# A simple and constructive proof to a generalization of Lüroth's theorem

François Ollivier

LIX, UMR CNRS 7161
École polytechnique
91128 Palaiseau cedex
France

francois.ollivier@lix.polytechnique.fr

Brahim Sadik

Département de Mathématiques
Faculté des Sciences Semlalia
B.P. 2390, 40000 Marrakech
Maroc

sadik@ucam.ac.ma

March 2022

**Abstract.** A generalization of Lüroth's theorem expresses that every transcendence degree 1 subfield of the rational function field is a simple extension. In this note we show that a classical proof of this theorem also holds to prove this generalization.

Keywords: Lüroth's theorem, transcendence degree 1, simple extension.

**Résumé.** Une généralisation du théorème de Lüroth affirme que tout sous-corps de degré de transcendance 1 d'un corps de fractions rationnelles est une extension simple. Dans cette note, nous montrons qu'une preuve classique permet également de prouver cette généralisation.

Mots-clés : Th. de Lüroth, degré de transcendance 1, extension simple.

Authors' extended version of : Ollivier (François) and Sadik (Brahim), "A simple and constructive proof to a generalization of Lüroth's theorem", *Turkish Journal of Mathematics*, on line, waiting for inclusion in an issue, 2022. DOI : 10.3906/mat-2110-11

# Introduction

Lüroth's theorem ([2]) plays an important role in the theory of rational curves. A generalization of this theorem to transcendence degree 1 subfields of rational functions field was proven by Igusa in [1]. A purely field theoretic proof of this generalization was given by Samuel in [6]. In this note we give a simple and constructive proof of this result, based on a classical proof [7, 10.2 p.218].

Let $k$ be a field and $k(x)$ be the rational functions field in $n$ variables $x_1, \ldots, x_n$. Let $\mathcal{K}$ be a field extension of $k$ that is a subfield of $k(x)$. To the subfield $\mathcal{K}$ we associate the prime ideal $\Delta(\mathcal{K})$ which consists of all polynomials of $\mathcal{K}[y_1, \ldots, y_n]$ that vanish for $y_1 = x_1, \ldots, y_n = x_n$. When the subfield $\mathcal{K}$ has transcendence degree 1 over $k$, the associated ideal is principal. The idea of our proof relies on a simple relation between coefficients of a generator of the associated ideal $\Delta(\mathcal{K})$ and a generator of the subfield $\mathcal{K}$. When $\mathcal{K}$ is finitely generated, we can compute a rational fraction $v$ in $k(x)$ such that $\mathcal{K} = k(v)$. For this, we use some methods developped by the first author in [3] to get a generator of $\Delta(\mathcal{K})$ by computing a Gröbner basis or a characteristic set.

# Main result

Let $k$ be a field and $x_1, \ldots, x_n, y_1, \ldots, y_n$ be $2n$ indeterminates over $k$. We use the notations $x$ for $x_1, \ldots, x_n$ and $y$ for $y_1, \ldots, y_n$. If $\mathcal{K}$ is a field extension of $k$ in $k(x)$ we define the ideal $\Delta(\mathcal{K})$ to be the prime ideal of all polynomials in $\mathcal{K}[y]$ that vanish for $y_1 = x_1, \ldots, y_n = x_n$.

$$\Delta(\mathcal{K}) = \{P \in \mathcal{K}[y] \quad : \quad P(x_1, \ldots, x_n) = 0\}.$$

*Lemma* 1. — *Let $\mathcal{K}$ be a field extension of $k$ in $k(x)$ with transcendence degree* 1 *over $k$.*

*i) The ideal $\Delta(\mathcal{K})$ is principal in $\mathcal{K}[y]$.*

*ii) If $\mathcal{K}_1 \subset \mathcal{K}_2$ and $\Delta(K_i) = \mathcal{K}_i[y]G$, for $i = 1, 2$, then $\mathcal{K}_1 = \mathcal{K}_2$.*

*iii) $\Delta(\mathcal{K}) = \tilde{\Delta}(\mathcal{K}) := (p(y) - p(x)/q(x)q(y) | p/q \in \mathcal{K})$.*

*iv) The ideal $\hat{\Delta}(\mathcal{K}) := k[x]\Delta(\mathcal{K}) \cap k[x, y]$ is a radical ideal, which is equal to $(q(x)p(y) - p(x)q(y) | p/q \in \mathcal{K})$.*

*v) Let $G$ be such that $\Delta(\mathcal{K}) = (G)$, with $G = \sum_{j=0}^{d} p_j(x)/q_j(x)y^j$ and $GCD(p_j, q_j) = 1$, for $0 \leq j \leq d$. Let $Q := PPCM(q_j \mid 0 \leq j \leq d)$, then $\hat{G} := QG$ is such that $G(y,x) = -G(x,y)$ and $\deg_x \hat{G} = \deg_y \hat{G} = d$.*

Proof. — i) In the unique factorization domain $\mathcal{K}[y]$, the prime ideal $\Delta(\mathcal{K})$ has codimension 1. Hence, it is principal.

ii) Assume that $\mathcal{K}_1 \neq \mathcal{K}_2$. There exists $p(x)/q(x) \in \mathcal{K}_2$ a reduced fraction, with $p(x)/q(x) \notin \mathcal{K}_1$. The set $\{1, p(x)/q(x)\}$ may be completed to form a basis $\{e_1 = 1, e_2 = p/q, \ldots, e_s\}$ of $\mathcal{K}_2$ as a $\mathcal{K}_1$-vector space. Then, $e$ is also a basis of $\mathcal{K}_2[y] = \mathcal{K}_2\mathcal{K}_1[y]$ as a $\mathcal{K}_1[y]$-module and $Ge$ is a basis of $\Delta(\mathcal{K}_2) = \mathcal{K}_2\Delta(\mathcal{K}_1)$ as a $\mathcal{K}_1[y]$-module. So, $p(y) - p(x)/q(x)q(y) \in \Delta(\mathcal{K}_2)$ is equal to $p(y)e_1 - q(y)e_2$, which implies that $G$ divides $p$ and $q$, a contradiction.

iii) We remark that $\tilde{\Delta}(\mathcal{K})$ does not define any prime component containing polynomials $k[y]$, so that $\tilde{\Delta}(\mathcal{K}) : k[y] = \tilde{\Delta}(\mathcal{K})$. The inclusion $\supset$ is immediate. Let $P \in \Delta(\mathcal{K})$ with $P(x,y) = \sum_{j=0}^{s} p_j(x)/q_j(x)y^j$. We have $P(x,x) = 0$ and by symmetry $P(y,y) = 0$, so $P = P(x,y) - P(y,y) = \sum_{j=0}^{s}(p_j(x)/q_j(x) - p_j(y)/q_j(y))y^j$. So, throwing away denominators in $k[y]$, $\prod_{j=1}^{s} q_i(y)P \in \tilde{\Delta}(\mathcal{K})$, so that $P \in \tilde{\Delta}(\mathcal{K}) : k[y] = \tilde{\Delta}(\mathcal{K})$, hence the result.

iv) The ideal $\Delta(\mathcal{K})$ is prime, so that $k(x)\Delta(\mathcal{K})$ and $\hat{\Delta}(\mathcal{K})$ are radical. We remark that $\hat{\Delta}(\mathcal{K})$ does not define any prime component containing polynomials $k[x]$ or in $k[y]$, so that $\hat{\Delta}(\mathcal{K}) : (k[x]k[y]) = \hat{\Delta}(\mathcal{K})$. The inclusion $\supset$ is immediate. Using the generators $p(y) - p(x)/q(x)q(y)$, $p/q \in \mathcal{K}$, a finite set of fractions $\Sigma$ is enough by Noetherianity, so that $\prod_{p/q\in\Sigma} q(x)\delta(\mathcal{K}) \subset (p(y) - p(x)/q(x)q(y) | p/q \in \mathcal{K})$, which provides the reverse inclusion, using the previous remark.

v) By construction, $\hat{G}$ is a generator of $\hat{\Delta}(\mathcal{K})$. All the generators of $\hat{\Delta}(\mathcal{K})$ in iv) being antisymmetric, $\hat{G}$ is antysymmetric, which also implies that $\deg_x \hat{G} = \deg_y \hat{G} = d$. ∎

Theorem 2. — *Let $\mathcal{K}$ be a field extension of $k$ in $k(x)$ with transcendence degree 1 over $k$. Then, there exists $v$ in $k(x)$ such that $\mathcal{K} = k(v)$.*

Proof. — By lem. 1 i), the prime ideal $\Delta(\mathcal{K})$ of $\mathcal{K}[y]$ is principal. Let $G$ be a monic polynomial such that $\Delta(\mathcal{K}) = (G)$ in $\mathcal{K}[y]$. Let $c_0(x), \ldots, c_r(x)$ be the coefficients of $F$ as a polynomial in $\mathcal{K}[y]$. Since $x_1, \ldots, x_n$ are transcendental over $k$ there must be a coefficient $v := c_i$ that lies in $\mathcal{K}\backslash k$.

Write $v = \frac{f(x)}{g(x)}$ where $f$ and $g$ are relatively prime in $k[x]$. By lem. 1 v), $\max(\deg_x f, \deg_x g) \leq d := \deg_x G$. As $g(x)f(y) - f(x)g(y)$ is a multiple of $\hat{G}$, $\max(\deg_x f, \deg_x g) = d$. Let $D := f(y) - vg(y)$. As $D \in \Delta(\mathcal{K})$, the remainder of the Euclidean division of $G$ by $D$ is also in $\Delta(\mathcal{K})$ and of degree less than the degree of $G$. It must then be 0. Therefore $D$ is a generator of $\Delta(k(v))$ and of $\Delta(\mathcal{K})$, with $k(v) \subset \mathcal{K}$, and by lem. 1 ii), we need have $\Delta(\mathcal{K}) = \Delta(k(v))$ and $\mathcal{K} = k(v)$. ∎

The following result, given by the first author in [3, prop. 4 p. 35] and [4, th. 1] in a differential setting that includes the algebraic case, permits to compute a basis for the ideal $\Delta(\mathcal{K})$.

Proposition 3. — *Let $\mathcal{K} = k(f_1, \ldots, f_r)$ where the $f_i = \frac{P_i}{Q_i}$ are elements of $k(x)$. Let $u$ be a new indeterminate and consider the ideal*

$$\mathcal{J} = \left( P_1(y) - f_1 Q_1(y), \ldots, P_r(y) - f_r Q_r(y), u \left( \prod_{i=1}^{r} Q_i(y) - 1 \right) \right)$$

*in $\mathcal{K}[y, u]$. Then*

$$\Delta(\mathcal{K}) = \mathcal{J} \cap \mathcal{K}[y].$$

# Conclusion

A generalization of Lüroth's theorem to differential algebra has been proven by J. Ritt in [5]. One can use the theory of characteristic sets to compute a generator of a finitely generated differential subfield of the differential field $\mathcal{F}\langle y \rangle$ where $\mathcal{F}$ is an ordinary differential field and $y$ is a differential indeterminate. In a forthcoming work we will show that Lüroth's theorem can be generalized to one differential transcendence degree subfields of the differential field $\mathcal{F}\langle y_1, \ldots, y_n \rangle$.

# References

[1] Igusa (Jun-ichi), "On a theorem of Lueroth", *Memoirs of the College of Science*, Univ. of Kyoto, Series A, vol. 26, Math. n° 3, 251–253, 1951.

[2] Lüroth (Jacob), "Beweis eines Satzes über rationale Curven", *Mathematische Annalen* 9, 163–165, 1875.

[3] Ollivier (François), *Le problème d'identifiabilité structurelle globale : approche théorique, méthodes effectives et bornes de complexité*, Thèse de doctorat en science, École polytechnique, 1991.

[4] Ollivier (François), "Standard bases of differential ideals", proceedings of AAECC 1990, *Lecture Notes in Computer Science*, vol. 508, Springer, Berlin, Heidelberg, 304–321, 1990.

[5] Ritt (Joseph Fels), *Differential Algebra*, Amer. Math. Soc. Colloquium Publication, vol. 33, Providence, 1950.

[6] Samuel (Pierre), "Some Remarks on Lüroth's Theorem", *Memoirs of the College of Science*, Univ. of Kyoto, Series A, vol. 27, Math. n° 3, 223–224, 1953.

[7] Van der Waerden (Bartel Leendert), *Algebra*, vol. 1, Frederick Ungar Publishing Company, New York, 1970, reprint by Springer 1991.