The action of $\text{GL}_2(\mathbb{F}_q)$ on irreducible polynomials over $\mathbb{F}_q$

Lucas Reis

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

**Abstract**

Let $\mathbb{F}_q$ be the finite field with $q$ elements, $p = \text{char} \mathbb{F}_q$. The group $\text{GL}_2(\mathbb{F}_q)$ 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 $\text{GL}_2(\mathbb{F}_q)$. We make a complete characterization of the fixed polynomials in the case when $H$ has only elements of the form $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$, corresponding to translations $x \mapsto x + b$, and, as a consequence, the case when $H$ is a $p$–subgroup of $\text{GL}_2(\mathbb{F}_q)$. This paper also contains alternative solutions for the cases when $H$ is generated by an element of the form $\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$, obtained by Garefalakis (2010) [3] and $H = \text{PGL}_2(\mathbb{F}_q)$, obtained by Stichtenoth and Topuzoglu (2011) [6].

**Keywords:** finite fields, irreducible polynomials, group action

2010 MSC: 12E20, 11T55

1. Introduction

Let $\mathbb{F}_q$ be the finite field with $q$ elements, $p = \text{char} \mathbb{F}_q$. As it was noticed in [3] and [6], there is a natural action of the group $\text{GL}_2(\mathbb{F}_q)$ on the set $I$ of irreducible polynomials of degree at least 2 in $\mathbb{F}_q[x]$. Namely, given $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $\text{GL}_2(\mathbb{F}_q)$ 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 all $A, B \in \text{GL}_2(\mathbb{F}_q)$.

From this definition, two interesting theoretical questions arise:

a) Given a subgroup $H$ of $\text{GL}_2(\mathbb{F}_q)$, which elements $f \in I$ are fixed by $H$, i.e., $A \circ f = f$ for all $A \in H$?

b) How many fixed elements exist?

In [6], 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 $\text{GL}_2(\mathbb{F}_q)$. Earlier, the same characterization was given in [3] for the special cases $A = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$ or $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$, corresponding to the homothety $x \mapsto ax$ and the translation $x \mapsto x + b$,
follows that polynomials of degree Lemma 1.

and write $S$ space then so is $S$

Proof. Definition 1.

Remark 1. 2. S-Translation Invariant Polynomials

Throughout this section $\mathbb{F}_q$ denotes the finite field with $q$ elements, where $q = p^k$ is a prime power.

If $S \subset \mathbb{F}_q$, 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 1. $f(x) = x^q - x$ is an $\mathbb{F}_q$-translation invariant polynomial.

Let $C_S(n)$ denote 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 $S' \subset \mathbb{F}_q$ is the $\mathbb{F}_p$-vector space generated by $S$, then $C_{S'}(n) \supset C_S(n)$.

The converse inclusion is obviously true and so $C_S(n) = C_{S'}(n)$. From now, $S \subset \mathbb{F}_q$ will denote an $\mathbb{F}_p$-vector space of dimension $r > 0$.

Remark 1. 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 1. Let $S, S' \subset \mathbb{F}_q$ 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 1. 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 $I_a(q)$ be the set of all monic irreducible polynomials of degree $n$ over $\mathbb{F}_q$ and

$$\tau_a : I_a(q) \rightarrow I_a(q) \quad f(x) \mapsto a^n f(a^{-1}x).$$

Clearly $\tau_a$ is well defined and is one to one. From Remark 1 we know that if $f(x) \in C_S(n)$ then $\tau_a(f(x)) \in C_{S'}(n)$. 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 the finite field $\mathbb{F}_q$.

**Theorem 1.** Let $S \subset \mathbb{F}_q$ 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 then there is nothing to prove. Suppose that the statement is true for all polynomials of degree at most $k$ and let $g(x)$ be an $S$-translation invariant polynomial of degree $k + 1$. We have $g(0) = g(s)$ for all $s \in S$ and so the polynomial $g(x) - g(0)$ has degree $k + 1 > 0$ and vanishes at $s$ for all $s \in S$. In particular we have that

$$g(x) - g(0) = P_S(x)G(x)$$

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 1.** Let $S \subset \mathbb{F}_q$ 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

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

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 $S' = \langle 1, a \rangle_{\mathbb{F}_p} = \{ j + ai \mid j, i \in \mathbb{F}_p \}$. In addition, notice that

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

The main result of this paper is the following:

**Theorem 2.** Let $\mathbb{F}_q$ be the finite field with $q = p^k$ elements and $S \subset \mathbb{F}_q$ 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

$$|C_S(n)| = \frac{p-1}{pm} \sum_{d \mid m} q^{\mu(d)} \mu(d).$$
2.1. Lemmata

In order to prove Theorem 2 we have to discuss the irreducibility of the polynomials \( f(P_S(x)) \in \mathbb{F}_q[x] \). In this direction, Lemmas 2 and 3 give some criteria to ensure the irreducibility of special polynomial compositions and Lemma 4 will be useful in the proof of the enumeration formula in Theorem 2.

**Lemma 2** ([1]). Let \( f(x) = x^n + Bx^{n-1} + \cdots + c \in \mathbb{F}_q[x] \) be an irreducible polynomial, where \( q = p^k \) is a prime power. The polynomial \( f(x^{p^t}) - ax^{p^t} - bx \) 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) \( \gcd(x^3 - ax - b, x^2 - x) \neq 1 \),
c) \( \text{Tr}_{L/K}(\beta^{-2}B) = \text{Tr}_{L/K}(\alpha^{-2} \beta) = 1 \), where \( L = \mathbb{F}_{2t}, K = \mathbb{F}_2 \) and \( \alpha, \beta \) are two elements in \( L \) such that \( \alpha^2 + \beta = a \) and \( \alpha \beta = b \).

**Lemma 3** ([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, \( p = \text{char}\mathbb{F}_q \) 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 \( \text{Tr}_{L/K}(nb - a_{n-1}) \neq 0 \) where \( L = \mathbb{F}_q \) and \( K = \mathbb{F}_p \).

**Lemma 4** ([5]). The number of monic irreducible polynomials over \( \mathbb{F}_q \) with degree \( n \) and a given trace \( a \neq 0 \) is

\[
\frac{1}{qn} \sum_{d|n, d \neq 1} q^{n/d} \mu(d).
\]

2.2. Proof of Theorem 2

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

a) Let \( n \) be a positive integer and \( S \subset \mathbb{F}_q \) 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 1 that any \( g(x) \in C_S(n) \) is of the form

\[
f(x^p - x^n(1 + (\gamma - \gamma^p)^{p-1}) + x(\gamma - \gamma^p)^{p-1}).
\]

Therefore, by Lemma 2 \( g(x) \) 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:

\[
\begin{cases}
\alpha^2 + \beta = a \\
\alpha \beta = b.
\end{cases}
\tag{2}
\]

Notice that, for any solution \((\alpha, \beta)\) of system (2), \( \alpha \) is a root of the equation \( \gamma^3 - ay + b = 0 \) 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.
b) This follows directly from Theorem 1 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 Lemma 1 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 3 the polynomial \( f(x^p - x) \in \mathbb{F}_q[x] \) is irreducible if, and only if, \( \text{Tr}_{L/K}(a_{m-1}) \neq 0 \) where \( L = \mathbb{F}_q \) and \( K = \mathbb{F}_p \). It is well known that for each \( a \in K \), the equation \( \text{Tr}_{L/K}(x) = a \) has \( \frac{q}{p} \) distinct solutions. Thus for exactly \( (p-1)\frac{q}{p} \) values of \( a_{m-1} \in \mathbb{F}_q \) we have \( \text{Tr}_{L/K}(-a_{m-1}) \neq 0 \) and any of these elements is nonzero. For a fixed \( \beta \in \mathbb{F}_q^* \), by Lemma 4 there exist exactly

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

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 is equal to

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

Since the polynomials \( f(x^p - x) \) are all distinct when \( f(x) \) runs through \( I_q(m) \), we are done.

3. Miscellanea

Using the results obtained in Section 2, we give alternative proofs of two interesting results concerning the action of \( \text{GL}_2(\mathbb{F}_q) \) 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. Let \( f(x) \) be a polynomial over \( \mathbb{F}_q \). 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 \( k = \text{ord}(a) \).

Proof. Notice that if \( f(ax) = f(x) \) and \( k = \text{ord}(a) \) 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[1] \( \square \)

Let \( N_a(nk) \) be the number of monic irreducible polynomials \( f(x) \in \mathbb{F}_q[x] \) of degree \( nk \) such that \( f(ax) = f(x) \), \( k = \text{ord}(a) \). Also, let \( L(n,k) \) be the number of monic irreducible polynomials of the form \( F(x^k) \), where \( F \) has degree \( n \). Notice that, from Theorem[3] \( N_a(nk) \) is exactly the number of monic irreducible polynomials of the form \( f(x^k - 1) \) where \( f \) has degree \( n \). Since \( f(x^k - 1) = F(x^k) \) for \( F(x) = f(x - 1) \) and \( \{f(x - 1)|f \in I_q(n)\} = I_q(n) \), the number of monic irreducible polynomials \( F \) of degree \( n \) for which \( F(x^k) \) is also irreducible is the same for the composition \( F(x^k - 1) \). In particular we have proved that \( N_a(nk) = L(n,k) \). Combining the previous equality with the enumeration formula for \( L(n,k) \) presented in [3], Theorem 3) we directly deduce the enumeration formula of Garefalakis for homotheties:

\[ N_a(nk) = \frac{\varphi(k)}{m} \sum_{d | \text{gcd}(k, n - 1)} \mu(d)(q^{mk/d} - 1). \]

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

Consider the projective linear group \( G = \text{PGL}_2(\mathbb{F}_q) \approx \text{GL}_2(\mathbb{F}_q)/{\sim} \), where \( A \sim B \) if \( A = \lambda B \) for some \( \lambda \in \mathbb{F}_q^* \). We are interested to find 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 [[6], Proposition 4.8] in general there are no such polynomials:

Theorem 5. 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 \( A \in \text{PGL}_2(\mathbb{F}_q) \). 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 \( \text{PGL}_2(\mathbb{F}_q) \), \( f \) must be an \( \mathbb{F}_q \)-translation invariant and, from Theorem[2] part a), we know that this is only possible when \( \mathbb{F}_q \) is a prime field. Thus \( q = p \) prime. Also, from Theorem[1] 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 \( a \in \mathbb{F}_p \setminus \{0, 1\} \) such that \( k = \text{ord}(a) > 1 \). Since all homotheties also belong to \( \text{PGL}_2(\mathbb{F}_q) \), 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] 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 \( \text{deg} f(x) = 2N = 2 \text{deg} g(x) \). Let
\[
\gamma, \gamma^2, \cdots, \gamma^{2N-1}
\]
be the roots of \( f(x) \). Notice that \( f(y + 1) = g(y^2 + \gamma) = 0 \) and then \( \gamma + 1 = \gamma^2 \) for some \( 0 < j < 2N \). In other words, \( F(x) = x^2 + x + 1 \in \mathbb{F}_2[x] \) 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 \( f^*(x) = x^f(1/x) \) also belong to \( \text{PGL}_2(\mathbb{F}_q) \), it follows that \( x^d f(1/x) = f(x) \) and so \( f^*(x) = f(x) \) divides \( F^*(x) = x^2 + x^2 + 1 \). 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 \( A \in \text{PGL}_2(\mathbb{F}_2) \).

4. \( p \)– subgroups of \( \text{GL}_2(\mathbb{F}_q) \)

Let \( p = \text{char} \mathbb{F}_q \). If \( S \subset \mathbb{F}_q \) is an \( \mathbb{F}_p \)–vector space of dimension \( r \), then 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 \( H \subset \text{GL}_2(\mathbb{F}_q) \), \( I_H(n) \) 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, we are able to characterize the numbers \( |I_H(n)| \):

**Theorem 6.** Let \( H \subset \text{GL}_2(\mathbb{F}_q) \) 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

\[ |I_H(n)| = \frac{p-1}{pm} \sum_{d \mid m} q^{m/d} \mu(d). \]

**Proof.** Notice that \( |\text{GL}_2(\mathbb{F}_q)| = q(q-1)^2(q+1) \) and the sets of all translations in \( \mathbb{F}_q \) corresponds to a Sylow \( p \)– subgroup \( G \) of \( \text{GL}_2(\mathbb{F}_q) \). Let \( H \subset \text{GL}_2(\mathbb{F}_q) \) be any group of order \( p^r \). We know that \( H \) is contained in some Sylow \( p \)– subgroup \( K \) of \( \text{GL}_2(\mathbb{F}_q) \). Since all Sylow \( p \)–subgroups are conjugate, there is some \( A \in \text{GL}_2(\mathbb{F}_q) \) 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:

\[ \tau_{HA} : I_H(n) \to I_{A^{-1}HA}(n) \]

\[ f(x) \mapsto k_{A,f,n}(A^{-1} \circ f(x)), \]

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 \( \tau_{HA} \) is well defined. Now, suppose that \( \tau_{HA}(f) = \tau_{HA}(g) \) 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 \( \tau_{HA} \) 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 \( p \)–subgroup of \( G \), i.e., \( I_{A^{-1}HA}(n) \) is equal to \( C_S(n) \) for some \( \mathbb{F}_p \)– vector space \( S \) of dimension \( r \). Now, the result follows from Theorem 2.

**Acknowledgments**

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

[1] S. Agou, *Irreductibilité des polynômes* $f(x^{p^2} - ax^p - bx)$ sur un corps fini $\mathbb{F}_p$, Journal of Number Theory 10 (1979), pp 20.

[2] S. D. Cohen, *On irreducible polynomials of certain types in finite fields*, Mathematical Proceedings of the Cambridge Philosophical Society 66 (1969), pp 335-344.

[3] T. Garefalakis, *On the action of GL$_2(\mathbb{F}_q)$ on irreducible polynomials over $\mathbb{F}_q$*, Journal of Pure and Applied Algebra. 215 (2011) pp 1835-1843.

[4] R. Lidl, H. Niederreiter, *Introduction to finite fields and their applications*. Cambridge University Press New York, NY, USA 1986.

[5] F. Ruskey, C. R. Miers, and J. Sawada, *The number of irreducible polynomials and Lyndon words with given trace*, SIAM J. Discrete Math. 14 (2001) pp 240-245.

[6] H. Stichtenoth, A. Topuzoglu, *Factorization of a class of polynomials over finite fields*, Finite Fields Appl. 18 (2012) pp 108-122.