LÜROTH'S AND IGUSA'S THEOREMS OVER DIVISION RINGS

FRANÇOIS LEGRAND AND ELAD PARAN

ABSTRACT. Let H be a division ring of finite dimension over its center, let $H[T]$ be the ring of polynomials in a central variable over H, and let $H(T)$ be its quotient skew field. We show that every intermediate division ring between H and $H(T)$ is itself of the form $H(f)$, for some f in the center of $H(T)$. This generalizes the classical Lüroth's theorem. More generally, we extend Igusa's theorem characterizing the transcendence degree 1 subfields of rational function fields, from fields to division rings.

1. INTRODUCTION

Let K be an arbitrary field and let $K(X)$ be the field of rational functions over K. Lüroth's theorem states that every intermediate field $K \subset F \subseteq K(X)$ is itself a rational function field over K. The theorem was first proven for $K = \mathbb{C}$ by Lüroth in [18], and for a general field K by Steinitz in [23]. This result is foundational for general field theory and for the theory of algebraic curves, see [22, §1.3]. The theorem was generalized to transcendence degree 1 subfields of rational function fields in any number of variables by Gordan in [8] for fields of characteristic 0, and in general by Igusa in [10]. Over the years, various proofs, employing different approaches, have been given to these results, e.g., in [3, p. 106], [21], [11], [19].

In the present work, we study Lüroth's and Igusa's theorems in the more general context of division rings.

Let H be a division ring (a.k.a. a skew field, or a division algebra over its center field), and let $H[T]$ be the ring of polynomials over H in a central variable T. The ring $H[T]$ is an Ore domain, hence admits a unique quotient skew field $H(T)$. The arithmetic of the ring $H[T]$ (and more generally, of skew polynomial rings) is well-studied (see the classical works [20], [9], and the modern works of Lam and Leroy [13], [14], [15], [16], [17], for example), however the study of the quotient skew field $H(T)$ is not as expansive. Our main result is the following one, whose first part generalizes Lüroth's theorem, and its second part generalizes Igusa's theorem.

Theorem 1.1. *Let H be a division ring of finite dimension over its center $Z(H)$, let n be a positive integer and let $H \subseteq L \subseteq H(T_1, \ldots, T_n)$ be an intermediate division ring.*
(1) Assume $n = 1$ and $L \neq H$. Then there exists $f \in Z(H)(T_1) \setminus Z(H)$ such that $L = H(f)$.
(2) Assume there is $g \in Z(H)(T_1, \ldots, T_n)$ such that $L/H(g)$ is algebraic and such that g is not algebraic over H. Then there exists $f \in Z(H)(T_1, \ldots, T_n) \setminus Z(H)$ such that $L = H(f)$.

Here $T_1, \ldots, T_n$ denote independent central variables and $H(f)$ denotes the division ring generated by f over H inside $H(T_1, \ldots, T_n)$ – the terminology and notations are reviewed in detail in §2.

In order to prove the theorem, we first prove several claims concerning extensions of division rings, that eventually allow us to deduce the theorem from the classical, commutative version of it. This is done in §3.

After concluding the proof of Theorem 1.1, we turn out attention to the more general skew polynomial ring $H[T, \sigma]$, where σ is an automorphism of the division ring H. In the present context, it is natural to ask whether a version of Lüroth's theorem holds for the quotient skew field $H(T, \sigma)$ of $H[T, \sigma]$. In the case where σ is an inner automorphism, we observe that such a

---

version immediately follows from our main result, see Remark 3.5. However, the case where σ is an arbitrary automorphism seems more difficult, even in the simplest case where H itself is a field and σ is of order 2. In §4, we consider the skew polynomial ring $\mathbb{C}[T, \sigma]$, where σ is the complex conjugation, and its quotient skew field $\mathbb{C}(T, \sigma)$, and study the intermediate division rings between $\mathbb{C}$ and $\mathbb{C}(T, \sigma)$. We prove that any intermediate division ring $\mathbb{C} \subseteq D \subseteq \mathbb{C}(T, \sigma)$ is of the form $\mathbb{C}(f)$, provided that D is σ-invariant, see Definition 4.2 and Theorem 4.4. However, we observe that σ-invariance is only a sufficient condition for D to be of this form, not a necessary one, see Proposition 4.6. It remains an open question whether Lüroth's theorem holds unconditionally for $\mathbb{C}(T, \sigma)$, and more generally for skew fields of the form $H(T, \sigma)$, see also Example 4.8. Another open question is whether Theorem 1.1 holds for division rings of infinite dimension over their center.

2. Preliminaries

In this section, we collect the basic material on division rings which will be used in the sequel.

A *division ring* is a (unital, associative) ring H in which every non-zero element is invertible. Given a non-zero element b of a division ring H, the conjugation by b in H is an *inner* automorphism of H, denoted by $I_H(b)$, and we let $\mathrm{Inn}(H)$ denote the group of all inner automorphisms of H.

For the next three items, we fix an extension L/H of division rings (i.e., $H \subseteq L$).

• The *degree* $[L : H]$ of L/H is the dimension of the (left) H-linear space L and L/H is *finite* if $[L : H] < \infty$. We also say that H is *centrally finite* if H is a finite extension of its center $Z(H)$.

• Given a subset S of L, we let $H(S)$ denote the intersection of all division rings contained in L and which contain both H and S, and we simply write $H(x)$ if $S = \{x\}$. We then say that an element x of L is *algebraic* over H if $H(x)/H$ is finite and that L/H is *algebraic* if every element of L is algebraic over H.

• Letting $\mathrm{Aut}(L/H)$ denote the group of all automorphisms of L fixing H point-wise, we say that L/H is *outer* if $\mathrm{Inn}(L) \cap \mathrm{Aut}(L/H) = \{\mathrm{id}_L\}$. Equivalently, if $C_L(H)$ denotes the *centralizer* of H in L, i.e., $C_L(H) = \{x \in L : xy = yx \ (y \in H)\}$, then L/H is outer if and only if $C_L(H)$ equals the center $Z(L)$ of L. In particular, if L/H is outer, then $Z(H) \subseteq Z(L)$.

Lemma 2.1. *Let L/H be an outer extension of division rings.*
(1) The extensions L/F and F/H are outer for every intermediate division ring $H \subseteq F \subseteq L$.
(2) Assume H is centrally finite and L/H is algebraic. Then $Z(L)/Z(H)$ is algebraic.

Proof. (1) First, if $I_L(a)$ $(a \in L \setminus \{0\})$ is in $\mathrm{Aut}(L/F)$, then $I_L(a) \in \mathrm{Aut}(L/H)$. As L/H is outer, we get $I_L(a) = \mathrm{id}_L$. Next, fix $a \in F \setminus \{0\}$ such that $I_F(a) \in \mathrm{Aut}(F/H)$. Then $I_L(a) \in \mathrm{Aut}(L/H)$ and, as L/H is outer, we get that $I_L(a) = \mathrm{id}_L$. In particular, $I_F(a) = \mathrm{id}_F$.
(2) Fix $x \in Z(L)$. As L/H is algebraic, x is in some intermediate division ring $H \subseteq F \subseteq L$ with F/H finite. Then, as H is centrally finite, $F/Z(H)$ is finite. Thus $F \cap Z(L)$ is a division ring which contains $Z(H)$ and x, which is contained in $Z(L)$ and which is a finite extension of $Z(H)$. $\square$

Lemma 2.2. *Let $H \subseteq L$ be division rings with L centrally finite. Then H is centrally finite.*

Comments on proof. The statement is well-known to experts but the authors could not find an explicit reference for it in the literature. For the sake of completeness, we provide a proof of the lemma in §A. $\square$

A non-zero ring R with no zero divisor is a *right Ore domain* if, for any $x, y \in R \setminus \{0\}$, there exist $r, s \in R \setminus \{0\}$ with $xr = ys$. If R is a right Ore domain, there is a division ring H which contains R and every element of which can be written as ab^{-1} with $a \in R$ and $b \in R \setminus \{0\}$ (see, e.g., [7, Theorem 6.8]). Moreover, H is unique up to isomorphism (see, e.g., [4, Proposition 1.3.4]).

Given a ring H and an automorphism σ of H, the polynomial ring $H[T, \sigma]$ is the ring of all polynomials of the form $a_0 + a_1 T + \cdots + a_n T^n$ with $n \geq 0$ and $a_0, \ldots, a_n \in H$, whose addition is defined component-wise and whose multiplication is given by the usual rule

$$\left(\sum_{i=0}^{n} a_i T^i \right) \cdot \left(\sum_{j=0}^{m} b_j T^j \right) = \sum_{k=0}^{n+m} \left(\sum_{\ell=0}^{k} a_\ell \sigma^\ell(b_{k-\ell}) \right) T^k.$$

In the sense of Ore (see [20]), the ring $H[T, \sigma]$ is the polynomial ring $H[T, \sigma, \delta]$ in the variable T, where the σ-derivation δ is the zero derivation.

For the rest of this section, we fix a division ring H. Then $H[T, \sigma]$ has no zero divisors, as the degree is additive on products. Moreover, $H[T, \sigma]$ is a right Ore domain (see, e.g., [7, Theorem 2.6 and Corollary 6.7]). The unique division ring which contains $H[T, \sigma]$ and each element of which can be written as ab^{-1} with $a \in H[T, \sigma]$ and $b \in H[T, \sigma] \setminus \{0\}$ is then denoted by $H(T, \sigma)$.

If $\sigma = \mathrm{id}_H$, we write $H[T]$ and $H(T)$ for simplicity, and the variable T is a central element of $H(T)$. One can iteratively construct polynomial rings in several central variables over H, by putting $H[T_1, T_2] = H[T_1][T_2]$, $H[T_1, T_2, T_3] = H[T_1, T_2][T_3]$, and so on. As the variables are central, the order in which they are added does not change the ring obtained. Furthermore, by an easy induction, the ring $H[T_1, \ldots, T_n]$ in n central variables over H is a right Ore domain for every $n \geq 1$. The unique division ring which contains $H[T_1, \ldots, T_n]$ and each element of which can be written as ab^{-1} with $a \in H[T_1, \ldots, T_n]$ and $b \in H[T_1, \ldots, T_n] \setminus \{0\}$ is then denoted by $H(T_1, \ldots, T_n)$. In the sequel, we will constantly use the equalities $H(T_1, \ldots, T_n, T_{n+1}) = H(T_1, \ldots, T_n)(T_{n+1})$ and $Z(H(T_1, \ldots, T_n)) = Z(H)(T_1, \ldots, T_n)$, and that $H(T_1, \ldots, T_n)$ is centrally finite if H is ($n \geq 1$). See, e.g., [1, Propositions 2 and 3] for more details.

We also consider the division ring $H((T))$ of Laurent series of the form $\sum_{i \geq i_0} a_i T^i$, where $i_0 \in \mathbb{Z}$ and $a_i \in H$ for $i \geq i_0$, whose addition and multiplication are defined component-wise and by

$$\left(\sum_{i \geq i_0} a_i T^i \right) \left(\sum_{i \geq i_1} b_i T^i \right) = \sum_{i \geq i_0 + i_1} \left(\sum_{\ell=0}^{i - i_0 - i_1} a_{i_0 + \ell} \, b_{i - i_0 - \ell} \right) T^i,$$

respectively. Since $H[T]$ is a right Ore domain contained in $H((T))$, we have $H(T) \subseteq H((T))$. See, e.g., [4, §2.3] for more details on division rings of Laurent series.

3. PROOF OF THEOREM 1.1

To prove Theorem 1.1, we will require the next four lemmas. The first one characterizes finite outer extensions of centrally finite division rings.

Lemma 3.1. *Let H be a centrally finite division ring and L a finite extension of H with $Z(H) \subseteq Z(L)$. The next three conditions are equivalent:*
(i) *the unique $Z(H)$-linear map $\psi : H \otimes_{Z(H)} Z(L) \to L$ which fulfills $\psi(x \otimes y) = xy$ for every $(x, y) \in H \times Z(L)$ is an isomorphism of $Z(H)$-algebras,*
(ii) *L/H is outer,*
(iii) *$[Z(L) : Z(H)] = [L : H]$.*

Proof. First, as the map

$$\begin{cases} H \times Z(L) & \to & L \\ (x, y) & \mapsto & xy \end{cases}$$

3

is $Z(H)$-bilinear, ψ is well-defined, and it is a morphism of $Z(H)$-algebras. Moreover, ψ is injective (see, e.g., [12, Proposition 2.36]). Furthermore, as

$$\dim_H(\mathrm{Im}(\psi)) \times [H : Z(H)] = \dim_{Z(L)}(\mathrm{Im}(\psi)) \times [Z(L) : Z(H)]$$

and as the left-hand side is finite, $[Z(L) : Z(H)]$ is also finite and hence $\dim_H(\mathrm{Im}(\psi)) = [Z(L) : Z(H)]$. Then (i) $\Leftrightarrow$ (iii) is clear. Next, the centralizer of $\mathrm{Im}(\psi)$ in L is the centralizer $C_L(H)$ of H in L. As L is centrally finite, the *double centralizer theorem* (see, e.g., [12, Theorem 2.43]) then yields $[L : Z(L)] = [C_L(H) : Z(L)] \times \dim_{Z(L)}(\mathrm{Im}(\psi))$. Hence, (i) $\Leftrightarrow$ (ii), as needed. $\qquad\square$

Our second lemma is a variant of the first one.

Lemma 3.2. *Let L/H be an outer extension of division rings such that L is centrally finite. Then the unique $Z(H)$-linear map $\psi : H \otimes_{Z(H)} Z(L) \to L$ which fulfills $\psi(x \otimes y) = xy$ for every $(x, y) \in H \times Z(L)$ is an isomorphism of $Z(H)$-algebras.*

Proof. First, $Z(H) \subseteq Z(L)$ as L/H is outer. Then, as in the proof of Lemma 3.1, the map ψ is a well-defined monomorphism of $Z(H)$-algebras. Moreover, as L is centrally finite, H is centrally finite, by Lemma 2.2. Furthermore, $\mathrm{Im}(\psi)$ is a ring with no zero divisors and a $Z(L)$-linear space with finite dimension $[H : Z(H)]$. Hence, $\mathrm{Im}(\psi)$ is a division ring (see, e.g., [4, Proposition 3.1.2]), whose center equals $Z(L)$. Using that $L/Z(L)$ is finite, we get that $L/\mathrm{Im}(\psi)$ is finite and that $\mathrm{Im}(\psi)$ is centrally finite. Moreover, since L/H is outer and since $\mathrm{Im}(\psi)$ is an intermediate division ring, $L/\mathrm{Im}(\psi)$ is outer, by Lemma 2.1(1). Thus, $L = \mathrm{Im}(\psi)$ by Lemma 3.1. $\qquad\square$

Our third lemma shows that every extension of the form $H(T_1, \ldots, T_n)/H$ is outer.

Lemma 3.3. (1) *Let L/H be an outer extension of division rings. Then $L((T))/H$ is outer.*
(2) *The extension $H(T_1, \ldots, T_n)/H$ is outer for every $n \geq 1$.*

Proof. (1) Let $a \in L((T))$ be such that $ac = ca$ for every $c \in H$. Set $a = \sum_{i \geq i_0} a_i T^i$, where $i_0 \in \mathbb{Z}$ and $a_i \in L$ for every $i \geq i_0$. As $ac = ca$ for every $c \in H$, we have $ca_i = a_i c$ for every $c \in H$, i.e., every a_i lies in the centralizer $C_L(H)$ of H in L. As the extension L/H is outer, we actually have $C_L(H) = Z(L)$ and hence $a \in Z(L)((T)) \subseteq Z(L((T)))$, as needed.
(2) We proceed by induction on $n \geq 1$. For $n = 1$, we get from (1) that $H((T_1))/H$ is outer. As $H(T_1)$ is an intermediate division ring, Lemma 2.1(1) yields that $H(T_1)/H$ is outer. Now, fix $n \geq 1$ and assume $H(T_1, \ldots, T_n)/H$ is outer. We may then use (1) to get that $H(T_1, \ldots, T_n)((T_{n+1}))/H$ is outer. Since $H(T_1, \ldots, T_n)(T_{n+1})$ is an intermediate division ring which equals $H(T_1, \ldots, T_{n+1})$, Lemma 2.1(1) yields that $H(T_1, \ldots, T_{n+1})/H$ is outer, thus ending the proof. $\qquad\square$

Our last lemma describes the division ring generated by a central element of $H(T_1, \ldots, T_n)$, if H is centrally finite.

Lemma 3.4. *Let H be a centrally finite division ring, $n \geq 1$ and $f \in Z(H)(T_1, \ldots, T_n)$. Then the unique $Z(H)$-linear map $\psi : H \otimes_{Z(H)} Z(H)(f) \to H(f)$ which fulfills $\psi(x \otimes y) = xy$ for every $(x, y) \in H \times Z(H)(f)$ is an isomorphism of $Z(H)$-algebras. In particular, $Z(H(f)) = Z(H)(f)$.*

Proof. First, by Lemma 2.1(1) and Lemma 3.3(2), the extension $H(f)/H$ is outer. In particular, $Z(H) \subseteq Z(H(f))$. Moreover, as $f \in Z(H)(T_1, \ldots, T_n)$, we have $f \in Z(H(f))$ and hence the inclusions $Z(H) \subseteq Z(H)(f) \subseteq Z(H(f))$ hold.

Now, as in the proof of Lemma 3.1, the map ψ is well-defined and injective. Moreover, as $Z(H)(f) \subseteq Z(H(f))$, it is a morphism of $Z(H)$-algebras. Furthermore, $\mathrm{Im}(\psi)$ is both a ring with no zero divisors and a $Z(H)(f)$-linear space with finite dimension $[H : Z(H)]$. Hence, $\mathrm{Im}(\psi)$ is a division ring, which is contained in $H(T_1, \ldots, T_n)$ and which contains H and f. Therefore, $H(f) = \mathrm{Im}(\psi)$, thus ending the proof. $\qquad\square$

Proof of Theorem 1.1. We prove each statement separately, by reducing to the commutative case.

(1) First, by Lemma 2.1(1) and 3.3(2), the extensions $H(T_1)/L$ and L/H are outer and, hence, $Z(H) \subseteq Z(L) \subseteq Z(H)(T_1)$. We may then consider the unique $Z(H)$-linear map $\psi : H \otimes_{Z(H)} Z(L) \to L$ which fulfills $\psi(x \otimes y) = xy$ for every $(x, y) \in H \times Z(L)$. Moreover, since $H(T_1)$ is centrally finite, L is centrally finite by Lemma 2.2. We may then apply Lemma 3.2 to get

$$L = \mathrm{Im}(\psi). \tag{3.1}$$

Next, assume $Z(L) = Z(H)$. Then $\mathrm{Im}(\psi) = H$, i.e., $L = H$ by (3.1), which cannot hold. Finally, by Lüroth's theorem and as $Z(L) \neq Z(H)$, there is $f \in Z(H)(T_1) \setminus Z(H)$ such that $Z(L) = Z(H)(f)$. Hence, by Lemma 3.4, we get $\mathrm{Im}(\psi) = H(f)$, i.e., $L = H(f)$ by (3.1).

(2) First, by Lemma 2.1(1) and 3.3(2), the extensions $H(T_1, \ldots, T_n)$ and L/H are outer and, hence, $Z(H) \subseteq Z(L) \subseteq Z(H)(T_1, \ldots, T_n)$. We may then consider the unique $Z(H)$-linear map $\psi : H \otimes_{Z(H)} Z(L) \to L$ which fulfills $\psi(x \otimes y) = xy$ for every $(x, y) \in H \times Z(L)$. Moreover, as $H(T_1, \ldots, T_n)$ is centrally finite, L is centrally finite (see Lemma 2.2). Lemma 3.2 then yields

$$L = \mathrm{Im}(\psi). \tag{3.2}$$

Moreover, $H(g)$ is centrally finite (again by Lemma 2.2) and, by Lemma 2.1(2), the extension $Z(L)$ of $Z(H(g)) = Z(H)(g)$ (see Lemma 3.4 for the last equality) is algebraic. Furthermore, if g is algebraic over $Z(H)$, then $Z(H)(g)/Z(H)$ is finite. As $H(g)$ is centrally finite, we get that $H(g)/H$ is finite, which cannot hold. Hence, $Z(L)/Z(H)$ has transcendence degree 1. We may then apply Igusa's generalization of Lüroth's theorem to get that there is $f \in Z(H)(T_1, \ldots, T_n) \setminus Z(H)$ with $Z(L) = Z(H)(f)$. Hence, by Lemma 3.4, we get $\mathrm{Im}(\psi) = H(f)$, i.e., $L = H(f)$ by (3.2). $\square$

Remark 3.5. Given a division ring H and $\sigma \in \mathrm{Inn}(H)$, say $\sigma = I_H(b)$ with $b \in H \setminus \{0\}$, we let $H[b^{-1}T]$ denote the intersection of all subrings of $H[T, \sigma]$ containing H and $b^{-1}T$. Then

$$H[b^{-1}T] = \{a_0 + a_1(b^{-1}T) + \cdots + a_n(b^{-1}T)^n : n \geq 0, a_0, \ldots, a_n \in H\} = H[T, \sigma] \tag{3.3}$$

and, as the $(b^{-1}T)^n$'s $(n \geq 0)$ are linearly independent over H, the ring $H[b^{-1}T]$ is the polynomial ring in the central variable $b^{-1}T$ over H. As $H(T, \sigma) = H(b^{-1}T)$ by (3.3), we get the next extension of Theorem 1.1:

Let H be a centrally finite division ring and let n be a positive integer. Fix $\sigma_1 \in \mathrm{Inn}(H)$ and, for every $i \in \{2, \ldots, n\}$, fix $\sigma_i \in \mathrm{Inn}(H(T_1, \sigma_1) \cdots (T_{i-1}, \sigma_{i-1}))$. Let $H \subseteq L \subseteq H(T_1, \sigma_1) \cdots (T_n, \sigma_n)$ be an intermediate division ring.

(1) Assume $n = 1$ and $L \neq H$. Then there is $f \in Z(H(T_1, \sigma_1)) \setminus Z(H)$ such that $L = H(f)$.

(2) Assume there is $g \in Z(H(T_1, \sigma_1) \cdots (T_n, \sigma_n))$ such that $L/H(g)$ is algebraic and such that g is not algebraic over H. Then there is $f \in Z(H(T_1, \sigma_1) \cdots (T_n, \sigma_n)) \setminus Z(H)$ such that $L = H(f)$.

4. THE CASE OF $\mathbb{C}(T, \sigma)$

In this section, we consider the division ring $\mathbb{C}(T, \sigma)$, where σ denotes the complex conjugation. Let $\mathbb{H}$ denote Hamilton's quaternions algebra, i.e., $\mathbb{H} = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$ where $i^2 = j^2 = k^2 = ijk = -1$. From now on, we view $\mathbb{C}$ as the subring $\mathbb{R} \oplus \mathbb{R}i$ of $\mathbb{H}$.

Lemma 4.1. *Consider the map*

$$\phi : \begin{cases} \mathbb{C}[T, \sigma] & \longrightarrow & \mathbb{H}[X] \\ a_0 + a_1T + \cdots + a_nT^n & \longmapsto & a_0 + a_1jX + \cdots + a_nj^nX^n \end{cases}.$$

Then ϕ is a ring homomorphism, which is injective and which fixes $\mathbb{C}$ point-wise.

Proof. Clearly, ϕ fixes $\mathbb{C}$ point-wise and ϕ is both additive and injective. Hence, to conclude the proof, it suffices to check that ϕ is multiplicative on monomials. To that end, consider two monomials aT^n and bT^m, with $n, m \in \mathbb{N}$ and $a, b \in \mathbb{C}$. By the definition of ϕ, we have

$$\phi(aT^n bT^m) = \phi(a\sigma^n(b)T^{n+m}) = a\sigma^n(b)j^{n+m}X^{n+m}. \tag{4.1}$$

By considering the four different possible residues of n modulo 4, one checks that $\sigma^n(b)j^n = j^n b$ for all $n \geq 0$. Thus, (4.1) yields $\phi(aT^n bT^m) = aj^n bj^m X^{n+m} = aj^n X^n bj^m X^m = \phi(aT^n)\phi(bT^m)$, as needed. $\qquad\square$

By, e.g., [7, Proposition 6.3] and since $\mathbb{C}[T, \sigma]$ is a right Ore domain, the monomorphism ϕ from Lemma 4.1 extends to the following monomorphism:

$$\phi : \begin{cases} \mathbb{C}(T, \sigma) & \to & \mathbb{H}(X) \\ PQ^{-1} & \mapsto & \phi(P)\phi(Q)^{-1} \end{cases}.$$

Now, we extend σ to $\mathbb{H}$ by setting

$$\sigma(a + bi + cj + dk) = a - bi + cj - dk$$

for $a, b, c, d \in \mathbb{R}$. Then σ is an automorphism of $\mathbb{H}$ of order 2. Moreover, we may extend σ to an automorphism of order 2 of $\mathbb{H}[X]$, by setting

$$\sigma(a_0 + a_1 X + \cdots + a_n X^n) = \sigma(a_0) + \sigma(a_1)X + \cdots + \sigma(a_n)X^n$$

for $n \geq 0$ and $a_0, \ldots, a_n \in \mathbb{H}$. Finally, σ extends to the next automorphism of order 2 of $\mathbb{H}(X)$:

$$\sigma : \begin{cases} \mathbb{H}(X) & \to & \mathbb{H}(X) \\ PQ^{-1} & \mapsto & \sigma(P)\sigma(Q)^{-1} \end{cases}.$$

Definition 4.2. We say that a subset S of $\mathbb{H}(X)$ is *σ-invariant* if $\sigma(S) = S$.

Example 4.3. Given a subset S of $\mathbb{C}(T, \sigma)$, we have $\phi(\mathbb{C}(S)) = \mathbb{C}(\phi(S))$ and, if $\phi(S)$ is σ-invariant, so is $\phi(\mathbb{C}(S))$. Using that $\sigma(i) = -i$ and that σ fixes $\phi(\mathbb{R}(T))$ point-wise, we have, in particular, that $\phi(\mathbb{C}(S))$ is σ-invariant for every subset S of $\mathbb{C}(T, \sigma)$ which is contained in $\mathbb{R}(T) \cup i\mathbb{R}(T)$.

The next result, which is a partial Lüroth's theorem over $\mathbb{C}(T, \sigma)$, is the aim of this section:

Theorem 4.4. *Let $\mathbb{C} \subseteq L \subseteq \mathbb{C}(T, \sigma)$ be an intermediate division ring such that $\phi(L)$ is σ-invariant. Then there is $v \in \mathbb{C}(T, \sigma)$ such that $L = \mathbb{C}(v)$.*

The key idea for proving Theorem 4.4 is to apply Theorem 1.1 to a suitable extension of L inside $\mathbb{H}(X)$. We will first need the following lemma:

Lemma 4.5. (1) *For every $f \in \mathbb{C}(T, \sigma)$, we have $j\phi(f) = \sigma(\phi(f))j$.*
(2) *We have $j \notin \phi(\mathbb{C}(T, \sigma))$. In particular, the $\phi(L)$-linear space $\phi(L) + \phi(L)j$ has dimension 2 for every division ring L contained in $\mathbb{C}(T, \sigma)$.*
(3) *Let L be a division ring contained in $\mathbb{C}(T, \sigma)$ such that $\phi(L)$ is σ-invariant. Then $\phi(L) + \phi(L)j$ is a division ring.*
(4) *For $i \in \{1, 2\}$, fix a division ring L_i contained in $\mathbb{C}(T, \sigma)$. Assume $\phi(L_1) \subseteq \phi(L_2)$ and $\phi(L_2) + \phi(L_2)j \subseteq \phi(L_1) + \phi(L_1)j$. Then $L_1 = L_2$.*

Proof of Lemma 4.5. (1) By additivity and the definition of ϕ, it suffices to consider the case where f is a monomial aT^n ($n \in \mathbb{N}$, $a \in \mathbb{C}$). As $j\phi(f) = jaj^n X^n$ and $\sigma(\phi(f))j = \sigma(aj^n)X^n j = \sigma(a)j^n X^n j = \sigma(a)j^{n+1}X^n$, it suffices to check that $ja = \sigma(a)j$, which was already mentioned in the proof of Lemma 4.1.
(2) If $j \in \phi(\mathbb{C}(T, \sigma))$, there are non-negative integers n, m and elements $a_0, \ldots, a_n, b_0, \ldots, b_m$ of $\mathbb{C}$ such that $b_0 + b_1 jX + \cdots + b_m j^m X^m \neq 0$ and such that

$$a_0 + a_1 jX + \cdots + a_n j^n X^n = j(b_0 + b_1 jX + \cdots + b_m j^m X^m).$$

6

Therefore, $a_\ell = jb_\ell$ for $0 \le \ell \le n = m$, i.e., every coefficient b_ℓ equals 0, which cannot hold.

(3) Fix $a, b, c, d \in L$. By (1), we have

$$(\phi(a) + \phi(b)j)(\phi(c) + \phi(d)j) = (\phi(a)\phi(c) - \phi(b)\sigma(\phi(d))) + (\phi(a)\phi(d) + \phi(b)\sigma(\phi(c)))j.$$

As we assumed that $\phi(L)$ is σ-invariant, $\phi(a)\phi(c) - \phi(b)\sigma(\phi(d))$ and $\phi(a)\phi(d) + \phi(b)\sigma(\phi(c))$ are in $\phi(L)$. Hence, $\phi(L) + \phi(L)j$ is a ring, which has no zero divisors. As $\phi(L) + \phi(L)j$ is also a finite dimensional $\phi(L)$-linear space, it is in fact a division ring (see, e.g., [4, Proposition 3.1.2]).

(4) By (2), we have

$$
\begin{aligned}
2 &= \dim_{\phi(L_1)} \phi(L_1) + \phi(L_1)j &&\ge \dim_{\phi(L_1)} \phi(L_2) + \phi(L_2)j \\
&&&= [\phi(L_2) : \phi(L_1)] \cdot \dim_{\phi(L_2)} \phi(L_2) + \phi(L_2)j \\
&&&= 2[\phi(L_2) : \phi(L_1)].
\end{aligned}
$$

Hence, $\phi(L_1) = \phi(L_2)$, i.e., $L_1 = L_2$. $\qquad\square$

Proof of Theorem 4.4. First, let us introduce the following map:

$$\tau : \begin{cases} \mathbb{H} & \longrightarrow & \mathbb{H} \\ a + bi + cj + dk & \longmapsto & a + bi - cj - dk \end{cases} .$$

Then τ is an automorphism of H of order 2. We may extend τ to an automorphism of $\mathbb{H}[X]$ of order 2, by setting

$$\tau(a_0 + a_1 X + \cdots + a_n X^n) = \tau(a_0) - \tau(a_1)X + \cdots + (-1)^n \tau(a_n)X^n \quad (n \ge 0, a_0, \ldots, a_n \in \mathbb{H}).$$

As $\mathbb{H}[X]$ is a right Ore domain, we may extend τ to an automorphism of $\mathbb{H}(X)$ of order 2, by setting

$$\tau(PQ^{-1}) = \tau(P)\tau(Q)^{-1} \quad (P \in \mathbb{H}[X], Q \in \mathbb{H}[X] \setminus \{0\}).$$

Now, consider the $\phi(L)$-linear space $\phi(L) + \phi(L)j$. Since τ fixes $\phi(\mathbb{C}(T, \sigma))$ point-wise and $\tau(j) = -j$, we have $\tau(\phi(a) + \phi(b)j) = \phi(a) + \phi(-b)j$ for $a, b \in L$. In particular,

$$\tau(\phi(L) + \phi(L)j) = \phi(L) + \phi(L)j \quad \text{and} \quad \phi(L) = \{u \in \phi(L) + \phi(L)j : \tau(u) = u\}. \tag{4.2}$$

Moreover, as $\phi(L)$ is σ-invariant, Lemma 4.5(3) yields that $\phi(L) + \phi(L)j$ is a division ring, which is contained in $\mathbb{H}(X)$ and which contains $\phi(\mathbb{C}) = \mathbb{C}$ and j, i.e., $\mathbb{H}$. By Theorem 1.1, we then have

$$\phi(L) + \phi(L)j = \mathbb{H}(f) \tag{4.3}$$

for some $f \in \mathbb{R}(X)$. Let us fix $g, h \in \mathbb{R}(X^2)$ such that

$$f = g + hX. \tag{4.4}$$

Since $\tau(X) = -X$ and τ fixes $\mathbb{R}$ point-wise, we have $\tau(g) = g$ and $\tau(h) = h$. Hence,

$$\tau(f) = g - hX \tag{4.5}$$

and, by (4.2) and (4.3), we get that $\tau(f) \in \phi(L) + \phi(L)j$. As $g = (f + \tau(f))/2$ by (4.4) and (4.5), we get that $g \in \phi(L) + \phi(L)j$ and, as g is invariant under τ, we may apply (4.2) to get

$$g \in \phi(L). \tag{4.6}$$

In particular, $jhX = j(f - g) \in \phi(L) + \phi(L)j$. Since $\tau(jhX)$ and jhX coincide, (4.2) actually gives

$$jhX \in \phi(L). \tag{4.7}$$

Next, as $f \in \mathbb{R}(X)$, f is central in $\mathbb{H}(f)$. As $\tau(\mathbb{H}(f)) = \mathbb{H}(f)$ by (4.2) and (4.3), we get that $\tau(f)$ is central in $\mathbb{H}(f)$, i.e., $\tau(f) \in \mathbb{R}(f)$ (see Lemma 3.4). As τ fixes $\mathbb{R}$ point-wise, the restriction of τ to $\mathbb{R}(f)$ is an $\mathbb{R}$-automorphism of order ≤ 2. Assume f is algebraic over $\mathbb{R}$. Then $\phi(L) + \phi(L)j = \mathbb{H}$ by (4.3). As $\mathbb{H} = \phi(\mathbb{C}) + \phi(\mathbb{C})j$ and as $\phi(\mathbb{C}) \subseteq \phi(L)$, we may apply Lemma 4.5(4) to get that $L = \mathbb{C}$.

Therefore, assume f is transcendental over $\mathbb{R}$. Hence, $\tau|_{\mathbb{R}(f)}$ is a Möbius transformation of order at most 2. First, assume $\tau(f) = f$, i.e., $g - hX = g + hX$ by (4.4) and (4.5). Hence, $h = 0$ and

$$\phi(L) + \phi(L)j = \mathbb{H}(g) \tag{4.8}$$

by (4.3). Moreover, as $g = \phi(g(-T^2)) \in \phi(\mathbb{R}(T))$, we get that $\mathbb{C}(g) = \phi(\mathbb{C}(g(-T^2)))$ is σ-invariant (see Example 4.3). We may then apply Lemma 4.5(3) to get that $\mathbb{C}(g) + \mathbb{C}(g)j$ is a division ring. But $\mathbb{C}(g) + \mathbb{C}(g)j$ contains $\mathbb{C}$, g and j, i.e., contains $\phi(L) + \phi(L)j$ by (4.8). As (4.6) yields $\mathbb{C}(g) \subseteq \phi(L)$, we may then apply Lemma 4.5(4) to get $L = \mathbb{C}(g(-T^2))$.

From now on, assume $\tau(f) \neq f$. Set

$$\tau(f) = \frac{af + b}{cf + d} \tag{4.9}$$

with $a, b, c, d \in \mathbb{R}$ satisfying $ad - bc \neq 0$. We then have

$$f = \tau^2(f) = \frac{(a^2 + bc)f + b(a + d)}{c(a + d)f + cb + d^2}. \tag{4.10}$$

First, assume $c = 0$, in which case (4.9) and (4.10) reduce to

$$\tau(f) = \frac{af + b}{d} \quad \text{and} \quad f = \frac{a^2 f + b(a + d)}{d^2},$$

respectively. In particular, from the second equality, we get that $f(1 - a^2/d^2)$ is a real number, which is possible only if $a^2 = d^2$. If $a = d$, then the second equality yields further $b = 0$. Hence, $\tau(f) = f$ by the first equality, which cannot hold. Therefore, $a = -d$ and the first equality yields $\tau(f) = -f - ba^{-1}$. Then, by (4.4) and (4.5), it follows that $g = -b(2a)^{-1} \in \mathbb{R}$. Thus

$$\phi(L) + \phi(L)j = \mathbb{H}(hX) \tag{4.11}$$

by (4.3) and (4.4). Moreover, as $jhX = \phi(Th(-T^2)) \in \phi(\mathbb{R}(T))$, we get that $\mathbb{C}(jhX) = \phi(\mathbb{C}(Th(-T^2)))$ is σ-invariant (see Example 4.3). Therefore, Lemma 4.5(3) yields that $\mathbb{C}(jhX) + \mathbb{C}(jhX)j$ is a division ring. But $\mathbb{C}(jhX) + \mathbb{C}(jhX)j$ contains $\mathbb{C}$, jhX and j, i.e., contains $\phi(L) + \phi(L)j$ by (4.11). As (4.7) yields $\mathbb{C}(jhX) \subseteq \phi(L)$, we get $L = \mathbb{C}(Th(-T^2))$ from Lemma 4.5(4).

Finally, assume $c \neq 0$. Then divide a, b and d by c to assume that $c = 1$. We then have

$$\tau(f) = \frac{af + b}{f + d} \quad \text{and} \quad f = \frac{(a^2 + b)f + b(a + d)}{(a + d)f + b + d^2},$$

by (4.9) and (4.10). By the second equality, we get $d = -a$ and the first equality then yields

$$\tau(f) = \frac{af + b}{f - a}.$$

In particular,

$$\tau(f - a) = \frac{af + b - a(f - a)}{f - a} = \frac{b + a^2}{f - a}.$$

As $a \in \mathbb{R}$, we have $\mathbb{R}(f) = \mathbb{R}(f - a)$ and, hence, $\mathbb{H}(f) = \mathbb{H}(f - a)$. Therefore, we may replace f with $f - a$ to assume $\tau(f) = 1/(\alpha f)$, where $\alpha = 1/(b + a^2)$. Set $f = P(X)/Q(X)$, where P and Q are coprime polynomials with real coefficients. Then

$$\frac{P(-X)}{Q(-X)} = \tau(f) = \frac{1}{\alpha f} = \frac{1}{\alpha} \cdot \frac{Q(X)}{P(X)},$$

i.e., $\alpha P(-X)P(X) = Q(-X)Q(X)$. In particular, $\alpha P(0)^2 = Q(0)^2$. If $P(0) = 0$, then we also have $Q(0) = 0$, which cannot hold since P and Q are coprime. Therefore, $\alpha = Q(0)^2/P(0)^2 > 0$.

Given a square root $\sqrt{\alpha}$ of α in $\mathbb{R}$, set

$$v = \frac{1 - \sqrt{\alpha}f}{1 + \sqrt{\alpha}f} \cdot j \in \mathbb{H}(f) = \phi(L) + \phi(L)j.$$

Then

$$\tau(v) = \frac{(1 - \sqrt{\alpha}(\alpha f)^{-1})}{1 + \sqrt{\alpha}(\alpha f)^{-1}} \cdot (-j) = \frac{(\alpha f - \sqrt{\alpha})}{\alpha f + \sqrt{\alpha}} \cdot (-j) = \frac{(1 - \sqrt{\alpha}f)}{1 + \sqrt{\alpha}f} \cdot j = v,$$

thus yielding $\mathbb{C}(v) \subseteq \phi(L)$ by (4.2). If $\phi(L) + \phi(L)j \subseteq \mathbb{C}(v) + \mathbb{C}(v)j$, then Lemma 4.5(4) yields $L = \mathbb{C}(w)$, where w is the unique element of $\mathbb{C}(T, \sigma)$ fulfilling $\phi(w) = v$. To get the desired inclusion, note first that, as $f \in \mathbb{R}(X)$ and as $\sqrt{\alpha} \in \mathbb{R}$, we have $\sigma(v) = v$. Therefore, $\mathbb{C}(v)$ is σ-invariant and, by Lemma 4.5(3), we get that $\mathbb{C}(v) + \mathbb{C}(v)j$ is a division ring. As $\phi(L) + \phi(L)j = \mathbb{H}(f)$ by (4.3) and as $\mathbb{H} \subseteq \mathbb{C}(v) + \mathbb{C}(v)j$, it then suffices to show that $f \in \mathbb{C}(v) + \mathbb{C}(v)j$. But, since

$$f \mapsto \frac{1 - \sqrt{\alpha}f}{1 + \sqrt{\alpha}f}$$

is a Möbius transformation of the rational function field $\mathbb{R}(f)$, there are $a_1, a_2, a_3, a_4 \in \mathbb{R}$ such that

$$f = \left(a_1 \frac{1 - \sqrt{\alpha}f}{1 + \sqrt{\alpha}f} + a_2\right)\left(a_3 \frac{1 - \sqrt{\alpha}f}{1 + \sqrt{\alpha}f} + a_4\right)^{-1} = (a_2 - a_1 vj)(a_4 - a_3 vj)^{-1}$$

and, since $\mathbb{C}(v) + \mathbb{C}(v)j$ is a division ring, we have $(a_2 - a_1 vj)(a_4 - a_3 vj)^{-1} \in \mathbb{C}(v) + \mathbb{C}(v)j$. $\square$

The following proposition shows that σ-invariance is not necessary in general for intermediate division rings $\mathbb{C} \subseteq L \subseteq \mathbb{C}(T, \sigma)$ to be of the form $\mathbb{C}(v)$ with $v \in \mathbb{C}(T, \sigma)$:

Proposition 4.6. *Set $v = T + iT^3 \in \mathbb{C}(T, \sigma)$. Then $\phi(\mathbb{C}(v))$ is not σ-invariant.*

Proof. First, note that $\phi(v) = jX + ij^3 X^3 = jX - ijX^3 = jX - kX^3$.

Now, assume $\phi(\mathbb{C}(v))$ is σ-invariant. Since $\phi(\mathbb{C}(v)) = \mathbb{C}(\phi(v)) = \mathbb{C}(jX - kX^3)$ (see Example 4.3 for the first equality), we have $\sigma(jX - kX^3) = jX + kX^3 \in \mathbb{C}(jX - kX^3)$. Therefore, $\mathbb{C}(jX - kX^3)$ contains $jX = \phi(T)$. Consequently, $\mathbb{C}(v)$ contains T, i.e.,

$$\mathbb{C}(v) = \mathbb{C}(T, \sigma). \tag{4.12}$$

Next, let R denote the intersection of all subrings of $\mathbb{C}[T, \sigma]$ which contain both $\mathbb{C}$ and v. Since $vi = -iv$, we have

$$R = \{a_0 + a_1 v + \cdots + a_n v^n : n \geq 0, a_0, \ldots, a_n \in \mathbb{C}\}.$$

Moreover, since v has positive degree, the v^n's ($n \geq 0$) are linearly independent over $\mathbb{C}$. Therefore, R is the polynomial ring $\mathbb{C}[v, \sigma]$. In particular, $\mathbb{C}(v)$, which is the intersection of all division rings contained in $\mathbb{C}(T, \sigma)$ and containing both $\mathbb{C}$ and v, equals $\mathbb{C}(v, \sigma)$. Hence, by, e.g., [2, lemme 2.3], the center of $\mathbb{C}(v)$ equals $\mathbb{R}(v^2) = \mathbb{R}(T^2 + T^6)$. By (4.12), we then obtain

$$\mathbb{R}(T^2) = \mathbb{R}(T^2 + T^6). \tag{4.13}$$

Finally, note that T^2 is a root of $X^3 + X - (T^2 + T^6) \in \mathbb{R}(T^2 + T^6)[X]$ and that $T^2 + T^6$ is transcendental over $\mathbb{R}$. Considering a transcendental Y, it is easily checked that $X^3 + X - Y$ has no root in $\mathbb{R}(Y)$, i.e., that $X^3 + X - Y$ is irreducible over $\mathbb{R}(Y)$. Consequently, $\mathbb{R}(T^2) = \mathbb{R}(T^2 + T^6)(T^2)$ is a degree 3 extension of $\mathbb{R}(T^2 + T^6)$, which contradicts (4.13). $\square$

To summarize, we have the following combination of Theorem 4.4 and Proposition 4.6:

Corollary 4.7. *Let $\mathbb{C} \subseteq L \subseteq \mathbb{C}(T, \sigma)$ be an intermediate division ring. For L to be of the form $\mathbb{C}(v)$ with $v \in \mathbb{C}(T, \sigma)$, it is sufficient, but not necessary in general, that $\phi(L)$ is σ-invariant.*

Finding a precise, unconditional version of Lüroth's Theorem for division rings of the form $D(T, \sigma)$ (where D is a division algebra) remains an open question. More generally, one may ask for a precise version of Igusa's Theorem for skew function fields of higher dimension. The following example demonstrates another type of obstruction for such a theorem.

Example 4.8. Let R be the first Weyl algebra over the complex numbers $\mathbb{C}$, with generators X, Y. That is, R is the quotient of the free $\mathbb{C}$-algebra in X, Y by the ideal $\langle XY - YX - 1 \rangle$. Let K be the first Weyl skew field, that is, the quotient skew field of R. Then K has transcendence degree 2 over $\mathbb{C}$, in the sense of Gelfand-Kirillov (see [6]). The skew field K contains a (commutative) subfield L, generated over $\mathbb{C}$ by elements a, b satisfying $a^2 - b^3 = 1$, by a theorem of Dixmier [5, Proposition 5.5], and such a subfield L is not generated over $\mathbb{C}$ by a single generator.

Appendix A. Proof of Lemma 2.2

Firstly, set $Z(H) \cdot Z(L) = \{x_1 y_1 + \cdots + x_n y_n : n \geq 1, x_1, \ldots, x_n \in Z(H), y_1, \ldots, y_n \in Z(L)\}$. Then $Z(H) \cdot Z(L)$ contains $Z(H)$ and $Z(L)$, is contained in L, is a commutative ring, and is a $Z(L)$-subspace of L. Moreover, $Z(H) \cdot Z(L)$ is an integral domain (since L is a division ring) and $\dim_{Z(L)} Z(H) \cdot Z(L) \leq \dim_{Z(L)} L < \infty$. Hence, $Z(H) \cdot Z(L)$ is a field.

Secondly, set $H \cdot Z(L) = \{x_1 y_1 + \cdots + x_n y_n : n \geq 1, x_1, \ldots, x_n \in H, y_1, \ldots, y_n \in Z(L)\}$. Then $H \cdot Z(L)$ contains H and $Z(L)$, is contained in L, is a ring, and is a $Z(L)$-subspace of L with $\dim_{Z(L)} H \cdot Z(L) < \infty$. In fact, $H \cdot Z(L)$ is a $(Z(H) \cdot Z(L))$-subspace of L and we have $\dim_{Z(H) \cdot Z(L)} H \cdot Z(L) < \infty$. Moreover, $Z(H) \cdot Z(L) \subseteq Z(H \cdot Z(L))$.

Thirdly, let $\{e_i\}_{i \in I}$ be a $Z(H)$-basis of H. We claim that $\{e_i\}_{i \in I}$ is a $(Z(H) \cdot Z(L))$-basis of $H \cdot Z(L)$. Since $\dim_{Z(H) \cdot Z(L)} H \cdot Z(L) < \infty$, we get that I is finite, as needed for the lemma.

To show the claim, we first show that the e_i's span $H \cdot Z(L)$ over $Z(H) \cdot Z(L)$. To that end, fix $n \geq 1$, $x_1, \ldots, x_n \in H$ and $y_1, \ldots, y_n \in Z(L)$. Then there is a finite subset J of I such that, for $k \in \{1, \ldots, n\}$, there are elements $\lambda_{k,j}$ $(j \in J)$ of $Z(H)$ verifying $x_k = \sum_{j \in J} \lambda_{k,j} e_j$. We then have

$$x_1 y_1 + \cdots + x_n y_n = \left(\sum_{j \in J} \lambda_{1,j} e_j \right) y_1 + \cdots + \left(\sum_{j \in J} \lambda_{n,j} e_j \right) y_n = \sum_{j \in J} (\lambda_{1,j} y_1 + \cdots + \lambda_{n,j} y_n) e_j.$$

Finally, let $\{i_1, \ldots, i_n\} \subseteq I$ and $\lambda_1, \ldots, \lambda_n \in Z(H) \cdot Z(L)$ be such that $\lambda_1 e_{i_1} + \cdots + \lambda_n e_{i_n} = 0$, i.e.,

$$e_{i_1} \lambda_1 + \cdots + e_{i_n} \lambda_n = 0 \tag{A.1}$$

(as $Z(H) \cdot Z(L) \subseteq Z(H \cdot Z(L))$). As $(x, y) \in H \times (Z(H) \cdot Z(L)) \mapsto xy \in H \cdot Z(L)$ is $Z(H)$-bilinear, there is a unique $Z(H)$-linear map $\psi : H \otimes_{Z(H)} (Z(H) \cdot Z(L)) \to H \cdot Z(L)$ which fulfills $\psi(x \otimes y) = xy$ for every $(x, y) \in H \times (Z(H) \cdot Z(L))$. Moreover, as $Z(H) \cdot Z(L) \subseteq Z(H \cdot Z(L))$, the map ψ is a morphism of $Z(H)$-algebras and, by, e.g., [12, Proposition 2.36], it is injective. Therefore, by (A.1), we have

$$e_{i_1} \otimes \lambda_1 + \cdots + e_{i_n} \otimes \lambda_n = 0. \tag{A.2}$$

Now, fix $Z(H)$-linear maps $f_1, \ldots, f_n : Z(H) \cdot Z(L) \to Z(H)$ and, for $j \in \{1, \ldots, n\}$, set

$$e_{i_j}^* : \begin{cases} H & \to & Z(H) \\ e_i & \mapsto & \delta_{i, i_j} \end{cases},$$

where δ_{i, i_j} denotes the Kronecker symbol. Since

$$F : \begin{cases} H \times (Z(H) \cdot Z(L)) & \to & Z(H) \\ (x, y) & \mapsto & e_{i_1}^*(x) f_1(y) + \cdots + e_{i_n}^*(x) f_n(y) \end{cases}$$

is $Z(H)$-bilinear, there is a unique $Z(H)$-linear map $\widetilde{F} : H \otimes_{Z(H)} (Z(H) \cdot Z(L)) \to Z(H)$ which fulfills $\widetilde{F}(x \otimes y) = F(x, y) = e_{i_1}^*(x) f_1(y) + \cdots + e_{i_n}^*(x) f_n(y)$ for every $(x, y) \in H \times (Z(H) \cdot Z(L))$.

By (A.2), we then have

$$0 = \widetilde{F}(e_{i_1} \otimes \lambda_1 + \cdots + e_{i_n} \otimes \lambda_n) = f_1(\lambda_1) + \cdots + f_n(\lambda_n).$$

In particular, fixing $j \in \{1, \ldots, n\}$ and setting $f_1 = \cdots = f_{j-1} = f_{j+1} = \cdots = f_n = 0$, we get $f_j(\lambda_j) = 0$. Fix a $Z(H)$-basis $\{\epsilon_i\}_{i \in I'}$ of $Z(H) \cdot Z(L)$ and, for $i \in I'$, set

$$\epsilon_i^* : \left\{ \begin{array}{ccc} Z(H) \cdot Z(L) & \to & Z(H) \\ \epsilon_{i'} & \mapsto & \delta_{i,i'} \end{array} \right. .$$

As f_j was arbitrary, we get $\epsilon_i^*(\lambda_j) = 0$ for every $i \in I'$, i.e., $\lambda_j = 0$. This concludes the proof.

References

[1] Gil Alon, François Legrand, and Elad Paran. Galois groups over rational function fields over skew fields. *C. R. Math. Acad. Sci. Paris*, 358(7):785–790, 2020.

[2] Angelot Behajaina, Bruno Deschamps, and François Legrand. Problèmes de plongement finis sur les corps non commutatifs. (French). *Israel J. Math.*, 249(2):617–650, 2022.

[3] Claude Chevalley. *Introduction to the Theory of Algebraic Functions of One Variable*. Mathematical Surveys, No. VI. American Mathematical Society, New York, N. Y., 1951. xi+188 pp.

[4] Paul Moritz Cohn. *Skew fields. Theory of general division rings*. Encyclopedia of Mathematics and its Applications, 57. Cambridge University Press, Cambridge, 1995. xvi+500 pp.

[5] Jacques Dixmier. Sur les algèbres de Weyl. *Bull. Soc. Math. Fr.*, 96:209–242, 1968.

[6] I. M. Gelfand and A. A. Kirillov. Sur les corps liés aux algèbres enveloppantes des algèbres de Lie. (French). *Publ. Math., Inst. Hautes Étud. Sci.*, 31:5–19, 1966.

[7] Kenneth R. Goodearl and Robert Breckenridge Warfield, Jr. *An Introduction to noncommutative Noetherian rings*. London Mathematical Society Student Texts, 61. Cambridge University Press, Cambridge, 2004. Second edition. xxiv+344 pp.

[8] Paul Gordan. Ueber biquadratische Gleichungen. (German). *Math. Ann.*, 29(3):318–326, 1887.

[9] Basil Gordon and Theodore S. Motzkin. On the zeros of polynomials over division rings. *Trans. Amer. Math. Soc.*, 116:218–226, 1965.

[10] Jun-ichi Igusa. On a theorem of Lueroth. *Mem. Coll. Sci. Univ. Kyoto Ser. A. Math.*, 26:251–253, 1951.

[11] Shigeru Iitaka. On the homogeneous Lüroth theorem. *Proc. Japan Acad. Ser. A Math. Sci.*, 55(3):88–91, 1979.

[12] Anthony W. Knapp. *Advanced algebra. Along with a companion volume Basic algebra*. Cornerstones. Birkhäuser Boston, Inc., Boston, MA, 2007. xxiv+730 pp.

[13] Tsit Yuen Lam. A general theory of Vandermonde matrices. *Exposition. Math.*, 4:193–215, 1986.

[14] Tsit Yuen Lam and André Leroy. Vandermonde and Wronskian matrices over division rings. *J. Algebra*, 119(2):308–336, 1988.

[15] Tsit Yuen Lam and André Leroy. Hilbert 90 theorems over division rings. *Trans. Amer. Math. Soc.*, 345(2):595–622, 1994.

[16] Tsit Yuen Lam and André Leroy. Wedderburn polynomials over division rings. I. *J. Pure Appl. Algebra*, 186(1):43–76, 2004.

[17] Tsit Yuen Lam, André Leroy, and Adem Ozturk. Wedderburn polynomials over division rings. II. In *Noncommutative rings, group rings, diagram algebras and their applications*, volume 456 of *Contemp. Math.*, pages 73–98. Amer. Math. Soc., Providence, RI, 2008.

[18] Jacob Lüroth. Beweis eines Satzes über rationale Curven. (German). *Math. Ann.*, 9(2):163–165, 1875.

[19] François Ollivier and Brahim Sadik. A simple and constructive proof to a generalization of Lüroth's theorem. *Turkish J. Math.*, 46(4):1291–1293, 2022.

[20] Oystein Ore. Theory of non-commutative polynomials. *Ann. of Math. (2)*, 34(3):480–508, 1933.

[21] Pierre Samuel. Some remarks on Lüroth's theorem. *Mem. Coll. Sci. Univ. Kyoto Ser. A. Math.*, 27:223–224, 1953.

[22] Igor R. Shafarevich. *Basic Algebraic Geometry. 1. Varieties in projective space*. Springer, Heidelberg, 2013. Third edition. Translated from the 2007 third Russian edition. xviii+310 pp.

[23] Ernst Steinitz. Algebraische Theorie der Körper. *J. Reine Angew. Math.*, 137:167–309, 1910.

Email address: `francois.legrand@unicaen.fr`

Normandie Univ., UNICAEN, CNRS, Laboratoire de Mathématiques Nicolas Oresme, 14000 Caen, France

Email address: paran@openu.ac.il

Department of Mathematics and Computer Science, the Open University of Israel, Ra'anana 4353701, Israel