Finite Fields and Their Applications 51 (2018) 218–237

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

A group action on multivariate polynomials over finite fields

Lucas Reis [1]

School of Mathematics and Statistics, Carleton University, 1125 Colonel By Drive, Ottawa ON, K1S 5B6, Canada

A R T I C L E   I N F O

Article history:
Received 14 September 2017
Received in revised form 6 January 2018
Accepted 29 January 2018
Available online xxxx
Communicated by Stephen D. Cohen

MSC:
12E20
11T55

Keywords:
Finite fields
Invariant theory
Group action
Multivariate polynomials

A B S T R A C T

Let $\mathbb{F}_q$ be the finite field with q elements, where q is a power of a prime p. Recently, a particular action of the group $\mathrm{GL}_2(\mathbb{F}_q)$ on irreducible polynomials in $\mathbb{F}_q[x]$ has been introduced and many questions concerning the invariant polynomials have been discussed. In this paper, we give a natural extension of this action on the polynomial ring $\mathbb{F}_q[x_1, \ldots, x_n]$ and study the algebraic properties of the invariant elements.

1. Introduction

Let $\mathbb{F}_q$ be a finite field with q elements, where q is a power of a prime p. Any matrix $A \in \mathrm{GL}_2(\mathbb{F}_q)$ induces a natural map on $\mathbb{F}_q[x]$. Namely, if we write $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, given

E-mail address: lucasreismat@gmail.com.

[1] Permanent address: Departamento de Matemática, Universidade Federal de Minas Gerais, UFMG, Belo Horizonte, MG, 30123-970, Brazil.

https://doi.org/10.1016/j.ffa.2018.01.011
1071-5797/

$f(x)$ of degree n we define $A\diamond f = (cx+d)^n f\left(\frac{ax+b}{cx+d}\right)$. It turns out that, when restricted to the set I_n of irreducible polynomials of degree n (for $n \geq 2$), this map is a permutation of I_n and, $\mathrm{GL}_2(\mathbb{F}_q)$ acts on I_n via the compositions $A \diamond f$. This was first noticed by Garefalakis [5]. Recently, this action (and others related) has attracted attention from several authors (see [6], [7] and [8]), and some fundamental questions have been discussed such as the characterization and number of invariant irreducible polynomials of a given degree. The map induced by A preserves the degree of elements in I_n (for $n \geq 2$), but not in the whole ring $\mathbb{F}_q[x]$: for instance, $A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ is such that $A\diamond(x^n - 1) = (x+1)^n - x^n$ has degree at most $n-1$. However, if the "denominator" $cx+d$ is trivial, i.e., $c = 0$ and $d = 1$, the map induced by A preserves the degree of any polynomial and, more than that, is an $\mathbb{F}_q$-automorphism of $\mathbb{F}_q[x]$. This motivates us to introduce the following: let $\mathcal{A}_n := \mathbb{F}_q[x_1, \ldots, x_n]$ be the ring of polynomials in n variables over $\mathbb{F}_q$ and G be the subgroup of $\mathrm{GL}_2(\mathbb{F}_q)$ comprising the elements of the form $A = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$. The set $G^n := \underbrace{G \times \cdots \times G}_{n \text{ times}}$, equipped with the coordinate-wise product induced by G, is a group. The group G^n induces $\mathbb{F}_q$-endomorphisms of $\mathcal{A}_n$: given $\mathbf{A} \in G^n$, $\mathbf{A} = (A_1, \ldots, A_n)$, where $A_i = \begin{pmatrix} a_i & b_i \\ 0 & 1 \end{pmatrix}$, and $f \in \mathcal{A}_n$, we define

$$\mathbf{A} \circ f := f(a_1x_1 + b_1, \ldots, a_nx_n + b_n) \in \mathcal{A}_n.$$

In other words, $\mathbf{A}$ induces the $\mathbb{F}_q$-endomorphism of $\mathcal{A}_n$ given by the substitutions $x_i \mapsto a_ix_i + b_i$. In this paper, we show that this map induced by $\mathbf{A}$ is an $\mathbb{F}_q$-automorphism of $\mathcal{A}_n$ and, in fact, this is an action of G^n on the ring $\mathcal{A}_n$, such that $\mathbf{A} \circ f$ and f have the same *multidegree* (a natural extension of degree in several variables). It is then natural to explore the algebraic properties of the fixed elements. We define $R_{\mathbf{A}}$ as the subring of $\mathcal{A}_n$ comprising the polynomials invariant by $\mathbf{A}$, i.e.,

$$R_{\mathbf{A}} := \{f \in \mathcal{A}_n \mid \mathbf{A} \circ f = f\}.$$

The ring $R_{\mathbf{A}}$ is frequently called the *fixed-point* subring of $\mathcal{A}_n$ by $\mathbf{A}$. The study of the fixed-point subring plays an important role in the *Invariant Theory of Polynomials*. Observe that $R_{\mathbf{A}}$ is an $\mathbb{F}_q$-algebra and a well-known result, due to Emmy Noether, ensures that rings of invariants from the action of finite groups are always finitely generated; for more details, see Theorem 3.1.2 of [1]. In particular, $R_{\mathbf{A}}$ is finitely generated and some interesting questions arise.

- Can we find a minimal generating set $S_{\mathbf{A}}$ for $R_{\mathbf{A}}$? What about the size of $S_{\mathbf{A}}$?
- Is $R_{\mathbf{A}}$ a free $\mathbb{F}_q$-algebra? That is, can $R_{\mathbf{A}}$ be viewed as a polynomial ring in some number of variables?