ON FREE SUBGROUPS IN DIVISION RINGS

JASON P. BELL AND JAIRO GONÇALVES

ABSTRACT. Let $K$ be a field and let $\sigma$ be an automorphism and let $\delta$ be a $\sigma$-derivation of $K$. Then we show that the multiplicative group of nonzero elements of the division ring $D = K(x; \sigma, \delta)$ contains a free non-cyclic subgroup unless $D$ is commutative, answering a special case of a conjecture of Lichtman. As an application, we show that division algebras formed by taking the Goldie ring of quotients of group algebras of torsion-free non-abelian solvable-by-finite groups always contain free non-cyclic subgroups.

1. Introduction

Let $D$ be a division ring and let $D^* = D \setminus \{0\}$ the multiplicative group of $D$. The existence of free subobjects in $D$ and $D^*$ has been studied in several different contexts (see, for example, [ML83, ML84, ML84A, ML84B, ML91, Lor86, Lic78, Lic82, FGF18]). The most important of these are the study of free multiplicative semigroups of rank two in $D$, free non-cyclic subgroups of $D^*$, and free subalgebras of rank two in $D$. The guiding philosophy in all of these conjectures is that division rings that are not locally finite-dimensional over their centres should be very large and unwieldy and have big subgroups and big subalgebras. The question of the existence of free non-cyclic subgroups in the nonzero elements of a division ring $D$, goes back to a work of Lichtman [Lic77], who conjectured that if $D$ is a division ring that is not a field then $D^*$ contains a free group of rank two. This is known in several cases, including the case when $D$ is finite-dimensional over its centre, where it can be deduced from the Tits alternative for linear groups [Lic78, Gon84]. Beyond this case, Lichtman’s conjecture has been verified for several special cases of algebras, including division rings whose multiplicative group contains a non-abelian nilpotent-by-finite subgroup [Lic78], division algebras of polycyclic-by-finite group algebras [Lic82], quotient division rings of enveloping algebras of finite-dimensional or solvable non-abelian Lie algebras over a field of characteristic zero [Lic84]. In terms of general results, arguably the best result concerning the existence of free subgroups in division rings is a result of Chiba’s [Chi96], who shows that if $D$ is a division ring with uncountable centre then $D^*$ contains a free group. In this note, we prove Lichtman’s conjecture in two cases that apply to a broad class of division rings: Ore extensions of fields and group algebras of torsion-free solvable-by-finite groups.

We recall that if $K$ is a field and $\sigma$ is an automorphism of $K$ and $\delta : K \to K$ is a $\sigma$-derivation (that is, $\delta(ab) = \delta(a)b + \sigma(a)\delta(b)$ for $a, b \in K$) then we can form a skew polynomial ring $K[x; \sigma, \delta]$, which is, as a set, just the polynomial ring $K[x]$ but with “skewed” multiplication given by the rule that multiplication of elements of $K$ remains the same, but for $\alpha \in K$ and $x$ the indeterminate we have the rule $x \cdot \alpha = \sigma(\alpha)x + \delta(\alpha)$. This ring is a noetherian domain and in a semiprime noetherian ring $R$ one can invert the regular elements (non-zero divisors of $R$) to obtain a quotient division ring $\text{Frac}(R)$, which is semiprime Artinian and which we think of as being a “noncommutative field of fractions.” In the case when $R = K[x; \sigma, \delta]$, we let $K(x; \sigma, \delta)$ denote $\text{Frac}(R)$, and this quotient

2010 Mathematics Subject Classification. 12E15, 16K40, 20E05.

Key words and phrases. Division rings, free groups, group algebras, solvable-by-finite groups, Ore extensions.
ring is a division ring that is not a field unless \( \sigma \) is the identity and \( \delta = 0 \). In the case that \( \delta = 0 \) we simply write \( K[x; \sigma] \) for \( K[x; \sigma, \delta] \) and call this an Ore extension of automorphism type. In the case when \( \sigma \) is the identity, \( \delta \) is just an ordinary derivation and we write \( K[x; \sigma, \delta] \) and call this an Ore extension of derivation type. Our main result is the following theorem.

**Theorem 1.1.** Let \( K \) be a field, let \( \sigma \) be an automorphism of \( K \) and let \( \delta \) be a \( \sigma \)-derivation of \( K \). Then if the division ring \( K(x; \sigma, \delta) \) is not commutative then the group of units of \( K(x; \sigma, \delta) \) contains a free non-cyclic subgroup.

In fact, in the pure automorphism case the result we prove is somewhat stronger than Theorem 1.1 (see the statement of Theorem 2.4). The stronger form is useful in terms of the strategy of proof, because we show there are “lifting” techniques which allow one to pass to simple homomorphic images of the rings we consider.

Division rings of the form \( K(x; \sigma, \delta) \) have been considered in this context (see, for example, [BR12, Lor86, FGS96, FGF18]), but results of the form given in Theorem 1.1, when \( K \) is countable, have only been proved in a few instances where one has an explicit form of the automorphism or some other constraints. Once one moves beyond division rings that are finite-dimensional over their centres, where Lichtman’s conjecture is known to hold [Lic78, Gon84], the first natural class of division rings to consider are precisely those formed by Ore extensions of fields, since they in some sense provide the first examples of division rings that are infinite-dimensional over their centres that are not locally finite-dimensional.

The main issue that arises in this context is that one quickly encounters thorny dynamical problems involving birational maps when studying the existence of free subgroups in this setting. We are able to prove this result by first reducing it to the case of algebras of the form \( K(x; \sigma) \) with \( K \) a finitely generated extension of the prime field. We then show that one can further reduce to the case when \( K \) has positive characteristic. Our main tool in this setting is the following deep result of Hrushovski’s, which the authors learned of through an application of this result by Amerik [Ame11].

**Theorem 1.2.** ([Hru04, Corollary 1.2]) Let \( U \) be an affine variety over a finite field \( \mathbb{F}_q \) and let \( S \subseteq U^2 \) be an irreducible subvariety over \( \overline{\mathbb{F}}_q \). Assume that the two projections of \( S \) to \( U \) are dominant. Let \( \phi_q \) denote the \( q \)-Frobenius map. Then for any proper subvariety \( W \) of \( U \), for sufficiently large \( m \), there exists \( x \in U(\overline{\mathbb{F}}_q) \) with \( (x, \phi_q^m(x)) \in S \) and \( x \notin W \).

Using Hrushovski’s result, we can reduce the positive characteristic case to the case of an algebra satisfying a polynomial identity, which we are able to handle via the Tits alternative. A consequence of Theorem 1.1 is the following result concerning group algebras.

**Corollary 1.3.** Let \( G \) be a non-abelian torsion-free solvable-by-finite group and let \( k \) be a field. Then the the quotient division algebra of the group algebra \( k[G] \) contains a free non-cyclic multiplicative subgroup.

The corollary follows from Theorem 1.1 in a straightforward manner. First, a non-abelian solvable group contains a non-abelian metabelian subgroup and so we can quickly reduce to the metabelian case. It can be shown that non-abelian metabelian groups either contain a non-abelian abelian-by-finite subgroup or a semidirect product of an abelian group with an infinite cyclic group; the second case can be handled with Theorem 1.1, while the first case follows from work of Passman and Isaacs along with earlier work of Lichtman using the Tits alternative.

The outline of the paper is as follows. In §2 we give the basic facts involving regular extensions and introduce the notion of pro-unipotence, which will be a key part of the argument in providing a
framework via which we can lift free subgroups. In §3 and §4 we will prove the automorphism case of Theorem 1.1 in the case when \( K \) is finitely generated over a prime subfield of positive characteristic and zero characteristic respectively. We need the result of Hrushovski mentioned above to handle the positive characteristic case; the characteristic zero case is handled via reduction to the positive characteristic case. In §5 we prove Theorem 1.1 and finally in §6 we prove Corollary 1.3.

2. Preliminaries

In this section, we give some of the basic concepts we will need in proving Theorem 1.1. We start with the notion of regular extensions. Let \( K \) be a field extension of a field \( k \). We recall that \( K \) is a regular extension of \( k \) if \( K \otimes_k F \) is an integral domain for every field extension \( F \) of \( k \). This in turn is equivalent to \( k \) being algebraically closed in \( K \) and \( K \) having a separating transcendence base (i.e., \( K \) has a subfield \( L \) that is a purely transcendental extension of \( k \) and such that \( K \) is separable over \( L \)). In characteristic zero, having a separating transcendence base is automatic; in positive characteristic, this simply means that there is a purely transcendental extension \( L \) of \( k \) inside of \( K \) such that \( K \) is a separable algebraic extension of \( L \). The main significance of regularity is given by the following result.

**Proposition 2.1.** Let \( C \) be a finitely generated commutative \( \mathbb{Z} \)-algebra and let \( R \) be a finitely generated commutative \( C \)-algebra with \( C \subseteq R \) and suppose that \( C \) and \( R \) are integral domains. If \( \text{Frac}(R) \) is a regular extension of \( \text{Frac}(C) \) then there is a nonzero \( c \in C \) such that \( R/PR \) is an integral domain for every prime \( P \) in \( \text{Spec}(C) \) such that \( c \notin P \).

**Proof.** Let \( X = \text{Spec}(R) \) and let \( Y = \text{Spec}(C) \). Then the inclusion \( C \to R \) and the fact that \( R \) is a finitely presented \( C \)-algebra gives a morphism of finite presentation \( f : X \to Y \). Let \( S = C \setminus \{0\} \). Then \( S^{-1}R \) is a \( \text{Frac}(C) \)-algebra with field of fractions \( \text{Frac}(R) \) and since \( \text{Frac}(R) \) is a regular extension of \( \text{Frac}(C) \), we have

\[
S^{-1}R \otimes_{\text{Frac}(C)} \overline{\text{Frac}(C)}
\]

is an integral domain. This means that the generic fiber of \( f \) is geometrically irreducible, and so by [Gro66, Theorem 9.7.7] there is a non-empty open subset \( U \) of \( Y \) such that for points \( P \in U \) we have \( R \otimes_C C/P = R/PR \) is an integral domain. Then since \( U \) is open, its complement is a closed subset and thus contained in a closed set of the form \( \{Q : c \in Q\} \) for some \( c \). It follows that \( U \) contains the open set of primes \( P \) such that \( c \notin P \) and so we obtain the result. \( \square \)

**Definition 2.2.** Let \( R \) be a commutative noetherian integral domain with an automorphism \( \sigma \). We say that an element \( u \) of the units group of \( \text{Frac}(R[x;\sigma]) \) is pro-unipotent with respect to \( R \) if it is of the form \((1 + a)(1 + b)^{-1}\) with \( a, b \in xR[x;\sigma] \). In the case that \( R \) is a field we will call elements that are pro-unipotent with respect to \( R \) simply pro-unipotent.

We recall that we can complete \( R[x;\sigma] \) at the prime ideal \((x)\) to obtain a skew power series ring \( R[[x;\sigma]] \). The justification for the term pro-unipotent comes from the fact that if we let \( I_n = x^nR[[x;\sigma]] \), then regarding a pro-unipotent element \( u = (1 + a)(1 + b)^{-1} \) (with respect to \( R \)) as an element of \( R[[x;\sigma]] \) (by expanding \((1 + b)^{-1}\) as a skew power series and left multiplying by \((1 + a)\)), we see that it has the property that \( u - 1 \) is nilpotent mod \( I_n \) and so the image of \( u \) is a unipotent element of \( R[[x;\sigma]]/I_n \) for every \( n \geq 1 \). We remark that in the case when \( R \) is a field it is straightforward to show that the pro-unipotent elements form a normal subgroup of \( \text{Frac}(R[x;\sigma])^* \). The significance for pro-unipotence is that pro-unipotent elements have well behaved lifting properties that allow us to lift free subgroups from homomorphic images. We make this precise with the following lemma.
Lemma 2.3. Let $R$ and $S$ be commutative noetherian integral domains, let $\sigma$ and $\tau$ be automorphisms of $R$ and $S$ respectively, and suppose that there is a surjective homomorphism $\phi : R[x; \sigma] \to S[x; \tau]$ of graded algebras; that is, $\phi(Rx^n) = Sx^n$ for $n \in \mathbb{N}$. Then if there exist elements $u, v$ in $\text{Frac}(S[x; \tau])$ that are pro-unipotent with respect to $S$ that generate a free non-cyclic subgroup of the units group of $\text{Frac}(S[x; \tau])$ then there exist $u', v'$ in $\text{Frac}(R[x; \sigma])$, pro-unipotent with respect to $R$, that generate a free non-cyclic subgroup of $\text{Frac}(R[x; \sigma])^\ast$.

Proof. Since $\phi$ is a degree-preserving homomorphism, $\phi$ extends to a surjective homomorphism $\hat{\phi} : R[[x; \sigma]] \to S[[t; \tau]]$. By assumption, there exist $a, b, c, d \in xS[x; \tau]$ such that $u := (1+a)(1+b)^{-1}$ and $v := (1+c)(1+d)^{-1}$ are units in $\text{Frac}(S[x; \tau])$ and such that they generate a free non-cyclic subgroup of the units group of $S[[x; \tau]]$. Now $\hat{\phi}$ is surjective and so we may pick $a', b', c', d' \in x\hat{R}[x; \sigma]$ such that $\hat{\phi}(a') = a, \hat{\phi}(b') = b, \hat{\phi}(c') = c, \hat{\phi}(d')$. Then $u' := (1+a')(1+b')^{-1}, v' := (1+c')(1+d')^{-1} \in \text{Frac}(R[x; \sigma])^\ast$ and regarding $u, v, u', v'$ as skew power series we have $\hat{\phi}(u') = u$ and $\hat{\phi}(v') = v$. Then since $u$ and $v$ generate a free group, we see that $u'$ and $v'$ must too, since a non-trivial relation involving $u'$ and $v'$ in $\text{Frac}(R[x; \sigma])^\ast$ would give a relation in $\text{Frac}(R[[x; \sigma]])^\ast$ and this would then give a corresponding non-trivial relation involving $u$ and $v$ via the map $\hat{\phi}$. \qed

Our goal is to use this lemma as a reduction tool in proving the following strengthening of Theorem 1.1.

Theorem 2.4. Let $K$ be a field and let $\sigma$ be an automorphism of $K$ that is not the identity. Then there exist pro-unipotent elements of $\text{Frac}(K[x; \sigma])$ that generate a non-cyclic multiplicative free group.

In the next section, we shall begin the proof of this result using Lemma 2.3 to provide a series of reductions.

3. Theorem 2.4 in the case that $K$ is finitely generated over a finite field

In this section we prove the following result, which deals with Theorem 2.4 in the case when $K$ is finitely generated over a finite field. This is really the key step in our analysis and we divide the proof into the cases when the automorphism $\sigma$ has finite order and when it has infinite order; the infinite order case reduces to the finite order case.

The finite-order case is relatively straightforward and we prove a more general result.

Proposition 3.1. Let $K$ be a field and let $\sigma$ be a non-identity automorphism of $K$ of finite order. Then there are pro-unipotent $u, v$ in $\text{Frac}(K[x; \sigma])$ that generate a free non-cyclic multiplicative subgroup of the units group.

Proof. Since $\sigma$ has finite order, $D = \text{Frac}(K[x; \sigma])$ is finite-dimensional over its centre. In particular, $D^\ast$ is a matrix group. Notice that the set of pro-unipotent elements forms a normal subgroup of $D^\ast$. Then since $N$ is non-abelian, we get the result in this case [Lic78, Gon84]. \qed

Proposition 3.2. Let $k$ be a finite field and let $K$ be a finitely generated extension of $k$ and let $\sigma$ be a non-identity $k$-algebra automorphism of $K$. Then there exist pro-unipotent elements $u$ and $v$ of $K(x; \sigma)$ such that $u$ and $v$ generate a free non-cyclic subgroup of the units group of $K(x; \sigma)$.

Proof. The case when $\sigma$ has finite order follows from Proposition 3.1. Thus we may assume that $\sigma$ has infinite order. By enlarging $k$ if necessary and replacing $\sigma$ by $\sigma^m$ for some $m \geq 1$, we may work instead with $K(x^m; \sigma^m)$ and assume that $k$ is algebraically closed in $K$ and that $\sigma$ restricts to the identity on $k$. Pick a transcendence base $t_1, \ldots, t_d$ for $K/k$ and let $K'$ denote the separable closure
of $k(t_1, \ldots, t_d)$ inside $K$. Then $K'$ is an extension of $k$ and by construction $k$ is algebraically closed in $K'$ and $K'$ has a separating transcendence base. Thus $K'$ is a regular extension of $k$. Then since the Frobenius map is surjective on $k$ and since $K$ is a finite extension of $K'$, there is some $s \geq 1$ such that $L := K^{p^s} := \{a^{p^s} : a \in K\}$ is contained in $K'$ and contains $k$. Then $L$ is a regular extension of $k$ as it is contained in $K'$. Moreover, $\sigma$ restricts to a non-identity automorphism of $L$ since $p^s$-th roots of elements are unique in $K$. Then $K'$ is a regular extension of $k$.

Since $K'/k$ is regular, it follows that $L := K' \otimes_k \bar{k}$ is a finitely generated field extension of $\bar{k}$ and thus $L$ is the field field of a normal projective variety $X$ defined over $\bar{k}$. Moreover, the automorphism $\sigma$ induces a non-identity automorphism of $L$ and hence induces a birational automorphism $\phi$ of $X$ that is not the identity. Let $t_1, \ldots, t_d$ be generators for $K'$ as a field extension of $k$. Since $K' \subseteq L = \bar{k}(X)$, we can regard each $t_i$ as a rational map from $X$ to $\mathbb{P}_k^1$. Then since $\sigma$ is not equal to the identity, we have $\sigma(t_i) \neq t_i$ for some $i$ and by reindexing, we may assume that $i = 1$. Then $\sigma(t_1) - t_1$ is a nonzero map from $X$ to $\mathbb{P}_k^1$, and we let $Y$ denote the zero locus of this map, which is a proper subvariety of $X$. Let $\phi$ be the birational map of $X$ induced by $\sigma$, let $I$ denote the indeterminacy locus of $\phi$ and let $Z$ denote the closed subvariety of $X \setminus I$ given by $\{x \in X \setminus I : \phi(x) = x\}$. We let $W$ denote a codimension-1 subvariety of $X$ such that $t_1, \ldots, t_d, \sigma(t_1)$ are regular on $X \setminus W$.

Then $X, Z, I, Y, W$, and $\phi$ are defined over $\bar{k}$, but since they are defined in terms of a finite amount of geometric data, they are in fact defined over a finite field $k'$ for some power extension $k' \supseteq k$, and $\phi$ is defined over $k'$. Let $q$ denote the size of $k$, and so the $q$-power Frobenius acts as the identity on $k$. Then $Z, I, Y, W$ all have a finite orbit under the action of the $q$-power Frobenius map. We let $V$ denote the union of the $q$-Frobenius orbits of $Z, I, Y, W$. Then $V$ is a proper subvariety of $X$ and by Hrushovski’s result (Theorem 1.2) we have that there is some $\bar{k}$-point $x \in X \setminus V$ such that $\phi(x) = F^j(x)$ for some $j$, where $F$ is the $q$-power Frobenius. Notice that since $\phi$ is defined over $k'$ and so $\phi(F^j(x)) = F^j(\phi(x))$ and since $x \notin I$, we see that $F^j(x) \notin V$ by definition of $V$ and so $F^j(x) \notin I$ and so we have $\phi^2(x) = F^{2j}(x)$ and similarly we have $\phi^m(x) = F^{mj}(x)$. Since $x$ is a $\bar{k}$-point and $\phi$ is defined over $k$ and since the orbit of $x$ avoids the indeterminacy locus of $\phi$, it has finite orbit under the automorphism $F^j$ and so there is some $m$ such that $\phi^m(x) = x$. Let $S = \{x_1, \ldots, x_d\}$ denote the orbit of $x$ under $\phi$. Then consider the semilocal ring $\mathcal{O}_{X,S}$, the collection of functions in $L$ that are regular at all points of $S$. By construction $\mathcal{O}_{X,S}$ is invariant under $\sigma$ and $\mathcal{O}_{X,S}$ has a $\sigma$-invariant ideal $P_{X,S}$, consisting of functions that vanish on $S$. Then $\mathcal{O}_{X,S}/P_{X,S} \cong \bar{k}^d$. We let $T$ denote the elements in $K'$ that are in $\mathcal{O}_{X,S}$. By construction, the functions $t_1, \ldots, t_d, \sigma(t_1)$ are all regular on $S$ and so they are in $T$. Thus $T$ has field of fractions equal to $K'$. Furthermore, by construction $t_1 - \sigma(t_1) \notin P_{X,S}$ and so $\sigma$ induces a non-identity automorphism of $T/P_{X,S} \cap T$. Notice that each element of $T$ is a rational function in $t_1, \ldots, t_d$ that is regular at all points of $S$. Moreover, modulo $P_{X,S}$, each element of $t_i$ maps to an element of $k^d$ and so $B := T/P_{X,S} \cap T$ is a finite reduced ring and $\sigma$ induces a non-identity automorphism of $B$. Notice also that if $f \in T$ vanishes on some $x_i$ then since $K'$ is a regular extension of $k$, we have, as a rational map from $X$ to $\mathbb{P}_k^1$, that $f$ is defined over $k$ and so $f \circ F^m(x_i) = F^m(f(x_i)) = 0$ and so $f$ vanishes on all of $S$. Thus $P_{X,S} \cap T$ is a prime ideal and so $B$ is a finite field. Then by Proposition 3.1, there are pro-unipotent elements $u, v \in \text{Frac}(B[t; \sigma])$ that generate a free group of rank two. Thus by Lemma 2.3, there are pro-unipotent elements $u', v' \in \text{Frac}(T[t; \sigma])$ that generate a free group of rank two. Then since $\text{Frac}(T[t; \sigma]) = \text{Frac}(K[x; \sigma])$ we get the result in this case. $\square$
4. Theorem 2.4 in the case when \( K \) is finitely generated over the rational numbers

In this section we show that Theorem 2.4 holds when \( K \) is a finitely generated extension of \( \mathbb{Q} \). To do this, we show that we can create a \( \sigma \)-invariant local subalgebra of \( K \) that surjects onto a finitely generated extension of a finite field; we then use the results of §3 and Lemma 2.3 to obtain the result in this case.

Lemma 4.1. Let \( K \) be a finitely generated extension of \( \mathbb{Q} \), let \( \sigma \) be a field automorphism of \( K \) that is not the identity automorphism, and let \( k \) be the fixed field of \( \sigma \). If \( K \) is a regular extension of \( k \) then there is a \( \sigma \)-invariant local subring \( S \subseteq K \) with maximal ideal \( P \) such that:

(i) \( S/P \) is a finitely generated extension of a finite field;

(ii) \( \sigma \) induces a non-identity automorphism \( \sigma \) of \( S/P \).

Proof. We pick a finitely generated subring \( C \) of \( k \) such that \( \text{Frac}(C) = k \). We pick a transcendence base \( t_1, \ldots, t_d \) for \( K \) over \( k \) Then \( K \) is a finite-dimensional \( k(t_1, \ldots, t_d) \)-vector space and we let \( 1 = a_1, \ldots, a_m \) be a basis for this space. Since \( k \) is algebraically closed in \( K \) and \( \sigma \) is not the identity, we may pick our transcendence base in such a way that \( \sigma(t_1) \neq t_1 \).

Then let \( S \) denote the finitely generated \( C \)-algebra generated by \( \sigma^j(t_i) \) and \( \sigma^j(a_i) \) for \( j = -1, 0, 1, i = 1, \ldots, d \), and \( \ell = 1, \ldots, m \). We let \( R = C[t_1, \ldots, t_d] \). Then there is some nonzero \( h \in R \) such that \( S[1/h] \) is integral over \( R[1/h] \) and \( S[1/\sigma(h)] \) is integral over \( \sigma(R)[1/\sigma(h)] \) and \( S[1/\sigma^{-1}(h)] \) is integral over \( \sigma^{-1}(R)[1/\sigma^{-1}(h)] \). By Proposition 2.1, we can invert a single element of \( C \) if necessary and assume that every prime ideal \( P \in \text{Spec}(C) \) has the property that \( PS \) is a prime ideal of \( S \) and \( PS[1/\sigma(h)] \) is a prime ideal of \( S[1/\sigma(h)] \) for \( j = -1, 0, 1 \), and so we may enlarge \( C \) if necessary and assume that this is the case.

Now since \( K \) is an algebraic over \( k(t_1, \ldots, t_d) \) and since \( \text{Frac}(S) = K \) and \( \text{Frac}(C[t_1, \ldots, t_d]) = k(t_1, \ldots, t_d) \), we see that there exists a nonzero polynomial \( q(t_1, \ldots, t_d) \in C[t_1, \ldots, t_d] \) such that \( q\sigma^j(t_i), q\sigma^j(a_i), q\sigma^j(h)^{-1} \in S \) for \( j = -2, \ldots, 2 \) and \( i = 1, \ldots, d \), and \( \ell = 1, \ldots, m \). Now since the intersection of primes of the form \( PS \) with \( P \) a maximal ideal of \( C \) has trivial intersection, we may pick a maximal ideal \( P \) of \( C \) such that \( (\sigma(t_1) - t_1)h \in S \). Now we claim that \( \sigma \) restricts to an automorphism of the local ring \( SP_S \). To see this, observe that by construction each generator \( u \) of the finite set of generators we have given for \( S \) has the property that \( \sigma(u), \sigma^{-1}(u) \in SP_S \), since \( q \notin PS \). Furthermore, we have \( \sigma(1/h) \) and \( \sigma^{-1}(1/h) \) are in \( SP_S \) by construction and so \( \sigma \) and \( \sigma^{-1} \) map \( S[1/h] \) into \( SP_S \). Since \( \sigma \) and \( \sigma^{-1} \) are \( C \)-linear we also have \( \sigma(PS[1/h]) \subseteq PS_P \) and \( \sigma^{-1}(PS[1/h]) \subseteq PS_P \). Now we claim that \( \sigma^{-1}(PS_P) \cap S[1/h] = PS[1/h] \). To see this, suppose that this is not the case. Then since \( \sigma(PS[1/h]) \subseteq PS_P \), we must have \( \sigma^{-1}(PS_P) \cap S[1/h] = Q \) for some \( Q \in \text{Spec}(S[1/h]) \) that properly contains \( PS \). Then since \( S[1/h] \) is integral over \( R[1/h] = C[t_1, \ldots, t_d][1/h] \), we see that \( Q \cap R[1/h] \) properly contains \( SP \cap R[1/h] = PR[1/h] \). Thus \( Q \cap R[1/h] \) contains a polynomial \( f(t_1, \ldots, t_d) \in C[t_1, \ldots, t_d] \) that is not in \( P[t_1, \ldots, t_d] \).

But then by construction \( \sigma(f) \in PS_P \). But notice that \( \sigma \) maps \( C[t_1, \ldots, t_d] \) into \( S \) and so \( \sigma(f) \in PS_P \cap S[1/h] = PS[1/h] \). But we showed \( \sigma^{-1}(PS[1/h]) \subseteq PS_P \) and so \( f \in PS_P \). But since \( f \in S[1/h] \) we see that \( f \in S[1/h] \cap PS_P = PS[1/h] \). In fact, we have \( f \in R[1/h] \) and so \( f \in PS[1/h] \cap R[1/h] \). But this intersection is equal to \( PR[1/h] \), which follows from the fact that \( P \) is a prime ideal of \( C \) and \( PR[1/h] \) is a prime ideal of \( R[1/h] \) since \( R \) is a polynomial ring over \( C \) and so \( PS[1/h] = (PR[1/h])S[1/h] \) by integrality we then have \( PS[1/h] \cap R[1/h] = PR[1/h] \). This is a contradiction. It follows that \( \sigma^{-1}(PS_P) \cap S[1/h] = PS[1/h] \) and similarly we have \( \sigma(PS_P) \cap S[1/h] = PS[1/h] \) but this means that the injective map \( \sigma : S[1/h] \to SP_S \) sends elements outside of \( PS[1/h] \) to units of \( SP_S \) and so \( \sigma \) restricts to an injective homomorphism from \( SP_S \) to itself; similarly, \( \sigma^{-1} : SP_S \to SP_S \) and so \( \sigma \) restricts to an automorphism of \( SP_S \). Now since
$C$ is a finitely generated $\mathbb{Z}$-algebra, we see that for maximal ideals $P$ of $C$ that $C/P$ is a finite field and $L := S_{PS}/PS \cong \text{Frac}(S/PS)$. By construction $\sigma$-induces a $C/P$-algebra automorphism of $L$; this automorphism is not the identity since $\sigma(t_1) - t_1 \in S$ and is not in $PS$ by construction and so we obtain the result.

From this we obtain the following result.

**Proposition 4.2.** Let $K$ be a finitely generated extension of $\mathbb{Q}$ and let $\sigma$ be an automorphism of $K$. Then there exist pro-unipotent elements $u$ and $v$ of $K(x; \sigma)$ such that $u$ and $v$ generate a free non-cyclic subgroup of the units group of $K(x; \sigma)$.

**Proof.** If $\sigma$ has finite order on $K$ then we get the result from Proposition 3.1. Thus we may assume that $\sigma$ has infinite order. Let $k$ denote the fixed field of $K$ and let $k_0$ denote the algebraic closure of $k$ in $K$. Then since $K$ is finitely generated over $k$, we have $k_0$ is finitely generated over $k$ [*Vám79] and so $k_0$ is a finite extension of $k$. Then there is some $m > 1$ such that $\sigma^m$ is the identity on $k_0$. Then we may replace $x$ by $x^m$ and $\sigma$ by $\sigma^m$ and assume that the fixed field of $\sigma$ is algebraically closed in $K$ and thus $K$ is a regular extension of its fixed field. Thus we can pick an $\sigma$-invariant local subring $S$ of $K$ satisfying the conditions of Lemma 4.1. Then $S[x; \sigma]$ surjects onto $(S/P)[x; \sigma]$ and the latter ring has the property that $\text{Frac}((S/P)[x; \sigma])$ contains pro-unipotent elements that generate a free non-cyclic multiplicative subgroup by Proposition 3.2, and so $\text{Frac}(S[x; \sigma])$ has this property too by Lemma 2.3. Thus we get the result in this case.

5. **Proof of Theorems 2.4 and 1.1**

We now prove the main result of this paper. We begin by completing the proof of the automorphism case of Theorem 1.1.

**Proof of Theorem 2.4.** We let $k_0$ denote the prime subfield of $k$ and we pick $c \in K$ such that $\sigma(c) \neq c$. Then let $K' = k_0(\{\sigma^n(c) : n \in \mathbb{Z}\})$. Then $\sigma$ induces a non-identity automorphism of $K'$ and since $K'(t; \sigma)$ embeds in $K(t; \sigma)$ it suffices to prove the result for $K'(t; \sigma)$.

If $K'$ is not finitely generated as an extension of $k_0$ then at least one of $K_1 := k_0(\{\sigma^n(c) : n \geq 0\})$ and $K_2 := k_0(\{\sigma^n(c) : n \leq 0\})$ must be non-finitely generated as a field extension of $k_0$. Without loss of generality, we may assume that $K_1$ is not finitely generated as an extension of $k_0$. Then by [BR12, Proposition 3.2] we have that the elements $cx$ and $cx^2$ generate a free $k_0$-subalgebra of $K(x; \sigma)$, and hence $a := \sigma(\sigma(c))x = (cx)(cx^2)$ and $b := \sigma^2(c)x^3 = (cx^2)(cx)$ generate a free $k_0$-subalgebra of $K(x; \sigma)$. But by a result of Sáchez [Sán18, Theorem pp. 2–3] we then have that $1 + a$ and $1 + b$ generate a free non-cyclic subgroup of $K(x; \sigma)^*$ and these elements are evidently pro-unipotent. Thus we may assume that $K'$ is a finitely generated extension of $k_0$ and so it suffices to consider the case when $K$ is a finitely generated extension of its prime subfield. If $k_0$ has characteristic zero, then we get the result from Proposition 4.2; if $k_0$ has positive characteristic then the result follows from Proposition 3.2. The result now follows.

We can now immediately deduce Theorem 1.1.

**Proof of Theorem 1.1.** A folklore result says that $K(x; \sigma, \delta)$ is isomorphic to a division ring of the form $K(x; \sigma)$ or $K(x; \delta)$ with $\sigma$ an automorphism and $\delta$ a derivation (see [BR12, Lemma 5.1] for a proof). In the case when $D = K(x; \delta)$ and $\delta \neq 0$, there is some $c \in K$ such that $b := \delta(c) \neq 0$. Then $[b^{-1}x, c] = 1$ and so $D$ contains a copy of the Weyl division algebra. It is known that the Weyl division algebra contains a free non-cyclic multiplicative subgroup regardless of the characteristic of $\mathbb{Z}$.

---

1We note that the argument in this paper was actually supplied by the anonymous referee.
the base field and so we get the result in this case. The automorphism case follows from Theorem 2.4.

6. Application to group algebras

In this section, we give as an application a result about the existence of free subgroups in group algebras of solvable groups. We note that when $G$ is a torsion-free solvable group, we have that the group algebra $k[G]$ is a domain and has a quotient division ring $\text{Frac}(k[G])$ (see [Pass11, KLM88]).

**Proof of Corollary 1.3.** We first consider the case when $G$ is a torsion-free non-abelian solvable group. To show that $\text{Frac}(k[G])$ contains a free group of rank two, first observe that $G$ contains a non-abelian metabelian subgroup $H$ and since Frac$(k[H])$ embeds in Frac$(k[G])$, it is enough to consider the case when $G$ is metabelian. We pick $a, b \in G$ that do not commute and since Frac$(k[(a, b)])$ embeds in Frac$(k[G])$, we can further assume that $G$ is finitely generated. Let $A = G'$ and pick $x \in G$ that does not commute with every element of the normal subgroup $A$. If $x^m \in A$ for some $m \geq 1$, then letting $B = \langle A, x \rangle$, we see that $B$ is a non-abelian group that is abelian-by-finite and so Frac$(k[B])$ is finite-dimensional over its centre and hence contains a free group of rank two by [Lic78, Gon84] and thus Frac$(k[G])$ contains a free group of rank two. Thus we may assume that $x^m \notin A$ for $m \geq 1$. Thus $E := \langle A, x \rangle \cong A \rtimes \mathbb{Z}$ and so $k[E] \cong k[A][t, t^{-1}; \sigma]$, where $\sigma$ is the non-identity automorphism of $k[A]$ induced by conjugation by $x$. Then Frac$(k[E])$ contains a free group of rank two by Theorem 1.1 and so Frac$(k[G])$ does since by construction it contains Frac$(k[E])$. The result follows in this case.

When $G$ is a non-abelian solvable-by-finite, either $G$ is has a non-abelian finite-index solvable subgroup in which case we get the result from the above, or $G$ is abelian-by-finite in which case $k[G]$ is a finite module over its centre and we get the result from [Lic78, Gon84].

**References**

[Ame11] E. Amerik, Existence of non-preperiodic algebraic points for a rational self-map of infinite order. *Math. Res. Lett.* **18** (2011), no. 2, 251–256.

[BG16] J. P. Bell and J. Z. Gonçalves, Free algebras and free groups in Ore extensions and free group algebras in division rings. *J. Algebra* **455** (2016), 235–250.

[BR12] J. P. Bell and D. Rogalski, Free subalgebras of quotient rings of Ore extensions. *Algebra Number Theory* **6** (2012), no. 7, 1349–1367.

[Chi96] K. Chiba, Free subgroups and free subsemigroups of division rings. *J. Algebra* **184** (1996) 570–574.

[FGF18] V. O. Ferreira, J. Z. Goncalves and E. Z. Fornaroli, Free algebras in a division ring with an involution. *J. Algebra* **509**, (2018), 292–306.

[FGS96] L. M. Figueiredo, J. Z. Gonçalves, and M. Shirvani, Free group algebras in certain division rings. *J. Algebra* **185** (1996) 298–313.

[Gon84] J. Z. Goncalves, Free groups in subnormal subgroups and the residual nilpotence of the group of units of group rings. *Canad. Math. Bull.* **27** (1984) 365–370.

[Gro66] Grothendieck, A. ‘Eléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. III. Inst. Hautes Études Sci. Publ. Math.* No. 28 1966, 255 pp.

[Hru04] E. Hrushovski, *The elementary theory of the Frobenius automorphism*, 2004. Available at arXiv:0406514v1.

[KLM88] P. H. Kropholler, P. A. Linnel and J. A. Moody, Applications of a new K-theoretic theorem to soluble group rings. *Proceedings of AMS* **104** (1988) 3, 675–684.

[Lic77] A. Lichtman, On subgroups of the multiplicative group of skew fields. *Proc. Amer. Math. Soc.* **63** (1977), no. 1, 15–16.

[Lic78] A. Lichtman, Free subgroups of normal subgroups of the multiplicative group of skew fields. *Proc. Amer. Math. Soc.* **71** (1978), no. 2, 174–178.

[Lic82] A. Lichtman, On normal subgroups of the multiplicative group of skew fields generate by poly cyclic-by-finite groups. *J. Algebra* **78** (1982), 548–577.
[Lic84] A. Lichtman, Matrix rings and linear groups over a field of fractions of enveloping algebras and group rings. \textit{J. Algebra} \textbf{88} (1984), 1–37.

[Lor86] M. Lorenz, On free subalgebras of certain division rings. \textit{Proceedings AMS} \textbf{98} (1986), 401–405.

[ML83] L. Makar-Limanov, The skew field of fractions of the Weyl algebra contains free noncommutative algebra. \textit{Comm. Algebra} \textbf{17} (1983), 2003–2006.

[ML84] \textit{On free subsemigroups of skew fields}. \textit{Proceedings AMS} \textbf{91} (1984), 2, 189–191.

[ML84A] \textit{On free subobjects of skew fields}. \textit{Methods in ring theory}. NATO ASI, Series C \textbf{233}. Reidel, Boston, 1984, 281–285.

[ML84B] \textit{On the group rings of nilpotent groups}. \textit{Israel J. Math.} \textbf{48} (1984), 245–248.

[ML91] \textit{On subalgebras of the first Weyl skew field}. \textit{Comm. Algebra} \textbf{91} (1991), 1971–1982.

[Pass11] D. S. Passman. \textit{The algebraic structure of group rings}. Dover Publications Inc., Mineola, New York, 2011.

[Sán18] J. Sánchez, \textit{Free group algebras in division rings with valuation I}. Available at arXiv:1806.10711.

[Vám79] P. Vamos, On the minimal prime ideal of a tensor product of two fields. \textit{Math. Proc. Cambridge Philos. Soc.} \textbf{84} (1978), no. 1, 25–35.

\textsc{Department of Pure Mathematics, University of Waterloo, Waterloo, ON N2L 3G1, Canada}

\textit{E-mail address:} jpbell@uwaterloo.ca

\textsc{Department of Mathematics, University of São Paulo, São Paulo, SP, 05508-090, Brazil}

\textit{E-mail address:} jz.goncalves@usp.br