ARAB JOURNAL OF
MATHEMATICAL SCIENCES

Arab J Math Sci **19**(2) (2013), 145–149

The Lüroth semigroups of a curve over a non-algebraically closed field

E. BALLICO *
Dept. of Mathematics, University of Trento, 38123 Povo (TN), Italy

Received 1 October 2011; revised 29 December 2012; accepted 15 January 2013
Available online 30 January 2013

Abstract. Let $C \subset \mathbb{P}^2$ be a smooth curve defined over a non-algebraically closed field $\boldsymbol{K}$. We study the Lüroth semigroups of $\boldsymbol{C}$ over $\boldsymbol{K}$, i.e. the set $\boldsymbol{L'(C,K)}$ of all degrees of finite morphisms $C \to \mathbb{P}^1$ defined over $\boldsymbol{K}$ and the set $\boldsymbol{L(C,K)}$ of all degrees >0 of some spanned line bundle on $\boldsymbol{C}$ defined over $\boldsymbol{K}$. If $\boldsymbol{K}$ is infinite, then $\boldsymbol{L'(C,K)} = \boldsymbol{L(C,K)}$, but for every prime power $\boldsymbol{q} \neq 2$ there is a smooth plane curve $\boldsymbol{C}$ defined over $\mathbb{F}_q$ with $L'(C,\mathbb{F}_q) \subseteq L(C,\mathbb{F}_q)$ and $C(\mathbb{F}_q) \neq \emptyset$. If $\boldsymbol{C}$ is a smooth plane curve, then $\boldsymbol{L(C,K)}$ determines (in several ways) if $\boldsymbol{C(K)} \neq \emptyset$.

Mathematics Subject Classification: 14H50; 14G25

Keywords: Lüroth semigroup; Plane curve; Curve over a finite field; Non-algebraically closed field

1. INTRODUCTION AND MAIN THEOREM

Let C be a smooth and geometrically connected projective curve defined over a field K. Let $\overline{K}$ denote the algebraic closure of K. For any field $E \supseteq K$ let $C(E)$ be the set of all points of C defined over the field E. If $C \subset \mathbb{P}^2$ is a smooth plane curve defined by a homogeneous equation $f \in K[x_0,x_1,x_2]$, then $C(E) := \{(a_1, a_2, a_3) \in \mathbb{P}^2(E) : f(a_1, a_2, a_3) = 0\}$. The Lüroth semigroup $L(C)$ of C (or of $C(\overline{K})$) is the set of all positive integers k such that there is a degree k morphism $f : C \to \mathbb{P}^1$ defined over $\overline{K}$, i.e. the set of all positive integers k such that there is a spanned $L \in \mathrm{Pic}^k(C)(\overline{K})$ [2–4]. If we impose that L is defined over K, then we get the definition of the K-Lüroth semigroup $L(C,K)$

* Tel.: +39 0461281646; fax: +39 04611624.
E-mail address: ballico@science.unitn.it

Peer review under responsibility of King Saud University.

ELSEVIER Production and hosting by Elsevier

http://dx.doi.org/10.1016/j.ajmsc.2013.01.002

of C. If we impose the condition that f is defined over K, then we get another semigroup $L'(C,K) \subseteq L(C)$. It is easy to check that $L'(C,K) \subseteq L(C,K)$ (Lemma 2). Obviously $L'(C,K) = L(C,K)$ if K is algebraically closed. We prove that $L'(C,K) = L(C,K)$ if K is infinite (Proposition 1).

For any finite field $\mathbb{F}_q \neq \mathbb{F}_2$ we give an example with $L'(C, \mathbb{F}_q) \subsetneq L(C, \mathbb{F}_q)$ and $C(\mathbb{F}_q) \neq \emptyset$. This example is the key point of this note. In the example the curve is a smooth plane curve of degree $q + 2$.

The first element gon(C,K) of $L'(C,K)$ is often called the K-gonality of C or the gonality of C over K [7]. Since $L'(C,K) = L(C,K)$ if K is infinite, gon(C,K) is also the first element of $L(C,K)$ if K is infinite. Over a finite field $\mathbb{F}_q$ we prove that gon$(C, \mathbb{F}_q)$ is the first element of $L(C, \mathbb{F}_q)$ if $C(\mathbb{F}_q) \neq \emptyset$ (see Proposition 2). Obviously $L'(C, E) = L(C, E) = L'(C, \overline{K}) = L(C, \overline{K}) = L(C)$ for any field $E \supseteq \overline{K}$.

Concerning smooth plane curves we prove the following result.

Theorem 1. *Let $C \subset \mathbb{P}^2$ be a degree $d \geqslant 4$ smooth plane curve defined over a field K. The following conditions are equivalent:*

(a) $C(K) = \emptyset$.
(b) $d - 1 \notin L(C,K)$.
(c) *gon*$(C,K) \neq d - 1$.
(d) *d is the first element of $L(C,K)$.*
(e) *there in an integer x such that $1 \leqslant x < \lfloor \sqrt{d} \rfloor$ and $xd - 1 \notin L(C,K)$.*
(f) *we have $xd - 1 \notin L(C,K)$ for every integer x such that $1 \leqslant x < \lfloor \sqrt{d} \rfloor$.*

If $C(K) \neq \emptyset$, then $xd - 1 \in L(C,K)$ for all $x \geqslant 1$ (see the last part of the proof of Theorem 1). The bound $x < \lfloor \sqrt{d} \rfloor$ in (e) and (f) comes from the application of a theorem of Max Noether [5, Theorem 2.1], [1, Theorem 3.2.1] on plane curves (see Lemma 1 and the proof of Theorem 1). The numerical bounds in Noether's theorem are sharp.

We thank the referees for their precious job.

2. Proof of Theorem 1 and the other results

Lemma 1. *Let $C \subset \mathbb{P}^2$ be a degree $d \geqslant 4$ smooth plane curve defined over a field K. Fix positive integers x,e such that $e < (x + 1)(d - x - 1)$ and $e \geqslant xd - d + 2$. If $e \in L(C,K)$, then $xd \geqslant e$ and there is a degree $xd - e$ effective divisor on C defined over K.*

Proof. Fix a degree e spanned line bundle L on C defined over K and any effective divisor E defined over K and with $L \cong \mathcal{O}_C(E)$. Since $e < (x + 1)(d - x - 1)$, we have $h^0(C, \mathcal{O}_C(x)(-E)) \neq 0$ ([1], first line of the proof of Theorem 3.2.1). Since C is a smooth plane curve, $d - 1$ is the first element of $L(C)$ ([5, Theorem 2.1]; see [2] for the computation of $L(C)$). Since $\deg(\mathcal{O}_C(x)(-E)) = xd - e \leqslant d - 2$, we have $h^0(C, \mathcal{O}_C(x)(-E)) = 1$, i.e. there is a unique effective divisor $Z \subset C$ such that $\mathcal{O}_C(Z) \cong \mathcal{O}_C(x)(-E)$. Since E and $\mathcal{O}_C(x)$ are defined over K, Z is defined over K. □

The thesis "there is a degree $xd - e$ effective divisor on C defined over K" in Lemma 1 is a statement concerning the structure of $C(F)$ for some finite field extensions F of K. For instance, if $x = 1$, it says that if $d \geqslant 9$ and $2d - 1 \in L(C,K)$, then $C(K) \neq \emptyset$. If $d \geqslant 8$ and $2d - 2 \in L(C,K)$, the case $x = 2$ and $e = 2d - 2$ of Lemma 1 gives the existence of a degree 2 effective divisor Z of C defined over K. If either $\mathrm{char}(K) \neq 2$ or K is perfect, then either $Z = 2P$ for some $P \in C(K)$ or there is a degree 2 Galois extension F of K such that $Z = P + \sigma(P)$ with $P \in C(F)\backslash C(K)$ and $\sigma{:}F \to F$ the non-trivial automorphism of F over K. Hence either $C(K) \neq \emptyset$ or there is a quadratic extension F of K with $\sharp(C(F)) \geqslant 2$.

Proof of Theorem 1. The line bundle $\mathcal{O}_C(1)$ is a degree d spanned line bundle defined over any field containing K. Hence $td \in L(C,K)$ for all integers $t \geqslant 1$. We recall that $\mathrm{gon}(C) = d - 1$ and that any pencil computing the gonality of C over the algebraically closed field $\overline{K}$ is of the form $\mathcal{O}_C(1)(-P)$ with P a uniquely determined element of $C(\overline{K})$ ([5, Theorem 2.1]; if $d \geqslant 6$, then use [1], case $\delta = 0$, i.e. C smooth and $e \leqslant d - 1$; if $d = 4$, then use $\omega_C \cong \mathcal{O}_C(1)$ and Riemann–Roch). Since $\mathcal{O}_C(1)$ is defined over K, the line bundle $\mathcal{O}_C(1)(-P)$ is defined over K if and only if $P \in C(K)$. Hence (a), (b), (c) and (d) are equivalent.

Fix an integer x such that $1 \leqslant x < \lfloor\sqrt{d}\rfloor$. Since $(x + 1)^2 \leqslant d$, we have $xd - 1 < (x + 1)(d - x - 1)$. The case $e = xd - 1$ of Lemma 1 shows that (a) implies (f). Obviously (f) implies (e). Now assume $C(K) \neq \emptyset$. Fix $P \in C(K)$ and an integer $x \geqslant 1$. Since $\mathcal{O}_C(x)$ is very ample, the line bundle $\mathcal{O}_C(x)(-P)$ is spanned. Hence (e) implies (a). □

Lemma 2. *Let C be a smooth and geometrically connected curve defined over a field K. Then $L'(C,K) \subseteq L(C,K)$.*

Proof. Fix a positive integer d and a degree d morphism $f : C \to \mathbb{P}^1$ defined over K. Since $\mathcal{O}_{\mathbb{P}^1}(1)$ is a degree 1 spanned line bundle defined over K, $f^*(\mathcal{O}_{\mathbb{P}^1}(1))$ is a degree d spanned line bundle on C defined over K. □

Proposition 1. *Let C be a smooth and geometrically connected curve defined over an infinite field K. Then $L'(C,K) = L(C,K)$.*

Proof. By Lemma 2 it is sufficient to prove the inclusion $L'(C,K) \supseteq L(C,K)$. Fix a positive integer $d \in L(C,K)$ and take a spanned $R \in \mathrm{Pic}^d(C)(K)$. Set $r := h^0(C,R) - 1$. Since R is spanned and defined over K, the complete linear system $|R|$ induces a morphism $f : C \to \mathbb{P}^r$ defined over K and with $\deg(f) \cdot \deg(f(C)) = d$. If $r = 1$, then we are done. Hence we may assume $r \geqslant 2$. Let $G(r - 2,r)$ be the Grassmannian of all $(r - 2)$-dimensional linear subspaces of $\mathbb{P}^r$. Since $G(r - 2,r)$ is a K-rational variety and K is infinite, $G(r - 2,r)(K)$ is Zariski dense in $G(r-2,r)(\overline{K})$. Set $\Omega := \{V \in G(r-2,r)(\overline{K}) : V \cap f(C)(\overline{K}) = \emptyset\}$. Ω is a non-empty open subset of $G(r - 2,r)$ defined over K, because $f(C)$ is defined over K. Hence $\Omega(K) \neq \emptyset$. Composing f with the linear projection from any $V \in \Omega(K)$ we obtain a degree d morphism $\psi : C \to \mathbb{P}^1$ defined over K. □

Example 1. Fix a prime power $q > 2$. There is a smooth degree $q + 2$ curve $C \subset \mathbb{P}^2$ defined over $\mathbb{F}_q$ and such that $C(\mathbb{F}_q) = \mathbb{P}^2(\mathbb{F}_q)$ (see [6] for a complete classification of all such curves). The spanned line bundle $\mathcal{O}_C(1)$ gives $q+2 \in L(C, \mathbb{F}_q)$. Let R be any spanned line bundle of degree $q + 2$ on C defined over $\overline{K}$. Since $q > 2$, we have $q + 2 < 2(q + 2 - 2)$. We look at the proof of Lemma 1 with $d = e = q + 2$ and $x = 1$ and get $h^0(C, \mathcal{O}_C(1) \otimes R^\vee) > 0$. Since $\deg(R) = \deg(\mathcal{O}_C(1))$, we get $R \cong \mathcal{O}_C(1)$. Hence the line bundle $\mathcal{O}_C(1)$ is the unique spanned line bundle on C with degree $q + 2$ over any field $E \supseteq \mathbb{F}_q$. Notice that $h^0(C, \mathcal{O}_C(1)) = 3$. Hence there is a bijection between the morphisms $h : C(\overline{\mathbb{F}_q}) \to \mathbb{P}^1(\overline{\mathbb{F}}_q)$ with $\deg(h) = q + 2$ and the two-dimensional linear subspaces $V_h \subset H^0(C, \mathcal{O}_C(1))(\overline{\mathbb{F}}_q) = H^0(\mathbb{P}^2, \mathcal{O}_C(1))(\overline{\mathbb{F}}_q)$ such that V_h spans $\mathcal{O}_C(1)$. Moreover, $h$is defined over $\mathbb{F}_q$ if and only if V_h is defined over $\mathbb{F}_q$. Each two-dimensional linear subspace of $H^0(\mathbb{P}^2, \mathcal{O}_{\mathbb{P}^2}(1))(\overline{\mathbb{F}}_q)$ is uniquely determined by an element of $\mathbb{P}^2(\overline{\mathbb{F}}_q)$ and a linear subspace V is defined over $\mathbb{F}_q$ if and only if the associated point $P_V \in \mathbb{P}^2(\overline{\mathbb{F}}_q)$ is contained in $\mathbb{P}^2(\mathbb{F}_q)$. Since $C(\mathbb{F}_q) = \mathbb{P}^2(\mathbb{F}_q)$, V does not span $\mathcal{O}_C(1)$ at the point $P_V \in C(\mathbb{F}_q)$.

Proposition 2. *Fix a prime power q. Let C be a geometrically connected smooth curve defined over* $\mathbb{F}_q$. *If* $C(\mathbb{F}_q) \neq \emptyset$, *then the first element of* $L(C, \mathbb{F}_q)$ *is the first element,* $\mathrm{gon}(C, \mathbb{F}_q)$, *of* $L'(C, \mathbb{F}_q)$. *Moreover, every spanned* $L \in \mathrm{Pic}(C)(\mathbb{F}_q)$ *such that* $\deg(L) = \mathrm{gon}(C, \mathbb{F}_q)$ *has* $h^0(C,L) = 2$.

Proof. Let d be the first element of $L(C, \mathbb{F}_q)$. Fix $P \in C(\mathbb{F}_q)$ and any spanned $L \in \mathrm{Pic}^d(C)(\mathbb{F}_q)$. To prove all the statements of Proposition 2 it is sufficient to see that $h^0(C,L) = 2$. Since $d > 0$ and L is spanned, we have $h^0(C,L) \geqslant 2$. Assume $a{:=}h^0(C,L) \geqslant 3$. Since L is spanned, we have $h^0(C,L(-P)) = a - 1 \geqslant 2$. Let R be the subsheaf of $L(-P)$ spanned by $H^0(C,L(-P))$. Since $h^0(C,L(-P)) \geqslant 2$, R is a positive degree spanned line bundle. Since L and P are defined over $\mathbb{F}_q$, $L(-P)$ is defined over $\mathbb{F}_q$. Hence the vector space $H^0(C,L(-P))$ is defined over $\mathbb{F}_q$. Hence R is defined over $\mathbb{F}_q$. Since $\deg(R) \leqslant a - 1 < a$, we obtained a contradiction. □

Acknowledgements

The author was partially supported by MIUR and GNSAGA of INdAM (Italy).

References

[1] M. Coppens, Free linear systems on integral Gorenstein curves, J. Algebra 145 (1992) 209–218.
[2] M. Coppens, The existence of base point free linear systems on smooth plane curves, J. Algebraic Geom. 4 (1) (1995) 1–15.
[3] S. Greco, G. Raciti, The Lüroth semigroup of plane algebraic curves, Pacific J. Math. 151 (1) (1991) 43–56.
[4] S. Greco, G. Raciti, Gap orders of rational functions on plane curves with few singular points, Manuscripta Math. 70 (4) (1991) 441–447.
[5] R. Hartshorne, Generalized divisors on Gorenstein curves and a theorem of Noether, J. Math. Kyoto Univ. 26 (1986) 375–386.

[6] M. Homma, S.J. Kim, Nonsingular plane filling curves of minimum degree over a finite field and their automorphism groups: supplement to a work of Tallini, Linear Algebra Appl. 438 (2013) 969–985.
[7] R. Pellikaan, On the gonality of curves, abundant codes and decoding, in: Coding theory and algebraic geometry (Luminy, 1991), Lecture Notes in Math. vol. 1518, Springer, Berlin, 1992, pp. 132–144.