On the action of $\mathrm{GL}_2(\mathbb{F}_q)$ on irreducible polynomials over $\mathbb{F}_q$

Theodoulos Garefalakis

Department of Mathematics, University of Crete, 714 09 Heraklion, Greece
Tel: +30 2810 393845, Fax: +30 2810 393861

Abstract

We show that $\mathrm{GL}_2(\mathbb{F}_q)$ acts on the set of irreducible polynomials over $\mathbb{F}_q$. We study this action and compute the cardinality of the set of fixed points of certain subgroups of $\mathrm{GL}_2(\mathbb{F}_q)$. Our results include enumeration of irreducible polynomials that are invariant under the substitution $X \mapsto X + b$ and under the substitution $X \mapsto aX$. From those results follow enumeration formulas for the set of fixed points of any element of order r, where r is a prime divisor of q or $q - 1$. The results are combined to provide enumeration formulas for the fixed points of upper triangular matrices.

Keywords: finite fields, irreducible polynomials, group action
2000 MSC: 12E20, 11T55

1. Introduction

Given a finite field $\mathbb{F}_q$ and a natural number n, there is a unique extension of $\mathbb{F}_q$ of degree n within a fixed algebraic closure, denoted $\mathbb{F}_{q^n}$. Such an extension is algebraically generated over $\mathbb{F}_q$ by a root θ of any irreducible polynomial $P \in \mathbb{F}_q[X]$ of degree n.

Any special properties of the irreducible P are naturally reflected in its roots θ^{q^j}, $0 \leq j \leq n - 1$. Such properties, that have been investigated, include primitivity, normality, having certain coefficients fixed to given values, combinations of those properties. For a survey of results in this line of research, we refer to [1] and the references therein.

Given a polynomial $f \in \mathbb{F}_q[X]$, it reciprocal f^R is defined as $f^R(X) = X^{\deg(f)} f(1/X)$. One class of polynomials that has been invesitgated [2, 3, 4, 5] is that of self-reciprocal irreducible polynomials, that is, irreducible polynomials that satisfy $P^R(X) = P(X)$. Besides the theoretical interest in their existence and density, self-reciprocal irreducible polynomials have been useful in application, and in particular in the construction of error-correcting codes [6, 7].

In this work, we observe that the group $\mathrm{GL}_2(\mathbb{F}_q)$ acts on the set of irreducible polynomials over $\mathbb{F}_q$ of degree at least 2. The "reciprocal" operator is given, in our setting, as the action of the matrix $R = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Our objective is to characterize the sets of fixed points of the action of single elements of $\mathrm{GL}_2(\mathbb{F}_q)$ (or equivalently of cyclic subgroups) on the set I_n of monic irreducibles of degree n, and to compute their cardinalities. It is well known that the order of

Email address: theo@math.uoc.gr (Theodoulos Garefalakis)

$\mathrm{GL}_2(\mathbb{F}_q)$ is $q(q-1)^2(q+1)$. We show that the set of fixed points of the action of any element of a p-Sylow subgroup $\mathrm{GL}_2(\mathbb{F}_q)$, where p is the characteristic of $\mathbb{F}_q$, relates to irreducibles that are invariant under the substitution $X \mapsto X + b$, and we compute its cardinality. Further, for any divisor ℓ of $q-1$, we express the substitution $X \mapsto aX$, as the action of a matrix of order ℓ and compute the cardinality of the set of fixed points this matrix. As a corollary, we obtain the number of even irreducible polynomials of given degree. Finally, we obtain enumeration formulas for the number of fixed points of any upper triangular matrix. We note that the irreducible polynomials that remain invarian under additive and multiplicative translations have been studied, by different methods, in [8] and [9] respectively. Methods similar to those in the present paper have been used in [10] to study the action of subgroups of $\mathrm{GL}_2(\mathbb{F}_2)$ on irreducible polynomials.

2. Group Action on Irreducibles

Let I_n^λ denote the set of irreducible polynomials in $\mathbb{F}_q[X]$ of degree n having leading coefficient equal to λ. For simplicity we denote I_n the set I_n^1 of monic irreducibles of degree n. The set of all irreducibles of degree n is denoted by I'_n. We denote by $\mathbb{P}_n$ the set of polynomials in $\mathbb{F}_q[X]$ of degree n that do not have roots in $\mathbb{F}_q$ and let $\mathbb{P} = \cup_{n\geq 2}\mathbb{P}_n$.

The group $\mathrm{GL}_2(\mathbb{F}_q)$ acts on the set $\mathbb{P}$ by the rule

$$f^A = (cX+d)^{\deg(f)} f\left(\frac{aX+b}{cX+d}\right), \text{ where } A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_q).$$

It is a simple calculation to show that the above rule defines an action of $\mathrm{GL}_2(\mathbb{F}_q)$ on $\mathbb{P}$, the crucial point being that if $f = \sum_{i=0}^n f_i X^i$, then the leading coefficient of f^A is $f_n a^n$ if $c = 0$ and $c^n f(a/c)$ if $c \neq 0$. Since A is invertible and f does not have roots in $\mathbb{F}_q$, the leading coefficient is non-zero in either case. It follows that the action preserves the degrees, so we get an action on $\mathbb{P}_n$, for $n \geq 2$.

Lemma 1. *Let $A \in \mathrm{GL}_2(\mathbb{F}_q)$ and $P \in I_n$, $n \geq 2$. Then $P^A \in I_n^\lambda$ for some $\lambda \in \mathbb{F}_q^*$. Further, θ is a root of P if and only if $(-d\theta+b)/(c\theta-a)$ is a root of P^A, where $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.*

Proof. Let $n = \deg(P)$, θ be a root of P and let $\beta = (-d\theta+b)/(c\theta-a)$. Note that β is well defined since θ does not belong to $\mathbb{F}_q$. Then $\theta = (a\beta+b)/(c\beta+d)$ and we compute

$$P^A(\beta) = (c\beta+d)^n P\left(\frac{a\beta+b}{c\beta+d}\right) = (c\beta+d)^n P(\theta) = 0.$$

So β is a root of P^A. If m is the degree of the minimal polynomial of β over $\mathbb{F}_q$, then $\mathbb{F}_{q^m} = \mathbb{F}_q(\beta) \subseteq \mathbb{F}_q(\theta) = \mathbb{F}_{q^n}$, which implies that $m|n$. Conversely, $\theta = (a\beta+b)/(c\beta+d)$ so that $\mathbb{F}_{q^n} \subseteq \mathbb{F}_{q^m}$, which implies that $n|m$. It follows that $m = n = \deg(P^A)$ and P^A is irreducible. Finally, note that if $\beta = (-d\theta+b)/(c\theta-a)$ is a root of P^A then $(c\beta+d)^n P(\theta) = 0$. Since β does not belong to $\mathbb{F}_q$, $c\beta+d \neq 0$ and it follows that $P(\theta) = 0$. □

From Lemma 1 it follows that the rule $P \mapsto P^A$ defines an action of $\mathrm{GL}_2(\mathbb{F}_q)$ on I'_n for $n \geq 2$. The following lemma is evident.

Lemma 2. *Let $\lambda \in \mathbb{F}_q^*$ and $P \in I'_n$, $n\geq 2$. Then $(\lambda P)^A = \lambda P^A$.*

Our objective is to compute the fixed points, in I_n, of certain subsets of $\mathrm{GL}_2(\mathbb{F}_q)$. If $S \subseteq \mathrm{GL}_2(\mathbb{F}_q)$, we denote

$$C_{I_n}(S) = \{P \in I_n : \ \forall A \in S, P^A = P\}.$$

Lemma 3. *Let $A, B \in \mathrm{GL}_2(\mathbb{F}_q)$ be conjugate. Then $|C_{I_n}(A)| = |C_{I_n}(B)|$.*

Proof. Since A and B are conjugate, there exists some $U \in \mathrm{GL}_2(\mathbb{F}_q)$, such that $B = U^{-1}AU$. We define the map

$$\begin{array}{rcl} \psi : C_{I_n}(A) & \longrightarrow & C_{I_n}(B) \\ P & \mapsto & \lambda_P P^U, \end{array}$$

where λ_P is the unique element in $\mathbb{F}_q^*$ that makes $\lambda_P P^U$ monic. The map is well defined since $\lambda_P P^U \in I_n$ by the definition of λ_P, and using Lemma 2, we have

$$(\lambda_P P^U)^B = \lambda_P P^{UU^{-1}AU} = \lambda_P P^{AU} = \lambda_P P^U.$$

The map is one-to-one, since $\lambda_{P_1} P_1^U = \lambda_{P_2} P_2^U$, by applying U^{-1} to both sides, implies that $\lambda_{P_1} P_1 = \lambda_{P_2} P_2$. Since P_1 and P_2 are monic, we conclude that $\lambda_{P_1} = \lambda_{P_2}$ and $P_1 = P_2$. The injectivity of ψ implies that $|C_{I_n}(A)| \leq |C_{I_n}(B)|$. The reverse inequality and the result follow by symmetry. □

Lemma 4. *Let $\lambda \in \mathbb{F}_q^*$ and $A \in \mathrm{GL}_2(\mathbb{F}_q)$. If $n \equiv 0 \pmod{\mathrm{ord}(\lambda)}$, then $C_{I_n}(A) = C_{I_n}(\lambda A)$.*

Proof. We first note that for $P \in I_n$, $P^{\lambda A} = \lambda^n P^A$. The extra assumption on the degree, implies that $P^{\lambda A} = P^A$. Therefore, $P \in C_{I_n}(A)$ if and only if $P \in C_{I_n}(\lambda A)$.

3. The substitution $X \mapsto X + b$

Let $A = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_q)$, $b \neq 0$. In this section, we consider the fixed points, in I_n, of A. Since $P^A(X) = P(X + b)$, we call the polynomials that are fixed by A periodic. The order of A in $\mathrm{GL}_2(\mathbb{F}_q)$ is equal to the characteristic p of $\mathbb{F}_q$. Therefore $\langle A \rangle$ is generated by any A^j, $0 < j < p$. Noting that A maps monic irreducibles of degree $n \geq 2$ to monic irreducibles of the same degree, we see that

$$P^A = P \iff P^{A^j} = P$$

for any $0 < j < p$.

Proposition 1. *Let $\mathbb{F}_q$ be of characteristic p, $P \in C_{I_n}(A)$, $n \geq 2$ and θ a root of P. Then $n = pm$ for some $m \in \mathbb{N}$. Further, the set $\{s \in \mathbb{N} : \ \theta^{q^s} = \theta - b\}$ is non-empty and $r = r_P = \min\{s \in \mathbb{N} : \theta^{q^s} = \theta - b\}$ satisfies $0 < r < pm$ and $m|r$.*

Proof. Since $P \in C_{I_n}(A)$ and $n \geq 2$ it follows from Lemma 1 that $\theta - b$ is a root of P. Therefore, $\theta^{q^s} = \theta - b$ for some $0 < s < n$ (note that $s \neq 0$ otherwise we would have $b = 0$). Thus the set $\{s \in \mathbb{N} : \ \theta^{q^s} = \theta - b\}$ is non-empty. Thus $r = r_P$ exists and, by its definition, $\theta^{q^r} = \theta - b$, $0 < r < n$. It is easy to see then, that $\theta^{jr} = \theta - jb$, so that $\theta^{pr} = \theta$. It follows that $n|pr$. If $p \not| n$, we would have $n|r$, which is impossible, since $0 < r < n$. Thus $n = pm$ for some $m \in \mathbb{N}$. Since $n|pr$ and $n = pm$ we obtain that $m|r$. □

It is clear that the integer r_P depends only on the polynomial P, and not on the root θ.

Definition 1. Let $P \in C_{I_{pm}}(A)$, $m \in \mathbb{N}$, θ a root of P, and $r_P = \min\{s \in \mathbb{N} : \theta^{q^s} = \theta - b\}$. The integer $t_P = r_P/m$ is called the type of P.

Clearly, the type t_P of a polynomial $P \in C_{I_{pm}}(A)$ lies in $\{1, \ldots, p-1\}$. In particular, $t_P \not\equiv 0 \pmod{p}$. For $0 < j < p$, we denote $C^{(j)}_{I_{pm}}(A) = \{P \in C_{I_{pm}}(A) : t_P = j\}$. The next proposition shows that the polynomials in $C_{I_{pm}}(A)$ are distributed equally with respect to their type.

Proposition 2. *For $m \in \mathbb{N}$ and $0 < j < p$, $|C^{(j)}_{I_{pm}}(A)| = |C^{(1)}_{I_{pm}}(A)|$.*

Proof. We fix some $0 < j < p$ and consider $U_j = \begin{pmatrix} j & 0 \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_q)$, and observe that $U_j A = A^j U_j$. If $P \in C^{(1)}_{I_{pm}}(A)$ and θ is one of its roots, then $\theta^{q^m} = \theta - b$ and by induction $\theta^{q^{jm}} = \theta - jb$. Define $Q = j^{-pm} P^{U_j} = j^{-pm} P(jX)$, so that Q is monic. The polynomial Q is fixed by A since

$$Q^A = (j^{-pm} P^{U_j})^A = j^{-pm} P^{A^j U_j} = j^{-pm} P^{U_j} = Q.$$

By Lemma 1, $\beta = \theta/j$ is a root of Q. We compute,

$$\beta^{q^{jm}} = \frac{\theta^{q^{jm}}}{j} = \frac{\theta}{j} - b = \beta - b.$$

Since $0 < j < p$, it follows that Q is of type j, so that $Q \in C^{(j)}_{I_{pm}}(A)$. We have shown that the map

$$\begin{array}{rcl} \psi : C^{(1)}_{I_{pm}}(A) & \longrightarrow & C^{(j)}_{I_{pm}}(A) \\ P & \mapsto & j^{-pm} P^{U_j} \end{array}$$

is well defined. The same argument as in the proof of Lemma 3 shows that ψ is injective. Finally, if $Q \in C^{(j)}_{I_{pm}}(A)$, then $P = j^{pm} Q^{U_j^{-1}}$ is fixed by A^j, and therefore fixed by A, and has type 1. Therefore, it is an element of $C^{(1)}_{I_{pm}}(A)$ and $\psi(P) = Q$. So the map is surjective. It follows that $|C^{(j)}_{I_{pm}}(A)| = |C^{(1)}_{I_{pm}}(A)|$. □

The sets $C^{(j)}_{I_{pm}}(A)$, $0 < j < p$ form a partition of $C_{I_{pm}}(A)$. Therefore,

$$|C_{I_{pm}}(A)| = \sum_{j=1}^{p-1} |C^{(j)}_{I_{pm}}(A)| = (p-1)|C^{(j)}_{I_{pm}}(A)|, \quad \text{for any } j = 1, \ldots, p-1.$$

Denoting $N_A(pm) = |C_{I_{pm}}(A)|$, we have

$$N_A(pm) = \frac{1}{p-1} |C^{(j)}_{I_{pm}}(A)|, \quad \text{for any } j = 1, \ldots, p-1. \tag{1}$$

Theorem 1. *Let $\mathbb{F}_q$ be of characteristic p, $k \in \mathbb{N}$, $F_{k,b} = X^{q^k} - X + b \in \mathbb{F}_q[X]$, and $P \in I_n$, $n \geq 2$. Then P divides $F_{k,b}$ if and only if*

1. $P \in C_{I_n}(A)$,
2. $n = pm$, *for some* $m \in \mathbb{N}$.
3. $m|k$,
4. $\frac{k}{m} \equiv t_P \not\equiv 0 \pmod{p}$.

Proof. Suppose that P divides $F_{k,b}$ and let θ be a root of P. Then $\theta^{q^k} = \theta - b$, which implies that $\theta - b$ is a root of P. Since P^A is irreducible, by Lemma 1, this forces $P^A|P$. Since P and P^A are monic irreducibles, this implies, by induction, that $P^A = P$, so that $P \in C_{I_n}(A)$. The equality $\theta^{q^k} = \theta - b$ implies that $\theta^{q^{jk}} = \theta - jb$ for $j \in \mathbb{N}$, so that $\theta^{q^{pk}} = \theta$. It follows that $n|pk$. If we assume that $p \nmid n$ then we would have $n|k$ which would imply that $\theta^{q^k} = \theta$, that is $b = 0$, a contradiction. Thus $n = pm$ for some $m \in \mathbb{N}$. Since $n = pm|pk$ we get $m|k$. Finally, since $P^A = P$, Proposition 1 implies that $\theta^{q^r} = \theta - b$ with $r = r_P = t_P m$ and $0 < t_P < n$. It follows that $\theta^{q^k} = \theta^{q^r}$, which implies that $k \equiv r \pmod{n}$, and therefore, $k/m \equiv t_P \pmod{p}$.

Conversely, suppose that $P \in C_{I_{pm}}(A)$, and θ is a root of P. Then by Proposition 1, $\theta^{q^{t_P m}} = \theta - b$. The assumption $k/m \equiv t_P \pmod{p}$ implies that $k \equiv t_P m \pmod{n}$, and we have $\theta^{q^k} = \theta^{q^{t_P m}} = \theta - b$. It follows that θ is a root of $F_{k,b}$ so $P|F_{k,b}$. □

We note, that the necessary and sufficient conditions in Theorem 1 can be written as $m|k$ and $P \in C^{(t)}_{I_{pm}}(A)$, with $t \equiv k/m \pmod{p}$. From this together with the fact that all the roots of $F_{k,b}$ are simple, which can be checked using the derivative, we obtain

$$X^{q^k} - X + b = \prod_{d|k} \prod_{P} P, \tag{2}$$

where the inner product is over irreducibles in $C^{(t)}_{I_{pm}}(A)$ with $t \equiv k/m \pmod{p}$.

We can use Eq.(2) and Eq.(1) to compute $N_A(pm)$ for any $m \in \mathbb{N}$.

Theorem 2. *Let* $n \in \mathbb{N}$. *If* $n \not\equiv 0 \pmod{p}$, *then* $N_A(n) = 0$. *If* $n = pm$, $m \in \mathbb{N}$, *then* $N_A(pm) = |C_{I_{pm}}(A)|$ *satisfies*

$$N_A(pm) = \frac{p-1}{pm} \sum_{\substack{d|m \\ d \not\equiv 0 \pmod{p}}} \mu(d) q^{m/d}.$$

Proof. From Eq.(2), comparing degrees, we have

$$q^k = \sum_{d|k} \sum_{P} pd|C^{(t)}_{I_{pm}}(A)|,$$

where the inner sum is over polynomials $P \in C^{(t)}_{I_{pm}}(A)$, where t is the remainder of k/d on division with p. Since $|C^{(0)}_{I_{pm}}(A)| = 0$ and $|C^{(j)}_{I_{pm}}(A)| = \frac{1}{p-1} N_A(pm)$ for $0 < j < p$, by Eq.(1), we have

$$q^k = \sum_{\substack{d|k \\ k/d \not\equiv 0 \pmod{p}}} \frac{p}{p-1} d N_A(pd).$$

Möbius inversion now yields

$$\frac{p}{p-1} k N_A(pk) = \sum_{\substack{d|k \\ d \not\equiv 0 \pmod{p}}} \mu(d) q^{k/d}.$$

□

The following corollary gives an estimate of $N_A(pm)$.

Corollary 1. *Let $m \in \mathbb{N}$. Then*

$$\left| N_A(pm) - \frac{p-1}{pm} \right| \leq \frac{p-1}{pm} \frac{q}{q-1} q^{\frac{m}{2}}.$$

Proof. From Theorem 2 we have

$$N_A(pm) = \frac{p-1}{pm} \sum_{\substack{d \mid m \\ d \not\equiv 0 \pmod p}} \mu(d) q^{m/d} = \frac{p-1}{pm} q^m + \frac{p-1}{pm} \sum_{\substack{d \mid m \\ d \not\equiv 0 \pmod p \\ d > 1}} \mu(d) q^{m/d}.$$

It follows that

$$\begin{aligned} \left| N_A(pm) - \frac{p-1}{pm} \right| &\leq \frac{p-1}{pm} \sum_{\substack{d \mid m \\ d \not\equiv 0 \pmod p \\ d > 1}} q^{m/d} \\ &\leq \frac{p-1}{pm} \sum_{i=1}^{\lfloor m/2 \rfloor} q^i \\ &\leq \frac{p-1}{pm} \frac{q}{q-1} q^{m/2}. \end{aligned}$$

□

A matrix of the form, $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ is a p-element of $\mathrm{GL}_2(\mathbb{F}_q)$. The set

$$T = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{F}_q \right\},$$

is in fact a subgroup of $\mathrm{GL}_2(\mathbb{F}_q)$ of order q. Since $|\mathrm{GL}_2(\mathbb{F}_q)| = q(q-1)(q^2-1)$, we see that T is a p-subgroup of $\mathrm{GL}_2(\mathbb{F}_q)$ of maximal order, and thus it is a p-Sylow subgroup. Consider now any p-Sylow subgroup S of $\mathrm{GL}_2(\mathbb{F}_q)$ and $D \in S$. Then S and T are conjugate, so D is conjugate to some element of T. Lemma 3 implies the following corollary.

Corollary 2. *Let S be a p-Sylow subgroup of $\mathrm{GL}_2(\mathbb{F}_q)$, $B \in S$, and $n \in \mathbb{N}$. If $n \not\equiv 0 \pmod p$, then $|C_{I_n}(B)| = 0$. If $n = pm$, $m \in \mathbb{N}$, then*

$$|C_{I_{pm}}(B)| = \frac{p-1}{pm} \sum_{\substack{d \mid m \\ d \not\equiv 0 \pmod p}} \mu(d) q^{m/d}.$$

4. The substitution $X \mapsto aX$

In this section, we consider the action of $B = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_q)$, $a \notin \{0,1\}$ on I_n. We denote $\ell = \mathrm{ord}(a)$ the order of a in $\mathbb{F}_q^*$. It is easy to see that ℓ is also the order of B in $\mathrm{GL}_2(\mathbb{F}_q)$.

Proposition 3. *Let $P \in C_{I_n}(B)$, $n \geq 2$ and θ a root of P. Then $n = \ell m$ for some $m \in \mathbb{N}$. Further, the set $\{s \in \mathbb{N} : \theta^{q^s} = \theta/a\}$ is non-empty and $r = r_P = \min\{s \in \mathbb{N} : \theta^{q^s} = \theta/a\}$ satisfies $0 < r < \ell m$, $m|r$, and $(r/m, \ell) = 1$.*

Proof. Let $P \in C_{I_n}(B)$. Then $P^B = P(aX)$ and the leading coefficient of P^B is a^n. Since $P = P^B$ is monic, we have $a^n = 1$, so $n = \ell m$ for some $m \in \mathbb{N}$. If θ is a root of P, then θ/a is a root of P^B, so θ/a is also a root of P. It follows that $\theta/a = \theta^{q^r}$ for some $0 < r < n$ (note that $r \neq 0$ since $a \neq 1$). Therefore, the set $\{s \in \mathbb{N} : \theta^{q^s} = \theta/a\}$ is non-empty and its minimum satisfies the stated bounds. Since the integers in the set are equivalent modulo n there is a unique element in this set that satisfies $0 < s < n$, so the minimum r_P is equal to r. By induction, we have $\theta^{q^{jr}} = \theta/a^j$ for any $j \in \mathbb{N}$. In particular, $\theta^{q^{\ell r}} = \theta$, therefore $n = \ell m | \ell r$, which implies $m|r$. Let $t = r/m$, $(t, \ell) = u$ and write $t = ut_1$, $\ell = u\ell_1$. Then

$$\begin{aligned} \theta^{q^{tm}} = \frac{\theta}{a} \quad &\Longrightarrow \quad \theta^{q^{tm\ell_1}} = \frac{\theta}{a^{\ell_1}} \quad \Longrightarrow \\ \theta^{q^{t_1 \ell m}} = \frac{\theta}{a^{\ell_1}} \quad &\Longrightarrow \quad a^{\ell_1} = 1 \quad \Longrightarrow \quad \ell = \ell_1, \end{aligned}$$

where we used the fact that $\theta^{q^{\ell m}} = \theta$. It follows that $u = (r/m, \ell) = 1$. □

As in the previous section, we see that r_P depends only on P and not on the particular root θ, which allows us to define its type.

Definition 2. Let $P \in C_{I_{\ell m}}(B)$, θ a root of P, and $r_P = \min\{s \in \mathbb{N} : \theta^{q^s} = \theta/a\}$. The integer $t_P = r_P/m$ is called the type of P.

It is clear from Proposition 3 that the type t_P of a polynomial $P \in C_{I_{\ell m}}(B)$ satisfies $0 < t_p < \ell$ and $(t_P, \ell) = 1$. We should emphasize that the type of a polynomial is defined with respect to, and depends on, the matrix B. For instance, if we choose $0 < j < \ell$ with $(j, \ell) = 1$, then $\langle B \rangle = \langle B^j \rangle$. It follows that $C_{I_{\ell m}}(B) = C_{I_{\ell m}}(B^j)$. However, the type of a polynomial $P \in C_{I_{\ell m}}(B)$ with respct to B may, and in general will, be different from its type with respect to B^j.

Following the notation of the previous section, we let

$$C^{(t)}_{I_{\ell m}}(B) = \{P \in C_{I_{\ell m}}(B) : \ t_P = t\}.$$

The sets $C^{(t)}_{I_{\ell m}}(B)$, $0 < t < \ell m$, $(t, \ell) = 1$ form a partition of $C_{I_{\ell m}}(B)$.

Proposition 4. *Let $0 < j, t < n$, with $(j, \ell) = (t, \ell) = 1$. Then*

$$C^{(j)}_{I_{\ell m}}(B^t) = C^{(jt^{-1})}_{I_{\ell m}}(B),$$

where the superscript jt^{-1} is computed modulo ℓ.

Proof. We start by noting that $B^t = \begin{pmatrix} a^t & 0 \\ 0 & 1 \end{pmatrix}$, and $\operatorname{ord}(a^t) = \ell$, since $(t, \ell) = 1$, thus Proposition 3 and Definition 2 apply to elements fixed by B^t. Let s be the inverse of t modulo ℓ. Then denoting θ a root of P, we have

$$\begin{aligned} P \in C^{(j)}_{I_{\ell m}}(B^t) \quad &\Longleftrightarrow \quad \theta^{q^{jm}} = \frac{\theta}{a^t} \quad \Longleftrightarrow \quad \theta^{q^{jsm}} = \frac{\theta}{a^{st}} \\ &\Longleftrightarrow \quad \theta^{q^{jsm}} = \frac{\theta}{a} \quad \Longleftrightarrow \quad P \in C^{(js)}_{I_{\ell m}}(B). \quad \square \end{aligned}$$

Theorem 3. *Let $k \in \mathbb{N}$, $a \in \mathbb{F}_q^*$ of order $\ell > 1$, $G_{k,a} = X^{q^k-1} - 1/a \in \mathbb{F}_q[X]$ and $P \in I_n$, $n \geq 2$. Then $P|G_{k,a}$ if and only if*

1. *$P \in C_{I_n}(B)$,*
2. *$n = \ell m$, for some $m \in \mathbb{N}$.*
3. *$m|k$,*
4. *$\frac{k}{m} \equiv t_P \pmod{\ell}$.*

Proof. Suppose that P divides $G_{k,a}$ and θ is a root of P. Then $\theta^{q^k} = \theta/a$, which implies that θ/a is a root of P. Since θ/a is a root of P^B, which is irreducible, by Lemma 1, and the leading coefficient of P^B is a^n, we have $P^B = a^n P$. The equality $\theta^{q^k} = \theta/a$ implies, by induction, that

$$\theta^{q^{jk}} = \theta/a^j \ \text{ for any } j \in \mathbb{N}. \tag{3}$$

In particular, we have $\theta^{q^{nk}} = \theta/a^n$. Since $\theta^{q^{nk}} = \theta$, we obtain $a^n = 1$. Thus, $n = \ell m$ for some $m \in \mathbb{N}$ and $P^B = P$, that is, $P \in C_{I_n}(B)$. From Eq.(3), for $j = \ell$ we have $\theta^{q^{\ell k}} = \theta$, which implies that $n = \ell m | \ell k$, that is $m|k$. Since $P \in C_{I_{\ell m}}(B)$, Proposition 3 implies that $\theta^{q^{t_P m}} = \theta/a$. Forces $t_P m \equiv k \pmod{\ell m}$, which implies that $k/m \equiv t_P \pmod{\ell}$.

Conversely, suppose that $P \in C_{I_{\ell m}}(B)$ and θ is a root of P. Then $\theta^{q^{t_P m}} = \theta/a$. Since $k/m \equiv t_P \pmod{\ell}$, we have $k \equiv t_P m \pmod{\ell m}$ and therefore $\theta^{q^k} = \theta^{q^{t_P m}}$. This implies that θ is root of $G_{k,a}$, so $P|G_{k,a}$. □

The polynomial $G_{k,a}$ has simple roots, as can be seen using the derivative. Theorem 3 is equivalent to the following factorization of $G_{k,a}$.

$$G_{k,a} = X^{q^k-1} - \frac{1}{a} = \prod_{\substack{d|k \\ (\frac{k}{d},\ell)=1}} \prod_{P \in C_{I_{\ell d}}^{(\frac{k}{d})}(B)} P, \tag{4}$$

where the superscript k/d is computed modulo ℓ.

In view of the comments after Definition 2, we see that we can apply Eq.(4) to the polynomials G_{k,a^t}, $0 < t < \ell$, $(t,\ell) = 1$ that correspond to the matrices B^t, to obtain

$$G_{k,a^t} = \prod_{\substack{d|k \\ (\frac{k}{d},\ell)=1}} \prod_{P \in C_{I_{\ell d}}^{(\frac{k}{d})}(B^t)} P, \quad \text{for } 0 < t < \ell, (t,\ell) = 1.$$

This equality can be rewritten, using Proposition 4, as

$$G_{k,a^t} = \prod_{\substack{d|k \\ (\frac{k}{d},\ell)=1}} \prod_{P \in C_{I_{\ell d}}^{(\frac{k}{d}t^{-1})}(B)} P, \quad \text{for } 0 < t < \ell, (t,\ell) = 1.$$

Putting all factorizations together, we have

$$\begin{aligned}
\prod_{\substack{0<t<\ell\\(t,\ell)=1}} G_{k,a^t} &= \prod_{\substack{0<t<\ell\\(t,\ell)=1}} \prod_{\substack{d|k\\(\frac{k}{d},\ell)=1}} \prod_{P\in C_{I_{\ell d}}^{(\frac{k}{d}t^{-1})}(B)} P\\
&= \prod_{\substack{d|k\\(\frac{k}{d},\ell)=1}} \prod_{\substack{0<t<\ell\\(t,\ell)=1}} \prod_{P\in C_{I_{\ell d}}^{(\frac{k}{d}t^{-1})}(B)} P\\
&= \prod_{\substack{d|k\\(\frac{k}{d},\ell)=1}} \prod_{\substack{0<t<\ell\\(t,\ell)=1}} \prod_{P\in C_{I_{\ell d}}^{(t)}(B)} P\\
&= \prod_{\substack{d|k\\(\frac{k}{d},\ell)=1}} \prod_{P\in C_{I_{\ell d}}(B)} P
\end{aligned}$$

where we used the facts that as t runs through $(\mathbb{Z}/\ell\mathbb{Z})^*$ so does $\frac{k}{d}t^{-1}$ and that the sets $C_{I_{\ell d}}^{(t)}(B)$, $0 < t < \ell$, $(t,\ell) = 1$ form a partition of $C_{I_{\ell d}}(B)$. Taking degrees, we have

$$\phi(\ell)(q^k - 1) = \sum_{\substack{d|k\\(\frac{k}{d},\ell)=1}} \ell d|C_{I_{\ell d}}(B)|.$$

Denoting $N_B(\ell d) = |C_{I_{\ell d}}(B)|$, we have

$$q^k - 1 = \sum_{\substack{d|k\\(\frac{k}{d},\ell)=1}} \frac{\ell d}{\phi(\ell)} N_B(\ell d). \tag{5}$$

Theorem 4. *Let $n \in \mathbb{N}$. If $n \not\equiv 0 \pmod{\ell}$, then $N_B(n) = 0$. If $n = \ell m$, $m \in \mathbb{N}$, then*

$$N_B(\ell m) = \frac{\phi(\ell)}{\ell m} \sum_{\substack{d|m\\(d,\ell)=1}} \mu(d)(q^{\frac{m}{d}} - 1),$$

where ϕ is Euler's function.

Proof. From Eq.(5) we have

$$q^k - 1 = \sum_{\substack{d|k\\(\frac{k}{d},\ell)=1}} \frac{\ell d}{\phi(\ell)} N_B(\ell d) = \sum_{d|k} \frac{\ell d}{\phi(\ell)} N_B(\ell d)\chi_1\left(\frac{k}{d}\right),$$

where χ_1 is the principal Dirichlet character modulo ℓ. Denoting $g(k) = q^k - 1$, $f(k) = \frac{\ell k}{\phi(\ell)} N_B(\ell k)$ we can write $g = f * \chi_1$, where $*$ is Dirichlet multiplication. The Dirichlet inverse of χ_1 is $\mu\chi_1$, since χ_1 is completely multiplicative, and we have $g * \mu\chi_1 = f$, that is

$$f(k) = \sum_{d|k} \mu(d)\chi_1(d) g\left(\frac{k}{d}\right) = \sum_{\substack{d|k\\(d,\ell)=1}} \mu(d) g\left(\frac{k}{d}\right). \quad \square$$

The proof of the following effective bounds of $N_B(\ell m)$ is similar to that of Corollary 1.

Corollary 3. *Let $m \in \mathbb{N}$. Then*

$$\left| N_B(\ell m) - \frac{\phi(\ell)}{\ell m} q^m \right| \leq \frac{2\phi(\ell)}{\ell m} q^{\frac{m}{2}}.$$

One interesting special case arises for $a = -1$. In this case, $\ell = 2$ and the polynomials that are fixed by the matrix $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ are even polynomials. The results of this section, applied in this case, are summarized in the following corollary.

Corollary 4. *The even irreducible polynomials in $\mathbb{F}_q[X]$ have even degree. The number $N_{even}(2m)$ of even irreducibles of degree $2m$ is given by*

$$N_{even}(2m) = \frac{1}{2m} \sum_{\substack{d|m \\ d\ odd}} \mu(d)(q^{\frac{m}{d}} - 1),$$

and satisfies

$$\left| N_{even}(2m) - \frac{1}{2m} q^m \right| \leq \frac{1}{m} q^{\frac{m}{2}}.$$

Remark 1. A polynomial f is called odd if $f(X) = -f(-X)$. Clearly, any odd polynomial has constant term zero, therefore odd irreducible polynomials of degree at least two do not exist. This is reflected in the fact that $|C_{I_n}(B)| = 0$ for $B = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ and n odd. Indeed, consider the matrix $C = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, and note that for $P \in I_n$, $P^C = (-1)^n P(-X)$. Thus, the fixed points of C of even degree are even irreducibles and the fixed points of C of odd degree are odd irreducibles. However, $R^{-1}BR = C$ for $R = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and Lemma 3 implies that $|C_{I_n}(B)| = |C_{I_n}(C)|$. For n odd, we know that $|C_{I_n}(B)| = 0$.

Proposition 5. *Let r be an odd prime divisor of $q - 1$ and $D = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$, with $a^r = b^r = 1$, $\max\{\mathrm{ord}(a), \mathrm{ord}(b)\} = r$. Then*

1. *If $a = b$,*

$$N_D(n) = \begin{cases} 0 & , \text{ if } n \not\equiv 0 \pmod r \\ |I_n| & , \text{ if } n \equiv 0 \pmod r \end{cases}$$

2. *If $a \neq b$,*

$$N_D(n) = \begin{cases} 0 & , \text{ if } n \not\equiv 0 \pmod r \\ \frac{r-1}{rm} \sum_{\substack{d|m \\ (d,r)=1}} \mu(d)(q^{\frac{m}{d}} - 1) & , \text{ if } n = rm \end{cases}$$

Proof. Assume first, that $a = b$. Then $D = aI$, and for $P \in I_n$, $P^D = a^n P$. Clearly, $|C_{I_n}(D)| = 0$ for $n \not\equiv 0 \pmod r$ and $|C_{I_n}(D)| = |I_n|$ for $n \equiv 0 \pmod r$.

Next, suppose that $a \neq b$. Since

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} = R^{-1} \begin{pmatrix} b & 0 \\ 0 & a \end{pmatrix} R,$$

Lemma 3 implies that the set of fixed points of $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ and $\begin{pmatrix} b & 0 \\ 0 & a \end{pmatrix}$ have the same cardinalities. So we may assume that $\max\{\mathrm{ord}(a), \mathrm{ord}(b)\} = \mathrm{ord}(a) = r$. For $P \in I_n$, the leading coefficient of $P^D = b^n P(aX/b)$ is a^n. This implies that $|C_{I_n}(D)| = 0$ for $n \not\equiv 0 \pmod r$. For $n \equiv 0 \pmod r$, we have $D = bB$, with $B = \begin{pmatrix} ab^{-1} & 0 \\ 0 & 1 \end{pmatrix}$. Lemma 4 implies that $C_{I_n}(D) = C_{I_n}(B)$, and the result follows from Theorem 4. □

Theorem 5. *Let r be an odd prime divisor of $q - 1$. Then for any $E \in \mathrm{GL}_2(\mathbb{F}_q)$ of order r the following statements hold.*

1. *If $n \not\equiv 0 \pmod r$, then $N_E(n) = 0$.*
2. *If $n = rm$, $E = aI$, for some $a \in \mathbb{F}_q^*$, then*

$$N_E(rm) = \sum_{d|rm} \mu(d) q^{\frac{rm}{d}}.$$

3. *If $n = rm$, $E \neq aI$ for every $a \in \mathbb{F}_q^*$, then*

$$N_E(rm) = \frac{r-1}{rm} \sum_{\substack{d|m \\ (d,r)=1}} \mu(d)(q^{\frac{m}{d}} - 1).$$

Proof. We write $q - 1 = r^e s$, with $(r, s) = 1$. The set

$$S = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a, b \in \mathbb{F}_q^*, a^{r^e} = b^{r^e} = 1 \right\}$$

is a subgroup of $\mathrm{GL}_2(\mathbb{F}_q)$ of order r^{2e}, and is an r-Sylow subgroup of $\mathrm{GL}_2(\mathbb{F}_q)$. Any $E \in \mathrm{GL}_2(\mathbb{F}_q)$ of order r belongs to an r-Sylow subgroup and therefore it is conjugate to some element of S, necessarily of order r. The elements of order r in S are the matrices described in Proposition 5. The result follows once we notice that the only conjugate of aI is aI itself. □

5. Upper triangular matrices

In this section, we combine the results we have to obtain enumeration formulas for the number of irreducible polynomials that are fixed by upper triangular matrices.

Theorem 6. *Let $U = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_q)$ and let ℓ_1 be the order of a and ℓ_2 the order of d/a in $\mathbb{F}_q^*$. Then the following statements hold.*

1. *If $n \not\equiv 0 \pmod{\ell_1}$ then $N_U(n) = 0$.*
2. *If $n \equiv 0 \pmod{\ell_1}$ and $a \neq d$, then*

$$N_U(n) = \begin{cases} 0 & , \text{ if } n \not\equiv 0 \pmod{\ell_2} \\ \frac{\phi(\ell_2)}{\ell_2 m} \sum_{\substack{d|m \\ (d,\ell_2)=1}} \mu(d)(q^{\frac{m}{d}} - 1) & , \text{ if } n = \ell_2 m \end{cases}$$

3. *If* $n \equiv 0 \pmod{\ell_1}$ *and* $a = d$*, then*

$$N_U(n) = \begin{cases} |I_n| & \text{, if } b = 0 \\ 0 & \text{, if } b \neq 0,\ n \not\equiv 0 \pmod{p} \\ \frac{p-1}{pm} \sum_{\substack{d|m \\ (d,p)=1}} \mu(d) q^{m/d} & \text{, if } b \neq 0,\ n = pm \end{cases}$$

Proof. We start by noting that for $P \in I_n$, the coefficient of the leading term of P^U is a^n. It follows that a necessary condition for P to be fixed by U is $n \equiv 0 \pmod{\ell}$. We assume that $n = \ell m$ for some $m \in \mathbb{N}$.

We consider the case $a \neq d$. Then

$$\begin{pmatrix} b & 1 \\ d-a & 0 \end{pmatrix}^{-1} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} b & 1 \\ d-a & 0 \end{pmatrix} = \begin{pmatrix} d & 0 \\ 0 & a \end{pmatrix}$$

From Lemma 4, follows that $N_U(n) = N_{U_1}(n)$, where

$$U_1 = \begin{pmatrix} da^{-1} & 0 \\ 0 & 1 \end{pmatrix}.$$

The stated result follows from Theorem 4.

For the case $a = d$, we note that

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} = a \begin{pmatrix} 1 & ba^{-1} \\ 0 & 1 \end{pmatrix}.$$

If $b = 0$ we have $N_U(n) = |I_n|$. If $b \neq 0$, the result follows from Lemma 4 and Theorem 2. □

Remark 2. The characteristic polynomial $m_A \in \mathbb{F}_q[X]$ of any matrix $A \in \mathrm{GL}_2(\mathbb{F}_q)$ has degree 2. Therefore, either m_A splits over $\mathbb{F}_q$ or it is irreducible. If m_A splits, it follows from Schur's Lemma that A is similar to an upper triangular matrix. Thus, Theorem 6 applies to matrices with all their eigenvalues in $\mathbb{F}_q$.

[1] S. D. Cohen, Explicit theorems on generator polynomials, Finite Fields Appl. 11 (2005) 337 – 357.

[2] L. Carlitz, Some theorems on irreducible reciprocal polynomials over a finite field, J. Reine Angew. Math. 227 (1967) 212 – 220.

[3] S. D. Cohen, The explicit construction of irreducible polynomials over finite fields, Designs Codes and Cryptography 2 (1992) 169 – 174.

[4] H. Meyn, On the construction of irreducible self-reciprocal polynomials over finite fields, Appl. Algebra Eng. Comm. Comp. 1 (1990) 43 – 53.

[5] H. Meyn, W. Götz, Self-reciprocal polynomials over finite fields, volume 413/S-21, Publ. I.R.M.A. Strasbourg, 1990, pp. 82 – 90.

[6] S. J. Hong, D. C. Bossen, On some properties of self-reciprocal polynomials, IEEE Trans. Inform. Theory IT-21 (1975) 462 – 464.

[7] J. L. Massey, Reversible codes, Information Control 7 (1964) 369 – 380.

[8] R. C. Mullin, J. L. Yucas, G. L. Mullen, A generalized counting and factoring method for polynomials over finite fields, J. Combin. Math. and Combin. Comput. 72 (2010) 121 – 143.

[9] S. D. Cohen, On irreducible polynomials of certain types in finite fields, Proc. Camb. Math. Soc. 66 (1969) 335 –344.

[10] J. F. Michon, P. Ravache, On different families of invariant irreducible polynomials over $\mathbb{F}_2$, Finite Fields Appl. 16 (2010) 163 – 174.