REVISTA MATEMÁTICA de la
Universidad Complutense de Madrid
Volumen 10, número Suplementario: 1997

A really elementary proof of real Lüroth's theorem.

T. RECIO* and J. R. SENDRA†

Abstract

Classical Lüroth theorem states that every subfield $\mathbf{K}$ of $K(t)$, where t is a transcendental element over K, such that $\mathbf{K}$ strictly contains K, must be $\mathbf{K} = K(h(t))$, for some non constant element $h(t) \in K(t)$. Therefore, $\mathbf{K}$ is K-isomorphic to $K(t)$. This result can be proved with elementary algebraic techniques, and therefore it is usually included in basic courses on field theory or algebraic curves. In this paper we study the validity of this result under weaker assumptions: namely, if $\mathbf{K}$ is a subfield of $\mathbf{C}(t)$ and $\mathbf{K}$ strictly contains $\mathbf{R}$ ($\mathbf{R}$ the real field, $\mathbf{C}$ the complex field), when does it hold that $\mathbf{K}$ is isomorphic to $\mathbf{R}(t)$? Obviously, a necessary condition is that $\mathbf{K}$ admits an ordering. Here we prove that this condition is also sufficient, and we call such statement the Real Lüroth's Theorem. There are several ways of proving this result (Riemann's theorem, Hilbert-Hurwitz [3]), but we claim that our proof is really elementary, since it does require just some basic background as in the classical version of Lüroth's.

1 Real Lüroth's Theorem

Lüroth's Theorem usually appears in courses on field theory or in courses on algebraic curves, and –as it is well known– states that every subfield

---

*Partially supported by CICyTPB92/0498/C0201 (Geometría Real y Algoritmos), Esprit/Bra 6846 (Posso), and TIC-1026-CE.

†Partially supported by Univ. Alcalá Proy. 030795.

AMS subject classification: 14H05, 14P05.

Servicio Publicaciones Univ. Complutense. Madrid, 1997.

$\mathbb{K}$ of the field $K(t)$ (t transcendental over K) transcendental over K (this means, in particular, that $\mathbb{K}$ contains K), is isomorphic to $K(t)$, see [4] vol. II pp. 515 (i.e $\mathbb{K}$ has the form $K(h(t))$, for some $h(t) \in K(t)$), or equivalently, that the field of rational functions of every K-rational plane curve is isomorphic to $K(t)$, see [7] vol. I pp. 9.

Let now K' be an algebraic extension of K, and $\mathbb{K}$ a subfield of $K'(t)$ (t transcendental over K') which is transcendental over K. Then the natural question of analyzing if $\mathbb{K}$ is isomorphic to $K(t)$ arises. In particular, if $K = \mathbb{R}$ and $K' = \mathbb{C}$ one may study if $\mathbb{K}$ is isomorphic to $\mathbb{R}(t)$. Clearly, this is not true for every $\mathbb{K}$. For instance if $\mathbb{K} = \mathbb{C}(t)$, with t transcendental over $\mathbb{C}$, it holds that $\mathbb{R} \subsetneq \mathbb{K} \subseteq \mathbb{C}(t)$, but $\mathbb{K}$ is not isomorphic to $\mathbb{R}(t)$. Similarly, if $\mathcal{C}$ is the curve defined by x^2+y^2+1 over $\mathbb{C}$, and $\mathbb{K} = \mathbb{R}(\mathcal{C})$ is the field of rational functions on $\mathcal{C}$ over $\mathbb{R}$, then $\mathbb{R} \subsetneq \mathbb{K} \subseteq \mathbb{C}(t)$, but $\mathbb{K}$ is not isomorphic to $\mathbb{R}(t)$ since $\mathbb{K}$ is not orderable ($x^2 + y^2 + 1 = 0$ in $\mathbb{K}$). Real Lüroth's theorem states under which conditions $\mathbb{K}$ and $\mathbb{R}(t)$ are isomorphic[1]. More precisely:

Real Lüroth's Theorem (Field theory version).
Every orderable subfield $\mathbb{K}$ of the field $\mathbb{C}(t)$ (t transcendental over $\mathbb{C}$) transcendental over $\mathbb{R}$, is isomorphic to $\mathbb{R}(t)$.

We remark here that it is equivalent, for a subfield $\mathbb{K}$ of $\mathbb{C}(t)$, to be both orderable and strictly containing $\mathbb{R}$ and to be orderable and transcendental over $\mathbb{R}$. In fact, if $\mathbb{K}$ strictly contains $\mathbb{R}$, then either is contained in $\mathbb{C}$ or contains some element in $\mathbb{C}(t) \setminus \mathbb{C}$. In the latter case, clearly it is transcendental over $\mathbb{R}$. In the first situation, $\mathbb{K}$ can not be orderable (since it will be an algebraic extension of $\mathbb{R}$). The converse is trivial.

Equivalently, for algebraic curves, the theorem can be stated as follows:

Real Lüroth's Theorem (Algebraic curves version).
Every real rational plane curve can be parametrized over the reals.

Let us remark that a real rational plane curve $\mathcal{C}$ is a curve parametrizable over $\mathbb{C}$ ([2] pp. 16,127,130), defined by $f \in \mathbb{R}[x, y]$, f irreducible, and such that $\mathbb{R}(\mathcal{C})$ is orderable (that is, $\mathcal{C}$ has infinitely many real

[1]This is equivalent to be $\mathbb{R}$-isomorphic. We thank the referee for pointing out this fact.

points). In other words, $\mathcal{C}$ is a true curve in $\mathbf{R}^2$ and its complexification is parametrizable over $\mathbb{C}$, i.e. it is the Zariski closure of a non constant rational map from $\mathbb{C}$ to $\mathbb{C}^2$. A similar definition gives the concept of curve parametrizable over the reals. Both imply, by the classical Lüroth's theorem, that the function field of the curve is isomorphic to $\mathbb{C}(t)$ or $\mathbf{R}(t)$, respectively.

Before giving a proof of real Lüroth's theorem, we first prove that both statements are equivalent: let us assume that the field theory version of real Lüroth's theorem holds and let $\mathcal{C}$ be a real rational plane curve. Then $\mathbf{R}(\mathcal{C})$ is orderable, and $\mathbf{R} \subsetneq \mathbf{R}(\mathcal{C}) \subseteq \mathbb{C}(t)$, with t transcendental over $\mathbb{C}$. Thus, by real Lüroth's theorem (field theory version) one has that $\mathbf{R}(\mathcal{C})$ is isomorphic to $\mathbf{R}(t)$, and therefore $\mathcal{C}$ is parametrizable over $\mathbf{R}$. Conversely, let us assume that the algebraic curves version of real Lüroth's theorem holds and let $\mathbf{K}$ be an orderable subfield of $\mathbb{C}(t)$ (t transcendental over $\mathbb{C}$) transcendental over $\mathbf{R}$. Then, since the transcendence degree of $\mathbf{K}$ over $\mathbf{R}$ is one, there exists a curve $\mathcal{C}$ defined by an irreducible $f \in \mathbf{R}[x, y]$ such that $\mathbf{K} = \mathbf{R}(\mathcal{C})$. Furthermore, $\mathcal{C}$ is a real rational plane curve ($\mathbf{R}(\mathcal{C})$ is orderable, and $\mathcal{C}$ is parametrizable over $\mathbb{C}$). Therefore, applying real Lüroth's theorem for algebraic curves, one obtains that $\mathcal{C}$ is parametrizable over $\mathbf{R}$.

In the sequel, we focus on the algebraic curves version of real Lüroth's theorem. Direct, non elementary proofs of the theorem can be deduced from [1] or [6] (where algorithmic techniques develop some ideas in [3]). The approach underlying parametrization algorithms can be applied to derive a direct and constructive proof [5],[6]: in order to parametrize a rational curve by means of adjoint curves, one considers the intersection of the curve with a linear subsystem, of dimension one, of a linear system of adjoint curves, obtained by introducing finitely many simple points on the original curves as simple base points of the linear system. Therefore, since the system of adjoint curves can be computed with ground field operations, it holds that the rational curve can be parametrized over the field extension of the ground field where the coordinates of the simple points belong to. Thus, since any real curve has infinitely many simple real points it follows that, taking real simple points in the sketched algorithm, any real rational plane curve can be parametrized over the reals; and therefore a direct and constructive proof (since methods for determining simple points of rational curves over optimal extensions are provided in [3],[6]) of real Lüroth's theorem is derived. Also, a direct but

non constructive proof can be given using the ideas of [1]: first one shows that under the hypothesis of the theorem, $\mathbb{K}$ is of genus zero (genus is defined in [1] through divisors). Since by extending the base field from $\mathbb{R}$ to $\mathbb{C}$, the genus of $\mathbb{K}$ and of the result, $\mathbb{K}'$, of such extension, is kept the same ([1], p. 99), we must just prove that the extended subfield $\mathbb{K}'$ of $\mathbb{C}(t)$ is of genus zero. This is achieved using the classical Lüroth theorem and the fact ([1] p. 22) that $\mathbb{C}(t)$ is of genus zero. Now [1], p. 22, shows that for genus zero algebraic function fields $\mathbb{K}$, if there is at least one place of degree one, then $\mathbb{K}$ is a purely transcendental extension of the field of constants $\mathbb{R}$. But the hypothesis that $\mathbb{K}$ is orderable implies that it has a real place, namely, a place with $\mathbb{R}$ as residue field, thus of degree one.

2 An Elementary Proof of Real Lüroth's Theorem

As announced before, the aim of this note is to provide an elementary proof of this theorem. By elementary we mean that it does not use material beyond what is standard in the traditional presentation of the classical Lüroth's theorem. Of course it requires the concept of orderable field, or –in the other version– of the idea (quite natural) of real plane curve $\mathcal{C}$, in the sense of being defined by a real polynomial and having an infinite number of real points. Now, assuming that $\mathcal{C}$ admits a rational parametrization with complex coefficients, we want to conclude that it also has a rational parametrization with real coefficients. Let $\mathcal{P}(t)$ be a proper (i.e. an almost always one to one) complex rational parametrization of $\mathcal{C}$, then we will proceed as follows: first one associates with $\mathcal{C}$ an additional curve $\tilde{\mathcal{C}}$ that provides the complex parameter values that generate –via $\mathcal{P}$– the real points on $\mathcal{C}$; afterwards, one proves that $\tilde{\mathcal{C}}$ has one real component $\mathcal{C}^\star$ that is either a circle or a line, and finally one shows that if $\mathcal{M} = (m_1(t), m_2(t))$ is any real parametrization of this real component $\mathcal{C}^\star$ of $\tilde{\mathcal{C}}$, then $\mathcal{P}(m_1(t) + i\, m_2(t))$ is a real parametrization of $\mathcal{C}$. Thus, since $\mathcal{C}^\star$ is always parametrizable over $\mathbb{R}$, one concludes that $\mathcal{C}$ is parametrizable over $\mathbb{R}$.

More precisely, let $t = t_1 + i\, t_2,\ t_1, t_2 \in \mathbb{R}$, denote a generic complex

number. Then the parametrization $\mathcal{P}(t)$ can be written in the form:

$$\mathcal{P}(t) = \left(\frac{h_1(t_1,t_2) + i\ f_1(t_1,t_2)}{n_1(t_1,t_2)}, \frac{h_2(t_1,t_2) + i\ f_2(t_1,t_2)}{n_2(t_1,t_2)}\right)$$

where $n_1, n_2, h_1, h_2, f_1, f_2 \in \mathbb{R}[x,y]$. Now, since $\mathcal{C}$ is real, there exist infinitely many points $(t_1,t_2) \in \mathbb{R}^2$ such that $\mathcal{P}(t_1 + i\,t_2)$ is a real point on $\mathcal{C}$. Therefore, if $\mathcal{F}_i$ is the set of zeros $(t_1,t_2) \in \mathbb{R}^2$ of the polynomials $f_i \in \mathbb{R}[x,y], i = 1,2$, the curves $\mathcal{F}_1$ and $\mathcal{F}_2$ have infinitely many common points, and hence, they have common components. Let $\tilde{\mathcal{C}}$ be the curve defined as the union of the common components of $\mathcal{F}_1$ and $\mathcal{F}_2$. It is a real curve, called the associated curve with $\mathcal{C}$ and $\mathcal{P}(t)$.

In the following, we analyze the algebraic properties of $\tilde{\mathcal{C}}$. We start with the following technical lemma. It roughly means that a curve in $\mathbb{C}^2$, defined by a real polynomial, that is intersected just on one point by a pencil of truly complex lines $x = a\,y + t$ (i.e. non real), must be either a conic or a line. The second part of the lemma, specifying the kind of conic is not really needed in our proof, since we always know how to parametrize a conic, but describes an interesting fact.

Lemma 1. *Let $f \in \mathbb{R}[x,y]$ be a non constant polynomial, and a a non real complex number, such that, for almost all $t \in \mathbb{C}$, one has $\deg_y(f(ay+t,y)) = 1$. Then it holds that $f(x,y)$ defines either a line or a conic. Furthermore, if f has degree two, then :*

(1) *If f is reducible over $\mathbb{C}$, then there exist $k \in \mathbb{C}$, such that f defines the pair of conjugate complex lines $(x - ay + k), (x - \bar{a}y + \bar{k})$, where $\bar{a}$ and $\bar{k}$ denote the conjugates of a and k, respectively.*

(2) *If f is irreducible over $\mathbb{C}$, then f defines an ellipse. Moreover, in this case, then f defines a circle if and only if $a = \pm i$.*

Proof. Let f be of degree d, and $f = f_d + \cdots + f_0$ be the decomposition of f in homogeneous components. The Taylor expansion at $x = ay$ of the polynomial $f_j \in \mathbb{R}[y][x]$ with respect to the variable x is

$$f_j(x) = \sum_{i=0}^{i=j} \frac{1}{i!} \frac{\partial f_j}{\partial x^i}(ay,y)(x - ay)^i,$$

and so

$$f(x,y) = \sum_{j=0}^{j=d} f_j(x,y) = \sum_{j=0}^{j=d}\sum_{i=0}^{i=j} \frac{1}{i!}\,\frac{\partial f_j}{\partial x^i}(ay,y)\,(x-ay)^i$$

$$= \sum_{j=0}^{j=d}\sum_{i=0}^{i=j} \frac{1}{i!}\,\frac{\partial f_j}{\partial x^i}(a,1)\,(x-ay)^i y^{j-i}$$

Therefore, if we replace $x = ay + t$ in the above expression, we get:

$$f(ay+t,y) = \sum_{j=0}^{j=d}\sum_{i=0}^{i=j} \frac{1}{i!}\,\frac{\partial f_j}{\partial x^i}(a,1)t^i y^{j-i}.$$

Changing indexes, we can rewrite the above expression as:

$$f(ay+t,y) = \sum_{k=0}^{k=d}\sum_{i=0}^{i=d-k} \frac{1}{i!}\,\frac{\partial f_{k+i}}{\partial x^i}(a,1)t^i y^k.$$

Since for almost all $t \in \mathbb{C}$ the degree of $f(ay+t,y)$ w.r.t y is one, it follows that for $k = 2,\ldots,d$ the polynomials $\sum_{i=0}^{i=d-k} \frac{1}{i!}\frac{\partial f_{k+i}}{\partial x^i}(a,1)t^i \in \mathbb{C}[t]$ vanish for infinitely many values of t. Hence, counting degrees, $\frac{\partial f_{k+i}}{\partial x^i}(a,1) = 0$ for $k = 2,\ldots,d$ and $i = 0,\ldots,d-k$. In particular, when $k+i = d$, one deduces that $\frac{\partial f_d}{\partial x^\ell}(a,1) = 0$ for $\ell = 0,\ldots,d-2$. Therefore $(x-a)^{d-1}$ divides $f_d(x,1)$. Now, since a is a non real complex number and $f_d(x,1) \in \mathbb{R}[x]$, it follows that $(x-\bar{a})^{d-1}$ also divides $f_d(x,1)$. Hence, $2(d-1) \leq d$, that is $d \leq 2$.

We now proceed to analyze the conic defined by f, so we assume $d = 2$. Then, taking into account that $(x-ay)(x-\bar{a}y)$ divides $f_d(x,y)$, one deduces that f can be written (up to a multiplicative constant) as

$$x^2 - 2a_0xy + (a_0^2 + a_1^2)y^2 + b_0x + b_1y + b_2$$

for some $b_0, b_1, b_2 \in \mathbb{R}$ (a_0 and a_1 denote the real and the imaginary part of a, respectively), and that $(a:1:0)$, $(\bar{a}:1:0)$ are the points at infinity of the conic. Hence, since $a \notin \mathbb{R}$, f is neither a parabola nor a hyperbola. Therefore, f has to be either a pair of conjugate complex lines (clearly, the lines are then $(x-ay+k)$, $(x-\bar{a}y+\bar{k})$ for some $k \in \mathbb{C}$) or an ellipse; depending on the reducibility of f.

In order to distinguish between general ellipses and circles, we assume that f is irreducible and we analyze the lengths of the axis of the conic, i.e. the eigenvalues of the matrix

$$B = \begin{pmatrix} 1 & -a_0 \\ -a_0 & a_0^2 + a_1^2 \end{pmatrix}$$

Thus, since $(trace(B))^2 = 4\det(B)$ is the condition for coincident eigenvalues, it follows that f is a circle if and only if $a_0^2 + (a_1 \pm 1)^2 = 0$, i.e., if and only if $a = \pm i$.

■

Lemma 2. *Let $\mathcal{C}$ be a rational real plane curve, $\mathcal{P}(t)$ a proper complex rational parametrization of $\mathcal{C}$, and $\tilde{\mathcal{C}}$ the associated curve of $\mathcal{C}$, via $\mathcal{P}(t)$. Then, there is a real component of $\tilde{\mathcal{C}}$ that is either a circle or a line.*

Proof. Let $T(x,y) = T_1(x,y) + iT_2(x,y) \in \mathbb{C}(x,y)$, with $T_1, T_2 \in \mathbb{R}(x,y)$, a rational inversion of $\mathcal{P}(t)$ (i.e. for almost all $(a,b) \in \mathcal{C}$ and almost all $t_0 \in \mathbb{C}$ it holds that $T(\mathcal{P}(t_0)) = t_0$ and $\mathcal{P}(T(a,b)) = (a,b)$). Since $\mathcal{P}(t)=\mathcal{P}(T_1(\mathcal{P}(t)) + iT_2(\mathcal{P}(t))$, and since there are infinitely many values of t that turn $\mathcal{P}(t)$ real, it follows that $\mathcal{Q}(t) = (T_1(\mathcal{P}(t)), T_2(\mathcal{P}(t)))$ parametrizes one real, irreducible component $\mathcal{C}^\star$ of $\tilde{\mathcal{C}}$ (here, since $\mathcal{P}$ is proper one obtains that $\mathcal{C}^\star$ has infinitely many real points).

In order to prove that $\mathcal{C}^\star$ is a line or a circle let $g^\star \in \mathbb{R}[x,y]$ be the irreducible polynomial (even over the complex field) that defines $\mathcal{C}^\star$. Then $m(t,y) = g^\star(-iy + t, y)$ is also irreducible (note that m is obtained by a change of coordinates of $g^\star$). Furthermore, since $T_1(\mathcal{P}(t)) + iT_2(\mathcal{P}(t)) = t$ one has that $m(t, T_2(\mathcal{P}(t))) = 0$, and therefore m is linear in y (note that $(y - T_2(\mathcal{P}(t)))$ divides $m(t,y) \in \mathbb{C}(t)[y]$ and m is irreducible). Thus for almost all $t_0 \in \mathbb{C}$ $deg_y(m(t_0,y)) = 1$. Hence, applying Lemma 1, and taking into account that $\mathcal{C}^\star$ can not be a pair of complex conjugate lines since it is real, one concludes that $\mathcal{C}^\star$ is either a line or a circle.

■

Summarizing, the previous results can be applied to give an elementary and constructive proof of real Lüroth's theorem: let $\mathcal{C}$ be a rational

real plane curve, $\mathcal{P}(t)$ a proper complex rational parametrization of $\mathcal{C}$, and $\tilde{\mathcal{C}}$ the associated curve with $\mathcal{C}$ and $\mathcal{P}(t)$. Then, by the previous theorem, $\tilde{\mathcal{C}}$ has a real component $\mathcal{C}^\star$ that is either a line or a circle. Let $\mathcal{M}(t) = (m_1(t), m_2(t))$ be a real rational parametrization of $\mathcal{C}^\star$, and consider the parametrization $\mathcal{R}(t) = \mathcal{P}(m_1(t) + i\, m_2(t))$. It covers a part of $\mathcal{C}$, but since $\mathcal{C}$ is irreducible, $\mathcal{C}$ must be the Zariski closure of this part. Moreover, since $\mathcal{C}^\star$ is a component of $\tilde{\mathcal{C}}$ it holds that $f_1(m_1, m_2) = f_2(m_1, m_2) = 0$, and therefore $\mathcal{R}(t) \in \mathbf{R}(t)^2$. Consequently, $\mathcal{C}$ can be parametrized over the reals.

References

[1] Chevalley C. (1951), *Introduction to the theory of algebraic functions of one variable.* Mathematical Surveys, VI. A.M.S. 1951.

[2] Cox D., Little J., O'Shea D. (1992), *Ideals, varieties and algorithms (An Introduction to Computational Algebraic Geometry and Commutative Algebra).* Springer Verlag.

[3] Hilbert D., Hurwitz A. (1890), *Über die Diophantischen Gleichungen vom Geschlecht Null.* Acta math. **14**, 217-224.

[4] Jacobson N. (1974), *Basic Algebra I, II.* W.H. Freeman and Company.

[5] Sendra J.R., Winkler F. (1991), *Symbolic Parametrization of Curves.* J. Symbolic Computation **12/ 6**, 607-631.

[6] Sendra J.R., Winkler F. (1994), *Optimal Parametrization of Algebraic Curves.* Techn. Rep. RISC 94-65, Research Inst. Symb. Comp., Univ. Linz.

[7] Shafarevich I.R., *Basic Algebraic Geometry I,II.* Springer Verlag, sec. edition (1994).

Dpto. de Matemáticas
Universidad de Cantabria
Santander 39071 (Spain)
recio@matsun1.unican.es

Dpto. de Matemáticas
Universidad de Alcalá
Madrid 28871 (Spain)
mtsendra@alcala.es