On a theorem of Ian Hughes about division rings of fractions

Warren Dicks[1], Dolors Herbera[2] and Javier Sánchez[3]

Departament de Matemàtiques
Universitat Autònoma de Barcelona
08193 Bellaterra (Barcelona), Spain

[1]dicks@mat.uab.es, [2]dolors@mat.uab.es,
[3]jsanchez@mat.uab.es

Abstract

Let G be a locally indicable group, K a division ring, and KG a crossed-product group ring. In 1961, Ian Hughes proved that, up to KG-isomorphism, at most one division ring of fractions of KG satisfies a certain independence condition, now called *Hughes freeness*. This result was applied by others in work on division rings of fractions of group rings of free groups. In this article, we introduce concepts that illuminate Hughes' arguments, and we simplify the proof of the theorem.

1991 Mathematics Subject Classification: 16S35, 12E15, 16S34, 16S36, 20E05, 16S10.

Key words and phrases: locally indicable group, division ring of fractions, Hughes-free.

1 Statement of Hughes' Theorem

In this section, we recall some terminology and state Hughes' theorem.

Let K be a division ring and G a multiplicative group.

Let KG be a *crossed-product group ring* (formed from K and G). Thus KG is a ring R having K as a subring (or, more precisely, there is a specified embedding of K in R), together with a specified left K-basis B of R, such that $K^\times B$ is a subgroup of the group of units of R, $K^\times$

is normal in $K^\times B$, and the resulting quotient group is G (or, more precisely, is isomorphic to G via a specified isomorphism).

Here, and in similar situations throughout, $K^\times$ denotes the group of units of K, and $K^\times B$ denotes the set of those elements of R which can be expressed as the product of an element of $K^\times$ followed by an element of B.

Notice that there is a bijection $B \to (K^\times B)/K^\times = G$. Although the inverse of this bijection determines an embedding $G \hookrightarrow KG$, we do not usually view G as a subset of KG (except in the case where B is closed under multiplication, that is, KG is a *skew group ring*). Nonetheless, we shall write $K^\times G$ to denote the group $K^\times B$.

It is not difficult to show that each subgroup H of G gives rise to a subring KH of KG which is a crossed-product group ring.

By a *division ring of fractions* of KG we mean a division ring D containing KG as a subring which rationally generates D. In other words, each element of D can be built up from the elements of KG in stages, using addition, subtraction, multiplication, and division by nonzero elements.

Two division rings of fractions of KG are said to be *KG-isomorphic* if there exists a (unique) isomorphism over KG between them.

We say that G is *indicable* if either G is trivial or G has an infinite cyclic quotient group. Thus free groups and free abelian groups are indicable.

If G is nontrivial and indicable, then there exists a normal subgroup H of G such that G/H is infinite cyclic. Here there exists an element t of G such that tH generates G/H. Let C denote the (cyclic) subgroup of G generated by t. Then G/H is a quotient of C, and therefore C is infinite and $C \cap H = 1$. Thus we have an expression of G as an internal semidirect product $G = H \rtimes C$ with C infinite cyclic. Groups with expressions of this form are precisely the nontrivial indicable groups.

We say that G is *locally indicable* if every finitely generated subgroup of G is indicable. Thus free groups, locally free groups, and torsion-free abelian groups are locally indicable.

Let G be locally indicable, for the remainder of this section.

Notice that G is torsion free. Graham Higman[1] showed that KG has no nonzero zerodivisors and that $K^\times G$ is the group of units of KG, since the grading arguments of his Section 4 apply to crossed-product group rings.

Suppose that D is a division ring of fractions of KG. For each subgroup H of G, let $D(H)$ be the (division) subring of D rationally generated by KH. We say that D is a *Hughes-free* division ring of fractions of KG if, for each nontrivial finitely generated subgroup H of G, and each expression of H as an internal semidirect product $N \rtimes C$ with C infinite

cyclic, the (faithful) image of C in $KC \subseteq D$ is left $D(N)$-independent in $D(N \rtimes C) = D(H)$. This latter condition means the following: If $t \in KC \subseteq D$ is the image of a generator of C, and $d_0, \ldots, d_n$ is a finite family in $D(N) \subseteq D$ for which $d_0 + d_1 t + \cdots + d_n t^n = 0_D$, then $d_0 = \cdots = d_n = 0$.

It is not known when KG has a Hughes-free division ring of fractions, or any division ring of fractions at all. In his 1961, Oxford DPhil thesis, written under the supervision of Graham Higman, Ian Hughes[2] proved that KG has *at most one* Hughes-free division ring of fractions, up to KG-isomorphism.

In 1970, Hughes[3] published the proof in a compressed form that is about one-sixth as long as the original proof. In this article, we introduce concepts that illuminate Hughes' arguments, and overall give a simplified, complete proof that is about two-thirds as long as the original proof.

Hughes' result has played an important rôle in the study of division rings of fractions of group rings of free groups, in that Jacques Lewin[4] and Peter Linnell[5],[6] have used it to link such diverse concepts as universal division rings of fractions of firs, Mal'cev-Neumann power-series group rings, and group von Neumann algebras.

2 Monoids and semirings

The purpose of this brief section is to introduce conventions and notation which will be used throughout.

2.1 Conventions. Additive semigroups (and, hence, additive monoids and groups) will be commutative; where there is a neutral element, it is called the *zero element* and denoted 0.

By an *additive map* we mean a morphism of additive semigroups.

Multiplicative monoids (and, hence, multiplicative groups) need not be commutative; the neutral element is called the *identity element* and denoted 1.

By a *multiplicative map* we mean a morphism of multiplicative monoids, so that the identity elements are respected. □

2.2 Notation. Let N be an additive monoid, and let X be a set.

We write N^X for the set of all functions from X to N, with the coordinate-wise additive-monoid structure. Here the zero element is the zero constant function.

For each $f \in N^X$, we define the *support* of f as

$$\operatorname{supp}(f) := \{x \in X \mid f(x) \neq 0\}.$$

Thus $\mathrm{supp}(f) = \emptyset$ if and only if $f = 0$.

We write $N^{(X)}$ for the submonoid of N^X consisting of all elements of N^X with finite support.

We define $N[X]$ to be the monoid $N^{(X)}$, but with each $f \in N^{(X)}$ expressed as $\sum_{x \in X} f(x)x \in N[X]$, the formal sum of the elements of the graph of f. □

We shall be interested in the case where $N = \mathbb{N}$.

2.3 Remarks. Let X be a set.

The free additive monoid on X is $\mathbb{N}[X]$, and the free additive semigroup on X is $\mathbb{N}[X] \setminus \{0\}$.

For $x \in X$, we identify x with the characteristic function of $\{x\}$, which sends x to 1, and sends all other elements of X to 0. Thus

$$X \subseteq \mathbb{N}[X] \setminus \{0\} \subset \mathbb{N}[X].$$

□

2.4 Definitions. By a *semiring* R we mean a set R endowed with an addition and a multiplication which give R the structure of an additive semigroup and a multiplicative monoid, respectively, and such that the multiplication is left and right distributive over the addition. In particular, R has an identity element but need not have a zero element.

If S is a semiring, then we define $S \cup \{\infty\}$ to be the semiring R which is the set consisting of S together with a new element, ∞, such that S is a subsemiring of R, and $\{\infty\} + R = \{\infty\} \cdot R = R \cdot \{\infty\} = \{\infty\}$.

By a *rational semiring* R we mean simply a semiring R endowed with a self-map, called the $*$-*map*, denoted $R \to R$, $r \mapsto r^*$. □

Eventually, we shall construct four rational semirings. The following is the first, and is fundamental.

2.5 Example. If D is a division ring, then D and $D \cup \{\infty\}$ are semirings, as in Definitions 2.4. We extend the map $D^\times \to D^\times$, $x \mapsto x^{-1}$, to a $*$-map on $D \cup \{\infty\}$ in which $0^* := \infty^* := \infty$. Thus $D \cup \{\infty\}$ is a rational semiring. □

3 The rational semiring of finite rooted trees

In this section, we collect together standard material on finite rooted trees, and construct the rational semiring which will be used to measure the complexity of elements of another rational semiring.

3.1 Definitions. Let $\mathcal{T}$ denote the set of all (isomorphism classes of) finite rooted trees.

We think of a rooted tree as an oriented tree in which each vertex is the terminal vertex of at most one edge, and the root is not the terminal vertex of any edge; this distinguishes the root.

We give $\mathcal{T}$ the structure of a rational semiring as follows.

Let $X, Y \in \mathcal{T}$.

The *sum* $X + Y$ is obtained from the disjoint union $X \cup Y$ by identifying the root of X with the root of Y, so the resulting vertex is the new root. (This is the *wedge* of X and Y, also denoted $X \vee Y$.) Then $\mathcal{T}$ is an additive monoid, and the zero element $0_{\mathcal{T}}$ is the tree with exactly one vertex.

We define the *family of* X, denoted $\mathrm{fam}(X)$, as the set of components of the graph obtained by deleting the root of X and all incident edges. We view $\mathrm{fam}(X)$ as a finite family of finite rooted trees, with multiplicities; here the root of each component is the vertex that was incident to the deleted edge. Notice that $\mathrm{fam}(0_{\mathcal{T}})$ is empty.

Since each element of $\mathrm{fam}(X)$ has fewer edges than X itself, we can recursively define $\mathrm{height}(X)$ as follows: $\mathrm{height}(0_{\mathcal{T}}) = 0$; if $X \neq 0_{\mathcal{T}}$, then $\mathrm{height}(X)$ is one more than the maximum of the heights of the elements of $\mathrm{fam}(X)$.

We define $\mathrm{width}(X)$ to be the number of elements in $\mathrm{fam}(X)$. In a tree of width one, the root is incident to a unique edge, called the *stem*.

We define *expanded* X, denoted $\exp(X)$, as the tree obtained from X by adding a stem, that is, we add a new vertex, and a new oriented edge which joins the new vertex to the root of X; here the new vertex is the root of $\exp(X)$. Notice that $\mathrm{height}(\exp(X)) = \mathrm{height}(X) + 1$.

We have

$$X = \sum_{X' \in \mathrm{fam}(X)} \exp(X'),$$

a (possibly empty) sum of trees with stems. We define the *product*

$$X \cdot Y := \sum_{X' \in \mathrm{fam}(X)} \sum_{Y' \in \mathrm{fam}(Y)} \exp(X' + Y').$$

Thus, the product of two trees with stems identifies the stems, and the multiplication is then extended distributively. Clearly, the multiplication is commutative. The identity element $1_{\mathcal{T}} = \exp(0_{\mathcal{T}})$ is the tree with exactly one edge.

We remark that $\mathrm{fam}(X + Y)$ can be thought of as $\mathrm{fam}(X) \cup \mathrm{fam}(Y)$, and that $\mathrm{fam}(X \cdot Y)$ can be thought of as $\mathrm{fam}(X) + \mathrm{fam}(Y)$, provided that multiplicities are taken into account.

It is readily verified that $\mathcal{T}$ is a semiring. We make $\mathcal{T}$ into a rational semiring with the $*$-map given by $X^* := \exp^2(X)$, which is X with a double-length stem adjoined. □

3.2 Definitions. We now define a total order $\geq$ on $\mathcal{T}$.

We let $0_{\mathcal{T}}$ be the least element of $\mathcal{T}$.

For $n \in \mathbb{N}$, let $\mathcal{T}_n$ denote the set consisting of all the elements of $\mathcal{T}$ which have at most n edges.

We have ordered $\mathcal{T}_0 = \{0_{\mathcal{T}}\}$.

Suppose that $n \geq 1$, and that we have ordered $\mathcal{T}_{n-1}$.

Consider any $X, Y \in \mathcal{T}_n \setminus \{0_{\mathcal{T}}\}$.

Notice that $\mathrm{fam}(X)$ is a nonempty, finite family in the totally ordered set $\mathcal{T}_{n-1}$. We define $\log X$ to be the largest element of $\mathcal{T}_{n-1}$ belonging to $\mathrm{fam}(X)$. Then $\exp(\log X)$ is a summand of X; we denote the complement by $X - \exp\log X$. Thus, X can be recovered from $\log X$ and $X - \exp\log X$ by adding an oriented edge joining the root of $X - \exp\log X$ to the root of $\log X$.

Now $\log X$, $\log Y$, $X - \exp\log X$ and $Y - \exp\log Y$ all lie in the totally ordered set $\mathcal{T}_{n-1}$. If $\log X = \log Y$ and $X - \exp\log X = Y - \exp\log Y$, then $X = Y$. We define $X > Y$ to mean

$$(\log X > \log Y) \text{ or } (\log X = \log Y \text{ and } X - \exp\log X > Y - \exp\log Y).$$

This completes the recursive definition of the total ordering on $\mathcal{T}$.

One can show, by induction on n, that the ordering on $\mathcal{T}$ refines the partial ordering by height and $\mathrm{height}(\log X) = \mathrm{height}(X) - 1$.

Clearly $\mathrm{width}(X - \exp\log X) = \mathrm{width}(X) - 1$. □

The following is well known.

3.3 Lemma. *$\mathcal{T}$ is well ordered.*

Proof. Suppose not, so that there exists a strictly descending sequence

$$T_0 > T_1 > T_2 > \cdots \tag{1}$$

in $\mathcal{T}$, and hence in $\mathcal{T} \setminus \{0_{\mathcal{T}}\}$. We shall obtain a contradiction.

We may assume that (1) has been chosen to minimize $\mathrm{height}(T_0)$. It follows that the set consisting of those elements of $\mathcal{T}$ whose height is at most $\mathrm{height}(T_0) - 1$, is well ordered. Thus, we may make the much stronger assumption that (1) has been chosen to minimize $\log T_0$.

With $\log T_0$ fixed, we may further assume that (1) has been chosen to minimize $\mathrm{width}(T_0)$.

By the definition of the ordering,

$$\log T_0 \geq \log T_1 \geq \log T_2 \geq \cdots .$$

If, for some $n \in \mathbb{N}$, $\log T_0 > \log T_n$, then we could omit the first n terms from (1) and obtain a contradiction to the minimality of $\log T_0$. Thus

$$\log T_0 = \log T_1 = \log T_2 = \cdots .$$

By the definition of the ordering,

$$T_0 - \exp\log T_0 > T_1 - \exp\log T_1 > T_2 - \exp\log T_2 > \cdots .$$

It follows from the minimality of $\log T_0$ that

$$\log(T_0 - \exp\log T_0) \geq \log(T_0);$$

clearly, equality must hold. It follows from the minimality of $\operatorname{width}(T_0)$ with $\log T_0$ fixed that $\operatorname{width}(T_0 - \exp\log T_0) \geq \operatorname{width}(T_0)$; this is absurd. □

We have not defined $\log(0_{\mathcal{T}})$, and it is convenient to have an interpretation for this expression.

3.4 Notation. Let $\mathcal{T} \cup \{-\infty\}$ be a semiring as in Definitions 2.4.

Extend the order on $\mathcal{T}$ to an order on $\mathcal{T} \cup \{-\infty\}$ so that $-\infty$ is the new smallest element.

Define $\log(0_{\mathcal{T}}) := -\infty$ and $\log(-\infty) := -\infty$. □

We leave the proof of the following to the reader.

3.5 Lemma. *If $X, Y, X', Y' \in \mathcal{T}$, then the following hold.*

(i) *If $X' \leq X$ and $Y' \leq Y$, then $X' + Y' \leq X + Y$, and equality holds if and only if $X' = X$ and $Y' = Y$.*

(ii) *$X \leq X + Y$, and equality holds if and only if $Y = 0_{\mathcal{T}}$.*

(iii) *If X and Y are nonzero, then $X \leq X \cdot Y$, and equality holds if and only if $Y = 1_{\mathcal{T}}$.*

(iv) $\log(X + Y) = \max\{\log X, \log Y\}$.

(v) $\log(X \cdot Y) = \log X + \log Y$.

(vi) $\log^2(X + Y) = \max\{\log^2 X, \log^2 Y\}$.

(vii) $\log^2(X \cdot Y) \leq \max\{\log^2 X, \log^2 Y\}$, *and equality holds if X and Y are nonzero.* □

4 Universal rational semirings

Throughout this section and the next, let U be a multiplicative group.

4.1 Definitions. By a *U-semiring* R we mean a semiring R given with a multiplicative map $\phi\colon U \to R$. Thus the identity elements are respected, and R has a U-biset structure.

By a *rational U-semiring* R we mean a rational semiring R which is a U-semiring such that the $*$-map on R is an *anti-map of U-bisets*, that is,

$$(urv)^* = v^{-1}r^*u^{-1} \text{ for all } r \in R, u, v \in U.$$

By a *morphism of rational U-semirings* $\Phi\colon R_1 \to R_2$ we mean a map between two rational U-semirings which commutes with all the operations, that is, the sum, the product, the identity element, the $*$-map, and the map from U. □

4.2 Examples. (i) If D is a division ring, then the rational semiring $D \cup \{\infty\}$ of Example 2.5 is a rational $D^\times$-semiring.

Hence, if U is a subgroup of $D^\times$, then $D \cup \{\infty\}$ is a rational U-semiring.

(ii) By Definitions 3.1, $\mathcal{T}$ is a rational semiring. We make $\mathcal{T}$ into a rational U-semiring via the trivial multiplicative map $U \to \mathcal{T}$ which sends every element of U to $1_{\mathcal{T}}$. Here the U-biset structure is trivial. □

We now explain how to construct formal rational expressions starting from U. First, we describe an aspect of the multiplication we shall be using.

4.3 Definitions. (i) Let X_1 and X_2 be U-bisets.

We define $X_1 \times_U X_2$ to be $(X_1 \times X_2)/\sim$ where $(x_1, x_2) \sim (x_1', x_2')$ if and only if there exists $u \in U$ such that $x_1 u = x_1'$ and $u^{-1}x_2 = x_2'$. This is easily seen to be an equivalence relation. The equivalence class of (x_1, x_2) will be denoted $x_1 \times_U x_2$ or $x_1 x_2$.

There is a natural U-biset structure on $X_1 \times_U X_2$.

If X_3 is a U-biset then there is a natural identification

$$(X_1 \times_U X_2) \times_U X_3 = X_1 \times_U (X_2 \times_U X_3),$$

and we denote this U-biset as $X_1 \times_U X_2 \times_U X_3$. Similar conventions apply for any finite number of U-bisets.

(ii) Suppose that U is a subgroup of some group W.

If Y is a W-biset, then a subset X of Y is said to be an *admissible U-sub-biset of the W-biset* Y if X is closed under left and right multiplication by the elements of U, and, moreover, for all $w \in W \setminus U$ both $X \cap wX$ and $X \cap Xw$ are empty.

If Y_1 and Y_2 are W-bisets and X_1 (resp. X_2) is an admissible U-sub-biset of the W-biset Y_1 (resp. Y_2), it is not difficult to show that the natural map $X_1 \times_U X_2 \to Y_1 \times_W Y_2$ is injective. In this situation, we usually identify $X_1 \times_U X_2$ with its image in $Y_1 \times_W Y_2$. It is not difficult to show that $X_1 \times_U X_2$ is (identified with) an admissible U-sub-biset of the W-biset $Y_1 \times_W Y_2$. □

Next, we describe the addition and multiplication we shall be using.

4.4 Definition. Let X be a U-biset.

The *free multiplicative monoid on X over U* is the multiplicative monoid

$$U\natural X := U \cup X \cup (X \times_U X) \cup \cdots = \bigcup_{n\in\mathbb{N}} X^{\times_U^n},$$

presented with generating set $U \cup X$, and with those relations which come from the multiplication in U, together with those which come from the left and right actions of U on X. (We suggest that here $U\natural X$ could be pronounced as 'U adjoin X' as well as 'U natural X'.) Clearly U is a submonoid of $U\natural X$.

The free additive semigroup on $U\natural X$, $\mathbb{N}[U\natural X]\setminus\{0\}$, then has a natural U-semiring structure. □

Let us digress to remark that $\mathbb{N}[U\natural X] \setminus \{0\}$ is a subsemiring of the monoid ring $\mathbb{Z}[U\natural X]$, and the latter can be viewed as the tensor ring

$$R\langle B\rangle := R \oplus B \oplus (B \otimes_R B) \oplus \cdots = \bigoplus_{n\in\mathbb{N}} B^{\otimes_R^n},$$

where R is the group ring $\mathbb{Z}[U]$, and B is the R-bimodule $\mathbb{Z}[X]$.

We next introduce the $*$-maps we shall be using.

4.5 Notation. If B is a U-biset, then $B^\dagger$ denotes a disjoint copy of B, with bijective map $B \to B^\dagger$, $b \mapsto b^*$, and we endow $B^\dagger$ with a U-biset structure by defining $ub^*v := (v^{-1}bu^{-1})^*$, for all $u, v \in U$, $b \in B$. □

We can now construct the rational U-semiring of interest.

4.6 Definition. Since $\mathbb{N}[U] \setminus \{0\}$ is a U-semiring, it is a U-biset; we set $X_1 := (\mathbb{N}[U] \setminus \{0\})^\dagger$, and $X_0 := \emptyset$, a U-sub-biset of X_1.

Now suppose that $n \geq 1$, and that we are given a U-biset X_n and a U-sub-biset X_{n-1}.

Then $\mathbb{N}[U\natural X_n]$ is a U-semiring, and $\mathbb{N}[U\natural X_n]\setminus\mathbb{N}[U\natural X_{n-1}]$ is a U-sub-biset. We set $X_{n+1} := (\mathbb{N}[U\natural X_n] \setminus \mathbb{N}[U\natural X_{n-1}])^\dagger \cup X_n$.

Thus we have recursively defined an ascending chain (X_n) of U-bisets.

We denote the union of this chain by X, a U-biset, and define the *universal rational U-semiring* as $\mathrm{Rat}(U) := \mathbb{N}[U\natural X] \setminus \{0\}$, a rational U-semiring with a $*$-map which carries $\mathbb{N}[U] \setminus \{0\}$ to X_1, and

$\mathbb{N}[U\natural X_n] \setminus \mathbb{N}[U\natural X_{n-1}]$ to $X_{n+1} \setminus X_n$, for each $n \geq 1$. By induction, the $*$-map carries $\mathbb{N}[U\natural X_n] \setminus \{0\}$ to X_{n+1}, for each $n \geq 0$. On taking unions we see that the $*$-map (bijectively) carries $\mathrm{Rat}(U)$ to X.

We define $\mathrm{Rat}(U) \cup \{0\}$ to be the U-semiring $\mathbb{N}[U\natural X]$. □

We now present the universal property of $\mathrm{Rat}(U)$ which we shall apply in four quite different situations.

4.7 Lemma. *If U is a multiplicative group, and R a rational U-semiring, then there exists a unique morphism $\Phi\colon \mathrm{Rat}(U) \to R$ of rational U-semirings.*

We remark that, if R has a zero element, then Φ extends to an additive map $\Phi'\colon \mathrm{Rat}(U) \cup \{0\} \to R$, and this is a morphism of U-semirings if we have

$$\{0_R\} \cdot R = R \cdot \{0_R\} = \{0_R\}.$$

Proof of Lemma 4.7. We use the notation of Definition 4.6.

Let $\psi_0\colon X_0\ (= \emptyset) \to R$ be the inclusion map, a morphism of U-bisets.

Suppose that $n \geq 0$, and that $\psi_n\colon X_n \to R$ is a morphism of U-bisets.

Then ψ_n induces a morphism of U-semirings $\phi_n\colon \mathbb{N}[U\natural X_n] \setminus \{0\} \to R$. Now we define $\psi_{n+1}\colon X_{n+1} \to R$, by

$$\psi_{n+1}(f^*) := (\phi_n(f))^* \text{ for all } f \in \mathbb{N}[U\natural X_n] \setminus \{0\}.$$

This is a morphism of U-bisets.

Thus we have recursively defined a sequence (ψ_n) of morphisms of U-bisets.

It is easy to prove, by induction, that ψ_{n+1} agrees with ψ_n on X_n, for all $n \geq 0$. Taking unions, or limits, we get a morphism of U-bisets, $\Psi\colon X \to R$, and this induces a morphism of rational U-semirings

$$\Phi\colon \mathbb{N}[U\natural X] \setminus \{0\} \to R,$$

as desired.

It is straightforward to check that there is only one such morphism. □

The following are important.

4.8 Examples. (i) If U is a subgroup of some group W, then, applying Lemma 4.7 with $R = \mathrm{Rat}(W)$, we get a morphism of rational U-semirings

$$\mathrm{Rat}(U) \to \mathrm{Rat}(W).$$

We leave it as an exercise to show that $\mathrm{Rat}(U)$ is (identified with) an admissible U-sub-biset of the W-biset $\mathrm{Rat}(W)$; in particular, $\mathrm{Rat}(U)$ can be treated as a rational subsemiring of $\mathrm{Rat}(W)$.

(ii) Let D be a division ring, and let $D \cup \{\infty\}$ have the structure of a rational $D^\times$-semiring, as in Example 4.2(i).

Applying Lemma 4.7 with $U = D^\times$ and $R = D \cup \{\infty\}$, we get a morphism of rational $D^\times$-semirings, $\Phi\colon \mathrm{Rat}(D^\times) \to D \cup \{\infty\}$.

Similarly, if U is a subgroup of $D^\times$, then we get a morphism of rational U-semirings, $\Psi\colon \mathrm{Rat}(U) \to D \cup \{\infty\}$, and Ψ can be thought of as the restriction of Φ.

(iii) By Example 4.2(ii), $\mathcal{T}$ is a rational U-semiring. Applying Lemma 4.7 with $R = \mathcal{T}$, we get a morphism of U-semirings,

$$\mathrm{Tree}\colon \mathrm{Rat}(U) \cup \{0\} \to \mathcal{T};$$

for $f \in \mathrm{Rat}(U) \cup \{0\}$, we call $\mathrm{Tree}(f)$ the *complexity* of f. □

We now record the basic properties of the complexity, most of which follow from Lemma 3.5.

4.9 Lemma. *If $f, g \in \mathrm{Rat}(U) \cup \{0\}$, then the following hold.*

(i) $\mathrm{Tree}(f) = 0_\mathcal{T}$ *if and only if* $f = 0$.

(ii) $\mathrm{Tree}(f) = 1_\mathcal{T}$ *if and only if* $f \in U$.

(iii) $\mathrm{Tree}(f + g) = \mathrm{Tree}(f) + \mathrm{Tree}(g)$.

(iv) $\mathrm{Tree}(f) \leq \mathrm{Tree}(f + g)$, *and equality holds if and only if* $g = 0$.

(v) $\mathrm{Tree}(fg) = \mathrm{Tree}(f) \cdot \mathrm{Tree}(g)$.

(vi) *If f and g are nonzero, then* $\mathrm{Tree}(f) \leq \mathrm{Tree}(fg)$, *and equality holds if and only if* $g \in U$.

(vii) $\log(\mathrm{Tree}(f + g)) = \max\{\log(\mathrm{Tree}(f)), \log(\mathrm{Tree}(g))\}$.

(viii) $\log(\mathrm{Tree}(fg)) = \log(\mathrm{Tree}(f)) + \log(\mathrm{Tree}(g))$.

(ix) $\log^2(\mathrm{Tree}(f + g)) = \max\{\log^2(\mathrm{Tree}(f)), \log^2(\mathrm{Tree}(g))\}$.

(x) $\log^2(\mathrm{Tree}(fg)) \leq \max\{\log^2(\mathrm{Tree}(f)), \log^2(\mathrm{Tree}(g))\}$, *and equality holds if f and g are nonzero.*

(xi) *If f is nonzero, then* $\mathrm{Tree}(f^*) > \log^2(\mathrm{Tree}(f^*)) = \mathrm{Tree}(f)$. □

5 Source subgroups

Again, throughout this section, U is a multiplicative group.

In this section, we study $\mathrm{Rat}(U)$ in some detail. The sole objective here is to prove that, for each $f \in \mathrm{Rat}(U)$, there exists a (unique) smallest subgroup V of U such that $f \in \mathrm{Rat}(V) \cdot U$; we will then observe that V is finitely generated. The techniques used underlie Hughes' original argument.

5.1 Definitions. We use the notation of Definition 4.6.

We define a subset Q of X, and a subset P of $\mathbb{N}[U\natural X] \setminus \{0\}$.

Let $Q_0 = X_0$ $(= \emptyset)$.

Suppose that $n \geq 0$, and that we have defined a subset Q_n of X_n.

Let $\langle Q_n \rangle$ denote the submonoid of $U\natural X_n$ generated by Q_n, and set

$$P_n := \langle Q_n \rangle + \mathbb{N}[U\natural X_n], \quad Q_{n+1} := P_n^*. \tag{2}$$

Notice $P_n \subseteq \mathbb{N}[U\natural X_n] \setminus \{0\}$, and therefore

$$Q_{n+1} = P_n^* \ \subseteq \ (\mathbb{N}[U\natural X_n] \setminus \{0\})^* = X_{n+1}.$$

Thus we have recursively defined a sequence (Q_n) of subsets of X, and we also have a sequence (P_n) of subsets of $\mathbb{N}[U\natural X] \setminus \{0\}$.

Clearly Q_0 $(= \emptyset)$ is contained in Q_1.

Suppose that $n \geq 1$, and that Q_{n-1} is contained in Q_n.

Then $\langle Q_{n-1} \rangle \subseteq \langle Q_n \rangle$, and, by (2), $P_{n-1} \subseteq P_n$ and $Q_n \subseteq Q_{n+1}$.

By induction, the sequence (Q_n) is an ascending chain.

We define Q to be the union of this chain.

By (2), (P_n) is an ascending chain. We define P to be the union of this chain, and call P the set of *primitive* elements of $\mathbb{N}[U\natural X] \setminus \{0\}$. □

5.2 Lemma. *With notation as in* Definitions 5.1*, the following hold.*

(i) $P = \langle Q \rangle + \mathbb{N}[U\natural X]$ *and* $Q = P^*$.

(ii) *The sets* Q, $\langle Q \rangle$ *and* P *are closed under* U*-conjugation.*

(iii) $QU = UQ = X$.

(iv) $\langle Q \rangle U = U\langle Q \rangle = U\natural X$.

(v) $PU = UP = \mathbb{N}[U\natural X] \setminus \{0\}$.

Proof. (i) holds because, for each n, we have (2), and we then take the ascending union over all n.

(ii)–(v) It is clear that Q_0 $(= \emptyset)$ is closed under U-conjugation, and that $Q_0U = UQ_0 = X_0$ $(= \emptyset)$.

Now suppose that $n \geq 0$, and that Q_n is closed under U-conjugation, and that $Q_nU = UQ_n = X_n$.

Then $\langle Q_n \rangle$ is closed under U-conjugation, and it is clear from (2) that P_n and Q_{n+1} are closed under U-conjugation.

Since $\langle Q_n \rangle$ is closed under U-conjugation, it follows that

$$U\langle Q_n \rangle = \langle Q_n \rangle U.$$

Moreover, the latter is a submonoid of $U\natural X_n$ which contains U and $UQ_n = X_n$, and these generate $U\natural X_n$. Thus $U\langle Q_n \rangle = \langle Q_n \rangle U = U\natural X_n$.

By (2),

$$UP_n = U(\langle Q_n\rangle + \mathbb{N}[U\natural X_n]) = U\natural X_n + \mathbb{N}[U\natural X_n] = \mathbb{N}[U\natural X_n]\setminus\{0\}.$$

Thus $X_{n+1} = (\mathbb{N}[U\natural X_n]\setminus\{0\})^* = (UP_n)^* = P_n^* U^{-1} = Q_{n+1}U$.

Similarly, $P_nU = \mathbb{N}[U\natural X_n]\setminus\{0\}$, and $X_{n+1} = UQ_{n+1}$.

Now by induction, and taking unions, (ii) and (iii) hold. Moreover, the foregoing argument shows that (iv) and (v) follow. □

5.3 Definition. We use the notation of Definitions 5.1.

Let $p \in P$ and $u \in U$.

Recall that $p^u \in P$ by Lemma 5.2(ii).

We now recursively define the *source subgroup for* p, which is denoted $\mathrm{source}_U(p)$, or $\mathrm{source}(p)$. In the course of the definition, we (need to) prove that

$$\mathrm{source}(p^u) = (\mathrm{source}(p))^u,$$

and, moreover, if $pu \in P$, then $u \in \mathrm{source}(p)$ and $\mathrm{source}(pu) = \mathrm{source}(p)$.

Without loss of generality, we assume that, for each element of P of lesser complexity, the source subgroup is defined and has the above properties; we call this type of hypothesis a "transfinite induction hypothesis".

We have a partition of $P = \langle Q\rangle + \mathbb{N}[U\natural X]$ into four sets:

$$\{1\}, \quad Q, \quad \langle Q\rangle\setminus(Q\cup\{1\}), \quad \langle Q\rangle + (\mathbb{N}[U\natural X]\setminus\{0\}). \tag{3}$$

We now consider these four sets in order of difficulty.

Case 1. We define source(1) to be the trivial subgroup of U, and it is clear that the desired properties hold.

Case 2. Suppose that $p \in \langle Q\rangle + (\mathbb{N}[U\natural X]\setminus\{0\})$.

There is then an expression

$$p = \sum_{i=1}^{n} f_i,$$

where $n \geq 2$, $f_i \in U\natural X = \langle Q\rangle U$ for each i, and $f_{i_0} \in \langle Q\rangle$ for some i_0. Thus $f_i = p_i u_i$ for some $p_i \in \langle Q\rangle$ and $u_i \in U$; by Lemma 4.9(vi) and (iv), $\mathrm{Tree}(p_i) = \mathrm{Tree}(f_i) < \mathrm{Tree}(p)$. Further, we may assume that $u_{i_0} = 1$. We then define source(p) to be the subgroup of U generated by $\bigcup_{i=1}^{n}(\mathrm{source}(p_i)\cup\{u_i\})$.

Consider the following argument. Suppose that $pu \in P$; then

$$f_{i_0'}u \in \langle Q\rangle \quad \text{for some } i_0'.$$

For each i, choose an expression $f_i u = p'_i u'_i$ with $p'_i \in \langle Q \rangle$ and $u'_i \in U$; then $p'_i = p_i u_i u u_i'^{-1}$ and $u_i u u_i'^{-1} \in \mathrm{source}(p'_i) = \mathrm{source}(p_i)$, by the transfinite induction hypothesis. Further, we may assume $u'_{i'_0} = 1$.

The special case of this argument where $u = 1$ shows that $\mathrm{source}(p)$ is well defined.

The general case, together with the fact that $u_{i_0} = u'_{i'_0} = 1$, shows that, if $pu \in P$, then $u \in \mathrm{source}(p) = \mathrm{source}(pu)$.

Using the transfinite induction hypothesis, one can show that

$$\mathrm{source}(p^u) = (\mathrm{source}(p))^u.$$

Case 3. Suppose that $p \in \langle Q \rangle \setminus (Q \cup \{1\})$.

There is then an expression $p = qr$, where $q \in Q$, and $r \in \langle Q \rangle \setminus \{1\}$. By Lemma 4.9(vi), $\mathrm{Tree}(q) < \mathrm{Tree}(p)$ and $\mathrm{Tree}(r) < \mathrm{Tree}(p)$. We define $\mathrm{source}(p)$ to be the subgroup of U generated by $\mathrm{source}(q) \cup \mathrm{source}(r)$.

Consider the following argument. Suppose that $pu \in P$. We can write $pu = q'r'$ where $q' \in Q$ and $r' \in \langle Q \rangle \setminus \{1\}$. In a natural way,

$$U\natural X = U \cup (X \times_U (U\natural X)),$$

and thus $q' \times_U r' = q \times_U ru$. This means that there exists $v \in U$ such that $q' = qv$ and $r' = v^{-1}ru$, that is, $r^v v^{-1} u$. By the transfinite induction hypothesis,

$$\begin{aligned} v &\in \mathrm{source}(q') = \mathrm{source}(q), \\ v^{-1}u &\in \mathrm{source}(r') = \mathrm{source}(r^v) = v^{-1}\,\mathrm{source}(r)v. \end{aligned}$$

The special case of this argument where $u = 1$ shows that $\mathrm{source}(p)$ is well defined.

The general case shows that, if $pu \in P$, then

$$u \in \mathrm{source}(p) = \mathrm{source}(pu).$$

Using the transfinite induction hypothesis, one can show that

$$\mathrm{source}(p^u) = (\mathrm{source}(p))^u.$$

Case 4. Suppose that $p \in Q$.

Then $p = r^*$ where $r \in P$. By Lemma 4.9(xi), $\mathrm{Tree}(r) < \mathrm{Tree}(p)$. We define $\mathrm{source}(p) = \mathrm{source}(r)$. Since r is unique, $\mathrm{source}(p)$ is well defined.

Now $p^u = r^{*u} = r^{u*}$, and hence

$$\mathrm{source}(p^u) = \mathrm{source}(r^u) = (\mathrm{source}(r))^u = (\mathrm{source}(p))^u.$$

Suppose $pu \in P$. Since $pu = r^*u = (u^{-1}r)^* = (r^u u^{-1})^*$, we see $r^u u^{-1} \in P$, and, by definition, $\mathrm{source}(pu) = \mathrm{source}(r^u u^{-1})$. Thus, r^u and $r^u u^{-1}$ lie in P, and, by the transfinite induction hypothesis,

$$u^{-1} \in \mathrm{source}(r^u u^{-1}) = \mathrm{source}(r^u) = (\mathrm{source}(r))^u.$$

Hence $u \in \mathrm{source}(r^u u^{-1}) = \mathrm{source}(r)$, that is,

$$u \in \mathrm{source}(pu) = \mathrm{source}(p).$$

This completes the recursive definition. □

5.4 Lemma. *If p is a primitive element of $\mathrm{Rat}(U)$, then the following hold.*

(i) $\mathrm{source}(p)$ *is finitely generated.*

(ii) $p \in \mathrm{Rat}(\mathrm{source}(p))$.

(iii) *If U is a subgroup of some group W, then p is primitive in $\mathrm{Rat}(W)$ and $\mathrm{source}_W(p) = \mathrm{source}_U(p)$.*

Proof. All these statements can be proved by transfinite induction, using the recursive definition of $\mathrm{source}(p)$. □

5.5 Definition. We use the notation of Definition 5.3.

Consider any $f \in \mathrm{Rat}(U) = \mathbb{N}[U\natural X] \setminus \{0\}$. By Lemma 5.2(v), we can write $f = pu$ for some $p \in P$, $u \in U$. We define

$$\mathrm{source}(f) = \mathrm{source}(p).$$

If $f = p'u'$ for some $p' \in P$, $u' \in U$, then $p' = puu'^{-1}$, and then, by Definition 5.3, $\mathrm{source}(p') = \mathrm{source}(p)$. Thus $\mathrm{source}(f)$ is well defined. □

5.6 Remark. It is immediate from Definition 5.5, and Lemma 5.4(i) and (ii), that, for each $f \in \mathrm{Rat}(U)$, the subgroup $\mathrm{source}(f)$ is finitely generated, and $f \in \mathrm{Rat}(\mathrm{source}(f)) \cdot U$. □

5.7 Theorem. *Let U be a multiplicative group, and let $f \in \mathrm{Rat}(U)$. The set consisting of those subgroups V of U such that $f \in \mathrm{Rat}(V) \cdot U$, has a (unique) smallest element,* $\mathrm{source}(f)$*, and* $\mathrm{source}(f)$ *is finitely generated.*

Proof. Suppose that V is a subgroup of U such that $f \in \mathrm{Rat}(V) \cdot U$. We can write $f = gu$ for some $g \in \mathrm{Rat}(V)$, $u \in U$. We can then write $g = pv$ for some $v \in V$, and p a primitive element of $\mathrm{Rat}(V)$, and hence of $\mathrm{Rat}(U)$, by the first part of Lemma 5.4(iii). Then $f = gu = pvu$, and, by the second part of Lemma 5.4(iii),

$$\mathrm{source}(f) = \mathrm{source}_U(p) = \mathrm{source}_V(p) \leq V.$$

Together with Remark 5.6, this completes the proof. □

6 Skew Laurent-series constructions

In this section, we let E be a division ring, and α be an automorphism of E.

For certain U, we shall find that elements of $\mathrm{Rat}(U)$ are controlled by elements of lesser complexity.

6.1 Definition. In the additive group $E^{\mathbb{Z}}$, let $E^{[\mathbb{Z}]}$ denote the subgroup consisting of all of those elements whose supports are well ordered, that is, bounded below.

Let t be an indeterminate, and form the *skew Laurent-series ring* $E((t;\alpha))$, abbreviated $E((t))$. As an additive group, $E((t))$ is $E^{[\mathbb{Z}]}$, but an element $f = (d_n) \in E^{[\mathbb{Z}]}$ is represented by the expression

$$\sum_{n\in\mathbb{Z}} d_n t^n \in E((t)),$$

or sometimes $\sum_{n\in\mathbb{Z}} f_n$, where we understand $f_n = d_n t^n$. Multiplication in $E((t))$ is given by using the formulas $t^n t^m := t^{n+m}$, $t^n d := \alpha^n(d) t^n$, for all $d \in E$, $m, n \in \mathbb{Z}$, and extending distributively and continuously.

It can be shown that $E((t))$ is again a division ring. It is worth mentioning inverses. Consider

$$f = \sum_{n\in\mathbb{Z}} f_n \in E((t)) \setminus \{0\},$$

and let N denote the least element of the support of f. Set $g = f_N - f$. Then $f f_N^{-1} = 1 - g f_N^{-1}$. Thus $\sum_{m\geq 0} (g f_N^{-1})^m$ converges to an element of $E((t))$, and this is the inverse of $f f_N^{-1}$, that is, $f_N f^{-1}$. Hence we can write

$$f^{-1} = \sum_{m\geq 0} f_N^{-1} (g f_N^{-1})^m.$$

Let $E[t;\alpha]$ denote the subring of $E((t))$ consisting of those elements whose support is a finite subset of $\mathbb{N}$. We call $E[t;\alpha]$ a *skew polynomial ring*. Then $E[t;\alpha]$ is a (not necessarily commutative) principal ideal domain, and therefore, up to $E[t;\alpha]$-isomorphism, it has a unique (Ore) division ring of fractions, denoted $E(t;\alpha)$, which we can take to be the subring of $E((t;\alpha))$ rationally generated by $E[t;\alpha]$.

Let $E^\times\langle t\rangle$ denote the subset of $E((t))$ consisting of elements whose support contains exactly one element. This is an internal semidirect product $E^\times \rtimes_\alpha \langle t\rangle$, and a subgroup of $(E((t;\alpha)))^\times$ and of $(E(t;\alpha))^\times$. □

We now consider a formal analogue of the foregoing; this is the most important construction in Hughes' argument.

6.2 Definitions. (i) We write $E((t))$ for $E((t;\alpha))$, and write $E^\times\langle t\rangle$ for $E^\times \rtimes_\alpha \langle t\rangle$.

As in Example 4.8(ii), there is a morphism of rational $E^\times\langle t\rangle$-semirings, $\Phi\colon \mathrm{Rat}(E^\times\langle t\rangle) \to E((t)) \cup \{\infty\}$, and, clearly, Φ extends to an additive map $\Phi'\colon \mathrm{Rat}(E^\times\langle t\rangle) \cup \{0\} \to E((t)) \cup \{\infty\}$.

We shall construct a rational $E^\times\langle t\rangle$-semiring $\mathrm{Rat}(E^\times)((t;\alpha)) \cup \{\infty\}$, and factor Φ through it.

(ii) First, we construct an $E^\times\langle t\rangle$-semiring $\mathrm{Rat}(E^\times)((t;\alpha))$, or, in abbreviated form, $\mathrm{Rat}(E^\times)((t))$.

Notice that α induces a group automorphism of $E^\times$, and, by Lemma 4.7, this induces a semiring automorphism of $\mathrm{Rat}(E^\times) \cup \{0\}$, again denoted α. The semiring $\mathrm{Rat}(E^\times\langle t\rangle)$ contains copies of $\mathrm{Rat}(E^\times)$ and $\langle t\rangle$, and we denote the product by $\mathrm{Rat}(E^\times)\langle t\rangle$; this is a multiplicative submonoid of $\mathrm{Rat}(E^\times\langle t\rangle)$ because t normalizes $\mathrm{Rat}(E^\times)$. Thus

$$E^\times\langle t\rangle \subseteq \mathrm{Rat}(E^\times)\langle t\rangle \subseteq \mathrm{Rat}(E^\times\langle t\rangle).$$

In the additive monoid $(\mathrm{Rat}(E^\times) \cup \{0\})^{\mathbb{Z}}$, let $(\mathrm{Rat}(E^\times) \cup \{0\})^{[\mathbb{Z}]}$ denote the submonoid consisting of all of those elements whose supports are bounded below. As an additive semigroup, $\mathrm{Rat}(E^\times)((t))$ is defined to be

$$(\mathrm{Rat}(E^\times) \cup \{0\})^{[\mathbb{Z}]} \setminus \{0\},$$

but with each $f = (d_n) \in (\mathrm{Rat}(E^\times) \cup \{0\})^{[\mathbb{Z}]} \setminus \{0\}$ represented as an expression

$$f = \sum_{n\in\mathbb{Z}} d_n t^n = \sum_{n\in\mathbb{Z}} f_n \in \mathrm{Rat}(E^\times)((t)), \tag{4}$$

where we understand $f_n = d_n t^n \in \mathrm{Rat}(E^\times)\langle t\rangle \cup \{0\}$.

Multiplication in $\mathrm{Rat}(E^\times)((t))$ is given by using the multiplication of the f_n defined in $\mathrm{Rat}(E^\times)\langle t\rangle \cup \{0\}$, and extending distributively and continuously. Then $\mathrm{Rat}(E^\times)((t))$ is a semiring. Moreover, we have multiplicative monoid inclusions $E^\times\langle t\rangle \subseteq \mathrm{Rat}(E^\times)\langle t\rangle \subseteq \mathrm{Rat}(E^\times)((t))$, and therefore $\mathrm{Rat}(E^\times)((t))$ is an $E^\times\langle t\rangle$-semiring.

(iii) We now define a morphism $\Omega\colon \mathrm{Rat}(E^\times)((t)) \cup \{\infty\} \to E((t)) \cup \{\infty\}$ of $E^\times\langle t\rangle$-semirings. We define $\Omega(\infty) := \infty$. Now suppose that we are given f as in (4). If, for some $n \in \mathbb{Z}$, $\Phi'(f_n) = \infty$, then we define $\Omega(f) := \infty$. In the remaining case, where, for all $n \in \mathbb{Z}$, $\Phi'(f_n) \neq \infty$, we define

$$\Omega(f) := \sum_{n\in\mathbb{Z}} \Phi'(f_n) = \sum_{n\in\mathbb{Z}} \Phi'(d_n)t^n \in E((t)).$$

It can be shown that Ω is a morphism of $E^\times\langle t\rangle$-semirings.

(iv) We now make the $E^\times\langle t\rangle$-semiring $\mathrm{Rat}(E^\times)((t)) \cup \{\infty\}$ into a rational $E^\times\langle t\rangle$-semiring by lifting back the $*$-map of $E((t)) \cup \{\infty\}$.

We define $\infty^* = \infty$.

Suppose that we are given f as in (4).

If $\Omega(f) \in \{0, \infty\}$, then we define $f^* := \infty$.

Thus we may assume that, for all $n \in \mathbb{Z}$, $\Phi'(f_n) \neq \infty$, and that there is a least $N \in \mathbb{Z}$ such that $\Phi'(f_N) \neq 0$, that is, $f_N = d_N t^N$ for some $d_N \in \mathrm{Rat}(E^\times)$. Now $\mathrm{Rat}(E^\times)$ contains the elements d_N^* and $\alpha^{-N}(d_N^*)$; we set

$$f_N^* := t^{-N} d_N^* = \alpha^{-N}(d_N^*) t^{-N} \in \mathrm{Rat}(E^\times)\langle t\rangle.$$

Also, $E^\times$ contains the element -1; we set $g = \sum_{n \geq N+1} (-1) f_n$. Then $\sum_{m \geq 0} f_N^* (g f_N^*)^m$ converges to some $h \in \mathrm{Rat}(E^\times)((t))$, and we take f^* to be h. The least element of the support of f^* is $-N$, and, for each $n \in \mathbb{Z}$, h_n is built up from $\{f_N^*\} \cup \{(-1) f_i \mid N+1 \leq i \leq 2N+n\}$ using addition and multiplication.

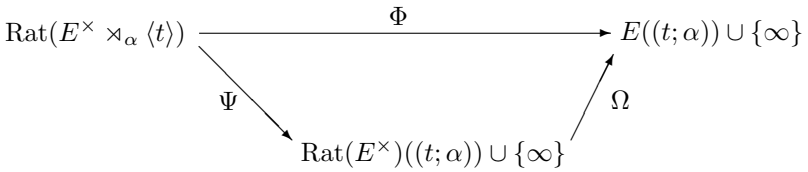
Thus we have a $*$-map, and it can be shown that

$$\mathrm{Rat}(E^\times)((t)) \cup \{\infty\}$$

is a rational $E^\times\langle t\rangle$-semiring, and Ω is a morphism of rational $E^\times\langle t\rangle$-semirings.

(v) By Lemma 4.7, with $U = E^\times\langle t\rangle$ and $R = \mathrm{Rat}(E^\times)((t)) \cup \{\infty\}$, we get a morphism $\Psi\colon \mathrm{Rat}(E^\times\langle t\rangle) \to \mathrm{Rat}(E^\times)((t)) \cup \{\infty\}$ of rational $E^\times\langle t\rangle$-semirings. For each $f \in \mathrm{Rat}(E^\times\langle t\rangle)$ such that $\Psi(f) \neq \infty$, we abuse notation and write $\Psi(f) = \sum_{n \in \mathbb{Z}} f_n$, where we understand that $f_n \in \mathrm{Rat}(E^\times) t^n \cup \{0\}$.

Notice that composing Ψ with Ω gives Φ, since the two routes both act as inclusion on $E^\times\langle t\rangle$.



We view Φ, Ψ and Ω as acting as the identity on $E^\times\langle t\rangle$.

We write $\Psi(f) = f$ if $f \in \mathrm{Rat}(E^\times\langle t\rangle)$ and there exist $n \in \mathbb{Z}$ and $d_n \in \mathrm{Rat}(E^\times)$ such that $f = d_n t^n \in \mathrm{Rat}(E^\times)\langle t\rangle$ and $\Psi(f)$ is the Laurent series having one nonzero summand $f_n = d_n t^n$. □

We now show that if $f \in \mathrm{Rat}(E^\times\langle t\rangle)$, then f is usually more complex than each of the summands of the series $\Psi(f)$.

6.3 Theorem. *With notation as in* Definition 6.2(v)*, if* $f \in \mathrm{Rat}(E^\times\langle t\rangle)$ *and* $\infty \neq \Psi(f) = \sum_{n\in\mathbb{Z}} f_n \in \mathrm{Rat}(E^\times)((t))$*, then either* $\Psi(f) = f$ *or* $\mathrm{Tree}(f_n) < \mathrm{Tree}(f)$ *for all* $n \in \mathbb{Z}$*.*

In other words, for each $n \in \mathbb{Z}$, $\mathrm{Tree}(f_n) \leq \mathrm{Tree}(f)$, and equality holds if and only if $\Psi(f) = f_n = f$.

Proof of Theorem 6.3. Without loss of generality, we suppose that the implication holds for elements of lesser complexity.

To simplify notation, write $U := E^\times\langle t\rangle$, so that

$$\mathrm{Rat}(U) = \mathbb{N}[U\natural X] \setminus \{0\},$$

in the notation of Definition 4.6.

We use the same sort of subdivision into cases as in (3); thus we partition $\mathbb{N}[U\natural X] \setminus \{0\}$ into the four sets

$$U, \quad X, \quad (U\natural X) \setminus (X \cup U), \quad \mathbb{N}[U\natural X] \setminus (U\natural X \cup \{0\}).$$

Again, we consider these four sets in order of difficulty.

Case 1. If $f \in U = E^\times\langle t\rangle$, then $\Psi(f) = f$, as desired.

Case 2. Suppose that $f \in \mathbb{N}[U\natural X] \setminus (U\natural X \cup \{0\})$.

Here, there exist $g, h \in \mathbb{N}[U\natural X] \setminus \{0\}$, such that $f = g + h$; in fact, we could even assume $g \in U\natural X$.

By Lemma 4.9(iv), $\mathrm{Tree}(g) < \mathrm{Tree}(f)$ and $\mathrm{Tree}(h) < \mathrm{Tree}(f)$; therefore, by the transfinite induction hypothesis, the implication holds for g and h.

Consider any $n \in \mathbb{Z}$.

We can write $f_n = g_n + h_n$, and

$$\mathrm{Tree}(f_n) = \mathrm{Tree}(g_n) + \mathrm{Tree}(h_n) \leq \mathrm{Tree}(g) + \mathrm{Tree}(h) = \mathrm{Tree}(f).$$

Now suppose that $\mathrm{Tree}(f_n) = \mathrm{Tree}(f)$. Then $\mathrm{Tree}(g_n) = \mathrm{Tree}(g)$ and $\mathrm{Tree}(h_n) = \mathrm{Tree}(h)$. Here $\Psi(g) = g$ and $\Psi(h) = h$. It follows that $\Psi(f) = f$, as desired.

Case 3. Suppose that $f \in (U\natural X) \setminus (X \cup U)$.

Here, there exist $g, h \in U\natural X \setminus U$, such that $f = gh$; in fact, we could even assume $g \in X$.

By Lemma 4.9(vi), $\mathrm{Tree}(g) < \mathrm{Tree}(f)$ and $\mathrm{Tree}(h) < \mathrm{Tree}(f)$; therefore, by the transfinite induction hypothesis, the implication holds for g and h.

Consider any $n \in \mathbb{Z}$.

We can write $f_n = \sum_{m\in\mathbb{Z}} g_m h_{n-m}$; only finitely many of the summands are nonzero. By Lemma 4.9(vii) and (viii),

$$\begin{aligned}\log(\mathrm{Tree}(f_n)) &= \max\{\log(\mathrm{Tree}(g_m)) + \log(\mathrm{Tree}(h_{n-m})) \mid m \in \mathbb{Z}\}\\ &\leq \log(\mathrm{Tree}(g)) + \log(\mathrm{Tree}(h)) = \log(\mathrm{Tree}(f)).\end{aligned}$$

If $\log(\mathrm{Tree}(f_n)) < \log(\mathrm{Tree}(f))$, then $\mathrm{Tree}(f_n) < \mathrm{Tree}(f)$.

Now suppose that $\log(\mathrm{Tree}(f_n)) = \log(\mathrm{Tree}(f))$. Then there is some $m \in \mathbb{Z}$ such that

$$\log(\mathrm{Tree}(g_m)) = \log(\mathrm{Tree}(g)) \text{ and } \log(\mathrm{Tree}(h_{n-m})) = \log(\mathrm{Tree}(h)).$$

Since $g, h \in U\natural X$, we have $\mathrm{width}(\mathrm{Tree}(g)) = \mathrm{width}(\mathrm{Tree}(h)) = 1$; therefore,

$$\mathrm{Tree}(g_m) \geq \mathrm{Tree}(g) \text{ and } \mathrm{Tree}(h_{n-m}) \geq \mathrm{Tree}(h).$$

Here $g = \Psi(g) = g_m$ and $h = \Psi(h) = h_{n-m}$; it follows that

$$f = \Psi(f) = f_n,$$

as desired.

Case 4. Suppose that $f \in X$.

Here, there exists $g \in \mathbb{N}[U\natural X] \setminus \{0\}$ such that $f = g^*$.

Now $\infty \neq \Psi(f) = (\Psi(g))^*$ and, by Lemma 4.9(xi),

$$\mathrm{Tree}(f) > \mathrm{Tree}(g).$$

By the transfinite induction hypothesis, the implication holds for g.

There exists $N \in \mathbb{Z}$ such that $-N$ is the least element of the support of $\Psi(f)$.

By Lemma 4.9(xi),

$$\log^2(\mathrm{Tree}(g_N^*)) = \mathrm{Tree}(g_N) \leq \mathrm{Tree}(g) = \log^2(\mathrm{Tree}(f)). \tag{5}$$

Also, for each $m \in \mathbb{Z}$, by Lemma 4.9(vi),

$$\begin{aligned}\log^2(\mathrm{Tree}((-1)g_m)) &< \mathrm{Tree}((-1)g_m)\\ &= \mathrm{Tree}(g_m) \leq \mathrm{Tree}(g) = \log^2(\mathrm{Tree}(f)).\end{aligned}$$

Consider any $n \in \mathbb{Z}$.

Now f_n is built up from $\{g_N^*, (-1)g_m \mid m = N+1, \ldots, 2N+n\}$ using multiplication and addition; hence, by Lemma 4.9(ix) and (x),

$$\begin{aligned}&\log^2(\mathrm{Tree}(f_n))\\ &\leq \max\{\log^2(\mathrm{Tree}(g_N^*)), \log^2(\mathrm{Tree}((-1)g_m)) \mid m = N+1, \ldots, 2N+n\}\\ &\leq \log^2(\mathrm{Tree}(f)).\end{aligned}$$

If $\log^2(\mathrm{Tree}(f_n)) < \log^2(\mathrm{Tree}(f))$, then $\mathrm{Tree}(f_n) < \mathrm{Tree}(f)$.

Now suppose $\log^2(\mathrm{Tree}(f_n)) = \log^2(\mathrm{Tree}(f))$. Since

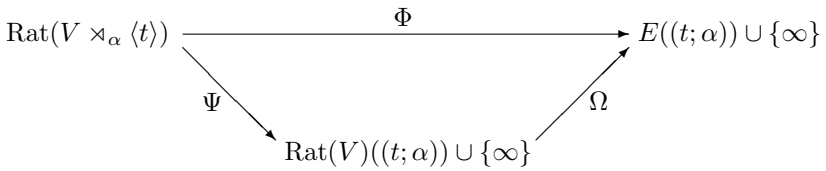
$$\max\{\log^2(\mathrm{Tree}((-1)g_m)) \mid m = N+1, \ldots, 2N+n\} < \log^2(\mathrm{Tree}(f)),$$

it follows that $\log^2(\mathrm{Tree}(g_N^*)) = \log^2(\mathrm{Tree}(f))$ and that equality holds throughout (5). Here $g = \Psi(g) = g_N$, and hence $f = \Psi(f) = f_{-N}$, as desired.

This completes the proof. □

6.4 Remark. Let V be a subgroup of $E^\times$ such that $\alpha(V) = V$ and $-1 \in V$.

We can form the group $V \rtimes_\alpha \langle t \rangle$, and, by restriction, we get a commutative diagram:



It is this version that we shall apply.

In the construction of this Ψ, V can be treated as an arbitrary multiplicative group given with an automorphism α, and a central element -1. However, Φ' is involved in the definition of the $*$-map for $\mathrm{Rat}(V)((t;\alpha)) \cup \{\infty\}$, because evaluation of the $*$-map requires the input of a value from $\mathbb{Z} \cup \{\infty\}$; that is, given f as in (4), Φ' acts as a black box that either declares f^* to be ∞, or produces the value of N to be used in defining f^*. □

7 The main result

We can now start the proof.

7.1 Theorem (Hughes[2],[3]**).** *Let G be a locally indicable group, K a division ring, and KG a crossed-product group ring. Suppose that D_1 and D_2 are Hughes-free division rings of fractions of KG. Then there is a (unique) ring isomorphism $D_1 \to D_2$ such that the induced map on KG is the identity.*

Proof. Let i denote a variable which ranges over $\{1, 2\}$.

Let $U = K^\times G$, viewed as a subgroup of $D_i^\times$.

Construct $\mathrm{Rat}(U)$ as in Definition 4.6, and construct a morphism of rational U-semirings $\Phi_i\colon \mathrm{Rat}(U) \to D_i \cup \{\infty_i\}$, as in Example 4.8(ii). Since KG rationally generates D_i, and $-1 \in U$, one can show that Φ_i is surjective.

We shall construct a map $\beta\colon D_1 \cup \{\infty_1\} \to D_2 \cup \{\infty_2\}$ such that, for every $f \in \mathrm{Rat}(U)$, β sends $\Phi_1(f)$ to $\Phi_2(f)$. We have to show that this is well defined. The key step is the following.

7.2 Lemma. *Let $f \in \mathrm{Rat}(U)$. Then $\Phi_1(f) = 0_{D_1}$ if and only if $\Phi_2(f) = 0_{D_2}$. Also, $\Phi_1(f) = \infty_1$ if and only if $\Phi_2(f) = \infty_2$.*

Proof of Lemma 7.2. We may suppose that the equivalences hold for elements of complexity less than $\mathrm{Tree}(f)$.

Let $U' = \mathrm{source}(f)$ as in Definition 5.5, so we can write $f = pu$ for some $p \in \mathrm{Rat}(U')$, $u \in U$.

Without loss of generality, in the context of the proof of the lemma, we can replace f with fu^{-1}. Thus we may assume that $u = 1$, and that $f \in \mathrm{Rat}(U')$.

Let G' denote the image of U' under the composition

$$U' \leq U = K^\times G \to (K^\times G)/(K^\times) = G,$$

so $G' \leq G$

For each subgroup H of G, let $D_i(H)$ denote the (division) subring of D_i rationally generated by the crossed-product group subring KH of KG.

Without loss of generality, in the context of the proof of the lemma, we can replace G with G', KG with KG', D_i with $D_i(G')$, and $U = K^\times G$ with $K^\times G'$, and thus assume that the map $U' \to G$ is surjective.

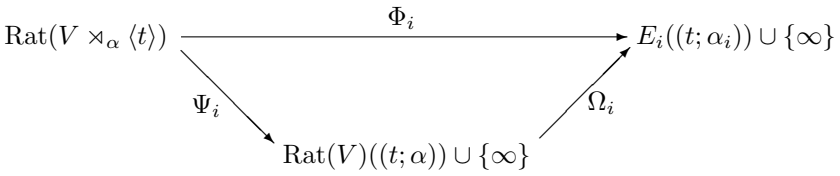
In particular, G is finitely generated, and is therefore indicable.

If $G = 1$, then $D_1 = D_2 = K$, and the equivalences hold.

Thus we may assume that G is a nontrivial indicable group, and therefore there exists an expression $G = H \rtimes C$, with C infinite cyclic. Lift a generator of C back to an element $t \in K^\times G$.

Let $E_i = D_i(H)$. Left conjugation by t induces an automorphism α_i on D_i, which acts on KH, and hence on E_i. Thus we have a ring homomorphism $E_i[t;\alpha_i] \to D_i$; the Hughes-freeness of D_i implies that this map is injective. Thus $E_i[t;\alpha_i]$ embeds in D_i, and rationally generates D_i. Hence, D_i is the unique division ring of fractions $E_i(t;\alpha_i)$ of $E_i[t;\alpha_i]$. Thus D_i is embedded in $E_i((t;\alpha_i))$.

Let $V = K^\times H$. Then $\alpha(V) = V$, and we can write $U = V \rtimes_\alpha \langle t \rangle$, and $-1 \in V$; by Definition 6.2(v) and Remark 6.4, we have a commutative diagram:



We now return to the last paragraph of Remark 6.4. Recall that f is constructed in stages in $\mathrm{Rat}(U)$, using U, addition, multiplication and the $*$-map, and at all non-final stages of the construction, the complexity is less than $\mathrm{Tree}(f)$. All coefficients in $\mathrm{Rat}(V)$ of the non-final stages of the corresponding construction of $\Psi_i(f)$ will then also have complexity less than $\mathrm{Tree}(f)$, by Theorem 6.3. In the construction of $\Psi_i(f)$, each evaluation of the $*$-map requires the input of a value from $\mathbb{Z} \cup \{\infty\}$, but the value will be the same for $i = 1$ and for $i = 2$, by the transfinite induction hypothesis. Hence, the constructions of $\Psi_1(f)$ and $\Psi_2(f)$ are identical, and $\Psi_1(f) = \Psi_2(f)$. We may assume

$$\infty \neq \Psi_1(f) = \Psi_2(f) = \sum_{n \in \mathbb{Z}} f_n.$$

We claim that $f \notin \mathrm{Rat}(V)\langle t \rangle$. Suppose not, so that

$$f \in \mathrm{Rat}(V)\langle t \rangle \subseteq \mathrm{Rat}(V)U.$$

Then, by Theorem 5.7, $\mathrm{source}(f) \leq V$, that is, $U' \leq K^\times H$. Passing to $K^\times G/K^\times$ $(= G)$, we see that $G \leq H$, a contradiction. This proves the claim, and now, by Theorem 6.3, $\mathrm{Tree}(f_n) < \mathrm{Tree}(f)$ for all $n \in \mathbb{Z}$.

Hence, by the transfinite induction hypothesis, for each $n \in \mathbb{Z}$, $\Phi'_1(f_n) = 0_{D_1}$ if and only if $\Phi'_2(f_n) = 0_{D_2}$, and $\Phi'_1(f_n) = \infty_1$ if and only if $\Phi'_2(f_n) = \infty_2$.

Now $\Phi_i(f) = \Omega_i(\Psi_i(f)) = \Omega_i(\sum_{n \in \mathbb{Z}} f_n)$. It follows that $\Phi_i(f) = 0_{D_i}$ if and only if $\Phi'_i(f_n) = 0_{D_i}$ for all $n \in \mathbb{Z}$. Also, $\Phi_i(f) = \infty_i$ if and only if $\Phi'_i(f_n) = \infty_i$ for some $n \in \mathbb{Z}$.

Thus, $\Phi_1(f)$ is 0_{D_1}, resp. ∞_1, if and only if $\Phi_2(f)$ is 0_{D_2}, resp. ∞_2, and we have proved Lemma 7.2. □

We can now conclude the proof of Theorem 7.1.

Suppose $f, f' \in \mathrm{Rat}(U)$ are such that $\Phi_1(f) = \Phi_1(f') \neq \infty_1$. Then $\Phi_1(f + (-1)f') = \Phi_1(f) + (-1)\Phi_1(f') = 0_{D_1}$. By Lemma 7.2, $\Phi_2(f) \neq \infty_2$, $\Phi_2(f') \neq \infty_2$, and $\Phi_2(f + (-1)f') = 0_{D_2}$. Hence,

$$\Phi_2(f) + (-1)\Phi_2(f') = 0_{D_2},$$

and $\Phi_2(f) = \Phi_2(f')$. Thus, β is well defined, as desired.

By symmetry, we have a bijective correspondence between $D_1 \cup \{\infty_1\}$ and $D_2 \cup \{\infty_2\}$ in which, for every $f \in \mathrm{Rat}(U)$, $\Phi_1(f)$ corresponds to $\Phi_2(f)$. It follows that $D_1 \cup \{\infty_1\}$ and $D_2 \cup \{\infty_2\}$ are isomorphic rational $K^\times G$-semirings, and hence that D_1 and D_2 are isomorphic division rings of fractions of KG. □

7.3 Corollary. *Let G be a locally indicable group, K a division ring, KG a crossed-product group ring, and D a Hughes-free division ring of fractions of KG. Let $\mathrm{Aut}(KG, K)$ denote the group consisting of those ring automorphisms of KG which induce automorphisms on K. Then there is a natural injective group homomorphism*

$$\mathrm{Aut}(KG, K) \hookrightarrow \mathrm{Aut}(D).$$

Proof. Suppose that $\alpha \in \mathrm{Aut}(KG, K)$.

The group of units of KG is precisely $K^\times G$, by a result of Higman's which we mentioned in Section 1. In fact, Higman's elegant argument is embedded in the proof of Lemma 7.2.

Since α permutes the units of KG, we have $\alpha(K^\times G) = K^\times G$. By hypothesis, $\alpha(K^\times) = K^\times$, so α induces an automorphism on the quotient $(K^\times G)/K^\times = G$.

The composition $KG \to KG \subseteq D$ gives a new division ring of fractions of KG by pullback along α. Using the above information, it is not difficult to show that the new division ring of fractions of KG is again Hughes-free. By Theorem 7.1, there exists a unique isomorphism $\alpha' \colon D \to D$ such that the induced map on KG is α.

Now the map $\mathrm{Aut}(KG, K) \to \mathrm{Aut}(D)$, $\alpha \mapsto \alpha'$, is easily seen to be an injective group homomorphism. □

Acknowledgments

We are grateful to Jacques Lewin and Peter Linnell for encouraging us to elucidate Hughes' proof.

We thank Penny Roberts of the Document Supply Department of the Radcliffe Science Library, Oxford University, for efficiently providing us with a copy of Hughes' DPhil thesis. We also thank Ian Hughes, who does not have a copy of his own thesis, for kindly directing us to the Science Library.

The research of the first-named author was partially supported by the DGI (Spain) through Project BFM2000-0354.

The research of the second- and third-named authors was partially supported by the DGESIC (Spain) through Project PB1998-0873, by the DGI and the European Regional Development Fund, jointly, through Project BFM2002-01390, and by the Comissionat per Universitats i Recerca of the Generalitat de Catalunya.

References

[1] Higman, G. The units of group-rings. Proc. London Math. Soc. (2) **1940**, *46*, 231–248.

[2] Hughes, I. P. *The embedding of group-rings in division rings*; DPhil Thesis, Oxford University, 1961; iv+92 pages.

[3] Hughes, I. Division rings of fractions for group rings. Comm. Pure Appl. Math. **1970**, *23*, 181–188.

[4] Lewin, J. Fields of fractions for groups algebras of free groups. Trans. Amer. Math. Soc. **1974**, *192*, 339–346.

[5] Linnell, P. A. Division rings and group von Neumann algebras. Forum Math. **1993**, *5* (6), 561–576.

[6] Linnell, P. A. A rationality criterion for unbounded operators. J. Funct. Anal. **2000**, *171* (1), 115–123.