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

ARTICLE INFO

Article history:
Received 14 September 2017
Received in revised form 6 January 2018
Accepted 29 January 2018
Available online 20 February 2018
Communicated by Stephen D. Cohen

MSC:
12E20
11T55

Keywords:
Finite fields
Invariant theory
Group action
Multivariate polynomials

ABSTRACT

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 $\mathbb{F}_q[x_1, \dots, x_n]$ 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.,

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

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?

Any polynomial is invariant by $\mathbf{A}$ if and only if is invariant by any element of the group $\langle \mathbf{A} \rangle$ generated by $\mathbf{A}$ in G^n. In particular, we can explore the fixed-point subring for any subgroup H of G^n. For $n = 1$, the equality $\mathbf{A} \circ f = f$ becomes $f(x) = f(ax+b)$ for some $a \in \mathbb{F}_q^*$ and $b \in \mathbb{F}_q$. In other words, we are taking the substitution $x \mapsto ax+b$. It turns out that, with an affine change of variable, we are able to reduce to the cases of translations $x \mapsto x + b$ and the homotheties $x \mapsto ax$. In these cases, the fixed-point subring is well understood and we can easily answer the questions above (see Theorems 2.5 and 3.1 of [7]).

In this paper, we discuss those questions for any $n \geq 1$. We find a minimal generating set $S_{\mathbf{A}}$ for $R_{\mathbf{A}}$ and show that the size of such set is related to the number of some special minimal product-one sequences in the multiplicative group $\mathbb{F}_q^*$. Also, we give necessary and sufficient conditions on the element $\mathbf{A}$ for $R_{\mathbf{A}}$ to be a free $\mathbb{F}_q$-algebra.

The paper is structured as follows. In Section 2, we recall some basic theory of multivariate polynomials over commutative rings and present some preliminary results. Section 3 provides many informations on the set $R_{\mathbf{A}}$, such as a minimal generating set $S_{\mathbf{A}}$ for $R_{\mathbf{A}}$ and conditions to be a free algebra. In Section 4, we find sharp estimates for the size of $S_{\mathbf{A}}$ and, in Section 5, we study the fixed-point subring by the action of H of G^n, where H is any Sylow subgroup of G^n.

2. Preliminaries

Throughout this paper, $\mathcal{A}_n := \mathbb{F}_q[x_1, \ldots, x_n]$ denotes the ring of polynomials in n variables over $\mathbb{F}_q$. Also, for elements $a \in \mathbb{F}_q^*$, $A \in \mathrm{GL}_2(\mathbb{F}_q)$ and $\mathbf{A} \in G^n$, we denote by $\mathrm{ord}(a)$, $\mathrm{ord}(A)$ and $\mathrm{ord}(\mathbf{A})$ the multiplicative orders of a, A and $\mathbf{A}$, respectively.

As mentioned before, the univariate polynomials that remains invariant by the substitution $x \mapsto ax + b$ are well described and, for completeness, we state the results.

Theorem 2.1. *Suppose that f is a polynomial over $\mathbb{F}_q$ and let $a, b \in \mathbb{F}_q$, with $a \neq 0$ and $k = \mathrm{ord}(a)$. The following hold:*

(i) *$f(x + b) = f(x)$ if and only if $f(x) = g(x^p - b^{p-1}x)$ for some $g \in \mathbb{F}_q[x]$.*
(ii) *$f(ax) = f(x)$ if and only if $f(x) = g(x^k)$ for some $g \in \mathbb{F}_q[x]$.*

For the proof of this result, see Theorems 2.5 and 3.1 of [7]. The case $a \neq 1$ and $b \neq 0$ can be reduced to the case $b = 0$. In fact, we have $f(ax + b) = f(x)$ if and only if $f_0(ax) = f_0(x)$, where $f_0(x) = f\left(x - \frac{b}{a-1}\right)$.

From Theorem 2.1, the fixed-point subrings are $\mathbb{F}_q[x^p - b^{p-1}x]$ and $\mathbb{F}_q[y^k]$, where $y = x + \frac{b}{a-1}$ or $y = x$. Clearly, these rings are isomorphic to $\mathbb{F}_q[z]$, the ring of univariate polynomials over $\mathbb{F}_q$. We start with some basic theory on multivariate polynomials over commutative rings. For more details, see Chapter 2 of [2].

Throughout this paper, we always consider the *graded lexicographical* order in $\mathcal{A}_n$, denoted by $<$, such that $x_1 > x_2 > \cdots > x_n$. For a given monomial in $\mathcal{A}_n$, say $x_1^{\alpha_1} \ldots x_n^{\alpha_n}$, we write $\mathbf{X}^\alpha$, where $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$. For convention, $x_i^0 = 1$. Sometimes, we simply write $\mathbf{X}$ or $\mathbf{Y}$ for generic monomials in $\mathcal{A}_n$. It turns out that the graded lexicographical order is induced by the following ordering of the vectors $\alpha \in \mathbb{N}^n$: given two elements $\alpha = (\alpha_1, \dots, \alpha_n)$ and $\alpha' = (\alpha_1', \dots, \alpha_n')$, we have $\alpha > \alpha'$ if and only if $\sum \alpha_i > \sum \alpha_i'$ or $\sum \alpha_i = \sum \alpha_i'$ and the leftmost nonzero coordinate of the difference vector $\alpha - \alpha'$ is positive. In this case, we write $\mathbf{X}^\alpha > \mathbf{X}^{\alpha'}$.

Any nonzero polynomial $f \in \mathcal{A}_n$ can be written uniquely as $\sum_{\alpha \in B} a_\alpha \mathbf{X}^\alpha$ for some nonzero elements $a_\alpha \in \mathbb{F}_q$ and a finite set B.

Definition 2.2. Let f be any nonzero element of $\mathcal{A}_n$. The *multidegree* of f is the maximum α (with respect to the graded lexicographical order) such that $\alpha \in B$.

2.1. A natural action of G^n over $\mathcal{A}_n$

In the following lemma, we observe that the compositions $\mathbf{A} \circ f$ have some basic properties. Its proof follows directly by calculations so we omit the details.

Lemma 2.3. *Given $\mathbf{A}, \mathbf{A}' \in G^n$ and $f, g \in \mathcal{A}_n$, the following hold:*

a) *If f is nonzero, f and $\mathbf{A} \circ f$ have the same multidegree;*
b) *If $\mathbf{I}$ denotes the identity element of G^n, $\mathbf{I} \circ f = f$;*
c) *$(\mathbf{A}'\mathbf{A}) \circ f = \mathbf{A}' \circ (\mathbf{A} \circ f)$ and, in particular, the endomorphism induced by $\mathbf{A}$ is an $\mathbb{F}_q$-automorphism of $\mathcal{A}_n$, with its inverse induced by $\mathbf{A}^{-1}$.*
d) *The automorphism induced by $\mathbf{A}$ on $\mathcal{A}_n$ is of finite order and its order coincides with the order of $\mathbf{A}$ in G^n.*

We observe that, from Lemma 2.3, the group G^n *acts* on $\mathcal{A}_n$ via the compositions $\mathbf{A} \circ f$. From now, $\mathbf{A}$ denotes an element of G^n and the automorphism of $\mathcal{A}_n$ induced by it. The order of the automorphism $\mathbf{A}$ coincides with $\mathrm{ord}(\mathbf{A})$. We observe that the order of any element in G is either p or a divisor of $q-1$. From this fact, we can easily deduce the following lemma.

Lemma 2.4. *The group G^n has $q^n(q-1)^n$ elements and any element has order a divisor of $p(q-1)$. Moreover, for $n > 1$, there exists an element of order $p(q-1)$.*

Recall that, in the univariate case (i.e., $n = 1$), the study of invariant polynomials can be reduced to the study of the invariants by translations $x \mapsto x + b$ or homotheties $x \mapsto ax$. The idea relies on the change of variable $y = x + \frac{b}{a-1}$. In terms of matrices, we are just taking conjugations. For an element $A \in G$ distinct from the identity, with $A = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$, we say that A is of *h-type* or *t-type*, according to $b = 0$ and $a \neq 1, 0$ or $a = b = 1$, respectively. We can easily see that any element of G, distinct from the identity, is conjugated in G to an element of h-type or t-type. The first case occurs when A is diagonalizable ($a \neq 1$) and the second one occurs when $a = 1$ and $b \neq 0$.

We have the following result.

Theorem 2.5. *Let* $\mathbf{A}$ *and* $\mathbf{B}$ *two elements in* G^n *that are conjugated,* $\mathbf{A} = \mathbf{A}_0\mathbf{B}\mathbf{A}_0^{-1}$, *where* $\mathbf{A}_0 \in G^n$*. The following hold:*

a) *The* $\mathbb{F}_q$*-automorphism induced by* $\mathbf{A}_0^{-1}$*, when restricted to* $R_{\mathbf{A}}$*, is an* $\mathbb{F}_q$*-isomorphism between* $R_{\mathbf{A}}$ *and* $R_{\mathbf{B}}$*. Moreover, if* $R_{\mathbf{A}} = \mathbb{F}_q[f_1, \dots, f_m]$*, where* $f_i \in \mathcal{A}_n$*, then* $R_{\mathbf{B}} = \mathbb{F}_q[\mathbf{A}_0^{-1} \circ f_1, \dots, \mathbf{A}_0^{-1} \circ f_m]$*.*

b) *There exist unique nonnegative integers* $t = t(\mathbf{A})$ *and* $h = h(\mathbf{A})$ *and an element* $\mathbf{A}' \in G^n$ *such that* t *entries of* $\mathbf{A}'$ *are of* t*-type,* h *are of* h*-type and the* $n - h - t$ *remaining equal to the identity matrix with the additional property that* $R_{\mathbf{A}}$ *and* $R_{\mathbf{A}'}$ *are isomorphic, via the isomorphism induced by an element* $\mathbf{A}_1 \in G^n$*.*

Proof. a) Notice that $\mathbf{A}_0^{-1}\mathbf{A}\mathbf{A}_0 = \mathbf{B}$. Hence, for any $f \in \mathcal{A}_n$, $\mathbf{B} \circ f = f$ if and only if $\mathbf{A} \circ (\mathbf{A}_0 \circ f) = \mathbf{A}_0 \circ f$, i.e., $\mathbf{A}_0 \circ f \in R_{\mathbf{A}}$. In other words, $R_{\mathbf{B}}$ is the homomorphic image of $R_{\mathbf{A}}$ by the $\mathbb{F}_q$-automorphism $\mathbf{A}_0^{-1}$ of $\mathcal{A}_n$. Hence, if $\varphi_{\mathbf{A},\mathbf{B}} : R_{\mathbf{A}} \to R_{\mathbf{B}}$ is the restriction of this automorphism to $R_{\mathbf{A}}$, $\varphi_{\mathbf{A},\mathbf{B}}$ is an $\mathbb{F}_q$-isomorphism. Suppose that $R_{\mathbf{A}} = \mathbb{F}_q[f_1, \dots, f_m]$, where $f_i \in \mathcal{A}_n$, and let $g \in R_{\mathbf{B}}$. In particular, $\varphi_{\mathbf{A},\mathbf{B}}^{-1}(g)$ is in $R_{\mathbf{A}}$, hence it is a polynomial expression in terms of the elements $f_1, \dots, f_m$. Therefore, $g = \varphi_{\mathbf{A},\mathbf{B}}(\varphi_{\mathbf{A},\mathbf{B}}^{-1}(g))$ is a polynomial expression in terms of $\varphi_{\mathbf{A},\mathbf{B}}(f_1), \dots, \varphi_{\mathbf{A},\mathbf{B}}(f_m)$. In other words, $R_{\mathbf{B}} \subseteq \mathbb{F}_q[\varphi_{\mathbf{A},\mathbf{B}}(f_1), \dots, \varphi_{\mathbf{A},\mathbf{B}}(f_m)]$. The inverse inclusion follows in a similar way. Notice that, from definition, each f_i is in $R_{\mathbf{A}}$, hence $\varphi_{\mathbf{A},\mathbf{B}}(f_i) = \mathbf{A}_0^{-1} \circ f_i$ for $1 \leq i \leq m$.

b) Write $\mathbf{A} = (A_1, \dots, A_n)$ and let C_H (resp. C_T) be the sets of integers i (resp. j) with $1 \leq i, j \leq n$ such that the i-th (resp. j-th) coordinate of $\mathbf{A} \in G$ is conjugated in G to an element of h-type (resp. t-type), and set $h = |C_H|$, $t = |C_T|$. Also, for each $i \in C_h \cup C_t$, let B_i be the element of G such that $B_iA_iB_i^{-1}$ is of t-type or h-type and $B_i = I$ for $i \notin C_h \cup C_t$. If we set $\mathbf{A}_1 = (B_1, \dots, B_n)$, the element $\mathbf{A}' = \mathbf{A}_1\mathbf{A}\mathbf{A}_1^{-1} \in G^n$ is such that t entries of $\mathbf{A}'$ are of t-type, h are of h-type and the $n - h - t$ remaining equal to the identity matrix. The result follows from the previous item. The uniqueness of h and t follows from the fact that the sets C_H and C_T are uniquely determined by $\mathbf{A}$. □

Theorem 2.5 shows that any element $\mathbf{A} \in G^n$ is conjugated to another element $\mathbf{A}' \in G^n$ in a reduced form (any coordinate is either of h-type, t-type or the identity matrix), such that the rings $R_{\mathbf{A}}$ and $R_{\mathbf{A}'}$ are isomorphic. We also note that, if we reorder the variables, no algebraic structure of the ring $R_{\mathbf{A}}$ is affected. From now, we assume that $\mathbf{A} \in G^n$ has the first coordinates as matrices of the h-type, the following ones of the t-type and the last ones equal to the identity matrix.

Definition 2.6. Let $\mathbf{A} \in G^n$. For nonnegative integers t and h such that $t + h \leq n$, $\mathbf{A}$ is *of type* (h, t) if the first h coordinates of $\mathbf{A}$ are of h-type, the following t are of t-type and the $n - h - t$ remaining equal to the identity matrix.

The type of $\mathbf{A}$, along the elements we are considering now, is well defined. We fix some notation on the coordinates of h-type of $\mathbf{A}$.

Definition 2.7. Let $\mathbf{A}$ be an element of G^n of type (h, t) and write $\mathbf{A} = (A_1, \dots, A_n)$. For $h = 0$, set $H(\mathbf{A}) = \emptyset$ and, for $h \geq 1$, set $H(\mathbf{A}) = \{a_1, \dots, a_h\}$, where each a_i is the first entry in the main diagonal of A_i and $a_i \neq 1$ for $1 \leq i \leq h$.

It is clear that an element $\mathbf{A} \in G^n$ of type (h, t) is uniquely determined by t and the set $H(\mathbf{A})$.

2.2. Translations and homotheties

We start looking at the elements of type $(0, t)$, i.e., maps consisting of translations $x_i \mapsto x_i + 1$ for $1 \leq i \leq t$, that fixes the remaining variables. In the univariate case we see that the set of invariant polynomials equals $\mathbb{F}_q[x^p - x]$. Let us see what happens in two variables: notice that $x^p - x$ and $y^p - y$ are polynomials invariant by the translations $x \mapsto x + 1$ and $y \mapsto y + 1$ and, if we consider these maps independently, i.e., if we look at the identity

$$f(x+1, y) = f(x, y+1) = f(x, y),$$

one can show that the fixed-point subring is $\mathbb{F}_q[x^p - x, y^p - y]$. However, we are considering a less restrictive identity, $f(x + 1, y + 1) = f(x, y)$ and, in this case, the polynomial $f(x, y) = x - y$ appears as an invariant element. Is not hard to see that $x - y$ does not belong to $\mathbb{F}_q[x^p - x, y^p - y]$. We ask if there is any other exception. We observe that any polynomial $f(x, y) \in \mathbb{F}_q[x, y]$ is written *uniquely* as an univariate polynomial in $(x - y)$ with coefficients in $\mathbb{F}_q[y]$. In fact, $f(x, y) = g(x - y, y)$, where $g(x, y) = f(x + y, y)$. Hence $f(x, y) = \sum_{i=0}^{m} (x - y)^i P_i(y)$, and then $f(x + 1, y + 1) = f(x, y)$ if and only if $P_i(y+1) = P_i(y)$. In particular, from Theorem 2.1, each $P_i(y)$ is a polynomial expression in $t = y^p - y$. From this fact, one can see that the fixed-point subring is $\mathbb{F}_q[x - y, y^p - y]$. We observe that $x^p - x = (x - y)^p - (x - y) + (y^p - y)$, hence $x^p - x \in \mathbb{F}_q[x - y, y^p - y]$, as expected.

As above, we are frequently interested in writing an arbitrary polynomial $f \in \mathcal{A}_n$ as a finite sum of the form $\sum_{i \in B} g_i h_i$, where the variables appearing in $g_i \in \mathcal{A}_n$ are disjoint (or at least not contained) from the ones appearing in each $h_i \in \mathcal{A}_n$. This allows us to reduce our identities to well-known cases. In the following lemma, we summarize this idea.

Lemma 2.8. *Let m and n be positive integers such that $m \le n$. Then any nonzero $f \in \mathcal{A}_n$ can be written uniquely as*

$$f = \sum_{\beta \in B} \mathbf{X}^{\beta} P_{\beta},$$

where B is a finite set (of distinct elements) and, for any $\beta \in B$, $\mathbf{X}^{\beta}$ is a monomial (or a constant) in $\mathbb{F}_q[x_1, \dots, x_m]$ and each P_β is a nonzero element of $\mathbb{F}_q[x_{m+1} \dots, x_n]$ (which is $\mathbb{F}_q$ for $m = n$).

Proof. Since the variables are independent, $\mathcal{A}_n$ can be viewed as the ring of polynomials in the variables $x_1, \dots, x_m$ with coefficients in the ring $R = \mathbb{F}_q[x_{m+1} \dots, x_n]$ and the result follows. □

It is straightforward to check that, in Lemma 2.8, we can replace $x_1, \dots, x_m$ and $x_{m+1}, \dots, x_n$ by any partition of $\{x_1, \dots, x_n\}$ into 2 sets. We present a natural extension of the ideas that we have discussed for translations in $\mathbb{F}_q[x, y]$.

Theorem 2.9. *Suppose that $\mathbf{A}$ is of type $(0, t)$, where $t \le n$ is a nonnegative integer. Then $R_{\mathbf{A}} = \mathcal{A}_n$ if $t = 0$, $R_{\mathbf{A}} = \mathbb{F}_q[x_1^p - x_1, x_2, \dots, x_n]$ if $t = 1$ and, for $t \ge 2$,*

$$R_{\mathbf{A}} = \mathbb{F}_q[x_1 - x_2, \dots, x_{t-1} - x_t, x_t^p - x_t, x_{t+1}, \dots, x_n].$$

Proof. The case $t = 0$ is straightforward since the only element of type $(0, 0)$ is the identity of G^n. For $t = 1$, we obtain $f(x_1 + 1, x_2, \dots, x_n) = f(x_1, \dots, x_n)$. From Lemma 2.8, any f is written uniquely as $f = \sum_{\alpha \in B} \mathbf{X}^{\alpha} P_{\alpha}(x_1)$, where B is a finite set and $\mathbf{X}^{\alpha}$ is a monomial in the variables $x_2, \dots, x_n$ and $P_\alpha \in \mathbb{F}_q[x_1]$. In particular, we have $f \in R_{\mathbf{A}}$ if and only if $f = \sum_{\alpha \in B} \mathbf{X}^{\alpha} P_{\alpha}(x_1 + 1)$, that is, $P_\alpha(x_1 + 1) = P_\alpha(x)$. From Theorem 2.1, we know that the last equality holds if and only if $P_\alpha(x_1)$ is a polynomial in $x_1^p - x_1$, and then

$$R_{\mathbf{A}} = \mathbb{F}_q[x_1^p - x_1, x_2, \dots, x_n].$$

Suppose now that $t \ge 2$; given $f \in \mathcal{A}_n$, notice that, from Lemma 2.8, $g = f(x_1 + x_2, x_2, \dots, x_n) \in \mathcal{A}_n$ is written uniquely as $g = \sum_{i=0}^{m} x_1^i P_i$, where $P_i \in \mathbb{F}_q[x_2, \dots, x_n]$ and P_n is nonzero. Therefore, $f = g(x_1 - x_2, x_2, \dots, x_n)$ is written uniquely as $f = \sum_{i=0}^{m} (x_1 - x_2)^i P_i$. In particular, $f \in R_{\mathbf{A}}$ if and only if

$$f = \sum_{i=0}^{m} (x_1 - x_2)^i \cdot \mathbf{A} \circ P_i.$$

From the uniqueness of the polynomials P_i, $\mathbf{A} \circ f = f$ if and only if $\mathbf{A} \circ P_i = P_i$, where each P_i is in $\mathbb{F}_q[x_2, \dots, x_n]$. In other words, $R_{\mathbf{A}} = L[x_1 - x_2]$, where L is the fixed-point subring of $\mathbb{F}_q[x_2, \dots, x_n]$ by $\mathbf{A}$. We follow in the same way for the ring L. After $t-1$ iteration of this process, we obtain

$$R_{\mathbf{A}} = L_0[x_1 - x_2, x_2 - x_3, \dots, x_{t-1} - x_t],$$

where L_0 is the fixed-point subring of $\mathbb{F}_q[x_t, \dots, x_n]$ by $\mathbf{A}$. Since $\mathbf{A}$ maps x_t to $x_t + 1$ and fixes x_i for $t < i \le n$, we are back to the case $t = 1$ (now with $n - t + 1$ variables) and so $L_0 = \mathbb{F}_q[x_t^p - x_t, x_{t+1}, \dots, x_n]$. □

The following notation is useful.

Definition 2.10.

(i) For any nonnegative integers h, t such that $h + t \le n$, set $L(h, 0) = \emptyset$, $L(h, 1) = \{x_{h+1}^p - x_{h+1}\}$ and, for $t \ge 2$,

$$L(h, t) = \{x_{h+1} - x_{h+2}, \dots, x_{h+t-1} - x_{h+t}, x_{h+t}^p - x_{h+t}\}.$$

(ii) For any nonnegative integer $d \le n$, set $V_d = \emptyset$ if $d = n$ and, for $d \le n - 1$, $V_d = \{x_{d+1}, \dots, x_n\}$.

From definition, Theorem 2.9 implies that if $\mathbf{A}$ is of type $(0, t)$, the set $L(0, t) \cup V_t$ is a set of generators for $R_{\mathbf{A}}$ as an $\mathbb{F}_q$-algebra. We have the following “translated” version of Theorem 2.9. Its proof is straightforward so we omit.

Corollary 2.11. *Let $\Psi(h, t)$ be the $\mathbb{F}_q$-automorphism of $\mathcal{A}_n$, that maps x_i to $x_i + 1$ for $h + 1 \le i \le h + t$, where h and t are nonnegative integers such that $h + t \le n$. Let f be a polynomial in $\mathbb{F}_q[x_{h+1}, \dots, x_n]$. Then f is invariant by $\Psi(h, t)$ if and only if f is a polynomial expression in terms of the elements of $L(h, t) \cup V_{h+t}$, i.e., the fixed point subring of $\mathbb{F}_q[x_{h+1}, \dots, x_n]$ by $\Psi(h, t)$ coincides with the $\mathbb{F}_q$-algebra generated by $L(h, t) \cup V_{h+t}$.*

We now look at the elements $\mathbf{A}$ of type $(h, 0)$, i.e., maps consisting of homotheties $x_i \mapsto a_i x_i$ for $1 \le i \le h$, that fixes the remaining variables.

Proposition 2.12. *Suppose that $\mathbf{A}$ is of type $(h, 0)$, where h is a nonnegative integer and, for $h \ge 1$, set $H(\mathbf{A}) = \{a_1, \dots, a_h\}$ and $d_i = \mathrm{ord}(a_i)$. For $h \ge 1$, let $C_{\mathbf{A}} \in \mathbb{N}^h$ be the set of all vectors $(b_1, \dots, b_h) \in \mathbb{N}^h$ such that $b_i \le d_i$, at least one b_i is nonzero and*

$$a_1^{b_1} \cdots a_h^{b_h} = 1. \tag{1}$$

For each $b \in C_{\mathbf{A}}$, $b = (b_1, \dots, b_h)$ we associate the monomial $\mathbf{Y}^b := x_1^{b_1} \dots x_h^{b_h}$. Let $M_{\mathbf{A}} := \{\mathbf{Y}^b \mid b \in C_{\mathbf{A}}\}$ and $h_{\mathbf{A}} := |M_{\mathbf{A}}|$. Then $R_{\mathbf{A}} = \mathcal{A}_n$ if $h = 0$ and, for $h \ge 1$,

$$R_{\mathbf{A}} = \mathbb{F}_q[y_1, \ldots, y_{h_{\mathbf{A}}}, x_{h+1}, \ldots, x_n],$$

where y_i runs through the distinct elements of $M_{\mathbf{A}}$.

Proof. The case $t = 0$ is straightforward since the only element of type $(0, 0)$ is the identity of G^n. Suppose that $h > 0$. From Lemma 2.8, we know that any $f \in \mathcal{A}_n$ can be written uniquely as $f = \sum_{\alpha \in B} \mathbf{X}^{\alpha} P_{\alpha}$, where B is a finite set, each $\mathbf{X}^{\alpha}$ is a monomial in the variables $x_1, \ldots, x_h$ and each P_{α} is a nonzero element of $\mathbb{F}_q[x_{h+1}, \ldots, x_n]$. Notice that

$$\mathbf{A} \circ f = \sum_{\alpha \in B} \mathbf{X}^{\alpha}(a_{\alpha} P_{\alpha}),$$

where, for each $\alpha = (c_1, \ldots, c_n) \in \mathbb{N}^n$, a_{α} is defined as the product $a_1^{c_1} \ldots a_h^{c_h}$. If $f \in R_{\mathbf{A}}$, then $\mathbf{A} \circ f = f$ and, from the uniqueness of the polynomials P_{α}, it follows that $a_{\alpha} P_{\alpha} = P_{\alpha}$ for any $\alpha \in B$. In particular, since $P_{\alpha} \neq 0$, we get $a_{\alpha} = 1$, that is, $a_1^{c_1} \cdots a_h^{c_h} = 1$.

If we write $c_i = d_i Q_i + r_i$, where $0 \leq r_i < d_i$, the last equality implies that $a_1^{r_1} \ldots a_h^{r_h} = 1$, i.e., $(r_1, \ldots, r_h)$ is either the zero vector or belongs to $C_{\mathbf{A}}$. In other words, $\mathbf{X}^{\alpha} = (x_1^{d_1})^{Q_1} \ldots (x_h^{d_h})^{Q_h} \cdot \mathbf{Y}^b$, where $\mathbf{Y}^b$ is either $1 \in \mathbb{F}_q$ or an element of $M_{\mathbf{A}}$. We observe that, since $a_i^{d_i} = 1$, each $x_i^{d_i}$ is in $M_{\mathbf{A}}$. Hence $f = \sum_{\alpha \in B} \mathbf{X}^{\alpha} P_{\alpha}$ is such that each $\mathbf{X}^{\alpha}$ is a finite product of elements in $M_{\mathbf{A}}$ (or equal to $1 \in \mathbb{F}_q$) and, in particular, $R_{\mathbf{A}} \subseteq \mathbb{F}_q[y_1, \ldots, y_{h_{\mathbf{A}}}, x_{h+1}, \ldots, x_n]$, where y_i runs through the distinct elements of $M_{\mathbf{A}}$. For the reverse inclusion $R_{\mathbf{A}} \supseteq \mathbb{F}_q[y_1, \ldots, y_{h_{\mathbf{A}}}, x_{h+1}, \ldots, x_n]$, notice that each monomial y_i satisfies $\mathbf{A} \circ y_i = y_i$ and $\mathbf{A}$ trivially fixes the variables $x_{h+1}, \ldots, x_n$. Thus, $R_{\mathbf{A}} = \mathbb{F}_q[y_1, \ldots, y_{h_{\mathbf{A}}}, x_{h+1}, \ldots, x_n]$ and we conclude the proof. □

Example 2.13. Let q be odd and, for $f \in \mathbb{F}_q[x, y, z]$, consider the identity $f(x, y, z) = f(-x, -y, z)$. In other words, $\mathbf{A} \circ f = f$, where $\mathbf{A} \in G^3$ is of type $(2, 0)$ and $H(\mathbf{A}) = \{-1, -1\}$. It follows from Proposition 2.12 that $M_{\mathbf{A}} = \{x^2, y^2, xy, x^2y^2\}$ and $R_{\mathbf{A}} = \mathbb{F}_q[x^2, y^2, xy, x^2y^2, z]$.

In the previous example, the element x^2y^2 is already in $\mathbb{F}_q[x^2, y^2, xy, z]$, since $x^2y^2 = x^2 \cdot y^2$ or even $x^2y^2 = (xy)^2$. We then may write $R_{\mathbf{A}} = \mathbb{F}_q[x^2, y^2, xy, z]$. We introduce a subset of $M_{\mathbf{A}}$ to remove these *redundant* elements.

Definition 2.14. Suppose that $\mathbf{A}$ is of type $(h, 0)$, where h is a non negative integer. Let $M^*_{\mathbf{A}} = \emptyset$ if $h = 0$ and, for $h \geq 1$, $M^*_{\mathbf{A}}$ is the subset of $M_{\mathbf{A}}$ comprising the monomials $\mathbf{X}^{\alpha}$ of $M_{\mathbf{A}}$ that are not divisible by any element of $M_{\mathbf{A}} \setminus \{\mathbf{X}^{\alpha}\}$, where $M_{\mathbf{A}}$ is as in Theorem 2.12. We set $N(\mathbf{A}) = |M^*_{\mathbf{A}}| - h$.

From definition, if $\mathbf{A}$ is of type $(h, 0)$, where $h \geq 1$ and $H(\mathbf{A}) = \{a_1, \ldots, a_h\}$, then $\{x_1^{d_1}, \ldots, x_h^{d_h}\} \subseteq M^*_{\mathbf{A}}$, where $d_i = \mathrm{ord}(a_i)$; one can verify that any other element of $M^*_{\mathbf{A}}$ is a "mixed" monomial. We always have the bound $N(\mathbf{A}) \geq 0$ and, in fact, $N(\mathbf{A})$ counts the number of mixed monomials appearing in $M_{\mathbf{A}}^*$. In the previous example, we have $M_{\mathbf{A}}^* = \{x^2, y^2, xy\}$ and $N(\mathbf{A}) = 1$.

We observe that any element of $M_{\mathbf{A}}$ is divisible by some element of $M_{\mathbf{A}}^*$. Moreover, from Eq. (1), if $\mathbf{X} \in M_{\mathbf{A}}$ is divisible by $\mathbf{Y} \in M_{\mathbf{A}}^*$, then $\mathbf{X}/\mathbf{Y} = 1$ or $\mathbf{X}/\mathbf{Y}$ is another element of $M_{\mathbf{A}}$. From this fact, one can see that any element of $M_{\mathbf{A}} \supseteq M_{\mathbf{A}}^*$ is a finite product of elements in $M_{\mathbf{A}}^*$. In particular, if $\mathbf{A}$ is of type $(h, 0)$, the sets $M_{\mathbf{A}}^* \cup V_h$ and $M_{\mathbf{A}} \cup V_h$ generate the same $\mathbb{F}_q$-algebra, i.e., $M_{\mathbf{A}}^* \cup V_h$ generates $R_{\mathbf{A}}$ as an $\mathbb{F}_q$-algebra. We finish this section showing that $M_{\mathbf{A}}^*$ is minimal in some sense.

Lemma 2.15. *For any $\mathbf{X}^\alpha \in M_{\mathbf{A}}^*$, $\mathbf{X}^\alpha$ cannot be written as a polynomial expression in terms of the elements in $M_{\mathbf{A}}^* \setminus \{\mathbf{X}^\alpha\}$.*

Proof. Suppose that there is an element $\mathbf{X}^\alpha \in M_{\mathbf{A}}^*$ with this property; such a polynomial expression in terms of the elements in $M_{\mathbf{A}}^* \setminus \{\mathbf{X}^\alpha\}$ has constant term equals zero (we can see this, for instance, evaluating at the point $(0, \dots, 0) \in \mathbb{F}_q^n$). In particular, $\mathbf{X}^\alpha$ belongs to the monomial ideal generated by the set $M_{\mathbf{A}}^* \setminus \{\mathbf{X}^\alpha\}$ in $\mathcal{A}_n$. But it is well known that, a monomial belongs to the monomial ideal $I \subset \mathcal{A}_n$ generated by a set C if and only if the monomial itself is divisible by some element in C. But, from definition, $\mathbf{X}^\alpha$ is not divisible by any element of $M_{\mathbf{A}} \setminus \{\mathbf{X}^\alpha\} \supseteq M_{\mathbf{A}}^* \setminus \{\mathbf{X}^\alpha\}$ and we get a contradiction. □

3. The structure of the fixed-point subring $R_{\mathbf{A}}$

In the previous section, we have characterized the fixed-point subring $R_{\mathbf{A}}$ in the case that $\mathbf{A}$ is of type $(0, t)$ or $(h, 0)$. We now extend this characterization to the general case.

Proposition 3.1. *Suppose that $\mathbf{A} \in G^n$ is of type (h, t). There exist unique elements $\mathbf{A}_1$ and $\mathbf{A}_2$ with the following properties:*

(i) *$\mathbf{A}_1$ if of type $(h, 0)$.*
(ii) *The first h and the last $n - h - t$ coordinates of $\mathbf{A}_2$ are the identity matrix and the remaining t (in the middle) are elements of t-type.*
(iii) *$\mathbf{A} = \mathbf{A}_1 \cdot \mathbf{A}_2$.*

Additionally, $R_{\mathbf{A}} = R_{\mathbf{A}_1} \cap R_{\mathbf{A}_2}$ and, in particular, $R_{\mathbf{A}}$ is the $\mathbb{F}_q$-algebra generated by $M_{\mathbf{A}_1}^* \cup L(h, t) \cup V_{h+t}$.

Proof. Write $\mathbf{A} = (A_1, \dots, A_n)$ and set $\mathbf{A}_1 = (A_1, \dots, A_h, I, \dots, I) \in G^n$, where each A_i is of h-type. Given $\mathbf{A}$ of type (h, t), such an $\mathbf{A}_1$ is unique. We notice that $\mathbf{A}_2 = \mathbf{A}_1^{-1}\mathbf{A}$ has the required properties. It turns out that the elements $\mathbf{A}_1$ and $\mathbf{A}_2$ commute in G^n and $D_1 = \mathrm{ord}(\mathbf{A}_1)$, $D_2 = \mathrm{ord}(\mathbf{A}_2)$ divide $q - 1$ and p, respectively. Since p and $q - 1$ are relatively prime, then so are D_1 and D_2. In particular, if $\mathbf{A} \circ f = f$, one can easily see that this implies $\mathbf{A}_1 \circ f = \mathbf{A}_2 \circ f = f$. Therefore, $R_{\mathbf{A}} \subseteq R_{\mathbf{A}_1} \cap R_{\mathbf{A}_2}$. The reverse inclusion is trivial and then $R_{\mathbf{A}} = R_{\mathbf{A}_1} \cap R_{\mathbf{A}_2}$.

Let R be the $\mathbb{F}_q$-algebra generated by the elements of $M^*_{\mathbf{A}_1} \cup L(h,t) \cup V_{h+t}$. From Theorem 2.9, Proposition 2.12 and Corollary 2.11, we see that any element $f \in R$ satisfies $\mathbf{A}_1 \circ f = \mathbf{A}_2 \circ f = f$ and then $R \subseteq R_{\mathbf{A}_1} \cap R_{\mathbf{A}_2} = R_{\mathbf{A}}$. Conversely, suppose that $f \in R_{\mathbf{A}} = R_{\mathbf{A}_1} \cap R_{\mathbf{A}_2}$. From Lemma 2.8, f can be written uniquely as $f = \sum_\alpha \mathbf{X}^\alpha P_\alpha$, where $B \subset \mathbb{N}^h$ is a finite set, each $\mathbf{X}^\alpha$ is a monomial in $\mathbb{F}_q[x_1, \dots, x_h]$ and P_α is a nonzero polynomial in $\mathbb{F}_q[x_{h+1}, \dots, x_n]$. Since $\mathbf{A}_2$ fixes each element of $\{\mathbf{X}^\alpha \,|\, \alpha \in B\}$ and $\mathbf{A}_2 \circ f = f$, we obtain $\mathbf{A}_2 \circ P_\alpha = P_\alpha$ and then, from Corollary 2.11, we see that each P_α is a polynomial expression in terms of the elements in $L(h,t) \cup V_{h+t}$. Also, since $\mathbf{A}_1$ fixes each polynomial $P_\alpha, \alpha \in B$ and $\mathbf{A}_1 \circ f = f$, we obtain $(\mathbf{A}_1 \circ \mathbf{X}^\alpha) \cdot P_\alpha = \mathbf{X}^\alpha \cdot P_\alpha$ and, since P_α is nonzero, we conclude that $\mathbf{A}_1 \circ \mathbf{X}^\alpha = \mathbf{X}^\alpha$. Therefore, from Theorem 2.12, each $\mathbf{X}^\alpha$ is a polynomial expression in terms of the elements in $M^*_{\mathbf{A}_1}$. In particular, f must be a polynomial expression in terms of the elements of $M^*_{\mathbf{A}_1} \cup L(h,t) \cup V_{h+t}$, i.e., $f \in R$. Thus $R = R_{\mathbf{A}}$, as desired. □

From now, if $\mathbf{A}$ is an element of type (h,t), the identity $\mathbf{A} = \mathbf{A}_1\mathbf{A}_2$ as in Proposition 3.1 is defined as the *canonical decomposition* of $\mathbf{A}$.

Example 3.2. Let q be odd and consider the element $\mathbf{A} \in G^5$ of type $(2,2)$, with $H(\mathbf{A}) = H(\mathbf{A}_1) = \{-1,-1\}$. The ring $R_{\mathbf{A}}$ comprises the elements $f \in A_5$ satisfying $f(x_1, \dots, x_5) = f(-x_1, -x_2, x_3+1, x_4+1, x_5)$. In this case, Proposition 3.1 implies

$$R_{\mathbf{A}} = \mathbb{F}_q[x_1^2, x_2^2, x_1x_2, x_3 - x_4, x_4^p - x_4, x_5].$$

We ask if $M^*_{\mathbf{A}_1} \cup L(h,t) \cup V_{h+t}$ contains redundant elements. This leads us to introduce the following definition.

Definition 3.3. Suppose that $R \subseteq \mathcal{A}_n$ is a finitely generated $\mathbb{F}_q$-algebra and let S be a set of generators for R. We say that S is a minimal generating set for R if there is no proper subset $S' \subset S$ such that S' generates R.

In other words, minimal generating sets S are those ones with the property that no element E of S can be written as a polynomial expression in terms of the elements in $S \setminus \{E\}$. We will prove that the set of generators for $R_{\mathbf{A}}$ given in Proposition 3.1 is minimal, but first we explore the *algebraic independence* on the set $M^*_{\mathbf{A}_1} \cup L(h,t) \cup V_{h+t}$ (which is, somehow, stronger than the concept of redundant elements).

3.1. Algebraic independence in positive characteristic

If K is an arbitrary field, given polynomials $f_1, \dots, f_m$ in $K[x_1, \dots, x_n]$, we say that $f_1, \dots, f_m$ are *algebraically independent* if there is no nonzero polynomial $P \in K[y_1, \dots, y_m]$ such that $P(f_1, \dots, f_m)$ is identically zero in $K[x_1, \dots, x_n]$. Given polynomials $f_1, \dots, f_n$ in $K[x_1, \dots, x_n]$, we define their *Jacobian* as the polynomial $\det(J(f_1, \dots, f_n))$, where $J(f_1, \dots, f_n)$ is the $n \times n$ matrix with entries $a_{ij} = \frac{\partial f_i}{\partial x_j}$. Here,

$\frac{\partial f_i}{\partial x_j}$ denotes the *partial derivative* of f_i with respect to x_j. The well known *Jacobian Criterion* says that, over characteristic zero, a set of n polynomials in $K[x_1, \ldots, x_n]$ is algebraically independent if and only if their Jacobian is nonzero. This may fail in positive characteristic; the elements x^p and y^p are algebraically independent over $\mathbb{F}_p[x, y]$, but $\det(J(x^p, y^p)) = 0$. However, we have at least one direction of this result.

Theorem 3.4 *(Jacobian Criterion – weak version). Suppose that $f_1, \ldots, f_n$ is a set of polynomials in $\mathbb{F}_q[x_1, \ldots, x_n]$ such that their Jacobian is nonzero. Then $f_1, \ldots, f_n$ are algebraically independent.*

For the proof of this result, see Theorem 3.1 of [3].

Corollary 3.5. *For any nonnegative integers h and t such that $h + t \leq n$ and any sequence $d_1, \ldots, d_h$ (which is empty for $h = 0$) of divisors of $q - 1$, the n elements of $\{x_1^{d_1}, \ldots, x_h^{d_h}\} \cup L(h, t) \cup V_{h+t}$ are algebraically independent.*

Proof. We observe that the Jacobian of the elements in $\{x_1^{d_1}, \ldots, x_h^{d_h}\} \cup L(h, t) \cup V_{h+t}$ equals $\varepsilon(t)$ if $h = 0$ and and equals

$$\varepsilon(t) \cdot (d_1 \cdots d_h) \cdot (x_1^{d_1 - 1} \cdots x_h^{d_h - 1}),$$

if $h \neq 0$, where $\varepsilon(t) = 1$ for $t = 0$ and $\varepsilon(t) = -1$ for $t \neq 0$. Since each d_i is a divisor of $q - 1$ (which is prime to the characteristic p), this Jacobian is never zero and the result follows from the (weak) Jacobian Criterion for $\mathbb{F}_q$. □

We are ready to prove the minimality of $M^*_{\mathbf{A}_1} \cup L(h, t) \cup V_{h+t}$.

Proposition 3.6. *Let $\mathbf{A} \in G^n$ be an element of type (h, t) and $\mathbf{A} = \mathbf{A}_1\mathbf{A}_2$ its canonical decomposition. Then $M^*_{\mathbf{A}_1} \cup L(h, t) \cup V_{h+t}$ is a minimal generating set for $R_{\mathbf{A}}$.*

Proof. We already know that this set is a generator. To prove the minimality of such set, let I_T be the ideal generated by $L(h, t) \cup V_{h+t}$ over the ring $R_{\mathbf{A}}$. We first show that no element of $M^*_{\mathbf{A}_1}$ is redundant. For this, suppose that an element $\mathbf{X}^\alpha \in M^*_{\mathbf{A}_1}$ is a polynomial expression in terms of the elements in $M^*_{\mathbf{A}_1} \cup L(h, t) \cup V_{h+t} \setminus \{\mathbf{X}^\alpha\}$. Looking at the quotient $R_{\mathbf{A}}/I_T$, this yields an equality $\mathbf{X}^\alpha \equiv P_\alpha \pmod{I_T}$, where P_α is a polynomial expression in terms of the elements in $M^*_{\mathbf{A}_1} \setminus \{\mathbf{X}^\alpha\}$. In other words, $\mathbf{X}^\alpha - P_\alpha$ is an element of I_T. One can see that this implies $\mathbf{X}^\alpha - P_\alpha = 0$, a contradiction with Lemma 2.15. In the same way (taking I_H as the ideal generated by $M^*_{\mathbf{A}_1} \cup V_{h+t}$ over $R_{\mathbf{A}}$), we see that if there is a redundant element T in $L(h, t)$, then such a T can be written as a polynomial expression in terms of the elements of $L(h, t) \setminus \{T\}$. But this yields a nonzero polynomial $P \in \mathbb{F}_q[y_1, \ldots, y_s]$ such that $P(T_1, \ldots, T_s) = 0$, where T_i runs through the elements of $L(h, t)$, which is impossible since Lemma 3.5 ensures that these elements are algebraically independent. Finally, it is clear that no element of V_{h+t} is redundant in $M^*_{\mathbf{A}_1} \cup L(h,t) \cup V_{h+t}$. $\square$

For an element $\mathbf{A}$ of type (h,t) with canonical decomposition $\mathbf{A} = \mathbf{A}_1\mathbf{A}_2$, $S_{\mathbf{A}} := M^*_{\mathbf{A}_1} \cup L(h,t) \cup V_{h+t}$ is the *canonical generating set* for $R_{\mathbf{A}}$. We note that $|S_{\mathbf{A}}| = n + N(\mathbf{A}_1)$ and, in fact, $|S_{\mathbf{A}}| - n = N(\mathbf{A}_1)$ is the number of "mixed" monomials in $S_{\mathbf{A}}$.

3.2. Free algebras

Given a field K and a finitely generated K-algebra $R \subseteq K[x_1, \dots, x_n]$, R is *free* if R can be generated by a sequence $f_1, \dots, f_m \in K[x_1, \dots, x_n]$ comprising algebraically independent elements. In other words, R (as a ring) is isomorphic to the polynomial ring of m variables over K, for some $m \geq 1$.

As follows, we have a simple criterion for $R_{\mathbf{A}}$ to be a free $\mathbb{F}_q$-algebra.

Theorem 3.7. *Let $\mathbf{A} \in G^n$ be an element of type (h,t) and $\mathbf{A} = \mathbf{A}_1\mathbf{A}_2$ its canonical decomposition. Write $H(\mathbf{A}) = H(\mathbf{A}_1) = \{a_1, \dots, a_h\}$ for $h \geq 1$ and $d_i = \mathrm{ord}(a_i) > 1$ for $1 \leq i \leq h$. The following are equivalent:*

(i) *$R_{\mathbf{A}}$ is free;*
(ii) *$h = 0, 1$ or $h > 1$ and the numbers d_i are pairwise relatively prime;*
(iii) *$N(\mathbf{A}_1) = 0$;*
(iv) *$R_{\mathbf{A}}$ is isomorphic to $\mathcal{A}_n$.*

Proof. **(i)** $\to$ **(ii)**: it suffices to prove that, if $h > 1$ and there are two elements d_i and d_j not relatively prime, then $R_{\mathbf{A}}$ is not a free $\mathbb{F}_q$-algebra. Without loss of generality, suppose that $\gcd(d_1, d_2) = d > 1$. If $R_{\mathbf{A}}$ were a free $\mathbb{F}_q$-algebra, then it would be isomorphic to the ring $K[y_1, \dots, y_m]$ of m variables over K for some m, which is always an *Unique Factorization Domain*. As we will see, the ring $R_{\mathbf{A}}$ does not have this property.

For a given primitive element $\theta \in \mathbb{F}_q^*$, notice that $a_1 = \theta^{\frac{q-1}{d_1} r_1}$ and $a_2 = \theta^{\frac{q-1}{d_2} r_2}$ for some positive integers $r_1 \leq d_1$ and $r_2 \leq d_2$ such that $\gcd(r_1, d_1) = \gcd(r_2, d_2) = 1$. In particular, since d divides d_1 and d_2, $\gcd(d, r_1) = \gcd(d, r_2) = 1$ and so there exists a positive integer $j \leq d - 1$ such that $jr_1 \equiv -r_2 \pmod{d}$. Notice that

$$a_1^{\frac{j}{d} d_1} a_2^{\frac{d_2}{d}} = \theta^{\frac{(q-1)(jr_1 + r_2)}{d}} = 1,$$

since $jr_1 + r_2$ is divisible by d. In particular, $(\frac{jd_1}{d}, \frac{d_2}{d}, 0 \dots, 0) \in \mathbb{N}^h$ satisfies Eq. (1). Clearly $u_1 := \frac{jd_1}{d} < d_1$ and $u_2 := \frac{d_2}{d} < d_2$, and so $\mathbf{Y} = x_1^{u_1} x_2^{u_2}$ belongs to $M_{\mathbf{A}_1}$. It follows from definition that this monomial is divisible by a monomial $\mathbf{X} := x_1^{v_1} x_2^{v_2} \in M^*_{\mathbf{A}_1}$ with $v_i \leq u_i < d_i$; in particular, $a_1^{v_1} a_2^{v_2} = 1$ and, since $v_i < d_i$, it follows that $v_1, v_2 > 0$.

Is not hard to see that $R_{\mathbf{A}}$, viewed as a ring, is an *Integral Domain* and any element of $M^*_{\mathbf{A}_1}$ is *irreducible* over $R_{\mathbf{A}}$. Notice that $\mathbf{Y}^d = (x_1^{d_1})^j \cdot x_2^{d_2}$, hence $\mathbf{X} = x_1^{v_1} x_2^{v_2}$ is an irreducible divisor of $\mathbf{Y}^d$ and, since $v_1, v_2 > 0$, $\mathbf{X}$ does not divide $(x_1^{d_1})^j$ or $x_2^{d_2}$. However, $x_1^{d_1}$ and $x_2^{d_2}$ are in $R_{\mathbf{A}}$ and then $R_{\mathbf{A}}$ cannot be an Unique Factorization Domain.

(ii) → **(iii)**: For $h = 0$ or 1, $M_{\mathbf{A}_1}^* = \emptyset$ or $\{x_1^{d_1}\}$, respectively, and in both cases $N(\mathbf{A}_1) = 0$. Let $h > 1$ and suppose that the numbers d_i are pairwise relatively prime. We find explicitly the set $M_{\mathbf{A}_1}^*$: suppose that $(b_1, \dots, b_h) \in \mathbb{N}^h$, where $b_i \le d_i$, at least one b_i is nonzero and $a_1^{b_1} \cdots a_h^{b_h} = 1$. Set $D = d_1 \cdots d_h$ and $D_j = \frac{D}{d_j}$, for $1 \le j \le h$. Raising powers D_j in the previous equality we obtain $a_j^{b_j D_j} = 1$, and so d_j divides $b_j D_j$. In particular, since the numbers d_i are pairwise relatively prime, it follows that d_j and D_j are relatively prime and then we conclude that d_j divides b_j. Since $0 \le b_j \le d_j$, it follows that, for each $1 \le j \le h$, either $b_j = 0$ or $b_j = d_j$. This shows that $M_{\mathbf{A}_1}^* = \{x_1^{d_1}, \dots, x_h^{d_h}\}$ and then

$$N(\mathbf{A}_1) = |M_{\mathbf{A}_1}^*| - h = h - h = 0.$$

(iii) → **(iv)**: If $N(\mathbf{A}_1) = 0$, we know that $M_{\mathbf{A}_1}^* = \{x_1^{d_1}, \dots, x_h^{d_h}\}$. From Proposition 3.1 and Corollary 3.5 it follows that $R_{\mathbf{A}}$ is an $\mathbb{F}_q$-algebra generated by n algebraically independent elements in $\mathcal{A}_n$. In particular, $R_{\mathbf{A}}$ is isomorphic to $\mathcal{A}_n$.

(iv)→ **(i)**: This follows directly by definition. □

In other words, Theorem 3.7 says that $R_{\mathbf{A}}$ is free if and only if $M_{\mathbf{A}_1}^*$ has no mixed monomials. For instance, if $q = 2$, $n \ge 1$ and $\mathbf{A} \in G^n$, $\mathbf{A}$ has no elements of h-type as coordinates. In particular, the algebra $R_{\mathbf{A}}$ is always isomorphic to $\mathcal{A}_n$.

In the following corollary, we show that we have a sharp upper bound on the number of coordinates of h-type in an element $\mathbf{A}$ such that $R_{\mathbf{A}}$ is free.

Corollary 3.8. *Suppose that $q > 2$ and let $\omega(q-1)$ be the number of distinct prime divisors of $q-1$. The following hold:*

(i) *If $\mathbf{A} \in G^n$ is of type (h, t) with $h > \omega(q-1)$, $R_{\mathbf{A}}$ is not free.*
(ii) *For any nonnegative integers $h \le \omega(q-1)$ and t such that $h + t \le n$, there exists an element $\mathbf{A}$ of type (h, t) such that $R_{\mathbf{A}}$ is free.*

Proof. (i) Let $\mathbf{A}$ be an element of type (h, t) with $h > \omega(q-1)$ such that $H(\mathbf{A}) = \{a_1, \dots, a_h\}$ and $d_i = \operatorname{ord}(a_i) > 1$ for $1 \le i \le h$. Since $h > \omega(q-1)$, from the *Pigeonhole Principle*, there exist two elements d_i and d_j that are divisible by some prime factor r of $q-1$ and it follows from Theorem 3.7 that $R_{\mathbf{A}}$ is not free.

(ii) If $\omega(q-1) \le 1$, then $h \le 1$ and Theorem 3.7 says that, for any element $\mathbf{A}$ of type (h, t), the $\mathbb{F}_q$-algebra $R_{\mathbf{A}}$ is free. Suppose that $\omega(q-1) > 1$, $2 \le h \le \omega(q-1)$ and let $p_1, \dots, p_h$ be distinct prime factors of $q-1$. For each $1 \le i \le h$, let $\theta_i \in \mathbb{F}_q^*$ be an element such that $\operatorname{ord}(\theta_i) = p_i$. For each nonnegative integer t with $h+t \le n$, consider $\mathbf{A}$ the element of type (h, t) such that $H(\mathbf{A}) = \{\theta_1, \dots, \theta_h\}$. Since the numbers p_i are pairwise relatively prime, from Theorem 3.7, $R_{\mathbf{A}}$ is a free $\mathbb{F}_q$-algebra. □

4. Minimal product-one sequences in $\mathbb{F}_q^*$ and bounds for $N(\mathbf{A}_1)$

So far we have provided a minimal generating set $S_{\mathbf{A}}$ for $R_{\mathbf{A}}$. We may ask how large is the set $S_{\mathbf{A}}$. We have seen that $|S_{\mathbf{A}}| = n + N(\mathbf{A}_1)$ and actually $N(\mathbf{A}_1) = 0$ when $\mathbf{A}$ is of type (h,t) for $h = 0, 1$ and some special cases of $h \geq 2$. Is then natural to ask what happens in the general case $h \geq 2$. In this section, we show that $N(\mathbf{A}_1)$ is, in general, related to the number of minimal solutions of Eq. (1) and show how this can be translated to the study of minimal product-one sequences in $\mathbb{F}_q^*$. We start with some basic theory on product-one sequences.

Definition 4.1. Given a finite abelian group H (written multiplicatively), a sequence of elements $(a_1, \dots a_k)$ (not necessarily distinct) in H is a product-one sequence if $a_1 \cdots a_k = 1$, where 1 is the identity of H; the number k is called the length of $(a_1, \dots, a_k)$. We say that the sequence $(a_1, \dots, a_k)$ is a minimal product-one sequence if $a_1 \cdots a_k = 1$ and no subsequence of $(a_1, \dots a_k)$ share the same property.

Since we are working in abelian groups, we consider the sequences up to permutation of their elements. The so-called *Davenport constant* of H, denoted by $D(H)$, is the smallest positive integer d such that any sequence of length d in H contains a product-one subsequence. In other words, $D(H)$ is the maximal length of minimal product-one sequences in H. In the case when H is cyclic, the constant $D(H)$ is known: from Theorem 2.1 in [4], we easily deduce the following result.

Theorem 4.2. *Suppose that C_m is the cyclic group with m elements. Then $D(C_m) = m$. Additionally, any minimal product-one sequence in C_m of length m is of the form $(g, \dots, g)$ for some generator g of C_m.*

Recall that, for an element $\mathbf{A}$ of type $(h, 0)$ with $h \geq 1$ and $H(\mathbf{A}) = \{a_1, \cdots a_h\}$, the set $M_{\mathbf{A}}$ is defined as the set of monomials $\mathbf{X} = x_1^{b_1} \cdots x_h^{b_h}$ such that at least one b_i is nonzero, $b_i \leq \operatorname{ord}(a_i)$ and $a_1^{b_1} \cdots a_h^{b_h} = 1$. In particular, $\mathbf{X} \in M_{\mathbf{A}}$ can be associated to the product-one sequence $a(\mathbf{X})$ in the cyclic group $\mathbb{F}_q^* = C_{q-1}$, where $a(\mathbf{X}) := (a_1, \dots, a_1, \dots, a_h, \dots, a_h)$ and each a_i appears b_i times. This sequence has length $\sum_{j=1}^{h} b_j$. We claim that, for each $\mathbf{X} \in M_{\mathbf{A}}^*$, its associated product-one sequence is minimal. In fact, if $a(\mathbf{X})$ were not minimal, there would exist nonnegative integers $b_1', \cdots, b_h'$ such that $b_i' \leq b_i$, at least one b_i' is nonzero, at least one b_j' is strictly smaller than the corresponding b_j and $a_1^{b_1'} \cdots a_h^{b_h'} = 1$. From definition, the monomial $\mathbf{Y} = x_1^{b_1'} \cdots x_h^{b_h'}$ is in $M_{\mathbf{A}}$ and divides $\mathbf{X}$, a contradiction since $\mathbf{X} \in M_{\mathbf{A}}^*$.

Based on this observation and Theorem 4.2, we can give a sharp upper bound for the numbers $N(\mathbf{A}_1)$.

Theorem 4.3. *Let $\mathbf{A} \in G^n$ be an element of type (h,t) and $\mathbf{A} = \mathbf{A}_1\mathbf{A}_2$ its canonical decomposition, where $h \geq 2$. Write $H(\mathbf{A}) = H(\mathbf{A}_1) = \{a_1, \dots, a_h\}$ and $d_i = \operatorname{ord}(a_i) > 1$*

for $1 \le i \le h$. Also, let $\ell(\mathbf{A})$ be the least common multiple of the numbers $d_1, \dots, d_h$. The following hold:

a) $N(\mathbf{A}_1) \le \binom{\ell(\mathbf{A})+h-1}{h-1} - h$ *and, in particular,* $|S_{\mathbf{A}}| \le \binom{\ell(\mathbf{A})+h-1}{h-1} + n - h$.

b) $N(\mathbf{A}_1) = \binom{\ell(\mathbf{A})+h-1}{h-1} - h$ *if and only if* $H(\mathbf{A}) = H(\mathbf{A}_1) = \{\theta, \theta, \dots, \theta\}$, *where* θ *is an element of order* $\ell(\mathbf{A})$ *in* $\mathbb{F}_q^*$.

Proof. a) Since each d_i divides $q-1$, it follows that $\ell(\mathbf{A})$ divides $q-1$. Let $C_{\ell(\mathbf{A})} \subseteq \mathbb{F}_q^*$ be the cyclic group of order $\ell(\mathbf{A})$. In particular, since $a_i^{\ell(\mathbf{A})} = 1$ for any $1 \le i \le h$, each a_i is in $C_{\ell(\mathbf{A})}$. We have seen that any element $x_1^{b_1} \cdots x_h^{b_h} \in M_{\mathbf{A}_1}^*$ can be associated to a minimal product-one sequence in $\mathbb{F}_q^*$ of length $\sum_{j=1}^h b_j$. In fact, since each a_i is in $C_{\ell(\mathbf{A})}$, such a minimal sequence is in $C_{\ell(\mathbf{A})}$. From Theorem 4.2, any minimal product-one sequence is of length at most $\ell(\mathbf{A})$, hence $\sum_{j=1}^h b_j \le \ell(\mathbf{A})$. In particular, any monomial $x_1^{b_1} \cdots x_h^{b_h} \in M_{\mathbf{A}_1}^*$ is such that $\sum_{j=1}^h b_j \le \ell(\mathbf{A})$. If $\mathcal{M}_h(d)$ denotes the set of all monomials $x_1^{r_1} \cdots x_h^{r_h}$ such that $\sum_{i=1}^h r_i = d$, we define the following map:

$$\begin{array}{rccc} \Lambda_h: & M_{\mathbf{A}_1}^* & \longrightarrow & \mathcal{M}_h(\ell(\mathbf{A})) \\ & x_1^{b_1} \cdots x_h^{b_h} & \longmapsto & x_1^{b_1} \cdot x_2^{b_2} \cdots x_h^{b_h + \ell(\mathbf{A}) - (b_1 + \cdots + b_h)}. \end{array}$$

Clearly, Λ_h is well defined. We claim that Λ_h is one-to-one. In fact, if there are two distinct elements $\mathbf{X}_1 = x_1^{b_1} \cdots x_h^{b_h}$ and $\mathbf{X}_1' = x_1^{b_1'} \cdots x_h^{b_h'}$ in $M_{\mathbf{A}_1}^*$ such that $\Lambda_h(\mathbf{X}_1) = \Lambda_h(\mathbf{X}_1')$, we have $b_i = b_i'$ for $1 \le i \le h-1$ and then, since the elements are distinct, it follows that $b_h \ne b_h'$. For instance, suppose $b_h > b_h'$, hence $\mathbf{X}_1$ is divisible by $\mathbf{X}_1'$, a contradiction with the definition of $M_{\mathbf{A}_1}^*$. Hence, Λ_h is one-to-one and so $|M_{\mathbf{A}_1}^*| \le |\mathcal{M}_h(\ell(\mathbf{A}))|$. A simple calculation yields $|\mathcal{M}_h(\ell(\mathbf{A}))| = \binom{\ell(\mathbf{A})+h-1}{h-1}$. Therefore,

$$N(\mathbf{A}_1) = |M_{\mathbf{A}_1}^*| - h \le \binom{\ell(\mathbf{A}) + h - 1}{h - 1} - h.$$

b) Suppose that $N(\mathbf{A}_1) = \binom{\ell(\mathbf{A})+h-1}{h-1} - h$. In particular, $|M_{\mathbf{A}_1}^*| = |\mathcal{M}_h(\ell(\mathbf{A}))|$, and so the map Λ_h defined above is an one-to-one correspondence. We first consider the case $h > 2$. We observe that the element

$$\mathbf{X} = x_1 \cdots x_{h-2} \cdot x_{h-1}^{\ell(\mathbf{A})-h+2} \in \mathcal{M}_h(\ell(\mathbf{A}))$$

is in the image of $M_{\mathbf{A}_1}^*$ by Λ_h and this easily implies that $\mathbf{X} \in M_{\mathbf{A}_1}^*$. We have seen that the product-one sequence $a(\mathbf{X})$ associated to $\mathbf{X}$ is minimal. Its length is $\ell(\mathbf{A}) = D(C_{\ell(\mathbf{A})})$ but, according to Theorem 4.2, only constant sequences composed by generators have this length. It follows that $a_i = a_1$ for any $i \le h-1$. Similarly, if we define the map Λ_h' as

$$\begin{array}{rccc} \Lambda_h': & M_{\mathbf{A}_1}^* & \longrightarrow & \mathcal{M}_h(\ell(\mathbf{A})) \\ & x_1^{b_1} \cdots x_h^{b_h} & \longmapsto & x_1^{b_1 + \ell(\mathbf{A}) - (b_1 + \cdots + b_h)} \cdot x_2^{b_2} \cdots x_h^{b_h}, \end{array}$$

one can show that Λ'_h must be an one-to-one correspondence and in the same way we obtain $a_i = a_h$ for any $i \geq 2$. Since $h > 2$, we conclude that $a_i = a_1 = \theta$ for every $1 \leq i \leq h$.
For $h = 2$, since Λ_h is onto, it follows that $x_1^k x_2^{\ell(\mathbf{A})-k}$ is in the image of $M^*_{\mathbf{A}_1}$ by Λ_h, for any $1 \leq k < \ell(\mathbf{A})$. But the pre-image of such element is $x_1^k x_2^{s(k)} \in M^*_{\mathbf{A}_1}$ for some positive integer $1 \leq s(k) < \ell(\mathbf{A})$. From the definition of $M^*_{\mathbf{A}_1}$, $x_1^j x_2^{s(j)}$ can not divide $x_1^k x_2^{s(k)}$ for any k and j, i.e., $j > k$ if and only if $s(j) < s(k)$. This shows that $s(1) = \ell(\mathbf{A}) - 1$. Therefore, $x_1 x_2^{\ell(\mathbf{A})-1}$ is in $M^*_{\mathbf{A}_1}$ and it follows from definition that $a_1 \cdot a_2^{\ell(\mathbf{A})-1} = 1$, i.e., $a_1 = a_2$. Hence, $\theta = a_1 = a_2$ is the desired element.
In any case, $H(\mathbf{A}) = H(\mathbf{A}_1) = \{\theta, \theta, \dots, \theta\}$, where θ is an element of order $\ell(\mathbf{A})$ in $\mathbb{F}_q^*$. Conversely, if $H(\mathbf{A}) = \{\theta, \dots, \theta\}$ for some element θ of order $\ell(\mathbf{A})$, we can easily verify that any element of $\mathcal{M}_h(\ell(\mathbf{A}))$ is in $M^*_{\mathbf{A}_1}$ and then $|\mathcal{M}_h(\ell(\mathbf{A}))| \leq |M^*_{\mathbf{A}_1}|$. Since Λ_h is one-to-one, Λ_h must is an one-to-one correspondence (in fact, Λ_h is the identity map in this case). Thus $|M^*_{\mathbf{A}_1}| = |\mathcal{M}_h(\ell(\mathbf{A}))|$, i.e.,

$$N(\mathbf{A}_1) = |M^*_{\mathbf{A}_1}| - h = \binom{\ell(\mathbf{A}) + h - 1}{h - 1} - h. \quad \square$$

Since the number $\ell(\mathbf{A})$ defined above is always a divisor of $q-1$ and $|S_{\mathbf{A}}| = N(\mathbf{A}_1) + n$, Theorem 4.3 implies the following:

Corollary 4.4. *Let $\mathbf{A} \in G^n$ be an element of type (h, t), where $h \geq 2$. Then $|S_{\mathbf{A}}| \leq \binom{q+h-2}{h-1} + n - h$ with equality if and only if there exists a primitive element $\theta \in \mathbb{F}_q^*$ such that $H(\mathbf{A}) = \{\theta, \dots, \theta\}$.*

Example 4.5. If $q = 3$, $-1 \in \mathbb{F}_3$ is the only nonzero element with order greater than one. In particular, for $h \geq 2$ and A an element of type (h, t), $|S_{\mathbf{A}}|$ always attain the bound $\binom{q+h-2}{h-1} + n - h = n + \frac{h(h-1)}{2}$. In fact, for $h = 0, 1$ we have $|S_{\mathbf{A}}| = n$ and so the same equality holds.

We have seen that the bounds for the number $N(\mathbf{A}_1)$ or even the criterion for when $R_{\mathbf{A}}$ is free depend only on the order of the elements in $H(\mathbf{A})$. We finish this section with a simple example, showing that $N(\mathbf{A}_1)$ depends strongly on the elements of $H(\mathbf{A})$, not only on their orders.

Example 4.6. Suppose that $q \equiv 1 \pmod 8$ and let λ be an element of order 8 in $\mathbb{F}_q^*$. Let $\mathbf{A}$ and $\mathbf{A}'$ be the elements of type $(2, 0)$ in G^2 such that $H(\mathbf{A}) = \{\lambda^3, \lambda^2\}$ and $H(\mathbf{A}') = \{\lambda^6, \lambda^7\}$. Both sets $H(\mathbf{A})$ and $H(\mathbf{A}')$ have an element of order 8 and an element of order 4. By a direct calculation, we find $M^*_{\mathbf{A}_1} = \{x^8, x^2y, y^4\}$ and $M^*_{\mathbf{A}'_1} = \{x^4, xy^6, x^2y^4, x^3y^2, y^8\}$. Hence $N(\mathbf{A}_1) = 1$ and $N(\mathbf{A}'_1) = 3$.

5. Invariants through the action of Sylow subgroups of G^n

So far we have studied the structure of the fixed-point subring $R_{\mathbf{A}}$ arising from the $\mathbb{F}_q$-automorphism induced by an element $\mathbf{A} \in G^n$. In this section we consider a more restricted class of invariants. For a subgroup $H \leq G^n$, we define R_H the set of elements in $\mathcal{A}_n$ that are fixed by any element $\mathbf{A} \in H$. In other words, $R_H = \{f \in \mathcal{A}_n \mid \mathbf{A} \circ f = f\,,\ \forall \mathbf{A} \in H\}$, is the *fixed-point* subring of $\mathcal{A}_n$ by H. We consider the ring of invariants R_H, for H a Sylow subgroup of G^n.

Recall that G^n has $q^n(q-1)^n$ elements and let $q-1 = r_1^{\beta_1} \cdots r_s^{\beta_s}$, be the prime factorization of $q-1$, where q is a power of a prime p and $s = \omega(q-1)$. From definition, the Sylow p-subgroups of G^n have order q^n and, for each $1 \leq i \leq s$, the Sylow r_i-subgroups of G^n have order $r_i^{n\beta_i}$. It is well known that any two Sylow r-subgroups are conjugated and, by small modification of Theorem 2.5, we see that any two conjugated groups $H, H' \in G^n$ have isomorphic fixed-point subrings. In particular, we just have to work with specific Sylow r-groups of G^n. We will naturally choose the simplest ones.

We summarize the ideas contained in this section. Essentially, we try to find a set of generators for H such that their correspondents $\mathbb{F}_q$-automorphisms leave fixed all but one variable in $\{x_1, \ldots, x_n\}$. Using separation of variables (Lemma 2.8), we characterize independently the ring of invariants for each automorphism. The ring R_H will be the intersection of such rings; at this step, we follow the same steps as in the proof of Proposition 3.1. For simplicity, we omit proofs that are completely analogous to the ones that we have already done.

5.1. *Homotheties and Sylow r_i-subgroups*

We start fixing some notation. For any nonzero element $a \in \mathbb{F}_q$, set $A(a) = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \in G$. For each prime divisor r_i of $q-1$, let $G(r_i) \leq G$ be the set of matrices $A(a)$, where $a \in \mathbb{F}_q^*$ is such that $a^{r_i^{\beta_i}} = 1$. Clearly $G(r_i)$ is a group with $r_i^{\beta_i}$ elements. Therefore, $H(r_i) := G(r_i)^n \leq G^n$ has order $r_i^{n\beta_i}$, i.e., $H(r_i)$ is a Sylow r_i-subgroup of G^n. If $\theta_i \in \mathbb{F}_q^*$ is an element of order $r_i^{\beta_i}$, we can verify that $H(r_i)$ is generated by $\{\mathbf{A}_j(\theta_i),\ 1 \leq j \leq n\}$, where $\mathbf{A}_j(\theta_i) = (I, \ldots, A(\theta_i), \ldots, I)$ is the element of G^n such that its k-th coordinate is the identity matrix I for $k \neq j$ and the j-th coordinate of $\mathbf{A}_j(\theta_i)$ is the matrix $A(\theta_i)$. In particular, the $\mathbb{F}_q$-automorphism induced by $\mathbf{A}_j(\theta_i)$ fixes each variable x_k for $k \neq j$ and maps x_j to $\theta_i x_j$. Since $\{\mathbf{A}_j(\theta_i), 1 \leq j \leq n\}$ generates $H(r_i)$, $f \in R_{H(r_i)}$ if and only if

$$f = \mathbf{A}_1(\theta_i) \circ f = \mathbf{A}_2(\theta_i) \circ f = \cdots = \mathbf{A}_n(\theta_i) \circ f. \tag{2}$$

In other words, $f(x_1, \ldots, x_n) = f(x_1, \theta_i x_2, \ldots, x_n) = \cdots = f(x_1, x_2, \ldots, \theta_i x_n)$.

We obtain the following:

Proposition 5.1. *For a fixed i such that $1 \le i \le s = \omega(q-1)$, set $d(i) = r_i^{\beta_i}$. Then $R_{H(r_i)} = \mathbb{F}_q[x_1^{d(i)}, \dots, x_n^{d(i)}]$ and, in particular, $R_{H(r_i)}$ is a free $\mathbb{F}_q$-algebra, isomorphic to $\mathcal{A}_n$.*

Proof. From Eq. (2), we can see that $R_{H(r_i)} = \bigcap_{1\le j\le n} R_{\mathbf{A}_j(\theta_i)}$. Also, a "translated" version of Proposition 2.12 for each $\mathbf{A}_j(\theta_i)$ yields

$$R_{\mathbf{A}_j(\theta_i)} = \mathbb{F}_q[x_1, \dots, x_j^{d(i)}, \dots, x_n].$$

Following the proof of Proposition 3.1, we obtain

$$\bigcap_{1\le j\le n} R_{\mathbf{A}_j(\theta_i)} = \mathbb{F}_q[x_1^{d(i)}, \dots, x_n^{d(i)}].$$

Therefore, $R_{H(r_i)} = \mathbb{F}_q[x_1^{d(i)}, \dots, x_n^{d(i)}]$. Since $d(i)$ is a divisor of $q-1$, it follows from Corollary 3.5 that $R_{H(r_i)}$ is generated by n algebraically independent elements of $\mathcal{A}_n$. In particular, $R_{H(r_i)}$ is a free $\mathbb{F}_q$-algebra, isomorphic to $\mathcal{A}_n$. □

5.2. Translations and Sylow p-subgroups

For any element $a \in \mathbb{F}_q$, set $B(a) = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \in G$. Also, let $G(p) \le G$ be the set of matrices of the form $B(a)$ for some $a \in \mathbb{F}_q$. Clearly $G(p)$ is a group with q elements. Hence $H(p) := G(p)^n \le G^n$ has order q^n, i.e., $H(p)$ is a Sylow p-subgroup of G^n. Notice that $G(p)$ is generated by the set $\{\mathbf{B}_j(a), a \in \mathbb{F}_q, 1 \le j \le n\}$, where $\mathbf{B}_j(a) = (I, \dots, B(a), \dots, I)$ is the element of G^n such that its i-th coordinate is the identity matrix I for $i \ne j$ and the j-th coordinate of $\mathbf{B}_j(a)$ is the matrix $B(a)$. We start looking at the case $n = 1$: $B(a) \circ f = f(x+a)$. From Theorem 2.5 of [7] we can easily deduce the following.

Lemma 5.2. *A polynomial $f(x) \in \mathbb{F}_q[x]$ satisfies $f(x) = f(x+b)$ for all $b \in \mathbb{F}_q$ if and only if $f(x) = g(x^q - x)$, for some $g(x) \in \mathbb{F}_q[x]$.*

We note that $R_{H(p)}$ comprises the elements $f \in \mathcal{A}_n$ such that

$$f(x_1, \dots, x_i + b, \dots, x_n) = f,$$

for any $1 \le i \le n$ and any $b \in \mathbb{F}_q$. Using the previous lemma and the same ideas in the proof of Proposition 5.1, we deduce the following result.

Proposition 5.3. *The fixed-point subring $R_{H(p)}$ of $\mathcal{A}_n$ by $H(p)$ satisfies*

$$R_{H(p)} = \mathbb{F}_q[x_1^q - x_1, \dots, x_n^q - x_n].$$

In particular, $R_{H(p)}$ is a free $\mathbb{F}_q$-algebra, isomorphic to $\mathcal{A}_n$.

Combining Propositions 5.1 and 5.3, we conclude the following theorem.

Theorem 5.4. *Let r be any prime divisor of $p(q-1)$ and H a Sylow r-subgroup of G^n. The fixed-point subring R_H of $\mathcal{A}_n$ by H is a free $\mathbb{F}_q$-algebra, isomorphic to $\mathcal{A}_n$.*

6. Conclusions

In this paper, we notice that, for

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}, a, b \in \mathbb{F}_q, a \neq 0 \right\},$$

the group $G^n \subset \mathrm{GL}_2(\mathbb{F}_q)^n$ acts on the ring of polynomials in n variables over $\mathbb{F}_q$. For $\mathbf{A} \in G^n$, we explore the algebraic properties of the fixed-point subring $R_{\mathbf{A}}$. In particular, we provide a minimal generating set $S_{\mathbf{A}}$ for $R_{\mathbf{A}}$. We give a criteria for when $R_{\mathbf{A}}$ is free, we provide upper bounds for the size of $S_{\mathbf{A}}$ and characterize the elements $\mathbf{A}$ for which this bound is attained. In our approach, some algebraic structures of $R_{\mathbf{A}}$ are naturally related to other topics, such as the minimal product-one sequences in abelian groups.

Acknowledgments

This work was conducted during a visit to Carleton University, supported by CAPES-Brazil (process – 88881.134747/2016-01).

References

[1] H.E.A. Campbell, D.L. Wehlau, Modular Invariant Theory, Encyclopedia of Mathematical Sciences, vol. 139, Springer, 2011.

[2] D. Cox, J. Little, D. O'Shea, Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra, Springer, 2015.

[3] Z. Dvir, A. Gabizon, A. Wigderson, Extractors and rank extractors for polynomial sources, Comput. Complex. 1 (2009) 1.

[4] W. Gao, W. Geroldinger, W.A. Schmid, Inverse zero-sum problems, Acta Arith. 128 (3) (2007) 245–279.

[5] T. Garefalakis, On the action of $\mathrm{GL}(2, q)$ on irreducible polynomials over $\mathbb{F}_q$, J. Pure Appl. Algebra 215 (2011) 1835–1843.

[6] G. Kapetanakis, Prescribing coefficients of invariant irreducible polynomials, J. Number Theory 180 (2017) 615–628.

[7] L. Reis, The action of $\mathrm{GL}_2(\mathbb{F}_q)$ on irreducible polynomials over $\mathbb{F}_q$, revisited, J. Pure Appl. Algebra 222 (2018) 1087–1094.

[8] H. Stichtenoth, A. Topuzoğlu, Factorization of a class of polynomials over finite fields, Finite Fields Appl. 18 (2012) 108–122.