

## IMAGES OF POLYNOMIAL MAPS ON AMPLE FIELDS

MICHIEL KOSTERS

**Abstract:** In this article we study the following problem. Let  $k$  be an infinite field and let  $f \in k[x]$ . Consider the evaluation map  $f_k : k \rightarrow k$ . Assume that  $f_k$  is not surjective. Is  $k \setminus f_k(k)$  infinite? We give a positive answer to this question when  $k$  is a perfect ample field. In fact, we prove that  $|k \setminus f_k(k)| = |k|$ . This conclusion follows from a similar statement about finite morphisms between normal projective curves over perfect ample fields.

**Keywords:** ample field, large field, polynomial map, surjective, valuation theory, curve.

### 1. Introduction

#### 1.1. Problem and results

A very natural problem is the following one.

**Problem 1.** Let  $k$  be an infinite field and let  $f \in k[x]$ . Consider the evaluation map  $f_k : k \rightarrow k$ . Assume that  $f_k$  is not surjective. Is  $k \setminus f_k(k)$  infinite?

This question was asked by Philipp Lampe on mathoverflow as Question 6820 in 2009. The problem is still unsolved in general. It is not hard to see that the problem has a positive answer when  $k$  is Hilbertian. Number fields are for example Hilbertian. Some other cases can be handled using topological arguments. In this article we will positively answer this problem for perfect ample fields. Our proof relies on valuation theory. Let us first define what a ample field is following [5].

**Definition 1.1.** A field  $k$  is called *ample* if every irreducible  $k$ -curve  $C$  with a  $k$ -rational smooth point has infinitely many  $k$ -points. In literature one often uses the word *large* instead of ample.

Note that ample fields are infinite. For more information on ample fields see the survey [5]. Some examples of ample fields are  $\mathbf{R}$ ,  $\mathbf{Q}_p$  ( $p$  prime),  $l((t))$  (where  $l$  is

---

This article is part of my PhD thesis written under the supervision of Hendrik Lenstra at the Universiteit Leiden. I would also like to thank the anonymous referee for his comments.

**2010 Mathematics Subject Classification:** primary: 12J10; secondary: 11R58

a field), infinite algebraic extensions of finite fields. Furthermore, finite extensions of ample fields are ample. In the definition of ample field we can replace the word smooth by normal if  $k$  is perfect [4, Corollary 4.3.33 and Lemma 8.2.21].

Problem 1 is also motivated by the case when  $k$  is a finite field. Let  $k$  be a finite field and let  $f \in k[x]$  be a non constant polynomial. Assume that the evaluation map  $f_k : k \rightarrow k$  is not surjective. Then one has  $|k \setminus f_k(k)| \geq \frac{|k|-1}{\deg(f)}$  ([7]). This result seems to suggest a positive answer to the problem when  $k$  is an infinite algebraic extension of a finite field, although the author does not know how to use the aforementioned result to prove this.

Our main theorem is the following (we follow [4] for the definition of a normal projective curve).

**Theorem 1.2.** *Let  $k$  be a perfect ample field. Let  $C, D$  be normal projective curves over  $k$ . Let  $f: C \rightarrow D$  be a finite morphism. Suppose that the induced map  $f_k: C(k) \rightarrow D(k)$  is not surjective. Then one has  $|D(k) \setminus f_k(C(k))| = |k|$ .*

The following corollary gives a positive answer to our problem for perfect ample fields, since ample fields are infinite.

**Corollary 1.3.** *Let  $k$  be a perfect ample field. Then the following hold.*

- i. *Let  $f \in k(x)$  such that the induced map  $f_k: \mathbf{P}_k^1(k) \rightarrow \mathbf{P}_k^1(k)$  is not surjective. Then one has  $|\mathbf{P}_k^1(k) \setminus f_k(\mathbf{P}_k^1(k))| = |k|$ .*
- ii. *Let  $f \in k[x]$  such that the induced evaluation map  $f_k: k \rightarrow k$  is not surjective. Then one has  $|k \setminus f_k(k)| = |k|$ .*

We do not know how to prove Theorem 1.2 or Corollary 1.3 when  $k$  is not perfect.

## 1.2. Strategy

As mentioned before, the proof of Theorem 1.2 relies on valuation theory. More specifically, it relies on a Galois theoretic approach to valuation theory.

We will sketch the proof of 1.3i when  $k$  is an infinite algebraic extension of a finite field, where we exclude some of the ramification issues. Let  $f \in k(x)$  and consider the map  $f_k: \mathbf{P}_k^1(k) \rightarrow \mathbf{P}_k^1(k)$  which is assumed to be non surjective. This map  $f_k$  corresponds to an extension of function fields  $L = k(x) \supseteq K = k(f(x))$ . We use Galois theory to study the extension  $L/K$ . Suppose  $M/K$  is finite normal with group  $G = \text{Aut}_K(M)$  such that the  $G$ -set  $X = \text{Hom}_K(L, M)$  of  $K$ -embeddings of  $L$  in  $M$  is not empty. To a rational places (or prime divisors)  $P$  of  $K$  we can associate a Frobenius element  $(P, M) \in G$  up to conjugation. For a rational places  $P$  of  $K$  the number of rational places above it in  $L$  is equal to  $\#X^{(P, M)}$ , the number of points of  $X$  which are fixed by  $(P, M)$ . A rational place  $P$  of  $K$  has no rational places above it in  $L$  iff  $X^{(P, M)} = \emptyset$ . Suppose that this is the case for a rational place  $P'$  of  $K$ . Hence it is enough to show that there are infinitely many rational points  $Q$  of  $K$  with  $(Q, M) = (P', M)$ . We parametrize the set of such  $Q$  by the set of rational places of some geometrically irreducible curve over  $k$ . Such a curve, by Hasse-Weil, has infinitely rational places. Hence the result follows.

In the general case, one needs to make one conceptual adjustment: the concept of a Frobenius element is replaced by the splitting of an exact sequence from valuation theory.

## 2. Prerequisites

In this section we will give some of the prerequisites on a Galois theoretic approach to valuation theory and give the connection with curves. Furthermore, this section is used to fix some notation. Most statements in this section are well-known, except for possibly Theorem 2.4ii and Proposition 2.5.

### 2.1. Valuations and curves

**Definition 2.1.** Let  $K$  be a field. Then a *valuation ring* on  $K$  is a subring  $\mathcal{O}$  of  $K$  such that for all  $x \in K^*$  one has  $x \in \mathcal{O}$  or  $x^{-1} \in \mathcal{O}$ .

Such a valuation ring is a local ring and it is integrally closed in  $K$ . Instead of writing  $\mathcal{O}$  for a valuation ring, we often view a valuation ring as a point  $P$ , with corresponding valuation ring  $\mathcal{O}_P$ , maximal ideal  $\mathfrak{m}_P$  and residue field  $k_P$ . We say that  $(K, P)$  is a valued field.

Let  $(K, P)$  be a valued field. Let  $L$  be a field extension of  $K$ . A valuation  $Q$  on  $L$  is an extension of  $P$  if  $\mathcal{O}_Q \cap K = \mathcal{O}_P$ . We denote such an extension by  $(K, P) \subseteq (L, Q)$ . Such an extension is called finite (Galois, normal, ...) if  $L/K$  is finite (Galois, normal, ...).

**Definition 2.2.** Let  $k$  be a field. A *function field* over  $k$  is a finitely generated field extension of  $k$  of transcendence degree 1.

A morphism between two function fields  $K$  and  $L$  over  $k$  is a  $k$ -algebra morphism  $\tau : K \rightarrow L$  such that  $L/\tau(K)$  is a finite field extension.

**Theorem 2.3.** *There is an anti-equivalence of categories between the category of normal projective curves over  $k$  with finite morphisms and the category of function fields over  $k$ . This equivalence maps a curve  $C$  to its function field  $k(C)$  and a finite morphism  $C \rightarrow D$  to the induced inclusion  $k(D) \subseteq k(C)$ .*

**Proof.** See [4, Proposition 7.3.13, Remark 7.3.14]. ■

Let  $C$  be a normal projective curve over a field  $k$ . Each closed point  $P$  gives rise to a valuation ring on  $k(C)$  which contains  $k$  but is not equal to  $k(C)$ , namely its stalk  $\mathcal{O}_P$ . Conversely, every such valuation ring corresponds to a point. This also motivates our notations for valuation rings. The set of such valuation rings is denoted by  $\mathcal{P}_{K/k}$ . We let  $\mathcal{P}_{K/k}^1 \subseteq \mathcal{P}_{K/k}$  be the subset consisting of valuation ring  $P$  which satisfy  $k_P = k$ . When  $K = k(C)$ , the set  $\mathcal{P}_{K/k}^1$  corresponds to  $C(k)$ .

## 2.2. Galois theory of valuations

We refer to [3] for a Galois theoretic approach to valuation theory. We recall some of the important statements.

Let  $K$  be a field with valuation  $P$  and let  $M$  be a normal extension of  $K$  with group  $G = \text{Aut}_K(M)$ . Let  $Q$  be an extension of  $P$  to  $M$ . Set  $D_{Q,K} = \{g \in G : gQ = Q\}$  (decomposition group). Note that we have a natural map  $D_{Q,K} \rightarrow \text{Aut}_{k_P}(k_Q)$ . The kernel of this map is called the *inertia group* and is denoted by  $I_{Q,K}$ .

The following theorem summarizes the results from general valuation theory which we need later on.

**Theorem 2.4.** *Let  $L$  be an intermediate extension of  $M/K$ . The following hold:*

- i. *The set of valuation rings extending  $P$  to  $M$  is not empty and the group  $G$  acts transitively on this set.*
- ii. *The sequence*

$$0 \rightarrow I_{Q,K} \rightarrow D_{Q,K} \rightarrow \text{Aut}_{k_P}(k_Q) \rightarrow 0$$

*is exact. It is right split as topological groups if  $k_Q$  is algebraically closed.*

- iii. *One has  $D_{Q,L} = \text{Aut}_L(M) \cap D_{Q,K}$  and  $I_{Q,L} = \text{Aut}_L(M) \cap I_{Q,K}$ .*
- iv. *If  $L/K$  is normal, then the maps  $D_{Q,K} \rightarrow D_{Q|L,K}$  and  $I_{Q,K} \rightarrow I_{Q|L,K}$  are surjective.*

**Proof.** i: See [3, Proposition 5.6].

ii: See [3, Theorem 3.8 iii].

iii: Follows directly from the definitions.

iv: See [3, Theorem 3.6]. ■

Let  $H$  be a group acting on a set  $X$ . Then by  $H \backslash X$  we denote the set of orbits of this action. For a subset  $S \subseteq H$  we denote by  $X^S = \{x \in X : \forall s \in S, s(x) = x\}$  the set of points which are fixed by  $S$ .

One of the reasons for assuming that  $k$  is perfect in our main theorem in the following proposition.

**Proposition 2.5.** *Let  $(K, P)$  be a valued field and let  $L$  be a finite algebraic extension of  $K$ . Assume that  $k_P$  is perfect. Let  $(M, Q) \supseteq (K, P)$  be a finite normal extension of valued fields with group  $G = \text{Aut}_K(M)$  such that the  $G$ -set  $X = \text{Hom}_K(L, M)$  is not empty. Then the cardinality of the set of valuation rings  $P'$  on  $L$  extending  $P$  such that  $k_{P'} = k_P$  is equal to  $\#(I_{Q,K} \backslash X)^{D_{Q,K}/I_{Q,K}}$ .*

**Proof.** Note that  $I_{Q,K}$  acts on  $X$ . The set of orbits is denoted by  $I_{Q,K} \backslash X$ . The group  $D_{Q,K}/I_{Q,K}$  naturally acts on  $I_{Q,K} \backslash X$ . See [3, Corollary 3.18] for the proof. ■

### 2.3. Function fields and ramification

**Proposition 2.6.** *Let  $K$  be a function field over a perfect field  $k$ . Let  $\bar{k}$  be an algebraic closure of  $k$  in an algebraic closure of  $K$ . The following hold:*

- i. *Let  $M/K$  be a finite normal extension. Then only finitely many primes  $P \in \mathcal{P}_{K/k}$  have an extension  $Q \in \mathcal{P}_{M/k}$  with the property that  $I_{Q,K} \neq 0$ .*
- ii. *For all primes  $Q \in \mathcal{P}_{\bar{k}K/\bar{k}}$  one has  $I_{Q,K} = 0$ . Furthermore, if  $k$  is algebraically closed in  $K$  ( $k$  is the full constant field of  $K$ ), then a prime  $P \in \mathcal{P}_{K/k}$  has a unique extension to  $\mathcal{P}_{\bar{k}K/\bar{k}}$  if and only if  $P \in \mathcal{P}_{K/k}^1$ .*

**Proof.** i. Since valuation extend uniquely in purely inseparable field extensions, we may assume that  $M/K$  is Galois. In that case, the statement is well-known: only finitely many primes ramify.

ii. This follows from [6, Theorem 3.6.3]. ■

### 3. Proofs of the theorems

**Definition 3.1.** Let  $K$  be a function field over a field  $k$  and let  $P \in \mathcal{P}_{K/k}^1$ . Let  $\bar{K}$  be an algebraic closure of  $K$ . Let  $M/K$  be a normal extension of  $K$  inside  $\bar{K}$  with group  $G = \text{Aut}_K(M)$ . Let  $\bar{k}$  be the algebraic closure of  $k$  inside  $\bar{K}$ . Set  $\Gamma = \text{Aut}_k(\bar{k})$ . Let  $Q$  be an extension of  $P$  to  $M$ . A *Frobenius map* for  $Q/P$  is a continuous morphism  $\varphi: \Gamma \rightarrow G$  such that the diagram, where  $N = \text{Aut}(M/M \cap (\bar{k}K))$  and  $\pi$  and  $\psi$  are the restriction maps,

$$\begin{array}{ccc}
 \Gamma & \xrightarrow{\varphi} & G \\
 & \searrow \psi & \downarrow \pi \\
 & & \text{Aut}(\bar{k} \cap M/k) \cong \text{Aut}((M \cap (\bar{k}K))/K) =: G/N
 \end{array}$$

commutes and such that  $\text{im}(\varphi) I_{Q,K} = D_{Q,K}$ . The set of all such Frobenius maps is denoted by  $\text{Frob}(Q/P)$ .

For the next proposition and lemma assume that  $M/K$  is a normal extension of function fields over a perfect field  $k$  inside  $\bar{K}$ . Let  $G = \text{Aut}_K(M)$ . Let  $P \in \mathcal{P}_{K/k}^1$  with  $Q$  above it in  $M$ .

Suppose  $\varphi \in \text{Frob}(Q/P)$ . We use the notation as in the definition of a Frobenius map. Consider  $\text{Graph}(\varphi) = \{(\gamma, \varphi(\gamma)) : \gamma \in \Gamma\} \subseteq \Gamma \times_{G/N} G = \text{Aut}(\bar{k}M/K)$ , which is a closed subgroup. Set  $M^\varphi = (\bar{k}M)^{\text{Graph}(\varphi)}$ . Note that  $M^\varphi/K$  is a finite extension. Furthermore, since  $k$  is perfect,  $k$  is integrally closed in  $M^\varphi$  ( $k$  is the full constant field of  $M^\varphi$ ). Finally, we have  $\bar{k}M^\varphi = \bar{k}M$ . We have the following



Let  $M$  be a finite normal extension of  $K$  such that  $X = \text{Hom}_K(L, M) \neq \emptyset$ . Assume  $P \in \mathcal{P}_{K/k}^1$ ,  $P \notin \text{im}(f_k)$ . Let  $Q$  be an extension of  $P$  to  $M$ . Let  $\varphi \in \text{Frob}(Q/P)$  with  $\mathcal{P}_{M^\varphi/k}^1 \neq \emptyset$  (Proposition 3.2). Since  $k$  is an ample field, one has  $|\mathcal{P}_{M^\varphi/k}^1| = |k|$  ([2, Proposition 5.4.3]). Note that we have  $\text{im}(\varphi)I_{Q,K} = D_{Q,K}$ . As  $P \notin \text{im}(f_k)$  we conclude from Proposition 2.5 that  $(I_{Q,K} \setminus X)^{D_{Q,K}/I_{Q,K}} = \emptyset$ . This implies  $X^{\text{im}(\varphi)} = \emptyset$ . Consider the restriction map  $\rho: \mathcal{P}_{M^\varphi/k}^1 \rightarrow \mathcal{P}_{K/k}^1$ . Let  $T$  be the set of  $P_0 \in \text{im}(\rho)$  such that for any extension  $Q_0$  of  $P_0$  to  $M$  one has  $I_{Q_0,K} = 1$ . Then  $T$  has cardinality  $|k|$  as well (Proposition 2.6i, Theorem 2.4i). For  $P_0 \in T$  there is a prime  $Q_0$  of  $M$  above  $P_0$  with  $\text{im}(\varphi) = D_{Q_0,K}$  (Lemma 3.3). We find

$$(I_{Q_0,K} \setminus X)^{D_{Q_0,K}/I_{Q_0,K}} = X^{D_{Q_0,K}} = X^{\text{im}(\varphi)} = \emptyset.$$

From Proposition 2.5 we conclude that  $P_0 \notin \text{im}(f_k)$ . This finishes the proof.  $\blacksquare$

**Proof of Corollary 1.3.** i: The statement is true if  $f$  is constant. Assume  $f \in k(x)$  is not constant. Then  $f$  induces a finite morphism  $\mathbf{P}_k^1 \rightarrow \mathbf{P}_k^1$  and we apply Theorem 1.2.

ii: This follows from i, since the map sends the point at infinity to the point at infinity.  $\blacksquare$

**Remark 3.4.** In the proof of Theorem 1.2 one can reduce directly to the case that the finite morphism  $C \rightarrow D$  is separable. Indeed, one can decompose  $C \rightarrow D$  into a map  $C \rightarrow C' \rightarrow D$ , with  $C \rightarrow C'$  purely inseparable and  $C' \rightarrow D$  separable, by field theory. Consider the map  $C(k) \rightarrow C'(k)$ . Since  $k$  is perfect, this map is a bijection and hence we only need to consider the finite separable map  $C' \rightarrow D$ . We did not include this from the beginning because we hope that our slightly more general approach one day might lead to a proof when  $k$  is not perfect.

**Remark 3.5.** One can also imagine a strategy to prove Corollary 1.3ii using the following equivalent definition of ample fields from [2, Lemma 5.3.1]:  $k$  is an ample field if and only if  $k$  is existentially closed in  $k((T))$ . This approach was suggested in [1], following ideas of Koenigsmann.

## References

- [1] L. Bary-Soroker, A. Fehm, *Open problems in the theory of ample fields*, in Geometric and differential Galois theories, vol. 27 of Sémin. Congr. Soc. Math. France, Paris, 2013, 1–11.
- [2] M. Jarden, *Algebraic Patching*, Springer Monographs in Mathematics. Springer, Heidelberg, 2011.
- [3] M. Kusters, *The algebraic theory of valued fields*, <http://arxiv.org/abs/1404.3916>, 2014, preprint.
- [4] Q. Liu, *Algebraic geometry and arithmetic curves*, vol. 6 of Oxford Graduate Texts in Mathematics, Oxford University Press, Oxford, 2002; translated from the French by Reinie Ern e, Oxford Science Publications.

- [5] F. Pop, *Little survey on large fields*, [http://www.math.upenn.edu/~pop/Research/files-Res/LF\\_6Oct2013.pdf](http://www.math.upenn.edu/~pop/Research/files-Res/LF_6Oct2013.pdf), 2013.
- [6] H. Stichtenoth, *Algebraic function fields and codes*, second ed., vol. 254 of Graduate Texts in Mathematics, Springer-Verlag, Berlin, 2009.
- [7] D.Q. Wan, *A  $p$ -adic lifting lemma and its applications to permutation polynomials*, in Finite fields, coding theory, and advances in communications and computing (Las Vegas, NV, 1991), vol. 141 of Lecture Notes in Pure and Appl. Math. Dekker, New York, 1993, pp. 209–216.

**Address:** Michiel Kusters: 340 Rowland Hall, University of California, Irvine, Irvine, CA 92697-3875.

**E-mail:** [kusters@gmail.com](mailto:kusters@gmail.com)

**Received:** 10 December 2014; **revised:** 19 November 2015