. Since $u = [y, m-x] = (m-x)/(m-x^{y^{-1}})$, it follows that $\theta(u)$ is a diagonal matrix with diagonal entries $(m-\sigma^{-i}(\varepsilon))/(m-\sigma^{-i+1}(\varepsilon))$ for $i = 0, 1, \ldots, q-1$. In particular, one entry has positive ν_p-value, one entry has negative ν_p-value, and all the remaining entries have zero ν_p-value.

It now follows from Lemma 4.2 that $\theta(u)$ and $\theta(u^v) = \theta(v)^{-1}\theta(u)\theta(v)$ generate a free group of rank 2. Hence the same is true for u and u^v, and of course since $y \in N \lhd D^\bullet$ and $u = [y, m-x]$, both u and u^v are contained in N. □

Obviously, there are numerous possibilities for the element v above, and we just took a particularly simple one. Of course, the integer m, used in defining u, depends somewhat on this choice of v.

5. When N contains a nonabelian solvable subgroup

Our final result applies a clever technique introduced by Chiba [1] to construct free subgroups in $D^\bullet$. We extend it to prove

Theorem 5.1. *Let D be a division ring with center Z, and suppose that Z has infinite transcendence degree over its prime subfield P. If $N \lhd D^\bullet$ and N contains a nonabelian solvable subgroup, then N contains a noncyclic free subgroup.*

We will need a number of lemmas given below. To start with, let A be an F-algebra and let $A[y]$ be the polynomial ring in the commuting indeterminate y over A. Then we have the lemma of [7, Section 2].

Lemma 5.2. *Assume that* $\operatorname{char} F = p > 0$ *and let α and β be elements of A such that $\alpha^2 = \beta^2 = 0$ and $\beta\alpha$ is not nilpotent. Let us define elements in $A[y]$ by*

$$x_1 = 1 + y\alpha,$$
$$x_2 = 1 + y\beta\alpha\beta,$$
$$x_3 = 1 + y(1-\beta)\alpha\beta\alpha(1+\beta).$$

Then x_1, x_2 and x_3 are units of order p in the polynomial ring $A[y]$, and $\langle x_1, x_2, x_3\rangle$ is naturally isomorphic to the free product $\mathbb{Z}_p * \mathbb{Z}_p * \mathbb{Z}_p$ of three copies of the cyclic group of order p.

In characteristic 0, we have

Lemma 5.3. *Let A be an algebra over a field F of characteristic* 0*, and let $\alpha, \beta \in A$ satisfy $\alpha^2 = \beta^2 = 0$. If $\alpha\beta$ is transcendental over F, then $1+\alpha$ and $1+\beta$ are units of A generating a free group of rank* 2*.*

Proof. Since $\operatorname{char} F = 0$, we have $F \supseteq \mathbb{Q}$, and hence $\alpha\beta$ is transcendental over the rational field $\mathbb{Q}$. With this, we can assume that $F = \mathbb{Q}$ and then that A is generated by $\mathbb{Q}$, α and β. The argument of [8, Lemma 1.2] now shows that A is isomorphic to a $\mathbb{Q}$-subalgebra of the 2×2 matrix algebra $\mathbb{C}[t]^{2\times 2}$ over the complex polynomial ring $\mathbb{C}[t]$. Indeed, here α corresponds to te_{21} and β corresponds to the matrix unit e_{12}. [8, Lemma 1.2(i)] now yields the result. □

We will need the following fact, [2, Lemma 7.1], concerning algebraically independent elements in division rings.

Lemma 5.4. *Let D be a division ring with center Z, and let D_0 be a division subring of D with center Z_0. Then any subset of Z that is algebraically independent over Z_0 is also algebraically independent over D_0.*

Again, let D be a division ring with center Z, and let $D[X, Y]$ be the polynomial ring over D in the commuting indeterminates X and Y. Then $D[X, Y]$ is a Noetherian domain, so by Goldie's theorem it has a division ring of fractions which we denote by $D(X, Y)$. In the following, we use $[a, b]_\ell = ab - ba$ for the Lie bracket of a and b. Let $R = D[X][[Y]]$ be the power series ring in Y with coefficients in $D[X]$, so that $R \supseteq D[X, Y]$. We start with two simple observations.

Lemma 5.5. *With the above notation, we have*

i. *If $r \in D[X, Y]$ and $r^{-1} \in R$, then $r^{-1} \in D(X, Y)$.*
ii. *Let a and b be noncommuting elements of $D^\bullet$ and suppose that $ab = bc + d$ for some $c, d \in D$ such that a, c and d all commute. Then there exists an element $\bar{b} \in D^\bullet$ that does not commute with a such that $a\bar{b} = \bar{b}c + \bar{d}$. Furthermore, $\bar{d} = 0$ if $a \neq c$, and $\bar{d} = 1$ if $a = c$.*

Proof. (i) Let L be the ring of Laurent series in Y over the division ring $D(X)$. Then L is a division ring containing R and $D[X, Y]$. Since the latter polynomial ring is an Ore domain, the set of fractions of $D[X, Y]$ in L is precisely $D(X, Y)$. With this, (i) is clear.

(ii) Suppose first that $a \neq c$ and let $\bar{b} = b + \beta$ for some $\beta \in Z(a, c, d)$. Then a does not commute with $\bar{b}$, and $a\bar{b} - \bar{b}c = a\beta - \beta c + d$, where the right-hand side is an expression in the commutative field $Z(a, c, d)$. In particular, since $a \neq c$, we can set $\beta = d/(c - a)$ and get $\bar{d} = 0$. On the other hand, if $a = c$, then $d \neq 0$ since a and b do not commute. Thus, setting $\bar{b} = bd^{-1}$ yields the result since d and a commute. □

We continue with the same notation. In particular, D is a division ring with center Z, $D(X, Y)$ is the division ring of fractions of the polynomial ring $D[X, Y]$, and $R = D[X][[Y]]$. The following lemma introduces additional notation and structure.

Lemma 5.6. *Let a and b be noncommuting elements of D, so that $[a, b]_\ell \neq 0$.*

i. *R has a left R-module structure denoted by $\circ$, where $D[[Y]]$ acts on R by left multiplication and where X acts via right multiplication by a. Furthermore, if F is any commutative subring of R centralizing a, then R becomes an (R, F)-bimodule with F acting on R via right multiplication.*
ii. *Let $M = 1F + bF$ be the rank 2 free right F-submodule of R and let us define $S = \{r \in R \mid r \circ M \subseteq M\}$. Then S is a subring of R and the restriction map determines a natural homomorphism $\theta\colon S \to F^{2\times 2}$, using the F-basis*

$\{1, b\}$ *of* M. *Furthermore, if* $s \in S$ *is invertible in* R *and if* $\theta(s)$ *is invertible in* $F^{2\times 2}$, *then* $s^{-1} \in S$.

iii. *If we define*

$$\begin{aligned} d_{11} &= -b[a,b]_\ell^{-1}(bab^{-1} - X) \\ d_{21} &= -b^2[a,b]_\ell^{-1}(bab^{-1} - X) \\ d_{12} &= [a,b]_\ell^{-1}(a - X) \\ d_{22} &= b[a,b]_\ell^{-1}(a - X) \end{aligned}$$

then each d_{ij} *is contained in* S *and* $\theta(d_{ij}) = e_{ij}$, *the matrix unit that has entry* 1 *in the* i, j*-position and* 0*'s elsewhere.*

Proof. (i) Since right and left multiplication commute as operators, this fact is clear for the smaller ring $D[[Y]][X]$. For the larger ring R, we can verify this directly or use the fact that it is a limit with respect to the variable Y of the polynomial ring $D[X, Y]$.

(ii) Since F centralizes a, but b does not, it follows that 1 and b are F-linearly independent, and M is indeed a rank 2 free right F-submodule of R. Of course, S is a subring of R and M is a left S-module. Indeed, S acts like F-linear transformations on M, so we obtain the homomorphism θ using the basis $\{1, b\}$. Finally, if $s \in S$ is invertible in R, and if $\theta(s)$ is invertible in $F^{2\times 2}$, then the latter implies that $s \circ M = M$. Applying $s^{-1} \in R$ yields $M = s^{-1}s \circ M = s^{-1} \circ M$ and $s^{-1} \in S$.

(iii) First observe that $(a-X)\circ 1 = a1-1a = 0$ and $(a-X)\circ b = ab-ba = [a,b]_\ell$. Also $(bab^{-1} - X) \circ 1 = bab^{-1} - a = -[a,b]_\ell b^{-1}$ and $(bab^{-1} - X) \circ b = ba - ba = 0$. The remaining computations are now immediate. □

At this point, we bring the normal subgroup N into play and assume that $a \in N$. Unlike the work in [1] where the free subgroup is allowed to be anywhere within the division ring, we need to force the free subgroup to be contained in N. This requires keeping better track of the element a, and we do this by assuming that $ab = bc + d$, where c and d commute with each other and with a. In view of Lemma 5.5(ii), we can suitably modify b and obtain two special cases according to whether $a \neq c$ or $a = c$. As we see below, the element a belongs to S but does not act on M as a scalar matrix. Because of this, it is less clear which elements of $F^{2\times 2}$ actually belong to the image $\theta(S)$. We settle this in the next result. Again, we use much of the previous notation. In particular, we use the elements d_{ij} as defined in Lemma 5.6(iii).

Lemma 5.7. *Let* a *and* b *be noncommuting elements of* $D^\bullet$.

i. *Assume that* $ab = bc$ *for some* $c \in D^\bullet$ *that commutes with* a. *Let* $F_0 = Z[a, a^{-1}, c, c^{-1}]$ *and set* $F = F_0[[Y]]$. *Then* $\theta(S \cap D[X])$ *contains* $F_0^{2\times 2}$.

ii. *Now suppose that* $ab - ba = 1$. *If* $F_0 = Z[a, a^{-1}]$ *and* $F = F_0[[Y]]$, *then again* $\theta(S \cap D[X])$ *contains* $F_0^{2\times 2}$.

Proof. We already know that each d_{ij} is contained in $S \cap D[X]$ and that $\theta(d_{ij}) = e_{ij}$. Because of this, it suffices to show that $\theta(S \cap D[X])$ contains $F_0 e_{11}$. Indeed, since θ is a Z-linear map, we need only show that $\theta(S \cap D[X])$ contains the additive generators of F_0 times e_{11}.

We consider part (ii) first. Here $ab = ba + 1$, so

$$\theta(a) = \begin{bmatrix} a & 0 \\ 1 & a \end{bmatrix}.$$

Notice that $\theta(a)$ is invertible in $F^{2\times 2}$ and that a is invertible in R. Thus, by Lemma 5.6(ii), we have $a^{-1} \in S$. Now, for any positive or negative integer k, the $1,1$-entry of $\theta(a^k)$ is a^k. Thus $\theta(d_{11}a^k d_{11}) = a^k e_{11}$ and this case is proved.

Finally, for part (i), we see that $\theta(a) = \operatorname{diag}(a, c)$ and hence $\theta(a^k) = \operatorname{diag}(a^k, c^k)$. Furthermore, $a^{-1} \in S$, as above. In particular, if k and ℓ are both integers, then $\theta(d_{11}a^k d_{11}\cdot d_{12}a^\ell d_{21}) = a^k c^\ell e_{11}$, and the lemma is proved. □

Since the above formulas are somewhat unpleasant, we abbreviate them so that if $f \in F_0$, then $f\#d_{ij}$ is the element we constructed in $S\cap D[X]$ with $\theta(f\#d_{ij}) = fe_{ij}$.

We now state our main applications of Chiba's method. Since there are two cases, according to whether $a = c$ or not, and since each case involves three different field characteristics, we split the conclusions into two different propositions. We start with the $a \neq c$ case.

Proposition 5.8. *Let D be a division ring with center Z, and let N be a normal subgroup of $D(X,Y)^\bullet$. Suppose there exist noncommuting elements $a \in N \cap D^\bullet$ and $b \in D^\bullet$ such that $ab = bc$ for some $c \in D^\bullet$ that commutes with a. Then N contains a noncyclic free subgroup. Specifically, we have*

i. *If $\operatorname{char} Z = 0$, then the elements $[a, 1 + Yd_{12}]$ and $[a, 1 + Yd_{21}]$ generate a noncyclic free subgroup of N.*
ii. *If $\operatorname{char} Z = p > 2$, set $u = [a, 1+Yd_{12}]$ and $v = [a, 1+Yd_{21}]$. Then uv and vu generate a free subgroup of N of rank 2.*
iii. *If $\operatorname{char} Z = p \geq 2$, set $u = [a, 1 + Yd_{12}]$, $v = [a, 1 + Yd_{21}]$ and*

$$w = 1 + Y(1 - ca^{-1})^2\#(d_{11} - d_{22} + d_{12} - d_{21}).$$

Then $[u, w]$ and $[v, w]$ generate a noncyclic free subgroup of N.

Proof. Notice that $a \neq c$ since a and b do not commute. We will work in $R = D[X][[Y]]$, a domain that contains some, but not all of, $D(X,Y)$. Here, using $F = Z[a.a^{-1}, c, c^{-1}][[Y]]$ in the previous two lemmas, we see that $a \in S$ with $\theta(a) = \operatorname{diag}(a, c)$ and $Y \in S$ with $\theta(Y) = \operatorname{diag}(Y, Y)$. Notice that a, $1 + Yd_{12}$ and $1 + Yd_{21}$ are invertible in R and that their images under θ are invertible in $F^{2\times 2}$. Thus a^{-1}, $(1 + Yd_{12})^{-1}$ and $(1 + Yd_{21})^{-1}$ are contained in S, by Lemma 5.6(ii). Of course, these inverses are also contained in $D(X,Y)$ by Lemma 5.5(i). Thus $u = [a, 1+Yd_{12}]$ and $v = [a, 1+Yd_{21}]$ are contained in $N \lhd D(X,Y)^\bullet$. Furthermore,

$$\theta(u) = \begin{bmatrix} 1 & (1 - ca^{-1})Y \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad \theta(v) = \begin{bmatrix} 1 & 0 \\ (1 - ca^{-1})Y & 1 \end{bmatrix}.$$

If $\operatorname{char} Z = 0$, we apply Lemma 5.3 with $\alpha = (1 - ca^{-1})Ye_{12}$ and with $\beta = (1 - ca^{-1})Ye_{21}$. Then $\alpha\beta = (1 - ca^{-1})^2Y^2e_{11}$ is transcendental over $Z(a, c)$, so $\theta(u)$ and $\theta(v)$ generate a free group of rank 2, and hence the same is true of u and v. This proves part (i).

On the other hand, if $\operatorname{char} Z = p > 0$, set

$$w = 1 + Y(1 - ca^{-1})^2\#(d_{11} - d_{22} + d_{12} - d_{21}),$$

using the notation of Lemma 5.7, so that

$$\theta(w) = 1 + Y(1 - ca^{-1})^2(e_{11} - e_{22} + e_{12} - e_{21}).$$

Again, w is a unit of S and, by Lemma 5.2 with $y = Y$, $\alpha = (1 - ca^{-1})e_{12}$ and $\beta = e_{21}$, we see that $\langle \theta(u), \theta(v), \theta(w) \rangle$ is naturally isomorphic to the free product $\mathbb{Z}_p * \mathbb{Z}_p * \mathbb{Z}_p$. In particular, if $p > 2$, then $\theta(u)\theta(v)$ and $\theta(v)\theta(u)$ generate a free group of rank 2, so the same is true of uv and vu. Thus part (ii) is proved.

Finally, if $p \geq 2$, then $[\theta(u), \theta(w)]$ and $[\theta(v), \theta(w)]$ generate a noncyclic free group, so the same is true of $[u, w]$ and $[v, w]$. The result follows. □

Next we consider the situation where $a = c$. Thus, in view of Lemma 5.5(ii), we can assume that $[a, b]_\ell = ab - ba = 1$. Obviously this simplifies the formulas for the various d_{ij} given in Lemma 5.6(iii).

Proposition 5.9. *Let D be a division ring with center Z, and let N be a normal subgroup of $D(X, Y)^\bullet$. Suppose there exist elements $a \in N \cap D^\bullet$ and $b \in D^\bullet$ such that $ab - ba = 1$. Then N contains a noncyclic free subgroup. Specifically, we have*

i. *If $\operatorname{char} Z = 0$, set $u = 1 + Yd_{12}$. Then a and a^u generate a noncyclic free subgroup of N.*
ii. *If $\operatorname{char} Z = p > 2$, set $x = 1 + Yd_{11}$ and $v = 1 + Ya^{-1}\#d_{12}$. Then $[a, x][a, x]^v$ and $[a, x]^v[a, x]$ generate a free subgroup of N of rank 2.*
iii. *If $\operatorname{char} Z = p \geq 2$, set $x = 1 + Yd_{11}$, $v = 1 + Ya^{-1}\#d_{21}$ and*

$$w = 1 + Ya^{-2}\#(d_{11} - d_{22} + d_{12} - d_{21}).$$

Then the triple commutators $[a, x, v]$ and $[a, x, w]$ generate a noncyclic free subgroup of N.

Proof. Clearly a and b do not commute. Again, we work in $R = D[X][[Y]]$ and we use $F = Z[a, a^{-1}][[Y]]$ in Lemmas 5.6 and 5.7. Notice that $a, Y \in S$ with

$$\theta(a) = \begin{bmatrix} a & 0 \\ 1 & a \end{bmatrix} \quad \text{and} \quad \theta(Y) = \begin{bmatrix} Y & 0 \\ 0 & Y \end{bmatrix}.$$

Also a, $x = 1 + Yd_{11}$, $u = 1 + Yd_{12}$, $v = 1 + Ya^{-1}\#d_{12}$ and w are invertible in R and their images under θ are invertible in $F^{2\times 2}$. Thus the inverses of these elements are contained in S by Lemma 5.6(ii), and then in $S \cap D(X, Y)$ by Lemma 5.5(i).

If $\operatorname{char} Z = 0$, write $\mathcal{A} = \operatorname{diag}(a, a) \in F^{2\times 2}$, so that $\theta(a) = \mathcal{A}(1 + \overline{\alpha})$, where $\overline{\alpha} = a^{-1}e_{21}$. Also $\theta(u) = 1 + \overline{\beta}$, where $\overline{\beta} = Ye_{12}$. Since $\overline{\alpha}^2 = \overline{\beta}^2 = 0$ and since $\overline{\alpha}\overline{\beta} = a^{-1}Ye_{22}$ is transcendental over Z, it follows from Lemma 5.3 that $1 + \overline{\alpha}$ and $1 + \overline{\beta}$ generate a free rank 2 subgroup of $\mathrm{GL}_2(F)$. Since this free subgroup has trivial center, we conclude that $\theta(a) = \mathcal{A}(1 + \overline{\alpha})$ and $\theta(u) = 1 + \overline{\beta}$ generate a noncyclic free group. Hence the same is true of the group $\langle a, u \rangle$ and then of $\langle a, a^u \rangle$. This proves (i).

Now suppose $\operatorname{char} Z = p \geq 2$ and note that $\theta([a, x]) = 1 + Y\alpha$ where $\alpha = a^{-1}e_{21}$. Then applying Lemma 5.2 with $y = Y$ and $\beta = e_{12}$, we see that the group $\langle \theta([a, x]), \theta(v), \theta(w) \rangle$ is naturally isomorphic to the free product $\mathbb{Z}_p * \mathbb{Z}_p * \mathbb{Z}_p$. If $p > 2$, it follows that $\theta([a, x])\theta([a, x])^{\theta(v)}$ and $\theta([a, x])^{\theta(v)}\theta([a, x])$ generate a free subgroup of $\mathrm{GL}_2(F)$, so (ii) is proved. Finally, for all $p \geq 2$, the commutators $[\theta([a, x]), \theta(v)]$ and $[\theta([a, x]), \theta(w)]$ generate a free subgroup of $\mathrm{GL}_2(F)$, so the result follows. □

As a consequence, we have

Corollary 5.10. *Let D be a division ring with uncountable center Z, and let N be a normal subgroup of $D^\bullet$. Suppose there exist noncommuting elements $a \in N$ and*

$b \in D^\bullet$ such that $ab = bc + d$ for suitable elements $c, d \in D$, such that a, c and d all commute. Then N contains a noncyclic free subgroup.

Proof. According to Lemma 5.5(ii), we can assume that either $a \neq c$ and $d = 0$, or $a = c$ and $d = 1$. Now let D_0 be the division subring of D generated by a, b, c and d, and let $Z_0 = \mathfrak{Z}(D_0)$. Then D_0 and Z_0 are countable. But, by assumption, Z is uncountable, so the field extension ZZ_0/Z_0 must have infinite transcendence degree. In particular, we can choose $X, Y \in Z$ that are algebraically independent over Z_0. By Lemma 5.4, X and Y are also algebraically independent over D_0, so the subring of D generated by D_0, X and Y is clearly the polynomial ring $D_0[X, Y]$. Since the latter ring is an Ore domain, we have $D_0(X, Y) \subseteq D$. Now $N_0 = N \cap D_0(X, Y)^\bullet$ is a normal subgroup of $D_0(X, Y)^\bullet$ and $a \in N_0$, so Propositions 5.8 and 5.9 imply that N_0 contains a noncyclic free subgroup. Hence the same is true of $N \supseteq N_0$. □

Finally, we combine a number of these techniques to prove our main result.

Proof of Theorem 5.1. Let $\overline{G}$ be the given nonabelian solvable subgroup of N and let G be the next to the last nonidentity term in its derived series. Then G is also nonabelian, but G' is abelian. Next, let H be a maximal abelian subgroup of G containing G'. Then $H \lhd G$ and maximality implies that G/H acts faithfully on H. Since H is not central in G, we can choose $a \in H$ and $b \in G \setminus H$ such that a and b do not commute. Furthermore, since H is abelian and $a \in H \lhd G$, all conjugates a^{b^m} commute. Of course, both a and b are contained in N.

Now let F be the subfield of D generated by P and all the $\langle b\rangle$-conjugates of a. Then $\langle b\rangle$ acts nontrivially on F and we let b^n generate the cyclic subgroup of $\langle b\rangle$ that is the centralizer of F in $\langle b\rangle$. We of course allow the possibility that $n = 0$. Set $F_0 = F(b^n)$ and note that $\langle b\rangle/\langle b^n\rangle$ acts faithfully on F_0. Furthermore, there is a natural homomorphism from a suitable crossed product $R = F_0 * (\langle b\rangle/\langle b^n\rangle)$ into D. Since this crossed product is simple, by Lemma 2.2, the homomorphism is an embedding, and we can view R as a subring of D. Furthermore, since $\langle b\rangle/\langle b^n\rangle$ is a cyclic group, the Hilbert basis theorem implies that R is a Noetherian domain. Hence, by Goldie's theorem, R has a division ring of fractions D_0, and D_0 is contained naturally in D.

Suppose first that F_0 is a finitely generated field extension of P, and let $Z_0 = \mathfrak{Z}(R)$. Then, by Lemma 2.2, Z_0 is a subfield of F_0 and $Z_0 = \mathfrak{Z}(D_0)$. Since F_0 is finitely generated, we have $\operatorname{tr.deg}(F_0/P) < \infty$ and hence $\operatorname{tr.deg}(Z_0/P) < \infty$. On the other hand, by assumption, $\operatorname{tr.deg}(Z/P) = \infty$. Thus, by considering the field extension ZZ_0/Z_0, we see that there exist elements $X, Y \in Z$ that are algebraically independent over Z_0. By Lemma 5.4, X and Y are also algebraically independent over D_0. But $X, Y \in Z$, so the subring of D generated by D_0, X and Y is clearly the polynomial ring $D_0[X, Y]$. Furthermore, D contains $D_0(X, Y)$. Now $a, b \in D_0$ and $ab = bc$, where $c = b^{-1}ab \neq a$ and c commutes with a. Since $a \in N_0 = N \cap D_0(X, Y)^\bullet \lhd D_0(X, Y)^\bullet$, Proposition 5.8 implies that N_0 contains a noncyclic free subgroup, and therefore the same is true for $N \supseteq N_0$.

Finally, suppose F_0 is not finitely generated over P, and let F_+ be the subfield of F_0 generated over P by all conjugates a^{b^m} with $m \geq 0$. Similarly, let F_- be the subfield of F_0 generated by all conjugates a^{b^m} with $m \leq 0$. Then one of F_+ or F_- is not finitely generated over P and, by replacing b by b^{-1} if necessary, we can assume that F_+ is not finitely generated over P. Note that there must be infinitely many $\langle b\rangle$-conjugates of a, so $\langle b\rangle$ is infinite cyclic and $n = 0$ in this case. If b acts on F_0 as

the automorphism σ, we see that the subring of $R = F_0*\langle b\rangle$ generated by F_0 and b is isomorphic to the skew polynomial ring $F_0[T;\sigma]$, where T plays the role of b. Furthermore, this ring satisfies all the hypotheses of Proposition 2.4. In particular, since $T = b \in N_1 = N \cap F_0(T;\sigma)^\bullet \lhd F_0(T;\sigma)^\bullet$, we conclude from part (iii) of that proposition that N_1 contains a noncyclic free subgroup. Hence the same is true for the normal subgroup $N \supseteq N_1$. □

References

[1] Chiba, K., *Free subgroups and free subsemigroups of division rings*, J. Algebra **184** (1996), 570–574.

[2] Ferreira, V. O., Gonçalves, J. Z. and Mandel, A., *Free symmetric and unitary pairs in division rings with involution*, Internat. J. Algebra Comp. **15**, 1 (2005), 15–36.

[3] Gonçalves, J. Z., *Free groups in subnormal subgroups and the residual nilpotence of the group of units of group rings*, Canad. Math. Bull. **27** (1984), 365–370.

[4] Gonçalves, J. Z. and Lichtman, A. I., *Free subgroups in division rings generated by group rings of soluble groups*, Int. J. Algebra Comp., **24**, 8 (2014), 1127–1140.

[5] Gonçalves, J. Z., Mandel, A. and Shirvani, M., *Free products in algebras I. Quaternion algebras*, J. Algebra **214** (1999), 301–316.

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

[7] Gonçalves, J. Z. and Passman, D. S., *Construction of free subgroups in the group of units of modular group algebras*, Commun. Algebra **24** (1996), 4211–4215.

[8] ———, *Involutions and free pairs of bicyclic units in integral group rings*, J. Group Theory, **13** (2010), 721–742.

[9] ———, *Unitary units in group algebras*, Israel J. Math. **125** (2001), 131–155.

[10] ———, *Free unit groups in algebras*, Commun. Algebra, **31**, 5 (2003), 2219–2227.

[11] ———, *Explicit free groups in division rings.* Proc. AMS, **143**, 2 (2015), 459–468.

[12] Gonçalves, J. Z. and Shirvani, M., *Free symmetric and unitary pairs in central simple algebras with involution*, Contemporary Math. **420** (2006), 121–139.

[13] ———, *Algebraic elements as free factors in simple artinian rings.* Contemporary Math. **499** (2009), 121–125.

[14] ———, *A survey on free objects in division rings and in division rings with an involution*, Commun. Algebra **40** (2012), 1704–1723.

[15] Lichtman, A. I., *On the subgroups of the multiplicative group of skewfields.* Proc. AMS **63** (1977), 15–16.

[16] ———, *Free subgroups of normal subgroups of the multiplicative group of skew fields*, Proc. AMS **7**, 2 (1978), 174–178.

[17] ———, *On normal subgroups of the multiplicative group of skew fields generated by polycyclic-by-finite groups.* J. Algebra **78** (1982), 548–577.

[18] ———, *Matrix rings and linear groups over a field of fractions of enveloping algebras and group rings I*, J. Algebra **88** (1984), 1–37.

[19] Magnus, W., Karras, A. and Solitar, D., *Combinatorial group theory: Presentations of groups in terms of generators and relations*, Dover, second edition, New York, 1976.

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

Department of Mathematics, University of São Paulo, São Paulo, 05508-090, Brazil
E-mail address: jz.goncalves@usp.br

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