Turkish Journal of Mathematics

http://journals.tubitak.gov.tr/math/

Research Article

Turk J Math
(2022) 46: 1291 – 1293
© TÜBİTAK
doi:10.3906/mat-2110-11

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

François OLLIVIER[1], **Brahim SADIK**[2,*]
[1]LIX, École polytechnique, Palaiseau CEDEX
[2]Department of Mathematics, Faculty of Sciences Semlalia, Avenue My Abdellah, Marrakech, Morocco

Received: 09.10.2021 • **Accepted/Published Online:** 09.03.2022 • **Final Version:** 05.05.2022

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.

Key words: Lüroth's theorem, one transcendence degree, simple extension

1. 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 t heoretic 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]).

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 developed by the first author in [3, 4] to get a generator of $\Delta(\mathcal{K})$ by computing a Gröbner basis or a characteristic set.

2. 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 $y_1 = x_1, \ldots, y_n = x_n$.

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

*Correspondence: sadik@uca.ac.ma
2010 *AMS Mathematics Subject Classification:* 12F20, 12Y05

Lemma 2.1 *Let $\mathcal{K}$ be a field extension of k in $k(x)$ with transcendence degree* 1 *over k. Then the ideal $\Delta(\mathcal{K})$ is principal in $\mathcal{K}[y]$.*
If $\mathcal{K}_1 = \mathcal{K}_2$ and $\Delta(\mathcal{K}_i) = \mathcal{K}_i[y]\ G$, for i = 1, 2, then $\mathcal{K}_1 = \mathcal{K}_2$

Proof In the unique factorization domain $\mathcal{K}[y]$ the prime ideal $\Delta(\mathcal{K})$ has codimension 1. Hence, it is principal. Assume that $\mathcal{K}_1 \neq \mathcal{K}_2$. There exists a reduced fraction $P/_q$ with $P/_q \in \mathcal{K}_2 \backslash \mathcal{K}_1$. The set $\{1,\ P/_q\}$ may be completed to form a basis $e = \{e_1 = 1, e_2 = P/_q,\ \ldots, e_s\}$ of $\mathcal{K}_2$ as a $\mathcal{K}_1$-vector space Then, Ge is a basis of $\Delta(\mathcal{K}_2) = \mathcal{K}_2\,\Delta(\mathcal{K}_1)$ as a $\mathcal{K}_1[y]$-module So $p(y)$-$P/_q\ q(y) \in \mathcal{K}_2$ is equal to $p(y)e_1 - q(y)e_2$ which implies that G divides p and q, a contradiction. $\square$

Theorem 2.2 *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 the last lemma 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 $\mathcal{K}[y]$. We arrange G with respect to a term order on y and we multiply by a suitable element $A \in k[x]$ so that $F = AG$ is primitive in $k[x][y]$. Let $A_0(x), \ldots, A_r(x)$ be the coefficients of F as a polynomial in $k[x][y]$ then all the ratios $\frac{A_i(x)}{A_r(x)}$ lie in $\mathcal{K}$. Since $x_1, \ldots, x_n$ are• transcendentals over k there must be a ratio $v = \frac{A_{i_0}(x)}{A_r(x)}$ that lies in $\mathcal{K} \backslash k$. Write $v = \frac{f(x)}{g(x)}$ where f and g are relatively prime in $k[x]$ and let $D = f(y)g(x) - f(x)g(y)$. The polynomial $f(y) - vg(y)$ lies in $\Delta(\mathcal{K})$, so G divides $f(y) - vg(y)$ in $\mathcal{K}[y]$. Therefore F divides D in $k(x)[y]$. But F is primitive in $k[x][y]$, so that F divides D in $k[x][y]$. Since $\deg_{x_i}(D) \leq \deg_{x_i}(F)$ and $\deg_{y_i}(D) \leq \deg_{y_i}(F)$ for $i = 1, \ldots, n$ there must be $c \in k$ such that $D = cF$. We have now $\Delta(\mathcal{K}) = \Delta(k(v))$. Hence $\mathcal{K} = k(v)$. $\square$

The following result, given by the first author in [3] and [4, th. 1], permits to compute a basis for the ideal $\Delta(\mathcal{K})$.

Proposition 2.3 *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

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

3. 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 J. On a theorem of Lüroth. Memoirs of the College of Science, University of Kioto 1951; (26): 251-253.

[2] Lüroth J. Beweis eines Satzes über rationale Curven. Mathematische Annalen 1876; (9): 163-165 (in German).

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

[4] Ollivier F. Standard bases of differential ideals. Lecture Notes in Computer Science 1990; 508: 304-321.

[5] Ritt JF. Differential Algebra. American Mathematical Society. USA: New York, 1950.

[6] Samuel P. Some Remarks on Lüroth's Theorem. Memoirs of the College of Science, University of Kioto 1953; (27): 223-224.

[7] Van Der Waerden BL. Modern Algebra. Volueme I, Frederic Ungar Publishing Company, 1931.