Finite Fields and Their Applications 50 (2018) 366–371

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Geometrically nilpotent subvarieties

Alexander Borisov

Department of Mathematical Sciences, Binghamton University, 4400 Vestal Parkway East, Binghamton, NY 13902-6000, USA

A R T I C L E   I N F O

Article history:
Received 25 May 2015
Received in revised form 4 September 2017
Accepted 20 December 2017
Available online 4 January 2018
Communicated by Michael Tsfasman

MSC:
primary 37P25
secondary 37P05, 14G15, 11G25

Keywords:
Polynomial map
Reduction
Iteration

A B S T R A C T

We construct some examples of polynomial maps over finite fields that admit subvarieties with a peculiar property: every geometric point is mapped to a fixed point by some iteration of the map, while the whole subvariety is not. Several related open questions are stated and discussed.

1. Introduction

Suppose X is a variety defined over a finite field F, and $T : X \to X$ is a morphism, defined over F. Then for every finite extension K of F the map T induces a map T_K on the set of K-points of X. These maps commute with the action of the Galois group of K over F and the iterations of these maps are induced by the iterations of T.

Note on the terminology. Every geometric point of X, i.e. a Spec(F)-morphism from Spec(F^{alg}) to X, factors through Spec(K) for some K. Because of that, we will call

E-mail address: borisov@math.binghamton.edu.

https://doi.org/10.1016/j.ffa.2017.12.009
1071-5797/

K-points geometric points, when we do not want to specify K. The absolute Galois group of F acts on the set of geometric points of X, and the orbits are exactly the closed scheme points of X. We prefer to work with the geometric points rather than with the closed scheme points because they are somewhat easier to visualize, especially if X is the affine space $\mathbb{A}^n$. However, most of our results can be recast with the closed scheme points in place of the geometric points.

The case when X is the affine space is indeed of special interest. Here the morphism T is usually called a polynomial map. It is given by n polynomials in n variables with coefficients in F. One particular source of these maps is reduction modulo p of integer polynomial maps. Such maps have been studied extensively in special cases, often in connection with factorization algorithms and cryptology. Generally speaking, this is an area of many questions and few complete answers [1,2,5].

In particular, it is interesting to ask when T_K is nilpotent (i.e. some power of it sends the entire set K^n to a single point). This is obviously true for every K if the morphism T itself is nilpotent (i.e. some power of it sends X to a single point). The following theorem is an almost immediate corollary of the density theorem of Borisov and Sapir [3].

Theorem 1. *Suppose T is a polynomial map defined over a finite field F. Then T_K is nilpotent for all K if and only if T is nilpotent.*

Proof. The "if" part is obvious. For the converse, suppose V is the Zariski closure of $T^{(n)}(\mathbb{A}^n)$, where $T^{(n)}$ is the n-th iteration of T. Then V is invariant under T, the restriction of T to V is dominant, and periodic geometric points of T (more precisely, quasi-fixed points) are dense in V [3]. Suppose $\dim V \geq 1$. Take any two distinct periodic points on V. Then for any K that contains both of their fields of definition, the map T_K is not nilpotent. $\square$

In contrast to the above mentioned density theorem, one can construct a simple two-variable polynomial map T over integers, such that all of its reductions modulo primes p are dominant morphisms, but the maps $T_{\mathbb{F}_p}$ are nilpotent [2]. Of course, this does not contradict the density theorem: the maps T_K have many periodic points for extensions K of $\mathbb{F}_p$.

The following two definitions are crucial for this paper.

Definition 2. Suppose X is a variety over a finite field F, $T : X \to X$ is defined over F, and Y is a subvariety of X. Then Y is a nilpotent subvariety of X with respect to T if for some point P of X, fixed by T, and some integer $k \geq 1$, $T^{(k)}(Y) = \{P\}$.

Definition 3. Suppose X is a variety over a finite field F, $T : X \to X$ is defined over F, and Y is a subvariety of X. Then Y is a geometrically nilpotent subvariety of X with respect to T if for some point P of X, fixed by T, every geometric point of Y is mapped to P by a sufficiently high (depending on the point!) iteration of T.