Posto de Carlitz de Polinômios de Permutação

Geovane Matheus Lemes Andrade

IM-UFRJ

2022

Posto de Carlitz de Polinômios de Permutação

por

Geovane Matheus Lemes Andrade

IM-UFRJ

Dissertação de Mestrado apresentada ao Programa de Pós-graduação do Instituto de Matemática, da Universidade Federal do Rio de Janeiro, como parte dos requisitos necessários à obtenção do título de Mestre em Matemática.

Orientadora: Luciane Quoos Conte

Rio de Janeiro

2022

Posto de Carlitz de Polinômios de Permutação

por

Geovane Matheus Lemes Andrade

Dissertação submetida ao Corpo Docente do Instituto de Matemática da Universidade Federal do Rio de Janeiro, como parte dos requisitos necessários para a obtenção do grau de Mestre em Matemática.

Área de concentração: Matemática

Aprovada por:

Profa. Dra. Luciane Quoos Conte - IM-UFRJ
(Orientadora)

Prof. Dr. Fabio Enrique Brochero Martinez - UFMG

Profa. Dra. Maral Mostafazadehfard - IM-UFRJ

Prof. Dr. Ariel Molinuevo - IM-UFRJ

Prof. Dr. Luca Scala - IM-UFRJ

Rio de Janeiro

2022

Resumo

O objetivo deste trabalho é mostrar alguns resultados que nos permitem calcular ou obter cotas para o posto de Carlitz de polinômios de permutação sobre corpos finitos, introduzido em [6]. Utilizamos três abordagens. A primeira consiste em associar cada polinômio de permutação sobre $\mathbb{F}_q$ a um elemento do grupo simétrico S_q , e utilizar a decomposição única em ciclos disjuntos de tal elemento. Por meio desta decomposição, obtemos o posto de Carlitz para algumas famílias de polinômios de permutação. A segunda é uma combinação do Lema de Burnside da Teoria de Grupos com um resultado recente de Z. Ding [26] sobre o posto de Carlitz. Através dela, calculamos o posto de Carlitz de uma família de polinômios de permutação. A terceira consiste em usar ferramentas da teoria de Curvas Algébricas a fim de obter uma relação entre o grau da diferença entre dois polinômios de permutação e o posto de Carlitz de um deles. Mediante esta relação, determinamos o posto de Carlitz de alguns mapas polinomiais completos.

Palavras-chave: posto de Carlitz, polinômios de permutação, ciclos, mapas polinomiais completos.

Abstract

The aim of this work is to show some results that allow us to compute the Carlitz rank of permutation polynomials over finite fields, introduced in [6]. We use three approaches. The first consists of associating each permutation polynomial over $\mathbb{F}_q$ to an element of the symmetric group S_q , and using the unique decomposition into disjoint cycles of such element. Through this decomposition, we obtain the Carlitz rank of some families of permutation polynomials. The second is a combination of the Burnside's Lemma of Group Theory with a recent result by Z. Ding [26] on Carlitz rank. As a consequence of it, we calculate the Carlitz rank of a family of permutation polynomials. The third consists of using tools from the theory of Algebraic Curves in order to obtain a relationship between the degree of difference between two permutation polynomials and the Carlitz rank of one of them. Through this relationship, we determine the Carlitz rank of some complete mapping polynomials.

Keywords: Carlitz rank, permutation polynomials, cycles, complete mapping polynomials.

Agradecimento

Agradeço, primeiramente, a Deus por ter me guiado e ajudado nos momentos difíceis desta caminhada. Quero também agradecer aos meus pais Maucilene e Gilsandro por todo incentivo, amor e apoio que me deram até agora. Aos meus irmãos Thiago e Gabriel, por terem proporcionado momentos de lazer. À minha irmã Mariana, pela grande alegria e paz que traz na minha vida.

Aos professores Fábio e Marcus Vinicius, por terem sempre me ajudado, incentivado e encorajado nesta jornada. Ao professor Montauban, pelas grandes orientações, conselhos e ajudas na graduação. Ao meu padrinho Pe Paulo, pelos maravilhosos ensinamentos. À minha orientadora de mestrado Luciane, por toda a ajuda, dedicação, paciência e pela excelente orientação no mestrado.

Sumário

Introdução	9
1 Conceitos de Teoria de Grupos	14
1.1 Grupo de Permutações	15
1.2 Ações de Grupos	15
2 Corpos	19
2.1 Conceitos Preliminares	19
2.2 Corpos Finitos	20
3 Noções sobre Curvas Algébricas	24
3.1 Polinômios	24
3.2 Curvas Algébricas Planas	29
4 Polinômios de Permutação	34
4.1 Permutações de $\mathbb{F}_q$	34
4.2 Posto de Carlitz	40
5 Ciclos e Posto de Carlitz	42
5.1 Decomposição de $\mathcal{P}_n$	42
5.2 Polos e $\mathcal{P}_n$	57
5.3 O Teorema Principal	61
6 Posto de Carlitz de uma família de polinômios de permutação	66
6.1 O Resultado Principal	66
7 Diferença entre polinômios de permutação	73

7.1	Uma relação entre o posto de Carlitz e o grau da diferença entre polinômios de permutação	73
	Referências	81

Introdução

A teoria de corpos finitos tem se mostrado muito útil nos últimos 50 anos por causa de suas diversas aplicações em combinatória, teoria de códigos, criptografia, entre outros. Veja, por exemplo, o Capítulo 9 de [18]. Suas origens vêm dos séculos XVII e XVIII, com a contribuição dos matemáticos Pierre de Fermat (1601-1665), Leonard Euler (1707-1783), Joseph-Louis Lagrange (1736-1813) e Adrien-Marie Legendre (1752-1833) na teoria de corpos finitos especiais, a saber, os chamados corpos finitos primos. Pode-se dizer que a teoria geral de corpos finitos começa com o trabalho de Carl Friedrich Gauss (1777-1855) e Evariste Galois (1811-1832), mas que apenas tornou-se de interesse para matemáticos aplicados nas últimas décadas com o crescimento e relevância da matemática discreta.

Seja $\mathbb{F}_q$ o corpo finito com q elementos. Uma das áreas da teoria de corpos finitos que vem despertando muito interesse é aquela relacionada a polinômios de permutação, que são polinômios $f(X) \in \mathbb{F}_q[X]$ que induzem uma bijeção de $\mathbb{F}_q$ em $\mathbb{F}_q$. O estudo desses polinômios começou com Hermite, no seu trabalho sobre permutações de sete letras em 1863 (veja [3]). Mais tarde em 1896, usando um resultado de Hermite, Dickson determinou em sua tese de Doutorado todos os polinômios de permutação de $\mathbb{F}_q$ de grau menor do que sete, onde o grau não é um múltiplo da característica de $\mathbb{F}_q$ (veja [14]). Em 2010, Li, Chandler e Xiang classificaram em [10] os polinômios de permutação de grau 6 e 7 sobre $\mathbb{F}_q$ com $q = 2^r$, para todo $r \geq 3$. Os estudos mais recentes sobre a classificação de polinômios de permutação de um dado grau d foram realizados por Fan em [23], [24] e [25], onde se obteve a classificação para $d = 7$ em corpos finitos de característica ímpar, e $d = 8$ para qualquer $\mathbb{F}_q$ com $q > 8$.

Em 1953, Carlitz provou em [13] que todo polinômio de permutação sobre $\mathbb{F}_q$ pode ser representado por uma composição de polinômios da forma X^{q-2} e $aX + b$, com $a, b \in \mathbb{F}_q$ e $a \neq 0$. Assim, para qualquer polinômio de permutação $f(X)$ sobre $\mathbb{F}_q$, existe um polinômio

$$\mathcal{P}_n(X) = \left(\dots \left((a_0X + a_1)^{q-2} + a_2 \right)^{q-2} \dots + a_n \right)^{q-2} + a_{n+1}, \quad (1)$$

onde $a_1, a_{n+1} \in \mathbb{F}_q$ e $a_i \in \mathbb{F}_q^*$ para todo $i \neq 1, n+1$, tal que $f(c) = \mathcal{P}_n(c)$ para todo $c \in \mathbb{F}_q$.

Motivados por este resultado, os autores de [6] introduziram o conceito de posto de Carlitz de um polinômio de permutação $f(X)$, que é o menor inteiro $n \geq 0$ satisfazendo $f(c) = \mathcal{P}_n(c)$ para todo $c \in \mathbb{F}_q$, para um polinômio $\mathcal{P}_n(X)$ da forma (1). Denotamos o posto de Carlitz de $f(X)$ por $Crk(f)$. É natural perguntarmos qual a importância desse conceito nas aplicações. Nos últimos dez anos, foram encontradas algumas interessantes. Em [1], os autores utilizaram o posto de Carlitz para produzir exemplos de classes de polinômios de permutação sobre $\mathbb{F}_p$, com p ímpar, que possuem dispersão alta, uniformidade diferencial baixa, grau alto. Tais propriedades são boas para as aplicações na Criptografia. Além disso, o posto de Carlitz nos permite estudar sequências formadas por iterações de polinômios de permutação. Veja, por exemplo, [4]. Uma aplicação inesperada acerca da distribuição de sequências infinitas de números reais no intervalo $[0, 1)$ foi obtida em [7].

Apesar das inúmeras aplicações, pouco se tem descoberto acerca de métodos para determinar o posto de Carlitz efetivamente. Em contrapartida, tem-se encontrado muitas relações entre ele e conceitos relativos a polinômios. Por exemplo, foi mostrado no Teorema 4 de [6] que se $f(X)$ é um polinômio de permutação sobre $\mathbb{F}_q$ de grau $d > 1$ então

$$d \geq q - Crk(f) - 1.$$

Além disso, foi obtido no Teorema 4 de [4] que se $f(X) \neq a + bX^{q-2}$, com $a, b \in \mathbb{F}_q$ e $b \neq 0$, então

$$Crk(f) > \frac{q}{\omega(f) + 2} - 1,$$

onde $\omega(f)$ denota o número de coeficientes não nulos de $f(X)$. Por este fato, temos uma cota inferior para $\omega(f)$ em termos do posto de Carlitz de $f(X)$, a saber

$$\omega(f) > \frac{q}{Crk(f) + 1} - 2.$$

Uma melhora significativa desta cota no caso em que $Crk(f) = 2$ foi dada em [9], Teorema 3.1, o qual foi provado que

$$\omega(f) \geq q - \frac{q}{p} - \sqrt{\frac{3p}{2} - \frac{39}{16}} - \frac{1}{4},$$

onde p é a característica de $\mathbb{F}_q$. Outro fato interessante é que apesar de ser um problema em aberto encontrar o número de polinômios de permutação de um dado grau, foi obtido em [6] a quantidade de polinômios de permutação sobre $\mathbb{F}_q$ de um dado posto de Carlitz n , sob a condição que $n < (q-1)/2$. Há vários outros resultados envolvendo o posto de Carlitz. Para o leitor interessado, em [15] podem ser encontrados desenvolvimentos recentes dessa área.

Neste trabalho, exploramos algumas abordagens que ajudam a calcular o posto de Carlitz de polinômios de permutação. A primeira delas é usar o fato de que cada polinômio de permutação sobre $\mathbb{F}_q$ pode ser identificado com uma permutação em S_q , o grupo simétrico com q elementos. Obtemos uma maneira simples de calcular o posto de Carlitz de um polinômio de permutação sobre $\mathbb{F}_q$ se é dada sua decomposição em produto de ciclos disjuntos como um elemento de S_q . Basicamente, tal resultado nos diz que se um polinômio de permutação $f(X)$ sobre $\mathbb{F}_q$ é identificado com o produto de ciclos disjuntos $\sigma_1 \cdots \sigma_m$ em S_q de comprimentos $\ell_1, \dots, \ell_m \geq 2$, respectivamente, então

$$Crk(f) = m + \sum_{i=1}^m \ell_i$$

se este valor é menor do que $(q-1)/2$ (caso particular de [6], Teorema 3). Por exemplo, se $f(X) \in \mathbb{F}_{23}[X]$ é um polinômio de permutação tal que $f(x) = (1\ 2)(3\ 5\ 13)(x)$ para cada $x \in \mathbb{F}_{23}$, onde $(1\ 2)$ e $(3\ 5\ 13)$ são ciclos de S_{23} , então $Crk(f) = 2 + 2 + 3 = 7$, uma vez que $7 < 11 = (23-1)/2$.

Na segunda abordagem, usamos algumas ferramentas da Teoria de Grupos, especialmente o Lema de Burnside. Juntamente com um resultado de Z. Ding em [26], conseguimos calcular

o posto de Carlitz de certos polinômios de permutação. Especificamente, provamos que, para cada primo ímpar p e corpo finito $\mathbb{F}_q$, onde $q \equiv 1 \pmod{2p^2}$, os polinômios da forma

$$g(X) = X^{\frac{q(p+2)+p-2}{2p}} - X^{\frac{q+1}{2}} - X^{\frac{q+p-1}{p}} - X \in \mathbb{F}_q[X]$$

são polinômios de permutação sobre $\mathbb{F}_q$ com posto de Carlitz igual a

$$\frac{(p^2 - 1)(q - 1)}{2p^2}$$

(veja Teorema 6.1.2). Vale ressaltar que este resultado foi fruto do esforço do autor desta dissertação inspirado num trabalho dos professores Luciane Quoos e Fabio Brochero.

Na terceira abordagem, recorreremos à teoria de Curvas Algébricas para obter uma relação entre o grau da diferença entre polinômios de permutação e o posto de Carlitz de um deles. Mais precisamente, sejam $f(X)$ e $f(X) + g(X)$ polinômios de permutação sobre $\mathbb{F}_q$, onde $\text{Crk}(f) = n \geq 1$ e o grau k de $g(X)$ satisfaz $1 \leq k < q - 1$. Mostramos, sob uma hipótese sobre $f(X)$, que

$$nk + k(k - 1)\sqrt{q} \geq q - \nu - n,$$

onde $\nu = (k, q - 1)$ é o máximo divisor comum entre k e $q - 1$ (veja [16], Teorema 2.1). Por meio desta relação, determinamos o posto de Carlitz de certos polinômios de permutação.

No Capítulo 1, apresentamos resultados sobre Teoria de Grupos, dando uma atenção especial a Ações de Grupos. No Capítulo 2, relatamos alguns conceitos e fatos sobre corpos e expomos brevemente propriedades de corpos finitos. No Capítulo 3, discutimos sobre Curvas Algébricas, priorizando noções de Curvas Algébricas sobre Corpos Finitos. No Capítulo 4, apresentamos conceitos sobre polinômios de permutação e introduzimos o posto de Carlitz. No Capítulo 5, estudamos a decomposição em ciclos de um polinômio de permutação $f(X)$ sobre $\mathbb{F}_q$ identificado por um elemento de S_q e obtemos um resultado que fornece em certos

casos o posto de Carlitz de $f(X)$ em função desta decomposição. No Capítulo 6, fornecemos uma família de polinômios de permutação e o posto de Carlitz de cada um deles. Por fim, no Capítulo 7, estudamos um resultado que relaciona o grau da diferença entre dois polinômios de permutação e o posto de Carlitz de um deles.

Capítulo 1

Conceitos de Teoria de Grupos

Nosso objetivo neste capítulo é apresentar alguns conceitos e resultados da Teoria de Grupos culminando no Lema de Burnside, o qual será uma ferramenta muito útil para o Capítulo 6. Começamos fixando algumas notações.

Em todo este trabalho, as letras m e n representam números inteiros, p denota um número primo e (m, n) representa o máximo divisor comum entre m e n . Se C é um conjunto, indicamos por $|C|$ a quantidade de elementos de C . Dado G um grupo, denotamos por e o elemento identidade de G . Se G é um grupo e a um elemento de G , escrevemos $\text{ord}(a)$ para denotar a ordem de a . Dados $a_1, \dots, a_n$ elementos de um grupo G , denotamos por $\langle a_1, \dots, a_n \rangle$ o subgrupo de G gerado por $a_1, \dots, a_n$. Dizemos que G é cíclico se $G = \langle a \rangle$ para algum $a \in G$. Enunciamos abaixo algumas propriedades que serão utilizadas nos capítulos posteriores. Para as demonstrações, veja Proposição 3 da Seção 2.3 de [5] e Teorema 1.15 de [18].

Proposição 1.0.1. Seja G um grupo.

- (i) Sejam $\alpha \in G$ e m, n inteiros. Se $\alpha^n = e$ e $\alpha^m = e$ então $\alpha^d = e$, onde $d = (m, n)$. Em particular, se $\alpha^k = e$ para algum $k \in \mathbb{Z}$ então $\text{ord}(\alpha) \mid k$.
- (ii) Se α é um elemento de G de ordem m e k é um inteiro, então a ordem de α^k é m/d , onde $d = (m, k)$. Em particular, $\text{ord}(\alpha^k) \mid m$.
- (iii) Se G é cíclico e finito, então para cada divisor positivo ℓ de $|G|$, existe um único subgrupo de G de ordem ℓ .

1.1 Grupo de Permutações

Dado C um conjunto não vazio, denotamos por S_C o grupo das permutações de C , também chamado grupo simétrico, e id o elemento identidade de S_C . Dizemos que $\alpha \in S_C$ fixa um elemento $x \in C$ se $\alpha(x) = x$, e que α move x se $\alpha(x) \neq x$.

Consideremos um conjunto finito não vazio C . Por simplicidade, escrevemos $C = \{1, 2, \dots, n\}$ e denotamos por S_n o grupo S_C . Se α é um ciclo de S_n , indicamos por $l(\alpha)$ o comprimento de α . Uma transposição é um ciclo de comprimento 2. Para $x \in C$, escrevemos $x \in \text{supp}(\alpha)$ se α move x . Abaixo, listamos alguns resultados relacionados a S_n . As demonstrações podem ser encontradas nas Proposições V.10.5 e V.10.8 de [2].

Proposição 1.1.1.

- (i) Seja $\alpha \in S_n$, $\alpha \neq id$. Então a permutação α pode ser escrita como um produto de ciclos disjuntos de comprimentos maiores do que ou iguais a 2; tal fatoração é única a menos da ordem dos fatores.
- (ii) O grupo S_n é gerado por transposições. Além disso, $S_n = \langle (a1), (a2), \dots, (an) \rangle$, para todo $a \in \{1, \dots, n\}$.

1.2 Ações de Grupos

Nesta seção, nosso intuito é apresentar o Lema de Burnside.

Dados G um grupo, H um subgrupo de G e $t \in G$, uma classe lateral à direita de H em G é $Ht = \{st : s \in H\}$ (uma classe lateral à esquerda é $tH = \{ts : s \in H\}$). O número de classes laterais à direita de H em G é igual ao número de classes laterais à esquerda de H em G (veja Teorema 2.10 de [11]). Denotamos por $[G : H]$ o índice de H em G , isto é, o número de classes laterais à direita de H em G . O Teorema de Lagrange afirma que se G é um grupo finito e H é um subgrupo de G então $[G : H]|H| = |G|$ (veja Teorema 2.11 de [11]).

Definição 1.2.1. Dizemos que um grupo G age num conjunto C se existe uma função $\alpha : G \times C \rightarrow C$ (chamada uma ação), denotada por $\alpha : (g, x) \mapsto gx$, tal que:

- (i) $ex = x$, para todo $x \in C$;
- (ii) $g(hx) = (gh)x$ para todo $g, h \in G$ e $x \in C$.

Se $C = \{1, \dots, n\}$ e G é um subgrupo de S_n , então G age em C , desde que a função $\alpha : G \times C \rightarrow C$ definida por $\alpha : (\sigma, x) \mapsto \sigma(x)$ é uma ação, pois satisfaz $id(x) = x$ para todo $x \in C$ e $\sigma_1(\sigma_2(x)) = (\sigma_1\sigma_2)(x)$ para todo $\sigma_1, \sigma_2 \in G$ e $x \in C$.

Definição 1.2.2. Dados um grupo G agindo num conjunto C e $x \in C$, a órbita de x é

$$\mathcal{O}(x) = \{gx : g \in G\} \subset C.$$

Notemos que C é a união das órbitas de C . Além disso, se $\mathcal{O}(x) \cap \mathcal{O}(y) \neq \emptyset$ então $\mathcal{O}(x) = \mathcal{O}(y)$. De fato, se $gx = hy$, com $g, h \in G$, então $x = g^{-1}hy \in \mathcal{O}(y)$ e $y = h^{-1}gx \in \mathcal{O}(x)$, de modo que $\mathcal{O}(x) = \mathcal{O}(y)$. Assim, podemos escrever C como uma união disjunta das órbitas distintas de C .

Definição 1.2.3. Dados um grupo G agindo num conjunto C e $x \in C$, o estabilizador de x é o subgrupo

$$G_x = \{g \in G : gx = x\} \leq G.$$

Lema 1.2.1. Seja G um grupo agindo num conjunto C . Sejam $x, y \in C$ tais que $y = gx$ para algum $g \in G$. Então $G_y = gG_xg^{-1}$ e $|G_y| = |G_x|$.

Demonstração. Temos

$$h \in gG_xg^{-1} \Leftrightarrow g^{-1}hg \in G_x \Leftrightarrow (g^{-1}hg)x = x$$

$$\Leftrightarrow (hg)x = gx \Leftrightarrow hy = y \Leftrightarrow h \in G_y.$$

Logo, $G_y = gG_xg^{-1}$. Agora, a aplicação $\beta : G_x \rightarrow gG_xg^{-1}$ definida por $\beta(h) = ghg^{-1}$ é uma bijeção. De fato, ela é sobrejetiva pela sua definição. Se $ghg^{-1} = gh'g^{-1}$ então multiplicando pela esquerda ambos os lados desta igualdade por g^{-1} e pela direita por g obtemos $h = h'$. Assim, β é injetiva. Por conseguinte, β é bijetiva, donde

$$|G_x| = |gG_xg^{-1}| = |G_y|.$$

□

Proposição 1.2.1. Se G age num conjunto C e $x \in C$, então

$$|\mathcal{O}(x)| = [G : G_x].$$

Demonstração. Dado $x \in C$, denotemos por G/G_x o conjunto de todas as classes laterais à esquerda de G_x em G . Consideremos a função $f : \mathcal{O}(x) \rightarrow G/G_x$ definida por $f(ax) = aG_x$, para todo $a \in G$. Esta aplicação está bem definida. De fato, se $ax = bx$ então $b^{-1}ax = x$, daí $b^{-1}a \in G_x$ e $a \in bG_x$. Por consequência, $aG_x \subset bG_x$. Como G_x é um grupo, temos $a^{-1}b = (b^{-1}a)^{-1} \in G_x$. Assim, $b \in aG_x$, donde $bG_x \subset aG_x$. Em vista disso, $aG_x = bG_x$ e f está bem definida. Além disso, se $f(cx) = f(dx)$ então $cG_x = dG_x$, de sorte que $d^{-1}c \in G_x$. Logo, $d^{-1}cx = x \Rightarrow cx = dx$. Concluimos então que f é injetiva. Agora, se $a \in G$ então $aG_x = f(ax)$ e, conseqüentemente, f é sobrejetiva. Portanto, f é uma bijeção e $|\mathcal{O}(x)| = |G/G_x| = [G : G_x]$. □

O próximo resultado é conhecido como Lema de Burnside (veja Teorema 3.22 de [11]).

Teorema 1.2.1. (Lema de Burnside) Seja G um grupo finito agindo num conjunto finito C . Se N é o número de órbitas de C , então

$$N = \frac{1}{|G|} \sum_{\tau \in G} \text{Fix}(\tau),$$

onde $Fix(\tau)$ é o número de elementos $x \in C$ fixados por τ .

Demonstração. Notemos que

$$\sum_{\tau \in G} Fix(\tau) = \sum_{\tau \in G} \sum_{\substack{x \in C \\ \tau x = x}} 1 = \sum_{x \in C} \sum_{\tau \in G_x} 1 = \sum_{x \in C} |G_x|.$$

Sejam $\mathcal{O}(x_1), \dots, \mathcal{O}(x_N)$ as órbitas distintas de C . Então $\mathcal{O}(x_i) \cap \mathcal{O}(x_j) = \emptyset$ para $i \neq j$, e $C = \bigcup_{i=1}^N \mathcal{O}(x_i)$. Dessa forma,

$$\sum_{x \in C} |G_x| = \sum_{i=1}^N \sum_{x \in \mathcal{O}(x_i)} |G_x|.$$

Se $x \in \mathcal{O}(x_i)$ então $x = gx_i$ para algum $g \in G$. Pelo Lema 1.2.1, $|G_x| = |G_{x_i}|$. Logo, a última soma acima é igual a

$$\sum_{i=1}^N |\mathcal{O}(x_i)| |G_{x_i}| = \sum_{i=1}^N [G : G_{x_i}] |G_{x_i}| = \sum_{i=1}^N |G| = N|G|,$$

onde na primeira igualdade usamos a Proposição 1.2.1 e, na segunda, o Teorema de Lagrange.

Portanto, $N|G| = \sum_{\tau \in G} Fix(\tau)$. □

Capítulo 2

Corpos

Neste capítulo, expomos alguns conceitos e propriedades relacionados a corpos. Uma atenção especial é dada para corpos finitos.

2.1 Conceitos Preliminares

Esta seção é dedicada à exposição de alguns conceitos gerais sobre corpos e extensões de corpos.

Dado K um corpo com elemento neutro multiplicativo 1 , a característica de K , denotada por $\text{char}(K)$, é o menor inteiro positivo n tal que $n \cdot 1 = 0$. Se não existir tal inteiro, dizemos que K tem característica zero e escrevemos $\text{char}(K) = 0$. Se K é finito então a sua característica é um número primo.

Se L é um corpo e $L \supset K$, dizemos que L é uma extensão de K e escrevemos L/K . Podemos olhar L como um espaço vetorial sobre K , onde os escalares e os vetores são os elementos de K e L , respectivamente. Com isso, se a dimensão de L sobre K é finita, dizemos que a extensão L/K é finita. Um elemento $\alpha \in L$ é dito ser *algébrico* sobre K se existe um polinômio $f(X) \in K[X]$ tal que $f(\alpha) = 0$. Se α não é algébrico, dizemos que α é *transcendente* sobre K . Uma extensão L de K é algébrica se todo elemento de L é algébrico sobre K . Dizemos que K é *algebricamente fechado* se todo polinômio não constante em $K[X]$ possui todas as suas raízes em K . Um corpo L é o *fecho algébrico* de K se L é algebricamente fechado e é uma extensão algébrica de K . Todo corpo admite um fecho algébrico (veja Teorema 3.14 de [17]). Denotamos por $\overline{K}$ o fecho algébrico de K .

Seja X um elemento transcendente sobre K . O corpo de funções racionais em uma

variável sobre K é definido por

$$K(X) = \left\{ \frac{f(X)}{g(X)} : f(X), g(X) \in K[X], g(X) \neq 0 \right\}.$$

Os elementos de $K(X)$ são chamados de funções racionais. O grau de uma função racional $u(X) = f(X)/g(X) \in K(X)$, onde $f(X)$ e $g(X)$ não possuem um fator comum, é $\deg u = \max\{\deg f, \deg g\}$.

2.2 Corpos Finitos

Nesta seção, expomos alguns conceitos e propriedades sobre corpos finitos.

Denotamos por ϕ a função de Euler, isto é,

$$\phi(n) = |\{i : 1 \leq i \leq n \text{ e } (i, n) = 1\}|$$

para todo $n \geq 1$.

Seja K um corpo finito de característica p . Lembremos que o anel $\mathbb{Z}/(p\mathbb{Z})$ de inteiros módulo p é um corpo com p elementos. Denotamos tal conjunto por $\mathbb{F}_p$. Seja 1_p o elemento neutro multiplicativo de $\mathbb{F}_p$. Consideremos a aplicação $\psi : \mathbb{F}_p \rightarrow K$ definida por $\psi(n \cdot 1_p) = n \cdot 1$ para $n \in \mathbb{Z}$. Desse modo, ψ é um homomorfismo não nulo entre corpos, donde é injetiva. Pelo Teorema dos Isomorfismos, temos $\mathbb{F}_p \cong \text{Im}(\psi) \subset K$. Assim sendo, podemos pensar em K como uma extensão de $\mathbb{F}_p$. Visto que K é finito, a dimensão de K sobre $\mathbb{F}_p$ é finita, de forma que existe uma base $\{\alpha_1, \dots, \alpha_n\}$ de K sobre $\mathbb{F}_p$. Cada elemento de K é escrito unicamente como $\alpha_1 a_1 + \dots + \alpha_n a_n$, onde $a_1, \dots, a_n \in \mathbb{F}_p$. Uma vez que há exatamente p possibilidades para cada a_i , segue-se que há p^n elementos da forma $\alpha_1 a_1 + \dots + \alpha_n a_n$, com $a_i \in \mathbb{F}_p$. Portanto, K possui p^n elementos. Por outro lado, dados $n \geq 1$ e p um primo, o

conjunto

$$\mathbb{F}_{p^n} := \{x \in \overline{\mathbb{F}_p} : x^{p^n} = x\}$$

munido das operações de soma e produto de $\overline{\mathbb{F}_p}$ é um corpo com p^n elementos. Além do mais, a menos de isomorfismo, $\mathbb{F}_{p^n}$ é o único corpo com p^n elementos (veja [18], Teorema 2.5).

Aproveitando o fato de $\mathbb{F}_q^*$ ser um grupo multiplicativo, temos as seguintes propriedades, decorrentes da Proposição 1.0.1 para $G = \mathbb{F}_q^*$.

- (A1) Sejam $\alpha \in \mathbb{F}_q^*$ e m, n inteiros. Se $\alpha^m = 1$ e $\alpha^n = 1$ então $\alpha^d = 1$, onde $d = (m, n)$. Em particular, se $\alpha^k = 1$ para algum $k \in \mathbb{Z}$ então $\text{ord}(\alpha) \mid k$.
- (A2) Se α é um elemento de $\mathbb{F}_q^*$ de ordem m e k é um inteiro, então a ordem de α^k é m/d , onde $d = (m, k)$. Em particular, $\text{ord}(\alpha^k) \mid m$.

Corpos finitos são objetos que possuem propriedades intrínsecas muito interessantes, tanto pela sua caracterização quanto pela sua estrutura multiplicativa. O teorema abaixo ilustra este fato. Antes, precisamos do seguinte lema.

Lema 2.2.1. Se n é um inteiro positivo então

$$\sum_{d|n} \phi(d) = n.$$

Demonstração. Consideremos as frações

$$\frac{1}{n}, \frac{2}{n}, \dots, \frac{n}{n}. \tag{2.1}$$

Reduzindo-as em frações irredutíveis, cada uma delas vai ser da forma i/d , onde $d \mid n$, $1 \leq i \leq d$ e $(i, d) = 1$. Assim, para cada divisor positivo d de n , existem $\phi(d)$ frações

irredutíveis da forma i/d em (2.1). Já que há n frações irredutíveis no total, concluímos que

$$\sum_{d|n} \phi(d) = n.$$

□

Teorema 2.2.1. Seja $\mathbb{F}_q$ o corpo finito com q elementos. Então o grupo multiplicativo $\mathbb{F}_q^*$ de elementos não nulos é cíclico.

Demonstração. Para cada divisor positivo d de $q - 1$, seja

$$\mu_d = \{a \in \mathbb{F}_q^* : \text{ord}(a) = d\}.$$

Suponhamos que $\mu_d \neq \emptyset$ para algum $d \mid q - 1$. Vamos provar que $|\mu_d| = \phi(d)$. Dados $a \in \mu_d$ e $1 \leq i \leq d$, temos

$$a^{id} - 1 = (a^d - 1)(a^{d(i-1)} + \dots + 1) = 0.$$

Logo, $1, a, a^2, \dots, a^{d-1}$ são d raízes de $X^d - 1 \in \mathbb{F}_q[X]$ e são distintas pois a ordem de a é d . Dessa forma, $1, a, a^2, \dots, a^{d-1}$ são as raízes de $X^d - 1$. Uma vez que cada elemento de μ_d é uma raiz de $X^d - 1$, concluímos que $\mu_d \subset \{1, a, \dots, a^{d-1}\}$. Por **(A2)**, a ordem de a^i é d se, e somente se, $(i, d) = 1$. Consequentemente, $|\mu_d| = \phi(d)$. Assim, para cada inteiro positivo d que divide $q - 1$, temos

$$|\mu_d| = \begin{cases} 0, & \text{se } \mu_d = \emptyset, \\ \phi(d), & \text{se } \mu_d \neq \emptyset \end{cases}.$$

Por conseguinte, utilizando o Lema 2.2.1, temos

$$q - 1 = |\mathbb{F}_q^*| = \left| \bigcup_{d|q-1} \mu_d \right| = \sum_{d|q-1} |\mu_d| \leq \sum_{d|q-1} \phi(d) = q - 1$$

$$\Rightarrow \sum_{d|q-1} |\mu_d| = \sum_{d|q-1} \phi(d) \Rightarrow |\mu_d| = \phi(d)$$

para todo divisor positivo d de $q - 1$. Em particular, $|\mu_{q-1}| = \phi(q - 1) \geq 1$, de sorte que existe um elemento em $\mathbb{F}_q^*$ de ordem $q - 1$. Portanto, $\mathbb{F}_q^*$ é cíclico. $\square$

Diante disso, utilizando a Proposição 1.0.1(iii) para $G = \mathbb{F}_q^*$, obtemos a seguinte propriedade.

(A3) Para cada divisor positivo ℓ de $q - 1$, existe um único subgrupo de $\mathbb{F}_q^*$ de ordem ℓ .

Além disso, temos o seguinte fato.

Proposição 2.2.1. O número de soluções em $\mathbb{F}_q^*$ da equação $X^k = 1$ é d , onde $d = (k, q - 1)$.

Demonstração. Seja $\alpha \in \mathbb{F}_q^*$ tal que $\alpha^k = 1$. Como $\mathbb{F}_q^*$ é um grupo com $q - 1$ elementos, temos $\alpha^{q-1} = 1$. Por **(A1)**, $\alpha^d = 1$, onde $d = (q - 1, k)$. Consequentemente, α pertence ao subgrupo G de $\mathbb{F}_q^*$ de ordem d . Além disso, todo elemento de G satisfaz a equação $X^k = 1$. Logo, as raízes de $X^k - 1$ são os elementos de G . Portanto, há exatamente d soluções em $\mathbb{F}_q^*$ para a equação $X^k = 1$. $\square$

Capítulo 3

Noções sobre Curvas Algébricas

Neste capítulo, apresentamos alguns conceitos e resultados sobre Curvas Algébricas que serão utilizados nos próximos capítulos, especialmente no Capítulo 7. Mostramos exemplos e demonstramos alguns fatos a fim de que o leitor, caso não familiarizado com a teoria, possa se habituar com o conteúdo. Além disso, um dos nossos principais objetivos é enunciar um caso particular da cota de Hasse-Weil, pois será útil para os resultados do Capítulo 7.

3.1 Polinômios

Seja K um corpo. Denotamos por $K[X, Y, Z]$ o anel de polinômios em 3 variáveis sobre K . Cada polinômio não nulo $f(X, Y, Z) \in K[X, Y, Z]$ é expresso unicamente como

$$f(X, Y, Z) = \sum_{i=0}^n a_i X^{u_i} Y^{v_i} Z^{w_i}, \quad (3.1)$$

onde $a_i \in K \setminus \{0\}$, u_i, v_i, w_i são inteiros não negativos e $(u_i, v_i, w_i) \neq (u_j, v_j, w_j)$ para todo $i \neq j$. O grau de um polinômio $f(X, Y, Z)$ expresso como em (3.1) é definido por

$$\deg f = \max\{u_i + v_i + w_i : i = 0, \dots, n\}.$$

Sejam $f(X, Y, Z), g(X, Y, Z) \in K[X, Y, Z]$, com $g(X, Y, Z) \neq 0$. Dizemos que $g(X, Y, Z)$ divide $f(X, Y, Z)$, denotado por $g(X, Y, Z) \mid f(X, Y, Z)$, se existe $h(X, Y, Z) \in K[X, Y, Z]$ tal que $f(X, Y, Z) = g(X, Y, Z)h(X, Y, Z)$. Um polinômio não constante $f(X, Y, Z) \in K[X, Y, Z]$ é dito ser irredutível sobre K se não existe um polinômio $g(X, Y, Z) \in K[X, Y, Z]$, com $1 \leq \deg g < \deg f$, tal que $g(X, Y, Z) \mid f(X, Y, Z)$.

Dizemos que um polinômio $f(X, Y, Z) \in K[X, Y, Z]$ é homogêneo de grau d se todos os monômios que aparecem com coeficientes não nulos tem grau d . Por exemplo, $X^3 + Y^3 + Z^3 - XYZ$ é um polinômio homogêneo de grau 3. Um produto de polinômios homogêneos é um polinômio homogêneo. Além disso, temos o seguinte fato.

(B) Todo fator de um polinômio homogêneo não nulo é homogêneo.

Para ver isso, sejam $f(X, Y, Z)$ um polinômio homogêneo de grau d , $f(X, Y, Z) \neq 0$, e $u(X, Y, Z), v(X, Y, Z) \in K[X, Y, Z]$ tais que

$$f(X, Y, Z) = u(X, Y, Z)v(X, Y, Z). \quad (3.2)$$

Consideremos ℓ_{max} e ℓ_{min} o maior e o menor grau dos termos de $u(X, Y, Z)$, respectivamente. Analogamente, sejam c_{max} e c_{min} o maior e o menor grau dos termos de $v(X, Y, Z)$. Já que $K[X, Y, Z]$ é um domínio, os monômios de mais alto grau que figuram no polinômio $u(X, Y, Z)v(X, Y, Z)$ possuem grau $\ell_{max} + c_{max}$, enquanto aqueles de menor grau tem grau $\ell_{min} + c_{min}$. Dado que $f(X, Y, Z)$ é homogêneo de grau d , concluimos por (3.2) que $d = \ell_{max} + c_{max} = \ell_{min} + c_{min}$, de sorte que

$$(\ell_{max} - \ell_{min}) + (c_{max} - c_{min}) = 0.$$

Uma vez que os números entre os parênteses são inteiros não negativos, obtemos $\ell_{max} = \ell_{min}$ e $c_{max} = c_{min}$. Portanto, $u(X, Y, Z)$ e $v(X, Y, Z)$ são homogêneos.

Proposição 3.1.1. Seja $g(X, Y) \in K[X, Y]$ não nulo de grau d . Então o polinômio $g^*(X, Y, Z) \in K[X, Y, Z]$ definido por

$$g^*(X, Y, Z) = Z^d g\left(\frac{X}{Z}, \frac{Y}{Z}\right)$$

é homogêneo de grau d .

Demonstração. Escreva

$$g(X, Y) = \sum_{i=0}^n a_i X^{u_i} Y^{v_i},$$

com $a_i \in K \setminus \{0\}$ e $(u_i, v_i) \neq (u_j, v_j)$ para todo $i \neq j$. Desde que $\deg g = d$, temos $d \geq u_i + v_i$ para qualquer $i = 0, \dots, n$. Desse modo,

$$g^*(X, Y, Z) = Z^d g\left(\frac{X}{Z}, \frac{Y}{Z}\right) = \sum_{i=0}^n a_i X^{u_i} Y^{v_i} Z^{d-u_i-v_i}.$$

Dado que $u_i + v_i + d - u_i - v_i = d$ para todo $i = 1, \dots, n$, segue-se que $g^*(X, Y, Z)$ é homogêneo de grau d . □

Notemos que $g^*(X, Y, 1) = g(X, Y)$. Além disso, se $g(X, Y) \neq 0$ então $g^*(X, Y, Z)$ não é divisível por Z . Caso contrário, pela Proposição 3.1.1, o polinômio

$$h(X, Y, Z) = \frac{1}{Z} g^*(X, Y, Z)$$

tem grau $d - 1$ e satisfaz $h(X, Y, 1) = g^*(X, Y, 1) = g(X, Y)$, donde $g(X, Y)$ tem grau no máximo $d - 1$, uma contradição.

Vale observar também que nem todo polinômio homogêneo $f(X, Y, Z) \in K[X, Y, Z]$ cumpre $f(X, Y, Z) = g^*(X, Y, Z)$ para algum $g(X, Y) \in K[X, Y]$. Por exemplo, não podemos ter

$$g^*(X, Y, Z) = XZ^2 + Y^2Z + Z^3 \in K[X, Y, Z]$$

para algum polinômio $g(X, Y) \in K[X, Y]$. Caso contrário,

$$g(X, Y) = g^*(X, Y, 1) = X + Y^2 + 1 \Rightarrow g^*(X, Y, Z) = XZ + Y^2 + Z^2,$$

o que é uma contradição. No entanto, se $f(X, Y, Z) \neq 0$ e Z^r é a maior potência de Z que

divide $f(X, Y, Z)$ então

$$Z^r g^*(X, Y, Z) = f(X, Y, Z),$$

onde $g(X, Y) = f(X, Y, 1)$. Com efeito, se

$$f(X, Y, Z) = \sum_{i=0}^n a_i X^{u_i} Y^{v_i} Z^{w_i}$$

como em (3.1), e $u_i + v_i + w_i = d$ para todo $i = 0, \dots, n$, então o polinômio homogêneo

$$\frac{1}{Z^r} f(X, Y, Z)$$

tem grau $d - r$ e não é divisível por Z . Logo, o polinômio $g(X, Y) = f(X, Y, 1)$ tem grau $d - r$. Assim,

$$\begin{aligned} Z^r g^*(X, Y, Z) &= Z^r Z^{d-r} g\left(\frac{X}{Z}, \frac{Y}{Z}\right) = \sum_{i=0}^n a_i X^{u_i} Y^{v_i} Z^{d-u_i-v_i} \\ &= \sum_{i=0}^n a_i X^{u_i} Y^{v_i} Z^{w_i} = f(X, Y, Z). \end{aligned}$$

Proposição 3.1.2. Sejam $f(X, Y), g(X, Y) \in K[X, Y]$, com $g(X, Y) \neq 0$. Então $g(X, Y) \mid f(X, Y)$ se, e somente se, $g^*(X, Y, Z) \mid f^*(X, Y, Z)$.

Demonstração. Suponhamos que $g(X, Y) \mid f(X, Y)$. Seja $h(X, Y) \in K[X, Y]$ tal que $f(X, Y) = g(X, Y)h(X, Y)$. Consideremos $d = \deg f, a = \deg g, b = \deg h$. Então $d = a + b$.

Dessa maneira,

$$Z^d f\left(\frac{X}{Z}, \frac{Y}{Z}\right) = Z^a g\left(\frac{X}{Z}, \frac{Y}{Z}\right) Z^b h\left(\frac{X}{Z}, \frac{Y}{Z}\right).$$

Portanto, $g^*(X, Y, Z) \mid f^*(X, Y, Z)$. Por outro lado, se $g^*(X, Y, Z) \mid f^*(X, Y, Z)$, existe

$t(X, Y, Z) \in K[X, Y, Z]$ tal que $f^*(X, Y, Z) = g^*(X, Y, Z)t(X, Y, Z)$. Assim,

$$f(X, Y) = f^*(X, Y, 1) = g^*(X, Y, 1)t(X, Y, 1) = g(X, Y)t(X, Y, 1),$$

de modo que $g(X, Y) \mid f(X, Y)$. □

Definição 3.1.1. Um polinômio $f(X, Y, Z) \in K[X, Y, Z]$ é absolutamente irredutível sobre K se ele é irredutível sobre qualquer extensão algébrica de K , isto é, se ele é irredutível em $\overline{K}[X, Y, Z]$.

Exemplo 3.1.1. Seja $g(X, Y) = X^2 - Y \in K[X, Y]$. Afirmamos que $g(X, Y)$ é absolutamente irredutível sobre K . Caso contrário, ele é o produto de dois polinômios de grau 1 em $L[X, Y]$ para alguma extensão algébrica L de K . Assim,

$$X^2 - Y = (aX + bY + c)(a_1X + b_1Y + c_1),$$

onde $a, b, c, a_1, b_1, c_1 \in L$. Comparando os coeficientes de X^2, XY, Y e Y^2 em ambos os lados desta igualdade, obtemos

$$aa_1 = 1, ab_1 + ba_1 = 0, cb_1 + c_1b = -1 \text{ e } bb_1 = 0.$$

Desse modo, a e a_1 são diferentes de zero e

$$b(ab_1 + ba_1) = 0 \Rightarrow 0 = abb_1 + b^2a_1 = b^2a_1 \Rightarrow b = 0,$$

pois $a_1 \neq 0$. Dessa maneira, temos

$$0 = a(ab_1 + ba_1) = a^2b_1 \Rightarrow b_1 = 0,$$

pois $a \neq 0$. Portanto, $b = b_1 = 0$ e $cb_1 + c_1b = 0$, contradizendo a igualdade $cb_1 + c_1b = -1$. Desse modo, $g(X, Y)$ é absolutamente irredutível sobre K .

3.2 Curvas Algébricas Planas

Dado K um corpo, seja $K^n = \{(x_1, x_2, \dots, x_n) : x_1, \dots, x_n \in K\}$. Consideremos a relação de equivalência $\sim$ em $K^n \setminus \{(0, \dots, 0)\}$ definida por:

$$(x_1, \dots, x_n) \sim (y_1, \dots, y_n) \Leftrightarrow \exists \lambda \in K \setminus \{0\} \text{ tal que } (x_1, \dots, x_n) = (\lambda y_1, \dots, \lambda y_n).$$

Denotamos por $[x_1 : \dots : x_n]$ a classe de equivalência de $(x_1, \dots, x_n) \in K^n \setminus \{(0, \dots, 0)\}$, ou seja,

$$[x_1 : \dots : x_n] = \{(y_1, \dots, y_n) \in K^n \setminus \{(0, \dots, 0)\} : (y_1, \dots, y_n) \sim (x_1, \dots, x_n)\}.$$

Definição 3.2.1. O espaço projetivo de dimensão n sobre um corpo K , denotado por $\mathbb{P}^n(K)$, é o conjunto das classes de equivalência de $K^n \setminus \{(0, \dots, 0)\}$ com respeito à relação $\sim$, isto é,

$$\mathbb{P}^n(K) = \{[x_1 : \dots : x_n] : (x_1, \dots, x_n) \in K^n \setminus \{(0, \dots, 0)\}\}.$$

Os elementos de $\mathbb{P}^n(K)$ são chamados de pontos. Dado um ponto $P = [x_1 : \dots : x_n] \in \mathbb{P}^n(K)$, dizemos que $x_1, \dots, x_n$ são coordenadas homogêneas para P . Chamamos $\mathbb{P}^1(K)$ de reta projetiva e $\mathbb{P}^2(K)$ de plano projetivo.

A reta projetiva $\mathbb{P}^1(K)$ pode ser identificada com K adicionado de um ponto fora de K . Com efeito, observemos que

$$\mathbb{P}^1(K) = \{[1 : x] : x \in K\} \cup \{[0 : 1]\}.$$

O ponto $[0 : 1]$ é chamado de ponto no infinito. Consideremos a aplicação

$$\tau : K \rightarrow \mathbb{P}^1(K) \setminus \{[0 : 1]\}$$

definida por $\tau(x) = [1 : x]$ para todo $x \in K$. Mostremos que τ é uma bijeção. Se $[1 : x] = [1 : y]$ então existe $\lambda \in K \setminus \{0\}$ tal que $1 = \lambda 1$ e $x = \lambda y$, donde $\lambda = 1$ e $x = y$. Por consequência, τ é injetiva. Se $z \in \mathbb{P}^1(K) \setminus \{[0 : 1]\}$ então $z = [1 : x]$ para algum $x \in K$, daí $z = \tau(x)$. Logo, τ é sobrejetiva e, consequentemente, é uma bijeção. Portanto, dado $x \in K$, podemos identificá-lo com o elemento $[1 : x]$ em $\mathbb{P}^1(K)$. Dessa forma, podemos enxergar $\mathbb{P}^1(K)$ como o conjunto K adicionado de um ponto fora de K correspondente ao ponto $[0 : 1]$. O ponto fora de K é denotado por ∞ . Assim, identificamos o conjunto $\mathbb{P}^1(K)$ com $K \cup \{\infty\}$.

Seja $f(X, Y, Z) \in K[X, Y, Z]$ um polinômio homogêneo de grau d expresso como em (3.1). Então $u_i + v_i + w_i = d$ para todo $i = 0, \dots, n$. Dado $t \in K \setminus \{0\}$, temos

$$f(tX, tY, tZ) = \sum_{i=0}^n t^{u_i+v_i+w_i} a_i X^{u_i} Y^{v_i} Z^{w_i} = \sum_{i=0}^n t^d a_i X^{u_i} Y^{v_i} Z^{w_i} = t^d f(X, Y, Z).$$

Portanto, se $(x, y, z) \in K^3$ então

$$f(x, y, z) = 0 \Leftrightarrow f(\lambda x, \lambda y, \lambda z) = 0, \forall \lambda \in K \setminus \{0\}.$$

Diante disso, dado $P = [x : y : z] \in \mathbb{P}^2(K)$, a veracidade da igualdade $f(x, y, z) = 0$ não depende da escolha de coordenadas homogêneas para P . Motivados por esta propriedade, dizemos que $P = [x : y : z] \in \mathbb{P}^2(K)$ é um zero de $f(X, Y, Z)$ se $f(x, y, z) = 0$. Neste caso, escrevemos $f(P) = 0$.

Definição 3.2.2. Uma curva algébrica plana $\mathcal{X}$ é o conjunto de zeros em $\mathbb{P}^2(\overline{K})$ de um

polinômio homogêneo não constante $f(X, Y, Z) \in K[X, Y, Z]$, isto é,

$$\mathcal{X} = \{P \in \mathbb{P}^2(\overline{K}) : f(P) = 0\}.$$

Dizemos que $\mathcal{X}$ está definida sobre K e que $f(X, Y, Z) = 0$ é a equação homogênea de $\mathcal{X}$. O grau da curva $\mathcal{X}$ é definido por $\deg \mathcal{X} = \deg f$. Um ponto afim de $\mathcal{X}$ é um ponto da curva $\mathcal{X}$ da forma $[x : y : 1]$. Um ponto no infinito de $\mathcal{X}$ é um ponto de $\mathcal{X}$ da forma $[x : y : 0]$. Se $f(X, Y, Z)$ é absolutamente irredutível sobre K , dizemos que a curva $\mathcal{X}$ é absolutamente irredutível.

Observemos que se a curva $\mathcal{X}$ é definida pela equação homogênea $g^*(X, Y, Z) = 0$ para algum polinômio não constante $g(X, Y) \in K[X, Y]$ absolutamente irredutível sobre K , então $\mathcal{X}$ é absolutamente irredutível. Com efeito, suponhamos, por absurdo, que existam polinômios $u(X, Y, Z), v(X, Y, Z) \in \overline{K}[X, Y, Z]$, onde $1 \leq \deg u, \deg v < \deg g$, tais que

$$g^*(X, Y, Z) = u(X, Y, Z)v(X, Y, Z).$$

Por **(B)**, $u(X, Y, Z)$ é homogêneo. Já que $g^*(X, Y, Z)$ não é divisível por Z , o mesmo vale para $u(X, Y, Z)$. Consequentemente, o polinômio $h(X, Y) = u(X, Y, 1)$ tem grau $\deg u$ e divide $g^*(X, Y, 1) = g(X, Y)$, o que não pode acontecer pois $g(X, Y)$ é irredutível em $\overline{K}[X, Y]$.

Notemos também que, na definição acima, a curva $\mathcal{X}$ consiste exatamente dos pontos afins e no infinito de $\mathcal{X}$, isto é,

$$\mathcal{X} = \{[x : y : 1] \in \mathbb{P}^2(\overline{K}) : f(x, y, 1) = 0\} \cup \{[x : y : 0] \in \mathbb{P}^2(\overline{K}) : f(x, y, 0) = 0\}.$$

Exemplo 3.2.1. Consideremos o corpo finito $\mathbb{F}_q$ de $q > 3$ elementos. Sejam

$$g(X, Y) = X^{q-2} - Y \in \mathbb{F}_q[X, Y]$$

e $\mathcal{X}$ a curva algébrica plana definida pela equação homogênea $g^*(X, Y, Z) = 0$. Como

$$g^*(X, Y, Z) = X^{q-2} - YZ^{q-3},$$

os pontos afins de $\mathcal{X}$ são os pontos $[x : y : 1] \in \mathbb{P}^2(\overline{\mathbb{F}}_q)$ tais que $y = x^{q-2}$. Desse modo, o conjunto dos pontos afins de $\mathcal{X}$ é

$$\{[x : x^{q-2} : 1] : x \in \overline{\mathbb{F}}_q\}.$$

Por outro lado, dado $[x : y : 0] \in \mathbb{P}^2(\overline{\mathbb{F}}_q)$, temos

$$g^*(x, y, 0) = 0 \Leftrightarrow x^{q-2} = 0 \Leftrightarrow x = 0.$$

Logo, $[0 : 1 : 0]$ é o único ponto no infinito de $\mathcal{X}$. Portanto, a curva $\mathcal{X}$ é o conjunto $\{[0 : 1 : 0], [x : x^{q-2} : 1] : x \in \overline{\mathbb{F}}_q\}$.

Definição 3.2.3. Sejam $\mathcal{X}$ e $\mathcal{X}'$ curvas algébricas planas definidas pelas equações homogêneas $f(X, Y, Z) = 0$ e $f'(X, Y, Z) = 0$, respectivamente. Dizemos que $\mathcal{X}'$ é uma componente de $\mathcal{X}$ se $f'(X, Y, Z)$ divide $f(X, Y, Z)$.

O próximo resultado é conhecido como Teorema de Bézout, cuja prova pode ser encontrada na Seção 3.2 de [12].

Teorema 3.2.1. (Teorema de Bézout) Se as curvas algébricas planas $\mathcal{X}$ e $\mathcal{X}'$ tem graus m e n , e não possuem componentes em comum, então elas têm no máximo mn pontos em comum.

Abaixo, enunciamos um caso particular da cota de Hasse-Weil, o qual é utilizado no Capítulo 7.

Teorema 3.2.2. ([12], Teorema 9.57(iii)) Seja $\mathcal{X}$ uma curva algébrica plana absolutamente irredutível de grau n definida sobre $\mathbb{F}_q$. Se $N(\mathcal{X})$ é a quantidade de pontos de $\mathcal{X}$ em $\mathbb{P}^2(\mathbb{F}_q)$, então

$$q + 1 - (n - 1)(n - 2)\sqrt{q} \leq N(\mathcal{X}) \leq q + 1 + (n - 1)(n - 2)\sqrt{q}.$$

Capítulo 4

Polinômios de Permutação

Neste capítulo, fazemos uma breve exposição sobre polinômios de permutação e introduzimos o conceito de posto de Carlitz. Um estudo mais completo sobre polinômios de permutação pode ser encontrado no Capítulo 7 de [18].

4.1 Permutações de $\mathbb{F}_q$

Dado um polinômio $f(X) \in \mathbb{F}_q[X]$, escrevemos f para denotar a função polinomial associada $f : c \mapsto f(c)$ de $\mathbb{F}_q$ em $\mathbb{F}_q$.

Definição 4.1.1. Dizemos que um polinômio $f(X) \in \mathbb{F}_q[X]$ é um polinômio de permutação sobre $\mathbb{F}_q$ se a função f é uma permutação de $\mathbb{F}_q$.

Observação 4.1.1. Notemos que uma função $f : \mathbb{F}_q \rightarrow \mathbb{F}_q$ sobrejetiva, ou injetiva, é uma permutação de $\mathbb{F}_q$.

Exemplo 4.1.1. Um polinômio $f(X) = aX + b \in \mathbb{F}_q[X]$, com $a \neq 0$, é um polinômio de permutação sobre $\mathbb{F}_q$. De fato, a função polinomial associada $f : \mathbb{F}_q \rightarrow \mathbb{F}_q$ definida por $f(c) = ac + b$, para todo $c \in \mathbb{F}_q$, é uma bijeção.

Exemplo 4.1.2. O monômio $f(X) = X^n$ é um polinômio de permutação sobre $\mathbb{F}_q$ se, e somente se, $(n, q-1) = 1$. Com efeito, seja ξ um gerador do grupo cíclico $\mathbb{F}_q^*$. Consideremos a função associada $f : \mathbb{F}_q \rightarrow \mathbb{F}_q$ definida por $f(c) = c^n$, para todo $c \in \mathbb{F}_q$. Notemos que $f(0) = 0$ e $\text{Im}(f) \setminus \{0\} = \langle \xi^n \rangle$. Logo, f é sobrejetiva se, e somente se, a ordem de ξ^n é $q-1$, o que equivale a $(n, q-1) = 1$ por **(A2)**.

Dados $f(X), g(X) \in \mathbb{F}_q[X]$ e uma função τ de $\mathbb{F}_q$ em $\mathbb{F}_q$, dizemos que $f(X)$ representa τ , ou que $f(X)$ é representado por τ , se $f = \tau$, isto é, se $f(c) = \tau(c)$ para todo $c \in \mathbb{F}_q$. Dizemos também que $f(X)$ representa $g(X)$ se $f = g$.

Proposição 4.1.1. Sejam $f(X), g(X) \in \mathbb{F}_q[X]$. Então $f(c) = g(c)$ para todo $c \in \mathbb{F}_q$ se, e somente se, $f(X) \equiv g(X) \pmod{(X^q - X)}$.

Demonstração. Pelo algoritmo da divisão, existem $t(X), r(X) \in \mathbb{F}_q[X]$ com $\deg r < q$, ou $r(X) = 0$, tais que $f(X) - g(X) = (X^q - X)t(X) + r(X)$. Observemos que se $r(X)$ tiver q raízes em $\mathbb{F}_q$ então não podemos ter $\deg r < q$, de sorte que $r(X) = 0$. Dessa forma, $f(c) = g(c)$ para todo $c \in \mathbb{F}_q$ se, e somente se, $r(c) = 0$ para todo $c \in \mathbb{F}_q$ o que significa $r(X) = 0$. Portanto, $f(c) = g(c)$ para todo $c \in \mathbb{F}_q$ se, e somente se, $X^q - X$ divide $f(X) - g(X)$, donde segue-se o resultado. $\square$

Vejamus neste momento que toda aplicação de $\mathbb{F}_q$ em $\mathbb{F}_q$ pode ser descrita por uma função polinomial. Mais precisamente, se $w : \mathbb{F}_q \rightarrow \mathbb{F}_q$ é uma função arbitrária de $\mathbb{F}_q$ em $\mathbb{F}_q$, então existe um único polinômio $g(X) \in \mathbb{F}_q[X]$ com $\deg g < q$ que representa w . Com efeito, definamos

$$g(X) = \sum_{c \in \mathbb{F}_q} w(c)(1 - (X - c)^{q-1}).$$

Seja $c_0 \in \mathbb{F}_q$. Então $(c_0 - c)^{q-1} = 1$ para todo $c \neq c_0$. Assim, quando calculamos $g(c_0)$, todas as parcelas vão se anular exceto a parcela onde $c = c_0$, que valerá $w(c_0)$. Logo, $g(c_0) = w(c_0)$. Já que c_0 é arbitrário, obtemos $g(c) = w(c)$ para todo $c \in \mathbb{F}_q$. Agora, se $h(X) \in \mathbb{F}_q[X]$ é um polinômio de grau menor do que q tal que $h(c) = w(c)$ para todo $c \in \mathbb{F}_q$, então $h(X) - g(X) \in \mathbb{F}_q[X]$ é um polinômio de grau menor do que ou igual a $q - 1$ com $h(c) - g(c) = 0$ para todo $c \in \mathbb{F}_q$. Consequentemente, $h(X) = g(X)$. Portanto, segue-se a unicidade de $g(X)$.

Dados $f(X), g(X) \in \mathbb{F}_q[X]$ dois polinômios de permutação sobre $\mathbb{F}_q$, a composição $t(X) = f(g(X))$ é também um polinômio de permutação sobre $\mathbb{F}_q$, pois a função associada $t : c \mapsto$

$f(g(c))$ é a composição das bijeções $f : c \mapsto f(c)$ e $g : c \mapsto g(c)$, de modo que t é uma bijeção de $\mathbb{F}_q$ em $\mathbb{F}_q$. A redução de $f(g(X))$ módulo $X^q - X$ é o único polinômio $h(X) \in \mathbb{F}_q[X]$ com $\deg h < q$ que representa t .

Seja P_q o conjunto dos polinômios de permutação sobre $\mathbb{F}_q$ de grau menor do que q . Consideremos a operação $*$ definida sobre os elementos de P_q da seguinte maneira: dados $f(X), g(X) \in P_q$, $f(X) * g(X) = h(X)$ onde $h(X)$ é o único polinômio de grau menor do que q tal que $f(g(X)) \equiv h(X) \pmod{X^q - X}$. Vamos mostrar que $(P_q, *)$ tem estrutura de grupo. A operação $*$ é associativa. De fato, dados $f(X), g(X), h(X) \in P_q$, escrevamos

$$f(X) * g(X) = t_1(X), t_1(X) * h(X) = l_1(X),$$

$$g(X) * h(X) = t_2(X) \text{ e } f(X) * t_2(X) = l_2(X).$$

Visto que $f(g(X)) \equiv t_1(X) \pmod{X^q - X}$, temos $f(g(c)) = t_1(c)$ para todo $c \in \mathbb{F}_q$. Analogamente,

$$t_1(h(c)) = l_1(c), g(h(c)) = t_2(c) \text{ e } f(t_2(c)) = l_2(c),$$

qualquer que seja $c \in \mathbb{F}_q$. Logo,

$$l_1(c) = t_1(h(c)) = f(g(h(c))) = f(t_2(c)) = l_2(c)$$

para cada $c \in \mathbb{F}_q$, donde $l_1(X) \equiv l_2(X) \pmod{X^q - X}$. Como $\deg l_1, \deg l_2 < q$, segue-se que $l_1(X) = l_2(X)$. Portanto,

$$(f(X) * g(X)) * h(X) = f(X) * (g(X) * h(X)).$$

Além disso, o polinômio $Id(X) = X$ satisfaz

$$f(Id(X)) = Id(f(X)) = f(X)$$

para todo $f(X) \in P_q$. Finalmente, observemos que se $f(X) \in P_q$ então a função associada $f : c \mapsto f(c)$ admite uma inversa f^{-1} , e existe um único polinômio $g(X) \in \mathbb{F}_q[X]$ com $\deg g < q$ que representa f^{-1} . Sendo f^{-1} uma bijeção de $\mathbb{F}_q$ em $\mathbb{F}_q$, temos $g(X) \in P_q$. Notemos que

$$f(g(c)) = c = g(f(c))$$

para todo $c \in \mathbb{F}_q$. Portanto, a Proposição 4.1.1 nos diz que

$$f(g(X)) \equiv Id(X) \equiv g(f(X)) \pmod{(X^q - X)},$$

donde $f(X) * g(X) = Id(X) = g(X) * f(X)$. Com isso, concluímos que P_q munido da operação $*$ é um grupo, com $Id(X)$ sendo o elemento identidade. Abaixo, mostramos que P_q é isomorfo ao grupo simétrico S_q .

Sejam $Q = \{\alpha_0, \alpha_1, \dots, \alpha_{q-1}\}$ o conjunto formado pelos elementos de $\mathbb{F}_q$ sem a estrutura de corpo, e S_q o grupo das bijeções de Q em Q com a operação de composição de funções.

Uma vez que cada $f(X) \in P_q$ define de maneira natural um elemento de S_q (a saber, a função polinomial associada $f : c \mapsto f(c)$ de Q em Q) definamos a função $\varphi : P_q \rightarrow S_q$ por $\varphi(f(X)) = f$. Essa aplicação é um isomorfismo de grupos. De fato, dados $f(X), g(X), h(X) \in P_q$ tais que $f(X) * g(X) = h(X)$, temos $f(g(\alpha_i)) = h(\alpha_i)$ para todo $i = 0, \dots, q-1$. Logo, para cada $i = 0, \dots, q-1$,

$$\varphi(f(X)) \circ \varphi(g(X))(\alpha_i) = \varphi(h(X))(\alpha_i),$$

de forma que

$$\varphi(f(X)) \circ \varphi(g(X)) = \varphi(h(X)) = \varphi(f(X) * g(X)).$$

Portanto, φ é um homomorfismo de grupos. Agora, se $f = g$ em S_q então $f(c) = g(c)$ para todo $c \in \mathbb{F}_q$. Sejam $f(X), g(X) \in P_q$ os polinômios que representam f e g , respectivamente. Já que $\deg f(X), \deg g(X) < q$ e $f = g$, temos $f(X) = g(X)$. Assim sendo, φ é injetiva. Se $f \in S_q$ então f induz uma função bijetiva de $\mathbb{F}_q$ em $\mathbb{F}_q$. Pelo o que vimos anteriormente, existe um único polinômio $g(X) \in P_q$ que representa f . Conseqüentemente, $f(\alpha_i) = g(\alpha_i)$ para todo $i = 0, \dots, q-1$, donde $\varphi(g(X)) = f$. Por conseguinte, φ é sobrejetiva. Portanto, φ é uma bijeção. Como também é um homomorfismo, segue-se que φ é um isomorfismo de grupos. Em vista disso, provamos o seguinte resultado.

Teorema 4.1.1. O conjunto dos polinômios de permutação sobre $\mathbb{F}_q$ de grau menor do que q munido da operação $*$ é um grupo isomorfo ao grupo simétrico S_q .

Com isso, podemos provar um importante resultado devido a L. Carlitz (veja [13]).

Teorema 4.1.2. Para $q > 2$, o grupo P_q é gerado por X^{q-2} e todos os polinômios da forma $aX + b$, com $a \neq 0$.

Demonstração. Pelos Exemplos 4.1.1 e 4.1.2, X^{q-2} e $aX + b$, com $a \neq 0$, pertencem a P_q . Assim, o grupo G gerado pelos polinômios X^{q-2} e $aX + b$ por meio da operação $*$ é um subgrupo de P_q . Queremos provar que $G = P_q$. Pela Proposição 1.1.1(ii), S_q é gerado por transposições da forma $(0 \alpha_i)$. Logo, como S_q e P_q são isomorfos, basta mostrarmos que para qualquer $0 \leq i \leq q-1$ tal que $\alpha_i \neq 0$, existe $g_i(X) \in G$ de tal modo que $\varphi(g_i(X)) = (0 \alpha_i)$. Para esse fim, dado $0 \leq i \leq q-1$ com $\alpha_i \neq 0$, consideremos o polinômio

$$f_i(X) = -\alpha_i^2 [((X - \alpha_i)^{q-2} + \alpha_i^{-1})^{q-2} - \alpha_i]^{q-2}.$$

Como $\alpha_i \neq 0$, temos $\alpha_i^{q-2} = \alpha_i^{-1}$. Por conseguinte,

$$\begin{aligned} f_i(0) &= -\alpha_i^2 [((-\alpha_i)^{q-2} + \alpha_i^{-1})^{q-2} - \alpha_i]^{q-2} \\ &= -\alpha_i^2 [((-\alpha_i)^{-1} + \alpha_i^{-1})^{q-2} - \alpha_i]^{q-2} \\ &= -\alpha_i^2 [-\alpha_i]^{q-2} = -\alpha_i^2 [-\alpha_i]^{-1} = \alpha_i, \end{aligned}$$

$$\begin{aligned} f_i(\alpha_i) &= -\alpha_i^2 [(\alpha_i^{-1})^{q-2} - \alpha_i]^{q-2} \\ &= -\alpha_i^2 [(\alpha_i^{-1})^{-1} - \alpha_i]^{q-2} = 0. \end{aligned}$$

Se $c, d \in \mathbb{F}_q^*$ então $c^{-1} \pm d^{-1} = c^{-1}d^{-1}(d \pm c)$ preservando o mesmo sinal em ambos os lados da igualdade. Assim sendo, se $c \neq \alpha_i$ então $(c - \alpha_i)^{q-2} = (c - \alpha_i)^{-1}$, o que nos dá

$$(c - \alpha_i)^{q-2} + \alpha_i^{-1} = (c - \alpha_i)^{-1} + \alpha_i^{-1} = (c - \alpha_i)^{-1} \alpha_i^{-1} c.$$

Logo, se $c \neq 0, \alpha_i$, então

$$\begin{aligned} f_i(c) &= -\alpha_i^2 [(c - \alpha_i)^{-1} \alpha_i^{-1} c]^{q-2} - \alpha_i]^{q-2} \\ &= -\alpha_i^2 [(c - \alpha_i)^{-1} \alpha_i^{-1} c]^{-1} - \alpha_i]^{q-2} \\ &= -\alpha_i^2 [(c - \alpha_i) \alpha_i c^{-1} - \alpha_i]^{q-2} \\ &= -\alpha_i^2 (-c^{-1} \alpha_i^2)^{q-2} = -\alpha_i^2 (-c^{-1} \alpha_i^2)^{-1} = c. \end{aligned}$$

Portanto, concluímos que $f_i(0) = \alpha_i$, $f_i(\alpha_i) = 0$ e $f_i(c) = c$ para todo $c \in \mathbb{F}_q$ com $c \neq 0, \alpha_i$. Desse modo, considerando $g_i(X)$ a redução de $f_i(X)$ módulo $X^q - X$, obtemos $g_i(X) \in P_q$ e $g_i(x) = (0 \ \alpha_i)(x)$ para todo $x \in \mathbb{F}_q$. Consequentemente, $\varphi(g_i(X)) = (0 \ \alpha_i)$. □

Posto que um polinômio de permutação $f(X)$ sobre $\mathbb{F}_q$ é representado por um polinômio

$g(X) \in P_q$, concluímos, pelo Teorema 4.1.2, que $f(X)$ pode ser representado por uma composição de polinômios da forma X^{q-2} e $aX + b$, com $a \neq 0$. A seguir, investigamos algumas consequências deste fato.

4.2 Posto de Carlitz

Nesta seção, definimos o posto de Carlitz, mencionamos algumas propriedades e damos alguns exemplos. Começamos explorando um pouco mais o Teorema 4.1.2. Por este teorema, todo polinômio de permutação sobre $\mathbb{F}_q$ pode ser representado por um polinômio da forma

$$\mathcal{P}_n(X) = \left(\dots \left((a_0X + a_1)^{q-2} + a_2 \right)^{q-2} \dots + a_n \right)^{q-2} + a_{n+1}, \quad (4.1)$$

com $a_1, a_{n+1} \in \mathbb{F}_q$ e $a_i \in \mathbb{F}_q^*$ para todo $i \neq 1, n+1$. Sempre que mencionarmos $\mathcal{P}_n(X)$, estaremos nos referindo a um polinômio da forma (4.1). Assim, se $f(X) \in \mathbb{F}_q[X]$ é um polinômio de permutação então existe um $\mathcal{P}_n(X)$ tal que $f(c) = \mathcal{P}_n(c)$ para todo $c \in \mathbb{F}_q$. Definindo $\mathcal{P}_0(X) = a_0X + a_1$, podemos escrever (4.1) como $\mathcal{P}_n(X) = \mathcal{P}_{n-1}(X)^{q-2} + a_{n+1}$ para $n \geq 1$. Além disso, dado $a \in \mathbb{F}_q^*$, o polinômio $a\mathcal{P}_n(X)$ é um outro polinômio da forma (4.1), pois como $(a^{q-2})^{q-2} = (a^{-1})^{-1} = a$, a constante a pode passar para dentro dos parênteses de modo a produzir um outro $\mathcal{P}_n(X)$. Vale observar também que $a_0, \dots, a_{n+1}$ não são únicos. Por exemplo,

$$f(X) = 2X^3 + 2X^2 + 4X + 4 \in \mathbb{F}_5[X]$$

é um polinômio de permutação e pode ser representado tanto por $(4X^3 + 4)^3$ quanto por $((4X+1)^3+1)^3+1$. Com efeito, um breve cálculo nos mostra que os valores destes polinômios em 0, 1, 2, 3 e 4 são iguais a 4, 2, 1, 3 e 0, respectivamente. Logo, podemos escolher tanto $(4X^3 + 4)^3$ quanto $((4X + 1)^3 + 1)^3 + 1$ para ser $\mathcal{P}_2(X)$. Além disso, é possível ter $\mathcal{P}_n(X)$ e $\mathcal{P}_m(X)$, com $m \neq n$, representando o mesmo polinômio. Para ilustrar este fato, o polinômio $\mathcal{P}_1(X) = X^3 \in \mathbb{F}_5[X]$ pode ser representado por $\mathcal{P}_3(X) = \left(((X + 1)^3 + 1)^3 + 1 \right)^3 + 1$. De

fato, os valores destes polinômios em 0, 1, 2, 3 e 4 são 0, 1, 3, 2 e 4, respectivamente.

Definição 4.2.1. O posto de Carlitz de um polinômio de permutação $f(X)$ sobre $\mathbb{F}_q$, denotado por $Crk(f)$, é o menor inteiro $n \geq 0$ que satisfaz $f = \mathcal{P}_n$ para um polinômio $\mathcal{P}_n(X)$.

Notemos que o posto de Carlitz de um polinômio de permutação $f(X) \in \mathbb{F}_q[X]$ é o mesmo para o polinômio $af(X)$ qualquer que seja $a \in \mathbb{F}_q^*$. Com efeito, seja $t = Crk(f)$ e suponhamos, por absurdo, que existam $a \in \mathbb{F}_q^*$ e um polinômio $\mathcal{P}_m(X)$ com $m < t$ que representa $af(X)$. Então $f(x) = a^{-1}\mathcal{P}_m(x)$ para todo $x \in \mathbb{F}_q$. Passando a^{-1} para dentro dos parênteses na definição de $\mathcal{P}_m(X)$, obtemos um novo polinômio da forma (4.1), com $n = m$, que apresenta $f(X)$, o que é uma contradição pela minimalidade de t .

Exemplo 4.2.1. Um polinômio $f(X) \in P_q$ tem posto de Carlitz zero se, e somente se, ele é linear. De fato, se $f(X) \in P_q$ com $Crk(f) = 0$ então existe um $\mathcal{P}_0(X) = a_0X + a_1$, $a_0 \neq 0$, tal que $\mathcal{P}_0(x) = f(x)$ para todo $x \in \mathbb{F}_q$. Dado que $\deg f, \deg \mathcal{P}_0 < q$, concluímos que $f(X) = \mathcal{P}_0(X)$, donde $f(X)$ é linear. Se $f(X) = aX + b \in \mathbb{F}_q[X]$ é linear então $a \neq 0$ e, assim, $f(X) = \mathcal{P}_0(X)$, com $a_0 = a$ e $a_1 = b$, de sorte que $Crk(f) = 0$. Além do mais, se $q = 3$ então $q - 2 = 1$, de modo que $\mathcal{P}_n(X)$ se reduz a um polinômio linear. Logo, todo polinômio de permutação sobre $\mathbb{F}_3$ tem posto de Carlitz zero. Para $q > 3$, cada polinômio $f(X) = (aX + b)^{q-2} + c$, com $a \neq 0$, tem posto de Carlitz igual a 1. De fato, $f(X) = \mathcal{P}_1(X)$, onde $a_0 = a$, $a_1 = b$ e $a_2 = c$. Assim, devemos mostrar que $Crk(f) \neq 0$. Se $Crk(f) = 0$ então $f(X)$ pode ser representado por um polinômio da forma $r(X) = dX + e$, com $d \neq 0$. Desse modo, devemos ter $f(X) = r(X)$ já que $\deg f, \deg r < q$. Mas, esta última igualdade é um absurdo pois $\deg f = q - 2 \neq 1$, uma vez que $q > 3$. Portanto, $Crk(f) = 1$.

Capítulo 5

Ciclos e Posto de Carlitz

Neste capítulo, vemos como o fato de conhecer a estrutura de ciclos de permutações de $\mathbb{F}_q$ pode auxiliar a encontrar o posto de Carlitz de polinômios de permutação. Além disso, dada uma permutação $\tau \in S_q$ escrita como um produto de ciclos disjuntos, conseguimos uma maneira de obter um polinômio $\mathcal{P}_n(X)$ tal que $\mathcal{P}_n(a) = \tau(a)$ para todo $a \in \mathbb{F}_q$.

Dado $f(X)$ um polinômio de permutação sobre $\mathbb{F}_q$, vimos no capítulo anterior que existe uma única permutação em S_q que representa $f(X)$. Assim, podemos identificar $f(X)$ unicamente como um produto de ciclos disjuntos

$$f(x) = \sigma_1 \cdots \sigma_m(x), \quad \forall x \in \mathbb{F}_q,$$

onde $\sigma_j = (x_1^j \cdots x_{\ell_j}^j) \in S_q$ e $\ell_j \geq 2$, para todo $j = 1, \dots, m$. Aqui, x_r^j representa um elemento de $\mathbb{F}_q$ indexado por j e r . Consideremos $N = m + \sum_{i=1}^m \ell_i$. Nosso principal objetivo neste capítulo é provar que, para $q > 3$, se $N < (q-1)/2$ então $\text{Crk}(f) = N$. Para isso, precisamos desenvolver algumas ferramentas.

Este capítulo é baseado no artigo [6].

5.1 Decomposição de $\mathcal{P}_n$

Seja $f(X)$ um polinômio de permutação sobre $\mathbb{F}_q$ representado na forma

$$\mathcal{P}_n(X) = \left(\dots \left((a_0 X + a_1)^{q-2} + a_2 \right)^{q-2} \dots + a_n \right)^{q-2} + a_{n+1},$$

com $a_1, a_{n+1} \in \mathbb{F}_q$, $n \geq 1$, e $a_i \in \mathbb{F}_q^*$ para todo $i \neq 1, n+1$. Defina

$$r_n(X) = \left(\dots \left((a_0X + a_1)^{-1} + a_2 \right)^{-1} \dots + a_n \right)^{-1} + a_{n+1}$$

e consideremos sua expansão em fração contínua

$$a_{n+1} + \frac{1}{a_n + \frac{1}{\dots a_2 + \frac{1}{a_0X + a_1}}}.$$

Definamos $R_0(X) = a_0X + a_1$ e, para cada $1 \leq k \leq n$,

$$R_k(X) = a_{k+1} + \frac{1}{R_{k-1}(X)},$$

denominada a k -ésima convergente da fração contínua $r_n(X)$. Sejam $\alpha_0 = 0, \alpha_1 = a_0, \beta_0 = 1, \beta_1 = a_1$ e, para $k \geq 2$,

$$\alpha_k = a_k \alpha_{k-1} + \alpha_{k-2} \quad \text{e} \quad \beta_k = a_k \beta_{k-1} + \beta_{k-2}. \quad (5.1)$$

Vamos mostrar que

$$R_k(X) = \frac{\alpha_{k+1}X + \beta_{k+1}}{\alpha_kX + \beta_k}, \quad (5.2)$$

para todo $0 \leq k \leq n$. De fato,

$$R_0(X) = a_0X + a_1 = \frac{\alpha_1X + \beta_1}{\alpha_0X + \beta_0}.$$

Suponhamos, por indução, que para um certo $1 \leq k \leq n$,

$$R_{k-1}(X) = \frac{\alpha_k X + \beta_k}{\alpha_{k-1} X + \beta_{k-1}}.$$

Então

$$\begin{aligned} R_k(X) &= a_{k+1} + \frac{1}{R_{k-1}(X)} = a_{k+1} + \frac{\alpha_{k-1} X + \beta_{k-1}}{\alpha_k X + \beta_k} \\ &= \frac{(a_{k+1} \alpha_k + \alpha_{k-1}) X + (a_{k+1} \beta_k + \beta_{k-1})}{\alpha_k X + \beta_k} \\ &= \frac{\alpha_{k+1} X + \beta_{k+1}}{\alpha_k X + \beta_k}. \end{aligned}$$

Logo, (5.2) vale para todo $0 \leq k \leq n$. Além disso, temos o seguinte lema.

Lema 5.1.1. Para cada $0 \leq \ell \leq n$, $\alpha_{\ell+1} \beta_\ell - \beta_{\ell+1} \alpha_\ell = (-1)^\ell a_0$. Em particular,

$$\alpha_{\ell+1} \beta_\ell - \alpha_\ell \beta_{\ell+1} \neq 0, \quad \forall \ell = 0, 1, \dots, n$$

e α_k, β_k não podem ser ambos nulos para todo $0 \leq k \leq n+1$.

Demonstração. Observemos que $\alpha_1 \beta_0 - \alpha_0 \beta_1 = a_0$. Se $1 \leq \ell \leq n$ então, pelas relações em (5.1),

$$\begin{aligned} \alpha_{\ell+1} \beta_\ell - \alpha_\ell \beta_{\ell+1} &= (\alpha_\ell a_{\ell+1} + \alpha_{\ell-1}) \beta_\ell - \alpha_\ell (\beta_\ell a_{\ell+1} + \beta_{\ell-1}) \\ &= \alpha_{\ell-1} \beta_\ell - \alpha_\ell \beta_{\ell-1} = (-1) (\alpha_\ell \beta_{\ell-1} - \alpha_{\ell-1} \beta_\ell). \end{aligned}$$

Assim, por indução, temos $\alpha_{\ell+1} \beta_\ell - \alpha_\ell \beta_{\ell+1} = (-1)^\ell (\alpha_1 \beta_0 - \alpha_0 \beta_1) = (-1)^\ell a_0 \neq 0$. $\square$

Veremos que as funções racionais $R_k(X)$, em especial $R_n(X)$, são muito úteis para estudar o polinômio $\mathcal{P}_n(X)$, além de serem relativamente fáceis de se manipular por conta das relações

em (5.1). Queremos comparar os valores de $\mathcal{P}_n(X)$ e $R_n(X)$ em um ponto. Inicialmente, observemos que dado $c \in \mathbb{F}_q$, temos

$$a_0c + a_1, (a_0c + a_1)^{-1} + a_2, \dots, \left(\dots \left((a_0c + a_1)^{-1} + a_2 \right)^{-1} \dots + a_n \right)$$

são não nulos se, e somente se, $R_0(c), R_1(c), \dots, R_{n-1}(c)$ são não nulos. Neste caso, $r_n(c)$ está bem definido. Dentro desta situação, vemos que

$$\begin{aligned} R_n(c) &= a_{n+1} + \frac{1}{R_{n-1}(c)} = a_{n+1} + \frac{1}{a_n + \frac{1}{R_{n-2}(c)}} = \dots \\ &= a_{n+1} + \frac{1}{a_n + \frac{1}{a_2 + \frac{1}{R_0(c)}}} \\ &= a_{n+1} + \frac{1}{a_n + \frac{1}{a_2 + a_0c + a_1}} = r_n(c). \end{aligned}$$

Por outro lado, do fato de $a^{q-2} = a^{-1}$ para todo $a \in \mathbb{F}_q^*$, obtemos $\mathcal{P}_n(c) = r_n(c)$, donde $\mathcal{P}_n(c) = R_n(c)$. Logo, se $R_0(c), R_1(c), \dots, R_{n-1}(c)$ são não nulos então $\mathcal{P}_n(c) = R_n(c)$.

Motivados pelo parágrafo precedente, queremos encontrar uma condição sobre $c \in \mathbb{F}_q$ para assegurar que $R_i(c) \neq 0$ para todo $0 \leq i \leq n-1$. Se $R_k(b) = 0$ para algum $0 \leq k \leq n-1$ e $b \in \mathbb{F}_q$, então $\alpha_{k+1} \neq 0$ pois caso contrário, $\beta_{k+1} = 0$ em vista de (5.2). Porém, pelo Lema 5.1.1, não podemos ter $\alpha_{k+1} = \beta_{k+1} = 0$, e isto nos dá uma contradição. Assim, $\alpha_{k+1} \neq 0$. Por (5.2) e do fato de $R_k(b) = 0$, vemos que $b = -\beta_{k+1}/\alpha_{k+1}$. Dessa forma, se $c \neq -\beta_k/\alpha_k$ para todo $1 \leq k \leq n$ tal que $\alpha_k \neq 0$, então $R_0(c), \dots, R_{n-1}(c)$ são não nulos, de modo que

$\mathcal{P}_n(c) = R_n(c)$. Portanto, temos o seguinte fato:

(I) $\mathcal{P}_n(c) = R_n(c)$ para todo $c \in \mathbb{F}_q \setminus \{-\beta_k/\alpha_k : 1 \leq k \leq n \text{ e } \alpha_k \neq 0\}$.

Lembremos que, no Capítulo 3, identificamos $\mathbb{P}^1(K)$ com $K \cup \{\infty\}$, onde ∞ é um elemento fora de K correspondente ao ponto $[0 : 1]$. Desse modo, se $\alpha_k \neq 0$ então podemos identificar $-\beta_k/\alpha_k$ com o ponto $[1 : -\beta_k/\alpha_k] = [\alpha_k : -\beta_k]$. Se $\alpha_k = 0$ então, pelo Lema 5.1.1, $\beta_k \neq 0$, donde $[\alpha_k : -\beta_k] = [0 : 1]$. Como este ponto está associado a ∞ , identificamos $-\beta_k/\alpha_k$ com ∞ . Notemos ainda que se $a = -\beta_k/\alpha_k$, com $\alpha_k \neq 0$, então o denominador de $R_k(a)$ se anula. Com essa motivação, chamamos de polos os elementos $-\beta_k/\alpha_k$, para $1 \leq k \leq n$. Consideremos então o conjunto de polos

$$\mathcal{O}_n = \{x_k : x_k = \frac{-\beta_k}{\alpha_k}, k = 1, \dots, n\} \subset \mathbb{P}^1(\mathbb{F}_q) = \mathbb{F}_q \cup \{\infty\}. \quad (5.3)$$

Com essas notações, concluímos por (I) que

$$f(c) = \mathcal{P}_n(c) = R_n(c) \text{ para todo } c \in \mathbb{F}_q \setminus \mathcal{O}_n.$$

Agora, definamos uma função $F_n : \mathbb{F}_q \rightarrow \mathbb{F}_q$ pondo $F_n(x) = R_n(x)$ se $x \neq x_n$ e $F_n(x_n) = \alpha_{n+1}/\alpha_n$ quando $x_n \in \mathbb{F}_q$. Afirmamos que F_n é bijetiva. De fato, se $\alpha_n = 0$ então $\alpha_{n+1}, \beta_n \neq 0$ pelo Lema 5.1.1. Logo, $R_n(X)$ é linear, daí R_n é uma permutação de $\mathbb{F}_q$. Além disso, de $x_n \notin \mathbb{F}_q$ resulta $F_n = R_n$. Neste caso, F_n é bijetiva. Suponhamos $\alpha_n \neq 0$ e $F_n(x) = \alpha_{n+1}/\alpha_n$, para algum $x \neq x_n$. Assim, $F_n(x) = R_n(x)$, donde

$$\begin{aligned} R_n(x) = \frac{\alpha_{n+1}}{\alpha_n} &\Rightarrow \frac{\alpha_{n+1}x + \beta_{n+1}}{\alpha_n x + \beta_n} = \frac{\alpha_{n+1}}{\alpha_n} \\ &\Rightarrow \alpha_{n+1}\alpha_n x + \beta_{n+1}\alpha_n = \alpha_{n+1}\alpha_n x + \alpha_{n+1}\beta_n \\ &\Rightarrow \alpha_{n+1}\beta_n - \alpha_n\beta_{n+1} = 0, \end{aligned}$$

o que não pode acontecer em vista do Lema 5.1.1. Por conseguinte, $F_n(x) = \alpha_{n+1}/\alpha_n \Rightarrow x = x_n$. Se $x, y \in \mathbb{F}_q \setminus \{x_n\}$ e $F_n(x) = F_n(y)$ então, usando o Lema 5.1.1,

$$\begin{aligned}
R_n(x) = R_n(y) &\Rightarrow \frac{\alpha_{n+1}x + \beta_{n+1}}{\alpha_n x + \beta_n} = \frac{\alpha_{n+1}y + \beta_{n+1}}{\alpha_n y + \beta_n} \\
&\Rightarrow \alpha_{n+1}\alpha_n xy + \alpha_{n+1}\beta_n x + \beta_{n+1}\alpha_n y + \beta_{n+1}\beta_n = \\
&= \alpha_{n+1}\alpha_n xy + \alpha_{n+1}\beta_n y + \beta_{n+1}\alpha_n x + \beta_{n+1}\beta_n \\
&\Rightarrow (\alpha_{n+1}\beta_n - \alpha_n\beta_{n+1})(x - y) = 0 \\
&\Rightarrow x = y.
\end{aligned}$$

Portanto, $F_n : \mathbb{F}_q \rightarrow \mathbb{F}_q$ é injetiva, donde é uma bijeção.

Queremos descrever $\mathcal{P}_n$ em função de F_n . Inicialmente, notemos que se x não é um polo então

$$\mathcal{P}_n(x) = R_n(x) = F_n(x).$$

Além disso, temos a seguinte propriedade.

Lema 5.1.2. Se $x \in \mathbb{F}_q$ e $x \neq x_n, x_{n-1}$ então

$$F_{n-1}(x)^{q-2} + a_{n+1} = R_{n-1}(x)^{q-2} + a_{n+1} = F_n(x).$$

Demonstração. De fato, a primeira igualdade segue-se por definição de F_{n-1} . Quanto à segunda, como $x \neq x_n, x_{n-1}$, vemos que $\alpha_n x + \beta_n, \alpha_{n-1} x + \beta_{n-1} \neq 0$ e $R_n(x) = F_n(x)$, de

forma que, usando as relações em (5.1),

$$\begin{aligned}
R_{n-1}(x)^{q-2} + a_{n+1} &= \left(\frac{\alpha_n x + \beta_n}{\alpha_{n-1} x + \beta_{n-1}} \right)^{q-2} + a_{n+1} = \left(\frac{\alpha_n x + \beta_n}{\alpha_{n-1} x + \beta_{n-1}} \right)^{-1} + a_{n+1} \\
&= \frac{\alpha_{n-1} x + \beta_{n-1}}{\alpha_n x + \beta_n} + a_{n+1} = \frac{(a_{n+1} \alpha_n + \alpha_{n-1}) x + a_{n+1} \beta_n + \beta_{n-1}}{\alpha_n x + \beta_n} \\
&= \frac{\alpha_{n+1} x + \beta_{n+1}}{\alpha_n x + \beta_n} = R_n(x) = F_n(x).
\end{aligned}$$

□

Abaixo, determinamos a estrutura de ciclo de $\mathcal{P}_n$ em função de F_n quando os polos estão em $\mathbb{F}_q$ e são distintos.

Lema 5.1.3. Suponha que os polos $x_1, x_2, \dots, x_n$ definidos por (5.3) estejam em $\mathbb{F}_q$ e sejam distintos. Então

$$\mathcal{P}_n(x_i) = \begin{cases} F_n(x_{i-1}) & \text{para } 2 \leq i \leq n, \\ F_n(x_n) & \text{para } i = 1 \end{cases}$$

para todo $n \geq 2$. Portanto, podemos expressar a permutação $\mathcal{P}_n$ como um produto do n -ciclo $(F_n(x_n)F_n(x_{n-1}) \cdots F_n(x_1))$ com F_n , isto é,

$$\mathcal{P}_n(x) = (F_n(x_n)F_n(x_{n-1}) \cdots F_n(x_1)) F_n(x), \quad \forall x \in \mathbb{F}_q. \quad (5.4)$$

Demonstração. Faremos a prova por indução sobre n . Consideremos

$$\mathcal{P}_2(X) = ((a_0 X + a_1)^{q-2} + a_2)^{q-2} + a_3,$$

com $a_0, a_2 \neq 0$. Assim, por (5.1), $\alpha_2 = a_2 \alpha_1 + \alpha_0 = a_2 a_0$ e $\beta_2 = a_2 \beta_1 + \beta_0 = a_2 a_1 + 1$. Com

isso, obtemos $\alpha_3 = a_3a_2a_0 + a_0$ e $\beta_3 = a_3a_2a_1 + a_3 + a_1$. Logo,

$$R_2(X) = \frac{(a_3a_2a_0 + a_0)X + a_3a_2a_1 + a_3 + a_1}{a_2a_0X + a_2a_1 + 1}.$$

Os polos são $x_1 = \frac{-a_1}{a_0}$ e $x_2 = \frac{-a_2a_1 - 1}{a_2a_0}$. Desse modo,

$$\begin{aligned} \mathcal{P}_2(x_1) &= a_2^{q-2} + a_3 = a_2^{-1} + a_3 = \frac{1 + a_2a_3}{a_2} = \frac{a_3a_2a_0 + a_0}{a_2a_0} = \frac{\alpha_3}{\alpha_2} = F_2(x_2), \\ F_2(x_1) &= R_2(x_1) = \frac{-a_3a_2a_1 - a_1 + a_3a_2a_1 + a_3 + a_1}{-a_2a_1 + a_2a_1 + 1} = a_3 \end{aligned}$$

e

$$\begin{aligned} \mathcal{P}_2(x_2) &= \left(\left(\frac{-a_2a_1 - 1}{a_2} + a_1 \right)^{q-2} + a_2 \right)^{q-2} + a_3 \\ &= ((-a_2^{-1})^{q-2} + a_2)^{q-2} + a_3 \\ &= ((-a_2^{-1})^{-1} + a_2)^{q-2} + a_3 = (-a_2 + a_2)^{q-2} + a_3 \\ &= a_3 = F_2(x_1). \end{aligned}$$

Se $x \neq x_1, x_2$ (ou seja, $x \in \mathbb{F}_q \setminus \mathcal{O}_2$), então $\mathcal{P}_2(x) = R_2(x) = F_2(x)$. Portanto, o resultado vale para $n = 2$. Para o passo de indução, lembremos que $\mathcal{P}_n(x) = \mathcal{P}_{n-1}(x)^{q-2} + a_{n+1}$ para todo $x \in \mathbb{F}_q$. Dessa maneira, suponhamos, por hipótese de indução, que $\mathcal{P}_{n-1}(x_i) = F_{n-1}(x_{i-1})$ para $2 \leq i \leq n-1$, e $\mathcal{P}_{n-1}(x_1) = F_{n-1}(x_{n-1})$. Como os polos são distintos, $x_{i-1} \neq x_n, x_{n-1}$ qualquer que seja $2 \leq i \leq n-1$. Pelo Lema 5.1.2, concluímos que

$$\mathcal{P}_n(x_i) = \mathcal{P}_{n-1}(x_i)^{q-2} + a_{n+1} = F_{n-1}(x_{i-1})^{q-2} + a_{n+1} = F_n(x_{i-1}), \quad \forall 2 \leq i \leq n-1.$$

Agora, notemos que $x_n \notin \mathcal{O}_{n-1}$ pois os polos são distintos. Assim,

$$\mathcal{P}_{n-1}(x_n) = R_{n-1}(x_n) = \frac{\alpha_n x_n + \beta_n}{\alpha_{n-1} x_n + \beta_{n-1}} = 0.$$

Dessa forma, $\mathcal{P}_n(x_n) = \mathcal{P}_{n-1}(x_n)^{q-2} + a_{n+1} = a_{n+1}$. Por outro lado,

$$\begin{aligned} F_n(x_{n-1}) &= R_n(x_{n-1}) = \frac{\alpha_{n+1} x_{n-1} + \beta_{n+1}}{\alpha_n x_{n-1} + \beta_n} \\ &= \frac{(a_{n+1} \alpha_n + \alpha_{n-1}) x_{n-1} + a_{n+1} \beta_n + \beta_{n-1}}{\alpha_n x_{n-1} + \beta_n} \\ &= \frac{a_{n+1} (\alpha_n x_{n-1} + \beta_n) + \alpha_{n-1} x_{n-1} + \beta_{n-1}}{\alpha_n x_{n-1} + \beta_n} = a_{n+1}. \end{aligned}$$

Logo, $\mathcal{P}_n(x_n) = F_n(x_{n-1})$. Finalmente, usando que $\alpha_n \neq 0$, pois $x_n \in \mathbb{F}_q$, e a hipótese $\mathcal{P}_{n-1}(x_1) = F_{n-1}(x_{n-1}) = \alpha_n / \alpha_{n-1}$, obtemos

$$\begin{aligned} \mathcal{P}_n(x_1) &= \mathcal{P}_{n-1}(x_1)^{q-2} + a_{n+1} = \left(\frac{\alpha_n}{\alpha_{n-1}} \right)^{q-2} + a_{n+1} = \left(\frac{\alpha_n}{\alpha_{n-1}} \right)^{-1} + a_{n+1} \\ &= \frac{\alpha_{n-1}}{\alpha_n} + a_{n+1} = \frac{a_{n+1} \alpha_n + \alpha_{n-1}}{\alpha_n} = \frac{\alpha_{n+1}}{\alpha_n} = F_n(x_n). \end{aligned}$$

Portanto, pelo Princípio de Indução, o resultado vale para todo $n \geq 2$. □

Tentaremos, agora, generalizar o lema anterior. Seja $\tau \in S_q$ um ciclo. Lembremos que $l(\tau)$ é o comprimento de τ e que $a \in \text{supp}(\tau)$ se τ move a . Suponhamos que a permutação $\mathcal{P}_n$ possa ser decomposta como

$$\mathcal{P}_n(x) = \tau_1^{(n)} \cdots \tau_m^{(n)} F_n(x), \quad \forall x \in \mathbb{F}_q, \quad (5.5)$$

onde $\tau_1^{(n)}, \dots, \tau_m^{(n)}$ são ciclos disjuntos, $l(\tau_j^{(n)}) \geq 2$, e

$$\tau_j^{(n)} = \left(F_n(x_1^j) \cdots F_n(x_{l_j}^j) \right),$$

para $1 \leq j \leq m$. Notemos que $\mathcal{P}_n(y) \neq F_n(y)$ se, e somente se, $F_n(y) \in \text{supp}(\tau_j^{(n)})$ para algum $1 \leq j \leq m$. Neste caso, y está no conjunto de polos $\mathcal{O}_n$, desde que $\mathcal{P}_n(x) = F_n(x)$ para todo $x \in \mathbb{F}_q \setminus \mathcal{O}_n$. Dada uma decomposição de $\mathcal{P}_n$ como em (5.5), definimos o conjunto $\overline{\mathcal{O}_n}$ por

$$\overline{\mathcal{O}_n} = \{y \in \mathcal{O}_{n-1} : F_n(y) \in \text{supp}(\tau_j^{(n)}), \text{ para algum } 1 \leq j \leq m\} \cup \{x_n\},$$

se $x_n \in \mathbb{F}_q$. Caso $x_n = \infty$, $\overline{\mathcal{O}_n}$ não contém x_n .

Para $k = n, n-1$ e $1 \leq j \leq m$, denotamos o ciclo $\left(F_k(x_1^j) \cdots F_k(x_{l_j}^j) \right)$ por $\tau_j^{(k)}$.

Teorema 5.1.1. Suponha que $x_{n-1}, x_n \in \mathbb{F}_q$ e

$$\mathcal{P}_{n-1}(x) = \tau_1^{(n-1)} \cdots \tau_m^{(n-1)} F_{n-1}(x), \quad \forall x \in \mathbb{F}_q, \quad (5.6)$$

é uma decomposição de $\mathcal{P}_{n-1}$ satisfazendo:

- (i) $\tau_1^{(n-1)}, \dots, \tau_m^{(n-1)}$ são ciclos disjuntos.
- (ii) Se $\mathcal{P}_{n-1}(x_{n-1}) \neq F_{n-1}(x_{n-1})$ assumimos, sem perda de generalidade, que $F_{n-1}(x_{n-1}) \in \text{supp}(\tau_1^{(n-1)})$ com $x_1^1 = x_{n-1}$, e $l(\tau_j^{(n-1)}) = l_j \geq 2$, para todo $1 \leq j \leq m$.
- (iii) Se $\mathcal{P}_{n-1}(x_{n-1}) = F_{n-1}(x_{n-1})$ assumimos, sem perda de generalidade, que $\tau_1^{(n-1)} = (F_{n-1}(x_{n-1}))$ e $l(\tau_j^{(n-1)}) = l_j \geq 2$, para todo $2 \leq j \leq m$.

Então $\mathcal{P}_n$ pode ser decomposto da seguinte maneira:

(1) se $x_n \notin \overline{\mathcal{O}_{n-1}}$ então

$$\mathcal{P}_n(x) = (F_n(x_n)F_n(x_{n-1}) \cdots F_n(x_{l_1}^1)) \tau_2^{(n)} \cdots \tau_m^{(n)} F_n(x), \quad \forall x \in \mathbb{F}_q;$$

(2) se $F_{n-1}(x_n) \in \text{supp}(\tau_1^{(n-1)})$, digamos $x_n = x_r^1$, então, para qualquer $x \in \mathbb{F}_q$,

$$\mathcal{P}_n(x) = (F_n(x_n)F_n(x_{r+1}^1) \cdots F_n(x_{l_1}^1)) (F_n(x_{n-1})F_n(x_2^1) \cdots F_n(x_{r-1}^1)) \tau_2^{(n)} \cdots \tau_m^{(n)} F_n(x);$$

(3) se $F_{n-1}(x_n) \in \text{supp}(\tau_j^{(n-1)})$, $j \neq 1$, digamos em $\text{supp}(\tau_2^{(n-1)})$ e $x_n = x_s^2$, então, para todo $x \in \mathbb{F}_q$,

$$\mathcal{P}_n(x) = (F_n(x_s^2)F_n(x_{s+1}^2) \cdots F_n(x_{l_2}^2)F_n(x_1^2) \cdots F_n(x_{s-1}^2)F_n(x_1^1) \cdots F_n(x_{l_1}^1)) \tau_3^{(n)} \cdots \tau_m^{(n)} F_n(x).$$

Demonstração. (1) Neste caso, temos que mostrar que:

(a) se $x \notin \overline{\mathcal{O}_{n-1}}$ e $x \neq x_n$ então $\mathcal{P}_n(x) = F_n(x)$;

(b) se $y \in \overline{\mathcal{O}_{n-1}}$ com $y \neq x_{l_1}^1$ e $\mathcal{P}_{n-1}(y) = F_{n-1}(y')$, então $\mathcal{P}_n(y) = F_n(y')$;

(c) $\mathcal{P}_n(x_{l_1}^1) = F_n(x_n)$ e $F_n(x_n) = F_n(x_{n-1})$.

Se $x \notin \overline{\mathcal{O}_{n-1}}$ então $\mathcal{P}_{n-1}(x) = F_{n-1}(x)$, e $x \neq x_{n-1}, x_n$. Pelo Lema 5.1.2,

$$\mathcal{P}_n(x) = \mathcal{P}_{n-1}(x)^{q-2} + a_{n+1} = F_{n-1}(x)^{q-2} + a_{n+1} = F_n(x).$$

Isso prova a parte (a). Para a parte (b), suponhamos que estejamos sob a hipótese (ii). Assim, $x_1^1 = x_{n-1}$, de modo que $\mathcal{P}_{n-1}(x_{l_1}^1) = F_{n-1}(x_{n-1})$. Se $\mathcal{P}_{n-1}(y) = F_{n-1}(y')$ então $y' \neq x_{n-1}$ pois $y \neq x_{l_1}^1$. Além disso, $y' \neq x_n$, caso contrário $\mathcal{P}_{n-1}(y) = F_{n-1}(x_n)$. Desde que $x_n \notin \overline{\mathcal{O}_{n-1}}$, vemos que $\mathcal{P}_{n-1}(x_n) = F_{n-1}(x_n)$ donde $y = x_n$, uma contradição pois $y \in \overline{\mathcal{O}_{n-1}}$.

Desse modo, $y' \neq x_n, x_{n-1}$. Usando o Lema 5.1.2, obtemos

$$\mathcal{P}_n(y) = \mathcal{P}_{n-1}(y)^{q-2} + a_{n+1} = F_{n-1}(y')^{q-2} + a_{n+1} = F_n(y').$$

Sob a hipótese (iii), temos $\mathcal{P}_{n-1}(x_{n-1}) = F_{n-1}(x_{n-1})$ e $x_{l_1}^1 = x_{n-1}$, daí $y' \neq x_{n-1}$ já que $y \neq x_{l_1}^1$. Como também $y \neq x_n$, podemos concluir que $\mathcal{P}_n(y) = F_n(y')$ da mesma forma como fizemos acima.

Agora, mostremos o item (c). Observemos que

$$\begin{aligned} F_n(x_{n-1}) &= R_n(x_{n-1}) = \frac{\alpha_{n+1}x_{n-1} + \beta_{n+1}}{\alpha_n x_{n-1} + \beta_n} \\ &= \frac{(a_{n+1}\alpha_n + \alpha_{n-1})x_{n-1} + a_{n+1}\beta_n + \beta_{n-1}}{\alpha_n x_{n-1} + \beta_n} \\ &= \frac{a_{n+1}(\alpha_n x_{n-1} + \beta_n) + \alpha_{n-1}x_{n-1} + \beta_{n-1}}{\alpha_n x_{n-1} + \beta_n} = a_{n+1}. \end{aligned}$$

Dado que $x_n \notin \overline{\mathcal{O}_{n-1}}$, temos

$$\mathcal{P}_{n-1}(x_n) = F_{n-1}(x_n) = \frac{\alpha_n x_n + \beta_n}{\alpha_{n-1} x_n + \beta_{n-1}} = 0.$$

Logo,

$$\mathcal{P}_n(x_n) = \mathcal{P}_{n-1}(x_n)^{q-2} + a_{n+1} = a_{n+1} = F_n(x_{n-1}).$$

Sob a hipótese (ii), vemos que

$$\mathcal{P}_{n-1}(x_{l_1}^1) = F_{n-1}(x_1^1) = F_{n-1}(x_{n-1}) = \frac{\alpha_n}{\alpha_{n-1}}.$$

Sob a hipótese (iii), $x_{l_1}^1 = x_{n-1}$ e

$$\mathcal{P}_{n-1}(x_{l_1}^1) = \mathcal{P}_{n-1}(x_{n-1}) = F_{n-1}(x_{n-1}) = \frac{\alpha_n}{\alpha_{n-1}}.$$

Portanto, em qualquer uma das hipóteses,

$$\begin{aligned}\mathcal{P}_n(x_{l_1}^1) &= \mathcal{P}_{n-1}(x_{l_1}^1)^{q-2} + a_{n+1} = \left(\frac{\alpha_n}{\alpha_{n-1}}\right)^{q-2} + a_{n+1} \\ &= \frac{\alpha_{n-1}}{\alpha_n} + a_{n+1} = \frac{a_{n+1}\alpha_n + \alpha_{n-1}}{\alpha_n} = \frac{\alpha_{n+1}}{\alpha_n} = F_n(x_n).\end{aligned}$$

(2) Suponhamos que $F_{n-1}(x_n) \in \text{supp}(\tau_1^{(n-1)})$, digamos $x_n = x_r^1$. Notemos que tanto na hipótese (ii) quanto na (iii) temos $x_1^1 = x_{n-1}$. Dessa forma,

$$\tau_1^{(n-1)} = (F_{n-1}(x_{n-1}) \cdots F_{n-1}(x_{r-1}^1) F_{n-1}(x_n) \cdots F_{n-1}(x_{l_1}^1)).$$

Neste caso, devemos mostrar que:

- (a) se $x \notin \overline{\mathcal{O}_{n-1}}$ então $\mathcal{P}_n(x) = F_n(x)$;
- (b) se $y \in \overline{\mathcal{O}_{n-1}}$ com $y \neq x_{l_1}^1, x_{r-1}^1$ e $\mathcal{P}_{n-1}(y) = F_{n-1}(y')$, então $\mathcal{P}_n(y) = F_n(y')$;
- (c) $\mathcal{P}_n(x_{l_1}^1) = F_n(x_n)$ e $\mathcal{P}_n(x_{r-1}^1) = F_n(x_{n-1})$.

Desde que $x_{n-1}, x_n \in \overline{\mathcal{O}_{n-1}}$, se $x \notin \overline{\mathcal{O}_{n-1}}$ então $x \neq x_n, x_{n-1}$, de maneira que o caso (a) segue-se da mesma forma como no caso (1)(a). O caso (b) e a primeira parte do caso (c) também seguem-se da mesma maneira como nos respectivos casos (1)(b) e (1)(c). Faltam mostrarmos que $\mathcal{P}_n(x_{r-1}^1) = F_n(x_{n-1})$. Pela decomposição de $\mathcal{P}_{n-1}$ e pela forma de $\tau_1^{(n-1)}$, temos $\mathcal{P}_{n-1}(x_{r-1}^1) = F_{n-1}(x_n)$. Além disso, como vimos no caso (1), $F_{n-1}(x_n) = 0$ e $F_n(x_{n-1}) = a_{n+1}$. Assim,

$$\mathcal{P}_n(x_{r-1}^1) = \mathcal{P}_{n-1}(x_{r-1}^1)^{q-2} + a_{n+1} = F_{n-1}(x_n)^{q-2} + a_{n+1} = a_{n+1} = F_n(x_{n-1}).$$

(3) Suponhamos que $F_{n-1}(x_n) \in \text{supp}(\tau_2^{(n-1)})$ e $x_n = x_s^2$. Nós precisamos mostrar os seguintes itens:

- (a) se $x \notin \overline{\mathcal{O}_{n-1}}$ então $\mathcal{P}_n(x) = F_n(x)$;
- (b) se $y \in \overline{\mathcal{O}_{n-1}}$ com $y \neq x_{l_1}^1, x_{s-1}^2$ e $\mathcal{P}_{n-1}(y) = F_{n-1}(y')$, então $\mathcal{P}_n(y) = F_n(y')$;
- (c) $\mathcal{P}_n(x_{l_1}^1) = F_n(x_n)$ e $\mathcal{P}_n(x_{s-1}^2) = F_n(x_{n-1})$.

As provas dos itens (a) e (b) seguem-se da mesma forma como no caso (1), e a do item (c) da mesma maneira como no caso (2).

□

Teorema 5.1.2. Suponha $x_n = \infty$ e $\mathcal{P}_{n-1}$ decomposto como em (5.6). Então

$$\mathcal{P}_n(x) = \tau_1^{(n)} \cdots \tau_m^{(n)} F_n(x), \quad \forall x \in \mathbb{F}_q.$$

Demonstração. Precisamos mostrar as seguintes propriedades:

- (a) se $x \notin \overline{\mathcal{O}_{n-1}}$ então $\mathcal{P}_n(x) = F_n(x)$;
- (b) se $y \in \overline{\mathcal{O}_{n-1}}$ satisfaz $\mathcal{P}_{n-1}(y) = F_{n-1}(y')$, então $\mathcal{P}_n(y) = F_n(y')$.

Se $x \notin \overline{\mathcal{O}_{n-1}}$ então $\mathcal{P}_{n-1}(x) = F_{n-1}(x)$ e $x \neq x_{n-1}$. Pelo Lema 5.1.2,

$$\mathcal{P}_n(x) = \mathcal{P}_{n-1}(x)^{q-2} + a_{n+1} = F_{n-1}(x)^{q-2} + a_{n+1} = F_n(x),$$

donde segue-se o item (a). Quanto ao item (b), se $y' \neq x_{n-1}$, então, pelo Lema 5.1.2,

$$\mathcal{P}_n(y) = \mathcal{P}_{n-1}(y)^{q-2} + a_{n+1} = F_{n-1}(y')^{q-2} + a_{n+1} = F_n(y').$$

Para $y' = x_{n-1}$, lembremos que $F_{n-1}(x_{n-1}) = \alpha_n/\alpha_{n-1}$ e $F_n(x_{n-1}) = a_{n+1}$. Como $x_n = \infty$,

temos $\alpha_n = 0$. Logo, se $\mathcal{P}_{n-1}(y) = F_{n-1}(x_{n-1})$ então

$$\begin{aligned}\mathcal{P}_n(y) &= \mathcal{P}_{n-1}(y)^{q-2} + a_{n+1} = F_{n-1}(x_{n-1})^{q-2} + a_{n+1} \\ &= \left(\frac{\alpha_n}{\alpha_{n-1}}\right)^{q-2} + a_{n+1} = a_{n+1} = F_n(x_{n-1}).\end{aligned}$$

□

Com esses teoremas, podemos relacionar os polos com a quantidade de ciclos na decomposição de $\mathcal{P}_n$ em (5.5). Consideremos a lista de polos $x_1, \dots, x_n$. Chamamos tal lista de corda de polos e, por abuso de notação, escrevemos

$$\mathcal{O}_n = x_1, \dots, x_n.$$

Aproveitando a demonstração do Lema 5.1.3, vemos que $x_1 = \frac{-a_1}{a_0}$ e $x_2 = \frac{-a_2 a_1 - 1}{a_2 a_0}$, de modo que $x_1 \neq x_2$, pois

$$x_1 = x_2 \Rightarrow \frac{-a_1}{a_0} = \frac{-a_2 a_1 - 1}{a_2 a_0} \Rightarrow a_0 = 0,$$

o que não pode acontecer. Pelo Lema 5.1.3, $\mathcal{P}_2(x) = (F_2(x_2)F_2(x_1))F_2(x)$ para todo $x \in \mathbb{F}_q$. Se $x_3 \in \{x_1, x_2\}$ então, pelo Teorema 5.1.1(2), a decomposição de $\mathcal{P}_3$ contém um ciclo a mais que $\mathcal{P}_2$. Se $x_3 \notin \{x_1, x_2\}$, então por (1) deste teorema ou pelo Teorema 5.1.2 caso $x_3 = \infty$, $\mathcal{P}_3$ contém a mesma quantidade de ciclos que $\mathcal{P}_2$. Continuando dessa maneira, vemos que $\mathcal{P}_4$ tem a mesma quantidade de ciclos que $\mathcal{P}_3$ se x_4 não é um dos polos x_1, x_2 ou x_3 . Caso x_4 seja um destes polos, $\mathcal{P}_4$ tem, no máximo, um ciclo a mais que $\mathcal{P}_3$ pelo Teorema 5.1.1 itens (2) e (3) ou pelo Teorema 5.1.2 caso $x_4 = \infty$. Vamos provar que se ℓ é a quantidade de polos repetidos na corda de polos $\mathcal{O}_n = x_1, \dots, x_n$, então $\mathcal{P}_n$ tem no máximo $\ell + 1$ ciclos em sua decomposição como em (5.5). Para esse fim, podemos considerar apenas polos em $\mathbb{F}_q$ já que

∞ não altera a quantidade de ciclos de $\mathcal{P}_k$, para $1 \leq k \leq n$, devido ao Teorema 5.1.2. Para $n = 2$, vimos que $\mathcal{O}_2 = x_1, x_2$ não possui polos repetidos e $\mathcal{P}_2(x) = (F_2(x_2)F_2(x_1))F_2(x)$ possui um ciclo em sua decomposição. Por indução, suponhamos que $\mathcal{O}_{n-1} = x_1, \dots, x_{n-1}$ possuam ℓ polos repetidos e que a quantidade de ciclos na decomposição de $\mathcal{P}_{n-1}$ seja menor do que ou igual a $\ell + 1$. Se $x_n \in \{x_1, \dots, x_{n-1}\}$ então $\mathcal{O}_n$ tem $\ell + 1$ polos repetidos e, pelo Teorema 5.1.1 itens (2) e (3), $\mathcal{P}_n$ vai ter no máximo $\ell + 2$ ciclos em sua decomposição. Se $x_n \notin \{x_1, \dots, x_{n-1}\}$ então $\mathcal{O}_n$ tem ℓ polos repetidos e, pelo Teorema 5.1.1(1), $\mathcal{P}_n$ tem no máximo $\ell + 1$ ciclos. Portanto, provamos o seguinte fato.

Corolário 5.1.1. Se $\mathcal{O}_n$ tem ℓ polos repetidos em $\mathbb{F}_q$ então $\mathcal{P}_n$ possui no máximo $\ell + 1$ ciclos em sua decomposição como em (5.5).

5.2 Polos e $\mathcal{P}_n$

O objetivo desta seção é desenvolver um procedimento que nos permite obter $\mathcal{P}_n(X)$ a partir da corda de polos $\mathcal{O}_n$ e de $R_n(X)$. Queremos determinar $a_0, \dots, a_{n+1}$ de forma a ter $\mathcal{P}_n(X)$ como em (4.1). Sejam $\mathcal{O}_n = x_1, \dots, x_n$ e $R_n(X) = \frac{aX + b}{cX + d} \in \mathbb{F}_q(X)$. Inicialmente, vamos relacionar a, b, c e d com $\alpha_{n+1}, \beta_{n+1}, \alpha_n$ e β_n . Por definição, temos

$$\frac{\alpha_{n+1}x + \beta_{n+1}}{\alpha_n x + \beta_n} = R_n(x) = \frac{ax + b}{cx + d}, \quad \forall x \in \mathbb{F}_q \setminus \{x_n\},$$

donde

$$\alpha_{n+1}cx^2 + \alpha_{n+1}dx + \beta_{n+1}cx + \beta_{n+1}d = \alpha_n ax^2 + \alpha_n bx + \beta_n ax + \beta_n b, \quad \forall x \in \mathbb{F}_q \setminus \{x_n\}.$$

Assumindo $q > 3$, a igualdade acima implica

$$\alpha_{n+1}c = \alpha_n a, \quad (5.7)$$

$$\alpha_{n+1}d + \beta_{n+1}c = \alpha_n b + \beta_n a, \quad (5.8)$$

$$\beta_{n+1}d = \beta_n b. \quad (5.9)$$

Afirmamos que existem $t_1, t_2 \in \mathbb{F}_q$ tais que

$$a = t_1 \alpha_{n+1}, \quad c = t_1 \alpha_n, \quad b = t_2 \beta_{n+1} \quad \text{e} \quad d = t_2 \beta_n. \quad (5.10)$$

De fato, se $\alpha_n \neq 0$, tomemos $t_1 = c/\alpha_n$, de forma que $c = t_1 \alpha_n$ e, por (5.7), $a = t_1 \alpha_{n+1}$. Neste caso, se $\beta_n = 0$, então, pelo Lema 5.1.1, $\beta_{n+1} \neq 0$. Desse modo, escolhamos $t_2 = b/\beta_{n+1}$, donde $b = t_2 \beta_{n+1}$ e, por (5.9), $d = t_2 \beta_n$. Se $\beta_n \neq 0$, tomemos $t_2 = d/\beta_n$, de maneira que $d = t_2 \beta_n$ e, por (5.9), $b = t_2 \beta_{n+1}$. Por outro lado, se $\alpha_n = 0$ então, pelo Lema 5.1.1, $\alpha_{n+1}, \beta_n \neq 0$. Assim, escolhamos $t_1 = a/\alpha_{n+1}$ e $t_2 = d/\beta_n$, daí $d = t_2 \beta_n$ e $a = t_1 \alpha_{n+1}$. Por (5.7) e (5.9) temos $c = t_1 \alpha_n$ e $b = t_2 \beta_{n+1}$, respectivamente. Portanto, segue-se (5.10). Além do mais, $t_1 = t_2$. Com efeito, substituindo em (5.8) os valores de a, b, c e d obtidos em (5.10), vemos que

$$\begin{aligned} \alpha_{n+1} \beta_n t_2 + \beta_{n+1} \alpha_n t_1 &= \alpha_n \beta_{n+1} t_2 + \beta_n \alpha_{n+1} t_1 \\ \Rightarrow (\alpha_{n+1} \beta_n - \alpha_n \beta_{n+1})(t_2 - t_1) &= 0 \\ \Rightarrow t_1 &= t_2, \end{aligned}$$

onde a última implicação segue-se do fato de que $\alpha_{n+1} \beta_n - \alpha_n \beta_{n+1} \neq 0$ em virtude do Lema 5.1.1. Consequentemente, existe $t \in \mathbb{F}_q$ tal que

$$\alpha_{n+1} = ta, \quad \beta_{n+1} = tb, \quad \alpha_n = tc, \quad \beta_n = td. \quad (5.11)$$

Notemos que $t \neq 0$, pois caso contrário $\alpha_{n+1} = \beta_{n+1} = 0$, contradizendo o Lema 5.1.1. Com isso, podemos obter $a_0, \dots, a_{n+1}$ recursivamente. De fato, por (5.11) temos

$$x_n = \frac{-\beta_n}{\alpha_n} = \frac{-td}{tc} = \frac{-d}{c}.$$

No caso de $R_n(X)$ ser linear, vemos que $\alpha_n = 0$ e $x_n = \infty$. Seja $i \in \{3, 4, \dots, n+1\}$ com $x_{i-2} \neq \infty$. Então $\alpha_{i-2} \neq 0$ e

$$x_{i-2} = \frac{-\beta_{i-2}}{\alpha_{i-2}} \Rightarrow \beta_{i-2} = -x_{i-2}\alpha_{i-2}.$$

Por (5.1), $\alpha_{i-2} = \alpha_i - a_i\alpha_{i-1}$, donde $\beta_{i-2} = -x_{i-2}(\alpha_i - a_i\alpha_{i-1})$. Além disso, pelo Lema 5.1.1,

$$\alpha_{i-2}\beta_{i-1} - \beta_{i-2}\alpha_{i-1} \neq 0 \Rightarrow \beta_{i-1} + x_{i-2}\alpha_{i-1} \neq 0.$$

Usando novamente as relações em (5.1), obtemos

$$\begin{aligned} \beta_i &= a_i\beta_{i-1} + \beta_{i-2} = a_i\beta_{i-1} - x_{i-2}(\alpha_i - a_i\alpha_{i-1}) \\ \Rightarrow a_i\beta_{i-1} + a_ix_{i-2}\alpha_{i-1} &= \beta_i + x_{i-2}\alpha_i \\ \Rightarrow a_i &= \frac{\beta_i + x_{i-2}\alpha_i}{\beta_{i-1} + x_{i-2}\alpha_{i-1}}. \end{aligned}$$

Se $x_{i-2} = \infty$ então $\alpha_{i-2} = 0$. Pelo Lema 5.1.1, $\alpha_{i-1} \neq 0$. Por consequência, de $\alpha_i = a_i\alpha_{i-1} + \alpha_{i-2}$ obtemos $a_i = \alpha_i/\alpha_{i-1}$. Portanto, podemos calcular recursivamente

$$a_i, \quad \alpha_{i-2} = \alpha_i - a_i\alpha_{i-1} \quad \text{e} \quad \beta_{i-2} = \beta_i - a_i\beta_{i-1},$$

para $i = n+1, n, \dots, 3$. Notemos que, por (5.1), α_i e β_i será sempre obtido na forma tw , com $w \in \mathbb{F}_q$. Falta calcularmos o valor de t . Já que $\alpha_0 = 0$, $\beta_0 = 1$ e $\alpha_2 = a_2\alpha_1 + \alpha_0 = a_2\alpha_1$,

temos $a_2 = \alpha_2/\alpha_1$. Suponhamos que $\beta_2 = tw_2$ e $\beta_1 = tw_1$, com $w_1, w_2 \in \mathbb{F}_q$. Como $\beta_2 = a_2\beta_1 + \beta_0 = a_2\beta_1 + 1$, vem $t = (w_2 - a_2w_1)^{-1}$, com $a_2 = \alpha_2/\alpha_1$.

Exemplo 5.2.1. Consideremos o corpo $\mathbb{F}_{17}$. Tomemos $R_6(X)$ e $\mathcal{O}_6 = x_1, x_2, x_3, x_4, x_5, x_6$ definidos por

$$R_6(X) = \frac{3X + 1}{2X + 3} \quad \text{e} \quad \mathcal{O}_6 = 5, 3, 7, 10, 4, 7.$$

Nossos valores iniciais são

$$\alpha_7 = 3t, \quad \beta_7 = t, \quad \alpha_6 = 2t, \quad \beta_6 = 3t.$$

Assim,

$$a_7 = \frac{\beta_7 + x_5\alpha_7}{\beta_6 + x_5\alpha_6} = \frac{t + 12t}{3t + 8t} = 12, \quad \alpha_5 = \alpha_7 - a_7\alpha_6 = 13t, \quad \beta_5 = \beta_7 - a_7\beta_6 = 16t,$$

$$a_6 = \frac{\beta_6 + x_4\alpha_6}{\beta_5 + x_4\alpha_5} = \frac{3t + 20t}{16t + 130t} = 4, \quad \alpha_4 = \alpha_6 - a_6\alpha_5 = t, \quad \beta_4 = \beta_6 - a_6\beta_5 = 7t,$$

$$a_5 = \frac{\beta_5 + x_3\alpha_5}{\beta_4 + x_3\alpha_4} = \frac{16t + 6t}{7t + 7t} = 4, \quad \alpha_3 = \alpha_5 - a_5\alpha_4 = 9t, \quad \beta_3 = \beta_5 - a_5\beta_4 = 5t,$$

$$a_4 = \frac{\beta_4 + x_2\alpha_4}{\beta_3 + x_2\alpha_3} = \frac{7t + 3t}{5t + 10t} = 12, \quad \alpha_2 = \alpha_4 - a_4\alpha_3 = 12t, \quad \beta_2 = \beta_4 - a_4\beta_3 = 15t,$$

$$a_3 = \frac{\beta_3 + x_1\alpha_3}{\beta_2 + x_1\alpha_2} = \frac{5t + 11t}{15t + 9t} = 12, \quad \alpha_1 = \alpha_3 - a_3\alpha_2 = t, \quad \beta_1 = \beta_3 - a_3\beta_2 = 12t,$$

$$a_2 = \frac{\alpha_2}{\alpha_1} = 12 \quad \text{e} \quad t = (15 - 12 \cdot 12)^{-1} = (7)^{-1} = 5.$$

Portanto, $a_0 = \alpha_1 = 5$, $a_1 = \beta_1 = 9$ e o polinômio $\mathcal{P}_6(X)$ é dado por

$$\mathcal{P}_6(X) = ((((((5X + 9)^{15} + 12)^{15} + 12)^{15} + 12)^{15} + 4)^{15} + 4)^{15} + 12.$$

5.3 O Teorema Principal

Estamos, agora, em condições de provar o principal resultado deste capítulo.

Teorema 5.3.1. Seja $f(X)$ um polinômio de permutação sobre $\mathbb{F}_q$, com $q > 3$, representado como o produto de ciclos disjuntos

$$f(x) = (x_1^1 x_2^1 \cdots x_{\ell_1}^1)(x_1^2 x_2^2 \cdots x_{\ell_2}^2) \cdots (x_1^m x_2^m \cdots x_{\ell_m}^m)(x), \quad \forall x \in \mathbb{F}_q, \quad (5.12)$$

com $\ell_i \geq 2, \forall i = 1, \dots, m$. Defina $n = m + \sum_{i=1}^m \ell_i$. Se $n < (q-1)/2$ então $\text{Crk}(f) = n$.

Demonstração. Consideremos $R_n(X) = X$ e a corda de polos

$$\begin{aligned} \mathcal{O}_n = & x_{\ell_1}^1, x_{\ell_1-1}^1, \dots, x_1^1, x_{\ell_2}^2, x_{\ell_2-1}^2, \dots, x_1^2, \dots, x_{\ell_{m-1}}^{m-1}, x_{\ell_{m-1}-1}^{m-1}, \dots, x_1^{m-1}, \\ & x_{\ell_m}^m, x_{\ell_m-1}^m, \dots, x_1^m, x_1^{m-1}, x_1^{m-2}, \dots, x_1^1, \infty. \end{aligned}$$

Como vimos na Seção 5.2, podemos obter $\mathcal{P}_n(X)$ a partir de $\mathcal{O}_n$ e $R_n(X)$. Notemos que a quantidade de elementos na corda de polos $\mathcal{O}_n$ é $n = m + \sum_{i=1}^m \ell_i$. Visto que os ciclos em (5.12) são disjuntos, segue-se que os polos

$$x_{\ell_1}^1, x_{\ell_1-1}^1, \dots, x_1^1, x_{\ell_2}^2, x_{\ell_2-1}^2, \dots, x_1^2, \dots, x_{\ell_{m-1}}^{m-1}, x_{\ell_{m-1}-1}^{m-1}, \dots, x_1^{m-1}, x_{\ell_m}^m, x_{\ell_m-1}^m, \dots, x_1^m$$

são distintos. Utilizando o Lema 5.1.3 para estes polos e $\mathcal{P}_k$, onde $k = \sum_{j=1}^m \ell_j$, vemos que

$$\mathcal{P}_k(x) = (F_k(x_1^m) \cdots F_k(x_{\ell_m}^m) F_k(x_1^{m-1}) \cdots F_k(x_{\ell_{m-1}}^{m-1}) \cdots F_k(x_1^1) \cdots F_k(x_{\ell_1}^1)) F_k(x),$$

para todo $x \in \mathbb{F}_q$. Como x_1^{m-1} é um polo repetido, usando o Teorema 5.1.1(2) temos

$$\mathcal{P}_{k+1}(x) = (F_{k+1}(x_1^{m-1}) \cdots F_{k+1}(x_{\ell_1}^1)) (F_{k+1}(x_1^m) \cdots F_{k+1}(x_{\ell_m}^m)) F_{k+1}(x) \quad \forall x \in \mathbb{F}_q.$$

Desde que x_1^{m-2} é também um polo repetido, o ciclo que contém $F_{k+1}(x_1^{m-2})$ se decompõe em dois pelo Teorema 5.1.1(2). Continuando dessa maneira, após a $(m-1)$ -ésima etapa e observando que $k+m-1=n-1$, temos

$$\mathcal{P}_{n-1}(x) = (F_{n-1}(x_1^1) \cdots F_{n-1}(x_{\ell_1}^1)) \cdots (F_{n-1}(x_1^m) \cdots F_{n-1}(x_{\ell_m}^m)) F_{n-1}(x), \quad \forall x \in \mathbb{F}_q.$$

Já que $x_n = \infty$ e $F_n(x) = x$ para todo $x \in \mathbb{F}_q$, pelo Teorema 5.1.2 temos

$$\begin{aligned} \mathcal{P}_n(x) &= (F_n(x_1^1) \cdots F_n(x_{\ell_1}^1)) \cdots (F_n(x_1^m) \cdots F_n(x_{\ell_m}^m)) F_n(x) \\ &= (x_1^1 \cdots x_{\ell_1}^1) \cdots (x_1^m \cdots x_{\ell_m}^m)(x) = f(x), \quad \forall x \in \mathbb{F}_q. \end{aligned}$$

Afirmamos que este n é o menor inteiro não negativo ℓ que satisfaz $\mathcal{P}_\ell(x) = f(x)$ e $R_\ell(x) = x$ para todo $x \in \mathbb{F}_q$. De fato, suponhamos que exista um $\mathcal{P}_v(X)$ tal que

$$\mathcal{P}_v(x) = (x_1^1 \cdots x_{\ell_1}^1) \cdots (x_1^m \cdots x_{\ell_m}^m)(x)$$

e $R_v(x) = x$ para todo $x \in \mathbb{F}_q$. Já que $\mathcal{P}_v(x_i^j) \neq R_v(x_i^j)$ para todos os índices i, j , concluímos que $\mathcal{O}_v$ contém todos os k elementos distintos x_i^j . Além disso, $x_v = \infty$ pois $R_v(X)$ é linear. Finalmente, como $\mathcal{P}_v$ tem m ciclos em sua decomposição, pelo Corolário 5.1.1 concluímos que $\mathcal{O}_v$ deve possuir no mínimo $m-1$ polos repetidos diferentes de ∞ . Portanto, se $\mathcal{O}_v = x_1, \dots, x_v$ é a corda de polos, devemos ter

$$v \geq k + m - 1 + 1 = k + m = m + \sum_{j=1}^m \ell_j = n.$$

Agora, suponhamos que $n < (q-1)/2$. Vamos admitir, por absurdo, que exista um $\mathcal{P}_m(X)$ com $m < n$ tal que

$$\mathcal{P}_m(x) = \mathcal{P}_n(x), \quad \forall x \in \mathbb{F}_q.$$

Então, como vimos no parágrafo precedente, as funções racionais $R_m(X)$ e $R_n(X)$ são distintas. Desde que, para $\ell = m, n$,

$$\mathcal{P}_\ell(x) = R_\ell(x), \quad \forall x \in \mathbb{F}_q \setminus \mathcal{O}_\ell,$$

as equações $\mathcal{P}_m(X) = R_m(X)$ e $\mathcal{P}_n(X) = R_n(X)$ têm, no mínimo, $q - m$ e $q - n$ soluções em $\mathbb{F}_q$, respectivamente. Visto que $\mathcal{P}_m(x) = \mathcal{P}_n(x)$ para todo $x \in \mathbb{F}_q$, a equação $R_m(X) = R_n(X)$ tem no mínimo $q - (m + n)$ soluções em $\mathbb{F}_q$. Além disso, a igualdade $R_m(X) = R_n(X)$ gera uma equação do segundo grau, donde $R_m(x) = R_n(x)$ vale para, no máximo, dois valores de x em $\mathbb{F}_q$. Portanto, $q - (m + n) \leq 2$. Uma vez que $m < n$, temos

$$q - 2n < q - (m + n) \leq 2 \Rightarrow n > (q - 2)/2 \Rightarrow n \geq (q - 1)/2,$$

o que é uma contradição, pois, por hipótese, $n < (q - 1)/2$. Assim, se $n < (q - 1)/2$ então $\text{Crk}(f) = n$.

□

Na demonstração acima, obtemos um polinômio $\mathcal{P}_n(X)$ que representa $f(X)$. Por consequência, $\text{Crk}(f) \leq n$. Diante disso, considerando $f(X)$ um polinômio de permutação sobre $\mathbb{F}_{17}$ representado por $(1\ 2\ 3)(5\ 7\ 9) \in S_{17}$, temos $q = 17$, e o valor de n no Teorema 5.3.1 é $2 + 3 + 3 = 8 = (q - 1)/2$. Desse modo, podemos apenas concluir que $\text{Crk}(f) \leq 8$. Por outro lado, se $f(X) \in \mathbb{F}_{17}[X]$ é um polinômio de permutação identificado por $(1\ 3\ 5\ 7\ 9) \in S_{17}$, então $\text{Crk}(f) = 6$, já que $n = 6 < 8$ para esta permutação. Além disso, vale notar que a prova anterior mostra que $\mathcal{P}_n(X)$ pode ser obtido explicitamente a partir da identificação de $f(X)$ como um produto de ciclos disjuntos, pois a corda de polos e a função racional $R_n(X)$ são dadas. O exemplo a seguir ilustra este fato.

Exemplo 5.3.1. Seja $f(X)$ um polinômio de permutação sobre $\mathbb{F}_q$, com $q > 3$, tal que

$f(x) = (a \ b)(x)$ para todo $x \in \mathbb{F}_q$, com a e b elementos distintos de $\mathbb{F}_q$. Procedendo como na demonstração do Teorema 5.3.1, consideremos $R_3(X) = X$ e a corda de polos $\mathcal{O}_3 = b, a, \infty$, de modo que $x_1 = b, x_2 = a$ e $x_3 = \infty$. Por (5.11), vemos que $\alpha_4 = \beta_3 = t$ e $\alpha_3 = \beta_4 = 0$ para algum $t \in \mathbb{F}_q^*$. Dessa forma,

$$a_4 = \frac{\beta_4 + x_2\alpha_4}{\beta_3 + x_2\alpha_3} = \frac{at}{t} = a, \quad \alpha_2 = \alpha_4 - a_4\alpha_3 = t, \quad \beta_2 = \beta_4 - a_4\beta_3 = -at,$$

$$a_3 = \frac{\beta_3 + x_1\alpha_3}{\beta_2 + x_1\alpha_2} = \frac{t}{-at + bt} = \frac{1}{b-a},$$

$$\alpha_1 = \alpha_3 - a_3\alpha_2 = \frac{-t}{b-a}, \quad \beta_1 = \beta_3 - a_3\beta_2 = t \left(1 + \frac{a}{b-a}\right),$$

$$a_2 = \frac{\alpha_2}{\alpha_1} = a - b \quad \text{e} \quad t = \left(-a - (a-b) \left(1 + \frac{a}{b-a}\right)\right)^{-1} = \frac{1}{b-a}.$$

Assim,

$$a_1 = \beta_1 = \frac{1}{b-a} \left(1 + \frac{a}{b-a}\right) = \frac{b}{(b-a)^2}$$

e

$$a_0 = \alpha_1 = -\frac{1}{b-a} \left(\frac{1}{b-a}\right) = \frac{-1}{(b-a)^2}.$$

Portanto,

$$\mathcal{P}_3(X) = \left(\left(\left(\frac{-X}{(b-a)^2} + \frac{b}{(b-a)^2} \right)^{q-2} + a - b \right)^{q-2} + \frac{1}{b-a} \right)^{q-2} + a.$$

Temos, então, explicitamente um polinômio $\mathcal{P}_3(X)$ que representa $f(X)$ e $Crk(f) \leq 3$. Além disso, se $q > 7$ então $(q-1)/2 > 3$, donde, pelo Teorema 5.3.1, $Crk(f) = 3$.

Para mais um exemplo de aplicação desse teorema, consideremos o polinômio

$$f(X) = 18X^{31} - 18X^{19} - 18X^{13} + 19X \in \mathbb{F}_{37}[X].$$

Calculando os valores de f em $\mathbb{F}_{37}$, vemos que f corresponde à permutação

$$(2\ 15\ 20)(5\ 13\ 19)(17\ 35\ 22)(18\ 32\ 24) \in S_{37}.$$

Desse modo, para este caso, o valor de n no Teorema 5.3.1 é $16 < 18 = (q - 1)/2$. Logo, $Crk(f) = 16$.

É importante notar que a hipótese $n < (q - 1)/2$ é fundamental para o Teorema 5.3.1. Com efeito, temos casos onde $n \geq (q - 1)/2$ mas $Crk(f) \neq n$. Por exemplo, $f(X) = X^5$ é um polinômio de permutação sobre $\mathbb{F}_7$ com posto de Carlitz 1. No entanto, observando os valores de f em $\mathbb{F}_7$, vemos que

$$f(x) = (2\ 4)(3\ 5)(x), \quad \forall x \in \mathbb{F}_7,$$

de modo que $n = 2 + 2 + 2 = 6 \neq Crk(f)$. Para um exemplo menos trivial, consideremos o polinômio

$$f(X) = 5X^8 + 5X^7 + 5X^6 + 4X^4 + 2X^3 + 5X^2 + 9X + 5 \in \mathbb{F}_{11}[X].$$

Veremos no Capítulo 7 que $f(X)$ é um polinômio de permutação sobre $\mathbb{F}_{11}$ com posto de Carlitz 5. Entretanto, os valores de f em $\mathbb{F}_{11}$ nos indicam que

$$f(x) = (0\ 5\ 4\ 10\ 8\ 2\ 9\ 3\ 1\ 7\ 6)(x), \quad \forall x \in \mathbb{F}_{11},$$

de forma que $n = 1 + 11 = 12 \neq Crk(f)$. Logo, a conclusão do Teorema 5.3.1 não vale para esses casos.

Capítulo 6

Posto de Carlitz de uma família de polinômios de permutação

Em 2020, Z. Ding obteve em [26] um resultado bem útil para calcular o posto de Carlitz de polinômios de permutação. Utilizando tal resultado e as ferramentas da Teoria de Grupos, conseguimos obter o posto de Carlitz de uma família de polinômios de permutação.

6.1 O Resultado Principal

Seja C um conjunto finito. Consideremos uma permutação $f : C \rightarrow C$ de ordem m e $G = \langle f \rangle$, o subgrupo de S_C gerado por f . Então G age no conjunto C pela ação $\psi : G \times C \rightarrow C$ definida por $\psi(f^i, x) = f^i(x)$ para todo $1 \leq i \leq m$ e $x \in C$. Dizemos que f tem uma órbita não trivial se existe uma órbita

$$\mathcal{O}(x) = \{f^i(x) : 1 \leq i \leq m\},$$

tal que $|\mathcal{O}(x)| > 1$. Notemos que se f fixa x então $|\mathcal{O}(x)| = 1$, e se f move x , $|\mathcal{O}(x)| > 1$.

O resultado abaixo pode ser encontrado no Teorema 11 de [26].

Teorema 6.1.1. Seja $f(X)$ um polinômio de permutação sobre $\mathbb{F}_q$. Suponha que $f = \mu \circ \sigma$, onde μ é uma função racional de grau um, e σ é uma permutação de $\mathbb{P}^1(\mathbb{F}_q)$ que move s pontos em $\mathbb{F}_q$ e tem t órbitas não triviais. Defina

$$n = \begin{cases} s + t, & \text{se } \sigma(\infty) = \infty, \\ s + t - 1, & \text{se } \sigma(\infty) \neq \infty \end{cases}.$$

Então o posto de Carlitz de $f(X)$ é no máximo n . Além disso, se $q \geq n + s + 2$ então $Crk(f) = n$.

Corolário 6.1.1. Seja $f(X)$ um polinômio de permutação sobre $\mathbb{F}_q$. Suponha que a permutação f move s pontos e tem t órbitas não triviais. Se $q \geq 2s + t + 2$ então $Crk(f) = s + t$.

Demonstração. Consideremos a função racional $\mu(X) = X$ e a permutação σ de $\mathbb{P}^1(\mathbb{F}_q)$ definida por

$$\sigma(a) = \begin{cases} f(a), & \text{se } a \in \mathbb{F}_q \\ \infty, & \text{se } a = \infty \end{cases}.$$

Por conseguinte, $f = \mu \circ \sigma$, σ move s pontos e tem t órbitas não triviais. Se $q \geq 2s + t + 2$ então, pelo Teorema 6.1.1, $Crk(f) = s + t$. $\square$

Combinando o Corolário 6.1.1 com o Lema de Burnside, podemos obter o posto de Carlitz de uma família de polinômios de permutação. O próximo teorema ilustra este fato.

Teorema 6.1.2. Seja p um primo ímpar. Considere o corpo $\mathbb{F}_q$ onde $q \equiv 1 \pmod{2p^2}$. Então o polinômio

$$g(X) = X^{\frac{q(p+2)+p-2}{2p}} - X^{\frac{q+1}{2}} - X^{\frac{q+p-1}{p}} - X \in \mathbb{F}_q[X]$$

é um polinômio de permutação sobre $\mathbb{F}_q$ com $Crk(g) = \frac{(p^2 - 1)(q - 1)}{2p^2}$.

Demonstração. Consideremos o polinômio $f(X) = ag(X)$, onde $a = -2^{-1}$. Assim, $g(X)$ é um polinômio de permutação sobre $\mathbb{F}_q$ se, e somente se, $f(X)$ o é. Além disso, $Crk(f) = Crk(g)$ pelo o que vimos na Seção 4.2. Logo, basta provarmos que $f(X)$ é um polinômio de permutação sobre $\mathbb{F}_q$ com posto de Carlitz igual a $\frac{(p^2 - 1)(q - 1)}{2p^2}$.

Começamos mostrando que $f(X)$ é um polinômio de permutação sobre $\mathbb{F}_q$.

Seja $F = \{\alpha \in \mathbb{F}_q : f(\alpha) = \alpha\}$ o conjunto de pontos fixos de f . Observemos que

$$f(X) = aX(X^{\frac{q-1}{p}} - 1)(X^{\frac{q-1}{2}} - 1) + X.$$

Por conseguinte, temos

$$F = \{\alpha \in \mathbb{F}_q : \alpha = 0, \alpha^{\frac{q-1}{p}} = 1 \text{ ou } \alpha^{\frac{q-1}{2}} = 1\}.$$

Usando a Proposição 2.2.1, as equações $X^{\frac{q-1}{p}} = 1$, $X^{\frac{q-1}{2}} = 1$ e $X^{\frac{q-1}{2p}} = 1$ possuem, respectivamente, $(q-1)/p$, $(q-1)/2$ e $(q-1)/2p$ soluções em $\mathbb{F}_q^*$. Além disso, utilizando **(A1)**, podemos concluir que α é uma solução comum das equações $X^{\frac{q-1}{p}} = 1$ e $X^{\frac{q-1}{2}} = 1$ se, e somente se, é uma solução de $X^{\frac{q-1}{2p}} = 1$, uma vez que $((q-1)/p, (q-1)/2) = (q-1)/2p$. Portanto, o número de pontos fixos de f é

$$1 + \frac{q-1}{p} + \frac{q-1}{2} - \frac{q-1}{2p} = \frac{q(p+1) + p - 1}{2p}.$$

Por consequência, f move $q - \frac{q(p+1)+p-1}{2p} = \frac{(p-1)(q-1)}{2p}$ pontos, isto é,

$$|\mathbb{F}_q \setminus F| = \frac{(p-1)(q-1)}{2p}. \quad (6.1)$$

Seja $\alpha \in \mathbb{F}_q \setminus F$. Então $\alpha^{\frac{q-1}{2}}, \alpha^{\frac{q-1}{p}} \neq 1$. Já que $\alpha^{\frac{q-1}{2}}$ é solução de $X^2 = 1$, devemos ter $\alpha^{\frac{q-1}{2}} = -1$. Desde que $a = -2^{-1}$, temos

$$f(\alpha) = \alpha[(a\alpha^{\frac{q-1}{p}} - a)(\alpha^{\frac{q-1}{2}} - 1) + 1] = \alpha(-2a\alpha^{\frac{q-1}{p}} + 2a + 1) = \alpha^{\frac{q+p-1}{p}}. \quad (6.2)$$

Como $\alpha \neq 0$, $f(\alpha) = \alpha^{\frac{q+p-1}{p}} \neq 0$. Além disso, desde que $(q-1)/2p, (q-1)/p^2 \in \mathbb{Z}$, temos

$$f(\alpha)^{\frac{q-1}{2}} = \left(\alpha^{\frac{q-1}{p}+1}\right)^{\frac{q-1}{2}} = \alpha^{\frac{q-1}{2}}(\alpha^{q-1})^{\frac{q-1}{2p}} = \alpha^{\frac{q-1}{2}} = -1$$

e

$$f(\alpha)^{\frac{q-1}{p}} = \left(\alpha^{\frac{q-1}{p}+1}\right)^{\frac{q-1}{p}} = \alpha^{\frac{q-1}{p}}(\alpha^{q-1})^{\frac{q-1}{p^2}} = \alpha^{\frac{q-1}{p}} \neq 1.$$

Assim, $f(\alpha) \notin F$. Por consequência, temos

$$f(\mathbb{F}_q \setminus F) \subset \mathbb{F}_q \setminus F.$$

Escreva $q = 2p^2k + 1$ para algum inteiro positivo k . Desse modo,

$$\left(\frac{q+p-1}{p}, q-1 \right) = (2pk+1, 2p^2k) = 1.$$

Logo, f define uma função injetiva de $\mathbb{F}_q \setminus F$ em $\mathbb{F}_q \setminus F$ e, portanto, uma bijeção. Visto que também $f(F) = F$, concluímos que f define uma permutação de $\mathbb{F}_q$. Portanto, $f(X)$ é um polinômio de permutação sobre $\mathbb{F}_q$.

Agora, vamos determinar o posto de Carlitz de $f(X)$. Começamos determinando a ordem de f como um elemento de S_q .

Temos que

$$f^n(\alpha) = \alpha^{\left(\frac{q+p-1}{p}\right)^n},$$

para todo $\alpha \in \mathbb{F}_q \setminus F$ e $n \geq 1$. Seja d a ordem de f pensado como um elemento de S_q . Seja ξ um gerador de $\mathbb{F}_q^*$. Temos que d é o menor inteiro positivo n tal que $f^n(\xi^m) = \xi^m$ para todo $1 \leq m \leq q-1$. Desde que $\text{ord}(\xi) = q-1$, temos $\xi^{\frac{q-1}{2}} \neq 1$ e $\xi^{\frac{q-1}{p}} \neq 1$. Em vista disso, $\xi \in \mathbb{F}_q \setminus F$. Dessa forma,

$$f^d(\xi) = \xi \Leftrightarrow \xi^{\left(\frac{q+p-1}{p}\right)^d} = \xi \Leftrightarrow \xi^{\left(\frac{q+p-1}{p}\right)^d - 1} = 1 \Leftrightarrow q-1 \mid \left(\left(\frac{q+p-1}{p} \right)^d - 1 \right).$$

Lembrando que $q = 2p^2k + 1$, temos

$$\begin{aligned}
q - 1 \mid \left(\left(\frac{q + p - 1}{p} \right)^d - 1 \right) &\Leftrightarrow 2p^2k \mid ((2pk + 1)^d - 1) \\
&\Leftrightarrow 2p^2k \mid \sum_{i=0}^{d-1} \binom{d}{i} (2pk)^{d-i} \\
&\Leftrightarrow 2p^2k \mid \binom{d}{d-1} 2pk \\
&\Leftrightarrow p \mid \binom{d}{d-1} = d.
\end{aligned}$$

Assim, a ordem de f é um múltiplo de p . Veremos que $d = p$. De fato, pelas equivalências acima,

$$\xi^{\left(\frac{q+p-1}{p}\right)^d} = \xi \Leftrightarrow p \mid d.$$

Logo, se $\xi^m \in \mathbb{F}_q \setminus F$ então

$$f^p(\xi^m) = \xi^{\left(\frac{q+p-1}{p}\right)^p m} = \xi^m.$$

Se $\xi^m \in F$ então $f(\xi^m) = \xi^m$, donde $f^p(\xi^m) = \xi^m$. Portanto, $d = p$. Além disso, temos o seguinte fato:

(a) Para todo $1 \leq i \leq p - 1$, $f^i(\alpha) \neq \alpha$ qualquer que seja $\alpha \in \mathbb{F}_q \setminus F$.

Com efeito, se $f^i(\alpha) = \alpha$ para algum $1 \leq i \leq p - 1$ e $\alpha \in \mathbb{F}_q \setminus F$, então

$$\alpha^{\left(\frac{q+p-1}{p}\right)^i} = \alpha \Rightarrow \alpha^{(2pk+1)^i} = \alpha \Rightarrow \alpha^{(2pk+1)^i - 1} = 1.$$

Como

$$((2pk + 1)^i - 1, q - 1) = ((2pk + 1)^i - 1, 2p^2k) = 2pk,$$

concluimos que $\alpha^{2kp} = 1$, de sorte que $\alpha^{\frac{q-1}{p}} = 1$, uma contradição pois $\alpha \notin F$.

Queremos utilizar o Corolário 6.1.1 para determinar o posto de Carlitz de $f(X)$. Para

isso, devemos determinar o número de órbitas não triviais de f , que será obtido usando o Lema de Burnside. Lembremos que se G é um grupo agindo num conjunto C e $\tau \in G$, $Fix(\tau)$ denota o número de elementos em C fixados por τ .

Consideremos $C = \mathbb{F}_q \setminus F$. Por (6.1),

$$|C| = \frac{(p-1)(q-1)}{2p}.$$

Além disso, como $f(C) = C$, f define uma permutação de C em C , a qual podemos considerá-la como um elemento do grupo simétrico S_C . Seja $G = \langle f \rangle$ o subgrupo de S_C gerado por f . Então G age no conjunto C pela ação $\psi : G \times C \rightarrow C$ definida por $\psi(f^j, x) = f^j(x)$ para todo $1 \leq j \leq p-1$ e $x \in C$. Já que a ordem de f é p , temos $|G| = p$. Pelo fato **(a)**, $Fix(f^j) = 0$, para todo $j = 1, 2, \dots, p-1$. Além disso, $Fix(id) = |C|$. Então, pelo Teorema 1.2.1, concluímos que o número N de órbitas de C é

$$N = \frac{(p-1)(q-1)}{2p^2}.$$

Uma vez que os elementos de C são exatamente aqueles de $\mathbb{F}_q$ que não são fixados por f , segue-se que N é o número de órbitas não triviais de f (pensado como um elemento de S_q). Por conseguinte, na notação do Corolário 6.1.1, vemos que

$$t = \frac{(p-1)(q-1)}{2p^2} \quad \text{e} \quad s = \frac{(p-1)(q-1)}{2p}.$$

Vamos mostrar que $q \geq 2s + t + 2$. Já que $q-1 = 2p^2k$, onde k é um inteiro positivo, temos

$t = k(p - 1)$ e $s = pk(p - 1)$. Logo,

$$\begin{aligned}
 2s + t + 2 &= 2pk(p - 1) + k(p - 1) + 2 \\
 &= 2p^2k - pk - k + 2 \\
 &= (2p^2k + 1) - k(p + 1) + 1 \\
 &< 2p^2k + 1 = q.
 \end{aligned}$$

Portanto, pelo Corolário 6.1.1, obtemos

$$Crk(f) = s + t = \frac{(p^2 - 1)(q - 1)}{2p^2}.$$

□

Exemplo 6.1.1. Consideremos o corpo $\mathbb{F}_q$ onde $q = 163351$. Temos $q - 1 = 2 \cdot 3^3 \cdot 5^2 \cdot 11^2$. Escolhendo $p = 3, 5, 11$ e usando o Teorema 6.1.2, concluimos que os polinômios

$$\begin{aligned}
 f(X) &= X^{136126} - X^{81676} - X^{54451} - X, \\
 g(X) &= X^{114346} - X^{81676} - X^{32671} - X, \\
 h(X) &= X^{96526} - X^{81676} - X^{14851} - X
 \end{aligned}$$

são polinômios de permutação sobre $\mathbb{F}_q$ com $Crk(f) = 72600$, $Crk(g) = 78408$ e $Crk(h) = 81000$.

Capítulo 7

Diferença entre polinômios de permutação

Um polinômio $f(X) \in \mathbb{F}_q[X]$ é dito ser um mapa polinomial completo se $f(X)$ e $f(X) + X$ são polinômios de permutação sobre $\mathbb{F}_q$. Em 1990, Cohen provou a conjectura de Chowla e Zassenhaus, a qual afirma que se $p > (d^2 - 3d + 4)^2$, então não existe um mapa polinomial completo $f(X)$ de grau $d \geq 2$ (veja Teorema 2 de [20]). Mais tarde em 1995, Cohen, Mullen and Shiue generalizaram significativamente este resultado, considerando diferenças entre polinômios de permutação. Mais precisamente, eles mostraram que se $f(X)$ e $f(X) + g(X)$ são polinômios de permutação sobre $\mathbb{F}_p$, onde $d = \deg f \geq 2$ e $p > (d^2 - 3d + 4)^2$, então o grau k de $g(X)$ satisfaz $k \geq 3d/5$, exceto pelo caso onde g é constante (veja Teorema 2 de [19]). Neste capítulo, assumindo que $f(X)$ e $f(X) + g(X)$ são polinômios de permutação em $\mathbb{F}_q[X]$, apresentamos uma cota inferior para k em termos de q e do posto de Carlitz de $f(X)$. Isso também nos proporciona uma ferramenta útil para obter o posto de Carlitz de certos polinômios, como veremos nos exemplos. Este capítulo é baseado no artigo [16].

7.1 Uma relação entre o posto de Carlitz e o grau da diferença entre polinômios de permutação

Consideremos $q \geq 3$. Seja $\mathcal{L}_1$ o conjunto de todos os polinômios de permutação $f(X)$ sobre $\mathbb{F}_q$ com $\text{Crk}(f) = n \geq 1$ e $\alpha_n \neq 0$, onde α_n é definido em (5.1).

Definição 7.1.1. Uma função racional $\ell(X)/t(X) \in \mathbb{F}_q(X)$ é chamada excepcional sobre $\mathbb{F}_q$ se o polinômio $F_{\ell/t}(X, Y) \in \mathbb{F}_q[X, Y]$ definido por

$$F_{\ell/t}(X, Y) = \frac{t(Y)\ell(X) - t(X)\ell(Y)}{X - Y}$$

não possui fator absolutamente irredutível em $\mathbb{F}_q[X, Y]$.

Usaremos mais adiante o seguinte teorema, provado por Stephen D. Cohen em [21].

Teorema 7.1.1. ([21], Teorema 5) Se uma função racional $\ell(X)/t(X) \in \mathbb{F}_q(X)$ é excepcional então a função associada $\ell/t : c \mapsto \ell(c)/t(c)$ define uma permutação de $\mathbb{F}_q$.

Lema 7.1.1. Sejam $h(X) \in \mathbb{F}_q[X]$ um polinômio de grau $1 \leq k < q - 1$ e $c \in \mathbb{F}_q^*$. Se M é o número de soluções $(x, y) \in \mathbb{F}_q^* \times \mathbb{F}_q^*$, com $x \neq y$, da equação

$$XY \frac{h(X) - h(Y)}{X - Y} + c = 0$$

então

$$M \geq q + 1 - k(k - 1)\sqrt{q} - (\nu + k + 2),$$

onde $\nu = (k, q - 1)$.

Demonstração. Consideremos a função racional $\ell(X)/t(X) = (Xh(X) - c)/X$. Então

$$\begin{aligned} F_{\ell/t}(X, Y) &= \frac{t(Y)\ell(X) - t(X)\ell(Y)}{X - Y} = \frac{Y(Xh(X) - c) - X(Yh(Y) - c)}{X - Y} \\ &= \frac{XY(h(X) - h(Y)) + c(X - Y)}{X - Y} = XY \frac{h(X) - h(Y)}{X - Y} + c. \end{aligned}$$

Assim, M é o número de soluções $(x, y) \in \mathbb{F}_q^* \times \mathbb{F}_q^*$, com $x \neq y$, da equação $F_{\ell/t}(X, Y) = 0$.

Notemos que $\deg F_{\ell/t}(X, Y) = k + 1$.

Como $t(0) = 0$, concluímos pelo Teorema 7.1.1 que $\ell(X)/t(X)$ não é excepcional, donde existe um fator absolutamente irredutível $w(X, Y)$ sobre $\mathbb{F}_q$ de $F_{\ell/t}(X, Y)$. Seja $d = \deg w$. Temos $d \leq k + 1$. Consideremos a curva algébrica plana $\mathcal{X}$ definida pela equação homogênea $w^*(X, Y, Z) = 0$. Lembrando que $w^*(X, Y, Z) = Z^d w(X/Z, Y/Z)$, o Teorema 3.2.2 nos diz que o número de soluções $[x : y : z] \in \mathbb{P}^2(\mathbb{F}_q)$ da equação $w^*(X, Y, Z) = 0$, denotado por

$N(\mathcal{X})$, satisfaz

$$N(\mathcal{X}) \geq q + 1 - (d - 1)(d - 2)\sqrt{q} \geq q + 1 - k(k - 1)\sqrt{q}.$$

Queremos obter uma cota inferior para o número de soluções $(x, y) \in \mathbb{F}_q^* \times \mathbb{F}_q^*$, com $x \neq y$, da equação $w(X, Y) = 0$. Para isso, vamos subtrair da cota acima o número de soluções em $\mathbb{P}^2(\mathbb{F}_q)$ da equação $w^*(X, Y, Z) = 0$ da forma $[x : y : 1]$ com $xy = 0$, $[x : y : 0]$, e $[x : y : z]$ com $x = y$. Se $xy = 0$ então $F_{\ell/t}(x, y) = c \neq 0$. Desse modo, o elemento $[x : y : 1]$ satisfaz $w^*(x, y, 1) = w(x, y) \neq 0$, desde que $w(X, Y) \mid F_{\ell/t}(X, Y)$. Portanto, não há soluções de $w^*(X, Y, Z) = 0$ da forma $[x : y : 1]$ com $xy = 0$.

Agora, vamos calcular o número de soluções de $w^*(X, Y, Z) = 0$ da forma $[x : y : 0] \in \mathbb{P}^2(\mathbb{F}_q)$. Dado que $w(X, Y) \mid F_{\ell/t}(X, Y)$, temos

$$w^*(X, Y, Z) \mid F_{\ell/t}^*(X, Y, Z),$$

em virtude da Proposição 3.1.2. Logo, todo zero de $w^*(X, Y, Z)$ é um zero de $F_{\ell/t}^*(X, Y, Z)$. Estimemos, então, o número de zeros de $F_{\ell/t}^*(X, Y, Z)$ da forma $[x : y : 0]$ em $\mathbb{P}^2(\mathbb{F}_q)$. Observemos que

$$\begin{aligned} F_{\ell/t}^*(X, Y, Z) &= Z^{k+1}F_{\ell/t}(X/Z, Y/Z) \\ &= Z^{k+1}(X/Z)(Y/Z)\frac{h(X/Z) - h(Y/Z)}{X/Z - Y/Z} + Z^{k+1}c \\ &= XY\frac{Z^k(h(X/Z) - h(Y/Z))}{X - Y} + Z^{k+1}c. \end{aligned}$$

Se aX^k e aY^k são os termos de maior grau de $h(X)$ e $h(Y)$, respectivamente, então os únicos termos de $Z^k(h(X/Z) - h(Y/Z))$ que não possuem o fator Z são aX^k e $-aY^k$. Dessa

maneira, se $[x : y : 0] \in \mathbb{P}^2(\mathbb{F}_q)$ é um zero de $F_{\ell/t}^*(X, Y, Z)$ então

$$0 = F_{\ell/t}^*(x, y, 0) = xy \frac{a(x^k - y^k)}{x - y} \Rightarrow xy \frac{x^k - y^k}{x - y} = 0.$$

Conseqüentemente, $[x : y : 0] = [0 : 1 : 0], [1 : 0 : 0]$ ou $x^k = y^k$ com $x, y \in \mathbb{F}_q^*$. A última igualdade significa $(x/y)^k = 1$, o que equivale a $x = ty$ para algum $t \in \mathbb{F}_q$ com $t^k = 1$. Desse modo, as soluções $[x : y : 0] \in \mathbb{P}^2(\mathbb{F}_q)$ de $(X/Y)^k = 1$ são da forma $[ty : y : 0] = [t : 1 : 0]$ onde $t \in \mathbb{F}_q$ e $t^k = 1$. Pela Proposição 2.2.1, há $(k, q - 1) = \nu$ soluções em $\mathbb{F}_q^*$ da equação $T^k = 1$. Portanto, o número de soluções em $\mathbb{P}^2(\mathbb{F}_q)$ do tipo $[x : y : 0]$ para a equação $(X/Y)^k = 1$ é ν . Assim sendo, existem no máximo $\nu + 2$ soluções para a equação $w^*(X, Y, Z) = 0$ da forma $[x : y : 0] \in \mathbb{P}^2(\mathbb{F}_q)$.

Por outro lado, $\mathcal{X}$ e a curva algébrica plana definida pela equação homogênea $X - Y = 0$ não possuem componentes em comum, uma vez que $w(X, Y)$ é absolutamente irredutível sobre $\mathbb{F}_q$. Por conseguinte, como o polinômio $w(X, Y)$ tem grau no máximo $k + 1$, o Teorema 3.2.1 nos garante que há no máximo $k + 1$ pontos $[x : y : z] \in \mathbb{P}^2(\mathbb{F}_q)$ tais que $w^*(x, y, z) = 0$ e $x = y$. Notemos que o ponto $[1 : 1 : 0]$ já foi contabilizado no parágrafo anterior. Logo, se este ponto é solução de $w^*(X, Y, Z) = 0$, então ele está sendo contabilizado mais uma vez. Se ele não é solução de $w^*(X, Y, Z) = 0$, devemos retirá-lo como solução contabilizada no parágrafo anterior. Em ambos os casos, o número de pontos $[x : y : z] \in \mathbb{P}^2(\mathbb{F}_q)$ de $\mathcal{X}$ tais que $z = 0$ ou $x = y$ é no máximo $(\nu + 2) + (k + 1) - 1 = \nu + k + 2$. Portanto,

$$M \geq q + 1 - k(k - 1)\sqrt{q} - (\nu + k + 2).$$

□

Com isso, podemos provar o principal resultado deste capítulo.

Teorema 7.1.2. Sejam $f(X)$ e $f(X) + g(X)$ polinômios de permutação sobre $\mathbb{F}_q$, onde

$Crk(f) = n \geq 1$, $f(X) \in \mathcal{L}_1$, e o grau k de $g(X)$ satisfaz $1 \leq k < q - 1$. Então

$$nk + k(k - 1)\sqrt{q} \geq q - \nu - n,$$

onde $\nu = (k, q - 1)$.

Demonstração. Como $f(X) \in \mathcal{L}_1$, vemos que

$$f(z) = R_n(z) = \frac{\alpha_{n+1}z + \beta_{n+1}}{\alpha_n z + \beta_n}, \quad \forall z \in \mathbb{F}_q \setminus \mathcal{O}_n,$$

onde $\alpha_n \neq 0$. Sejam $a = \alpha_{n+1}/\alpha_n$, $b = \beta_{n+1}/\alpha_n$ e $d = \beta_n/\alpha_n$. Dessa forma,

$$R_n(Z) = \frac{aZ + b}{Z + d}.$$

Além disso, usando o Lema 5.1.1 temos

$$ad - b = \frac{\alpha_{n+1}\beta_n - \alpha_n\beta_{n+1}}{\alpha_n^2} \neq 0.$$

Seja $G_n(Z) = R_n(Z) + g(Z)$. Visto que $f(X) + g(X)$ é um polinômio de permutação sobre $\mathbb{F}_q$, a função induzida por G_n sobre $\mathbb{F}_q \setminus \mathcal{O}_n$ é injetiva. Defina

$$H_n(X) = G_n(X - d) = \frac{a(X - d) + b}{(X - d) + d} + g(X - d) = \frac{aX - c}{X} + h(X),$$

onde $c = ad - b$ e $h(X) = g(X - d)$. Dado $u \in \mathbb{F}_q$, $x \in \mathbb{F}_q^*$ é solução de $H_n(X) = u$ se, e somente se, $z = x - d \neq -d$ é solução de $G_n(Z) = u$. Sejam

$$S = \{(x, y) \in \mathbb{F}_q \times \mathbb{F}_q : x \neq y \text{ e } H_n(x) = H_n(y)\},$$

$$V_{H_n} = \{u \in \mathbb{F}_q : \exists x \in \mathbb{F}_q \text{ com } H_n(x) = u\}$$

e para cada $u \in V_{H_n}$ consideremos

$$H_n^{-1}(u) = \{x \in \mathbb{F}_q : H_n(x) = u\}.$$

Notemos que $0 \notin H_n^{-1}(u)$ para qualquer $u \in V_{H_n}$. Defina $n_u = |H_n^{-1}(u)|$ e $\mu = |S|$. Observe-mos que

$$x \in H_n^{-1}(u) \Leftrightarrow \frac{ax - c}{x} + h(x) = u \Leftrightarrow xh(x) - x(u - a) - c = 0.$$

Uma vez que o polinômio $Xh(X) - X(u - a) - c$ tem grau $k + 1$, ele tem no máximo $k + 1$ raízes em $\mathbb{F}_q$. Conseqüentemente, $n_u \leq k + 1$. Além disso, para cada $x \in H_n^{-1}(u)$, existem exatamente $n_u - 1$ elementos $y \in \mathbb{F}_q$ tais que $x \neq y$ e $H_n(x) = H_n(y)$. Portanto,

$$\mu = \sum_{u \in V_{H_n}} n_u(n_u - 1) \leq (k + 1) \sum_{u \in V_{H_n}} (n_u - 1). \quad (7.1)$$

Ademais, para cada $u \in V_{H_n}$, existem n_u elementos distintos $x \in \mathbb{F}_q$ satisfazendo $H_n(x) = u$, de modo que há n_u elementos distintos $z \in \mathbb{F}_q$ tais que $G_n(z) = u$. Como G_n é injetivo em $\mathbb{F}_q \setminus \mathcal{O}_n$, pelo menos $n_u - 1$ elementos $z \in \mathcal{O}_n$ satisfazem $G_n(z) = u$. Assim, usando (7.1) e o fato de que $-d \in \mathcal{O}_n$, concluímos que

$$n \geq |\mathcal{O}_n| \geq 1 + \sum_{u \in V_{H_n}} (n_u - 1) \geq 1 + \frac{\mu}{k + 1}. \quad (7.2)$$

Agora, vamos determinar μ em função de q e k . Dados $x, y \in \mathbb{F}_q^*$ com $x \neq y$, temos

$$\begin{aligned} H_n(x) = H_n(y) &\Leftrightarrow y(ax - c + xh(x)) = x(ay - c + yh(y)) \\ &\Leftrightarrow xy(h(x) - h(y)) + c(x - y) = 0 \\ &\Leftrightarrow xy \frac{h(x) - h(y)}{x - y} + c = 0. \end{aligned}$$

Conseqüentemente, μ é igual ao número de soluções $(x, y) \in \mathbb{F}_q^* \times \mathbb{F}_q^*$ com $x \neq y$ da equação

$$XY \frac{h(X) - h(Y)}{X - Y} + c = 0.$$

Pelo Lema 7.1.1 e lembrando que $k = \deg h$, obtemos

$$\mu \geq q + 1 - k(k - 1)\sqrt{q} - (\nu + k + 2),$$

onde $\nu = (k, q - 1)$. Portanto, usando (7.2), concluimos que

$$\begin{aligned} n(k + 1) &\geq k + 1 + \mu \geq k + 1 + q + 1 - k(k - 1)\sqrt{q} - (\nu + k + 2) \\ &\Rightarrow nk + k(k - 1)\sqrt{q} \geq q - \nu - n. \end{aligned}$$

□

Corolário 7.1.1. Seja $f(X)$ um polinômio de permutação sobre $\mathbb{F}_q$, com $Crk(f) = n \geq 1$ e $f(X) \in \mathcal{L}_1$. Se $n < (q - 1)/2$ então $f(X)$ não é um mapa polinomial completo.

Demonstração. Suponhamos que $f(X)$ e $f(X) + X$ sejam polinômios de permutação sobre $\mathbb{F}_q$. Tomando o polinômio $g(X) = X$, concluimos pelo Teorema 7.1.2 que $n \geq q - 1 - n$, donde $n \geq (q - 1)/2$. Logo, tem-se o resultado. □

Observação 7.1.1. Aproveitando esta última demonstração, vemos que $Crk(f) \geq (q - 1)/2$ se $f(X)$ é um mapa polinomial completo e $f(X) \in \mathcal{L}_1$. Se, além disso, $f(X)$ tiver uma representação $\mathcal{P}_m(X)$ com $m = (q - 1)/2$, então teremos $Crk(f) = m$. Utilizando isso, podemos obter o posto de Carlitz de vários polinômios de permutação. Veremos, a seguir, alguns exemplos.

Dados $n \geq 0$ e q uma potência de um primo, consideremos os conjuntos

$$\mathcal{P}_{n,q} = \{f(X) \in \mathbb{F}_q[X] : f = \mathcal{P}_n, \text{ para algum } \mathcal{P}_n \text{ da forma (4.1)}\}$$

e

$$\mathcal{P}_{n,q}^{(1)} = \{f(X) \in \mathcal{P}_{n,q} : \alpha_i \neq 0, \text{ para } i = 3, \dots, n\},$$

onde os α_i são definidos em (5.1). Dessa maneira, todo elemento de $\mathcal{P}_{n,q}^{(1)}$ pertence a $\mathcal{L}_1$. Em [8], foram obtidos vários exemplos de mapas polinomiais completos $f(X) \in \mathcal{P}_{n,q}^{(1)}$, com $n = (q - 1)/2$ (veja Tabela 4.1 de [8]). Pela Observação 7.1.1, o posto de Carlitz desses polinômios vale $(q - 1)/2$. Por exemplo, temos os seguintes mapas polinomiais completos retirados da Tabela 4.1 de [8]:

- $f(X) = 5X^8 + 5X^7 + 5X^6 + 4X^4 + 2X^3 + 5X^2 + 9X + 5 \in \mathcal{P}_{5,11}^{(1)}$;
- $g(X) = 10X^{10} + 5X^9 + 5X^8 + 8X^7 + 12X^6 + 7X^5 + 2X^4 + 6X^3 + 4X^2 + 4X + 3 \in \mathcal{P}_{6,13}^{(1)}$;
- $h(X) = 7X^{14} + 13X^{13} + 3X^{12} + 14X^9 + 10X^8 + 5X^7 + X^6 + 6X^5 + 2X^4 + 2X^3 + 5X^2 + 13X + 3 \in \mathcal{P}_{8,17}^{(1)}$.

Assim, $Crk(f) = 5$, $Crk(g) = 6$ e $Crk(h) = 8$. Há mais exemplos nessa tabela dos quais podemos obter o posto de Carlitz. Além disso, existe um resultado que fornece muito mais exemplos de mapas polinomiais completos que pertencem a $\mathcal{P}_{n,q}^{(1)}$, com $n = (q - 1)/2$. Para o leitor interessado, veja Teorema 2.20 de [8].

Referências

- [1] A. Çeşmeliöğlü, W. Meidl, A. Topuzoğlü, *Permutations of finite fields with prescribed properties*, J. Comput. Appl. Math., **259**, 536–545, 2014.
- [2] A. Garcia, Y. Lequain, *Elementos de Álgebra*, Projeto Euclides, 6 ed., IMPA, Rio de Janeiro, 2015.
- [3] C. Hermite, *Sur les fonctions de sept lettres*, C. R. Acad. Sci. Paris, **57**, 750-757, 1863.
- [4] D. Gomez-Perez, A. Ostafe, A. Topuzoğlü, *On the Carlitz rank of permutations of $\mathbb{F}_q$ and pseudorandom sequences*, J. Complexity, **30**, 279–289, 2014.
- [5] D.S. Dummit, R.M. Foote, *Abstract Algebra*, John Wiley and Sons, 3 ed., 2004.
- [6] E. Aksoy, A. Çeşmeliöğlü, W. Meidl, A. Topuzoğlü, *On the Carlitz rank of permutation polynomials*, Finite Fields and Their Applications, **15**, 428-440, 2009.
- [7] F. Pausinger, A. Topuzoğlü, *On the discrepancy of two families of permuted van der Corput sequences*, Unif. Distrib. Theory, **13**, no.1, 47–64, 2018.
- [8] I. Leyla, *On complete mappings and value sets of polynomials over finite fields*, PhD Thesis, Sabanci University, 2015.
- [9] J.A. Oliveira, F.E.B. Martinez, *Permutation polynomials with Carlitz rank 2*, Discrete Mathematics, **344**, 112155, 2021.
- [10] J. Li, D.B. Chandler, Q. Xiang, *Permutation polynomials of degree 6 or 7 over finite fields of characteristic 2*, Finite Fields and Their Applications, **16**, 406-419, 2010.
- [11] J. Rotman, *An introduction to the theory of groups*, Springer-Verlag, 1995.

- [12] J.W.P. Hirschfeld, G. Korchmáros, F. Torres, *Algebraic curves over a finite field*, Princeton University Press, 2013.
- [13] L. Carlitz, *Permutations in a finite field*, Proc. Amer. Math. Soc., **4**, 538, 1953.
- [14] L.E. Dickson, *The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group*, Ann. of Math., **11**, 65-120, 161-183, 1896/1897.
- [15] N. Anbar, A. Odžak, V. Patel, L. Quoos, A. Somoza, A. Topuzoğlu, *On the Carlitz rank of permutation polynomials over finite fields: recent developments*, Women in Numbers Europe II, **11**, 2018.
- [16] N. Anbar, A. Odžak, V. Patel, L. Quoos, A. Somoza, A. Topuzoğlu, *On the difference between permutation polynomials over finite fields*, Finite Fields and Their Applications, **49**, 132-142, 2018.
- [17] P. Morandi, *Fields and Galois Theory*, Graduate Texts in Mathematics, Springer-Verlag New York, 1996.
- [18] R. Lidl, H. Niederreiter, *Finite Fields*, Cambridge University Press, Cambridge, 1997.
- [19] S.D. Cohen, G.L. Mullen, P.J.-S. Shiue, *The difference between permutation polynomials over finite fields*, Proc. Amer. Math. Soc., **123**, 2011–2015, 1995.
- [20] S.D. Cohen, *Proof of a conjecture of Chowla and Zassenhaus on permutation polynomials*, Canad. Math. Bull., **33**, 230-234., 1990.
- [21] S.D. Cohen, *The distribution of polynomials over finite fields*, Acta Arithmetica, **17**, 255-271, 1970.
- [22] W. Fulton, *Algebraic curves: An introduction to Algebraic Geometry*, 2008.

- [23] X. Fan, *A classification of permutation polynomials of degree 7 over finite fields*, Finite Fields and Their Applications, **59**, 1-21, 2019.
- [24] X. Fan, *Permutation polynomials of degree 8 over finite fields of characteristic 2*, Finite Fields and Their Applications, **64**, 101662, 2020.
- [25] X. Fan, *Permutation polynomials of degree 8 over finite fields of odd characteristic*, Bull. Aust. Math. Soc., 101 (1), 40-45, 2020.
- [26] Z. Ding, *Connecting two types of representations of a permutation of $\mathbb{F}_q$* , Discrete Mathematics, **343**(4), 111793, 2020.