Journal of Pure and Applied Algebra 222 (2018) 1087–1094

Contents lists available at ScienceDirect

Journal of Pure and Applied Algebra

www.elsevier.com/locate/jpaa

# The action of $\mathrm{GL}_2(\mathbb{F}_q)$ on irreducible polynomials over $\mathbb{F}_q$, revisited

Lucas Reis

*Departamento de Matemática, Universidade Federal de Minas Gerais, UFMG, Belo Horizonte, MG, 30123-970, Brazil*

ARTICLE INFO

*Article history:*
Received 4 October 2016
Received in revised form 6 April 2017
Available online 9 June 2017
Communicated by I.M. Duursma

*MSC:*
12E20; 11T55

ABSTRACT

Let $\mathbb{F}_q$ be the finite field with $q$ elements, $p = \mathrm{char}(\mathbb{F}_q)$. The group $\mathrm{GL}_2(\mathbb{F}_q)$ acts naturally in the set of irreducible polynomials over $\mathbb{F}_q$ of degree at least 2. In this paper we are interested in the characterization and number of the irreducible polynomials that are fixed by the elements of a subgroup $H$ of $\mathrm{GL}_2(\mathbb{F}_q)$. We make a complete characterization of the fixed polynomials in the case when $H$ has only elements of the form $\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)$, corresponding to translations $x \mapsto x + b$ and, as a consequence, the case when $H$ is a $p$-subgroup of $\mathrm{GL}_2(\mathbb{F}_q)$. This paper also contains alternative solutions for the cases when $H$ is generated by an element of the form $\left(\begin{smallmatrix} a & 0 \\ 0 & 1 \end{smallmatrix}\right)$, obtained by Garefalakis (2010) and $H = \mathrm{PGL}_2(\mathbb{F}_q)$, obtained by Stichtenoth and Topuzoglu (2011).



## 1. Introduction

Let $\mathbb{F}_q$ be the finite field with $q$ elements, $p = \mathrm{char}(\mathbb{F}_q)$. As it was noticed in [3] and [7], there is a natural action of the group $\mathrm{GL}_2(\mathbb{F}_q)$ on the set $I$ of irreducible polynomials of degree at least 2 in $\mathbb{F}_q[x]$. Namely, given $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in $\mathrm{GL}_2(\mathbb{F}_q)$ and $f(x) \in I$ of degree $n$ we can define

$$A \circ f = (cx + d)^n f\left(\frac{ax + b}{cx + d}\right).$$

It can be verified that $f$ and $A \circ f$ have the same degree and $A \circ (B \circ f) = (AB) \circ f$ for any $A, B \in \mathrm{GL}_2(\mathbb{F}_q)$. From this definition, two interesting theoretical questions arise:

a) Given a subgroup $H$ of $\mathrm{GL}_2(\mathbb{F}_q)$, which elements $f \in I$ are fixed by $H$, i.e., $A \circ f = f$ for any $A \in H$?
b) How many fixed elements of a given degree exist?

*E-mail address:* lucasreismat@gmail.com.

http://dx.doi.org/10.1016/j.jpaa.2017.06.008
0022-4049/

In [7], the authors gave a complete characterization of the elements $f \in I$ that are fixed by $H = \langle A \rangle$, where $A$ is any element of $\mathrm{GL}_2(\mathbb{F}_q)$. Earlier, the same characterization was given in [3] for the special cases $A = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$, corresponding to the homothety $x \mapsto ax$ and the translation $x \mapsto x+b$, respectively, including enumeration formulas. Combining those results, in [3] the author also obtained enumeration formulas for the case when $A$ is an upper triangular matrix in $\mathrm{GL}_2(\mathbb{F}_q)$.

In this paper we also consider only translations and homotheties but with an alternative characterization of the invariant polynomials. Section 2 is devoted to extend the results of Garefalakis [3] for translations, considering now any family of translations $\{x \mapsto x+s\,; s \in S\}$, where $S \subseteq \mathbb{F}_q$. Section 3 includes alternative proofs of the enumeration formula in [3] for homotheties and the characterization in [7] of all irreducible polynomials that are invariant under the action of the whole group $\mathrm{PGL}_2(\mathbb{F}_q)$. In Section 4, using the canonical conjugation in $\mathrm{GL}_2(\mathbb{F}_q)$ and the results of Section 2, we count the irreducible polynomials that are fixed by a given $p$-subgroup $H$ of $\mathrm{GL}_2(\mathbb{F}_q)$.

## 2. S-translation invariant polynomials

Throughout this paper $\mathbb{F}_q$ denotes the finite field with $q$ elements, where $q = p^l$ is a prime power and $\mathrm{ord}(a)$ denotes the multiplicative order of an element $a \in \mathbb{F}_q^*$. Also, for an irreducible polynomial $f(x) = x^n + ax^{n-1} + \cdots + c \in \mathbb{F}_q[x]$, the element $a$ is called the *trace* of $f(x)$.

If $S \subseteq \mathbb{F}_q$, we say that $f(x) \in \mathbb{F}_q[x]$ is an $S$-translation invariant polynomial if $f(x+s) = f(x)$ for all $s \in S$.

**Example 2.1.** $f(x) = x^q - x$ is an $\mathbb{F}_q$-translation invariant polynomial.

For $S \subseteq \mathbb{F}_q$ and $n \geq 2$, let $C_S(n)$ be the set of all $S$-translation invariant monic irreducible polynomials of degree $n$ over $\mathbb{F}_q$. Suppose that $a, b \in \mathbb{F}_q^*$ and $f(x) \in \mathbb{F}_q[x]$ is a polynomial such that $f(x+a) = f(x)$ and $f(x+b) = f(x)$. Clearly $f(x+0) = f(x)$ and then, by induction, we have that

$$f(x + ia + jb) = f(x)$$

for all $i, j \in \mathbb{F}_p$. In particular, if $S' \subseteq \mathbb{F}_q$ is the $\mathbb{F}_p$-vector space generated by $S$, then $C_{S'}(n) \supseteq C_S(n)$. The converse inclusion is obviously true and so $C_{S'}(n) = C_S(n)$. From now, $S \subseteq \mathbb{F}_q$ denotes an $\mathbb{F}_p$-vector space of dimension $r > 0$.

**Remark 2.2.** If $f(x) \in \mathbb{F}_q[x]$ is an $S$-translation invariant polynomial and $a \in \mathbb{F}_q^*$, then $g(x) = a^n f(a^{-1}x)$ is an $S'$-translation invariant polynomial, where $S' = \{as \,|\, s \in S\}$. Moreover, if $S$ is an $\mathbb{F}_p$-vector space then so is $S'$.

The observations above lead us to the following definition:

**Definition 2.3.** Let $S, S' \subseteq \mathbb{F}_q$ be $\mathbb{F}_p$-vector spaces. We say that $S$ and $S'$ are $\mathbb{F}_q$-*linearly equivalent* and write $S \sim_{\mathbb{F}_q} S'$ if there exists $a \in \mathbb{F}_q^*$ such that $S' = \{as \,|\, s \in S\}$.

It is immediate from definition that the relation $\sim_{\mathbb{F}_q}$ is an equivalence relation. Moreover, this relation gives an interesting invariant:

**Lemma 2.4.** *If $S \sim_{\mathbb{F}_q} S'$, then $|C_S(n)| = |C_{S'}(n)|$ for all $n \in \mathbb{N}$.*

**Proof.** If $S \sim_{\mathbb{F}_q} S'$, then $S' = \{as \,|\, s \in S\}$ for some $a \in \mathbb{F}_q^*$. Let $I_n(q)$ be the set of all monic irreducible polynomials of degree $n$ over $\mathbb{F}_q$ and

$$\begin{array}{rccc} \tau_a: & I_n(q) & \to & I_n(q) \\ & f(x) & \mapsto & a^n f(a^{-1}x). \end{array}$$

Clearly $\tau_a$ is well defined and is one to one. From Remark 2.2, we know that $\tau_a(f(x)) \in C_{S'}(n)$ for any $f(x) \in C_S(n)$. Therefore we have that $|C_S(n)| \leq |C_{S'}(n)|$. Since the relation $\sim_{\mathbb{F}_q}$ is symmetric, it follows that $|C_{S'}(n)| \leq |C_S(n)|$ and this completes the proof. □

The following theorem gives a characterization of the $S$-translation invariant polynomials over $\mathbb{F}_q$.

**Theorem 2.5.** *Let $S \subseteq \mathbb{F}_q$ be an $\mathbb{F}_p$-vector space of dimension $r > 0$ and*

$$P_S(x) := \prod_{s \in S} (x - s).$$

*Then $g(x) \in \mathbb{F}_q[x]$ is an $S$-translation invariant polynomial if, and only if, there exists some polynomial $f(x) \in \mathbb{F}_q[x]$ such that $g(x) = f(P_S(x))$. In particular, any $S$-translation invariant polynomial has degree divisible by $\deg P_S(x) = |S| = p^r$.*

**Proof.** Assume that $g(x)$ is an $S$-translation invariant polynomial over $\mathbb{F}_q$. We proceed by induction on $n = \deg g(x)$. If $g(x)$ is constant, there is nothing to prove. Suppose that the statement is true for all polynomials of degree at most $n$ and let $g(x)$ be an $S$-translation invariant polynomial of degree $n+1$. We have $g(0) = g(s)$ for all $s \in S$ and so the polynomial $g(x) - g(0)$ has degree $n + 1 > 0$ and vanishes at $s$ for all $s \in S$. In particular we have that

$$g(x) - g(0) = P_S(x)G(x), \tag{1}$$

for some non-zero polynomial $G(x) \in \mathbb{F}_q[x]$. Since $g(x + s) - g(0) = g(x) - g(0)$ and $P_S(x + s) = P_S(x)$ for all $s \in S$, by equation (1) it follows that $G(x)$ is an $S$-translation invariant polynomial over $\mathbb{F}_q$ and $\deg G(x) < \deg g(x)$. By the induction hypothesis we have that $G(x) = F(P_S(x))$ for some $F(x) \in \mathbb{F}_q[x]$. Therefore $g(x) = P_S(x)F(P_S(x)) + g(0)$ and so $g(x) = f(P_S(x))$ where $f(x) = xF(x) + g(0)$. The converse is obviously true. □

If $1, a \in S$ where $a \notin \mathbb{F}_p$, we have the following:

**Corollary 2.6.** *Let $S \subseteq \mathbb{F}_q$ be an $\mathbb{F}_p$-vector space such that $1, a \in S$ where $a \notin \mathbb{F}_p$. Then any $S$-translation invariant polynomial in $\mathbb{F}_q[x]$ is of the form*

$$f(x^{p^2} - x^p(1 + (a - a^p)^{p-1}) + x(a - a^p)^{p-1})$$

*for some polynomial $f(x) \in \mathbb{F}_q[x]$.*

**Proof.** Since $1, a \in S$ and $a \notin \mathbb{F}_p$, we have that any $S$-translation invariant polynomial is also a $S'$-translation invariant, where $S' = \langle 1, a \rangle_{\mathbb{F}_p} = \{j + ai \,|\, i, j \in \mathbb{F}_p\}$. In addition, notice that

$$P_{S'}(x) = \prod_{0 \leq i,j \leq p-1} (x - j - ai) = x^{p^2} - x^p(1 + (a - a^p)^{p-1}) + x(a - a^p)^{p-1}. \quad \square$$

The main result of this paper is the following:

**Theorem 2.7.** *Let $\mathbb{F}_q$ be the finite field with $q = p^l$ elements and $S \subseteq \mathbb{F}_q$ be an $\mathbb{F}_p$-vector space of dimension $r > 0$.*

a) *If* $r > 1$ *then* $|C_S(n)| = 0$ *for all* $n$.
b) *If* $r = 1$ *and* $n$ *is not divisible by* $p$ *then* $|C_S(n)| = 0$.
c) *If* $r = 1$ *and* $n = pm$, *then*

$$|C_S(n)| = \frac{p-1}{pm} \sum_{\substack{d|m \\ \gcd(d,p)=1}} q^{m/d}\mu(d).$$

**Remark 2.8.** In [5], the authors define **translation invariant polynomials** over $\mathbb{F}_q$, which are the polynomials $f(x) \in \mathbb{F}_q[x]$ such that $f(x+b) = f(x)$ for all $b \in \mathbb{F}_q$, and obtain an enumeration formula for irreducible polynomials: if $n$ is not divisible by $q$, the number of **translation invariant** monic irreducible polynomials over $\mathbb{F}_q$ of degree $n$ is zero and, if $n = mq$, this number is

$$\frac{q-1}{qm} \sum_{\substack{d|m \\ \gcd(d,p)=1}} q^{m/d}\mu(d).$$

In this context, item (a) of Theorem 2.7 shows that this only holds in the case when $q = p$ is prime. In fact, if $q > p$, then $S = \mathbb{F}_q$ is an $\mathbb{F}_p$-vector space of dimension greater than one and, from item (a) of Theorem 2.7, there are no irreducible polynomials over $\mathbb{F}_q$ such that $f(x+b) = f(x)$ for all $b \in \mathbb{F}_q$.

### *2.1. Lemmata*

In order to prove Theorem 2.7, we have to discuss the irreducibility of the polynomials $f(P_S(x)) \in \mathbb{F}_q[x]$. In this direction, Lemmas 2.9 and 2.10 give some criteria to ensure the irreducibility of special polynomial compositions and Lemma 2.11 will be useful in the proof of the enumeration formula in Theorem 2.7.

**Lemma 2.9** *([1]). Let* $f(x) = x^n + Bx^{n-1} + \cdots + c \in \mathbb{F}_q[x]$ *be an irreducible polynomial, where* $q = p^l$ *is a prime power. The polynomial* $f(x^{p^{2t}} - ax^{p^t} - bx)$ *is also irreducible over* $\mathbb{F}_q[x]$ *if and only if the following conditions are satisfied:*

a) $p = 2, t = 1, n$ *is odd and* $B \neq 0$,
b) $\gcd(x^3 - ax - b, x^{2^l} - x) \neq 1$,
c) $\mathrm{Tr}_{L/K}(\beta^{-2}B) = \mathrm{Tr}_{L/K}(\alpha^{-2}\beta) = 1$, *where* $L = \mathbb{F}_{2^l}, K = \mathbb{F}_2$ *and* $\alpha, \beta$ *are two elements in* $L$ *such that* $\alpha^2 + \beta = a$ *and* $\alpha\beta = b$.

**Lemma 2.10** *([4], Theorem 3.82). Let* $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + c \in \mathbb{F}_q[x]$ *be an irreducible polynomial,* $p = \mathrm{char}(\mathbb{F}_q)$ *and* $b \in \mathbb{F}_q$. *The polynomial* $f(x^p - x - b)$ *is also irreducible over* $\mathbb{F}_q[x]$ *if and only if* $\mathrm{Tr}_{L/K}(nb - a_{n-1}) \neq 0$ *where* $L = \mathbb{F}_q$ *and* $K = \mathbb{F}_p$.

**Lemma 2.11** *([6]). The number of monic irreducible polynomials over* $\mathbb{F}_q$ *with degree* $n$ *and a given trace* $a \neq 0$ *is*

$$\frac{1}{qn} \sum_{\substack{d|n \\ \gcd(d,p)=1}} q^{n/d}\mu(d).$$

### *2.2. Proof of Theorem 2.7*

If $S \subseteq \mathbb{F}_q$ is any $\mathbb{F}_p$-vector space of dimension $r > 0$ and $a \in S \setminus \{0\}$, then $a^{-1}S \sim_{\mathbb{F}_q} S$ and $1 \in a^{-1}S$. Thus, using Lemma 2.4, we can suppose that $1 \in S$.

a) Let $n$ be a positive integer and $S \subseteq \mathbb{F}_q$ be an $\mathbb{F}_p$-vector space of dimension $r > 1$ such that $1 \in S$. Since $r > 1$, there is some element $\gamma \in S \setminus \mathbb{F}_p$. It follows from Corollary 2.6 that any $g(x) \in C_S(n)$ is of the form

$$f(x^{p^2} - x^p(1 + (\gamma - \gamma^p)^{p-1}) + x(\gamma - \gamma^p)^{p-1}).$$

Therefore, by Lemma 2.9, $g(x)$ is reducible whenever $p > 2$.
If $p = 2$, we have that $g(x) = f(x^4 - ax^2 - bx)$ where $a = \gamma^2 + \gamma + 1$ and $b = \gamma^2 + \gamma$. Now consider the following system of equations:

$$\begin{aligned} \alpha^2 + \beta &= a \\ \alpha\beta &= b. \end{aligned} \tag{2}$$

Notice that, for any solution $(\alpha, \beta)$ of system (2), $\alpha$ is a root of the equation $y^3 - ay + b = 0$ and $\beta = a - \alpha^2$. In particular the system (2) has at most three solutions and since $(\alpha, \beta) = (1, \gamma^2+\gamma), (\gamma, \gamma+1), (\gamma+1, \gamma)$ are solutions these are all of them.
Condition (c) of Lemma 2.9 says that, for some solution $(\alpha, \beta)$ of (2), we have $\mathrm{Tr}_{L/K}(\alpha^{-2}\beta) = 1$ where $L = \mathbb{F}_{2^l}$ and $K = \mathbb{F}_2$. In particular, if $(\alpha, \beta) = (1, \gamma^2 + \gamma)$, then

$$\mathrm{Tr}_{L/K}(\alpha^{-2}\beta) = \mathrm{Tr}_{L/K}(\gamma^2) + \mathrm{Tr}_{L/K}(\gamma) = \mathrm{Tr}_{L/K}(\gamma) + \mathrm{Tr}_{L/K}(\gamma) = 0 \neq 1.$$

The other two solutions of (2) satisfy $\beta = \alpha + 1$ and in these cases we have

$$\mathrm{Tr}_{L/K}(\alpha^{-2}\beta) = \mathrm{Tr}_{L/K}(\alpha^{-1}) + \mathrm{Tr}_{L/K}((\alpha^{-1})^2) = \mathrm{Tr}_{L/K}(\alpha^{-1}) + \mathrm{Tr}_{L/K}(\alpha^{-1}) = 0 \neq 1.$$

Thus $g(x)$ is never irreducible if $r > 1$ and this completes the proof of a).

b) It follows directly from Theorem 2.5, since any polynomial of the form $f(P_S(x))$ has degree divisible by $|S| = p$.

c) Since $r = 1$ and $1 \in S$, we have $S = \mathbb{F}_p$. Let $m$ be any positive integer and $g(x)$ be an irreducible polynomial of degree $pm$. From Theorem 2.5 we have that $g(x) \in C_S(pm)$ if and only if $g(x)$ is of the form $f(P_S(x)) = f(x^p - x)$, where $f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0$ is an irreducible polynomial over $\mathbb{F}_q$.
From Lemma 2.10, the polynomial $f(x^p - x) \in \mathbb{F}_q[x]$ is irreducible if, and only if, $\mathrm{Tr}_{L/K}(a_{m-1}) \neq 0$, where $L = \mathbb{F}_q$ and $K = \mathbb{F}_p$. It is well known that for each $a \in K$, the equation $\mathrm{Tr}_{L/K}(y) = a$ has $\frac{q}{p}$ distinct solutions. Thus for exactly $(p-1)\frac{q}{p}$ elements $a_{m-1} \in \mathbb{F}_q$ we have $\mathrm{Tr}_{L/K}(-a_{m-1}) \neq 0$ and any of these elements is nonzero. For a fixed $\beta \in \mathbb{F}_q^*$, by Lemma 2.11, there exist exactly

$$\frac{1}{qm} \sum_{\substack{d|m \\ \gcd(d,p)=1}} q^{m/d}\mu(d)$$

monic irreducible polynomials over $\mathbb{F}_q$ with degree $m$ and trace $\beta$. Thus the number of monic irreducible polynomials $f(x) \in \mathbb{F}_q[x]$ of degree $m$ such that $f(x^p - x) \in \mathbb{F}_q[x]$ is also irreducible equals

$$(p-1)\frac{q}{p} \cdot \frac{1}{qm} \sum_{\substack{d|m \\ \gcd(d,p)=1}} q^{m/d}\mu(d) = \frac{p-1}{pm} \sum_{\substack{d|m \\ \gcd(d,p)=1}} q^{m/d}\mu(d).$$

Since the polynomials $f(x^p - x)$ are all distinct when $f(x)$ runs through $I_m(q)$, we are done.

## 3. Miscellanea

Using some ideas and results presented in Section 2, we give alternative proofs of two interesting results concerning the action of $\mathrm{GL}_2(\mathbb{F}_q)$ on irreducible polynomials.

### 3.1. Polynomials invariant under homotheties

Given $a \in \mathbb{F}_q \setminus \{0,1\}$, we are interested in counting the number of monic irreducible polynomials $g(x)$ that are invariant under the homothety $x \mapsto ax$, i.e., $g(ax) = g(x)$. We have the following characterization:

**Theorem 3.1.** *Let $f(x) \in \mathbb{F}_q[x]$, $a \in \mathbb{F}_q^*$ and $k = \mathrm{ord}(a)$. Then $f(ax) = f(x)$ if and only if there exists $g(x) \in \mathbb{F}_q[x]$ such that*

$$f(x) = g(P_a(x)),$$

*where $P_a(x) = \prod_{i=0}^{k-1}(x - a^i) = x^k - 1$. In particular, any polynomial invariant under the homothety $x \mapsto ax$ has degree divisible by $k$.*

**Proof.** Notice that if $f(ax) = f(x)$ and $k = \mathrm{ord}(a)$ is the order of $a \in \mathbb{F}_q$, then $f(1) = f(a^i)$ for all $0 \leq i \leq k-1$; from now, the proof is quite similar to the one of Theorem 2.5. □

For an element $a \in \mathbb{F}_q^*$, let $N_a(n)$ be the number of monic irreducible polynomials $f(x) \in \mathbb{F}_q[x]$ of degree $n$ such that $f(ax) = f(x)$. From the previous theorem, we know that $N_a(n) = 0$ if $n$ is not divisible by $k = \mathrm{ord}(a)$. Let $L(m,k)$ be the number of monic irreducible polynomials of the form $F(x^k)$, where $F$ has degree $m$. Notice that, from Theorem 3.1, $N_a(mk)$ is exactly the number of monic irreducible polynomials of the form $f(x^k - 1)$ where $f$ has degree $m$. Since $f(x^k - 1) = F(x^k)$ for $F(x) = f(x-1)$ and $\{f(x-1) | f \in I_m(q)\} = I_m(q)$, the number of monic irreducible polynomials $F$ of degree $m$ for which $F(x^k)$ is also irreducible is the same for the composition $F(x^k - 1)$. In particular, we have proved that $N_a(mk) = L(m,k)$. Combining the previous equality with the enumeration formula for $L(m,k)$ presented in [2, Theorem 3], we directly deduce the enumeration formula of Garefalakis for homotheties:

**Theorem 3.2** *([3], Theorem 4). If $n$ is not divisible by $k = \mathrm{ord}(a)$, then $N_a(n) = 0$ and, if $n = mk$, we have*

$$N_a(mk) = \frac{\varphi(k)}{mk} \sum_{\substack{d|m \\ \gcd(d,k)=1}} \mu(d)(q^{m/d} - 1).$$

### 3.2. The action of $\mathrm{PGL}_2(\mathbb{F}_q)$ on irreducible polynomials

Consider the projective linear group $G = \mathrm{PGL}_2(\mathbb{F}_q) \approx \mathrm{GL}_2(\mathbb{F}_q)/\sim$, where $A \sim B$ if $A = \lambda B$ for some $\lambda \in \mathbb{F}_q^*$. We are interested in finding the monic irreducible polynomials $f(x) \in \mathbb{F}_q[x]$ such that $A \circ f = f$ for any $A \in G$. As it was shown in [7], in general there are no such polynomials:

**Theorem 3.3** *([7], Proposition 4.8). Let $f \in \mathbb{F}_q[x]$ be a monic irreducible polynomial of degree $n \geq 2$. Suppose that $A \circ f = f$ for all $A \in \mathrm{PGL}_2(\mathbb{F}_q)$. Then $n = q = 2$ and $f(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$.*

Here we give an alternative proof of this fact: let $f \in \mathbb{F}_q[x]$ be as above. Since all $2 \times 2$ matrices corresponding to translations belong to $\mathrm{PGL}_2(\mathbb{F}_q)$, $f$ must be an $\mathbb{F}_q$-translation invariant and, from Theorem 2.7 part a), we know that this is only possible when $\mathbb{F}_q$ is a prime field. Thus $q = p$ prime. Also, from Theorem 2.5, we know that there exists some polynomial $g(x)$ with nonzero trace such that $f(x) = g(x^p - x)$.

Now, if $p > 2$, then there is some element $a \in \mathbb{F}_p$ such that $k = \mathrm{ord}(a) > 1$. Since all homotheties also belong to $\mathrm{PGL}_2(\mathbb{F}_q)$, it follows that $f(x) = f(ax)$ or, equivalently, $g(x^p - x) = g_2(x^p - x)$, where $g_2(x) = g(ax)$. Therefore $g(x) = g_2(x)$, i.e., $g(x)$ is also invariant under the homothety $x \mapsto ax$. From Theorem 3.1 we have that $g(x) = h(x^k - 1)$ for some $h(x) \in \mathbb{F}_p[x]$. Since $k > 1$, a direct calculation shows that $g(x)$ has trace equal to zero, a contradiction.

Thus $p = 2$, $f(x) = g(x^2 + x)$ and $\deg f(x) = 2N = 2 \deg g(x)$. Let

$$\gamma, \gamma^2, \cdots, \gamma^{2^{2N-1}}$$

be the roots of $f(x)$. Notice that $f(\gamma + 1) = g(\gamma^2 + \gamma) = 0$ and then $\gamma + 1 = \gamma^{2^j}$ for some $0 < j < 2N$. In other words, $F(x) = x^{2^j} + x + 1 \in \mathbb{F}_2[x]$ has $\gamma$ as a root. By hypothesis, $f(x) \in \mathbb{F}_2[x]$ is irreducible, and thus $f(x)$ divides $F(x)$. Now, since the inversion $f^*(x) = x^n f(1/x)$ also belong to $\mathrm{PGL}_2(\mathbb{F}_q)$, it follows that $x^n f(1/x) = f(x)$ and so $f^*(x) = f(x)$ divides $F^*(x) = x^{2^j} + x^{2^j - 1} + 1$. Thus $f(x)$ divides $F(x) + x(F^*(x) + F(x)) = x^2 + x + 1$. Since $\deg f(x) \geq 2$, the only possibility is $f(x) = x^2 + x + 1$. It can be easily verified that $f(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$ is irreducible and $A \circ f = f$ for all $A \in \mathrm{PGL}_2(\mathbb{F}_2)$.

## 4. $p$-Subgroups of $\mathbf{GL_2}(\mathbb{F}_q)$

Let $p = \mathrm{char}(\mathbb{F}_q)$. If $S \subseteq \mathbb{F}_q$ is an $\mathbb{F}_p$-vector space of dimension $r$, the set of translations $\{x + s; s \in S\}$ corresponds to the $p$-group $H_S$ of the matrices $\begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix}$ where $s$ runs through $S$, $|H_S| = |S| = p^r$. This correspondence is an one-to-one correspondence between the subgroups of $H_{\mathbb{F}_q}$ and $\mathbb{F}_p$-vector spaces of $\mathbb{F}_q$.

For a $p$-group $H \leq \mathrm{GL}_2(\mathbb{F}_q)$, $I_H(n)$ denotes the set of all monic irreducible polynomials in $\mathbb{F}_q$ of degree $n$ such that $A \circ f = f$ for all $A \in H$. In the previous correspondence, the sets $I_{H_S}(n)$ and $C_S(n)$ (defined in Section 2) are the same.

Combining the observations above with Theorem 2.7 we are able to characterize the numbers $|I_H(n)|$:

**Theorem 4.1.** *Let $H \leq \mathrm{GL}_2(\mathbb{F}_q)$ be any group of order $p^r$.*

a) *If $r > 1$ or $n$ is not divisible by $p$, then $|I_H(n)| = 0$.*
b) *If $r = 1$ and $n = pm$, then*

$$|I_H(n)| = \frac{p-1}{pm} \sum_{\substack{d|m \\ \gcd(d,p)=1}} q^{m/d} \mu(d).$$

**Proof.** Notice that $|\mathrm{GL}_2(\mathbb{F}_q)| = q(q-1)^2(q+1)$ and the sets of all translations in $\mathbb{F}_q$ corresponds to a Sylow $p$-subgroup $G$ of $\mathrm{GL}_2(\mathbb{F}_q)$. Let $H \leq \mathrm{GL}_2(\mathbb{F}_q)$ be any group of order $p^r$. We know that $H$ is contained in some Sylow $p$-subgroup $K$ of $\mathrm{GL}_2(\mathbb{F}_q)$. Since all Sylow $p$-subgroups are conjugate, there is some $A \in \mathrm{GL}_2(\mathbb{F}_q)$ such that $A^{-1}KA = G$ and then $A^{-1}HA$ is a subgroup of $G$ and has order $p^r$. Consider now the following map:

$$\begin{array}{rccc} \tau_{H,A}: & I_H(n) & \to & I_{A^{-1}HA}(n) \\ & f(x) & \mapsto & k_{A,f,n}(A^{-1} \circ f(x)), \end{array}$$

where $k_{A,f,n}$ is the only element in $\mathbb{F}_q$ such that $k_{A,f,n}(A^{-1} \circ f(x))$ is monic. A direct calculation shows that $\tau_{H,A}$ is well defined. Now, suppose that $\tau_{H,A}(f) = \tau_{H,A}(g)$ for some $f, g \in I_H(n)$, i.e., $k_{A,f,n}(A^{-1} \circ f(x)) = k_{A,g,n}(A^{-1} \circ g(x))$. Applying $A$ we get $k_{A,f,n} f = k_{A,g,n} g$. Since $f$ and $g$ are monic irreducible we conclude that $f = g$ and then $\tau_{H,A}$ is one to one. In a similar way we can define a map from $I_{A^{-1}HA}(n)$ into $I_H(n)$. Thus $|I_{A^{-1}HA}(n)| = |I_H(n)|$.

The advantage is that $A^{-1}HA$ is a subgroup of $G$, i.e., $I_{A^{-1}HA}(n) = C_S(n)$ for some $\mathbb{F}_p$-vector space $S$ of dimension $r$. Now, the results follow directly from Theorem 2.7. □

**Acknowledgements**

I would like to thank Daniel Panario and John MacQuarrie for some helpful suggestions in the conclusion of this work.

**References**

[1] S. Agou, Irréductibilité des polynómes $f(x^{p^{2r}} - ax^{p^r} - bx)$ sur un corps fini $\mathbb{F}_{p^s}$, J. Number Theory 10 (1979) 20.
[2] S.D. Cohen, On irreducible polynomials of certain types in finite fields, Math. Proc. Camb. Philos. Soc. 66 (1969) 335–344.
[3] T. Garefalakis, On the action of $\mathrm{GL}_2(\mathbb{F}_q)$ on irreducible polynomials over $\mathbb{F}_q$, J. Pure Appl. Algebra 215 (2011) 1835–1843.
[4] R. Lidl, H. Niederreiter, Introduction to Finite Fields and Their Applications, Cambridge University Press, New York, NY, USA, 1986.
[5] R.C. Mullin, J.L. Yucas, G.L. Mullen, A generalized counting and factoring method for polynomials over finite fields, J. Comb. Math. Comb. Comput. 72 (2010) 121–143.
[6] F. Ruskey, C.R. Miers, J. Sawada, The number of irreducible polynomials and Lyndon words with given trace, SIAM J. Discrete Math. 14 (2001) 240–245.
[7] H. Stichtenoth, A. Topuzoglu, Factorization of a class of polynomials over finite fields, Finite Fields Appl. 18 (2012) 108–122.