ISRAEL JOURNAL OF MATHEMATICS **143** (2004), 341–359

FINITELY GENERATED SIMPLE ALGEBRAS: A QUESTION OF B. I. PLOTKIN

BY

A. I. LICHTMAN*

Department of Mathematics, University of Wisconsin-Parkside
Kenosha, WI 53141, USA
e-mail: lichtman@uwp.edu

AND

D. S. PASSMAN

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

ABSTRACT

In his recent series of lectures, Prof. B. I. Plotkin discussed geometrical properties of the variety of associative K-algebras. In particular, he studied geometrically noetherian and logically noetherian algebras and, in this connection, he asked whether there exist uncountably many simple K-algebras with a fixed finite number of generators. We answer this question in the affirmative using both crossed product constructions and HNN extensions of division rings. Specifically, we show that there exist uncountably many nonisomorphic 4-generator simple Ore domains, and also uncountably many nonisomorphic division algebras having 2 generators as a division algebra.

* The first author is grateful to Professor B. I. Plotkin for communicating this problem to him and for stimulating conversations.
Received September 3, 2002

1. Introduction

In his recent series of lectures [Pl], B. I. Plotkin discussed some geometrical properties of the variety of associative K-algebras. In particular, he considered geometrically noetherian and logically noetherian algebras and, in this connection, he asked whether there exist uncountably many simple K-algebras with a fixed finite number of generators. We answer this question in the affirmative using both crossed product constructions and HNN extensions of division rings. To be precise, we show that there exist uncountably many nonisomorphic 4-generator simple Ore domains, and also uncountably many nonisomorphic division algebras having 2 generators as a division algebra. These results can be viewed as algebra analogs of the well-known theorem [N] which asserts that there exist uncountably many nonisomorphic 2-generator groups. Indeed, it was shown in [H] that there exist uncountably many nonisomorphic 6-generator simple groups (see [LS, Theorems IV.3.3 and IV.3.5]).

Our first three results use crossed product constructions and are proved in the next two sections. As will be apparent, a key ingredient here is the fact that any field K has uncountably many nonisomorphic field extensions of transcendence degree 1.

THEOREM 1.1: *Suppose that K is a field having an element ζ of infinite multiplicative order with its nth roots, for all $n = 1, 2, 3, \ldots$, also contained in K. Then there exist uncountably many nonisomorphic K-algebras R such that*

(i) *R is a simple right and left Ore domain.*
(ii) *R is generated as a K-algebra by four elements.*
(iii) *$\mathbb{Z}(R) = K$.*

Each such ring R is a crossed product $E*G$, where E is a K-algebra integral domain with quotient field F having transcendence degree 1 over K. Furthermore, G is the wreath product $G = C \wr C$ with C infinite cyclic.

Since $\mathbb{Z}(R) = K$, the above algebras are actually nonisomorphic as rings. As a consequence of the above construction, we also show

THEOREM 1.2: *Let K be a field containing all nth roots of unity. Then there exist uncountably many nonisomorphic K-algebras D such that*

(i) *D is a division ring.*
(ii) *D is generated as a K-division algebra by two elements.*
(iii) *$\mathbb{Z}(D) = K(t)$, the rational function field over K in one variable t.*

Each such D is the division ring of fractions of a crossed product $E*G$, where E is a K-algebra integral domain with quotient field F having transcendence *degree 1 over K. Furthermore, G is the wreath product $G = C \wr C$ with C infinite cyclic.*

In the next result, we allow the centers of the algebras to vary.

PROPOSITION 1.3: *If K is an arbitrary field, then there exist uncountably many nonisomorphic K-algebras R such that*

(i) *R is a right and left Ore domain with division ring of fractions D.*
(ii) *R is generated as a K-algebra by four elements. D is generated as a K-division algebra by two elements.*
(iii) *$F = \mathbb{Z}(D)$ is the field of fractions of $E = \mathbb{Z}(R)$, and these fields F, each of transcendence degree 1 over K, are different K-algebras for the different choices of R.*

Each such ring R is a twisted group ring $E^t[G]$, where $G = C \wr C$ with C infinite cyclic. Furthermore, if K is countable then these examples can be constructed with $E = F$ and hence with R a simple ring.

The remaining two results concern division algebras. They are proved, by means of HNN extensions, in the last section of this paper. Again, we use the fact that any field K has uncountably many nonisomorphic field extensions of transcendence degree 1.

THEOREM 1.4: *If K is an arbitrary field, then there exist uncountably many nonisomorphic K-algebras D such that*

(i) *D is a division ring.*
(ii) *D is generated as a K-division algebra by two elements.*
(iii) *$\mathbb{Z}(D) = K(t)$, the rational function field over K in one variable t.*

Each such D is the universal field of fractions of an HNN extension of the free field $F\langle\!\langle x, y\rangle\!\rangle$, with F a field extension of K of transcendence degree 1.

Finally, we allow the centers to vary, and obtain

PROPOSITION 1.5: *If K is an arbitrary field, then there exist uncountably many nonisomorphic K-algebras D such that*

(i) *D is a division ring.*
(ii) *D is generated as a K-division algebra by two elements.*
(iii) *$F = \mathbb{Z}(D)$ is a field of transcendence degree 1 over K, and these fields are different K-algebras for the different choices of D.*

Each such D is the universal field of fractions of an HNN extension of the free field $F\langle\!\langle x, y\rangle\!\rangle$ on two generators.

2. Crossed product constructions

Let K be a field and let F be a countably generated field extension. Suppose $\mathcal{F}$ is such a countable generating set consisting of nonzero elements, so that $F = K(\mathcal{F})$. We assume for convenience that either each element of $\mathcal{F}$ has infinite multiplicative order or that each element has finite multiplicative order, but that these orders are unbounded. In addition, let σ be a given field automorphism of F whose fixed field F^σ contains K, and let E be the K-subalgebra of F generated by the set $\mathcal{F} \cup \mathcal{F}^{-1}$ and all its conjugates under the cyclic group $\langle\sigma\rangle$. The goal of this section is to construct four K-algebras based upon the above information. First, $T = F^t[A]$ is a twisted group algebra over F of the countably generated free abelian group A. Next, $S = TC = F{*}G$ is a skew group ring over T of the infinite cyclic group C. It can also be viewed as a crossed product over F of the wreath product group $G = C \wr C$. Thirdly, R is the K-subalgebra of S given by $R = E{*}G \subseteq F{*}G = S$. Then R is a right and left Ore domain, and it is a finitely generated K-algebra. Furthermore, if E is σ-simple, then R is a simple ring. In any case, we let D denote its division ring of fractions.

LEMMA 2.1: *Construction of the twisted group algebra $T = F^t[A]$.*

Proof: Suppose $\mathcal{F} = \{g_0, g_1, g_2, \ldots\}$ and define $\mathcal{F}_1 = \{f_1, f_2, f_3, \ldots\} \subseteq F$ so that $f_1 = g_0$, $f_2 = g_1$, $f_4 = g_2$ and in general $f_{2^n} = g_n$. Furthermore, set $f_i = 1$ if i is not a power of 2. Then this new sequence contains all the given generators of F along with arbitrarily long subsequences of 1's.

Now let H be the free class 2 nilpotent group on countably many generators $\{a_i \mid i \in Z\}$, where Z is the set of all integers. Then the commutator subgroup H' of H is central and generated by the commutators $u_{i,j} = [a_i, a_j]$ for all $i, j \in Z$ with $i > j$. Indeed, H/H' is free abelian with generators $\{a_i H' \mid i \in Z\}$ and H' is free abelian with generators $\{u_{i,j} \mid i > j\}$. Form the group ring $F[H]$ and let P be the kernel of the homomorphism φ: $F[H'] \to F$ given by $\varphi(u_{i,j}) = \sigma^j(f_{i-j})$. Since H' is central, it follows that $Q = P{\cdot}F[H]$ is an ideal of $F[H]$ and then $T = F[H]/Q$ is clearly a twisted group algebra of $A = H/H'$ over F. Indeed, if $\bar{a}_i$ denotes the image of a_i in $F[H]/Q$, then T has as an F-basis all expressions $\bar{a} = \prod_i \bar{a}_i^{k_i}$, with the product in the natural order. Furthermore, $[\bar{a}_i, \bar{a}_j] = (\bar{a}_i)^{-1}(\bar{a}_j)^{-1}\bar{a}_i\bar{a}_j = \sigma^j(f_{i-j})$ for all $i > j$. Hence we can write $T = F^t[A]$, and we let $\bar{A} = \{\bar{a} \mid a \in A\}$ denote the corresponding basis. ∎

LEMMA 2.2: *T is a simple right and left Ore domain with center F.*

Proof: If $a \in A$, then a determines a map λ_a: $A \to F^\bullet$, the multiplicative group of F, given by $\bar{x}^{-1}\bar{a}\bar{x} = \lambda_a(x)\bar{a}$ for all $x \in A$ or equivalently $\lambda_a(x) = \bar{a}^{-1}\bar{x}^{-1}\bar{a}\bar{x} = [\bar{a}, \bar{x}]$. It is easy to see that each such λ_a is a group character, namely a group homomorphism to $F^\bullet$. Furthermore, $\lambda_{ab} = \lambda_a\lambda_b$ for all $a, b \in A$. We claim now that if $a \neq 1$, then $\lambda_a \neq 1$. To this end, let $a = \prod_m^n a_i^{k_i}$ with $k_n \neq 0$. Then the nature of the $\mathcal{F}_1$-sequence guarantees that we can find a sufficiently negative subscript $j < m$ so that f_{n-j} has multiplicative order larger than $|k_n|$, while $f_{i-j} = 1$ for the remaining subscripts i satisfying $m \leq i < n$. Recall that the generators in $\mathcal{F}$ are assumed to either all have infinite multiplicative order or they all have finite multiplicative order, but that these orders are unbounded. In particular, since $\lambda_{a_i}(a_j) = \sigma^j(f_{i-j})$ for $i > j$, we conclude that $\lambda_a(a_j) = \prod_{i=m}^n \lambda_{a_i}(a_j)^{k_i} = \lambda_{a_n}(a_j)^{k_n} = \sigma^n(f_{n-j})^{k_n} \neq 1$. Thus $\lambda_a \neq 1$, as required.

Now suppose $\alpha = \sum_a \alpha_a\bar{a}$ is central in T, with each $\alpha_a \in F$. Then for all $x \in A$, we have $\sum_a \alpha_a\bar{a} = \alpha = \bar{x}^{-1}\alpha\bar{x} = \sum_a \alpha_a\lambda_a(x)\bar{a}$. In particular, if $\alpha_a \neq 0$, then $\lambda_a = 1$ and $a = 1$. In other words, $\alpha = \alpha_1 \in F$, and hence $\mathbb{Z}(T) = F$. Next, suppose I is a nonzero ideal of T and choose $0 \neq \beta \in I$ having minimal support size, that is with the minimal number of $\bar{A}$ terms occurring. By multiplying β by some element of $\bar{A}$ if necessary, we can assume that $1 \in \operatorname{supp}\beta$. Then $\beta = \sum_a \beta_a\bar{a}$ with $\beta_a \in F$ and $\beta_1 \neq 0$. Note that, for each $x \in A$, we have $\sum_a \beta_a\lambda_a(x)\bar{a} = \bar{x}^{-1}\beta\bar{x} \in I$ and hence $\gamma(x) = \sum_a \beta_a(\lambda_x(x)-1)\bar{a} = \bar{x}^{-1}\beta\bar{x} - \beta \in I$. But 1 is no longer in the support of $\gamma(x)$, so $\gamma(x)$ has smaller support than β and hence $\gamma(x) = 0$ for all x. In particular, β is central in T, so $0 \neq \beta \in F$, $I = T$, and T is simple. Finally, since $T = F^t[A]$ with A a torsion free abelian group, it is clear that T is locally noetherian and hence an Ore domain. ∎

LEMMA 2.3: *Construction of the skew group ring $S = TC = F{*}G$. Furthermore, if u and $1+u$ are units of S, then $u \in F$.*

Proof: Let $C = \langle c\rangle$ be an infinite cyclic group and define the map τ: $F^t[A] \to F^t[A]$ to extend σ on F and to satisfy $\tau(\bar{a}_i) = \bar{a}_{i+1}$. Since $(i+1) - (j+1) = i - j$, it follows that τ preserves the relations $[\bar{a}_i, \bar{a}_j] = \sigma^j(f_{i-j})$. Thus τ is an automorphism of $T = F^t[A]$, and we can form the skew group ring $S = TC = F^t[A]C$ with $\bar{c}$ acting like τ.

Since $\bar{A}\bar{C}$ is an F-basis for S, it is easy to see that $S = F{*}G$ is a crossed product over F of the group $G = C \wr C$. Indeed, G has a base group $B \cong A$ which is the direct product of countably many copies of C, and $G = B \rtimes \langle z\rangle$ with z acting as the shift operator. We write $\bar{G} = \bar{A}\bar{C}$.

Now it is easy to see that if G_1 and G_2 are ordered groups, then so is $G_1 \wr G_2$.

Thus $G = C \wr C$ is ordered, and it follows that every unit u of $F{*}G$ is trivial, that is of the form $u = f\bar{g}$ with $f \in F^\bullet$ and $\bar{g} \in \bar{G}$. In particular, if $1 + u$ is also a unit, then $g = 1$ and $u \in F$. ∎

LEMMA 2.4: *S is a simple right and left Ore domain with center F^σ, the fixed field of F under the action of σ.*

Proof: Since T is a right and left Ore domain and $S = TC$ with C an infinite cyclic group, it is clear that S is also a right and left Ore domain. Now let α be central in S and write $\alpha = \sum_i \bar{c}^i \alpha_i$ with $\alpha_i \in T$. Since $\bar{c}^{-i}\bar{a}_0\bar{c}^i = \bar{a}_i$, we have $\sum_i \bar{c}^i \alpha_i \bar{a}_0 = \alpha\bar{a}_0 = \bar{a}_0\alpha = \sum_i \bar{c}^i \bar{a}_i \alpha_i$ and hence $\bar{a}_i\alpha_i = \alpha_i\bar{a}_0$. In particular, if $W_i = \operatorname{supp}\alpha_i$, then $a_iW_i = W_ia_0$ and hence the finite set $W_i \subseteq A$ is closed under multiplication by $a_ia_0^{-1}$. Now, if $\alpha_i \neq 0$, then $W_i \neq \emptyset$ and therefore $a_ia_0^{-1}W_i = W_i$ implies that W_i is a union of cosets of the cyclic group $\langle a_ia_0^{-1}\rangle$. Hence $a_ia_0^{-1}$ must have finite order. But this can occur only when $i = 0$, so $\alpha = \alpha_0 \in T$ and, since α is now central in T, it follows from Lemma 2.2 that $\alpha \in F$. Furthermore, $\bar{c}$ acts on F like σ does, so $\alpha = \bar{c}^{-1}\alpha\bar{c} = \alpha^\sigma$ and $\alpha \in F^\sigma$. Since the reverse inclusion is obvious, we conclude that $\mathbb{Z}(S) = F^\sigma$.

Now let I be a nonzero ideal of $S = TC$. Since I is closed under multiplication by $\bar{c}$ and $\bar{c}^{-1}$, we can clearly choose $0 \neq \beta = \sum_{i=0}^n \beta_i\bar{c}^i \in I$, with $\beta_i \in T$, $\beta_0 \neq 0$, and with n minimal. Set $J = \{\gamma_0 \in T \mid \gamma = \sum_{i=0}^n \gamma_i\bar{c}^i \in I \text{ with } \gamma_i \in T\}$. Then J is easily seen to be an ideal of T, and $J \neq 0$ since $\beta_0 \in J$. Thus, Lemma 2.2 implies that $J = T$, and we can now assume that $\beta_0 = 1$. With this, it is easy to see, for any element $\delta = f\bar{g} \in S$ with $f \in F$ and $\bar{g} \in \bar{G}$, that $(\delta\beta - \beta\delta)\bar{c}^{-1} \in I$ is a polynomial in $\bar{c}$ of degree at most $n-1$. The minimality of n now yields $\delta\beta = \beta\delta$ and, since this holds for all such elements $\delta = f\bar{g}$, we have $\beta \in \mathbb{Z}(S) \subseteq F$. Thus $\beta = 1$, $I = S$, and S is a simple ring. ∎

LEMMA 2.5: *$R = E{*}G \subseteq S$ is an Ore domain with center E^σ. It is generated as a K-algebra by $\bar{a}_0, \bar{a}_0^{-1}, \bar{c}$ and $\bar{c}^{-1}$. Furthermore, if E is σ-simple, that is if E has no proper σ-stable ideal, then R is a simple ring.*

Proof: Note that E contains all elements of the form $\sigma^j(f_{i-j}) = [\bar{a}_i, \bar{a}_j]$, for $i > j$, and their inverses. Thus $E^t[A]$ is a subring of $F^t[A]$. Since E is σ-stable, $E^t[A]$ is τ-stable, and hence $R = E^t[A]C$ is a subring of $S = F^t[A]C$. Indeed, since $R = E\bar{A}\bar{C} = E\bar{G}$, we see that $R = E{*}G \subseteq F{*}G = S$. Of course, E is a right and left Ore domain, so the same is true of $E^t[A]$ and of $R = E^t[A]C$ in turn.

Let R' be the K-subalgebra of R generated by $\bar{a}_0, \bar{a}_0^{-1}, \bar{c}$ and $\bar{c}^{-1}$. Since $\bar{c}^{-1}\bar{a}_i\bar{c} = \bar{a}_{i+1}$ and $\bar{c}\bar{a}_i\bar{c}^{-1} = \bar{a}_{i-1}$, we see that R' contains all $\bar{a}_i$, and similarly it contains all $\bar{a}_i^{-1}$. Next, for $i > 0$, we see that $[\bar{a}_i, \bar{a}_0] = f_i$ and $[\bar{a}_0, \bar{a}_i] = [\bar{a}_i, \bar{a}_0]^{-1} = f_i^{-1}$ are contained in R'. Thus, since $\bar{c}$ acts on E like σ does, we conclude that R' contains all $\sigma^k(f_i)$ and $\sigma^k(f_i)^{-1}$. Hence $R' \supseteq E, \bar{A}$ and $\bar{C}$, so $R' = R$, as required.

Finally, suppose E is σ-simple and let I be a nonzero ideal of R. Since $S = FR = RF$, it follows that FIF is a nonzero ideal of S. Hence, by Lemma 2.4, we have $FIF = S$, and in particular $1 \in FIF$. But F is the field of fractions of $E \subseteq R$, so by taking common denominators, we see that $e_1^{-1}\alpha e_2^{-1} = 1$ for some $\alpha \in I$ and $e_1, e_2 \in E^\bullet$. In other words, $\alpha = e_1 e_2 \in E^\bullet$, so we conclude that $I \cap E$ is a nonzero ideal of E. Now $I \cap E$ is closed under conjugation by $\bar{c}$, and $\bar{c}$ acts like σ on E, so $I \cap E$ is actually a σ-stable ideal of E. Thus, when E is assumed to be σ-simple, we have $I \cap E = E$, so $1 \in I \cap E \subseteq I$, $I = R$, and R is a simple ring. ∎

LEMMA 2.6: *If D is the division ring of fractions of S, then D is the division ring of fractions of R, it is generated as a K-division algebra by $\bar{a}_0$ and $\bar{c}$, and $\mathbb{Z}(D) = F^\sigma$. Furthermore, if L is a field extension of F^σ of finite degree, then $L \otimes_{F^\sigma} D$ has zero divisors if and only if $L \otimes_{F^\sigma} F$ has zero divisors.*

Proof: Let D be the division ring of fractions of S. Then $D \supseteq R$, so every nonzero element of R is invertible in D. Furthermore, since $S = FR = RF$ and since F is the field of fractions of $E \subseteq R$, we see that every element of D is a quotient of two elements of S. Hence D is also the division ring of fractions of R. In particular, Lemma 2.5 implies that D is generated as a K-division algebra by $\bar{a}_0$ and $\bar{c}$.

Now $S = F{*}G$ with $G = C \wr C$, and $1 \in G$ is the unique element of this group having only finitely many G-conjugates. Thus it follows, as in [Pa, Theorem 4.4.5], that the center of D is the quotient field of the center of S. In particular, Lemma 2.4 implies that $\mathbb{Z}(D) = F^\sigma$.

Finally, let L be a field extension of F^σ of finite degree. If $L \otimes_{F^\sigma} F$ has zero divisors, then so does $L \otimes_{F^\sigma} D$ since $F \subseteq D$. Conversely, assume that $L' = L \otimes_{F^\sigma} F$ has no zero divisors. Then L' is a commutative domain, finite dimensional over the field F, and hence L' is a field. Furthermore, since $S = F{*}G$, we see that $S' = L \otimes_{F^\sigma} S = (L \otimes_{F^\sigma} F){*}G = L'{*}G$, and hence S' is also an Ore domain with division ring of fractions D'. Now $D' \supseteq S$, so $D' \supseteq D$, and of course $D' \supseteq L$. Furthermore, L is central in D' and any linear relation between

L and D gives rise, by taking common denominators, to a linear relation between L and S. With this, we see that $D' \supseteq L \otimes_{F^\sigma} D$ and consequently $L \otimes_{F^\sigma} D$ has no zero divisors. ∎

3. Fields of transcendence degree 1

We will, of course, use the constructions of the previous section to prove our first two main results, namely Theorems 1.1 and 1.2. Since K is given, we can only vary F and the field automorphism σ in this process. As will be apparent here, we use the same family of fields F for both of these results, but we use two essentially different types of automorphisms. In the case of Proposition 1.3, we use the same field F, but uncountably many distinct field automorphisms.

To start with, let $K(t)$ be the rational function field over K in the one variable t, and let $\mathcal{P}$ be the set of all prime numbers different from the characteristic of K. Then, working in a fixed algebraic closure of $K(t)$, we let t_p be a fixed pth root of t for each prime $p \in \mathcal{P}$. Of course, $K(t_p)$ is also a rational function field in the single variable t_p, and $|K(t_p) : K(t)| = p$. It is easy to see that if $p_1, p_2, \ldots, p_k$ are finitely many distinct primes with $p_1 p_2 \cdots p_k = n$, then $K(t_{p_1}, t_{p_2}, \ldots, t_{p_k}) = K(t_n)$ for some element t_n with $(t_n)^n = t$. Consequently,

$$|K(t_{p_1}, t_{p_2}, \ldots, t_{p_k}) : K(t)| = |K(t_n) : K| = n = p_1 p_2 \cdots p_k.$$

Now, if $\mathcal{I}$ is a nonempty subset of $\mathcal{P}$, then we let $F_{\mathcal{I}}$ be the field extension of $K(t)$ generated by all t_p with $p \in \mathcal{I}$. It is easy to see that $F_{\mathcal{I}}$ determines $\mathcal{I}$ provided we know how $K(t)$ is embedded in the field. Specifically, we have

LEMMA 3.1: *Let $\mathcal{I}$ be a nonempty subset of $\mathcal{P}$.*

(i) *$\mathcal{I}$ is precisely the set of all primes $p \in \mathcal{P}$ such that $F_{\mathcal{I}} \supseteq L \supseteq K(t)$ for some field L with $|L : K(t)| = p$.*

(ii) *If $p \in \mathcal{P} \setminus \mathcal{I}$ and if L is a field extension of $K(t)$ with $|L : K(t)| = p$, then $L \otimes_{K(t)} F_{\mathcal{I}}$ has no zero divisors.*

(iii) *If $p \in \mathcal{I}$, then there exists a field extension L of $K(t)$ with $|L : K(t)| = p$ and such that $L \otimes_{K(t)} F_{\mathcal{I}}$ has zero divisors.*

Proof: (i) This is clear since any such field L must be contained in some $K(t_n)$ with $n = p_1 p_2 \cdots p_k$ and $p_1, p_2, \ldots, p_k \in \mathcal{I}$.

(ii) It suffices to observe that, for each n as above, $L \otimes_{K(t)} K(t_n)$ is a field. Equivalently, we need to show that the polynomial $X^n - t \in L[X]$ is irreducible. To this end, let s be a root of the polynomial and consider the field $L[s]$. Then

$L[s] \supseteq K(s) \supseteq K(t)$ and $|K(s):K(t)| = n$. Thus, the relatively prime integers n and p both divide $|L[s]:K(t)|$. It therefore follows that $|L(s):K(t)| = np$, and hence $|L[s]:L| = n$, as required.

(iii) If $p \in \mathcal{I}$, take $L = K(t_p)$ so that $|L:K(t)| = p$. Then $L \otimes_{K(t)} K(t_p)$ is not a domain and hence neither is $L \otimes_{K(t)} F_{\mathcal{I}}$. ∎

Since $\mathcal{P}$ is an infinite set, there are uncountably many nonempty subsets $\mathcal{I} \subseteq \mathcal{P}$ and hence there are potentially uncountably many fields $F_{\mathcal{I}}$, viewed as K-algebras. We show below that this is indeed the case. For convenience, if $\mathcal{I}$ and $\mathcal{J}$ are subsets of $\mathcal{P}$, then we write $\mathcal{I} \sim \mathcal{J}$ if and only if $\mathcal{I}$ and $\mathcal{J}$ differ by just finitely many elements. In other words, $\mathcal{I} \sim \mathcal{J}$ if and only if there exist finite subsets $\mathcal{I}_0$ and $\mathcal{J}_0$ of $\mathcal{P}$ with $\mathcal{I} \cup \mathcal{I}_0 = \mathcal{J} \cup \mathcal{J}_0$. It is clear that $\sim$ is an equivalence relation and that each equivalence class is countable, since $\mathcal{P}$ has only countably many finite subsets. Of course, the collection of all finite subsets of $\mathcal{P}$ forms one equivalence class, and obviously, there are uncountably many other such classes. We have

LEMMA 3.2: *Let $\mathcal{I}$ and $\mathcal{J}$ be nonempty subsets of $\mathcal{P}$. Then the fields $F_{\mathcal{I}}$ and $F_{\mathcal{J}}$ are K-isomorphic if and only if $\mathcal{I} \sim \mathcal{J}$.*

Proof: Let $\mathcal{I}$ be given and suppose $q \in \mathcal{P} \setminus \mathcal{I}$. Then, for each prime $p \in \mathcal{I}$, it is easy to see that $K(t_q, t_p) = K(t_q, t'_p)$, where $(t'_p)^p = t_q$. In particular, if $\mathcal{I}' = \mathcal{I} \cup \{q\}$, then $F_{\mathcal{I}'} = K(t_q, t_p \mid p \in \mathcal{I}) = K(t_q, t'_p \mid p \in \mathcal{I})$. But $K(t) \cong K(t_q)$ via the K-isomorphism given by $t \mapsto t_q$, and then this map extends to a K-isomorphism $F_{\mathcal{I}} \cong F_{\mathcal{I}'}$ given by $t_p \mapsto t'_p$ for all $p \in \mathcal{I}$. It now follows by induction on the size of the change that $\mathcal{I} \sim \mathcal{J}$ implies $F_{\mathcal{I}} \cong F_{\mathcal{J}}$.

Conversely, suppose $F_{\mathcal{I}}$ is K-isomorphic to $F_{\mathcal{J}}$. Then we can write $F_{\mathcal{I}} = F_{\mathcal{J}}$ provided we rename the generators of $F_{\mathcal{J}}$ as s and s_q for all $q \in \mathcal{J}$. Now there exist primes $p_1, p_2, \ldots, p_k \in \mathcal{I}$, with $n = p_1 p_2 \cdots p_k$, such that

$$s \in K(t_{p_1}, t_{p_2}, \ldots, t_{p_k}) = K(t_n),$$

and thus $|K(t_n):K(s)| = m < \infty$. Now if $q \in \mathcal{J}$, then $F_{\mathcal{I}} = F_{\mathcal{J}} \supseteq K(s_q) \supseteq K(s)$ with $|K(s_q):K(s)| = q$. Thus either $q|m$ or $K(t_n)$ has an extension of degree q in $F_{\mathcal{I}}$ and hence $q \in \mathcal{I}$. In other words, $\mathcal{J} \subseteq \mathcal{I} \cup \mathcal{I}_0$ for some finite subset $\mathcal{I}_0$ of $\mathcal{P}$. Similarly, $\mathcal{I} \subseteq \mathcal{J} \cup \mathcal{J}_0$, and then clearly $\mathcal{I} \sim \mathcal{J}$. ∎

Now suppose that K contains an element $\zeta \neq 0$ of infinite multiplicative order such that all mth roots of ζ are also in K. For example, K could be the algebraic closure of a nonabsolute field. For each $p \in \mathcal{P}$, let $\zeta_p \in K$ be a fixed pth root of

ζ. If $\mathcal{I}$ is any nonempty subset of $\mathcal{P}$, we can then define a field automorphism σ' of $F_{\mathcal{I}}$ over K by $\sigma'\colon t \mapsto \zeta t$ and $\sigma'\colon t_p \mapsto \zeta_p t_p$ for all $p \in \mathcal{I}$. As usual, if $p_1, p_2, \ldots, p_k$ are finitely many distinct primes in $\mathcal{I}$ with $p_1 p_2 \cdots p_k = n$, then $K(t_{p_1}, t_{p_2}, \ldots, t_{p_k}) = K(t_n)$ and $\sigma'\colon t_n \mapsto \zeta_n t_n$, where $\zeta_n \in K$ is some nth root of ζ. With this, it is clear that σ' is indeed a field automorphism.

LEMMA 3.3: *For each nonempty subset $\mathcal{I} \subseteq \mathcal{P}$, we have $(F_{\mathcal{I}})^{\sigma'} = K$. Furthermore, if E is a σ'-stable K-subalgebra of $F_{\mathcal{I}}$ containing all t_p and t_p^{-1} with $p \in \mathcal{I}$, then E is a σ'-simple ring.*

Proof: If $s \in (F_{\mathcal{I}})^{\sigma'}$, then $s \in K(t_n)$ for some n as above. But σ' is an automorphism of infinite order on $K(t_n)$, so $|K(t_n) : K(s)| = \infty$ and $s \in K$, as required.

Now let I be a nonzero σ'-stable ideal of E. Then there exists an integer $n = p_1 p_2 \cdots p_k$ with $I \cap K(t_n) \neq 0$. Furthermore, since $t_n, t_n^{-1} \in E$ and since $K(t_n)$ is the field of fractions of the K-subalgebra $N = K[t_n, t_n^{-1}]$, we see that $J = I \cap N$ is a nonzero σ'-stable ideal of N. Note that $N = K[\langle t_n \rangle]$ is the group algebra of the infinite cyclic group $\langle t_n \rangle$ and that $\sigma'\colon t_n \mapsto \zeta_n t_n$. Now, using group algebra notation, choose $0 \neq \alpha \in J$ to be an element of minimal support size. Multiplying by some element of $\langle t_n \rangle$ if necessary, we can assume that $\alpha = \sum_{i=0}^{m} k_i (t_n)^i$ with $k_0 \neq 0$. Then $\sigma'(\alpha) - \alpha \in J$ and $\sigma'(\alpha) - \alpha = \sum_{i=1}^{m} k_i (\zeta_n^i - 1)(t_n)^i$ has smaller support. Thus $\sigma'(\alpha) - \alpha = 0$ and, since $\zeta_n \in K$ has infinite multiplicative order, we conclude that $k_i = 0$ for all $i \neq 0$. Hence $\alpha = k_0 \in K^\bullet$, so $1 \in J \subseteq I$, $I = E$, and E is a σ'-simple ring. ∎

We can now verify our first main result.

Proof of Theorem 1.1: Since K is assumed to have a nonzero element ζ of infinite multiplicative order with all its mth roots also contained in K, we can use the above notation. For each infinite subset $\mathcal{I}$ of $\mathcal{P}$, we construct a K-algebra $R_{\mathcal{I}}$ using the results of the preceding section. Specifically, we take $F = F_{\mathcal{I}}$, $\sigma = \sigma'$ and $\mathcal{F} = \{t_p,\ 1 + t_p \mid p \in \mathcal{I}\}$, with the primes listed in their natural order, and then we let $R_{\mathcal{I}}$ be the K-algebra given by Lemma 2.5. In particular, we know that $R_{\mathcal{I}}$ is an Ore domain, generated as a K-algebra by four elements, and that $\mathbb{Z}(R_{\mathcal{I}}) = E^{\sigma'}$. Furthermore, by Lemma 3.3 and the fact that E is generated by all $\langle \sigma' \rangle$-conjugates of $\mathcal{F} \cup \mathcal{F}^{-1}$, we see that $\mathbb{Z}(R_{\mathcal{I}}) = E^{\sigma'} = K$ and that E is σ'-simple. Thus, by Lemma 2.5 again, we conclude that $R_{\mathcal{I}}$ is a simple ring.

Finally, we claim that $R_{\mathcal{I}}$ determines $F_{\mathcal{I}}$. To this end, let $L_{\mathcal{I}}$ be the K-subalgebra of $R_{\mathcal{I}}$ generated by all units u of $R_{\mathcal{I}}$ with $u + 1$ also a unit. By

Lemma 2.3, we know that $L_{\mathcal{I}} \subseteq F_{\mathcal{I}}$. Furthermore, since $\mathcal{F}$ contains both t_p and $1+t_p$, we see that each t_p, with $p \in \mathcal{I}$, is contained in $L_{\mathcal{I}}$. Thus $F_{\mathcal{I}}$ is the field of fractions of $L_{\mathcal{I}}$, and hence this field is indeed determined by $R_{\mathcal{I}}$. In particular, if $R_{\mathcal{I}}$ and $R_{\mathcal{J}}$ are K-isomorphic, then $F_{\mathcal{I}}$ and $F_{\mathcal{J}}$ are K-isomorphic, so $\mathcal{I} \sim \mathcal{J}$ by Lemma 3.2. But there are uncountably many equivalence classes under $\sim$ consisting of infinite subsets of $\mathcal{P}$, so in this way we obtain uncountably many nonisomorphic K-algebras $R_{\mathcal{I}}$, as required. ∎

Now suppose, instead, that K contains all mth roots of unity and, for each prime $p \in \mathcal{P}$, let $\varepsilon_p \in K$ be a primitive pth root of 1. Recall that, by definition, $\mathcal{P}$ avoids the characteristic of K. If $\mathcal{I}$ is a nonempty subset of $\mathcal{P}$, we define the field automorphism σ'' of $F_{\mathcal{I}}$ over $K(t)$ by $\sigma''\colon t_p \mapsto \varepsilon_p t_p$ for all $p \in \mathcal{I}$. As above, it is clear that σ'' is indeed a $K(t)$-field automorphism. Furthermore, if $p_1, p_2, \ldots, p_k$ are distinct primes in $\mathcal{I}$ with $p_1 p_2 \cdots p_k = n$, then $K(t_{p_1}, t_{p_2}, \ldots, t_{p_k}) = K(t_n)$ and $\sigma''\colon t_n \mapsto \varepsilon_n t_n$, where ε_n is a suitable primitive nth root of unity in K. In particular, σ'' has order n in its action on $K(t_n)$ and, since $|K(t_n) : K(t)| = n$, it follows immediately that $(F_{\mathcal{I}})^{\sigma''} = K(t)$. With this, we have

Proof of Theorem 1.2: We use the above notation. For each infinite subset $\mathcal{I}$ of $\mathcal{P}$, we construct a K-division algebra $D_{\mathcal{I}}$ using the results of the preceding section. Specifically, we take $F = F_{\mathcal{I}}$, $\sigma = \sigma''$ and $\mathcal{F} = \{t_p \mid p \in \mathcal{I}\}$, with the primes in their natural order, and we let $D_{\mathcal{I}}$ be the division ring given by Lemma 2.6. Then we know that $D_{\mathcal{I}}$ is generated as a K-division algebra by two elements and furthermore that $\mathbb{Z}(D_{\mathcal{I}}) = F^{\sigma''} = K(t)$.

It remains to show that $D_{\mathcal{I}}$ determines $\mathcal{I}$. To this end, let L be a field containing $\mathbb{Z}(D_{\mathcal{I}}) = K(t)$ with $|L : K(t)| = p \in \mathcal{P}$. Then, by Lemma 2.6, $L \otimes_{K(t)} D_{\mathcal{I}}$ contains a zero divisor if and only if $L \otimes_{K(t)} F_{\mathcal{I}}$ has a zero divisor. Furthermore, by Lemma 3.1(ii)(iii), the latter cannot occur if $p \notin \mathcal{I}$ and it can and does occur if $p \in \mathcal{I}$. Thus $\mathcal{I}$ is indeed determined by $D_{\mathcal{I}}$, and consequently we obtain uncountably many nonisomorphic division algebras in this way. ∎

We close this section with the

Proof of Proposition 1.3: Let K be an arbitrary field and again use the above notation. For each infinite subset $\mathcal{I}$ of $\mathcal{P}$, let $R_{\mathcal{I}}$ be the K-algebra given by Lemma 2.5 with $F = F_{\mathcal{I}}$, $\sigma = 1$, and $\mathcal{F} = \{t_p \mid p \in \mathcal{I}\}$, where the primes are listed in their natural order. Since $\sigma = 1$, we know that $R_{\mathcal{I}} = (E_{\mathcal{I}})^t[G]$ is a twisted group ring with $\mathbb{Z}(R_{\mathcal{I}}) = E_{\mathcal{I}} = K[t_p, t_p^{-1} \mid p \in \mathcal{I}]$, and with four generators as a K-algebra. Furthermore, $R_{\mathcal{I}}$ is a right and left Ore domain with field of fractions $D_{\mathcal{I}}$ given by Lemma 2.6. Thus $D_{\mathcal{I}}$ is generated as a K-division algebra by two elements, and $\mathbb{Z}(D_{\mathcal{I}}) = F_{\mathcal{I}}$, the field of fractions of $E_{\mathcal{I}}$. Finally, if $R_{\mathcal{I}} \cong R_{\mathcal{J}}$ is a K-isomorphism, then $F_{\mathcal{I}} = \mathbb{Z}(D_{\mathcal{I}}) \cong \mathbb{Z}(D_{\mathcal{J}}) = F_{\mathcal{J}}$ is also a K-isomorphism. In particular, Lemma 3.2 implies that $\mathcal{I} \sim \mathcal{J}$, and hence we obtain uncountably many different K-algebras $R_{\mathcal{I}}$ and K-division algebras $D_{\mathcal{I}}$.

If K is a countable field, then so is each $F_{\mathcal{I}}$, and we change the above construction by taking $\mathcal{F}$ to be the set of all nonzero elements of $F_{\mathcal{I}}$ having infinite multiplicative order. Then $E_{\mathcal{I}} = K[\mathcal{F} \cup \mathcal{F}^{-1}] = F_{\mathcal{I}}$, since if $0 \neq f \in F_{\mathcal{I}}$ has finite order, then $f \in K[tf, t^{-1}]$ and both tf and t^{-1} have infinite order. In this case, $E_{\mathcal{I}}$ is σ-simple, since it is a field, and hence $R_{\mathcal{I}}$ is a simple ring by Lemma 2.5. ∎

4. HNN constructions

We start with a brief summary of several results and concepts from the theory of skew fields which will be used in the proofs of Theorem 1.4 and Proposition 1.5. We refer the reader to [C1, C2] for a more detailed exposition.

Let R be an arbitrary ring and recall that an $n \times n$ R-matrix α is said to be full if every factorization $\alpha = \beta\gamma$, with β an $n \times m$ matrix and with γ of size $m \times n$, implies that $m \geq n$. It is not true, in general, that every invertible matrix is full, but we do have

LEMMA 4.1: *Let R be a ring.*

(i) *If R is locally noetherian, then every invertible R-matrix is full.*

(ii) *If D is a K-division algebra and if L is a commutative K-algebra, then $R = L \otimes_K D$ is locally noetherian.*

Proof: (i) Let α be an invertible $n \times n$ matrix which can be factored as $\alpha = \beta\gamma$ with β of size $n \times m$ and γ of size $m \times n$. Then $1 = \beta(\gamma\alpha^{-1})$ yields a factorization of the identity matrix with the matrix factors having the same parameters n and m. In other words, we can assume that α is the identity matrix. Furthermore, since R is locally noetherian and since α, β, and γ have only finitely many entries, we can now also assume that R is noetherian.

Next, let $\bar{R}$ be a prime homomorphic image of R. Then the map $R \to \bar{R}$ yields a factorization $\bar{\alpha} = \bar{\beta}\bar{\gamma}$ of $\bar{R}$-matrices with the same sizes. Thus, we can now assume that R is a prime noetherian ring. But then, by Goldie's theorem, R embeds in $\mathrm{M}_t(D)$, the $t \times t$ matrix ring over a division ring D, and we can view α, β, and γ as matrices over this larger ring. Indeed, since an $n \times m$ matrix over $\mathrm{M}_t(D)$ can be viewed as an $nt \times mt$ matrix over D, we obtain $\alpha^* = \beta^*\gamma^*$, where α^* is the $nt \times nt$ identity matrix, β^* is a D-matrix of size $nt \times mt$, and γ^* has size $mt \times nt$.

The latter matrices translate to D-linear transformations $D^{nt} \to D^{mt} \to D^{nt}$ with composite map the identity. In particular, the map $D^{mt} \to D^{nt}$ is onto, so dimension considerations yield $mt \geq nt$ and hence $m \geq n$, as required.

(ii) If $R = L \otimes_K D$, then any finite subset of R is contained in a subring of the form $K[z_1, z_2, \ldots, z_k] \otimes_K D$ with $z_1, z_2, \ldots, z_k$ in the commutative algebra L. Since this subring is a homomorphic image of the ordinary polynomial ring $D[x_1, x_2, \ldots, x_k]$, and since D is a division ring, the result follows. ∎

A ring R is said to be a fir (semifir) if every left ideal (finitely generated left ideal) is free of unique rank. It is known that every semifir has a universal field of fractions $\mathcal{U}(R)$ which is a skew field containing R and generated by it. Furthermore, every isomorphism between two semifirs extends uniquely to an isomorphism of their universal fields of fractions. However, an embedding of semifirs need not give rise to an embedding of their universal fields of fractions.

We will need the following observations. Part (i) is standard and part (ii) comes from the proof of [C2, Proposition 6.4.4].

Lemma 4.2: *Let $R \subseteq R'$ be semifirs, let Σ be the set of full matrices of R, and let Σ' be the set of full matrices of R'.*

(i) *Suppose $S \supseteq \mathcal{U}(R)$ is a ring with the property that all invertible S-matrices are full. If the embedding $R \to \mathcal{U}(R)$ extends to a homomorphism $R' \to S$, then $\Sigma \subseteq \Sigma'$ and $\mathcal{U}(R)$ embeds naturally in $\mathcal{U}(R')$.*

(ii) *If R is a K-algebra and $R' = L \otimes_K R$, where L is a field extension of K, then $\Sigma \subseteq \Sigma'$ and $\mathcal{U}(R) \subseteq \mathcal{U}(R')$. Furthermore, if $Z = \mathbb{Z}(\mathcal{U}(R))$ and if $L \otimes_K Z$ is a field, then $L \otimes_K \mathcal{U}(R) \subseteq \mathcal{U}(R')$ and hence $L \otimes_K \mathcal{U}(R)$ is a domain.*

Proof: (i) If $\alpha \in \Sigma$, then α becomes invertible over the ring $\mathcal{U}(R)$ and hence over the larger ring S. In particular, α is full when viewed as a matrix over S. Thus, since $R' \to S$ extends the embedding $R \to \mathcal{U}(R)$, it follows that α, when viewed as a matrix over R', must also be full. In other words, $\Sigma \subseteq \Sigma'$ and hence all matrices in Σ are invertible in $\mathcal{U}(R')$. This implies that there exists a homomorphism $\mathcal{U}(R) \to \mathcal{U}(R')$ and, since $\mathcal{U}(R)$ is a division ring, we obtain the required embedding.

(ii) The embedding $R \to \mathcal{U}(R)$ clearly extends to a map $R' = L \otimes_K R \to L \otimes_K \mathcal{U}(R)$, and $L \otimes_K \mathcal{U}(R)$ is locally noetherian by Lemma 4.1(ii). Thus, by Lemma 4.1(i), all invertible matrices of $L \otimes_K \mathcal{U}(R)$ are full, and consequently part (i) above implies that $\Sigma \subseteq \Sigma'$ and $\mathcal{U}(R) \subseteq \mathcal{U}(R')$. Furthermore, since $\mathcal{U}(R)$ is the localization R_Σ, it is clear that $L \otimes_K \mathcal{U}(R)$ is obtained from $R' = L \otimes_K R$ by inverting the matrices in Σ, or equivalently $L \otimes_K \mathcal{U}(R) = R'_\Sigma$. Thus, since $\Sigma \subseteq \Sigma'$, we have a homomorphism $R'_\Sigma \to R'_{\Sigma'} = \mathcal{U}(R')$. Now observe that $\mathcal{U}(R)$ is a division algebra, so every nonzero ideal of $L \otimes_K \mathcal{U}(R)$ must meet $L \otimes_K Z$ nontrivially. In particular, if $L \otimes_K Z$ is a field, then $L \otimes_K \mathcal{U}(R)$ must be a simple ring. In this case, the homomorphism $L \otimes_K \mathcal{U}(R) \to \mathcal{U}(R')$ is necessarily one-to-one. ∎

Now let $X = \{x_i \mid i \in \mathcal{I}\}$ be a set, and let $K<X>$ denote the free algebra over the field K in the system of generators $x_i \in X$. Then $K<X>$ is a fir, and we let $K\langle\!\langle X\rangle\!\rangle$ denote its universal field of fractions. This division ring $K\langle\!\langle X\rangle\!\rangle$ is known as the free field over K having X as free system of generators, and $\mathbb{Z}(K\langle\!\langle X\rangle\!\rangle) = K$ when $|X| \geq 2$. Now suppose L is a field containing K. Then, by [C2, Theorem 6.4.6] or by Lemma 4.2(ii), we have a natural embedding

$$L\langle\!\langle X\rangle\!\rangle \supseteq L \otimes_K K\langle\!\langle X\rangle\!\rangle \supseteq K\langle\!\langle X\rangle\!\rangle.$$

Finally, it is easy to see that if X is infinite, then $K\langle\!\langle X\rangle\!\rangle$ cannot be finitely generated as a K-division algebra. Otherwise, $K\langle\!\langle X\rangle\!\rangle$ would be generated by a finite subset $X' \subseteq X$, and hence any K-automorphism of the free field fixing X' would necessarily fix $K\langle\!\langle X\rangle\!\rangle$. But any nontrivial permutation of the elements of $X \setminus X'$ gives rise to a nontrivial automorphism of this division algebra fixing X', and hence we have the required contradiction. In particular, if $K\langle\!\langle X\rangle\!\rangle$ is isomorphic to $K\langle\!\langle Y\rangle\!\rangle$, then Y must also be infinite.

For convenience, if x and y are elements of a ring R, we let $[x, y]_n$ denote the n-fold Lie commutator given by $[x, y]_n = [x, y, \ldots, y] = x\cdot(\mathrm{ad}_y)^n$. In particular, we have $[x, y]_0 = x$.

LEMMA 4.3: *Let $K<x, y>$ be the free K-algebra on the two generators x and y and, for each integer $n \geq 0$, let $a_n = [x, y]_n + k_n \in K<x, y>$ for some $k_n \in K$. If $\mathcal{A} = \{a_0, a_1, a_2, \ldots\}$, then the skew subfield of $K\langle\!\langle x, y\rangle\!\rangle$ generated by K and $\mathcal{A}$ is the free field $K\langle\!\langle \mathcal{A}\rangle\!\rangle$ over K having $\mathcal{A}$ as a free system of generators. Furthermore, $K\langle\!\langle \mathcal{A}\rangle\!\rangle$ is properly smaller than $K\langle\!\langle x, y\rangle\!\rangle$.*

Proof: For the most part, this follows from [L, Corollary 3], but we sketch a more elementary argument. Let $\mathcal{L}'$ be the free K-Lie algebra generated by x and y, and let $\mathcal{L}$ be the free Lie subalgebra generated by the set

$$\mathcal{B} = \{[x, y]_0, [x, y]_1, [x, y]_2, \ldots\}.$$

Then $R' = K\langle x,y\rangle$ is the enveloping algebra of $\mathcal{L}'$, and $R = K\langle\mathcal{B}\rangle$ is the enveloping algebra of $\mathcal{L}$. Furthermore, $\mathcal{L} \triangleleft \mathcal{L}'$ and $\mathcal{L}' = \mathcal{L} \dot{+} Ky$, so $R' = R[y;\delta]$ can be viewed as a differential polynomial ring in the one variable y. Since the derivation δ can be extended to a derivation of $\mathcal{U}(R)$, by [C1, Exercise 1, page 419], it follows that the embedding $R \to \mathcal{U}(R)$ can be extended to a homomorphism $R' = R[y;\delta] \to \mathcal{U}(R)[y;\delta]$. But $\mathcal{U}(R)[y;\delta]$ is certainly a principal ideal domain, so Lemmas 4.1(i)(ii) and 4.2(i) now imply that $\mathcal{U}(R) = K\langle\!\langle\mathcal{B}\rangle\!\rangle$ embeds naturally in $\mathcal{U}(R') = K\langle\!\langle x,y\rangle\!\rangle$. We can therefore conclude from [C2, Lemma 5.5.7] that $K\langle\!\langle\mathcal{A}\rangle\!\rangle \subseteq K\langle\!\langle x,y\rangle\!\rangle$, and since $K\langle\!\langle\mathcal{A}\rangle\!\rangle \not\cong K\langle\!\langle x,y\rangle\!\rangle$, as we observed above, the embedding must be proper. ∎

HNN-extensions for rings were systematically studied in the paper [D]. Let R be a K-algebra which is a fir (or semifir), let A and B be division subalgebras, and suppose that φ: $A \to B$ is a K-isomorphism. Then the HNN-extension of R determined by φ is the ring S generated by R and an invertible element u satisfying $u^{-1}au = \varphi(a)$ for all $a \in A$. It is known that R embeds in S and, by one of the results of [D], that S is a fir (or semifir). If $\mathcal{U}(S)$ is the universal field of fractions of S, then an alternate description of this division ring is given in [C2, Theorem 5.5.1], and requires that we endow R with two distinct bimodule structures. First, we have ${}_RR_A$, where R and A act on R by way of the usual left and right multiplication. Next, we have ${}_AR_R$, where R acts by right multiplication and where A acts via $a{\cdot}r = \varphi(a)r$ for all $a \in A$ and $r \in R$. Now let M be the (R,R)-bimodule defined by $M = R\otimes_A R = ({}_RR_A)\otimes_A({}_AR_R)$, and let

$$T(M) = R \dot{+} M \dot{+} M\otimes M \dot{+} M\otimes M\otimes M \dot{+} \cdots$$

be its tensor ring. Then this graded ring is a fir (or semifir), generated by its 0-component R and the element $x = 1\otimes 1 \in M$ of degree 1. Furthermore, $\mathcal{U}(T(M))$ is naturally isomorphic to $\mathcal{U}(S)$ with $x \in T(M)$ corresponding to $u \in S$. We will need two additional facts about these extensions. For simplicity, we assume that $R = D$ is a K-division algebra.

Lemma 4.4: *In the above situation, assume that $D \neq A$ or $D \neq B$. Then the center Z of $\mathcal{U}(S)$ is given by $Z = \{a \in A\cap\mathbb{Z}(D) \mid \varphi(a) = a\} \subseteq A \cap B$.*

Proof: By symmetry, we can assume that $D \neq A$, so that $\{d_1, d_2, \ldots\}$, an A-basis for D_A, has size at least 2. Since $\{d_1\otimes 1, d_2\otimes 1, \ldots\}$ is a D-basis for M_D, it is easy to see that the nonzero right ideals $(d_1\otimes 1)T(M)$ and $(d_2\otimes 1)T(M)$ are disjoint. In particular, $T(M)$ is not an Ore domain and hence it is not a principal ideal domain.

[C1, Theorem 7.8.4] now implies that the center Z of $\mathcal{U}(S) = \mathcal{U}(T(M))$ coincides with the center of $T(M)$. Furthermore, Z is certainly a field, so $Z = \mathbb{Z}(T(M))$ consists of invertible elements in $T(M)$. But $T(M)$ is a graded ring, so all invertible elements must be contained in its 0-component, namely D. Indeed, since $T(M)$ is generated by D and the element $1 \otimes 1 \in M$, it follows that Z is the set of elements of $\mathbb{Z}(D)$ that commute with $1 \otimes 1$. Now if $r \in Z$, then

$$r \otimes 1 = r(1 \otimes 1) = (1 \otimes 1)r \in (r \otimes 1)T(M) \cap (1 \otimes 1)T(M),$$

so the above basis information implies that r must be contained in A and consequently, since $a(1 \otimes 1) = (1 \otimes 1)\varphi(a)$ for all $a \in A$, the result follows. ∎

Next, we consider the behavior of HNN extensions under a field extension.

LEMMA 4.5: *Let K be a field and let L be a field extension of K of finite degree. Suppose D is a division algebra, let A and B be proper K-subdivision algebras, and let φ: $A \to B$ be a K-isomorphism. Write $A' = L \otimes_K A$, $B' = L \otimes_K B$, $D' = L \otimes_K D$ and let $\varphi' = 1 \otimes \varphi$: $A' \to B'$ be the natural extension of φ to an L-isomorphism. If D' is a domain, then D', A' and B' are all division algebras. Furthermore, if S is the HNN extension of D determined by the map φ, and if S' is the HNN extension of D' determined by the map φ', then $L \otimes_K \mathcal{U}(S) \subseteq \mathcal{U}(S')$, and hence $L \otimes_K \mathcal{U}(S)$ is a division algebra.*

Proof: Since $D' = L \otimes D$ is a domain and $|L : K| < \infty$, it follows that D' is a division algebra. Similarly, $A', B' \subseteq D'$ are also division algebras. Now let $M = D \otimes_A D$ be the (D, D)-bimodule constructed from φ, and let $M' = D' \otimes_{A'} D'$ be the (D', D')-bimodule constructed from φ'. Since $A' \supseteq L$ and φ' is the identity on L, it follows that all L-factors in $D' \otimes_{A'} D'$ can be moved to the front. With this, it is clear that $M' = L \otimes_K M$. Furthermore, since D' contains L, it follows that all L-factors of $M' \otimes_{D'} M' \otimes_{D'} \cdots \otimes_{D'} M'$ can also be moved to the front. Again this says that $(M')^{\otimes n} = L \otimes_K (M)^{\otimes n}$ for all $n \geq 0$ and hence $T(M') = L \otimes_K T(M)$.

We wish to apply Lemma 4.2(ii) with $R = T(M)$ and $R' = T(M') = L \otimes_K R$, and we already know that both $T(M)$ and $T(M')$ are firs. Furthermore, if Z is the center of $\mathcal{U}(R)$ then, by Lemma 4.4 and the fact that D properly contains A, we see that Z is a field contained in D. In particular, since $L \otimes_K D$ has no zero divisors, $L \otimes_K Z$ has no zero divisors and hence it is a field. Lemma 4.2(ii) now implies that $L \otimes_K \mathcal{U}(R) \subseteq \mathcal{U}(R')$, as required. ∎

We can now offer our basic HNN construction. The inclusion of the intermediate field E allows us to control the center of R.

LEMMA 4.6: *Let $F \supseteq E \supseteq K$ be fields and let $\mathcal{F} = \{0 = f_0, f_1, f_2, \ldots\}$ be a countable sequence of elements of F. Then there exists a K-division algebra $R = \mathcal{U}(S)$, where S is an HNN extension of the free field $F\langle\!\langle x, y\rangle\!\rangle$, such that*

(i) $\mathbb{Z}(R) = E$.

(i) *If $K(\mathcal{F}) = F$, then R has two generators as a K-division algebra.*

(i) *If L is a field extension of E of finite degree, then $L \otimes_E R$ has zero divisors if and only if $L \otimes_E F$ has zero divisors.*

Proof: Let $D = F\langle\!\langle x, y\rangle\!\rangle$ be the free field over F generated by x and y, and consider the two sequences $\mathcal{A} = \{a_0, a_1, a_2, \ldots\}$ and $\mathcal{B} = \{b_0, b_1, b_2, \ldots\}$ given by $a_i = [x, y]_i$ and $b_i = [y, x]_i + f_i$. Then, by Lemma 4.3, the skew subfield of D generated by F and $\mathcal{A}$ is $F\langle\!\langle \mathcal{A}\rangle\!\rangle$, the free field generated over F by $\mathcal{A}$. In particular, we have $D \supseteq F\langle\!\langle \mathcal{A}\rangle\!\rangle \supseteq F{<}\mathcal{A}{>}$. Furthermore, by our previous observations, $F{<}\mathcal{A}{>} \supseteq E{<}\mathcal{A}{>}$ and hence $D \supseteq F\langle\!\langle \mathcal{A}\rangle\!\rangle \supseteq E\langle\!\langle \mathcal{A}\rangle\!\rangle = A$. Similarly, $D \supseteq F\langle\!\langle \mathcal{B}\rangle\!\rangle \supseteq E\langle\!\langle \mathcal{B}\rangle\!\rangle = B$, and we can define the E-isomorphism $\varphi\colon A \to B$ by $\varphi(a_i) = b_i$. Let S be the HNN extension of D determined by φ, and set $R = \mathcal{U}(S)$.

Since A is properly smaller than R, by Lemma 4.3, it follows from Lemma 4.4 that $\mathbb{Z}(R) \subseteq \mathbb{Z}(A)$. Thus, by [C1, Theorem 7.8.4], $\mathbb{Z}(R) \subseteq E$ and then $\mathbb{Z}(R) = E$ since φ is an E-isomorphism. Now recall that S is generated by $D = F\langle\!\langle x, y\rangle\!\rangle$ and an invertible element u with $u^{-1}au = \varphi(a)$ for all $a \in A$. In particular, if R_0 is the K-subdivision algebra of R generated by x and u, then R_0 contains u^{-1}, $u^{-1}xu = u^{-1}a_0u = \varphi(a_0) = b_0 = y$, since $f_0 = 0$. Consequently, it contains all $[x, y]_i$, and all $[y, x]_i$. Furthermore, R_0 contains all $u^{-1}[x, y]_iu = u^{-1}a_iu = \varphi(a_i) = b_i = [y, x]_i + f_i$, so $R_0 \supseteq \mathcal{F}$. Thus, if $K(\mathcal{F}) = F$, then R_0 contains $F{<}x, y{>}$, u and u^{-1}, so this division algebra contains D, S and hence also $\mathcal{U}(S) = R$. In other words, if $K(\mathcal{F}) = F$, then R is generated as a K-division algebra by the two elements x and u. Thus (i) and (ii) are proved.

For (iii), let L be a field extension of E with $|L : E| < \infty$. If $L \otimes_E F$ contains zero divisors, then $L \otimes_E R$ has zero divisors since $F \subseteq R$. Conversely, suppose $F' = L \otimes_E F$ is a domain. Then F' is a field, and consequently we know that $F'\langle\!\langle x, y\rangle\!\rangle \supseteq L \otimes_E F\langle\!\langle x, y\rangle\!\rangle \supseteq F\langle\!\langle x, y\rangle\!\rangle$. In particular, $D' = L \otimes_E D$ is a domain, so Lemma 4.5 implies that $L \otimes_E R = L \otimes_E \mathcal{U}(S)$ is a domain, and (iii) is proved. ∎

It is now a simple matter to prove our last two main results.

Proof of Theorem 1.4: We use the field extensions described in the previous section. Specifically, we start with the rational function field $K(t)$ and, for each infinite subset $\mathcal{I}$ of $\mathcal{P}$, we let $F_{\mathcal{I}}$ be the field extension of $K(t)$ generated by all t_p with $p \in \mathcal{I}$. Now for each such $\mathcal{I} \subseteq \mathcal{P}$, let $F = F_{\mathcal{I}}$, $E = K(t)$, and let $\mathcal{F} = \{0 = f_0, f_1, f_2, \ldots\}$ be given by $f_i = t_{p_i}$, where p_i is the ith prime contained in $\mathcal{I}$. Then we can let $D_{\mathcal{I}}$ be the E-division algebra given by Lemma 4.6. It follows that $\mathbb{Z}(D_{\mathcal{I}}) = E = K(t)$ and that $D_{\mathcal{I}}$ has two generators as a K-division algebra, since $K(\mathcal{F}) = F_{\mathcal{I}}$.

Since there are uncountably many such subsets $\mathcal{I}$, it remains to show that $D_{\mathcal{I}}$ determines $\mathcal{I}$. To this end, let L be a field containing $\mathbb{Z}(D_{\mathcal{I}}) = K(t)$ of degree $|L : K(t)| = p \in \mathcal{P}$. Then, by Lemma 4.6(iii), $L \otimes_{K(t)} D_{\mathcal{I}}$ contains a zero divisor if and only if $L \otimes_{K(t)} F_{\mathcal{I}}$ has a zero divisor. Furthermore, by Lemma 3.1(ii)(iii), the latter cannot occur if $p \notin \mathcal{I}$ and it can and does occur if $p \in \mathcal{I}$. Thus $\mathcal{I}$ is indeed determined by $D_{\mathcal{I}}$, and consequently we obtain uncountably many nonisomorphic division algebras in this way. ∎

Proof of Proposition 1.5: Here, for each such $\mathcal{I} \subseteq \mathcal{P}$, we take $E = F = F_{\mathcal{I}}$, and we let $\mathcal{F} = \{0 = f_0, f_1, f_2, \ldots\}$ be given by $f_i = t_{p_i}$, where p_i is the ith prime contained in $\mathcal{I}$. Again, let $D_{\mathcal{I}}$ be the E-division algebra given by Lemma 4.6. It follows that $\mathbb{Z}(D_{\mathcal{I}}) = E = F_{\mathcal{I}}$ and that $D_{\mathcal{I}}$ has two generators as a K-division algebra, since $K(\mathcal{F}) = F_{\mathcal{I}}$. Finally, if $D_{\mathcal{I}} \cong D_{\mathcal{J}}$ is a K-isomorphism, then $F_{\mathcal{I}} = \mathbb{Z}(D_{\mathcal{I}}) \cong \mathbb{Z}(D_{\mathcal{J}}) = F_{\mathcal{J}}$ is also a K-isomorphism. In particular, Lemma 3.2 implies that $\mathcal{I} \sim \mathcal{J}$, and hence we conclude that there are uncountably many different K-division algebras $D_{\mathcal{I}}$. ∎

References

[C1] P. M. Cohn, *Free Rings and Their Relations,* Academic Press, London, 1985.

[C2] P. M. Cohn, *Skew Fields (Theory of General Division Rings),* Cambridge University Press, Cambridge, 1995.

[D] W. Dicks, *The HNN construction for rings,* Journal of Algebra **81** (1983), 434–487.

[H] P. Hall, *On the embedding of a group in a join of given groups,* Journal of the Australian Mathematical Society **17** (1974), 434–495.

[L] A. I. Lichtman, *On universal fields of fractions for free algebras,* Journal of Algebra **231** (2000), 652–676.

[LS] R. C. Lyndon and P. E. Schupp, *Combinatorial Group Theory,* Springer-Verlag, Berlin–New York, 1977.

[N] B. H. Neumann, *Some remarks on infinite groups,* Journal of the London Mathematical Society **12** (1937), 120–127.

[Pa] D. S. Passman, *The Algebraic Structure of Group Rings*, Wiley-Interscience, New York, 1977.

[Pl] B. I. Plotkin, *Seven Lectures on Universal Algebraic Geometry*, The Hebrew University, Jerusalem, preprint, 2002.