UNIVERSIDADE FEDERAL DE MINAS GERAIS
Instituto de Ciências Exatas
Programa de Pós-graduação em Matemática

Daniela Alves de Oliveira

Ações de grupos sobre polinômios irredutíveis

Belo Horizonte
2019

DANIELA ALVES DE OLIVEIRA

Ações de grupos sobre polinômios irredutíveis

Dissertação de mestrado apresentada como parte dos requisitos para obtenção do título de Mestre pelo Departamento de Matemática do Instituto de Ciências Exatas da Universidade Federal de Minas Gerais.

Orientador : Fabio Enrique Brochero Martínez
Coorientador: Lucas da Silva Reis (USP - São Carlos)

BELO HORIZONTE
MARÇO DE 2019

Oliveira, Daniela Alves de.

O48a Ações de grupos sobre polinômios irredutíveis [manuscrito] / Daniela Alves de Oliveira. - 2019.
xv, 47 f. il.

Orientador: Fabio Enrique Brochero Martínez.
Coorientador: Lucas da Silva Reis.
Dissertação (mestrado) - Universidade Federal de Minas Gerais, Instituto de Ciências Exatas, Departamento de Matemática.
Referências: f.47
.
1. Matemática – Teses. 2. Polinômios – Teses. 3. Corpos finitos (Algebra) – Teses. 4. Modulos projetivos (Algebra) – Teses. I. Brochero Martínez, Fabio Enrique. II. Reis, Lucas da Silva. III Universidade Federal de Minas Gerais; Instituto de Ciências Exatas, Departamento de Matemática. IV.Título.

CDU 51(043)

Ficha catalográfica elaborada pela bibliotecária Belkiz Inez Rezende Costa
CRB 6ª Região nº 1510

Universidade Federal de Minas Gerais
Departamento de Matemática
Programa de Pós-Graduação em Matemática

FOLHA DE APROVAÇÃO

Ações de grupos sobre polinômios irredutíveis

DANIELA ALVES DE OLIVEIRA

Dissertação defendida e aprovada pela banca examinadora constituída pelos Senhores:

Prof. Fabio Enrique Brochero Martínez
UFMG

Prof. Lucas da Silva Reis
USP

Prof. André Luis Contiero
UFMG

Prof. Renato Vidal da Silva Martins
UFMG

Belo Horizonte, 15 de março de 2019.

Av. Antônio Carlos, 6627 – Campus Pampulha - Caixa Postal: 702
CEP-31270-901 - Belo Horizonte – Minas Gerais - Fone (31) 3409-5963
e-mail: pgmat@mat.ufmg.br - home page: http://www.mat.ufmg.br/pgmat

Aos meus queridos pais, pelo imenso amor e cuidado.

Agradecimentos

Primeiramente agradeço a Deus por ter me guiado ao longo desses anos e por estar ao meu lado durante essa jornada.

Aos meus pais, Maria e Geraldo, por sempre me apoiaram e acreditarem em mim. Por estarem ao meu lado, em todos os momentos difíceis, mesmo distante. À minha irmã Sabrina, por sempre me ver com admiração, o seu apoio foi essencial. Aos meus irmãos Tiago e Diego, por todo carinho e companheirismo.

Ao meu orientador Fabio, o meu mais sincero obrigada, serei eternamente grata por todo carinho e confiança. Por todas manhãs em que você não desistiu de mim, seus conselhos foram primordiais, obrigada por toda orientação e por todo incentivo.

Ao meu coorientador Lucas da Silva Reis, pela amizade e pela orientação nesse trabalho. Obrigada por nunca ter me deixado desistir ao longo desses anos e por acreditar em mim.

Aos professores do Departamento de Matemática da UFMG, pelos ensinamentos e amizades adquiridas ao longo da graduação e do mestrado. Em especial, ao professor Michel Spira, pelo carinho e conselhos ao longo da minha graduação.

Aos professores da minha banca, André Luís Contiero e Renato Vidal da Silva Martins, pelo tempo dedicado a este trabalho e por suas valorosas sugestões.

Aos meus amigos da Matemática e os que conheci após me mudar para BH, por todo carinho e compreensão ao longo desses últimos anos. Vocês foram essenciais nessa caminhada e tornaram ela mais leve.

As secretárias Andréa e Kelli, por estarem sempre dispostas e com um sorriso no rosto para nos ajudar.

A OBMEP, que foi onde nasceu a minha relação com a Matemática e ao PICME por todas oportunidades oferecidas.

Ao suporte financeiro oferecido pela CAPES.

Resumo

Seja n um inteiro positivo e $\mathbb{F}_{q^n}$ o corpo finito com q^n elementos. O objetivo deste trabalho é estudar uma ação do *Grupo Projetivo Semi-Linear* $\mathrm{P\Gamma L}(2,q^n) = \mathrm{PGL}(2,q^n) \rtimes \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ sobre o conjunto dos polinômios mônicos irredutíveis sobre o corpo finito $\mathbb{F}_{q^n}$. Os principais resultados dizem respeito à caracterização e ao número de pontos fixos desta ação.

Palavras Chaves: Corpos Finitos, polinômios irredutíveis, ação de grupos, pontos fixos.

Abstract

Let n be a positive integer and let $\mathbb{F}_{q^n}$ be the finite field with q^n elements, where q is a prime power. The aim of this work is to study a natural action of the *Projective Semilinear Group* $\mathrm{P\Gamma L}(2,q^n) = \mathrm{PGL}(2,q^n) \rtimes \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ on the set of irreducible monic polynomials over the finite field $\mathbb{F}_{q^n}$. Our main results concern the characterization and number of fixed points of this action.

Keywords: Finite Fields, irreducible polynomials, group action, fixed points.

SUMÁRIO

Página

Introdução

Dado q uma potência de primo, existe um único corpo finito com q elementos, que denotaremos por $\mathbb{F}_q$. Sobre este corpo podemos considerar o anel de polinômios $\mathbb{F}_q[x]$, que é um domínio de fatoração única. Uma pergunta natural é: quantos polinômios irredutíveis de grau fixo existem neste domínio? Se definimos

$$C_q(n) = \{f \in \mathbb{F}_q[x] | f(x) \text{ é irredutível, mônico e grau } (f) = n\} \quad \text{e} \quad N_q(n) := |C_q(n)|,$$

temos que a fatoração do polinômio $x^{q^n} - x$ é

$$x^{q^n} - x = \prod_{d|n} \prod_{f \in C_q(d)} f(x).$$

Ao igualarmos os graus dos polinômios na identidade anterior, obtemos $q^n = \sum_{d|n} dN_q(d)$.

A partir disso, a fórmula de inversão de Möbius, permite encontrar uma fórmula explicita para $N_q(n)$. De fato, uma relação assintótica devida a J. C. F. Gauss, conhecida é a seguinte

$$N_q(n) \approx \frac{q^n}{n},$$

onde a notação $a_n \approx b_n$ para sequências reais $(a_n)_{n\geq 1}, (b_n)_{n\geq 1}$ significa que $\lim a_n/b_n \to 1$ quando $n \to \infty$.

Um polinômio mônico é chamado auto-recíproco se $f(x) = x^n f(1/x)$.Um resultado similar é conhecido para polinômios mônicos irredutíveis auto-recíprocos sobre $\mathbb{F}_q$. O grau de polinômios mônicos irredutíveis auto-recíprocos não lineares é par, e foi mostrado por H. Meyn em [4], que os fatores irredutíveis não lineares do polinômio

$$H_r(x) = x^{q^r+1} - 1 \tag{1}$$

são exatamente os polinômios mônicos irredutíveis auto-recíprocos de grau $2k$, onde k divide r e r/k é ímpar. A partir da equação (1) se obtém uma fórmula assintótica para

$$\sigma_q(n) := |A_q(n)|,$$

onde

$$A_q(n) = \{f(x) \in \mathbb{F}_q[x] | f(x) \text{ é mônico, irredutível e auto-recíproco de grau } 2n\}.$$

Mais especificamente, obtemos

$$\sigma_q(2n) \approx \frac{q^n}{2n}.$$

Em [5], uma generalização desse resultado foi feita por H. Stichtenoth e A. Topuzoğlu, considerando os polinômios da forma

$$F_r(x) = bx^{q^r+1} - ax^{q^r} + dx - c, \text{ para } r \geq 0 \tag{2}$$

com $a, b, c, d \in \mathbb{F}_q$ e $ad - bc \neq 0$. Para isso, considera-se para cada inteiro $n \geq 1$ e o conjunto $\mathscr{I}_n$ de polinômios mônicos irredutíveis de grau n sobre $\mathbb{F}_q$. O Grupo Linear Projetivo $\mathrm{PGL}(2,q)$ age sobre os conjuntos $\mathscr{I}_n$, com $n \geq 2$ da seguinte forma: para $[A] \in \mathrm{PGL}(2,q)$ com $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ e $f \in \mathscr{I}_n$, definimos $[A] \circ f$ sendo o único polinômio mônico que é múltiplo escalar do polinômio

$$A \circ f(x) := (cx+d)^n \cdot f\left(\frac{ax+b}{cx+d}\right). \tag{3}$$

Um dos resultados principais em [5], mostra que os $[A]$-invariantes são exatamente os fatores irredutíveis dos polinômios F_r. A partir deste resultado, como antes, conseguimos uma fórmula assintótica para o número de $[A]$-invariantes de grau fixo. De fato, se

$$\Lambda(A,r) := \{f \in \mathbb{F}_q[x] | f \text{ é irredutível, mônico e } \deg(f) = r \text{ e } f \text{ divide } F_r(x)\}, \tag{4}$$

sendo $D = \mathrm{ord}([A])$ e

$$\lambda(A,r) := |\Lambda(A,r)|,$$

então $\lambda(A,r) = 0$ se D não é divisível por r e

$$\lambda(A, Dm) \approx \frac{\varphi(D)}{Dm} q^m.$$

O principal objetivo dessa dissertação é estudar uma generalização dos resultados obtidos [5]. Fixamos n um inteiro positivo e consideramos a fatoração sobre $\mathbb{F}_{q^n}$ dos polinômios

$$F_{A,nr,i}(x) := b^{q^{n-i}} x^{q^{nr-i}+1} - a^{q^{n-i}} x^{q^{nr-i}} + d^{q^{n-i}} x - c^{q^{n-i}}, \tag{5}$$

onde $a, b, c, d \in \mathbb{F}_{q^n}$ com $ad - bc \neq 0$ e $nr \geq i$.

Seja $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ o Grupo de Galois da extensão $\mathbb{F}_{q^n}/\mathbb{F}_q$. Sabemos que esse grupo é gerado pelo automorfismo de Frobenius $\sigma_1 : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ com $\alpha \mapsto \alpha^q$. Para cada $i \geq 1$, denotemos por σ_i a i-ésima composição de σ_1. Podemos estender naturalmente σ_i para o anel de polinômios $\mathbb{F}_{q^n}[x]$, onde $x \mapsto x$ e por simplicidade, denotaremos essa extensão por σ_i.

O Grupo Semi-Linear Projetivo $\mathrm{P\Gamma L}(2,q^n) = \mathrm{PGL}(2,q^n) \rtimes \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ induz uma aplicação sobre o conjunto de polinômios irredutíveis mônicos sobre $\mathbb{F}_{q^n}$. Seja $\mathscr{M}_k$ o conjunto dos polinômios mônicos irredutíveis sobre $\mathbb{F}_{q^n}$ de grau k, com $k \geq 2$, $f \in \mathscr{M}_k$ e $[A, \sigma_i] \in \mathrm{P\Gamma L}(2,q^n)$. Definimos a operação

$$[A, \sigma_i] * f := [A] \circ (\sigma_i(f)).$$

Esta operação define uma ação do grupo $\mathrm{P\Gamma L}(2,q^n)$ nos conjuntos $\mathscr{M}_k$, com $k \geq 2$. Em cada $\mathscr{M}_k$ será estimado o número de $[A,\sigma_i]$-invariantes e assim obtemos uma fórmula assintótica do número de invariantes para um grau arbitrário, sendo estes zero se k não é da forma Ds, onde D é a ordem do elemento $[A^*] \in \mathrm{PGL}(2,q^n)$, onde $A^* = A\sigma_1(A)\cdots\sigma_{n-1}(A)$, com $\mathrm{mdc}(s,n) = 1$. Se $k > 2$ é da forma Ds, com $\mathrm{mdc}(s,n) = 1$, o número $n_A(Ds)$ de polinômios mônicos irredutíveis de grau k que são invariantes por $[A,\sigma_i]$ cumpre que

$$n_A(Ds) \approx \frac{q^s}{Ds}\varphi(D).$$

A estrutura desta dissertação é a seguinte

No capítulo 1 é feita uma breve exposição sobre resultados básicos de corpos finitos que serão úteis nos capítulos seguintes. Veja [3] para mais detalhes. O Capítulo 2 discorre sobre os resultados obtidos por H. Stichtenoth e A. Topuzoğlu em [5]. Estudamos as propriedades da ação definida em (3) e o número assintótico de pontos fixos. Por fim, o capítulo 3 apresenta uma generalização da ação definida em (3). Estudamos as propriedades dessa ação, além da caracterização e estimativa do número de pontos fixos para esta ação.

CAPÍTULO 1

PRELIMINARES

Neste primeiro capítulo apresentamos definições, notações e resultados da teoria de Corpos Finitos e Álgebra que nos serão úteis nos próximos capítulos. Entre os resultados tratados neste capítulo incluiremos uma seção sobre funções multiplicativas que será útil para a contagem de polinômios irredutíveis em um corpo finito. Essencialmente, todos os resultados contidos neste capítulo podem ser encontrados em [3].

1.1 Corpos Finitos

O objeto fundamental estudado nessa dissertação são corpos finitos. O exemplo mais básicos de corpos finitos é o anel de resíduos módulo p denotado por $\mathbb{Z}/(p)$, onde p é um primo. Em geral, se $\mathbb{F}_q$ é um corpo finito com q elementos, temos que $q = p^r$, para algum primo p e r inteiro positivo, sendo p a característica do corpo. É conhecido (Teorema 1.3) que, a menos de isomorfismos, existe um único corpo finito de cardinalidade q.

Definição 1.1. Seja $f(x) \in \mathbb{F}[x]$ um polinômio de grau $n > 0$ e $\mathbb{L}$ uma extensão do corpo $\mathbb{F}$. Dizemos que $f(x)$ se decompõe em $\mathbb{L}$ se $f(x)$ pode ser escrito como o produto de fatores lineares em $\mathbb{L}[x]$, isto é, se existem elementos $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{L}$ tais que

$$f(x) = a(x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n),$$

onde a é o coeficiente líder de $f(x)$. O corpo $\mathbb{L}$ é corpo de decomposição de $f(x)$ sobre $\mathbb{F}$ quando $f(x)$ se decompõe em $\mathbb{L}$ e se $\mathbb{L} = \mathbb{F}(\alpha_1, \alpha_2, \cdots, \alpha_n)$.

Lema 1.2. *Dado um corpo finito $\mathbb{L}$ com q elementos e $\mathbb{F}$ um subcorpo qualquer de $\mathbb{L}$, então $\mathbb{L}$ é corpo de decomposição do polinômio $x^q - x$ sobre $\mathbb{F}$. Em particular, este polinômio se fatora em $\mathbb{L}[x]$ da seguinte maneira*

$$x^q - x = \prod_{a \in \mathbb{L}} (x - a). \tag{1.1}$$

Em outras palavras, todo $\alpha \in \mathbb{L}$ satisfaz que $\alpha^q = \alpha$.

Demonstração. O polinômio $x^q - x$ de grau q tem no máximo q raízes em $\mathbb{L}$. Como o grupo multiplicativo $\mathbb{L}^* = \mathbb{L} \setminus \{0\}$ tem ordem $q-1$, temos pelo Teorema de Lagrange, que para $\alpha \in \mathbb{L}^*$, $\alpha^{q-1} = 1$, isto é, $\alpha^q = \alpha$. Portanto, todos os elementos de $\mathbb{L}$ são raízes de $x^q - x$. Ou seja, $f(x)$ se decompõe em $\mathbb{L}$, como indicado em (1.1) e como tem q raízes distintas, não pode se decompor em nenhum corpo menor. ■

Teorema 1.3. *(Existência e Unicidade de Corpos Finitos). Para cada primo p e todo inteiro positivo n, existe um corpo finito com p^n elementos. Qualquer corpo finito com $q = p^n$ elementos é isomorfo ao corpo de decomposição de $x^q - x$ sobre $\mathbb{F}_p$.*

Demonstração. *(Existência)* Para $q = p^n$, consideremos o polinômio $f(x) = x^q - x$ em $\mathbb{F}_p[x]$, e $\mathbb{L}$ seu corpo de decomposição sobre $\mathbb{F}_p$.O polinômio $f(x)$ tem q raízes distintas em $\mathbb{L}$, pois sua derivada $f'(x) = qx^{q-1} - 1 = -1$ é uma constante não nula. Seja $S = \{a \in \mathrm{F} : a^q - a = 0\}$. Então S é subcorpo de $\mathbb{L}$, uma vez que:

(i) S contém 0 e 1;

(ii) $a, b \in S$ implica que $(a-b)^q = a^q - b^q = a - b$ e então $a - b \in S$;

(iii) Para $a, b \in S$ e $b \neq 0$ temos $(ab^{-1})^q = a^q b^{-q} = ab^{-1}$, assim $ab^{-1} \in S$.

Mas, por outro lado, $x^q - x$ deve se decompor em S, pois S contém todas raízes de $f(x)$. Portanto $\mathbb{L} = S$ e como S tem q elementos, $\mathbb{L}$ é um corpo finito com q elementos.

(Unicidade) Seja $\mathbb{L}$ um corpo finito com $q = p^n$ elementos. A característica de $\mathbb{L}$ é p, portanto $\mathbb{L}$ contém $\mathbb{F}_p$ como subcorpo. Pelo lema anterior, $\mathbb{L}$ é corpo de decomposição de $x^q - x$ sobre $\mathbb{F}_p$. Como quaisquer dois corpos de decomposição de $f(x)$ sobre $\mathbb{F}_p$ são isomorfos, temos a unicidade.

■

Observemos que se $\mathbb{F}$ e $\mathbb{L}$ são corpos finitos com q^n e q^m elementos respectivamente, então $\mathbb{F} \subseteq \mathbb{L}$ se, e somente se, $x^{q^n} - x$ divide $x^{q^m} - x$, que equivale a n dividir m. Em geral o seguinte resultado é válido.

Lema 1.4. *Seja $f(x) \in \mathbb{F}_q[x]$ um polinômio irredutível sobre $\mathbb{F}_q$ de grau m. Então $f(x)$ divide $x^{q^n} - x$ se, e somente se, m divide n.*

Demonstração. ($\Rightarrow$) Suponhamos que $f(x)$ divide $x^{q^n} - x$. Seja α uma raiz de $f(x)$ no corpo de decomposição de $f(x)$ sobre $\mathbb{F}_q$. Então $\alpha^{q^n} = \alpha$, ou seja, $\alpha \in \mathbb{F}_{q^n}$. Em outras palavras, $\mathbb{F}_q(\alpha)$ é subcorpo de $\mathbb{F}_{q^n}$. Mas $[\mathbb{F}(\alpha) : \mathbb{F}_q] = m$ e $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$ e com isso temos que m divide n.

($\Leftarrow$) Se m divide n, então temos que $\mathbb{F}_{q^m}$ é subcorpo de $\mathbb{F}_{q^n}$. Seja α uma raiz de $f(x)$ no corpo decomposição de $f(x)$ sobre $\mathbb{F}_q$, então $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$. Consequentemente, $\alpha \in \mathbb{F}_{q^n}$, ou seja, $\alpha^{q^n} = \alpha$. Sendo assim, α é raiz de $x^{q^n} - x \in \mathbb{F}_q[x]$. Como $f(x)$ é irredutível, temos que $f(x)$ divide $x^{q^n} - x$. ■

A partir da prova do lema anterior, segue que se $f(x) \in \mathbb{F}_q[x]$ é irredutível de grau m, então $f(x)$ divide $x^{q^m} - x$, assim todas as raízes de $f(x)$ estão em $\mathbb{F}_{q^m}$. Logo uma pergunta natural é qual a estrutura, caso exista, do conjunto de tais raízes? O seguinte teorema responde esta pergunta.

Teorema 1.5. *Seja $f(x) \in \mathbb{F}_q[x]$ polinômio irredutível de grau k. Então $f(x)$ tem uma raiz α em $\mathbb{F}_{q^k}$ e todas as raízes de $f(x)$ são simples, dadas por $\alpha, \alpha^q, \ldots, \alpha^{q^{k-1}}$.*

Demonstração. Seja α uma raiz de $f(x)$ em um corpo de decomposição de $\mathbb{F}_q$. Como $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = k$, segue que $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^k}$. Portanto, $\alpha \in \mathbb{F}_{q^k}$. Agora mostraremos que se β é uma raiz de $f(x)$, então β^q também será uma raiz de $f(x)$. Seja $f(x) = \sum_{j=0}^{k} a_j x^j$ com $a_j \in \mathbb{F}_q$ para $0 \leq j \leq k$. Calculando $f(\beta^q)$, temos

$$\begin{aligned} f(\beta^q) &= a_0 + a_1\beta^q + \cdots + a_k\beta^{qk} = a_0^q + a_1^q\beta^q + \cdots + a_k^q\beta^{qk} \\ &= (a_0 + a_1\beta + \cdots + a_k\beta^k)^q = f(\beta)^q = 0. \end{aligned}$$

Assim $\alpha, \alpha^q, \ldots, \alpha^{q^{k-1}}$ são raízes de $f(x)$. Afirmamos que nessa lista os elementos são distintos e logo ela contém todas as raízes. Suponhamos, por contradição, que existe $0 \leq i < j < k$ tais que $\alpha^{q^i} = \alpha^{q^j}$. Em particular,

$$\alpha^{q^{k-j+i}} = \alpha^{q^k} = \alpha.$$

Isso somente é possível se k divide $k - j + i$, porém como $0 < k - j + i < k$, obtemos uma contradição. Portanto todas raízes são distintas, e o número delas coincide com o grau de $f(x)$. ■

Corolario 1.6. *Seja $f(x)$ um polinômio irredutível em $\mathbb{F}_q[x]$ de grau k. Então o corpo de decomposição de $f(x)$ sobre $\mathbb{F}_q$ é dado por $\mathbb{F}_{q^k}$.*

Demonstração. Pelo teorema anterior, $f(x)$ se decompõe em $\mathbb{F}_{q^k}$. Além disso, $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^k}$. Portanto, $\mathbb{F}_q(\alpha, \alpha^q, \cdots, \alpha^{q^{k-1}}) = \mathbb{F}_q(\alpha) = \mathbb{F}_{q^k}$, onde α é uma raiz de $f(x)$ em $\mathbb{F}_{q^k}$. ■

Definição 1.7. Seja $\mathbb{F}_{q^n}$ uma extensão de $\mathbb{F}_q$ e seja $\alpha \in \mathbb{F}_{q^n}$. Os elementos

$$\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}$$

são chamados de conjugados de α com respeito a $\mathbb{F}_q$.

Os conjugados de $\alpha \in \mathbb{F}_{q^n}$ em relação a $\mathbb{F}_q$ serão distintos se, e somente se, o polinômio minimal f_α de α sobre $\mathbb{F}_q$ tiver grau n. Por outro lado, se o grau de f_α for d, um divisor de n, os conjugados de α em relação a $\mathbb{F}_q$ são os elementos distintos $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{d-1}}$ e cada um se repete $\frac{n}{d}$ vezes.

Exemplo 1.8. *Seja $\alpha \in \mathbb{F}_{64}$ uma raiz de $f(x) = x^6 + x + 1 \in \mathbb{F}_2[x]$. Então os conjugados de α em relação a $\mathbb{F}_2$ são*

$$\alpha,\ \alpha^2,\ \alpha^4,\ \alpha^8 = (\alpha+1)\alpha^2 = \alpha^3 + \alpha^2,\ \alpha^{16} = (\alpha^3+\alpha^2)^2 = \alpha^4 + \alpha + 1, \text{ e}$$
$$\alpha^{32} = (\alpha^4 + \alpha + 1)^2 = \alpha^3 + \alpha^2 + \alpha^2 + 1 = \alpha^3 + 1.$$

Os conjugados de α com respeito a $\mathbb{F}_4$ são

$$\alpha,\ \alpha^4,\ \alpha^{16} = (\alpha+1)^2\alpha^4 = \alpha^4 + \alpha + 1.$$

Uma outra estrutura interessante de um corpo é o grupo dos elementos que são diferentes de zero. No caso que o corpo seja finito, o grupo associado é muito simples, como se mostra no seguinte teorema.

Definição 1.9. Um gerador do grupo cíclico $\mathbb{F}_q^*$ é chamado de um elemento primitivo de $\mathbb{F}_q$.

Como um grupo cíclico G de ordem n possui $\varphi(n)$ elementos geradores da forma g^i com $1 \leq i \leq n$ e $\text{mdc}(i,n) = 1$, o grupo $\mathbb{F}_q^*$ tem $\varphi(q-1)$ elementos primitivos.

Existe uma relação importante entre os elementos conjugados e os homomorfismos de um corpo finito: consideremos a extensão $\mathbb{F}_{q^n}$ de $\mathbb{F}_q$ e seja $\sigma : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ um homomorfismo injetivo de $\mathbb{F}_{q^n}$ em $\mathbb{F}_{q^n}$ que fixa os elementos de $\mathbb{F}_q$, ou seja, $\sigma(\alpha+\beta) = \sigma(\alpha) + \sigma(\beta)$ e $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$ para todos $\alpha, \beta \in \mathbb{F}_{q^n}$ e $\sigma(a) = a$ para todo $a \in \mathbb{F}_q$. Como todo elemento

$\alpha \in \mathbb{F}_{q^n}$ é raiz de um polinômio irredutível em $\mathbb{F}_q$ de grau d, com n divisível por d, pelo Lema 1.4, todas as raízes desse polinômio estão em $\mathbb{F}_{q^n}$. Se σ denota, por abuso de notação, a extensão como homomorfismo de anéis para $\mathbb{F}_q[x]$, onde $\sigma(x) = x$, então $f(x)$ é invariante por σ e $\sigma(a) \in \mathbb{F}_{q^n}$ é raiz de $\sigma(f(x)) = f(x)$. Assim, quando trabalhamos em corpos finitos, toda extensão é normal, e os homomorfismos injetivos são automorfismos.

Como os automorfismos formam um grupo, no caso considerado ele será cíclico, como é mostrado a seguir.

Teorema 1.10. *Os distintos automorfismos de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ são exatamente as aplicações $\sigma_0, \sigma_1, \ldots, \sigma_{n-1}$, definidas por $\sigma_i(\alpha) = \alpha^{q^i}$ para $\alpha \in \mathbb{F}_{q^n}$ e $0 \leq i \leq n-1$.*

Demonstração. Para cada σ_i e $\alpha, \beta \in \mathbb{F}_{q^n}$ quaisquer, é válido que

$$\sigma_i(\alpha\beta) = \sigma_i(\alpha)\sigma_i(\beta)$$
$$\sigma_i(\alpha + \beta) = \sigma_i(\alpha) + \sigma_i(\beta)$$

Logo σ_i é um endomorfismo de $\mathbb{F}_{q^n}$. Assim precisamos mostrar que está aplicação é injetiva. Mas isso segue do fato que $\sigma_i(\alpha) = 0$ se, e somente se, $\alpha^{q^i} = 0$. Como $\mathbb{F}_{q^n}$ é um corpo finito, segue que σ_i é um automorfismo de $\mathbb{F}_{q^n}$. Além disso, $\sigma_i(a) = a$ equivale a $\alpha^{q^i} = a$, que implica que $a \in \mathbb{F}_{q^i}$, em particular, $\sigma_i(a) = a$ para todo $a \in \mathbb{F}_q$. Portanto, cada σ_i é um automorfismo de $\mathbb{F}_{q^n}$ que fixa $\mathbb{F}_q$. As aplicações $\sigma_0, \sigma_1, \ldots, \sigma_{n-1}$ são distintas, pois elas tem distintos valores para um elemento primitivo de $\mathbb{F}_{q^n}$.

Agora suponha que σ é um automorfismo de $\mathbb{F}_{q^n}$ que fixa $\mathbb{F}_q$. Sejam β um elemento primitivo de $\mathbb{F}_{q^n}$ e $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{F}_q[x]$ o polinômio minimal de β sobre $\mathbb{F}_q$. Então

$$\begin{aligned} 0 &= \sigma(\beta^n + a_{n-1}\beta^{n-1} + \cdots + a_0) \\ &= \sigma(\beta)^n + a_{n-1}\sigma(\beta)^{n-1} + \cdots + a_0, \end{aligned}$$

Ou seja, $\sigma(\beta)$ é uma raiz de $f(x)$ em $\mathbb{F}_{q^n}$. Pelo Teorema 1.5 $\sigma(\beta) = \beta^{q^i}$ para algum i, com $0 \leq i \leq n-1$. Como σ é um homomorfismo e todo elemento diferente de zero é uma potência de β, concluímos que $\sigma(\alpha) = \alpha^{q^i}$ para todo $\alpha \in \mathbb{F}_{q^n}$. ■

Definição 1.11. Seja $\mathbb{F}_{q^n}$ uma extensão de $\mathbb{F}_q$, então a aplicação $\sigma : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$, definida para cada $a \in \mathbb{F}_{q^n}$ por

$$\sigma(a) = a^q$$

é um automorfismo chamado de homomorfismo de Frobenius. Definimos σ_i como sendo o homomorfismo de Frobenius aplicado i vezes, isto é, para $a \in \mathbb{F}_{q^n}$

$$\sigma_i(a) = \sigma^i(a) = a^{q^i}.$$

Notemos que como para $\alpha \in \mathbb{F}_{q^n}$ temos que $\alpha^{q^n} = \alpha$, segue que σ^n é a função identidade sobre os elementos de $\mathbb{F}_{q^n}$.

A extensão natural do automorfismo de Frobenius para o anel de polinômios $\mathbb{F}_{q^n}[x]$ é definida como

$$\sigma(a) = a^q \text{ para todo } a \in \mathbb{F}_{q^n}$$
$$\sigma(x) = x,$$

e tal que seja um homomorfismo de anéis. Um resultado importante sobre esse homomorfismo estendido é que ele preserva a irredutibilidade de polinômios, como veremos no seguinte teorema.

Teorema 1.12. *Seja $\mathbb{F}_{q^n}$ uma extensão de $\mathbb{F}_q$ e σ o homomorfismo de Frobenius em $\mathbb{F}_{q^n}$, então $f(x) \in \mathbb{F}_{q^n}[x]$ é irredutível sobre $\mathbb{F}_{q^n}$ se, e somente se, $\sigma(f(x))$ é irredutível sobre $\mathbb{F}_{q^n}$.*

Demonstração. ($\Rightarrow$) Suponhamos que $\sigma(f(x))$ é redutível. Ou seja, existem $g(x), h(x) \in \mathbb{F}_{q^n}[x]$ tais que $\sigma(f(x)) = g(x)h(x)$, onde $g(x)$ e $h(x)$ são polinômios não constantes. Aplicando o homomorfismo de Frobenius $n-1$ vezes a essa identidade, obtemos

$$f = \sigma^n(f) = \sigma^{n-1}(g) \cdot \sigma^{n-1}(h).$$

Como $f(x)$ é irredutível um dos polinômios $\sigma^{n-1}(g)$ ou $\sigma^{n-1}(h)$ é um polinômio constante. Sem perda de generalidade, podemos supor $\sigma^{n-1}(g(x))$ constante, logo $g(x) = \sigma(\sigma^{n-1}(g))$ é constante, o que é contraditório. Portanto $\sigma(f(x))$ é irredutível.

($\Leftarrow$) Suponhamos $f(x)$ redutível, isto é, existem $r(x), s(x) \in \mathbb{F}_{q^n}[x]$, polinômios não constantes, tais que $f = r(x)s(x)$. Aplicando o homomorfismo de Frobenius

$$\sigma(f) = \sigma(r(x)) \cdot \sigma(s(x)),$$

Assim $\sigma(f(x))$ é redutível, pois $\sigma(r(x))$ ou $\sigma(s(x))$ possuem os mesmo graus que r e s respectivamente, uma contradição.

■

1.2 Polinômios irredutíveis

Dado um polinômio $f \in \mathbb{F}_q[x]$ irredutível de grau n, sabemos que toda raiz de $f(x)$ está em $\mathbb{F}_{q^n}$ e logo é um fator de $x^{q^n} - x$. Uma pergunta natural é quantos polinômios irredutíveis de grau n existem, que pela afirmação anterior, estão limitados por $\frac{q^n}{n}$. Sobre isso, temos o seguinte resultado.

Teorema 1.13. *Para todo corpo finito $\mathbb{F}_q$ e todo $n \in \mathbb{N}$, o produto de todos polinômios mônicos irredutíveis sobre $\mathbb{F}_q$ cujo grau divide n é igual a $x^{q^n} - x$.*

Demonstração. Pelo Lema 1.4, os polinômios mônicos sobre $\mathbb{F}_q$ que aparece na fatoração de $g(x) = x^{q^n} - x$ em $\mathbb{F}_q[x]$ são precisamente os que tem grau que divide n. Como $g'(x) = -1$, g não tem raízes múltiplas e cada polinômio mônico irredutível sobre $\mathbb{F}_q$ cujo grau divide n ocorre exatamente uma vez na fatoração de g em $\mathbb{F}_q[x]$. ■

Corolario 1.14. *Se $N_q(d)$ é o número de polinômios mônicos irredutíveis em $\mathbb{F}_q[x]$ de grau d, então*

$$q^n = \sum_{d|n} dN_q(d) \quad \textit{para todo } n \in \mathbb{N},$$

onde a soma é estendida sobre todos divisores positivos d de n.

Demonstração. A igualdade segue do teorema anterior, comparando o grau do polinômio $g(x) = x^{q^n} - x$ com o grau dos polinômios da fatoração de $g(x)$. ■

Para encontrar o valor exato de $N_q(d)$ introduzimos a função de Möbius.

Definição 1.15. A função Möbius $\mu : \mathbb{N}_{>0} \to \mathbb{Z}$ é definida por:

$$\mu(n) = \begin{cases} 1 & \text{se } n = 1, \\ 0 & \text{se } a^2 | n \text{ para algum inteiro } a > 1, \\ (-1)^k & \text{se } n \text{ é o produto de } k \text{ primos distintos.} \end{cases}$$

Lema 1.16. *Para todo n inteiro positivo*

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \textit{se } n = 1, \\ 0, & \textit{se } n > 1. \end{cases}$$

Demonstração. No caso $n = 1$, não temos nada a provar. Precisamos considerar os divisores d de n tais que $\mu(d) \neq 0$, em outras palavras, $d = 1$ ou d é o produto de primos distintos. Se $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, então

$$\begin{aligned} \sum_{d|n} \mu(d) &= \sum_{0 \leq \beta_i \leq \alpha_i} \mu(p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}) \\ &= \mu(1) + \sum_{i=1}^{k} \mu(p_i) + \sum_{1 \leq i_1 < i_j \leq k}^{k} \mu(p_{i_1} p_{i_2}) + \cdots + \mu(p_1 p_2 \cdots p_k) \\ &= 1 + \binom{k}{1}(-1) + \binom{k}{2}(-1)^2 + \cdots + \binom{k}{k}(-1)^k \\ &= (1 + (-1))^k = 0. \end{aligned}$$

■

Teorema 1.17. *(Fórmula de Inversão de Möbius)*

(i) Caso aditivo: Seja h e H duas funções de $\mathbb{N}$ *em um grupo abeliano aditivo G. Então para todo n inteiro positivo,*

$$H(n) = \sum_{d|n} h(d) \tag{1.2}$$

se, e somente se,

$$h(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) H(d) = \sum_{d|n} \mu(d) H\left(\frac{n}{d}\right). \tag{1.3}$$

(ii) Caso multiplicativo: Seja h e H duas funções de $\mathbb{N}$ *em um grupo abeliano multiplicativo G. Então para todo n inteiro positivo,*

$$H(n) = \prod_{d|n} h(d)$$

se, e somente se,

$$h(n) = \prod_{d|n} H(d)^{\mu(\frac{n}{d})} = \prod_{d|n} H\left(\frac{n}{d}\right)^{\mu(d)}.$$

Demonstração. Suponhamos que (1.2) é válido. Observemos que para todo $n \in \mathbb{N}$

$$\begin{aligned}\sum_{d|n} \mu\left(\frac{n}{d}\right) H(d) &= \sum_{d|n} \mu(d) H\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \sum_{c|\frac{n}{d}} h(c) \\ &= \sum_{c|n} \sum_{d|\frac{n}{c}} \mu(d) h(c) = \sum_{c|n} h(c) \sum_{d|\frac{n}{c}} \mu(d) = h(n),\end{aligned}$$

onde a última igualdade segue do lema anterior.

Por outro lado, se (1.3) vale, temos

$$\begin{aligned}\sum_{d|n} h(d) &= \sum_{d|n} \sum_{d'|d} \mu\left(\frac{d}{d'}\right) H(d') = \sum_{d'|n} H(d') \sum_{d|\frac{n}{d'}} \mu(d) \\ &= H(n),\end{aligned}$$

como queríamos demonstrar. A prova do segundo item segue analogamente ao primeiro item, substituindo as somas por produtos e multiplicação por potência. ■

Teorema 1.18. *O número* $N_q(n)$ *de polinômios mônicos irredutíveis em* $\mathbb{F}_q[x]$ *de grau n é dado por*

$$N_q(n) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d = \frac{1}{n} \sum_{d|n} \mu(d) q^{\frac{n}{d}}.$$

Demonstração. Pelo Corolário 1.14 e como $q^n = \sum_{d|n} dN_q(d)$, aplicando a fórmula de inversão de Möbius no caso aditivo para o grupo aditivo dos inteiros, com $h(d) = dN_q(d)$ e $H(n) = q^n$, obtemos

$$nN_q(n) = \sum_{d|n} \mu(d) q^{\frac{n}{d}} = \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$$

ou seja,

$$N_q(n) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d = \frac{1}{n} \sum_{d|n} \mu(d) q^{\frac{n}{d}}.$$

■

Corolario 1.19. *Assintoticamente, o número $N_q(n)$ de polinômios mônicos irredutíveis em $\mathbb{F}_q[x]$ de grau n é dado por*

$$N_q(n) \approx \frac{q^n}{n},$$

onde $a_s \approx b_s$ representa $\lim_{s\to\infty} \frac{a_s}{b_s} = 1$.

Exemplo 1.20. *O número de polinômios irredutíveis em $\mathbb{F}_q[x]$ de grau 12 é dado por:*

$$\begin{aligned} N_q(12) &= \frac{1}{12} \sum_{d|12} \mu(d) q^{\frac{12}{d}} \\ &= \frac{1}{12} \left(\mu(1)q^{12} + \mu(2)q^6 + \mu(3)q^4 + \mu(4)q^3 + \mu(6)q^2 + \mu(12)q\right) \\ &= \frac{1}{12}(q^{12} - q^6 - q^4 + q^2). \end{aligned}$$

Observemos que se $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ com $p_1 < p_2 < \cdots < p_k$ primos distintos, então $k < \log_2 n$ e

$$N_q(n) > \frac{1}{n}\left(q^n - q^{\frac{n}{p_1}} - \cdots q^{\frac{n}{p_k}}\right) > \frac{1}{n}\left(q^n - (\log_2 n)\sqrt{q^n}\right) > \frac{q^n}{n}\left(1 - \frac{\log_2 n}{\sqrt{q^n}}\right),$$

Logo "quase" todo fator de $x^{q^n} - x$ tem grau n. Ou seja, assintoticamente o número polinômios irredutíveis sobre $\mathbb{F}_q$ de grau n é $\frac{q^n}{n}$.

1.3 Grupo Projetivo

Nessa seção traremos de algumas definições e resultados básicos do Grupo Linear. Esse grupo será útil nos próximos capítulos.

1.3.1 Grupo Linear Projetivo

Definição 1.21. Seja n um número natural. O grupo linear de grau n sobre $\mathbb{F}_q$ é o grupo das matrizes invertíveis $n \times n$ com entradas em $\mathbb{F}_q$, munido da operação multiplicação usual de matrizes. Este grupo é denotado por $\mathrm{GL}(n,q)$.

Sobre os elementos de $\mathrm{GL}(n,q)$, se define a seguinte relação de equivalência:

$$A \sim B : \text{ se, e somente se, } B = \lambda A \text{ para algum } \lambda \in \mathbb{F}_q^*.$$

A classe de equivalência de $A \in \mathrm{GL}(n,q)$ é denotada por $[A]$. Estas classes de equivalência determinam o grupo apresentado a seguir.

Definição 1.22. O Grupo Linear Projetivo de grau n é o quociente de $\mathrm{GL}(n,q)$ pela relação de equivalência $\sim$. Este grupo é denotado por $\mathrm{PGL}(n,q)$, com a estrutura de grupo $[A]\cdot[B] = [AB]$.

O lema a seguir determina a ordem desses grupos.

Lema 1.23. *As ordens dos grupos $GL(n,q)$ e $PGL(n,q)$ são dadas por*

$$\begin{aligned} |GL(n,q)| &= (q^n-1)(q^n-q)(q^n-q^2)\cdots(q^n-q^{n-1}) \\ &= q^{n(n-1)/2}(q-1)(q^2-1)\cdots(q^n-1). \end{aligned}$$

$$|PGL(n,q)| = q^{n(n-1)/2}(q^2-1)\cdots(q^n-1).$$

Demonstração. Uma matriz $n \times n$ é invertível se, e somente se, suas linhas são linearmente independentes. Assim para escolha da primeira linha temos q opções para cada entrada, excluído todas entradas nulas, isto é, temos $q^n - 1$ possibilidades. Para segunda linha, como precisamos que ela seja linearmente independente a primeira linha, temos q^n escolhas, excluindo uma linha múltipla da anterior, que são q, assim temos $q^n - q$ possibilidades. Analogamente, para as i-ésimas linhas se tem $q^n - q^i$ possibilidades. Portanto a ordem do grupo linear é

$$(q^n-1)(q^n-q)(q^n-q^2)\cdots(q^n-q^{n-1}) = q^{n(n-1)/2}(q-1)(q^2-1)\cdots(q^n-1),$$

Para o grupo $\mathrm{PGL}(n,q)$ basta perceber que o número de elementos em cada classe de equivalência é $q-1$, que corresponde ao número de escolhas de elementos em $\mathbb{F}_q^*$, portanto basta dividirmos a ordem de $\mathrm{GL}(n,q)$ por $q-1$, ou seja, a ordem será

$$\frac{(q^n-1)(q^n-q)(q^n-q^2)\cdots(q^n-q^{n-1})}{q-1} = q^{n(n-1)/2}(q^2-1)\cdots(q^n-1).$$

■

Exemplo 1.24. *Consideremos o grupo $GL(2,2)$. Pelo lema anterior*

$$|GL(2,2)| = 2(2-1)(2^2-1) = 6,$$
$$PGL(2,2) = 2(2^2-1) = 6.$$

Em outras palavras o grupo projetivo linear e o grupo linear são os mesmos para $n = 2$ e $q = 2$. Explicitamente, os elementos do grupo $GL(2,2)$ são

$$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}, \begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}, \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}, \begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}, \begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}.$$

1.3.2 Grupo Semi-Linear Projetivo

Definição 1.25. Seja $\mathbb{F}_{q^n}$ um corpo finito e m um número natural. O grupo semi-linear projetivo de grau m sobre $\mathbb{F}_{q^n}$, denotado por $\mathrm{P\Gamma L}(m,q^n)$, é definido como o grupo do produto externo semi-direto do grupo linear $\mathrm{PGL}(m,q^n)$ pelo grupo de $\mathbb{F}_q$-automorfismos do corpo $\mathbb{F}_{q^n}$, isto é,

$$\mathrm{P\Gamma L}(m,q^n) = \mathrm{PGL}(m,q^n) \rtimes \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q).$$

Lembremos que o grupo de Galois de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ é o grupo cíclico gerado pelo automorfismo de Frobenius σ, definido em 1.11. Nesse caso os elementos do grupo de automorfismo são da forma σ_i, para $0 \le i < n$. Este grupo age nos elementos de $\mathbb{F}_{q^n}$, assim $\mathrm{P\Gamma L}(n,q)$ pode ser visto como uma ação sobre o espaço vetorial $\mathbb{F}_{q^n}^m$, onde para $A \in \mathrm{PGL}(m,q^n)$ e $\sigma_i \in \mathrm{Aut}(\mathbb{F}_{q^n})$ com $0 \le i \le m-1$. Esta ação é definida como

$$(A,\sigma_i)\begin{pmatrix}\alpha_1\\ \alpha_2\\ \vdots\\ \alpha_m\end{pmatrix} = A\begin{pmatrix}\sigma_i(\alpha_1)\\ \sigma_i(\alpha_2)\\ \vdots\\ \sigma_i(\alpha_m)\end{pmatrix}.$$

A operação nesse grupo será denotada por $\diamond$ e é definida da seguinte maneira: para $[A,\sigma_i],[B,\sigma_j] \in \mathrm{P\Gamma L}(m,q^n)$

$$[A,\sigma_i]\diamond[B,\sigma_j] = [A\sigma_i(B),\sigma_{i+j}].$$

O elemento identidade desse grupo é $[E,\sigma_0]$, onde E é a matriz identidade $m \times m$. Este grupo será importante no Capítulo 3, onde iremos definir uma ação dos elementos desse grupo, sobre polinômios em $\mathbb{F}_{q^n}$.

CAPÍTULO 2

AÇÃO DO GRUPO LINEAR PROJETIVO

Dado um conjunto S e um grupo G agindo sobre S, uma das perguntas mais pertinentes é a de caracterizar pontos fixos dessa ação. Em particular, estimar o número de pontos fixos.

2.1 Ação do grupo PGL$(2,q)$

Neste capítulo denotaremos o conjunto dos polinômios sobre $\mathbb{F}_q[x]$ que não possuem raízes em $\mathbb{F}_q$ por

$$\mathscr{I} := \{f(x) \in \mathbb{F}_q[x] | f(x) \text{ não tem raízes em } \mathbb{F}_q\}.$$

Sobre o conjunto $\mathscr{I}$, definiremos a seguinte operação:

Definição 2.1. Para $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2,q)$ e um polinômio $f(x) \in \mathscr{I}$ de grau n, definimos o polinômio

$$(A \circ f)(x) := (bx+d)^n f\left(\frac{ax+c}{bx+d}\right).$$

Afirmamos que esta operação satisfaz as condições necessárias para ser uma ação de grupos. Além disso, esta operação preserva algumas estruturas nos polinômios, como o grau e a irredutibilidade, como veremos no seguinte lema.

Lema 2.2. *Seja $A, B \in GL(2,q)$ e $f(x), g(x) \in \mathscr{I}$ e E a matriz identidade 2×2. As seguintes afirmações são válidas:*

(i) $A \circ f \in \mathscr{I}$ *e* $\deg(A \circ f) = \deg(f)$,

(ii) $E \circ f = f$,

(iii) $(AB) \circ f = A \circ (B \circ f)$,

(iv) $A \circ (f \cdot g) = (A \circ f) \cdot (A \circ g)$,

(v) $f(x)$ *é irredutível se, e somente se,* $A \circ f$ *é irredutível.*

Demonstração. (i) Seja $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2,q)$ e $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathscr{I}$, com $a_n \neq 0$. Se verifica que $A \circ f$ é um polinômio, pois $A \circ f = \sum_{i=0}^{n} a_i (ax+c)^i (bx+d)^{n-i}$ e

$$\begin{aligned} (A \circ f)(x) &= a_n (ax+c)^n + a_{n-1}(ax+c)^{n-1}(bx+d) + \cdots + a_0 (bx+d)^n \\ &= (a_n a^n + a_{n-1} a^{n-1} b + \cdots + a_1 a b^{n-1} + a_0 b^n) x^n + \cdots . \end{aligned} \tag{2.1}$$

Se $b \neq 0$, o coeficiente de x^n é $b^n \left(a_n \left(\frac{a}{b}\right)^{n-1} + \cdots + a_0 \right) = b^n \cdot f\left(\frac{a}{b}\right) \neq 0$, pois $f(x)$ não possui raízes em $\mathbb{F}_q$. Se $b = 0$, então $a \neq 0$ e o coeficiente de x^n é $a_n x^n \neq 0$. Logo $\deg(f(x)) = \deg(A \circ f)$.

Falta mostrar que $A \circ f$ não tem raízes em $\mathbb{F}_q$. Seja $\gamma \in \mathbb{F}_q$. Se $b\gamma + d \neq 0$ então $(A \circ f)(\gamma) = (b\gamma + d)^n f((a\gamma + c)/(b\gamma + d)) \neq 0$, pois $f((a\gamma + c)/(b\gamma + d)) \neq 0$. Se $b\gamma + d = 0$ então pela equação (2.1) , $(A \circ f)(\gamma) = a_n (a\gamma + c)^n$. Observemos que $a\gamma + c \neq 0$, pois caso contrário

$$\gamma(a,b) + (c,d) = (0,0),$$

uma combinação linear não trivial sobre $\mathbb{F}_q$, uma contradição, pois as linhas da matriz A são linearmente independentes. Portanto $(A \circ f)(\gamma) \neq 0$.

(ii) Segue da definição.

(iii) Sejam $f(x) \in \mathscr{I}$, $\deg(f(x)) = n$, $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ e $B = \begin{pmatrix} r & s \\ u & v \end{pmatrix}$. Então

$$(B \circ f)(x) = (sx+v)^n \cdot f\left(\frac{rx+u}{sx+v}\right),$$

e

$$\begin{aligned} (A \circ (B \circ f))(x) &= (bx+d)^n \left(s\left(\frac{ax+c}{bx+d}\right) + v \right)^n \cdot f\left(\frac{r\frac{ax+c}{bx+d} + u}{s\frac{ax+c}{bx+d} + v} \right) \\ &= ((as+bv)x + (cs+v)^n \cdot f\left(\frac{(ar+bu)x + (cr+du)}{(as+bv)x + (cs+dv)} \right) \\ &= ((AB) \circ f)(x), \end{aligned}$$

onde a última igualdade segue do fato que $AB = \begin{pmatrix} ar+bu & as+bv \\ cr+du & cs+dv \end{pmatrix}$.

(iv) Observemos que

$$A \circ (f \cdot g) = (bx+d)^{\deg(f)+\deg(g)} \cdot f\left(\frac{ax+c}{bx+d}\right) g\left(\frac{ax+c}{bx+d}\right) = (A \circ f) \cdot (A \circ g).$$

(v) Segue diretamente dos itens (iii) e (iv).

■

Como consequência deste lema, $E \circ f = f$ e $(AB) \circ f = A \circ (B \circ f)$, ou seja, esta operação define uma ação do grupo $\mathrm{GL}(2,q)$ sobre $\mathscr{I}$. A partir de agora, iremos restringir essa ação aos seguintes conjuntos

$$\mathscr{I}'_n := \{f(x) \in \mathscr{I} \mid \deg f(x) = n \text{ e } f(x) \text{ é irredutível}\},$$

que fornece uma ação do grupo $\mathrm{GL}(2,q)$ em $\mathscr{I}_n$, para todo $n \geq 2$.

Consideremos a relação de equivalência em $\mathscr{I}$ dada por

$$f \sim g :\Leftrightarrow g = \lambda f \text{ para algum } \lambda \in \mathbb{F}_q, \lambda \neq 0.$$

A classe de equivalência de $f(x) \in \mathscr{I}$ é denotada por $[f]$. O seguinte lema mostra que as relações de equivalência são preservadas pela ação do grupo $\mathrm{GL}(2,q)$.

Lema 2.3. *Para $A, B \in GL(2,q)$ e $f, g \in \mathscr{I}$,*

(i) Se $A \sim B$ então $A \circ f \sim B \circ f$,

(ii) Se $f \sim g$ então $A \circ f \sim A \circ g$.

Como consequência definimos a ação do grupo linear projetivo $\mathrm{PGL}(2,q)$ nas classes de equivalência $\mathscr{I}/\sim$ e $\mathscr{I}'_n/\sim$ como

$$[A] \circ [f] := [A \circ f].$$

Toda classe de equivalência $[f] \in \mathscr{I}/\sim$ contém um único polinômio mônico, assim definimos de forma natural uma ação de $\mathrm{PGL}(2,q)$ sobre os conjuntos

$$\mathscr{I}_n := \{f(x) \in \mathbb{F}_q[x] | f(x) \text{ é irredutível, mônico e grau}(f(x)) = n\}, \quad n \geq 2.$$

Definição 2.4. Para $[A] \in \mathrm{PGL}(2,q)$ e $f(x) \in \mathscr{I}_n$,

$$[A] \circ f := \text{ o único polinômio mônico } g \text{ com } g \sim A \circ f.$$

Também definiremos uma ação de $\mathrm{PGL}(2,q)$ sobre $\overline{\mathbb{F}}_q \setminus \mathbb{F}_q$.

Definição 2.5. Para $\alpha \in \overline{\mathbb{F}}_q \setminus \mathbb{F}_q$ e $[A] \in \mathrm{PGL}(2,q)$ com $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, definimos a operação

$$[A] \circ \alpha := \frac{d\alpha - c}{-b\alpha + a}. \tag{2.2}$$

Lema 2.6. *Para* $[A],[B] \in PGL(2,q)$ *e* $\alpha \in \overline{\mathbb{F}}_q \setminus \mathbb{F}_q$,

$$[A] \circ ([B] \circ \alpha) = [AB] \circ \alpha.$$

Demonstração. Sejam $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ e $B = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$. Por definição,

$$\begin{aligned}
[A] \circ ([B] \circ \alpha) &= [A] \circ \left(\frac{h\alpha - g}{-f\alpha + e} \right) \\
&= \frac{d\frac{h\alpha - g}{-f\alpha + e} - c}{-b\frac{h\alpha - g}{-f\alpha + e} + a} \\
&= \frac{d(h\alpha - g) - c(-f\alpha + e)}{-b(h\alpha - g) + a(-f\alpha + e)} \\
&= \frac{(cf + dh)\alpha - (ce + dg)}{-(af + bh)\alpha + (ae + bg)} \\
&= [AB] \circ \alpha,
\end{aligned}$$

pois $[AB] = \begin{pmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{pmatrix}$.

■

Como $[E] \circ \alpha = \alpha$, onde E é a matriz identidade em $\mathrm{PGL}(2,q)$, pelo lema anterior, segue que a operação definida em (2.2) é uma ação do grupo $\mathrm{PGL}(2,q)$ sobre $\overline{\mathbb{F}}_q \setminus \mathbb{F}_q$. As raízes de $f(x)$ e $[A] \circ f$ estão relacionadas como segue.

Lema 2.7. *Seja* $f \in \mathscr{I}$ *e* $A \in GL(2,q)$. *Então para* $\alpha \in \overline{\mathbb{F}}_q$,

$$f(\alpha) = 0 \text{ se, e somente se, } (A \circ f)([A] \circ \alpha) = 0.$$

Demonstração. Seja $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ e $n := \deg((f)$. Calculando $(A \circ f)(A \circ \alpha)$

$$\begin{aligned}(A \circ f)([A] \circ \alpha) &= (A \circ f)\left(\frac{d\alpha - c}{-b\alpha + a}\right). \\ &= \left(b \cdot \frac{d\alpha - c}{-b\alpha + a} + d\right)^n f\left(\frac{a \cdot \frac{d\alpha - c}{-b\alpha + a} + c}{-b\frac{d\alpha - c}{-b\alpha + a} + d}\right) \\ &= \left(\frac{ad - bc}{-b\alpha + a}\right)^n \cdot f\left(\frac{a(d\alpha - c) + c(-b\alpha + a)}{-b(d\alpha - c) + d(-b\alpha + a)}\right) \\ &= \left(\frac{ad - bc}{-b\alpha + a}\right)^n \cdot f(\alpha).\end{aligned}$$

Como $ad - bc \neq 0$ e $-b\alpha + a \neq 0$, temos que $f(\alpha) = 0$ se, e somente se, $(A \circ f)([A] \circ \alpha) = 0$. ■

Como consequência, o polinômio minimal de $[A] \circ \alpha$ é determinado explicitamente pelo polinômio minimal de α, dado pela seguinte proposição.

Proposição 2.8. *Seja* $[A] \in PGL(2, q)$ *e* $\alpha \in \overline{\mathbb{F}}_q$ *uma raiz de* $f(x) \in \mathscr{I}_n, n \geq 2$. *Então* $[A] \circ f$ *é o polinômio minimal de* $[A] \circ \alpha$ *sobre* $\mathbb{F}_q$.

Demonstração. Seja $f_\alpha(x)$ o polinômio minimal de $[A] \circ \alpha$. Pelo lema anterior, $[A] \circ \alpha$ é raiz de $[A] \circ f$, logo f_α divide $([A] \circ f)$. Pelo item (v) do Lema 2.2, $([A] \circ f)$ é irredutível e como f_α é minimal, f_α é é irredutível e portanto $f_\alpha = [A] \circ f$. ■

Corolario 2.9. *Seja* $[A] \in PGL(2, q)$ *e* $\alpha \in \overline{\mathbb{F}}_q$ *raiz do polinômio* $f(x) \in \mathscr{I}_n (n \geq 2)$. *Então*

$$[A] \circ f = f \text{ se, e somente se, } f([A] \circ \alpha) = 0.$$

2.2 Propriedades de polinômios irredutíveis invariantes

Seja H um subgrupo de $\mathrm{PGL}(2, q)$. Denotamos o conjunto dos polinômios irredutíveis que são invariantes pela ação de H, por

$$\mathscr{I}_n(H) := \{f(x) \in \mathscr{I}_n | [B] \circ f = f \text{ para todo } [B] \in H\},$$

para todo $n \geq 2$. Veremos que com uma exceção, o conjunto $\mathscr{I}_n(\mathrm{PGL}(2, q))$ é vazio. Nos casos onde $H = \langle [A] \rangle$ é um grupo cíclico gerado por um elemento não-trivial $[A] \in \mathrm{PGL}(2, q)$, denotaremos

$$\mathscr{I}_n([A]) := \mathscr{I}_n(\langle [A] \rangle) = \{f \in \mathscr{I}_n | [A] \circ f = f\}.$$

Definição 2.10. Seja

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{F}_q[x]$$

com $a_n \neq 0$. O polinômio recíproco $f^*(x)$ de $f(x)$ é definido por:

$$f^*(x) = x^n f\left(\frac{1}{x}\right) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n.$$

Dizemos que um polinômio é auto-recíproco se $f^*(x) = f(x)$.

Exemplo 2.11. *O polinômio reciproco de* $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{F}_q[x]$, *com* $a_0 \cdot a_n \neq 0$, *é o polinômio* $f^*(x) := a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n$. *Este polinômio pode ser obtido a partir de* $f(x)$ *pela ação da matriz* $S := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, *pois* $[S] \circ f = x^n f\left(\frac{1}{x}\right)$. *Assim um polinômio* $f(x)$ *arbitrário é invariante pela matriz* S *se, e somente se, ele é auto-recíproco.*

O seguinte teorema relaciona a ordem de um subgrupo H de $\mathrm{PGL}(2,q)$, com o grau de um polinômio invariante pelo elementos de H.

Teorema 2.12. *Seja* H *um subgrupo de* $PGL(2,q)$ *de ordem* $D \geq 2$. *Assumamos que* $f(x) \in \mathscr{I}_n$ *é invariante por* H, *isto é ,* $[B] \circ f = f$ *para todo* $[B] \in H$. *Então ou* $n = 2$ *ou* n *é divisível por* D. *Em particular, se* $[A] \in PGL(2,q)$ *tem ordem* $\mathrm{ord}[A] = D \geq 2$ *e* $\mathscr{I}_n[A] \neq \emptyset$, *então* $n = 2$ *ou* D *divide* n.

Demonstração. Seja $W \subset \overline{\mathbb{F}}_q$ o conjunto das raízes de $f(x)$. A cardinalidade de W é n, pois $f(x)$ é separável. Para $\alpha \in W$ e $[B] \in H$, como $f(\alpha) = 0$, pela Proposição 2.8, temos

$$f([B] \circ \alpha) = ([B] \circ f)([B] \circ \alpha) = 0,$$

logo $[B] \circ \alpha \in W$. Assim H age sobre W permutando as raízes.

Afirmamos que para $n \geq 3$, esta ação não tem ponto fixo. De fato, suponha que $[B] \in H$ fixa algum $\alpha \in W$. Se $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in H$ então,

$$\frac{d\alpha - c}{-b\alpha + a} = \alpha,$$

isto é,

$$b\alpha^2 + (d-a)\alpha - c = 0.$$

Como o polinômio minimal de α sobre $\mathbb{F}_q$ tem grau $n \geq 3$, concluímos que $a = d$ e $b = c = 0$, ou seja $[B] = [E]$.

Consequentemente, o estabilizador desta ação do grupo H em W tem cardinalidade $D = |H|$, e como ordem da órbita divide a ordem do grupo, temos que D divide $|W|$. ■

Corolario 2.13. *Suponha que $n \geq 2$ é primo relativo com $q(q^2-1)$. Então todas as órbitas de $\mathscr{I}_n$ sobre a ação de $PGL(2,q)$ tem tamanho $q(q^2-1)$.*

Demonstração. Para $f(x) \in \mathscr{I}_n$ seja $\mathscr{O}(f) = \{[C] \circ f \,|\, [C] \in \mathrm{PGL}(2,q)\}$ a órbita de $f(x)$ e $\mathrm{Stab}(f) = \{[C] \in \mathrm{PGL}(2,q) | [C] \circ f = f\}$ seu estabilizador. Então

$$|\mathscr{O}(f)| \cdot |\mathrm{Stab}(f)| = |(\mathrm{PGL}(2,q))| = q(q^2-1).$$

Pelo teorema anterior, o estabilizador de $f(x)$ é o trivial, pois $|\mathrm{Stab}(f)|$ divide n, logo $|\mathrm{Stab}(f)|$ divide $\mathrm{mdc}(n, q(q^2-1)) = 1$. Portanto $|\mathscr{O}(f)| = q(q^2-1)$.

■

2.3 Polinômios $[A]$-invariantes.

A partir de agora, vamos assumir que

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2,q),$$

é uma matriz que não é escalar da matriz identidade E e, consequentemente, $[A]$ é um elemento não trivial de $\mathrm{PGL}(2,q)$.

Definição 2.14. Seja $[A] \in \mathrm{PGL}(2,q)$ não trivial e $r \geq 0$. Dado um representante $A \in [A]$, onde $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, definimos o polinômio $F_{A,r}(x) \in \mathbb{F}_q[x]$ como

$$F_{A,r}(x) := bx^{q^r+1} - ax^{q^r} + dx - c. \tag{2.3}$$

Note que as raízes de $F_{A,r}(x)$ independem do representante da classe de $[A]$. Assim, para simplificar a notação escreveremos

$$F_r(x) := F_{A,r}(x),$$

onde A é uma matriz fixa que determina a classe de $[A]$. Para $r \geq 1$, o grau de $F_r(x)$ é ou q^r+1 ou q^r, pois os coeficiente a, b não podem ser ambos nulos. Além disso, os fatores irredutíveis de $F_r(x)$ não ocorrem com multiplicidade maior que um, como veremos no próximo lema.

Lema 2.15. *Para todo $r \geq 0$, os polinômios $F_r(x)$ são separáveis, isto é, não possuem fatores irredutíveis múltiplos.*

Demonstração. Suponha que $F_r(x)$ e sua derivada $F_r'(x)$ possuem um zero em comum $\gamma \in \overline{\mathbb{F}}_q$, então

$$F_r'(\gamma) = b\gamma^{q^r} + d = (b\gamma + d)^{q^r} = 0,$$

e usando esta identidade no polinômio $F_r(x)$,

$$F_r(\gamma) = \gamma(b\gamma^{q^r} + d) - (a\gamma^{q^r} + c) = -(a\gamma + c)^{q^r} = 0.$$

Então $a\gamma + c = b\gamma + d = 0$ e com isso temos uma combinação linear não trivial,

$$\gamma(a,b) + (c,d) = (0,0)$$

das entradas da matriz A. Isto é uma contradição, pois A é não singular. ■

A relação entre os polinômios $F_r(x)$ e os polinômios irredutíveis $[A]$- invariantes, é descrita pelo seguinte teorema.

Teorema 2.16. *Seja $f(x) \in \mathbb{F}_q[x]$ um polinômio mônico irredutível de grau $n \geq 2$. As seguintes afirmações são equivalentes:*

(i) *$f(x)$ divide $F_r(x)$ para algum $r \geq 0$.*

(ii) $[A] \circ f = f$.

Demonstração. Seja $\alpha \in \overline{\mathbb{F}}_q$ uma raiz de $f(x)$.

(i) $\Rightarrow$ (ii) : Pela hipótese, temos que $F_r(\alpha) = 0$. Ou seja,

$$\alpha^{q^r}(b\alpha - a) = -d\alpha + c,$$

que é equivalente a $[A] \circ \alpha = \alpha^{q^r}$. Como α^{q^r} é um conjugado de α, pelo Teorema 1.5, α^{q^r} é também uma raiz de $f(x)$ e com isso concluímos que $f([A] \circ \alpha) = 0$. Segue da Proposição 2.8 que $[A] \circ f = f$.

(ii) $\Rightarrow$ (i) : Suponha que $[A]\circ f = f$. Pelo Lema 2.7

$$f([A]\circ\alpha) = ([A]\circ f)([A]\circ\alpha) = 0.$$

Assim $[A]\circ\alpha$ é também uma raiz de $f(x)$ e como as raízes de $f(x)$ são conjugadas, segue do Teorema 1.5 que $[A]\circ\alpha = \alpha^{q^r}$ para algum $r \geq 0$, isto é

$$\frac{d\alpha - c}{-b\alpha + a} = \alpha^{q^r},$$

que é o mesmo que,

$$b\alpha^{q^r+1} - a\alpha^{q^r} + d\alpha - c = 0,$$

logo α também é raiz de $F_r(x)$. Como $f(x)$ é irredutível, $f(x)$ divide F_r. ■

Corolario 2.17. *Para todo* $[A] \in PGL(2,q)$ *existem infinitos polinômios irredutíveis* $[A]$*-invariantes em* $\mathbb{F}_q[x]$.

Demonstração. Do teorema anterior e do Lema 2.15, segue que para cada $r \geq 0$, os fatores irredutíveis de $F_r(x)$ são $[A]$-invariantes e como $F_r(x)$ é separável, temos infinitos destes fatores. ■

Como consequência da prova do Teorema 2.16, mostramos o seguinte fato: para $\alpha \in \overline{\mathbb{F}}_q$,

$$F_r(\alpha) = 0 \Leftrightarrow [A]\circ\alpha = \alpha^{q^r}, \tag{2.4}$$

para algum $r \geq 0$. Indutivamente temos o seguinte resultado.

Lema 2.18. *Assuma que* $f(x)$ *é um polinômio irredutível* $[A]$*-invariante de grau* $n \geq 2$. *Seja* $\alpha \in \overline{\mathbb{F}}_q$ *uma raiz de* $f(x)$ *e assuma que* $[A]\circ\alpha = \alpha^{q^r}$. *Então*

$$[A]^j \circ \alpha = \alpha^{q^{jr}} \quad \textit{para todo } j \geq 0.$$

Demonstração. Mostraremos o resultado por indução em j. No caso $j = 0$, o resultado se tem trivialmente. Podemos assim, assumir que $[A]^j \circ \alpha = \alpha^{q^{jr}}$ para algum $j \geq 0$. Então:

$$\begin{aligned}
[A]^{j+1}\circ\alpha &= [A]\circ([A]^j\circ\alpha) = [A]\circ\alpha^{q^{jr}} \\
&= \frac{d\alpha^{q^{jr}} - c}{-b\alpha^{q^{jr}} + a} = \left(\frac{d\alpha - c}{-b\alpha + a}\right)^{q^{jr}} \\
&= ([A]\circ\alpha)^{q^{jr}} \\
&= (\alpha^{q^r})^{q^{jr}} \\
&= \alpha^{q^{(j+1)r}}.
\end{aligned}$$

■

Uma questão que surge é se dado $f(x)$ polinômio irredutível $[A]$-invariante qual é a relação entre os $r \geq 0$ tais que $F_r(x)$ é divisível por $f(x)$. Veremos no seguinte teorema, que r está relacionado com o grau de $f(x)$ e a ordem da matriz $[A]$.

Teorema 2.19. *Seja $A \in PGL(2,q)$ de ordem D, $f(x)$ um polinômio irredutível $[A]$-invariante de grau $n \geq 2$, e suponha que $f(x)$ divide $F_r(x)$. Então vale as seguintes afirmações:*

(i) Para todo inteiro não negativo t,

$$f(x) \text{ divide } F_t(x) \text{ se, e somente se, } t \equiv r \pmod{n}.$$

Em particular, existe um único $s \in \{0,1,\ldots,n-1\}$ tal que $f(x)$ divide $F_s(x)$.

(ii) Se $n \geq 3$ então D divide n e

$$r = m \cdot \frac{n}{D} \quad \text{para algum inteiro } m \text{ satisfazendo } \operatorname{mdc}(m,D) = 1.$$

Em particular, existe um único $s \in \{0,1,\ldots,n-1\}$ com $f(x)$ divide $F_s(x)$ e tal s tem a seguinte forma

$$s = l \cdot \frac{n}{D} \quad \text{com } 1 \leq l \leq D-1 \text{ e } \operatorname{mdc}(l,D) = 1.$$

Demonstração. Fixamos $\alpha \in \{overline\mathbb{F}_q$ uma raiz de $f(x)$.

(i) Suponha que $f(x)$ divide $F_r(x)$ e $F_t(x)$ e podemos assumir que $t > r$. Por hipótese, temos que $F_r(\alpha) = F_t(\alpha) = 0$, isto é,

$$b\alpha^{q^r+1} - a\alpha^{q^r} + d\alpha - c = b\alpha^{q^t+1} - a\alpha^{q^t} + d\alpha - c,$$

simplicando,

$$\alpha^{q^r}(b\alpha - a) = \alpha^{q^t}(b\alpha - a).$$

Como $\alpha \notin \mathbb{F}_q$, consequentemente

$$\alpha^{q^r} = \alpha^{q^t}, \tag{2.5}$$

que podemos escrever da forma $\alpha^{q^t} = (\alpha^{q^r})^{q^{t-r}}$. Substituindo na equação (2.5), temos

$$\alpha^{q^r} = (\alpha^{q^r})^{q^{t-r}}.$$

Assim segue que $\alpha^{q^r} \in \mathbb{F}_{q^{t-r}}$ e portanto $\alpha \in \mathbb{F}_{q^{t-r}}$. Como $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^n}$, obtemos que $\mathbb{F}_{q^n} \subseteq \mathbb{F}_{q^{t-r}}$ e por consequência n divide $t-r$.

A implicação inversa, segue do mesmo argumento: Se $t \equiv r \pmod{n}$ e $f(x)$ divide $F_r(x)$, temos que $F_r(\alpha) = 0$, isto é , $b\alpha^{q^r+1} - a\alpha^{q^r} + d\alpha - c = 0$. Como $t \equiv r \pmod{n}$, temos que $\alpha^{q^r} = \alpha^{q^t}$ e, usando o fato de que $F_r(\alpha) = 0$, obtemos

$$b\alpha^{q^t+1} - a\alpha^{q^t} + d\alpha - c = 0.$$

Em outras palavras, $F_t(\alpha) = 0$.

(ii) Primeiro vamos assumir que $r = 0$, então $[A] \circ \alpha = \alpha$, ou seja,

$$\frac{d\alpha - c}{-b\alpha + a} = \alpha,$$

que equivale a $b\alpha^2 + (a-d)\alpha + c = 0$, ou seja, uma equação não trivial para α sobre $\mathbb{F}_q$ de grau menor ou igual a dois, o que contradiz a hipótese de que $n \geq 3$. Assumamos que $r \geq 1$. Pelo lema anterior, para todo $j \geq 1$, $[A]^j \circ \alpha = \alpha^{q^{jr}}$. Colocando $j = D$ segue que

$$\alpha^{q^{Dn}} = [A]^D \circ \alpha,$$

consequentemente $\mathbb{F}_q(\alpha) \subseteq \mathbb{F}_{q^{Dr}}$. Como $[\mathbb{F}_q(\alpha) : \mathbb{F}] = n$, isso implica que n divide Dr, assim $Dr = mn$ para m inteiro positivo. Pelo Teorema 2.12, D divide n, então

$$r = m\frac{n}{D}.$$

Assim, falta mostrar que m e D são relativamente primos.

Assuma por contradição, que $e := \text{mdc}(n, D) > 1$. Então $k := \frac{D}{e} < D$. Pelo lema anterior, obtemos

$$[A]^k \circ \alpha = \alpha^{q^{rk}}.$$

Substituindo os valores de r e k na igualdade anterior

$$[A]^k \circ \alpha = \alpha^{q^{m \cdot \frac{n}{D} \cdot \frac{D}{e}}} = \alpha^{q^{n\frac{m}{e}}} = \alpha, \tag{2.6}$$

donde a última igualdade segue pelo fato que n é o grau de $f(x)$ e portanto $\alpha^{q^n} = \alpha$. Como $k < D$, a matriz A^k não é múltipla escalar da matriz identidade E. Se $A^k = \begin{pmatrix} a_k & b_k \\ c_k & d_k \end{pmatrix}$, então a equação (2.6) é equivalente a

$$\frac{d_k\alpha - c_k}{-b_k\alpha + a_k} = \alpha,$$

isto é,

$$b_k\alpha^2 + (d_k - a_k)\alpha - c_k = 0.$$

Obtemos uma equação não trivial de α sobre $\mathbb{F}_q$ de grau menor ou igual a 2, o que contradiz a hipótese de que $n \geq 3$. ■

Exemplo 2.20. *Considere a matriz* $S := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. *Então* $\mathscr{I}_n[S]$ *é o conjunto de todos polinômios mônicos irredutíveis e auto-recíproco sobre* $\mathbb{F}_q$ *de grau* $n \geq 2$. *Como* $\text{ord}[S] = 2$, *pelo Teorema 2.12* $\mathscr{I}_n[S] = \emptyset$ *se* n *é ímpar. Pelo Teorema 2.19, para* $n = 2m$, *todo* $f \in \mathscr{I}_n[S]$ *é um divisor do polinômio* $F_s(x)$ *onde* $s = \frac{n}{2} = m$, *isto é,* $f(x)$ *divide* $(x^{q^m+1} - 1)$.

Reciprocamente, seja $h(x)$ *um fator irredutível do polinômio* $F_t(x) = x^{q^r+1} - 1$ *de grau maior ou igual a* 2. *Então* h *é auto-recíproco,* $\deg h$ *é par, digamos* $deg(h) = 2k$ *e* $h(x)$ *divide* $F_k(x)$. *Pelo Teorema 2.19,* $t \equiv k \pmod{2k}$ *onde* $t = k \cdot j$ *com* $j \equiv 1 \pmod 2$.

Com os resultados obtidos nessa seção podemos mostrar que, em geral, não existem polinômios irredutíveis que são invariantes por todos elementos do grupo $\text{PGL}(2, q)$. De fato, a única exceção ocorre no caso especial em que o corpo finito tem dois elementos.

Proposição 2.21. *Seja* $f(x) \in \mathbb{F}_q[x]$ *um polinômio irredutível de grau* $n \geq 2$. *Suponha que* $[A] \circ f = f$ *para todo* $[A] \in PGL(2, q)$. *Então* $q = 2$ *e* $f(x) = x^2 + x + 1$. *Reciprocamente, o polinômio* $x^2 + x + 1 \in \mathbb{F}_2[x]$ *é irredutível e é invariante sobre todos elementos do grupo linear projetivo.*

Demonstração. Vamos dividir a demonstração em casos.

- Assumamos $q \neq 2$ e $n \geq 3$. Seja $\lambda \in \mathbb{F}_q \setminus \{0, 1\}$ e consideremos as seguintes matrizes

$$A := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{e} \quad B := \begin{pmatrix} 0 & 1 \\ \lambda & 0 \end{pmatrix}.$$

Observemos que $\text{ord}[A] = \text{ord}[B] = 2$, e pelos Teoremas 2.12 e 2.19 obtemos que $n = 2e$ e além disso, $f(x)$ divide os polinômios $x^{q^e+1} - 1$ e $x^{q^e+1} - \lambda$. Porém este polinômios são relativamente primos, uma contradição.

- Seja $q \geq 4$ e assuma que o polinômio $f(x)$ de grau 2 é invariante sobre $\text{PGL}(2, q)$. Considere as matrizes

$$A := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad B := \begin{pmatrix} 0 & 1 \\ \lambda & 0 \end{pmatrix} \quad e \quad C := \begin{pmatrix} 0 & 1 \\ \mu & 0 \end{pmatrix},$$

onde os elementos $1, \lambda, \mu$ são distintos e não nulos. Pelo Teorema 2.19, $f(x)$ é um divisor comum dos polinômios

$$x^{q^r+1} - 1, \quad x^{q^s+1} - \lambda, \quad x^{q^t+1} - \mu,$$

com $r, s, t \in \{0, 1\}$. Com isso, pelo menos dois dos números r, s, t são iguais. Sem perda de generalidade, suponhamos que seja $r = s$, pois os outros casos são análogos. Então $f(x)$ divide $x^{q^r+1} - 1$ e $x^{q^r+1} - \lambda$, que são polinômios relativamente primos, uma contradição.

• Consideremos o caso em que $q = 3$ e $f(x)$ é um polinômio irredutível de grau 2 que é invariante pela matriz

$$A := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Seja α uma raiz de $f(x)$, com isso $\alpha \in \mathbb{F}_{q^2}$ e $\alpha^{q^2} = \alpha$. Pelo Teorema 2.19, $f(x)$ divide o polinômio $x^{q^r+1} - x^{q^r} + x$. Consequentemente

$$\alpha^{q^r+1} - \alpha^{q^r} + \alpha = 0. \tag{2.7}$$

Assim, no caso em que r é par, a partir de (2.7) temos

$$\alpha^2 - \alpha + \alpha = 0,$$

ou seja,

$$\alpha^2 = 0 \Rightarrow \alpha = 0,$$

uma contradição, pois $f(x)$ é irredutível de grau pelo menos 2. Por outro lado, se r é ímpar, pela equação (2.7) , temos

$$\alpha^{q+1} - \alpha^q + \alpha = 0, \tag{2.8}$$

e elevando está equação a potência q, obtemos

$$\alpha^{q^2+q} - \alpha^{q^2} + \alpha^q = 0,$$

isto é,

$$\alpha^{q+1} - \alpha + \alpha^q = 0 \tag{2.9}$$

Somando as equações (2.8) e (2.9)

$$2\alpha^{q+1} = 0 \Rightarrow \alpha = 0,$$

que novamente é uma contradição.

• No caso que $q = 2$ e $f(x) \in \mathbb{F}_2[x]$ é um polinômio irredutível, invariante sobre PGL(2,2) e grau $f = n \geq 3$. Sejam as matrizes

$$A := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{e} \quad B := \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},$$

tais que $f(x)$ é invariantes por cada uma delas. Notemos que ord$[A]$ = ord$[B]$ = 2 e, pelo Teorema 2.12 o grau de $f(x)$ é par, isto é, $n = 2k$. Pelo Teorema 2.19, $f(x)$ divide os polinômios

$$x^{q^k+1}+1 \quad \text{e} \quad x^{q^k+1}+x^{q^k}+1,$$

o que é contraditório, pois estes são relativamente primos. Portanto, só resta o caso em que $q = 2$ e $n = 2$. Existe um único polinômio de grau 2 que é irredutível sobre $\mathbb{F}_2$, especificamente $F(x) = x^2 + x + 1$ e este é invariante sobre todas 6 matrizes do grupo PGL(2,2) (ver exemplo 1.24).

■

2.4 Resultados Assintóticos

Nessa seção vamos considerar a matriz não singular $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ sobre $\mathbb{F}_q$ que não é múltipla escalar da matriz identidade. A ordem da matriz $[A]$ em PGL$(2,q)$ é denotada por D. Consideraremos a fatoração dos polinômios da forma

$$F_r(x) = bx^{q^r+1} - ax^{q^r} + dx - c$$

em polinômios irredutíveis sobre $\mathbb{F}_q[x]$. Pelo Teorema 2.19, os fatores irredutíveis de $F_r(x)$, $r \geq 1$ podem ser das seguintes formas:

(a) fatores irredutíveis de grau Dr,

(b) fatores irredutíveis de grau Dk com $k < r$, $r = km$ e mdc$(m, D) = 1$,

(c) fatores irredutíveis de grau ≤ 2.

Para um inteiro $j \geq 0$ que não é múltiplo de D, denotamos

$$A^j := \begin{pmatrix} a_j & b_j \\ c_j & d_j \end{pmatrix}$$

e

$$F_r^{(j)}(x) := b_j x^{q^r+1} - a_j x^{q^r} + d_j x - c_j.$$

Em particular, $F_r(x) = F_r^{(1)}(x)$. Demonstraremos nessa seção que a maioria dos fatores irredutíveis de $F_r(x)$ tem grau Dr.

Lema 2.22. *Seja $r \geq 1$ e k um divisor de r tal que $m := \frac{r}{k}$ é relativamente primo com D. Então vale as seguintes afirmações:*

(i) Para algum inteiro $j \geq 1$ *com* $\mathrm{mdc}(j,D) = 1$*, os fatores irredutíveis de* $F_r(x)$ *de grau* Dk *são exatamente os fatores irredutíveis de* $F_k^{(j)}(x)$ *de grau* Dk*.*

(ii) O número de fatores irredutíveis de $F_r(x)$ *de grau* Dk *é no máximo* $\frac{q^k+1}{Dk}$*.*

Demonstração. (i) Por hipótese $r = mk$ onde $\mathrm{mdc}(m,D) = 1$. Seja $j \geq 0$ com $jm \equiv 1 \pmod{D}$, então $[A] = [A]^{jm}$. Se $f(x)$ é um fator irredutível de $F_r(x)$ de grau $n = Dk$ e $\alpha \in \overline{\mathbb{F}}_q$ é uma raiz de $f(x)$, então

$$[A] \circ \alpha = \alpha^{q^r}.$$

Com isso, concluímos do Lema 2.18 que

$$[A]^j \circ \alpha = \alpha^{q^{rj}} = \alpha^{q^{mkj}}.$$

Como $jm \equiv 1 \pmod{D}$, segue que $jmk \equiv k \pmod{Dk}$ e $\alpha^{q^{Dk}} = \alpha$. Substituindo na equação anterior obtemos

$$[A]^j \circ \alpha = \alpha^{q^k}.$$

Como $F_r(\alpha) = 0$ se, e somente se, $[A] \circ \alpha = \alpha^{q^r}$, temos que $f(x)$ é um divisor do polinômio $F_k^{(j)}(x)$. Reciprocamente, se $f(x)$ é um fator irredutível de $F_k^{(j)}(x)$ de grau Dk, então

$$[A]^j \circ \alpha = \alpha^{q^k}$$

e do Lema 2.18,

$$[A] \circ \alpha = [A]^{jm} \circ \alpha = ([A]^j)^m \circ \alpha = \alpha^{q^{km}} = \alpha^{q^r},$$

onde a última igualdade segue da hipótese que $km = r$. Consequentemente $f(x)$ divide $F_r(x)$. Com isto fica provado o item (i).

(ii) Como $\deg(F_k^{(j)}) \leq q^k + 1$, o número máximo de fatores irredutíveis de grau Dk de $F_k^{(j)}$ é $\frac{q^k+1}{Dk}$.

■

Com isso, podemos associar o número de fatores irredutíveis de F_r e os de $F_r^{(j)}$, para j inverso multiplicativo de m módulo D. Para estimar assintoticamente o número de polinômios mônicos $f(x)$ em $\mathbb{F}_q[x]$ de grau Dr, tais que $f(x)$ divide $F_r(x)$, isto é, estimar o número

$$\lambda([A], r) := |\{f(x) \in \mathbb{F}_q[x] | f(x) \text{ é irredutível, mônico } \deg(f(x)) = Dr \text{ e } f(x) \text{ divide } F_r(x)\}|,$$

precisamos das seguintes definições.

Definição 2.23. Sejam $f(x), g(x)$ duas funções reais, dizemos que

(i) $f(x) \approx g(x)$ se $\lim_{x\to\infty} \dfrac{f(x)}{g(x)} = 1$.

(ii) $f(x) = O(g(x))$ se existe uma constante $c \in \mathbb{R}$ e $x_0 \in \mathbb{R}$ tal que

$$|f(x)| \leq c|g(x)| \text{ para todo } x \geq x_0.$$

Teorema 2.24. *Seja* $[A] \in PGL(2,q)$ *e* $D = \text{ord}[A] \geq 2$. *Então*

$$\lambda([A],r) = \frac{q^r}{Dr} + O(rq^{\frac{r}{2}+1}).$$

Em particular,

$$\lambda([A],r) \approx \frac{q^r}{Dr}.$$

Em outras palavras, quase todos fatores irredutíveis de $F_r(x)$ *tem grau* Dr*, para valores grandes de* r.

Demonstração. A fatoração de $F_r(x)$ em fatores irredutíveis foi descrito no início desta seção e é composta por

(a) fatores irredutíveis de grau Dr;

(b) fatores irredutíveis de grau Dk com $k < r$, $r = km$ e $\text{mdc}(m, D) = 1$;

(c) fatores irredutíveis de grau ≤ 2.

Se k divide r com $\text{mdc}\left(D, \frac{r}{k}\right) = 1$ e j é tal que $j\frac{r}{k} \equiv 1 \pmod{D}$, pelo Lema 2.22 o número de fatores irredutíveis de grau Dk de $F_r(x)$ e $F_r^{(j)}(x)$ é o mesmo, com isso

$$\deg((F_r(x)) = Dr \cdot \lambda([A],r) + \sum_{\substack{k|r \\ 2<k<r}} Dk \cdot \lambda([A^{j_k}],k) + 2h_2 + h_1, \tag{2.10}$$

onde a soma percorre todos inteiros k que dividem r tais que $\text{mdc}(\frac{r}{k}, D) = 1$ e $k < r$, os expoentes j_k são escolhidos como no Lema 2.22, e h_1, h_2 são o número de fatores irredutíveis de $F_r(x)$ de grau 1 e 2, respectivamente. Pelo item (ii) do Lema 2.22 sabemos que

$$Dk \cdot \lambda([A^j],k) \leq q^k + 1.$$

Logo,

$$\sum_{\substack{k|r \\ 2<k<r}} Dk \cdot \lambda([A^{j_k},k) \leq \sum_{i=1}^{\lfloor r/2 \rfloor} Di \cdot (q^i + 1) \leq \frac{Dr}{2} \sum_{i=1}^{\lfloor r/2 \rfloor} (q^i + 1),$$

assim

$$\sum Dk \cdot \lambda([A^{j_k}, k) \leq \frac{Dr}{2} \cdot \left(\frac{q^{\frac{r+2}{2}} - 1}{q-1} + \frac{r}{2} \right).$$

Temos que

$$\frac{\frac{Dr}{2} \cdot \left(\frac{q^{\frac{r+2}{2}} - 1}{q-1} + \frac{r}{2} \right)}{q^r} = O\left(\frac{r}{q^{r/2+1}} \right).$$

Como os termos h_1 e h_2 são limitados independentemente de r, pela equação (2.10) obtemos

$$\lim_{r \to \infty} \frac{Dr \cdot \lambda([A], r) + O(rq^{\frac{r}{2}+1})}{q^r} = 1,$$

e portanto

$$\lambda([A], r) \approx \frac{q^r}{Dr}$$

■

Também podemos estimar assintoticamente o número de polinômios irredutíveis $[A]$-invariantes. Para isso definimos

$$\mu([A], n) := |\{f(x) \in \mathbb{F}_q[x] | f(x) \text{ é irredutível, mônico e } \deg(f(x)) = n \text{ e } [A] \circ f = f\}|.$$

Se $n \geq 3$ não é divisível por D, pelo Teorema 2.12 $\mu([A], n) = 0$. Para os múltiplos de D, vale o seguinte teorema.

Teorema 2.25. *Seja* $[A] \in PGL(2, q)$ *e* $\text{ord}[A] = D \geq 1$. *Então*

$$\mu([A], Dn) \approx \varphi(D) \cdot \frac{q^n}{Dn},$$

onde φ *é a função Phi de Euler.*

Demonstração. No caso em que $D = 1$, a matriz A é múltipla escalar da matriz identidade. Portanto $[A] \circ f = f$. Pelo Corolário 1.19 temos que $\mu([A], n) \approx \frac{q^n}{n}$. Assim podemos assumir $D \geq 2$. Pelo Teorema 2.19, todo polinômio irredutível $[A]$-invariante de grau Dn é fator exatamente de um dos polinômios $F_{ln}(x)$, com $1 \leq l \leq D-1$ onde $\text{mdc}(l, D) = 1$. Para cada um dos polinômios $F_{ln}(x)$, pelo Lema 2.22, o número de fatores irredutíveis de grau Dn é o mesmo que no caso $l = 1$ e neste caso, o teorema anterior implica que o número de fatores de grau Dn de $F_n(x)$ é assintoticamente $\frac{q^n}{Dn}$. Como existem $\varphi(D)$ escolhas para l, obtemos

$$\mu([A], Dn) \approx \varphi(D) \cdot \frac{q^n}{Dn}.$$

■

CAPÍTULO 3

AÇÃO DO GRUPO SEMI-LINEAR PROJETIVO

A ação definida no capítulo anterior pode ser estendida ao *Grupo Projetivo Semilinear* $\mathrm{P\Gamma L}(2,q^n) = \mathrm{PGL}(2,q^n) \rtimes \mathrm{Gal}(\mathbb{F}_{q^n},\mathbb{F}_q)$, onde aplicamos o automorfismo de Frobenius σ_i ao polinômio para depois aplicarmos a operação $\circ$. Veremos que essa composição define uma ação do grupo $\mathrm{P\Gamma L}(2,q^n)$ sobre os polinômios mônicos irredutíveis sobre $\mathbb{F}_{q^n}$. Como anteriormente, estamos interessados na caracterização e contagem dos pontos fixos.

3.1 Ação do grupo $\mathrm{P\Gamma L}(2,q^n)$

Ao longo deste capítulo, fixamos q uma potência de um número primo e n um inteiro positivo. Seja $\mathscr{M}_k$ o conjunto dos polinômios mônicos irredutíveis de grau k sobre $\mathbb{F}_{q^n}$. Para os polinômios nos conjuntos $\mathscr{M}_k$ definimos a seguinte operação, que é a extensão natural da ação introduzida no capítulo anterior.

Definição 3.1. Seja $[A,\sigma_i] \in \mathrm{P\Gamma L}(2,q^n)$ e $f(x) \in \mathscr{M}_k$. Definimos:

$$([A,\sigma_i] * f)(x)$$

como sendo o único polinômio mônico múltiplo escalar de $[A] \circ \sigma_i(f))(x)$.

O seguinte lema mostra que esta operação define uma ação do grupo $\mathrm{P\Gamma L}(2,q^n)$ sobre $\mathscr{M}_k$.

Lema 3.2. *Seja $A,B \in GL(2,q^n)$, $f(x) \in \mathscr{M}_k$ e E a matriz identidade 2×2. As seguintes afirmações são verdadeiras:*

(i) $[A,\sigma_i] * f \in \mathscr{M}_k$*, ou seja,* $[A,\sigma_i] * f$ *é irredutível e* $\deg([A,\sigma_i] * f) = \deg(f)$*,*

(ii) $[E,\sigma_0] * f = f$*,*

(iii) $([B,\sigma_j] \diamond [A,\sigma_i]) * f = [B,\sigma_j] * ([A,\sigma_i] * f)$*,*

Demonstração. (i) Pelo Teorema 1.12, $\sigma_i(f)$ preserva irredutibilidade e pelo item (v) do Lema 2.2, $[A] \circ \sigma_i(f)$ é irredutível. Portanto $[A,\sigma_i] * f$ é irredutível.

Resta mostrar que $\deg([A,\sigma_i] * f) = \deg(f)$. Isto segue do fato que $a_k^{q^i} \neq 0$ e, portanto, $\deg(\sigma_i(f(x))) = \deg(f(x))$. Consequentemente, pelo Lema 2.2, o resultado segue.

(ii) Como $E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ e $\sigma_0(f) = f$, obtemos que $[E,\sigma_0] * f = [E] \circ f = f$.

(iii) Observemos que $([B,\sigma_j]) * ([A,\sigma_i] * f) = [B,\sigma_j] * ([A] \circ \sigma_i(f)) = [B] \circ \sigma_j([A] \circ \sigma_i(f))$. Segue disso, usando o item (iii) do Lema 2.2, que

$$\begin{aligned} ([B,\sigma_j]) * ([A,\sigma_i] * f) &= [B\sigma_j(A)] \circ \sigma_{i+j}(f) \\ &= [B\sigma_j(A),\sigma_{i+j}] * f = ([B,\sigma_j] \diamond [A,\sigma_i]) * f. \end{aligned}$$

■

Desse lema, concluímos que $[A,\sigma_i] * f$ define uma ação do grupo $\mathrm{P\Gamma L}(2,q^n)$ sobre $\mathscr{M}_k$, para todo $k \geq 2$. Além disso, podemos estender também a operação $[A] \circ \alpha$ definida como na equação (2.2).

Definição 3.3. Seja $\alpha \in \overline{\mathbb{F}}_{q^n} \setminus \mathbb{F}_{q^n}$ e $[A] \in \mathrm{PGL}(2,q^n)$ com $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, definimos:

$$[A,\sigma_i] * \alpha := [A] \circ \sigma_i(\alpha) = \frac{d\alpha^{q^i} - c}{-b\alpha^{q^i} + a}.$$

Verificamos que está operação define uma ação do grupo $\mathrm{PGL}(2,q^n) \rtimes \mathbb{Z}$ sobre o conjunto $\alpha \in \overline{\mathbb{F}}_q \setminus \mathbb{F}_{q^n}$.

Lema 3.4. *Para* $[A],[B] \in \mathrm{PGL}(2,q^n)$ *e* $\alpha \in \overline{\mathbb{F}}_{q^n} \setminus \mathbb{F}_{q^n}$*, temos:*

$$[A,\sigma_i] * ([B,\sigma_j] * \alpha) = [A\sigma_i(B),\sigma_{i+j}] * \alpha.$$

Demonstração. Por definição, segue que

$$\begin{aligned}[A,\sigma_i]*([B,\sigma_j]*\alpha) &= [A,\sigma_i]*([B]\circ\sigma_j(\alpha)) \\ &= [A]\circ(\sigma_i(B)\circ\sigma_{i+j}(\alpha)) \\ &= [A\sigma_i(B)]\circ\sigma_{i+j}(\alpha) \\ &= [A\sigma_i(B),\sigma_{i+j}]*\alpha.\end{aligned}$$

■

Lema 3.5. *Seja* $A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in \mathrm{PGL}(2,q^n)$ *e* $f\in\mathscr{M}_k$, $k\geq 2$. *Então para cada* $\alpha\in\overline{\mathbb{F}}_{q^n}$,

$$f(\alpha)=0 \Leftrightarrow ([A,\sigma_i]*f)([A,\sigma_i]*\alpha)=0.$$

Demonstração. Pelo Lema 2.7 temos que $f(\alpha)=0$ se, e somente se, $\sigma_i(f)(\sigma_i(\alpha))=0$ e isso ocorre se, e somente se, $([A]\circ\sigma_i(f))([A]\circ\sigma_i(\alpha))=0$ (usando o fato que $g(\beta)=0\Leftrightarrow([A]\circ g)([A]\circ\beta)=0$), e isto é equivalente a $([A,\sigma_i]*f)([A,\sigma_i]*\alpha)=0$. ■

Proposição 3.6. *Seja* $[A]\in\mathrm{PGL}(2,q^n), k\geq 2$ *e* $f\in\mathscr{M}_k$. *Se* $\alpha\in\overline{\mathbb{F}}_{q^n}$ *é uma raiz de* $f(x)$, *então* $[A,\sigma_i]*f$ *é o polinômio minimal de* $[A,\sigma_i]*\alpha$ *sobre* $\mathbb{F}_{q^n}$.

Demonstração. Seja $f_\alpha(x)$ o polinômio minimal de $[A,\sigma_i]*\alpha$. Pelo lema anterior, $[A,\sigma_i]*\alpha$ é raiz de $[A,\sigma_i]*f$, logo f_α divide $([A,\sigma_i]*f)$. Pelo item (v) do Lema 3.2, $([A,\sigma_i]*f)$ é irredutível e portanto $f_\alpha=[A,\sigma_i]*f$. ■

Corolario 3.7. *Seja* $[A,\sigma_i]\in P\Gamma L(2,q^n), k\geq 2$ *e* $f\in\mathscr{M}_k$. *Se* $\alpha\in\overline{\mathbb{F}}_{q^n}$ *é uma raiz de* $f(x)$ *então*

$$[A,\sigma_i]*f=f\Leftrightarrow f([A,\sigma_i]*\alpha)=0.$$

Corolario 3.8. *Seja* $\alpha\in\overline{\mathbb{F}}_{q^n}\setminus\mathbb{F}_{q^n}$ *uma raiz do polinômio irredutível* $f(x)\in\mathbb{F}_{q^n}[x]$. *Então:*

$$[A,\sigma_i]*f=f\Leftrightarrow[A,\sigma_i]*\alpha=\alpha^{q^{nr}} \text{ para algum } r\geq 0.$$

Demonstração. As raízes de $f(x)$ e $[A,\sigma_i]*f$ são as mesmas se, e somente se, $[A,\sigma_i]*f=f$. Pela proposição anterior, $[A,\sigma_i]*\alpha$ é raiz de $[A,\sigma_i]*f$, ou seja de $f(x)$. Como as raízes de $f(x)$ são conjugadas, temos que $[A,\sigma_i]*\alpha=\alpha^{q^{nr}}$ para algum $r\geq 0$. Reciprocamente, se $[A,\sigma_i]*\alpha=\alpha^{q^{nr}}$, segue que α e $[A,\sigma_i]*\alpha$ são conjugados sobre $\mathbb{F}_{q^n}$, logo seus polinômios minimais são iguais. Como $f(x)$ é o polinômio minimal de α, também é o polinômio minimal de $[A,\sigma_i]*\alpha$, assim $f(x)$ é irredutível e $f([A,\sigma_i]*\alpha)=0$. Pelo corolário anterior, segue que $[A,\sigma_i]*f=f$. ■

3.2 Uma redução do caso geral

Nessa seção mostraremos que para estudar os polinômios irredutíveis que são invariantes por um elemento de $\mathrm{P\Gamma L}(2,q^n)$ basta considerar, sem perda de generalidade, os elementos da forma $[A,\sigma_1] \in \mathrm{P\Gamma L}(2,q^n)$.

Seja $[A,\sigma_i] \in \mathrm{P\Gamma L}(2,q^n)$ um elemento genérico . Se $t = \mathrm{mdc}(i,n)$, segue que $\mathrm{ord}([A,\sigma_i])$ é divisível por n/t (basta notar que o índice de σ_i precisa ser divisível por n). Definindo $B = A\sigma_i(A)\cdots\sigma_{i(\frac{n}{t}-1)}(A)$, temos que $\mathrm{ord}([A,\sigma_i]) = \mathrm{ord}([B])\cdot\frac{n}{t}$, pois $[A,\sigma_i]^{n/t} = [A\sigma_i(A)\cdots\sigma_{i(\frac{n}{t}-1)}(A),\sigma_{n\frac{i}{t}}] = [B,\sigma_0]$. A partir disso, temos o seguinte lema.

Lema 3.9. *Seja* $[A,\sigma_i] \in P\Gamma L(2,q^n)$*,* $D = \mathrm{ord}[B]$ *e* $t = \mathrm{mdc}(n,i)$*. Então* $\mathrm{ord}[A,\sigma_i] = D\cdot\frac{n}{t}$*.*

Além disso, para $j > 1$ relativamente primo com $\mathrm{ord}([A,\sigma_i])$, temos que $f \in \mathscr{M}_k$, com $k \geq 2$, é $[A,\sigma_i]$-invariante se, e somente se, é $[A,\sigma_i]^j$-invariante. Como i/t e n/t são relativamente primos, existe um inteiro positivo a tal que $a\cdot\frac{i}{t} \equiv 1 \pmod{\frac{n}{t}}$, ou equivalentemente, $ai \equiv t \pmod{n}$. Neste caso a e n/t são relativamente primos e então, pelo Teorema de Dirichlet, existem infinitos primos da forma $n/t\cdot R + a$. Seja P um primo nessa sequência tal que $P > \mathrm{ord}([A,\sigma_i])$. Assim sendo, $f(x) \in \mathscr{M}_k$, com $k \geq 2$, é $[A,\sigma_i]$-invariante se, e somente se, é $[A,\sigma_i]^P$-invariante. Porém, como $P \equiv a \pmod{\frac{n}{t}}$, temos que $[A,\sigma_i]^P = [C,\sigma_t]$ para algum $C \in \mathrm{PGL}(2,q^n)$. Em particular, mostramos o seguinte resultado.

Teorema 3.10. *Para todo* $[A,\sigma_i] \in P\Gamma L(2,q^n)$*, existe um divisor* t *de* n *e um elemento* $[C,\sigma_t] \in P\Gamma L(2,q^n)$ *tal que os* $[A,\sigma_i]$*-invariantes são exatamente os* $[C,\sigma_t]$*-invariantes.*

Observemos se $Q = q^t$ e $\tau = \sigma_t$, onde $\tau : \alpha \to \alpha^Q$ é o gerador de $\mathrm{Gal}(\mathbb{F}_{Q^{n/t}}/\mathbb{F}_Q)$, então $q^n = Q^{n/t}$ e além disso $[A,\sigma_t] = [A,\tau]$. Em outras palavras, não há perda de generalidade em considerarmos somente elementos da forma $[A,\sigma_1]$, pois se necessário, basta mudarmos o corpo base para algum adequado.

Definição 3.11. Para $A \in \mathrm{PGL}(2,q^n)$, definimos

$$A_i^* = A\sigma_1(A)\cdots\sigma_{i-1}(A),$$

$$A^* = A_n^*$$

$$D = \mathrm{ord}([A^*]).$$

Definição 3.12. Para $[A,\sigma_i] \in \mathrm{P\Gamma L}(2,q^n)$ com $A_i^* = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ e um inteiro não negativo m, definimos $F_{A,m}$ como na definição 2.14 e para inteiros não negativos i,m com $m \geq i$, definimos

$$F_{A,m,i}(x) = \sigma_{-i}(F_{A_i^*,m-i}(x)) = b^{q^{n-i}} x^{q^{mr-i}+1} - a^{q^{m-i}} x^{q^{nr-i}} + d^{q^{n-i}} x - c^{q^{n-i}}.$$

Lema 3.13. *Para inteiros não-negativos i,m com $m \geq i$, o polinômio $F_{A,m,i}$ é separável.*

Demonstração. Pelo Lema 2.15 segue que o polinômio $F_{A_i^*,m-i}(x)$ é separável, e portanto $\sigma_{-i}(F_{A_i^*,m-i}(x))$ também é separável e o resultado segue.

■

Lema 3.14. *Seja $[A] \in PGL(2,q^n)$, com $D = \mathrm{ord}([A^*])$ e $f(x) \in \mathscr{M}_k$ tal que $k \geq 2$ e $[A,\sigma_1] * f = f$. Então $[A^*] \circ f = f$. Em particular, se $\deg(f(x)) > 2$, $\deg(f(x))$ é divisível por D.*

Demonstração. Se $[A,\sigma_1] * f = f$ então $[A,\sigma_1]^n * f = f$. Pelo Lema 3.2, temos

$$[A,\sigma_1]^n = [A\sigma_1(A)\ldots\sigma_{n-1}(A),\sigma_n],$$

e com isto

$$[A^*,\sigma_n] * f = f.$$

Como, $\sigma_n(f) = f$, segue que

$$[A^*] \circ f = f,$$

Portanto $f(x)$ é $[A^*]$-invariante. Pelo Lema 2.12 , se $\deg(f(x)) > 2$, então $\deg(f(x))$ é divisível por $D = \mathrm{ord}([A^*])$. ■

Proposição 3.15. *Seja $k \geq 2, f(x) \in \mathscr{M}_k$ e $\alpha \in \overline{\mathbb{F}}_q \setminus \mathbb{F}_{q^n}$ uma raiz de $f(x)$. Para $[A,\sigma_1] \in P\Gamma L(2,q^n)$, as seguintes afirmações são equivalentes:*

(i) $f(x)$ é $[A,\sigma_1]$-invariante;

(ii) $[A,\sigma_1] * \alpha = \alpha^{q^{nr}}$ para algum inteiro não negativo r;

(iii) $f(x)$ divide $F_{A,nr,1}$, para algum inteiro não negativo r .

Demonstração. Pelo Corolário 3.8, temos que os itens (i) e (ii) são equivalentes. Por definição $[A,\sigma_1] * \alpha = \alpha^{q^{nr}}$ se, e somente se, $F_{A,nr,1}(\alpha) = 0$. Como $f(x)$ é irredutível e $f(\alpha) = 0$, segue que $f(x)$ divide $F_{A,nr,1}$ se, e somente se, $F_{A,nr,1}(\alpha) = 0$. Portanto os itens (ii) e (iii) também são equivalentes. Consequentemente, temos a equivalência dos itens (i), (ii) e (iii). ■

Pelo Lema 3.14, para todo polinômio $f(x) \in \mathbb{F}_{q^n}[x]$ que seja $[A,\sigma_1]$-invariante, o $\deg(f)$ é da forma $D \cdot s$, para algum inteiro positivo s. Além disso, s e n estão relacionados, como mostra a seguinte proposição.

Proposição 3.16. *Seja* $[A] \in \mathrm{PGL}(2,q^n)$*,* $k \geq 3$ *e* $f(x) \in \mathscr{M}_k$*. Se* $[A,\sigma_1] * f = f$ *então* $\deg(f) = D \cdot s$*, para algum* $s \geq 1$ *. Além disso, se* $f(x)$ *divide* $F_{A,nr,1}$*, então* s *divide* $rn-1$ *e, em particular,* $\mathrm{mdc}(s,n) = 1$*.*

Demonstração. Pelo Lema 3.14, $\deg(f)$ é divisível por D, isto é, $\deg(f) = Ds$ para algum inteiro $s > 0$. Seja $r \geq 0$ tal que f divide $F_{A,r,1}$ e $\alpha \in \overline{\mathbb{F}}_{q^n} \setminus \mathbb{F}_{q^n}$ uma raiz de $f(x)$. Portanto

$$[A,\sigma_1] * \alpha = \alpha^{q^{nr}}. \tag{3.1}$$

Elevando o elemento $[A,\sigma_1]$ a potência Dn, obtemos

$$[A,\sigma_1]^{Dn} = [A^*,\sigma_n]^D = [E,\sigma_{nD}],$$

que aplicado em α resulta

$$[A,\sigma_1]^{Dn} * \alpha = \alpha^{q^{nD}}.$$

Por um argumento indutivo na equação (3.1), vale

$$[A,\sigma_1]^{Dn} * \alpha = (\alpha^{q^{nr}})^{Dn} = \alpha^{q^{n^2rD}},$$

e comparando as duas equações obtidas, segue que

$$\alpha^{q^{nD}} = \alpha^{q^{n^2rD}}.$$

Como α é raiz de $f(x)$, que tem grau Ds, pelo Teorema 1.5 concluímos que

$$n^2rD \equiv nD \pmod{nDs},$$

ou seja,

$$rn \equiv 1 \pmod{s}.$$

Portanto s divide $rn-1$ e $\mathrm{mdc}(s,n) = 1$. ■

Teorema 3.17. *Seja* $f(x) \in \mathscr{M}_k$ *um polinômio irredutível* $[A,\sigma_1]$*-invariante de grau maior ou igual a* 2*, e suponha que* $f(x)$ *divide* $F_{A,nr,1}$*. Então vale as seguintes afirmações:*

(i) Para algum inteiro $r' \geq 0$*,*

$$f(x) \text{ divide } F_{A,nr',1} \Leftrightarrow r' \equiv r \pmod{k}.$$

Consequentemente, existe um único $v \in \{0,\ldots,k-1\}$ *tal que* $f(x)$ *divide* $F_{A,nv,1}$*.*

(ii) Se $k \geq 3$, então k é da forma $D \cdot s$ onde s é um divisor de $nr-1$ com $\mathrm{mdc}\left(\frac{nr-1}{s}, D\right) = 1$.

Demonstração. Seja α uma raiz de $f(x)$ em $\overline{\mathbb{F}}_{q^n}$ e $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Pelo Lema 3.14, temos que $\deg(f(x)) = Ds$ para algum inteiro $s > 0$.

(i) Suponha que $f(x)$ divide a $F_{A,nr,1}$ e $F_{A,nr',1}$. Podemos assumir que $r' > r$. Como $F_{A,nr,1}(\alpha) = F_{A,nr',1}(\alpha) = 0$, ou seja,

$$b^{q^{n-1}}\alpha^{q^{nr-1}+1} - a^{q^{n-1}}\alpha^{q^{nr-1}} + d^{q^{n-1}}\alpha - c^{q^{n-t1}} = \\ = b^{q^{n-1}}\alpha^{q^{nr'-1}+1} - a^{q^{n-1}}\alpha^{q^{nr'-1}} + d^{q^{n-1}}\alpha - c^{q^{n-1}},$$

o que implica,

$$\alpha^{q^{nr}}(b^{q^{n-1}}\alpha - a^{q^{n-1}}) = \alpha^{q^{nr'}}(b^{q^{n-1}}\alpha - a^{q^{n-1}}).$$

Como $\alpha \notin \mathbb{F}_{q^n}$, segue que $b^{q^{n-1}}\alpha - a^{q^{n-1}} \neq 0$, portanto

$$\alpha^{q^{nr}} = \alpha^{q^{nr'}} = (\alpha^{q^{nr}})^{q^{nr'-nr}}.$$

Assim $\alpha^{q^{nr}} \in \mathbb{F}_{q^{n(r'-r)}}$ e $\alpha \in \mathbb{F}_{q^{n(r'-r)}}$. Como α é raiz de $f(x)$, que é um polinômio irredutível de grau Ds, $\mathbb{F}_{q^n}(\alpha) = \mathbb{F}_{q^{nDs}}$. Dessa forma, concluímos que $\mathbb{F}_{q^{nDs}} \subseteq \mathbb{F}_{q^{n(r'-r)}}$, ou seja, nDs divide $n(r'-r)$, e portanto $r' \equiv r \pmod{Ds}$. Por outro lado, se $r' \equiv r \pmod{Ds}$ e $f(x)$ divide $F_{A,nr,1}$, segue que $F_{A,nr',1}(\alpha) = 0$ e consequentemente $f(x)$ divide $F_{A,nr',1}$.

(ii) Seja $e := \mathrm{mdc}(\frac{nr-1}{k}, D)$. Suponhamos, por contradição, que $e > 1$ e definamos $k := \frac{D}{e} < D$. Como

$$[A, \sigma_1] * \alpha = \alpha^{q^{nr}},$$

aplicando $[A, \sigma_1]$ indutivamente kn vezes,

$$[A, \sigma_1]^{kn} * \alpha = \alpha^{q^{nrkn}},$$

que equivale a

$$[(A^*)^k, \sigma_{nk}] * \alpha = \alpha^{q^{nrkn}}.$$

Se $M := rn - 1$, substituindo na igualdade anterior, temos:

$$[(A^*)^k, \sigma_{nk}] * \alpha = \alpha^{q^{nMk+nk}} = \alpha^{q^{nk}},$$

pois $\deg(f) = Ds$ e s divide M. Assim,

$$[(A^*)^k] \circ \sigma_{nk}(\alpha) = \sigma_{nk}(\alpha).$$

Observemos que, como $k < D$, $[(A^*)^k] \neq [E]$ e denotando por $B = (A^*)^k = \begin{pmatrix} a_k & b_k \\ c_k & d_k \end{pmatrix}$ e $\beta = \sigma_{nk}(\alpha)$, a equação anterior é equivalente a

$$[B]^k \circ \beta = \beta$$

ou seja,

$$\frac{d_k\beta - c_k}{-b_k\beta + a_k} = \beta$$

Com isso, obtemos uma equação não trivial de grau no máximo 2 para β, que pelo item (ii) do Lema 2.19 é uma contradição, pois β é uma conjugado de α.

■

3.3 Sobre o número de $[A, \sigma_1]$-invariantes

Nessa seção estimaremos o número de fatores irredutíveis do polinômio $F_{A,nr,1}$, de acordo com seu grau. Para isso, relacionaremos os fatores do polinômio $F_{A,nr,1}$ com os fatores de um outro polinômio da forma $F_{B,t,u}$.

Teorema 3.18. *Seja r um inteiro positivo e seja s um divisor de $nr-1$ tal que $nr-1 = sm$ com* $\text{mdc}(m, D) = 1$. *Se j é o menor inteiro positivo tal que $jm \equiv 1 \pmod{Dn}$, então vale as seguintes afirmações.*

(i) Para cada divisor $l > 2$ de Ds, os divisores irredutíveis de grau l do polinômio $F_{A,nr,1}$ são exatamentes os divisores irredutíveis de grau l do polinômio $F_{A_j^*, j+s, j}$. Em particular, o número de divisores irredutíveis de grau Ds do polinômio $F_{A,nr,1}$ é no máximo $\frac{q^s+1}{Ds}$.

(ii) Todos os fatores irredutíveis de $F_{A_j^*, j+s, j}$, de grau maior ou igual a 3 tem grau da forma Dt, onde t divide s.

Em particular, se N é o número de divisores irredutíveis de grau Ds do polinômio $F_{A,nr,1}$, então

$$N = \frac{q^s}{Ds} + O(q^{\frac{s}{2}}).$$

Demonstração. (i) Como j é o menor inteiro tal que $jm \equiv 1 \pmod{Dn}$, podemos escrever $jm = Dnk + 1$. Seja l um divisor de Ds e $f(x)$ um fator irredutível de grau l

do polinômio $F_{A,nr,1}$. Se $\alpha \in \overline{\mathbb{F}}_q \setminus \mathbb{F}_{q^n}$ é uma raiz de $f(x)$, segue que $[A,\sigma_1] * \alpha = \alpha^{q^{nr}}$ e $[A,\sigma_1]^j * \alpha = \alpha^{q^{nrj}}$. Usando o fato que $nr - 1 = sm$ e $jm = Dnk + 1$, temos então

$$[A,\sigma_i] * \alpha = [A_j^*,\sigma_j] * \alpha = \alpha^{q^{nrj}} = \alpha^{q^{msj+j}} = \alpha^{q^{s+j+Dnsk}} = \alpha^{q^{s+j}}.$$

A última igualdade é consequência de $\deg(f(x)) = l$ dividir Ds, e assim $\alpha^{q^{Dnsk}} = \alpha$. Em particular, α é raiz de $F_{A_j^*,j+s,j}$ e por consequência tal polinômio é divisível por $f(x)$. Reciprocamente, se $f(x)$ tem grau l e divide $F_{A_j^*,j+s,j}$, podemos concluir que cada raiz α de $f(x)$ satisfaz $[A,\sigma_1]^j * \alpha = \alpha^{q^{s+j}} = \alpha^{q^{nrj}}$ e como l divide Ds temos que $\alpha^{q^{Dsn}} = \alpha$. Então $[A,\sigma_1]^j * \alpha = \alpha^{q^{s+j+Dnsk}} = \alpha^{q^{nrj}}$, onde esta última igualdade vem do fato que $Dnsk = jms - s$ e $jms = nrj - j$. Como $jm \equiv 1 \pmod{Dn}$, temos que $[A,\sigma_1]^{mj-1} = [A^{*D},\sigma_{mj-1}] = [E,\sigma_{nj-1}]$ e, portanto,

$$[A,\sigma_1]^{mj} * \alpha = [A,\sigma_{nj}] * \alpha = \alpha^{q^{nrjm}}.$$

Definamos $\beta = \alpha^{q^{Dnk}} = \alpha^{q^{mj-1}}$. Com isso, a última igualdade é equivalente a

$$[A,\sigma_1] * \beta = \beta^{q^{jm(nr-1)+1}} = \beta^{q^{(sm)(Dnk+1)+1}} = \beta^{q^{mk(nDs)+nr}} = \beta^{q^{nr}},$$

pois como β é conjugado de α sobre $\mathbb{F}_{q^n}$ temos $\beta^{q^{nDs}} = \beta$. Dessa igualdade, concluímos que β é raiz de $F_{A,nr,1}$. Portanto, como α e β são conjugados sobre $\mathbb{F}_{q^n}$, obtemos que $f(x)$ divide $F_{A,nr,1}$.

Para concluir, como o polinômio $F_{A_j^*,j+s,j}$ tem grau no máximo $q^s + 1$, o número de divisores irredutíveis de grau Ds do polinômio $F_{A,nr,1}$ é no máximo $\frac{q^s+1}{Ds}$.

(ii) Seja $f(x)$ um fator irredutível de grau l do polinômio $F_{A_j^*,j+s,j}$, onde $l > 2$, e tomemos $\alpha \in \overline{\mathbb{F}}_q \setminus \mathbb{F}_{q^n}$ uma raiz de $f(x)$. Por definição, $[A_j^*,\sigma_j] * \alpha = \alpha^{q^{s+j}}$, que equivale a

$$[A_j^*,\sigma_{n-s}] * \beta = \beta^{q^n}, \tag{3.2}$$

onde $\alpha = \beta^{q^{n-s-j}}$. Seja g o polinômio minimal de β sobre $\mathbb{F}_{q^n}$. Assim $g = \sigma_{n-s-j}(f)$ e tem grau l. Além disso, como $sm = nr - 1$, $jm = Dnk + 1$ e $\mathrm{mdc}(m,n) = 1$, segue que $s \equiv -j \pmod{n}$, logo $j \equiv n - s \pmod{n}$ e, pela equação (3.2), temos que g é $[A_j^*,\sigma_j]$-invariante. Uma vez que j é relativamente primo com nD (a ordem de $[A,\sigma_1]$), segue que g também é $[A,\sigma_1]$-invariante. Além disso, como $l > 2$, segue das Proposições 3.15 e 3.17 que $l = Dt$ para algum inteiro positivo t. De novo, como $j \equiv n - s \pmod{n}$, temos que $\sigma_{n-s}(A_j^*) = \sigma_j(A_j^*)$ e pela equação (3.2) obtemos que

$$[A_{jnD}^*,\sigma_{nD(n-s)}] * \beta = [A_j^*,\sigma_j]^{nD} * \beta = \beta^{q^{n^2D}}.$$

Contudo, $[A^*_{jnD}] = [(A^*)^{jD}] = [E]$ e com isso a equação anterior implica que $\beta^{q^{nD(n-s)}} = \beta^{q^{n^2D}}$ ou, equivalentemente, $\beta^{q^{nDs}} = \beta$. Em particular, l divide Ds, isto é, t divide s. Portanto, $f(x)$ tem grau da forma Dt, onde t divide s. Isso mostra o item (ii).

Observemos que $F_{A^*_j, j+s, j}$ é separável e tem grau q^s ou q^s+1. Para cada divisor t de s, seja C_t o conjunto dos divisores irredutíveis de grau Dt de $F_{A^*_j, j+s, j}$ e $N = |C_s|$. Se μ denota o número de divisores irredutíves de $F_{A^*_j, j+s, j}$ de grau no máximo dois, o item (ii) mostra que

$$q^s - 2\mu \leq N \cdot Ds + \sum_{\substack{t|s \\ t<s}} |C_t| \cdot Dt \leq q^s + 1. \tag{3.3}$$

Fixemos t um divisor de s e escrevamos $nr - 1 = t(s/t)m$. O item (i) e a Proposição 3.17 implicam que C_t é vazio ou s/t é relativamente primo com D e em ambos os casos, temos que C_t tem no máximo $\frac{q^t+1}{Dt}$ elementos. Em qualquer caso, $Dt \cdot |C_t| \leq q^t + 1$. Assim sendo,

$$\sum_{\substack{t|s \\ t<s}} |C_t| \cdot Dt \leq \sum_{1 \leq i \leq s/2} (q^t + 1) \leq \frac{s(q^{s/2}+1)}{2}.$$

Em particular,

$$q^s - 2\mu \leq N \cdot Ds + \frac{s(q^{s/2}+1)}{2}.$$

Isolando N, obtemos

$$\frac{q^s - 2\mu - s(q^{s/2}+1)/2}{Ds} < N < \frac{q^s}{Ds} + 1,$$

e como o número de polinômios mônicos irredutíveis de grau no máximo dois sobre $\mathbb{F}_{q^n}$ é no máximo q^{2n}, temos a seguinte desigualdade

$$\frac{q^s}{Ds} - e(s) < N < \frac{q^s}{Ds} + 1,$$

onde $e(s) = O(q^{s/2})$. ■

Provaremos que, para qualquer s tal que $\mathrm{mdc}(s,n) = 1$, existem inteiros positivos r para os quais s divide $nr - 1$ com $nr - 1 = sm$ onde $\mathrm{mdc}(m,D) = 1$. De fato, obtemos o número exato de valores de números não congruentes a r modulo Ds com tal propriedade.

Lema 3.19. *Seja s, n, D inteiros positivos tais que* $\mathrm{mdc}(s,n) = 1$. *Então existem $\varphi(D)$ inteiros positivos $r \leq Ds$ tais que s divide $rn - 1$ com* $\mathrm{mdc}\left(\frac{rn-1}{s}, D\right) = 1$.

Demonstração. Seja R o menor inteiro positivo tal que $Rn \equiv 1 \pmod{s}$ e seja $M = \frac{Rn-1}{s}$. Consequentemente, s divide os inteiros $r_i n - 1$, onde $r_i = R + i \cdot s$, com $0 \leq i < D$ e

$\frac{r_i n-1}{s} = M + i$. Observemos que os inteiros r_i estão todos entre 1 e Ds. Além disso, o conjunto $\{M+i\}$ com $0 \leq i < D$ é um conjunto completo de resíduos módulo D. Portanto o número de inteiros r_i tais que $\text{mdc}(M+i, D) = 1$ é $\varphi(D)$. ■

Como consequência do lema anterior e do Teorema 3.18, é possível calcular assintoticamente o número de polinômios invariantes para um elemento em $\text{P}\Gamma\text{L}(2, q^n)$, como é mostrado no seguinte teorema.

Teorema 3.20. *Seja* $[A, \sigma_1] \in P\Gamma L(2, q^n)$*. Então, para qualquer* $k > 2$*, o número* $n_A(k)$ *de* $[A, \sigma_1]$*-invariantes de grau* k *é igual a zero se, e somente se,* k *não é da forma* Ds *com* $\text{mdc}(s, n) = 1$*. Se* $k > 2$ *é da forma* Ds *com* $\text{mdc}(s, n) = 1$*, então*

$$n_A(Ds) \approx \frac{\varphi(D)}{Ds} q^s.$$

Demonstração. Pela Proposição 3.17, no caso em que k não é da forma Ds com $\text{mdc}(s, n) = 1$, não existe invariantes. Por outro lado, se $k > 2$ é da forma Ds, com $\text{mdc}(s, n) = 1$, pelo Teorema 3.18 todo polinômio $[A, \sigma_1]$-invariante de grau Ds é fator de exatamente um dos polinômios $F_{A_j^*, j+s, j}$ com $0 < j < D$ onde $\text{mdc}(j, D) = 1$. Para cada um dos polinômios $F_{A_j^*, j+s, j}$ o número de fatores irredutíveis de grau Ds para cada j primo relativo com D é assintoticamente o mesmo e como temos $\varphi(D)$ possibilidades para j, obtemos que o número de invariantes assintoticamente é $\varphi(D)\frac{q^s}{Ds} + O(q^{s/2})$, ou equivalentemente,

$$n_A(Ds) \approx \frac{\varphi(D)}{Ds} q^s.$$

■

3.4 O subgrupo $\text{PGL}(2, q) \times \text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$

Nessa seção, estudaremos os $[A, \sigma_i]$-invariantes no caso especial em que que $[A] \in \text{PGL}(2, q)$. Em outras palavras, restringimos a ação ao grupo

$$\text{PGL}(2, q) \times \text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \text{ um subgrupo de } \text{P}\Gamma\text{L}(2, q^n).$$

Em particular, consideraremos somente os elementos da forma $[A, \sigma_i]$ com $[A] \in \text{PGL}(2, q)$ e $1 \leq i < n$.

Fixemos $[A] \in \text{PGL}(2, q)$, $d := \text{ord}([A])$ e $d_0 := \text{mdc}(d, n)$. Consequentemente, a ordem de $[A, \sigma_i]$ é igual a nd/d_0. Na notação do Teorema 3.20, temos $[A^*] = [A]^n$ e então

$D = \text{ord}([A^*]) = d/d_0$. Seguindo os mesmos passos da Proposição 3.15 e 3.17, os $[A,\sigma_i]$-invariantes de grau maior que 2 tem grau da forma $\frac{d}{d_0}\cdot s$, onde $\text{mdc}(s,n) = 1$. Pela redução do caso geral podemos supor, sem perda de generalidade, que $\text{mdc}(i,n) = 1$. Como consequência obtemos a seguinte relação entre os $[A,\sigma_j]$-invariantes com $\text{mdc}(j,n) = 1$ e os $[A]$-invariantes.

Teorema 3.21. *Seja $[A] \in PGL(2,q)$ um elemento de ordem d, $d_0 = \text{mdc}(d,n)$ e $f(x)$ um polinômio mônico irredutível em $\mathbb{F}_{q^n}[x]$ de grau $\frac{d}{d_0}\cdot s > 2$. As seguintes afirmações são equivalentes:*

(i) $f(x)$ é $[A,\sigma_i]$-invariante para algum $1 \le i \le n$ tal que $\text{mdc}(i,n) = 1$;

(ii) $f(x)$ é $[A,\sigma_i]$-invariante para algum $1 \le i \le n$ tal que $\text{mdc}(i,n) = 1$ e o menor inteiro positivo t tal que $f(x) \in \mathbb{F}_{q^t}[x]$ é $t = d_0$;

(iii) $f(x)$ divide um polinômio irredutível $G \in \mathbb{F}_q[x]$ de grau ds que é $[A]$-invariante, ou seja, $[A]\circ G = G$.

Demonstração. Para mostrarmos que (i) implica (ii), suponhamos que $f(x)$ é $[A,\sigma_i]$-invariante para algum $1 \le i \le n$ tal que $\text{mdc}(i,n) = 1$ e seja t o menor inteiro positivo tal que $f(x) \in \mathbb{F}_{q^t}[x]$. Como $f(x) \in \mathbb{F}_{q^n}[x]$, temos que t divide n. Em particular $f(x)$ é também $[A,\sigma_i]^t = [A^t,\sigma_{ti}]$-invariante e, como $f(x) \in \mathbb{F}_{q^t}[x]$, segue que $[A]^t \circ f = f$, isto é, $f(x)$ é $[A]^t$-invariante. Pelo Teorema 2.19, $\frac{d}{d_0}\cdot s > 2$ é divisível por $\text{ord}([A]^t) = d/\text{mdc}(t,d)$. Como t divide n e s é relativamente primo com n, necessariamente $\text{mdc}(t,d) = d_0$ e então t é divisível por d_0. Ainda, $f(x)$ é $[A,\sigma_i]^d = [E,\sigma_{id}]$-invariante e então $f(x) \in \mathbb{F}_{q^{id}}[x]$. Como $\text{mdc}(n,id) = d_0$, obtemos que $f(x) \in \mathbb{F}_{q^{d_0}}[x]$ e portanto t divide d_0. Logo, $t = d_0$.

Para mostrarmos que (ii) implica (iii), suponhamos que $f(x)$ é $[A,\sigma_i]$-invariante para algum $1 \le i \le n$ tal que $\text{mdc}(i,n) = 1$ e que o menor inteiro positivo t tal que $f(x) \in \mathbb{F}_{q^t}[x]$ é $t = d_0$. Em particular, $\sigma_{d_0}(f) = f$ e então $f(x)$ é $[A]^{d_0}$-invariante, isto é, $[A]^{d_0} \circ f = f$. Além disso, se $G \in \mathbb{F}_q[x]$ denota o único polinômio mônico irredutível que é divisível por $f(x)$, G é justamente o polinômio minimal (sobre $\mathbb{F}_q$) de alguma raiz de $f(x)$. Pela minimalidade de d_0, necessariamente

$$G(x) = f(x)\cdot \prod_{j=1}^{d_0-1} \sigma_j(f(x)) = f(x)\cdot \prod_{j=1}^{d_0-1} \sigma_{ij}(f(x)), \tag{3.4}$$

onde na última equação usamos o fato que $\sigma_l(f(x)) = \sigma_{l_0}(f(x))$ sempre que $l \equiv l_0 \pmod{d_0}$ e $\text{mdc}(i,d_0) = 1$. Portanto, como $f(x)$ é $[A,\sigma_i]$-invariante, $\sigma_i(f(x)) = [A]^{-1} \circ f$ e indutivamente, $\sigma_{ij}(f(x)) = [A]^{-j} \circ f$ para $j \in \mathbb{N}$. Assim sendo, a equação (3.4) e a igualdade

$[A]^{d_0} \circ f = f$ implicam

$$G(x) = \prod_{j=1}^{d_0} [A]^{-j} \circ f(x) = \prod_{j=1}^{d_0} [A]^{j} \circ f(x).$$

Novamente, como $[A]^{d_0} \circ f = f$, concluímos que $[A] \circ G = G$.

Para verificar que (iii) implica (i), suponhamos que $f(x)$ divide o polinômio mônico irredutível $G \in \mathbb{F}_q[x]$ de grau ds que é $[A]$-invariante. Como $f(x) \in \mathbb{F}_{q^n}[x]$ e $\mathrm{mdc}(n, ds) = d_0$, necessariamente temos que G se decompõe em d_0 polinômios mônicos irredutíveis sobre $\mathbb{F}_{q^{d_0}}$, cada um de grau $\frac{d}{d_0} \cdot s$. Em particular, $f(x) \in \mathbb{F}_{q^{d_0}}[x]$ e a fatoração de G sobre $\mathbb{F}_q$ é dada por

$$G(x) = f(x) \cdot \prod_{j=1}^{d_0-1} \sigma_j(f(x)).$$

Como G é $[A]$-invariante, temos que $[A] \circ f = \sigma_{d_0-j}(f)$ para algum $0 \leq j \leq d_0 - 1$. Afirmamos que $\mathrm{mdc}(j, d_0) = 1$. Seja $k = \mathrm{mdc}(j, d_0)$. Assim sendo, $d_0(d_0 - j)/k$ é divisível por d_0 e da igualdade $[A] \circ f = \sigma_{d_0-j}(f)$ segue que

$$[A]^{d_0/k} \circ f = \sigma_{\frac{d_0(d_0-j)}{k}}(f) = f.$$

Observemos que um elemento da forma $[A]^{d_0/k}$ tem ordem dk/d_0. Consequentemente, pelo Teorema 2.19, dk/d_0 divide o grau de $f(x)$, ou seja, k divide s. Contudo, k divide d_0, e portanto k divide n. Como $\mathrm{mdc}(s, n) = 1$, temos que $k = 1$. Em particular, $f(x)$ é $[A, \sigma_i]$-invariante para algum $i \leq d_0$ tal que $\mathrm{mdc}(i, d_0) = 1$. Uma vez que $f(x) \in \mathbb{F}_{q^{d_0}}[x]$, temos que $f(x)$ é $[A, \sigma_{i+d_0 l}]$-invariante para todo inteiro positivo l. Como $\mathrm{mdc}(i, d_0) = 1$, pelo Teorema de Dirichlet segue a existência de infinitos números primos da forma $i + d_0 l$. Se tomamos um primo P dessa forma, de tal modo que $P > n$ e p_0 é o menor inteiro positivo tal que $P \equiv p_0 \pmod{n}$, temos que $f(x)$ é $[A, \sigma_{p_0}]$-invariante, com $1 \leq p_0 < n$ e $\mathrm{mdc}(p_0, n) = 1$. ■

3.4.1 Polinômios auto-recíprocos conjugados

Em [1], os autores A. Boripan; S. Jitman e P. Udomkavanich, introduziram os chamados *polinômios mônicos irredutíveis auto-recíprocos conjugados* (em inglês *self-reciprocal irreducible monic*, denotados por SCRIM). Estes são os polinômios mônicos irredutíveis em $f \in \mathbb{F}_{q^2}[x]$, distintos de x, tais que seu *recíprocos mônico* $f^*(x) := f(0)^{-1} \cdot x^{\deg(f)} f(1/x)$ coincide com seu *conjugado* $\sigma_1(f)$ sobre $\mathbb{F}_q$, isto é, $f^*(x) = \sigma_1(f)$. Esta é uma variação dos chamados polinômios *mônicos irredutíveis auto-recíprocos* (SRIM) [4], que são os polinômios que satisfazem $f^*(x) = f(x)$. Os autores exploraram a existência e o números dos polinômios SCRIM e alguns de seus resultados são dados como segue.

Teorema 3.22. *O grau de qualquer SCRIM é ímpar. Se n é ímpar e D_n denota o conjuntos dos divisores de q^n+1 que não dividem qualquer q^k+1 com $0 \le k \le n-1$, então o número de polinômios SCRIM de grau n é igual a*

$$\frac{1}{n}\sum_{d\in D_n}\varphi(d).$$

Para mais detalhes, veja os Teoremas 3.3 e 3.15 de [1]. Mais recentemente, os mesmos autores usaram tais polinômios para estudar códigos Hermitianos sobre anéis finitos [2]. Observemos que os recíprocos conjugados podem ser vistos pela ação presente nesse capítulo. De fato, seja $B=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$ e $\mathfrak{g}_0=[B,\sigma_1]\in \mathrm{P\Gamma L}(2,q^2)$, temos que os $\mathfrak{g}_0$-invariantes são exatamente os SCRIM. Note que $[B]$ tem ordem 2. Em particular, obtemos o seguinte resultado.

Corolario 3.23. *Fixe n um inteiro ímpar. Então um polinômio mônico irredutível $f\in \mathbb{F}_{q^2}[x]$ de grau n é um polinômio SCRIM se, e somente se, $f(x)$ divide um polinômio mônico irredutível auto-recíproco $G\in\mathbb{F}_q[x]$ de grau $2n$. Em particular, o números de SCRIM de grau $n>1$ é igual a*

$$\frac{1}{n}\sum_{d|n}\mu(d)q^{n/d}.$$

Demonstração. O fato de que os polinômios SCRIM de grau n sobre $\mathbb{F}_{q^2}$ são exatamente os fatores irredutíveis dos polinômios auto-recíprocos de grau $2n$ sobre $\mathbb{F}_q$ segue diretamente do Teorema 3.21. Assim sendo, se $a(n)$ é o número de SCRIM de grau n e $b(n)$ é o número polinômios irredutíveis mônicos auto-reciproco de grau $2n$ sobre $\mathbb{F}_q$, temos que $a(n)=2\cdot b(n)$. De acordo com o Teorema 3 em [4], para $n>1$ ímpar,

$$b(n)=\frac{1}{2n}\sum_{d|n}\mu(d)q^{n/d},$$

e com isso o resultado segue. ■

Os polinômios recíprocos conjugados podem ser vistos pela ação introduzida nesse capítulo, de fato para $B=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$ e $\mathfrak{g}_0=[B,\sigma_1]\in \mathrm{P\Gamma L}(2,q^2)$, temos que os $\mathfrak{g}_0$-invariantes são exatamente os SCRIM. Note que $[B]$ tem ordem 2. Para $f\in\mathbb{F}_{q^2}$, temos

$$f^*=\sigma_1(f) \iff \sigma_1(f)=[B]\circ f$$

$$\Updownarrow$$

$$[B] \circ \sigma_1(f) = f$$

$$\Updownarrow$$

$$\mathfrak{g}_0 * f = f.$$

Como ord$[B] = 2$, temos que $[B^*] = [E]$ e então $D = 1$. O Teorema 3.20 diz que o número assintótico de $\mathfrak{g}_0$-invariantes de grau s (ímpar) é

$$\frac{q^s}{s} = \frac{q^s}{1 \cdot s} \cdot \varphi(1),$$

que coincide com o resultado do corolário, que diz que o número de SCRIM de grau s é duas vezes $b(n)$ que é dado por $\frac{1}{2n} \sum_{d|n} \mu(d) q^{n/d}$.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] Boripan, A.; Jitman, S.; Udomkavanich, P.
Self-conjugate-reciprocal irreducible monic polynomials over finite fields.
Proceedings of the 20th Annual Meeting in Mathematics 2015. Department of Mathematics, Faculty of Science, Silpakorn University, Nakhom Pathon, 2015, pp. 35–43.

[2] Boripan, A.; Jitman, S.; Udomkavanich,P.
Self-conjugate-reciprocal irreducible monic factors of $x^n - 1$ over finite fields and their applications.
Finite Fields Appl. 55 (2019) 78–96.

[3] Lidl, R.; Niederreiter, H.
Finite Fields.
Encyclopedia of Mathematics and Its Applications, Vol 20, Addison-Wesley 1983.

[4] Meyn, H.; Götz, W.
Self-reciprocal polynomials over finite fields.
Publ. Inst. Rech. Math. Av. 413/S-21 (1990) 82–90.

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