UFRR

UNIVERSIDADE FEDERAL DE RORAIMA
CENTRO DE CIÊNCIAS E TECNOLOGIA
DEPARTAMENTO DE MATEMÁTICA
CURSO DE BACHARELADO EM MATEMÁTICA

Leonardo Angelo de Oliveira

UMA INTRODUÇÃO AOS CORPOS FINITOS

BOA VISTA, RR

2022

Leonardo Angelo de Oliveira

UMA INTRODUÇÃO AOS CORPOS FINITOS

Trabalho de Conclusão de Curso de graduação apresentado ao Departamento de Matemática da Universidade Federal de Roraima como parte dos requisitos para obtenção do título de Bacharel em Matemática.

Orientadora: Dra. Lays Grazielle Cardoso Silva de Jesus

BOA VISTA, RR
2022

Leonardo Angelo de Oliveira

UMA INTRODUÇÃO AOS CORPOS FINITOS

Trabalho de Conclusão de Curso de graduação apresentado ao Departamento de Matemática da Universidade Federal de Roraima como parte dos requisitos para obtenção do título de Bacharel em Matemática.

Dra. Lays Grazielle Cardoso Silva de Jesus
Orientadora/UFRR

Dr. Allan Ramos de Souza
Membro/UFRR

Dra. Franciele Conrado dos Santos
Membro/UFS

Dr. Aldo Henrique de Souza Medeiros
Suplente/IFNMG

Number theory is the
queen of mathematics.
Author: Carl F. Gauß

Agradecimentos

A minha família, por todo o apoio que recebi. Em especial, aos meus pais, Cleia Izidório Angelo e Ivan de Oliveira, que sempre me incentivaram a seguir nos estudos e me deram todo o suporte necessário.

A minha professora orientadora, Lays Grazielle Cardoso Silva de Jesus, por todo seu profissionalismo e dedicação em nossas reuniões durante a elaboração deste trabalho. Sem dúvidas, foi enorme sua contribuição para minha formação, acadêmica e pessoal.

Ao professor Maycon Sullivan Santos Araújo, que gentilmente me convidou para um projeto de pesquisa no início do curso. Nossas reuniões nessa época foram um dos primeiros contatos que tive com matemática rigorosa e formal, e por isso sou grato.

Aos professores da UFRR. Em especial, Erivaldo Diniz, José Luis, Renato Enco.

Aos amigos que a universidade me trouxe. Em especial, cito os seguintes: João Paulo, Kemilly Kathrem, Gabriel Ramos, Gabriel Spies, Debohra Andrade, e Felipe Farias.

A banca examinadora, por aceitarem ler, avaliar e contribuir com este trabalho.

To Erwin Smith.

RESUMO

Neste trabalho, apresentamos a teoria de corpos finitos introduzindo os principais conceitos e abordando os principais resultados para proporcionar um texto em português que sirva de base para estudos teóricos ou para consulta no caso de o interesse ser nas aplicações.

Palavras-chave: Corpo finito; extensão de corpo; corpo ciclotômico.

ABSTRACT

In this work, we present the theory of finite fields by introducing the main concepts and covering the key results to provide a Portuguese-based text that serves as a basis for theoretical studies or for reference in case the interest lies in applications.

Keywords: Finite field; field extension; cyclotomic extension.

Sumário

Introdução

Conceitos subjacentes da teoria dos corpos finitos remontam aos séculos XVII e XVIII, em trabalhos de matemáticos eminentes como Pierre de Fermat (1601-1665), Leonhard Euler (1707-1768), Joseph-Louis Lagrange (1736-1813), e Adrien-Marie Legendre (1752-1833). No entanto, foi no século XIX que o o desenvolvimento desta teoria ocorreu com maior vigor. Com as contribuições extraordinárias de Carl Friedrich Gauß (1777-1855) e Évarist Galois (1811-1832), pode-se dizer que foi nessa época que a teoria geral dos corpos finitos se consolidou como a conhecemos hoje.

Nos dias atuais, essa teoria tem se provado especialmente interessante para questões práticas. As áreas de aplicação são vastas, entre elas citamos criptografia, teoria dos códigos, processamento digital de sinais e transformada discreta de Fourier. São notáveis também as aplicações em outras áreas da matemática, tais como combinatória, geometria algébrica, geometria aritmética, geometria finita e teoria dos números [p. xii de (LIDL; NIEDERREITER, 1997) e p. 2 de (PANARIO, 2007)].

O estudo de corpos finitos está, portanto, mais do que justificado, tanto por seus aspectos teóricos, quanto por suas aplicações práticas. Nosso objetivo com este trabalho é apresentar as principais definições e resultados básicos, a fim de proporcionar um texto em português que sirva como ponto de partida para estudos teóricos mais profundos, ou para consulta no caso de o interesse ser nas aplicações.

O primeiro capítulo consiste em uma revisão dos fundamentos básicos de álgebra, notação e terminologia que serão utilizados no decorrer do texto.

O segundo capítulo trata dos principais conceitos da teoria de corpos finitos. Iniciamos apresentando questões relacionadas à estrutura, como número de elementos e caracterização de subcorpos. Em seguida, investigamos corpos finitos do ponto de vista da álgebra linear. Além disso, tratamos de alguns tópicos adicionais, como extensões ciclotômicas, o Teorema de Wedderburn e representação. Por fim, apresentamos o conceito de ordem de um polinômio e deduzimos alguns resultados e aplicações.

Capítulo 1

Fundamentos de álgebra

Nosso propósito neste capítulo introdutório é apresentar algumas definições e resultados elementares, bem como algumas notações necessárias para o desenvolvimento deste trabalho. Alguns resultados serão apresentados sem demonstração. Os leitores interessados em maiores detalhes podem consultar os livros (LIDL; NIEDERREITER, 1997), (HUNGERFORD, 1980) e (GONÇALVES, 1979).

Uma estrutura algébrica é um conjunto não vazio munido de uma ou mais operações binárias. Quando uma estrutura algébrica satisfaz certas propriedades, ela recebe um nome particular. Neste capítulo, apresentamos as estruturas de grupos, anéis e corpos, com ênfase no que é necessários para o estudo dos corpos finitos no capítulo seguinte.

1.1 Grupos

Iniciamos com o conceito de grupo e deduzimos algumas de suas propriedades. Essa estrutura algébrica, embora seja a mais simples do ponto de vista axiomático, é extremamente rica tanto do ponto de vista teórico quanto de suas aplicações.

Definição 1.1 *Seja G um conjunto não vazio e $*$ uma operação binária em G. Dizemos que $(G, *)$ é um* ***grupo*** *quando as seguintes condições são satisfeitas:*

1. *A operação $*$ é associativa em G, isto é, $(a * b) * c = a * (b * c)$ para quaisquer $a, b, c \in G$.*
2. *Existe um elemento identidade, o qual denotaremos por $e_G \in G$, tal que $e_G * a = a * e_G = a$ para qualquer $a \in G$.*
3. *Para cada $a \in G$, existe $a' \in G$ tal que $a * a' = a' * a = e_G$.*

Observação 1.1 *Seja $(G, *)$ um grupo.*

- *É possível provar a unicidade do elemento identidade e_G.*
- *Dado $a \in G$, o elemento $a' \in G$ do item 3 da definição 1.1 é chamado de elemento oposto, ou inverso, de $a \in G$ com respeito à operação $*$.*
- *Se a operação $*$ é comutativa em G, isto é, se $a * b = b * a$ para quaisquer $a, b \in G$, dizemos que G é um **grupo abeliano**.*
- *Por simplicidade, quando a operação $*$ estiver clara no contexto, escrevemos apenas G para denotar o grupo $(G, *)$, e escrevemos apenas ab para denotar $a * b$.*

Definição 1.2 *Seja G um grupo e H um subconjunto não vazio de G. Dizemos que H é **subgrupo** de G quando H é grupo com a operação de G restrita a H.*

Exemplo 1.1 *O conjunto $\mathbb{R}$ dos reais é um grupo abeliano com respeito à operação usual de adição. Além disso, o conjunto $\mathbb{Q}$ dos racionais é um subgrupo de $\mathbb{R}$.*

Verificar que um subconjunto não vazio é um subgrupo as vezes pode ser trabalhoso, no sentido de que é preciso garantir que todos os axiomas do grupo são válidos para os elementos deste subconjunto. No entanto, o resultado a seguir nos fornece uma caracterização para subgrupos, o que nos permite verificar isso de uma forma mais simples.

Teorema 1.1 (Critério de subgrupo) *Seja G um grupo e H um subconjunto não vazio de G. Então H é subgrupo de G se, e somente se $ab' \in H$ sempre que $a, b \in H$.*

Segue do Teorema 1.1 que G e $H = \{e_G\}$ são subgrupos de G, os quais são chamados **subgrupos triviais** de G.

Observação 1.2 *Podemos construir subgrupos não triviais de um grupo $G = (G, *)$. Para isso, fixamos um elemento $a \in G$ e, denotando o elemento inverso de a por a^{-1}, consideramos para cada m inteiro que*

$$a^m = \begin{cases} a * a * \cdots * a \text{ (m parcelas)} & \text{se } m > 0 \\ (a^{-1}) * (a^{-1}) * \cdots * (a^{-1}) \text{ (m parcelas)} & \text{se } m < 0 \\ e_G & \text{se } m = 0 \end{cases}.$$

*Nestas condições, podemos provar com um argumento de indução que a operação entre os elementos a^m e a^n, com m e n inteiros, ocorre de maneira semelhante ao que já conhecemos da aritmética elementar. Assim, valem para $a \in G$ propriedades operacionais tais como $a^m a^n = a^{m+n}$, $(a^m)^n = a^{mn}$ e outras relacionadas. Dizemos que a^m é uma **potência** de a.*

Teorema 1.2 *Seja G um grupo e seja $a \in G$. Então, o conjunto das potências de a, $H = \{a^m : m \in \mathbb{Z}\}$, é subgrupo abeliano de G.*

***Demonstração**:* Observamos que $H \neq \emptyset$ pois, tomando $m = 0$ temos $a^m = a^0 = e_G \in H$. Se $a^m, a^n \in H$ com $m, n \in \mathbb{Z}$, então $a^m(a^n)^{-1} = a^m a^{-n} = a^{m-n} \in H$, logo H é subgrupo de G pelo Teorema 1.1. Além disso, H é abeliano pois $a^n a^m = a^{m+n} = a^{n+m} = a^n a^m$.

Definição 1.3 *Seja G um grupo e $a \in G$. Chamamos de **subgrupo gerado** por a, e denotamos por $\langle a \rangle$, ao subgrupo de G cujos elementos são potências de a, isto é,*

$$\langle a \rangle = \{g \in G : g = a^m, m \in \mathbb{Z}\}.$$

Definição 1.4 *Seja G um grupo. Definimos a **ordem** do grupo G, a qual denotaremos por $|G|$, como sendo o número de elementos do conjunto G. Se $|G| = n$ com n inteiro positivo, dizemos que G é um **grupo finito** de ordem n.*

A **ordem do subgrupo gerado** por a, a qual denotaremos por $|a|$, é o número de elementos do conjunto $\langle a \rangle$, isto é,

$$|a| = |\langle a \rangle|.$$

Teorema 1.3 *Seja G um grupo e suponha que $a \in G$ tem ordem finita. Então $|a| = k$ se, e somente se k é o menor inteiro positivo tal que $a^k = e_G$. No caso afirmativo, se $a^h = e_G$, então k divide h.*

Definição 1.5 *Seja G um grupo. Dizemos que G é um **grupo cíclico** quando existe $b \in G$ tal que*

$$G = \langle b \rangle.$$

Exemplo 1.2 *O conjunto dos $\mathbb{Z}$ dos inteiros com a operação usual de soma é um grupo abeliano cíclico gerado por 1. De fato, é fácil verificar que os axiomas do grupo são satisfeitos. Para mostrarmos que $\mathbb{Z} = \langle 1 \rangle$, basta notarmos que para qualquer $m \in \mathbb{Z}$, temos*

$$m = \begin{cases} 1 + 1 + \cdots + 1 \text{ (m parcelas)} & \text{se } m > 0 \\ (-1) + (-1) + \cdots + (-1) \text{ (m parcelas)} & \text{se } m < 0 \\ 0 & \text{se } m = 0 \end{cases}.$$

Exemplo 1.3 *Fixemos m inteiro positivo. Vejamos que o **conjunto dos múltiplos** de m, $m\mathbb{Z} := \{ma : a \in \mathbb{Z}\}$, é subgrupo de $\mathbb{Z}$ com a operação usual de soma. De fato, temos que $m\mathbb{Z} \neq \emptyset$ pois $m0 = 0 \in m\mathbb{Z}$. Além disso, para quaisquer $ma, mb \in m\mathbb{Z}$, temos que*

$ma - mb = m(a-b) \in m\mathbb{Z}$. *Enfatizamos que* $m(a-b)$ *denota* $(a-b)$ *somado consigo mesmo* m *vezes como descrevemos na Observação 1.2 - aqui não consideramos a operação de multiplicação. Logo, o critério de subgrupo implica que* $m\mathbb{Z}$ *é subgrupo de* $\mathbb{Z}$. *Além disso, seguindo os mesmo passos do Exemplo 1.2 vemos que* $m\mathbb{Z}$ *é grupo cíclico e* $m\mathbb{Z} = \langle m \rangle$.

Agora, estamos interessados em descrever outros grupos que serão de nosso interesse no decorrer deste trabalho. Iniciamos recordando o conceito de congruência nos inteiros. Sejam a e b inteiros e m um inteiro positivo. Dizemos que a é **congruente a** b **módulo** m, e denotamos por $a \equiv b \pmod{m}$, quando m divide $(a-b)$, isto é, $(a-b) \in m\mathbb{Z}$. Em outras palavras, $a \equiv b \pmod{m}$ quando $(a-b)$ é múltiplo inteiro de m. Podemos então estabelecer uma relação R entre inteiros a e b através da congruência módulo m:

$$aRb \iff a \equiv b \pmod{m}.$$

A seguir, vemos como o conceito de congruência pode ser generalizado e introduzido na teoria de grupos através do conceito de classes laterais. Para maiores detalhes sobre esse assunto, indicamos a seção 4 do capítulo 1 de (HUNGERFORD, 1980).

Definição 1.6 *Sejam* G *um grupo,* H *um subgrupo de* G *e* $a, b \in G$. *Dizemos que* a *é* ***congruente à direita*** *de* b *módulo* H, *e denotamos* $a \equiv_d b \pmod{H}$, *se* $ab^{-1} \in H$.

Observação 1.3 *Dizemos que* a *é* ***congruente à esquerda*** *de* b ***módulo*** H, *e denotamos* $a \equiv_e b \pmod{H}$, *se* $a^{-1}b \in H$. *No que se segue, apresentamos apenas o caso "congruente à direita", pois o caso "congruente à esquerda"é tratado de modo inteiramente análogo. Observamos que, se* G *é abeliano, então as congruências à esquerda e à direita módulo* H *coincidem, pois* $ab^{-1} \in H \iff (ab^{-1})^{-1} = ba^{-1} = a^{-1}b \in H$.

Teorema 1.4 *Seja* H *um subgrupo do grupo* G.

1. *A congruência à direita módulo* H *é uma relação de equivalência em* G.
2. *A classe de equivalência de* $a \in G$ *com respeito à congruência à direita módulo* H *é o conjunto* $Ha = \{ha : h \in H\}$.
3. *Para qualquer* $a \in G$, *temos* $\#(Ha) = |H|$.

Demonstração*:* Sejam $a, b, c \in G$.

1. Temos $a \equiv_d a \pmod{H}$ pois $aa^{-1} = e_G \in H$ (reflexividade). Se $a \equiv_d b \pmod{H}$, então $ab^{-1} \in H$ implica $(ab^{-1})^{-1} = ba^{-1} \in H$, ou seja, $b \equiv_d a \pmod{H}$ (simetria). Além disso, se $a \equiv_d b \pmod{H}$ e $b \equiv_d c \pmod{H}$, então $(ab^{-1}), (bc^{-1}) \in H$. Logo $(ab^{-1})(bc^{-1}) = ac^{-1} \in H$, isto é, $a \equiv_d c \pmod{H}$ (transitividade).

2. Fixemos $a \in G$. A classe de equivalência de a é o conjunto

$$\begin{aligned}\{x \in G : x \equiv_d a \pmod{H}\} &= \{x \in G : xa^{-1} \in H\} \\ &= \{x \in G : xa^{-1} = h \in H\} \\ &= \{x \in G : x = ha, \text{ com } h \in H\} \\ &= Ha.\end{aligned}$$

3. Se $x \in Ha$, então $x = ha$ para algum $h \in H$ pelo item 2. Consideremos a aplicação $\psi : Ha \to H$ dada por $\psi(ha) = h$. Se $\psi(ha) = \psi(h'a)$, então $h = h'$ implica $ha = h'a$, logo ψ é injetiva. Além disso, ψ é sobrejetiva pois, se $h \in H$, então $ha \in Ha$ é tal que $\psi(ha) = h$. Os conjuntos Ha e H têm mesma cardinalidade pois estão em bijeção.

Definição 1.7 *Seja G um grupo, H um subgrupo de G e $a \in G$. O conjunto Ha é chamado de **classe lateral à direita** de H, e o conjunto aH é chamado de **classe lateral à esquerda** de H.*

Corolário 1.1 *Seja G um grupo, H um subgrupo de G e $a, b \in G$.*

1. *Os conjuntos Ha e Hb ou são iguais ou são disjuntos.*
2. *G é união disjunta das classes laterais à direita de H.*
3. *$Ha = Hb$ se, e somente se $ab^{-1} \in H$.*
4. *Seja D o conjunto das distintas classes laterais à direita de H em G, e E o conjunto das distintas classes laterais à esquerda de H em G. Então, $\#(D) = \#(E)$ e $|H| = \#(aH) = \#(Hb)$ para quaisquer $a, b \in G$.*

***Demonstração**:* Os itens 1 e 2 seguem do item 1 do Teorema 1.4. Provemos o item 3. Suponhamos que $Ha = Hb$. Como $a \in Ha = Hb$, então pelo item 2 do Teorema 1.4 $a = hb$ para algum $h \in H \implies h = ab^{-1} \in H$. Reciprocamente, se $ab^{-1} = h$ para algum $h \in H$, então $a = hb \implies a \in Hb$. Como $a \in Ha \bigcap Hb$, então pelo item 1 vemos que $Ha = Hb$. Para provar o item 4, consideremos a aplicação $\psi : D \to E$ dada por $\psi(Ha) = a^{-1}H$. Se $\psi(Ha) = \psi(Hb)$, então $a^{-1}H = b^{-1}H \implies a^{-1}b \in H$ pelo item 3 $\implies a^{-1}b = h$ para algum $h \in H \implies b = ha \implies Ha = Hb$ pelo item 1. Logo ψ é injetiva. Além disso, por construção ψ é sobrejetiva, pois dada $a^{-1}H \in E$, temos que $aH \in D$ cumpre $\psi(Ha) = a^{-1}H$. Portanto, $\#(D) = \#(E)$ pois os conjuntos D e E estão em bijeção, e pelo item 3 do Teorema 1.4 vale $\#(Ha) = |H|$ e $\#(bH) = |H|$ para quaisquer $a, b \in G$.

Definição 1.8 *Seja H um subgrupo do grupo G. O **índice** de H em G, denotado por $[G : H]$, é a cardinalidade do conjunto das distintas classes laterias à direita de H em G.*

A seguir, apresentamos um dos principais resultados da teoria de grupos. Ele relaciona a ordem de um grupo finito com a ordem de seus subgrupos.

Teorema 1.5 (Lagrange) *Seja G um grupo finito e H um subgrupo de G. Então a ordem de G é igual ao produto da ordem de H pelo índice de H em G, isto é, $|G| = |H|[G : H]$. Em particular, $|H|$ divide $|G|$ e $|G|/|H| = [G : H]$.*

***Demonstração**:* Como G é um grupo finito, então existe um número finito k de distintas classes à direita de H, digamos $Ha_1, Ha_2, \cdots Ha_k$. Então $k = [G : H]$ e, pelo item 3 do Teorema 1.4 temos que $\#(Ha_i) = |H|$ para cada $i \in \{1, 2, \cdots, k\}$. Pelos itens 2 e 3 do Teorema 1.4, G é a união disjunta dos conjuntos $Ha_1, Ha_2, \cdots, Ha_k$, todos com a mesma cardinalidade que H. Portanto,

$$\begin{aligned} |G| &= \#(Ha_1 \cup Ha_2 \cup \cdots \cup Ha_k) \\ &= \#(Ha_1) + \#(Ha_2) + \cdots + \#(Ha_k) \\ &= |H| + |H| + \cdots + |H| \text{ (k fatores)} \\ &= |H|k \\ &= |H|[G : H]. \end{aligned}$$

Corolário 1.2 *Seja G um grupo finito e seja $a \in G$. Então $|a|$ divide $|G|$.*

Corolário 1.3 *Todo grupo de ordem prima, é cíclico.*

***Demonstração**:* Seja G um grupo de ordem p com p primo. Consideremos o subgrupo $H = \langle a \rangle$ com $a \neq e_G$. Como p é primo, os únicos divisores positivos de p são 1 e $p = |G|$. Pelo Teorema de Lagrange, H deve conter 1 ou p elementos. Se fosse $H = \{e_G\}$, então teríamos $a = e_G$, contrariando a escolha de a. Portanto, $H = G$ e G é grupo cíclico.

Exemplo 1.4 *Seja m um inteiro positivo. Vamos analisar novamente os grupo aditivo $\mathbb{Z}$ e seu subgrupo $\langle m \rangle$. Pelo Teorema 1.4, a relação de congruência à direita módulo $\langle m \rangle$ é uma relação de equivalência em $\mathbb{Z}$, logo induz uma partição de $\mathbb{Z}$. Isso nos permite escrever $\mathbb{Z}$ como união disjunta dessas classes de equivalência. Por outro lado, sabemos da aritmética elementar que $a \equiv b \pmod{m}$ se, e somente se a e b deixam o mesmo resto na divisão por m. De acordo com o Algoritmo da Divisão para os inteiros, os possíveis restos dessa divisão são $0, 1, \cdots m-1$. Dessa forma, podemos ver que $[\mathbb{Z} : \langle m \rangle] = m$ e escrever*

$$\mathbb{Z} = [0] \cup [1] \cup \cdots \cup [m-1],$$

sendo que $[i]$ denota classe de i, isto é,

$$[i] = \langle m \rangle + i = \{km + i : k \in \mathbb{Z}\}. \tag{1.1}$$

Podemos olhar para $[i]$ como o conjuntos dos inteiros que deixam resto i na divisão por m.

Teorema 1.6 *Seja m um inteiro positivo e considere o conjunto $H = \{[0], [1], \cdots, [m-1]\}$, onde $[i]$ é como descrito em (1.1). Então, a operação binária $\oplus$ dada por $[a] \oplus [b] = [a+b]$ está bem definida em H. Além disso, $(H, \oplus)$ é um grupo abeliano.*

***Demonstração**:* Observamos primeiro que $\oplus$ está definida, uma vez que, para quaisquer $a, b \in \mathbb{Z}$, temos $[a] \oplus [b] \in H$. Vamos mostrar que $[a] \oplus [b]$ está bem definida, isto é, independe da escolha de $x \in [a]$ e $y \in [b]$. De fato, sejam $x, x' \in [a]$ e $y, y' \in [b]$. Temos $x \equiv x' \pmod{m}$ e $y \equiv y' \pmod{m}$, logo $(x+y) \equiv (x'+y') \pmod{m}$. Dessa forma, $[x] \oplus [y] = [x+y] = [x'+y'] = [x'] \oplus [y']$. Para ver que $(H, \oplus)$ é grupo abeliano, basta observar que o elemento neutro é $[0]$, o inverso de $[a]$ é $[-a]$, e a associatividade e comutatividade seguem da soma usual de inteiros.

Definição 1.9 *O grupo aditivo apresentado no Teorema 1.6 é chamado de **grupo aditivo dos inteiros módulo** m, e será denotado por $\mathbb{Z}_m$.*

Observação 1.4 *Observamos que $\mathbb{Z}_m = \mathbb{Z}/\langle m \rangle$. Na literatura, é usual a notação $\overline{a}$ para indicar a classe $[a]$ em $\mathbb{Z}_m$. Também é comum indicar a soma $\oplus$ simplesmente por $+$. No que se segue, adotaremos a notação $\overline{a}$ para classe determinada por a e $+$ para indicar a soma em $\mathbb{Z}_m$.*

Exemplo 1.5 *Vejamos como operar no grupo $\mathbb{Z}_{12}$. Segue do exemplo 1.4 que*

$$\mathbb{Z}_{12} = \{\overline{0}, \overline{1}, \cdots, \overline{11}\}.$$

Isso é um sistema completo de restos módulo 12, pois qualquer outro inteiro é congruente a um dos elementos de $\mathbb{Z}_{12}$. Operamos dois elementos de $\mathbb{Z}_{12}$ de acordo com o Teorema 1.6. Por exemplo, temos que $\overline{6} + \overline{11} = \overline{5}$. Para verificar essa igualdade, basta checarmos que 5 é o resto que $6 + 11 = 17$ deixa na divisão por 12. De forma geral, temos o seguinte modo de operar em $\mathbb{Z}_{12}$: $\bar{a} + \bar{b} = \bar{c}$, onde c é o resto que $(a+b)$ deixa na divisão por 12.

Agora, vamos construir grupos a partir da operação usual de produto dos inteiros.

Teorema 1.7 *Seja m um inteiro positivo e considere o conjunto $H = \{\overline{0}, \overline{1}, \cdots, \overline{m-1}\}$, onde $[i]$ é como descrito em (1.1). Então, a operação binária $\odot$ dada por $\overline{a} \odot \overline{b} = \overline{ab}$ está bem definida em H.*

***Demonstração**:* Seguimos a mesma ideia da demonstração do Teorema 1.6. Primeiro, a operação $\odot$ está definida pois, para quaisquer $a, b \in \mathbb{Z}$ temos que $\overline{a} \odot \overline{b} \in H$. Para ver que $\odot$ está bem definida, sejam $x, x' \in \overline{a}$ e $y, y' \in \overline{b}$. Sendo $x \equiv x' \pmod{m}$ e $y \equiv y' \pmod{m}$, temos $xy \equiv x'y' \pmod{m}$. Portanto, $\overline{x} \odot \overline{y} = \overline{xy} = \overline{x'y'} = \overline{x'} \odot \overline{y'}$.

A operação $\odot$ do Teorema 1.7 é associativa e comutativa, e seu elemento neutro é $\overline{1}$. Para formamos um grupo com a operação induzida da multiplicação de inteiros, resta apenas garantirmos que todo elemento não neutro de H admita inverso multiplicativo. A seguir mostramos que isso ocorre se, e somente se m é número primo.

Teorema 1.8 *Seja m um inteiro positivo e considere o conjunto $I = \{\overline{1}, \cdots, \overline{m-1}\}$. Então, $(I, \odot)$ é grupo com a operação dada no Teorema 1.7 se, e somente se m é um número primo.*

***Demonstração**:* Suponhamos que $\mathbb{Z}_m$ é grupo mas m não é primo. Então $m = ab$ com $1 < a \leq b < m$ implica $\overline{a} \odot \overline{b} = \overline{ab} = \overline{m} = \overline{0}$, mas $\overline{0}$ não pertence a I, absurdo. Reciprocamente, se m é primo, então m é relativamente primo com $1, 2, \cdots, m-1$. Dado $a \in I$, então $a \in \{1, 2, \cdots, m-1\}$ e pelo Lema de Bézout existem $p, q \in \mathbb{Z}$ tais que $ap + mq = 1$. Como $mq \equiv 0 \pmod{m}$, então $ap \equiv 1 \pmod{m}$. Portanto a admite elemento inverso com respeito à operação $\odot$.

Definição 1.10 *Seja p um número primo. O conjunto $\{\overline{1}, \overline{2} \cdots, \overline{p-1}\}$, munido da operação $\overline{a} \odot \overline{b} = \overline{ab}$, é chamado de **grupo multiplicativo dos inteiros módulo** p, e será denotado por $\mathbb{Z}_p^*$.*

Exemplo 1.6 *No grupo $\mathbb{Z}_p^*$, é usual escrevermos $\overline{a} \cdot \overline{b}$ para denotarmos $\overline{a} \odot \overline{b}$. As operações nesses grupos ocorrem de maneira análoga ao caso dos grupos $\mathbb{Z}_m$, no sentido de que podemos operar normalmente e depois olharmos para o resto da divisão por m. Consideramos, por exemplo, o grupo multiplicativo $\mathbb{Z}_5^*$. Temos que $\overline{3} \cdot \overline{4} = \overline{3 \cdot 4} = \overline{12} = \overline{2}$, e o inverso multiplicativo de $\overline{2}$ é $\overline{3}$, pois $\overline{2} \cdot \overline{3} = \overline{6} = \overline{1}$.*

Agora apresentamos uma importante função conhecida como função de Euler, a qual denotaremos pela letra φ no decorrer deste trabalho. Essa função aparece de forma natural e com frequência na teoria dos grupos e teoria dos números.

Definição 1.11 *Definimos a **função de Euler** $\varphi : \mathbb{N} \to \mathbb{N}$ por*

$$\varphi(m) = \#\{a \in \mathbb{Z} : \text{mdc}(a, m) = 1\}.$$

Em outras palavras, para $1 \leq m$ inteiro, a função de Euler indica o número de inteiros positivos s, com $1 \leq s \leq m$, que são relativamente primos com m.

O resultado a seguir sumariza as principais propriedades do grupos cíclicos.

Teorema 1.9 (Estrutura dos grupos cíclicos) *São válidas as seguinte propriedades:*

1. *Todo subgrupo de um grupo cíclico é um grupo cíclico.*
2. *Seja $G = \langle a \rangle$ um grupo cíclico de ordem m, e seja $H = \langle a^k \rangle$. Então, H é subgrupo de G de ordem $m/\operatorname{mdc}(k, m)$.*
3. *Se d é um divisor da ordem do grupo cíclico $H = \langle a \rangle$, então H contém um, e somente um subgrupo de ordem d.*
4. *Para cada divisor positivo d da ordem do grupo cíclico $H = \langle a \rangle$, existem $\varphi(d)$ elementos de ordem d em H.*

***Demonstração**:*

1. Seja G um grupo cíclico, isto é, existe $a \in G$ tal que $G = \langle a \rangle$. Consideremos H um subgrupo de G e suponhamos $H \neq \{e_G\}$. Então existe existe $x \in H$ tal que $x \neq e_G$. Como $x = a^n$ para algum inteiro não nulo n, então $x^{-1} = a^{-n} \in H$. Logo, H contém pelo menos uma potência de a com expoente positivo. Seja d o menor inteiro positivo tal que $a^d \in H$, e consideremos $a^s \in H$. Aplicando o Algoritmo da Divisão para os inteiros s e d, temos que existem únicos q e r tais que $s = qd + r$ com $0 \leq r < d$. Assim, $a^{s-qd} = a^r \in H$, o que contraria a minimalidade de d, exceto no caso em que $r = 0$. Logo d divide s. Isso e a minimalidade de d implicam que $H = \langle a^d \rangle$, pois $y \in H \implies y = a^s$ para algum $s = qd \implies x = (a^d)^q \implies y \in \langle a^d \rangle$. Por outro lado, se $y' \in \langle a^d \rangle$, então existe inteiro r' tal que $y' = (a^d)^{r'} = a^{dr'} \in H$.
2. Sejam $d = \operatorname{mdc}(k, m)$ e $n = |\langle a^k \rangle|$. Então pelo Teorema 1.3, n é o menor inteiro positivo tal que $(a^k)^n = a^{kn} = e_G$. Mas como $m = |G| = |\langle a \rangle|$, então novamente pelo Teorema 1.3, a igualdade $a^{kn} = e_G$ implica que m divide nk, o que é equivalente a m/d dividir n, pois d é o maior divisor comum de m e k. Dessa forma, $(m/d)|n \iff n = j(m/d) \iff nk = jm(k/d) \iff m|nk$. Agora, como n deve ser o menor inteiro positivo que é múltiplo de m/d, podemos concluir que $m/d = n$.
3. Se d é um divisor de $|a|$, então $|a| = kd$ para algum inteiro positivo k. Segue do item 2 que $\langle a^k \rangle$ é subgrupo de ordem $d = |a|/k$ pois $\operatorname{mdc}(|a|, k) = k$. Além disso, o Teorema de Lagrange implica que $|a| = (|a|/k)[|a| : \langle a^k \rangle]$, logo $[|a| : \langle a^k \rangle] = k$. Se H é outro subgrupo de G de índice k, então $H = \langle a^j \rangle$ pelo item 1, e pelo Teorema de Lagrange, temos que $|H| = |a|/k = d$. Assim, $\langle a^j \rangle$ e $\langle a^k \rangle$ tem ordem d. Agora, segue do Teorema 1.3 que d é o menor inteiro positivo tal que $a^{dj} = e_G$ e $a^{dk} = e_G$, logo $a^{dj} = a^{dk} = e_G$. Mas isso implica que dk divide dj e dj divide dk. Portanto $k = j$, e H é o único subgrupo de G com d elementos.

4. Seja $|a| = m$ e suponhamos que $m = df$. Segue do item 2 que o subgrupo $< a^k >$ tem ordem d se, e somente se $\text{mdc}(k, m) = f$. Assim, o número de elementos de ordem d é igual ao número de inteiros k tais que $1 \leq k \leq m$ e $\text{mdc}(k, m) = f$. Escrevendo $k = fh$ com $1 \leq h \leq d$, temos que $\text{mdc}(k, m) = f$ equivale a $\text{mdc}(h, d) = 1$. Concluímos que o número de $h's$ com essa propriedade é exatamente $\varphi(d)$.

A seguir apresentamos o importante conceito de **morfismo** entre estruturas algébricas. Esse é o nome dado a aplicações entre estruturas algébricas que preservam as operações e que são de grande interesse teórico. No caso dos grupos, temos o seguinte.

Definição 1.12 *Sejam $(G, *)$ e $(H, \cdot)$ grupos. Dizemos que a aplicação $f : G \to H$ é um* ***homomorfismo de grupos*** *se, para quaisquer $a, b \in G$ vale $f(a * b) = f(a) \cdot f(b)$. Se além disso f é bijetiva, dizemos que f é um* ***isomorfismo de grupos****.*

Definição 1.13 *Seja $f : G \to H$ um homomorfismo de grupos. Chamamos de* ***kernel*** *ou* ***núcleo*** *do homomorfismo f, o qual denotaremos por* $\ker f$*, ao conjunto dos elementos $a \in G$ tais que $f(a) = e_H$, isto é,* $\ker f = \{a \in G : f(a) = e_H\}$.

Dado um homomorfismo $f : G \to H$, é possível mostrar que $\ker f$ é subgrupo de G, $f(G)$ é subgrupo de H e $f(e_G) = e_H$. Além disso, para quaisquer $g \in G$ e $s \in \ker f$, temos

$$f(gsg^{-1}) = f(g)f(s)f(g^{-1}) = f(g)f(g^{-1}) = f(gg^{-1}) = f(e_G) = e_H$$

Isso mostra que $g(\ker f)g^{-1} \subseteq \ker f$. Este é um exemplo de um tipo especial de grupo:

Definição 1.14 *Seja N um subgrupo do grupo G. Dizemos que N é um* ***subgrupo normal*** *de G se $gNg^{-1} := \{gng^{-1} : n \in N\} \subseteq N$ para qualquer $g \in G$.*

Observamos que todo subgrupo de um grupo abeliano é subgrupo normal. Como veremos, os subgrupos normais são importantes para a Teoria dos Grupos. Um dos motivos disso é que, a partir deles podemos obter outros grupos, como mostra o resultado a seguir.

Teorema 1.10 *Se N é um subgrupo normal do grupo G, então o conjunto das classes laterais à direita de N forma um grupo com a operação $(Na)(Nb) = Nab$.*

Demonstração*:* Fixemos $a, b \in G$, e consideremos $x \in Na$ e $y \in Nb$. Vejamos que $(xy) \in Hab$ independente da escolha de x e de y, isto é, a operação enunciada está bem definida. Pelo item 2 do Teorema 1.4, existem $r, s \in N$ tais que $xa^{-1} = r$ e $yb^{-1} = s$. Além disso, sendo N subgrupo normal, então existe $t \in N$ tal que $xsx^{-1} = t$, logo $xs = tx$. Portanto, $(xy)(ab)^{-1} = xyb^{-1}a^{-1} = xsa^{-1} = txa^{-1} = tr \in N$, ou seja, $(xy) \in Nab$. Para concluirmos que essa operação forma um grupo, observamos que o elemento neutro é $Ne_G = N$, o inverso de Ha é Ha^{-1} e a associatividade segue da associatividade de G.

Definição 1.15 *Seja N um subgrupo normal do grupo G. O grupo apresentado no Teorema 1.10 é chamado de* ***grupo quociente*** *de G por N, e denotado por G/N.*

Sejam G e H estruturas. Se G e H são isomorfas, podemos garantir que certas propriedades que são válidas em G também são válidas em H. Uma vez que em certa estrutura pode ser complicado de se trabalhar, obter um isomorfismo entre tal estrutura e outra da qual já são conhecidas algumas características, ou propriedades, é bastante útil.

Exemplo 1.7 *Segue do Teorema 1.9 que $\mathbb{Z}_{12}$ tem um subgrupo de ordem 4, $H = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\}$. Consideramos a aplicação $f : \mathbb{Z}_4 \to H$ dada por $\overline{a} \in \mathbb{Z}_4 \mapsto f(\overline{a}) = 3 \cdot \overline{a}$. Sem dificuldades, verifica-se que f é um isomorfismo. Além disso, $\mathbb{Z}_{12}/H$ é grupo e consta de 3 elementos, que são $H+\overline{0}, H+\overline{1}, H+\overline{2}$. Mais ainda: $\mathbb{Z}_{12}/H$ é isomorfo a $\mathbb{Z}_3$ com a aplicação $g : \mathbb{Z}_3 \to \mathbb{Z}_{12}/H$ dada por $g(\overline{a}) = H + \overline{a}$.*

Teorema 1.11 (Isomorfismo) *Seja $f : G \to H$ um homomorfismo de grupos. Então, $G/\ker f$ é isomorfo a $f(G)$.*

A seguir recordamos algumas noções necessárias para apresentarmos a equação das classes, a qual utilizaremos em especial na demonstração do Teorema de Wedderburn. Para isso, nossa referência é a seção 4 do capítulo 6 de (GONÇALVES, 1979).

Seja G um grupo. Dados $a, b \in G$, diremos que a se relaciona com b, e denotamos por $a \sim b$, se existe $g \in G$ tal que $a = gbg^{-1}$. Verifica-se facilmente que esta é uma relação de equivalência em G. Denotaremos por C_a a classe determinada por $a \in G$ com respeito a relação $\sim$, isto é, $C_a = \{b \in G : a = gbg^{-1}$ para algum $g \in G\}$. O conjunto C_a é chamado de **classe de conjugação** determinada pelo elemento a.

O **normalizador** de a em G, o qual denotaremos por N_a, é conjunto dos elementos de G que comutam com $a \in G$, isto é, $N_a = \{b \in G : ab = ba\}$. O **centro** do grupo G, o qual denotaremos por $Z(G)$, é o conjunto dos elementos de G que comutam com todos os elementos de G, isto é, $Z(G) = \{g \in G : gb = bg$ para todo $b \in G\}$. É fácil mostrar que N_a e $Z(G)$ são subgrupos de G.

Teorema 1.12 *Se G é um grupo finito e $a \in G$, então $\#(C_a) = [G : N_a]$. Em particular, $\#(C_a)$ divide $|G|$.*

***Demonstração**:* Seja $H = N_a$. Note que $G/H := \{Hg : g \in G\}$ é o conjunto de todas as classes de equivalência de $g \in G$ com respeito à congruência à direita módulo H. Consideremos a aplicação

$$\begin{aligned} \Psi \colon G/H &\longrightarrow C_a \\ Hg &\longmapsto \Psi(Hg) = gag^{-1}. \end{aligned}$$

Claramente Ψ é sobrejetiva. Além disso, Ψ é injetiva pois se $\Psi(Hx) = \Psi(Hy)$ então $gxg^{-1} = gyg^{-1} \implies x = y \implies Hx = Hy$. Logo Ψ é bijetiva e assim $\#(G/H) = \#(C_a)$. Mas por definição de índice, $\#(G/H) = [G : H]$. Portanto $[G : H] = \#(C_a)$ divide $|G|$ pelo Teorema de Lagrange.

Teorema 1.13 (Equação das Classes) *Suponhamos que G é um grupo finito. Sejam $C_{x_1}, C_{x_2}, \cdots C_{x_k}$ as distintas classes de conjugação em G. Então*

$$|G| = |Z(G)| + \sum_{x \notin Z(G)} \#(C_x). \tag{1.2}$$

***Demonstração**:* Sendo $\sim$ uma relação de equivalência em G, temos

$$|G| = \#(C_{x_1}) + \#(C_{x_2}) + \cdots + \#(C_{x_k}).$$

Agora observamos que $x_i \in Z(G)$ se, e somente se $C_{x_i} = \{x_i\}$, pois se $x_i \in Z(G)$ então

$$\begin{aligned} C_{x_i} &= \{b \in G : x_i = gbg^{-1} \text{ para algum } g \in G\} \\ &= \{b \in G : x_i g = gb \text{ para algum } g \in G\} \\ &= \{b \in G : gx_i = gb\} \\ &= \{b \in G : x_i = b\} \\ &= \{x_i\}; \end{aligned}$$

e reciprocamente, se $C_{x_i} = \{x_i\}$, então x_i é o único elemento do conjunto $\{b \in G : x_i = gbg^{-1} \text{ para algum } g \in G\}$, logo $x_i = gx_ig^{-1} \iff gx_i = x_ig \implies x_i \in Z(G)$. Assim,

$$|Z(G)| = \sum_{x_i \in Z(G)} \#(\{x_i\}) = \sum_{x_i \in Z(G)} \#(C_{x_i}),$$

portanto

$$|G| = \left(\sum_{x_i \in Z(G)} \#(C_{x_i}) \right) + \left(\sum_{x_i \notin Z(G)} (\#C_{x_i}) \right) = |Z(G)| + \sum_{x_i \notin Z(G)} \#(C_{x_i}).$$

1.2 Anéis

Nesta seção apresentamos o conceito de anel e deduzimos algumas propriedades. Assim como a teoria do grupos, a teoria dos anéis é vasta e pode ser investigada teoricamente para diversos fins. Vamos nos concentrar no que é necessário para o estudo dos corpos, que são um tipo particular de anel.

Definição 1.16 *Um **anel** é um conjunto não vazio A, munido de duas operações binárias $+$ e $\cdot$ chamadas respectivamente de soma e multiplicação, satisfazendo as seguintes condições:*

1. *$(A,+)$ é grupo abeliano.*
2. *A multiplicação é associativa em A, isto é, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ para quaisquer $a, b, c \in A$.*
3. *Valem as leis de distributividade, isto é, $(a+b)\cdot c = a\cdot c + b\cdot c$ e $a\cdot(b+c) = a\cdot b + a\cdot c$ para quaisquer $a, b, c \in A$.*

Exemplo 1.8 *Os conjuntos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ são anéis com as operações usuais de soma e multiplicação. O conjunto dos naturais $\mathbb{N}$ não é anel pois $(\mathbb{N}, +)$ não é grupo.*

Definição 1.17 *Seja A um anel.*

1. *Dizemos que A é um **anel com identidade** se existe $1_A \in A$, chamado de **elemento neutro de A com respeito a multiplicação**, tal que $a1_A = a1_A = a$ para todo $a \in A$.*
2. *Dizemos que A é um **anel comutativo** se a multiplicação é comutativa em A, isto é, se $ab = ba$ para quaisquer $a, b \in A$.*
3. *Dizemos que A é um **domínio de integridade** se A é anel comutativo com identidade $1_A \neq 0_A$ e sem **divisores de zero**, isto é, sempre que $a, b \in A$ são tais que $ab = 0$, então $a = 0$ ou $b = 0$.*
4. *Dizemos que A é um **anel de divisão** se os elementos não nulos de A formam um grupo com respeito à operação de multiplicação.*
5. *Dizemos que A é um **corpo** se A é um anel de divisão comutativo.*

De modo equivalente, podemos olhar para um corpo $(A, +, *)$ do seguinte modo: $(A, +)$ é grupo abeliano, $(A \setminus \{0_A\}, *)$ é grupo abeliano e valem as leis de distributividade.

Teorema 1.14 *Todo corpo é domínio de integridade.*

***Demonstração**:* Seja F um corpo e sejam $a, b \in F$ tais que $ab = 0$ com $a \neq 0_F$. Então, multiplicando $ab = 0$ por $a^{-1} \in F$, temos $b = a^{-1}(ab) = a^{-1} \cdot 0 = 0$.

A recíproca deste Teorema é válida quando o domínio de integridade for finito:

Teorema 1.15 *Todo domínio de integridade finito é um corpo.*

***Demonstração**:* Seja D um domínio de integridade com um número finito de elementos. É suficiente mostrarmos que todo elemento não nulo de D admite inverso multiplicativo, pois os demais axiomas são satisfeitos pela definição de domínio de integridade. Seja $b \in D$ um elemento não nulo e considere a aplicação $f : D \to D$ dada por $f(x) = bx$. Observemos que $f(r) = f(s)$ implica $br = bs \iff b(r-s) = 0_D$ e, sendo D um domínio de integridade e $b \neq 0_D$, temos que $r = s$ logo f é injetiva. Como D é um conjunto finito, então f também é sobrejetiva, logo é bijetiva. Assim, todo elemento de D é da forma bx. Em particular, $1_D = bc$, para algum $c \in D$, isto é, b admite inverso multiplicativo.

Definição 1.18 *Seja A um anel e S um subconjunto não vazio de A. Dizemos que S é **subanel** de A se S é anel com as operações de A restritas a S.*

O resultado a seguir caracteriza os subanéis com apenas duas condições.

Teorema 1.16 (Critério de subanel) *Seja A um anel e S um subconjunto não vazio de A. Então S é subanel de A se, e somente se $a - b \in S$ e $ab \in S$ sempre que $a, b \in S$.*

Exemplo 1.9 *Dado $m \in \mathbb{Z}$, o conjunto $\langle m \rangle = \{km : k \in \mathbb{Z}\}$ é subanel de $\mathbb{Z}$. De fato, se $am, bm \in \langle m \rangle$, então $(am - bm) = (a-b)m \in \langle m \rangle$ e $(am)(bm) = (amb)m \in \langle m \rangle$.*

Assim como no caso dos grupos, vamos construir anéis especiais que provém de um quociente de anéis. Para isso, introduzimos o uma importante classe de subanéis:

Definição 1.19 *Seja A um anel comutativo e I um subconjunto não vazio de A. Dizemos que I é um **ideal** de A quando as seguintes condições são satisfeitas:*

1. *$a - b \in I$ sempre que $a, b \in I$.*
2. *$ai \in I$ sempre que $a \in A$ e $i \in I$.*

Segue imediatamente da definição 1.19 que todo ideal é subanel.

Exemplo 1.10 *Dado $m \in \mathbb{Z}$, o conjunto $< m >$ é ideal de $\mathbb{Z}$. De fato, se $am, bm \in < m >$, então $am - bm = (a-b)m \in < m >$. Além disso, se $z \in \mathbb{Z}$ e $am \in < m >$, então $z(am) = (za)m \in < m >$.*

Seja A um anel e S um subanel de A. Ignoremos por um instante a operação multiplicação de A. Segue do Teorema 1.10 que $(A/S, +)$ é grupo abeliano. Denotaremos

por $\overline{a}$ o elemento $I + a \in A/S$. Diremos que dois elementos $a, b \in A$ são **congruentes** módulo S se $\overline{a} = \overline{b}$, ou equivalentemente pelo item 3 do Corolário 1.1, se $(a - b) \in S$.

O resultado a seguir nos dá condições necessárias e suficientes para que A/S seja um anel com a operação multiplicação induzida pela multiplicação de A.

Teorema 1.17 *Seja $A = (A, +, \cdot)$ um anel comutativo e I um subanel de A. Então, as seguintes afirmações são equivalentes:*

1. *I é ideal de A.*
2. *O grupo quociente aditivo A/I é anel com a operação de multiplicação dada por*

$$\overline{a} \odot \overline{b} = \overline{a \cdot b}.$$

***Demonstração**:* (1) implica (2). Supondo que I é um ideal de A, temos que $(I, +)$ é subgrupo normal de $(A, +)$. A soma em A/I dada por $\overline{a} \oplus \overline{b} = \overline{a + b}$ está bem definida pelo Teorema 1.10, e $(A/I, \oplus)$ é grupo abeliano. Para quaisquer $a, b \in A$ e quaisquer $i, j \in I$, temos

$$\overline{a} \odot \overline{b} = (a + i)(b + j) = ab + \underbrace{(aj + ib + ij)}_{\in I} \in \overline{ab},$$

logo a operação $\odot$ está definida para quaisquer $a, b \in A/I$. Mostremos que a igualdade estipulada no item 2 independe da escolha de $x \in \overline{a}$ e $y \in \overline{b}$. Sejam $x, x' \in \overline{a}$ e $y, y' \in \overline{b}$. Então, $x' \in \overline{x} = \overline{x'}$, logo $x' = x + k$ para algum $k \in I$. Similarmente, $y' = y + l$ para algum $l \in I$. Assim,

$$x'y' = (x + k)(y + l) = xy + \underbrace{(xl + ky + kl)}_{\in I} \in \overline{xy},$$

e a operação $\odot$ está bem definida. Além disso, a associatividade e distributividade da multiplicação em A/I decorrem da associatividade e distributividade da multiplicação em A. Portanto, $(A/I, \oplus, \odot)$ é anel.

(2) implica (1). Suponha que A/I é anel mas I não é ideal. Existem $a \in A$ e $s \in I$ tais que $as \notin I$, ou seja, $\overline{as} \neq \overline{0_A}$. Por outro lado, temos que $s \in S$ implica $\overline{s} = \overline{0_A}$. Portanto, $\overline{a \cdot s} = \overline{a} \odot \overline{s} = \overline{a} \odot \overline{0_A} = \overline{a \cdot 0_A} = \overline{0_A}$, ou seja, $as \in I$, o que é absurdo pois contraria o fato de que $as \notin I$. Portanto, I deve ser ideal de A.

Definição 1.20 *O anel apresentado no Teorema 1.17 é chamado **anel quociente**, ou **anel das classes residuais**, de A módulo o ideal I, e será denotado por A/I.*

Definição 1.21 *Seja m um inteiro não negativo. Denotamos por $\mathbb{Z}_m$, e chamamos de **anel dos inteiros módulo** m, ou simplesmente **anel** $\mathbb{Z}_m$, ao anel quociente $\mathbb{Z}/\langle m \rangle$.*

Exemplo 1.11 *Vamos analisar o anel $\mathbb{Z}_{12}$. Recordamos que para checar a igualdade $\overline{a} = \overline{b}$ no anel $\mathbb{Z}_{12}$, basta verificar que a e b deixam o mesmo resto quando divididos por 12, o que é equivalente a verificar que $(a - b)$ é múltiplo de m. Já vimos como somar em $\mathbb{Z}_m$ no Exemplo 1.5, e também como multiplicar no Exemplo 1.6. Acontece que estas operações interagem entre si de maneira natural. Por exemplo, para verificarmos que $\overline{3}(\overline{5} + \overline{6}) = \overline{9}$, observamos que pela distributividade em $\mathbb{Z}_{12}$, temos $\overline{3}(\overline{5} + \overline{6}) = \overline{3 \cdot 5} + \overline{3 \cdot 6} = \overline{15} + \overline{18}$. Como $\overline{15} = \overline{3}$ e $\overline{18} = \overline{6}$, concluímos que $\overline{15} + \overline{18} = \overline{3} + \overline{6} = \overline{9}$.*

O resultado a seguir caracteriza os anéis $\mathbb{Z}_m$ que são corpos.

Teorema 1.18 *O anel $\mathbb{Z}_m$ é corpo se, e somente se m é primo.*

***Demonstração**:* Suponhamos que $\mathbb{Z}_m$ é corpo mas m não é primo. Pelo Teorema 1.14, temos que $\mathbb{Z}_m$ é domínio de integridade. Como m não é primo, então existem r, s inteiros com $1 < r \leq s < m$ tais que $m = rs$. Logo, $\overline{m} = \overline{r} \cdot \overline{s} = \overline{0}$ com $\overline{r} \neq \overline{0}$ e $\overline{s} \neq \overline{0}$, isto é, $\mathbb{Z}_m$ não é domínio de integridade, absurdo. Portanto, m deve ser primo.

Reciprocamente, suponhamos que m é primo. Observemos que $\mathbb{Z}_m$ é anel comutativo e contém a identidade multiplicativa $\overline{1}$. Dados $\overline{a}, \overline{b} \in \mathbb{Z}_m$, temos $\overline{a} \cdot \overline{b} = \overline{ab} = \overline{0}$ se, e somente se $ab \in < m >$, isto é, se $ab = km$ para algum $k \in \mathbb{Z}$. Como m é primo, temos duas possibilidades: m divide a (neste caso $\overline{a} = \overline{0}$) ou m divide b (neste caso $\overline{b} = \overline{0}$). Isso mostra que $\mathbb{Z}_m$ é domínio de integridade finito, e portanto é corpo pelo Teorema 1.15.

Dado um primo p, podemos facilmente obter a **tabela de operações** do corpo $\mathbb{Z}_p$.

Exemplo 1.12 *Os elementos do corpo $\mathbb{Z}_5$ são $\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ e sua tabela de operações é*

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

A seguir, apresentamos algumas noções sobre morfismos de anéis.

Definição 1.22 *Sejam $A = (A, +, \cdot)$ e $B = (B, \oplus, \odot)$ anéis.*

1. *Dizemos que uma aplicação $f : A \to B$ é um **homomorfismo de anéis** se*

$$f(x + y) = f(x) \oplus f(y) \text{ e } f(x \cdot y) = f(x) \odot f(y) \text{ para quaisquer } x, y \in A.$$

2. *Dizemos que $f : A \to B$ é um **isomorfismo de anéis** se f é homomorfismo de anéis e é bijetiva. Neste caso, dizemos que A e B são **isomorfos**.*

3. O ***núcleo*** *de um homomorfismo de anéis $f : A \to B$ é definido e denotado por*

$$\ker f = \{a \in A : f(a) = 0_B\}.$$

Dado um homomorfismo de anéis $f : A \to B$, observemos que o núcleo $\ker f$ é um ideal de A e a imagem $f(A)$ é subanel de B. O resultado a seguir nos diz que podemos obter um isomorfismo de anéis a partir de um homomorfismo de anéis.

Teorema 1.19 (Isomorfismo) *Seja $f : A \to B$ um homomorfismo de anéis. Então, $A/\ker f$ é isomorfo a B. Além disso, se I é um ideal de A, então a aplicação $g : A \to A/I$ dada por $g(a) = \overline{a}$ é um homomorfismo de anéis sobrejetor cujo núcleo é I.*

Teorema 1.20 *Seja p primo. A aplicação*

$$\begin{aligned} \pi \colon \mathbb{Z} &\longrightarrow \mathbb{Z}_p \\ a &\longmapsto \pi(a) = \overline{a} \end{aligned}$$

é um homomorfismo de anéis sobrejetor com $\ker \pi = \langle p \rangle$.

Demonstração*:* Para quaisquer $x, y \in \mathbb{Z}$, temos

$$\pi(x+y) = \overline{x+y} = \overline{x} + \overline{y} = \pi(x) + \pi(y)$$

e

$$\pi(xy) = \overline{xy} = \overline{x} \cdot \overline{y} = \pi(x) \cdot \pi(y),$$

logo π é homomorfismo de anéis, o qual é sobrejetivo pois $\pi(a) = \overline{a}$ para $a \in \{0, 1, \cdots, p-1\}$. Agora, seja $u \in \ker \pi$ e suponha por absurdo que u não é múltiplo de p. Pelo Algoritmo da Divisão para os inteiros u e p, existem únicos k, r tais que $u = kp + r$ com $0 < r < p$. Sendo π homomorfismo de anéis, temos $\overline{0} = \pi(u) = \pi(kp + r) = \overline{k} \cdot \overline{p} + \overline{r} = \overline{r}$, o que é absurdo pois $0 < r < p$, logo r não pode ser múltiplo de p. Assim, todo $u \in \ker \pi$ é da forma kp para algum $k \in \mathbb{Z}$, isto é, $\ker \pi = \langle p \rangle$.

O homomorfismo do Teorema 1.20 é chamado **projeção canônica** de $\mathbb{Z}$ sobre $\mathbb{Z}_p$.

Definição 1.23 *Seja A um anel. A* ***característica*** *de A, a qual denotaremos por $\operatorname{char} A$, é o menor inteiro positivo n tal que $na = 0_A$ para todo $a \in A$. Caso não exista um inteiro positivo com esta propriedade, definimos $\operatorname{char} A = 0$ e, neste caso, dizemos que A tem* ***característica zero****.*

Exemplo 1.13 *Seja m um inteiro positivo. Temos que o anel $\mathbb{Z}_m$ tem característica m. De fato, dado $\overline{x} \in \mathbb{Z}_m$ temos $m \cdot \overline{x} = 0$, mas $a \cdot \overline{1} = \overline{a} \neq \overline{0}$ para todo $0 < a < m$.*

A característica de um anel com identidade pode ser facilmente determinada:

Teorema 1.21 *Seja $A = (A, +, \cdot)$ um anel com identidade e considere o grupo $G = (A, +)$.*

1. *Se 1_A tem ordem infinita no grupo G, então A tem característica zero.*
2. *Se 1_A tem ordem finita m no grupo G, então A tem característica m.*

***Demonstração**:*

1. Suponhamos que 1_A tem ordem infinita no grupo G. Então não existe inteiro positivo m tal que $0_A = a + a + \cdots + a = m \cdot a$ (m parcelas), ou seja, $\operatorname{char} A = 0$.
2. Suponhamos agora que 1_A tem ordem finita m no grupo G. Temos $b \cdot 1_A \neq 0_A$ para $0 < b < m$, o que implica $m = \operatorname{char} A$ pois $0_A = 1_A + 1_A + \cdots + 1_A = m \cdot 1_A$ e assim, para qualquer $b \in A$,

$$\begin{aligned} m \cdot b &= b + b + \cdots + b \ (m \text{ parcelas}) \\ &= 1_A b + 1_A b + \cdots 1_A b \\ &= (1_A + 1_A + \cdots + 1_A) \cdot b \\ &= (m \cdot 1_A) \cdot b \\ &= 0_A \cdot b \\ &= 0_A. \end{aligned}$$

A seguir, classificamos a característica dos domínios de integridade.

Teorema 1.22 *A característica de um domínio de integridade ou é zero ou é um número primo.*

***Demonstração**:* Seja D um domínio de integridade. Suponha que $\operatorname{char} D = p > 0$. Como D possui pelos menos os elementos 0_D e 1_D, então $p \geq 2$. Suponhamos por absurdo que p não é primo, ou seja, $p = rs$ com $1 < r \leq s < p$. Então, $0_D = p \cdot 1_D = (rs) \cdot 1_D = (r \cdot 1_D)(s \cdot 1_D)$. Logo, $(r \cdot 1_D) = 0_D$ ou $(s \cdot 1_D) = 0_D$ pois D é domínio de integridade. Assim, para $0_D \neq a \in D$ teríamos que $r \cdot a = r \cdot (1_D a) = (r \cdot 1_D)a = 0_D a = 0_D$. Ou, de modo análogo, teríamos $s \cdot a = 0_D$. Mas qualquer destas alternativas contraria a minimalidade de p. Portanto, p deve ser primo.

Corolário 1.4 *Todo corpo finito tem característica prima.*

***Demonstração**:* Seja F um corpo com um número finito de elementos. É suficiente mostrarmos que F tem característica positiva, pois F é domínio de integridade pelo Teorema 1.14, e portanto F terá característica prima pelo Teorema 1.22. Seja e o elemento identidade com relação à multiplicação de F. Considere os elementos $e, 2e, 3e, \cdots$. Sendo F um conjunto finito, existem $1 \leq k < n$ tais que $ke = ne$, o que implica $(n-k)e = 0$. Agora, para qualquer $a \in F$, temos que $a = ea$, logo $(n-k)a = ((n-k)e)a = 0_F a = 0_F$. Portanto, $\operatorname{char} F = n - k > 0$.

Teorema 1.23 *Seja A um anel comutativo com característica prima p. Então,*

$$(a \pm b)^{p^n} = a^{p^n} \pm b^{p^n} \text{ para quaisquer } a, b \in A \text{ e qualquer } n \in \mathbb{N}.$$

***Demonstração**:* Procedemos por indução sobre n. Para $n = 1$, observemos que

$$\binom{p}{i} = \frac{p(p-1)\cdots(p-i+1)}{1 \cdot 2 \cdots i} \equiv 0 \pmod{p} \text{ para cada } 0 < i < p,$$

pois nestes casos o numerador sempre é um múltiplo do primo p. Logo,

$$(a+b)^p = a^p + \binom{n}{1} a^{p-1}b + \cdots + \binom{p}{p-1} ab^{p-1} + b^p = a^p + b^p.$$

Suponhamos agora que $(a+b)^{p^n} = a^{p^n} + b^{p^n}$ para algum $1 < n$. Temos

$$(a+b)^{p^{n+1}} = ((a+b)^{p^n})^p = (a^{p^n} + b^{p^n})^p = a^{p^{n+1}} + b^{p^{n+1}}.$$

Além disso, $a^{p^n} = ((a-b)+b)^{p^n} = (a-b)^{p^n} + b^{p^n}$, portanto $(a \pm b)^{p^n} = a^{p^n} \pm b^{p^n}$.

1.3 Ideais

De acordo com o Teorema 1.17, o quociente A/I só é anel quando I é um ideal do anel A. Nesta seção, analisamos alguns tipos especiais de ideais e classificamos os anéis quocientes associados.

Definição 1.24 *Seja A um anel comutativo com identidade.*

1. *Um elemento $a \in A$ é chamado de **divisor** de $b \in A$ se existe $c \in A$ tal que $ac = b$.*
2. *Um elemento $u \in A$ é chamado de **inversível** de A se é um divisor da identidade, isto é, se existe $r \in A$ tal que $ru = 1_A$.*
3. *Dois elementos $a, b \in A$ são chamados de **associados** se existe um elemento inversível $u \in A$ tal que $a = ub$.*

4. *Um elemento $c \in A$ é chamado de **elemento primo** de A se c não é inversível e tem como divisores apenas os inversíveis de A e os associados de c.*

5. *Dizemos que P é um **ideal primo** de A se P é um ideal de A, $P \neq A$ e, sempre que $a, b \in A$ são tais que $ab \in P$, então $a \in P$ ou $b \in P$.*

6. *Dizemos que M é um **ideal maximal** de A se M é um ideal de A, $M \neq A$ e sempre que I é um ideal de A com $M \subseteq I$, então $I = M$ ou $I = A$.*

7. *Dizemos que P é um **ideal principal** de A se P é um ideal de A e existe $b \in A$ tal que $P = \langle b \rangle = \{bk : k \in A\}$.*

8. *Dizemos que A é um **domínio de ideais principais** se A é um domínio de integridade tal que todo ideal de A é um ideal principal.*

Teorema 1.24 *A interseção arbitrária de ideais é um ideal.*

***Demonstração**:* Seja $\{I_\lambda\}_{\lambda \in L}$ uma família de ideais do anel A. Vejamos que

$$J := \bigcap_{\lambda \in L} I_\lambda$$

é um ideal de A. De fato, se $a, b \in J$, então $a, b \in I_\lambda$ implica que $a - b \in I_\lambda$ para cada $\lambda \in L$ pois cara I_λ é ideal de A. Logo, $a - b \in J$. Além disso, se $r \in J$ e $a \in A$, então $r \in I_\lambda$ implica $ra \in I_\lambda$ para cada $\lambda \in L$ pois cada I_λ é ideal, ou seja, $ra \in J$.

Corolário 1.5 *Seja A um anel e $c \in A$. O conjunto*

$$(c) = \bigcap_{\substack{c \in I \\ I \text{ é ideal de } A}} I$$

é o menor ideal de A que contém c.

***Demonstração**:* Sendo A um ideal de A que contém c, a interseção estipulada é não vazia. Tomando $L = \{I \subseteq A : I \text{ é ideal de } A \text{ e } c \in I\}$ e aplicando o Teorema 1.24, vemos que (c) é ideal de A. Além disso, se J é um ideal de A que contém c e $J \subseteq (c)$, então J é um dos conjuntos sobre os quais a interseção é tomada, logo $(c) \subseteq J$ e portanto $J = (c)$.

O ideal apresentado no Corolário 1.5 é chamado de **ideal gerado** por c.

O resultado a seguir é de grande importância teórica. Ele nos dá uma caracterização de certos ideias em termos do anel quociente associado.

Teorema 1.25 *Seja A um anel com identidade.*

1. *Um ideal M de A é maximal se, e somente se A/M é corpo.*
2. *Um ideal P de A é primo se, e somente se A/P é domínio de integridade.*
3. *Todo ideal maximal é um ideal primo.*
4. *Suponha que A é um domínio de ideais principais. Então, $A/(c)$ é corpo se, e somente se c é um elemento primo de A.*

***Demonstração**:*

1. Suponhamos que M é um ideal maximal de A. Por definição, existe $t \in A \setminus M$. Para $t \notin M$ fixo, consideremos o conjunto $J = \{ta + m : a \in A \text{ e } m \in M\}$. Temos que $J \neq \emptyset$ pois existem $1_A \in A$ e $m \in M$ tais que $t1_A + m = t + m \in J$. Além disso,

   - Se $u, v \in J$, então $u = ta+m, v = ta'+m'$ com $a, a' \in A$ e $m, m' \in M$. Como A e M são anéis, então $a-a' \in A$ e $m-m' \in M$; logo $t(a-a')+(m-m') = u-v \in J$.
   - Se $u \in J$ e $b \in A$, então $u = ta+m$ com $a \in A$ e $m \in M$, logo $ub = (ta+m)b = t(ba) + mb$, mas $ba \in A$ e, sendo M ideal, temos $mb \in M$ e portanto $ub \in J$.

   Logo, J é um ideal. Tomando $a = 0_A$ na definição de J, vemos que J contém propriamente o ideal maximal M, consequentemente $J = A$. Como A contém a identidade 1_A, temos que $1_A = ta + m$ para algum $a \in A$ e algum $m \in M$. Dessa forma, se $\overline{0} \neq \overline{a} \in A/M$, então existe o inverso multiplicativo de $\overline{a}$. Portanto, A/M é corpo. Reciprocamente, suponhamos que A/M é corpo. Seja I um ideal de A com $M \subsetneq I$. Vamos mostrar que $I = A$. Seja $a \in I \setminus M$. Sendo A/M um corpo e $\overline{a} \neq \overline{0_A}$ (pois $a \notin M$), existe o inverso multiplicativo de $\overline{a}$, isto é, existe $\overline{r} \in A/M$ tal que $\overline{ar} = \overline{1_A}$. Isso implica que $ar + m = 1_A$ para algum $m \in M$. Como $a \in I$, $m \in M \subsetneq I$ e I é ideal, temos $1_A \in I$. Logo, $A \subseteq I$ pois $b \cdot 1_A \in I$ para qualquer $b \in A$.

2. Seja P um ideal primo de A. Claramente A/P é anel comutativo com identidade $\overline{1_A} \neq \overline{0_A}$. Sejam $\overline{x}, \overline{y} \in A/P$ tais que $\overline{xy} = \overline{0}$. Então, $xy \in P$ e, sendo P primo, temos que $x \in P$ (o que implica $\overline{x} = \overline{0}$) ou $y \in P$ (o que implica $\overline{y} = \overline{0}$). Isso implica que A/P é domínio de integridade. Reciprocamente, suponhamos que A/P é domínio de integridade. Sejam $x, y \in P$. Então, $\overline{xy} = \overline{0}$ implica $\overline{x} = \overline{0}$ (logo $x \in P$) ou $\overline{y} = \overline{0}$ (logo $y \in P$). Portanto, P é ideal primo.

3. Seja M um ideal maximal de A. Segue do item 1 que A/M é corpo, logo é domínio de integridade pelo Teorema 1.14. Portanto, M é ideal primo pelo item 2.

4. Suponhamos que $A/(c)$ é um corpo mas c não é elemento primo, isto é, c é inversível ou c admite como divisor um elemento que não é associado de c. Se c é inversível, então $c \in (c)$ e $c^{-1} \in A$ implicam $cc^{-1} = 1_A \in (c)$. Logo, para qualquer $b \in A$, temos $b \cdot 1_A \in (c)$. Assim, $A = (c)$ e o conjunto $A/(c)$ possui um só elemento, portanto não é corpo. Isso mostra que c não pode ser inversível. Seja agora $a \in A$ um divisor de c que não é inversível nem associado de c, isto é, $c = ab$ para algum $b \in A$ não inversível. Observe que $a \neq 0_A$ pois do contrário $c = 0_A$ e a seriam associados de c. Afirmamos que $a \notin (c)$. Do contrário, existiria $d \in A$ tal que $a = cd = abd$, ou seja, $a(1_A - bd) = 0_A$. Sendo $a \neq 0_A$, temos que $bd = 1_A$, isto é, b é inversível. Mas isso é absurdo pois isso contraria a hipótese de que a e c não são associados. Assim, $(c) \subsetneq (a) \subsetneq A$, portanto $A/(c)$ não é corpo pelo item 1. Reciprocamente, suponhamos que c seja um elemento primo. Então, $(c) \neq A$ pois do contrário, $1_A = bc$ para algum $b \in A$, logo c seria inversível, absurdo. Agora, se J é um ideal de A com $(c) \subseteq J$, então $J = (a)$ para algum $a \in A$ pois A é domínio de ideais principais. Segue-se que $c \in (a)$, logo a é um divisor de c. Sendo c um elemento primo, temos que a é inversível (o que implica $A = J$) ou é um associado de c (o que implica $J = (c)$). Portanto, (c) é ideal maximal de A, e daí $A/(c)$ é corpo pelo item 1.

1.4 Polinômios

A noção de polinômios é bem conhecida e constitui uma importante ferramenta neste trabalho. Sabemos somar e multiplicar polinômios com coeficientes reais e operações usuais. Nesta seção, generalizamos estes conceitos e deduzimos alguns resultados.

Definição 1.25 *Seja A um anel. Um **polinômio** sobre A é uma expressão da forma*

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + \cdots + a_n x^n,$$

*com n inteiro não negativo e $a_i \in A$ para $1 \leq i \leq n$. Os elementos a_i são chamados de **coeficientes**, e x é chamado **indeterminada** sobre A.*

Como é usual na literatura, omitimos o termo $a_i x^i$ quando $a_i = 0_A$. Observemos que o polinômio $f(x)$ da definição 1.25 pode ser escrito como $f(x) = a_0 + a_1 x + \cdots + a_n x^n + 0_A x^{n+1} + \cdots + 0_A x^{n+h}$ para qualquer h inteiro positivo. Dados dois polinômios $f(x), g(x)$ sobre A, podemos assumir que neles aparecem as mesmas potências de x.

Definição 1.26 *Seja A um anel. Denotaremos por $A[x]$ o conjunto dos polinômios na indeterminada x com coeficientes em A. Dados $f(x) = \sum_{i=0}^{n} a_i x^i$ e $g(x) = \sum_{i=0}^{n} b_i x^i$, definimos a **soma de polinômios** por*

$$f(x) + g(x) = \sum_{i=0}^{n} (a_i + b_i)x^i.$$

Para $f(x) = \sum_{i=0}^{n} a_i x^i$ *e* $g(x) = \sum_{i=0}^{m} b_i x^i$, *definimos o* ***produto de polinômios*** *por*

$$f(x)g(x) = \sum_{k=0}^{m+n} c_k x^k \text{ onde } c_k = \sum_{i+j=k} a_i b_j \text{ com } 0 \leq i \leq n,\ 0 \leq j \leq m.$$

É fácil ver que $A[x]$ é um anel, o qual chamaremos **anel de polinômios** sobre A.

Teorema 1.26 *Seja A um anel. Então,*

1. *$A[x]$ é comutativo se, e somente se A é comutativo.*
2. *$A[x]$ possui identidade se, e somente se A possui identidade.*
3. *$A[x]$ é domínio de integridade se, e somente se A é domínio de integridade.*

Definição 1.27 *Seja A um anel e $f(x) = \sum_{i=0}^{n} a_i x^i \in A[x]$ um polinômio não nulo com $a_n \neq 0$.*

1. *Dizemos que a_n é o* ***coeficiente líder*** *de $f(x)$, e a_0 é o* ***coeficiente constante*** *de $f(x)$.*
2. *Dizemos que n é o* ***grau*** *de $f(x)$, o qual denotaremos por* $\deg(f(x))$. *Por convenção, definimos* $\deg(0) = -\infty$.
3. *Dizemos que polinômios com grau 0 ou $-\infty$ são* ***polinômios constantes***.
4. *Dizemos que $f(x)$ é um* ***polinômio mônico*** *se A possui identidade multiplicativa 1_R e o coeficiente líder de $f(x)$ é 1_R.*

A fim de simplificarmos a notação, sempre que não houver dúvidas, indicamos apenas $f \in A[x]$ para indicar $f(x) \in A[x]$, e escrevemos $\deg(f)$ para indicar $\deg(f(x))$.

Comparando os coeficientes líderes de dois polinômios, temos o seguinte resultado.

Teorema 1.27 *Para quaisquer $f, g \in A[x]$, temos*

1. $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$.
2. $\deg(fg) \leq \deg(f) + \deg(g)$.
3. $\deg(fg) = \deg(f) + \deg(g)$, *sempre que A é domínio de integridade.*

Como estamos interessados em anéis de polinômios com coeficientes em um corpo, no que se segue F sempre denotará um corpo. Observamos que a definição 1.24 se aplica ao anel $F[x]$. Neste caso, dados $f, g \in F[x]$, dizemos que f **divide** g, ou g é **múltiplo** de f, se existe $h \in F[x]$ tal que $f(x) = g(x)h(x)$. Note que os inversíveis de $F[x]$ são os elementos não nulos de F.

A seguir, uma terminologia especial para os elementos primos de $F[x]$.

Definição 1.28 *Dizemos que um polinômio $i \in F[x]$ é **irredutível** sobre F se i tem grau positivo e, sempre que $a, b \in F[x]$ são tais que $i = ab$, temos que a ou b é constante. Chamamos de **redutível** um polinômio que não é irredutível.*

Lema 1.1 *Sejam m e n inteiros positivos. Então, m divide n se, e somente se $x^m - 1_F$ divide $x^n - 1_F$ em $F[x]$.*

***Demonstração**:* Suponha que m divide n, isto é, $n = km$ para algum inteiro positivo k. Temos que $x^m - 1_F$ divide $x^n - 1_F$ pois

$$x^n - 1_F = x^{km} - 1_F = (x^m - 1_F)(x^{m(k-1)} + x^{m(k-2)} + \cdots + x^m + 1_F).$$

Reciprocamente, suponha que $x^m - 1_F$ divide $x^n - 1_F$. Pelo Algoritmo da Divisão, existem únicos r, s inteiros tais que $n = rm + s$ com $0 \leq s < m$. Logo

$$x^n - 1_F = x^{rm+s} - 1_F = (x^{sm} - 1_F)x^r + (x^r - 1_F).$$

Como m divide sm, então $x^m - 1_F$ divide $x^{sm} - 1_F$ e, como $x^m - 1_F$ divide $x^n - 1_F$ por hipótese, temos que $x^m - 1_F$ divide $x^r - 1_F$. Mas esta divisão só é possível se $r = 0$ pois $r < m$, logo $r = 0$. Assim, $x^n - 1_F = x^{sm} - 1_F$ implica que m divide n.

A seguir, apresentamos a generalização da divisão de inteiros.

Teorema 1.28 (Algoritmo da divisão) *Seja $g \in F[x]$ um polinômio não nulo. Para qualquer $f \in F[x]$, existem polinômios $q, r \in F[x]$ tais que*

$$f(x) = q(x)g(x) + r(x) \text{ com } \deg(r) < \deg(g).$$

Um domínio de integridade no qual é válido o algoritmo da divisão é chamado de **domínio Euclidiano**.

Teorema 1.29 *$F[x]$ é um domínio de ideais principais, e para cada ideal $I \neq \{0_F\}$ de $F[x]$, existe um único polinômio mônico $f \in F[x]$ irredutível sobre F com $I = (f)$.*

O resultado a seguir é o análogo para polinômios do mdc de inteiros.

Teorema 1.30 (mdc para polinômios) *Sejam $f_1, f_2 \cdots, f_n \in K[x]$ polinômios não todos nulos. Existe um único polinômio mônico $d \in F[x]$ com as seguintes propriedades:*

1. *d divide f_i para $1 \leq i \leq n$.*
2. *Se $c \in F[x]$ divide cada f_i, então c divide d.*

Além disso, d pode ser escrito da forma $d = b_1 f_1 + \cdots + b_n f_n$ com $b_i \in F[x]$ para $1 \leq i \leq n$.

O polinômio d do Teorema 1.30 é chamado de **máximo divisor comum** dos polinômios $f_1, \cdots f_n$, e será denotado por $d = \text{mdc}(f_1, \cdots, f_n)$.

Dizemos que os polinômios $f_1, \cdots, f_n$ são

1. **relativamente primos** se $\text{mdc}(f_1, \cdots, f_n) = 1$.
2. **primos em pares** se $\text{mdc}(f_i, f_j) = 1$ para $1 \leq i < j \leq n$.

Para polinômios também vale o análogo de mmc de inteiros.

Teorema 1.31 (mmc para polinômios) *Sejam $f_1, \cdots, f_n \in F[x]$ polinômios não nulos. Existe um único polinômio $m \in F[x]$ com as seguintes propriedades:*

1. *m é múltiplo de cada f_i para $1 \leq i \leq n$.*
2. *Se $b \in F[x]$ é múltiplo de cada f_i com $1 \leq i \leq n$, então b é múltiplo de m.*

O polinômio m do Teorema 1.31 é chamado **mínimo múltiplo comum** de $f_1, \cdots, f_n$, e será denotado por $m = \text{mmc}(f_1, \cdots, f_n)$.

Exemplo 1.14 *$p(x) = x^2 - 2 \in \mathbb{Q}[x]$ é irredutível sobre $\mathbb{Q}$, mas é redutível sobre $\mathbb{R}$.*

Teorema 1.32 *Sejam $p, f_1, f_2, \cdots f_n \in F[x]$ com p irredutível sobre F. Se p divide o produto $f_1 f_2 \cdots f_n$, então p divide pelo menos um dos fatores f_i.*

Teorema 1.33 (Fatoração única) *Todo polinômio $f \in F[x]$ de grau positivo pode ser fatorado na forma*

$$f = a p_1^{e_1} \cdots p_k^{e_k}, \tag{1.3}$$

onde $a \in F$, $p_1, \cdots, p_k \in F[x]$ são polinômios mônicos distintos e irredutíveis sobre F, e $e_1, \cdots, e_k$ são inteiros positivos. Essa fatoração é única a menos da ordem dos fatores.

Um domínio de integridade no qual vale o Teorema 1.33 é chamado **domínio de fatoração única**. A igualdade (1.3) é chamada de **fatoração canônica** do polinômio f.

A seguir vemos como obter um corpo a partir de um polinômio irredutível.

Teorema 1.34 *Seja $f \in F[x]$. O anel quociente $F[x]/(f)$ é um corpo se, e somente se f é um polinômio irredutível sobre F.*

***Demonstração**:* Segue imediatamente do item 4 do Teorema 1.25, pois f ser irredutível sobre F equivale a f ser elemento primo de $F[x]$.

Exemplo 1.15 *$p(x) = x^2 - 1$ é irredutível sobre $\mathbb{R}$ e $\mathbb{R}[x]/(p)$ é um corpo isomorfo a $\mathbb{C}$.*

Exemplo 1.16 *Sejam $F = \mathbb{Z}_p$ com p primo e $f \in F[x]$ um polinômio, não necessariamente irredutível, de grau positivo m. Dado um polinômio $g \in F[x]$, temos pelo Algoritmo da Divisão que $g = fq + r$ com $\deg(r) < m$. Dessa forma, no anel quociente $F[x]/(f)$ temos $\overline{g} = \overline{fg} + \overline{r} = \overline{r}$. Observando que os possíveis $r(x)$ são da forma $r(x) = a_0 + a_1x + \cdots + a_{m-1}x^{m-1}$, e para cada $k \in \{0, 1, \cdots, n-1\}$ o coeficiente a_k admite os p valores de F. Temos pelo princípio de contagem que existem p^m classes em $F[x]/(f)$.*

Seja $f \in F[x]$ um polinômio não nulo. Lembramos que $b \in F$ é uma **raiz** de f se $f(b) = 0_F$. O resultado a seguir caracteriza as raízes.

Teorema 1.35 *O elemento $b \in F$ é raiz de $f \in F[x]$ se, e somente se $(x - b)$ divide $f(x)$.*

Definição 1.29 *Seja $b \in F$ uma raiz do polinômio não nulo $f \in F[x]$ e k um inteiro positivo. Dizemos que k é a **multiplicidade** da raiz b se $f(x)$ é divisível por $(x - b)^k$, mas $f(x)$ não é divisível por $(x - b)^{k+1}$. Dizemos que b é uma **raiz simples** se $k = 1$, e dizemos que b é uma **raiz múltipla** se $k \geq 2$.*

Teorema 1.36 *Seja $f \in F[x]$ um polinômio não nulo de grau m. Se $b_1, \cdots b_m \in F$ são raízes de f com multiplicidades $k_1, \cdots k_m$ respectivamente, então $(x - b_1)^{k_1} \cdots (x - b_m)^{k_m}$ divide f. Além disso, $m_1 + \cdots m_k \leq m$ e f tem no máximo m raízes distintas em F.*

Definição 1.30 *Seja $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in F[x]$. A **derivada** de f, a qual denotaremos por f', é definida por $f'(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1}$.*

A derivada nos permite caracterizar polinômios cujas raízes são simples.

Teorema 1.37 *Todas as raízes de um polinômio $f \in F[x]$ são simples se, e somente se $\text{mdc}(f, f') = c$ com $c \in F$ constante.*

A seguir, dois critérios de redutibilidade.

Teorema 1.38 *Seja $f \in F[x]$ um polinômio de grau 2 ou 3. Então, f é redutível sobre F se, e somente se f tem uma raiz em F.*

Lema 1.2 (Gauss) *Seja $f \in \mathbb{Z}[x]$. Se f é redutível sobre $\mathbb{Q}$, então f é redutível sobre $\mathbb{Z}$.*

1.5 Corpos

Nesta seção investigamos com mais profundidade a estrutura corpo. Para nossos objetivos neste trabalho, estamos interessados nas chamadas extensões finitas.

Definição 1.31 *Sejam F e K corpos. Dizemos que K é **subcorpo** de F se $K \subseteq F$ e K é corpo com as operações de F restritas a K. No caso afirmativo, dizemos que F é uma **extensão** de K, e denotamos isso por $F|K$.*

O resultado a seguir caracteriza os subcorpos.

Teorema 1.39 *Seja F um corpo e K um subconjunto não vazio de F. Então, K é subcorpo de F se, e somente se as seguintes condições são satisfeitas:*

1. *Se $a, b \in K$ então $a - b \in K$.*
2. *Se $a, b \in K$ e $b \neq 0_F$ então $ab^{-1} \in K$.*

Seja F uma extensão do corpo K. Podemos olhar para F como um espaço vetorial sobre K - basta tomarmos vetores em F e escalares em K e observarmos que os axiomas de espaço vetorial são satisfeitos.

Definição 1.32 *Seja F uma extensão de K. Definimos o **grau** de F sobre K, o qual denotamos por $[F : K]$, como sendo a dimensão de F como espaço vetorial sobre K, isto é,*

$$[F : K] = \dim_K F.$$

*Dizemos que F é uma **extensão finita** de K quando $[F : K]$ é finito; caso contrário, dizemos que a extensão é infinita.*

Teorema 1.40 *Sejam L uma extensão de F e F uma extensão de K. Então,*

1. *$[L : K] = [L : F][F : K]$.*
2. *$[L : K]$ é finito se, e somente se $[L : F]$ e $[F : K]$ são finitos.*

3. $[F : K] = 1$ *se, e somente se* $F = K$*.*

***Demonstração**:*

1. Suponhamos que $L|F$ e $F|K$ tenham grau m e n respectivamente. Seja $\{l_1, \cdots l_m\}$ uma base de L sobre F, e $\{f_1, \cdots f_n\}$ uma base de F sobre K. Mostraremos que o conjunto $G = \{l_i f_j\}$ com $1 \leq i \leq m$ e $1 \leq j \leq n$ é L.I. sobre K e gera L sobre K. Seja $a_1, \cdots, a_m \in F$ tais que
$$0 = \sum_{i=1}^{m} a_i l_i.$$
Como $\{f_1, \cdots f_n\}$ é base de F sobre K, então para cada $a_i \in F$ existem únicos $b_1^i, \cdots, b_n^i \in K$ tais que
$$a_i = \sum_{j=1}^{n} b_j^i f_j.$$
Assim,
$$0 = \sum_{i=1}^{m} a_i l_i = \sum_{i=1}^{m} (\sum_{j=1}^{n} b_j^i f_j) l_i$$
implica que $\sum_{j=1}^{n} b_j^i f_j = 0$ para cada i pois $\{l_1, \cdots l_m\}$ é base. Mas $\{f_1, \cdots f_n\}$ também é base, logo que $b_j^i = 0$ para cada i e cada j. Portanto G é um conjunto L.I. com mn elementos. Por um argumento análogo, dado $u \in L$, temos que existem únicos $c_j^i \in K$, com $1 \leq i \leq m$ e $1 \leq j \leq n$ tais que
$$u = \sum_{i=1}^{m} (\sum_{j=1}^{n} c_j^i f_j) l_i.$$
Isso mostra que G gera L sobre K e portanto vale $[L : K] = mn = [L : F][F : K]$ sempre que $[L : F] = m$ e $[F : K] = n$. Se pelo menos um dos termos à direita desta igualdade é infinito, digamos $[F : K] = \infty$, então L contém um subconjunto infinito L.I. sobre K, portanto $[L : K] = \infty$.

2. Segue imediatamente do item 1.

3. Suponhamos que $[F : K] = 1$. Seja $\{b\}$ uma base de F sobre K. Sendo $1_F \in F$, então existe $0 \neq a \in K$ tal que $1_F = ba$. Portanto, $a^{-1} = b \in K$. Dessa forma, $F \subseteq K$. A inclusão $K \subseteq F$ é válida pois F é extensão de K por hipótese. Portanto, $F = K$.

Definição 1.33 *Um corpo que não contém subcorpo próprio é chamado de* ***corpo primo****.*

Teorema 1.41 *A interseção arbitrária de subcorpos de* F *é um subcorpo de* F*.*

É possível classificar os subcorpos primos em termos da característica.

Teorema 1.42 *Seja F um corpo e K o subcorpo primo de F. Então,*

1. *K é isomorfo a $\mathbb{Z}_p$, se* $\operatorname{char} F = p$.
2. *K é isomorfo a $\mathbb{Q}$, se* $\operatorname{char} F = 0$.

Definição 1.34 *Seja K um subcorpo de F e M um subconjunto de F. Definimos a* ***extensão de K por adjunção*** *dos elementos de M, a qual denotaremos por $K(M)$, como sendo o corpo obtido pela interseção de todos os subcorpos de F que contém K e M.*

Escrevemos $K(M) = K(a_1, \cdots, a_n)$ se $M = \{a_1, \cdots, a_n\}$ é um conjunto finito.

Definição 1.35 *Se $M = \{\theta\}$, dizemos que $L := K(\theta)$ é uma* ***extensão simples*** *de K, e chamamos θ de* ***elemento extensor*** *de L sobre K.*

Definição 1.36 *Seja F uma extensão de K e $\theta \in F$. Dizemos que θ é* ***algébrico*** *sobre K se $f(\theta) = 0_F$ para algum polinômio não constante $f \in K[x]$. Dizemos que F é uma* ***extensão algébrica*** *de K se todo elemento de F é algébrico sobre K.*

Teorema 1.43 *Toda extensão finita do corpo K é algébrica sobre K.*

Seja F extensão de K e $\theta \in F$ algébrico sobre K. É fácil ver que o conjunto $J = \{f \in K[x] : f(\theta) = 0_F\}$ é um ideal de $K[x]$, logo existe um único polinômio mônico $g \in K[x]$ irredutível sobre K tal que $(g) = J$ pelo Teorema 1.29.

Definição 1.37 *Seja F uma extensão de K e seja $\theta \in F$ algébrico sobre K. Definimos o* ***polinômio minimal*** *de θ sobre K como sendo o polinômio mônico $g \in K[x]$ tal que $(g) = \{f \in K[x] : f(\theta) = 0_F\}$. Definimos o* ***grau*** *de θ sobre K como sendo o grau de g.*

A seguir, uma condição suficiente para a determinação do polinômio minimal.

Teorema 1.44 *Seja F uma extensão de K e seja $\theta \in F$ algébrico sobre K. Se $g \in K[x]$ é um polinômio mônico e irredutível sobre K tal que $g(\theta) = 0_F$, então g é o polinômio minimal de θ sobre K.*

Temos uma caracterização para o polinômio minimal.

Teorema 1.45 *Seja F uma extensão de K e seja $\theta \in F$ algébrico sobre K. Se $g \in K[x]$ é o polinômio minimal de θ sobre K, então vale o seguinte:*

1. *g é irredutível sobre K.*
2. *Dado $f \in K[x]$, temos que $f(\theta) = 0_F$ se, e somente se g divide f.*
3. *g é o polinômio mônico em $K[x]$ de menor grau tal que $g(\theta) = 0_F$.*

Teorema 1.46 *Seja F uma extensão de K e seja $\theta \in F$ algébrico sobre K de grau n sobre K. Se g é o polinômio minimal de θ sobre K, então*

1. *$K(\theta)$ é isomorfo a $F[x]/(g)$.*
2. *$[K(\theta) : K] = n$ e $\{1, \theta, \cdots, \theta^{n-1}\}$ é uma base de $K(\theta)$ como espaço vetorial sobre K.*
3. *Todo $\alpha \in K(\theta)$ é algébrico sobre K e o grau de α sobre K é um divisor de n.*

Em particular, $K(\theta)$ pode ser visto como o conjunto dos polinômios de grau menor que $\deg(g)$ *na indeterminada θ e com coeficientes em K.*

O resultado a seguir é fundamental para a teoria dos corpos.

Teorema 1.47 (Kronecker) *Se $f \in K[x]$ é um polinômio não constante, então existe uma extensão algébrica simples L de K cujo elemento extensor é uma raiz de f.*

Teorema 1.48 *Sejam α e β duas raízes do polinômio irredutível $f \in K[x]$ em alguma extensão de K. Então, $K(\alpha)$ é isomorfo a $K(\beta)$ via uma aplicação que deixa fixos os elementos do K.*

Definição 1.38 *Seja $f \in K[x]$ um polinômio de grau positivo e F uma extensão de K. Dizemos que f de* ***decompõe*** *em F se f pode ser escrito como produto de fatores lineares em $F[x]$, isto é, se existem $a, a_1, \cdots, a_n \in F$ tais que*

$$f(x) = a(x - a_1) \cdots (x - a_n),$$

Dizemos que F é o ***corpo de decomposição*** *de f sobre K se f se decompões em F e $F = K(a_1, \cdots, a_n)$.*

Temos que o corpo de decomposição F de $f \in K[x]$ sobre K é o menor corpo que estende K e contém todas as raízes de f. Como nenhum outro subcorpo próprio de F possui essa propriedade, temos essa caracterização para o corpo de decomposição de um polinômio. Na realidade, a unicidade ocorre a menos de isomorfismo, como descrito precisamente no resultado a seguir.

Teorema 1.49 (Existência e unicidade do corpo de decomposição) *Se K é um corpo e $f \in K[x]$ é um polinômio de grau positivo, então existe o corpo de decomposição de f sobre K. Além disso, quaisquer dois corpos de decomposição de f sobre K são isomorfos via um isomorfismo que deixa fixos os elementos de K e aplica as raízes de f em outras raízes de f.*

Capítulo 2

Corpos finitos

Um **corpo finito** é um corpo cujo número de elementos é finito. Pelo Corolário 1.4, todo corpo finito possui característica prima p e, além disso, admite um subcorpo que é isomorfo a $\mathbb{Z}_p$ pelo Teorema 1.42. Nosso objetivo neste capítulo é investigar mais detalhes relacionados aos corpos finitos. Nossa referência é (LIDL; NIEDERREITER, 1997).

2.1 Estrutura

Nesta seção, mostramos que, a menos de isomorfismo, existe apenas um corpo finito contendo p^n elementos, para cada primo p e cada inteiro positivo n. Obtemos uma descrição da estrutura de subcorpos de um corpo finito. Além disso, mostramos que todo corpo finito é uma extensão algébrica simples de seu subcorpo primo, e que existem polinômios irredutíveis de grau n sobre qualquer corpo finito, para qualquer inteiro positivo n.

Lema 2.1 *Seja F um corpo finito e K um subcorpo de F contendo q elementos. Então F possui q^m elementos, onde m é a dimensão de F como espaço vetorial sobre K.*

***Demonstração**:* Seja F um corpo finito, K um subcorpo de F e suponhamos que m é a dimensão de F como espaço vetorial sobre K. Então existe uma base $\{b_1, \cdots, b_m\}$ de F sobre K e cada elemento de F pode ser escrito de forma única como

$$a_1 b_1 + \cdots a_m b_m \text{ com } a_1, \cdots a_m \in K.$$

Observando que cada a_i admite q valores distintos, pois K contém q elementos, segue do princípio de contagem que F contém exatamente q^m elementos.

Teorema 2.1 *Seja F um corpo finito com q elementos. Então $q = p^n$, onde p é a característica de F e n é o grau de F sobre seu subcorpo primo K.*

Demonstração: Pelo Corolário 1.4, a característica do corpo finito F é um número primo p. Logo, seu subcorpo primo K contém p elementos pois K é isomorfo a $\mathbb{Z}_P$ pelo Teorema 1.42. Se n é o grau de F sobre K, então pelo Lema 2.1 F contém $q = p^n$ elementos.

Seja $q = p^n$ e seja F o corpo de decomposição do polinômio $f(x) = x^q - x \in \mathbb{Z}_p[x]$. Como $f'(x) = -1$, então as q raízes de $f(x)$ são distintas pelo Teorema 1.37. Considere $L = \{a \in F; a^q - a = 0\}$ o conjunto formado pelas raízes do polinômio $f(x)$ e note que

- $0, 1 \in L$ pois $0^q - 0 = 0$ e $1^q - 1 = 0$.
- Se $a, b \in L$, então $(a - b) \in L$ pois $a - b = a^q - b^q = (a - b)^q$.
- Se $a, b \in L$ e $b \neq 0$ então $ab^{-1} \in L$ pois $ab^{-1} = a^q b^{-q} = (ab^{-1})^q$.

Logo, L é subcorpo de F. Por outro lado, como F é o corpo de decomposição de f e L é um corpo que contém todas as raízes de f, então $F = L$ e portanto F é um corpo finito com $q = p^n$ elementos. Além disso, a unicidade do corpo de decomposição implica que qualquer corpo finito com p^n elementos é isomorfo a F.

Mostramos que, para cada primo p e cada inteiro positivo n existe, a menos de isomorfismo, um único corpo finito com p^n elementos. Além disso, o Teorema 2.1 implica que todo corpo finito tem como número de elementos a potência de algum número primo.

Para cada $q = p^n$, com p primo e n inteiro positivo, denotaremos por $\mathbb{F}_q$ o **corpo finito** de característica p que contém q elementos. Por conveniência, no decorrer deste capítulo, usaremos a letra minúscula q apenas para denotar a potência de algum primo p.

O resultado a seguir caracteriza os elementos de $\mathbb{F}_q$.

Lema 2.2 *Seja E uma extensão de $\mathbb{F}_q$ e $\alpha \in E$. Então $\alpha \in \mathbb{F}_q$ se, e somente se $\alpha^q = \alpha$.*

Demonstração: Seja $\alpha \in \mathbb{F}_q$. A identidade $0^q = 0$ é imediata. Suponhamos então que $0 \neq \alpha$. Como os elementos não nulos de $\mathbb{F}_q$ formam um grupo de ordem $q - 1$ com respeito a operação de multiplicação, então $\alpha^{q-1} = 1$ implica $\alpha^q = \alpha$.

Reciprocamente, o polinômio $f(x) = x^q - x$ tem no máximo q raízes em E. Como $\mathbb{F}_q$ é o corpo de decomposição de $f(x)$ e $f'(x) = -1$, então os q elementos de $\mathbb{F}_q$ são raízes de $f(x)$. Se $\alpha \in E$ é tal que $\alpha^q = \alpha$, então α é uma raiz de $f(x)$ e portanto $\alpha \in \mathbb{F}_q$.

Corolário 2.1 *Seja $f(x) \in \mathbb{F}_q[x]$. Então $f(x^{q^n}) = (f(x))^{q^n}$ para todo inteiro positivo n.*

Demonstração: Procedemos por indução sobre n. O caso $n = 0$ é imediato. Para o caso $m = 1$, considere $f(x) = a_k x^k + \cdots + a_1 x + a_0 \in \mathbb{F}_q[x]$. Sendo q uma potência da característica de $\mathbb{F}_q$, segue do Teorema 1.23 e do Lema 2.2 que

$$(f(x))^q = (a_k x^k + \cdots + a_1 x + a_0)^q = a_k^q x^{qk} + \cdots + a_1^q x^q + a_0^q = a_k x^{qk} + \cdots + a_1 x^q + a_0 = f(x^q).$$

Supondo por indução que $f(x^{q^n}) = (f(x))^{q^n}$, temos que

$$(f(x))^{q^{n+1}} = ((f(x))^{q^n})^q = (f(x^{q^n}))^q = f((x^{q^n})^q) = f(x^{q^{n+1}}),$$

onde a segunda igualdade segue da hipótese de indução e a terceira segue do caso $m = 1$.

Descrevemos a seguir a estrutura de subcorpos de um corpo finito.

Teorema 2.2 *Seja $\mathbb{F}_q$ um corpo finito, onde $q = p^n$. Então,*

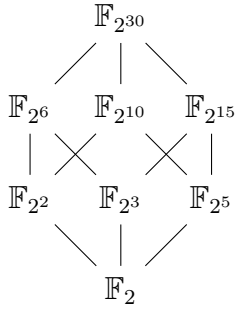
1. *Todo subcorpo de $\mathbb{F}_q$ tem p^m elementos, onde m é um divisor positivo de n.*
2. *Se m é um divisor positivo de n, então existe exatamente um subcorpo de $\mathbb{F}_q$ cujo número de elementos é p^m.*

***Demonstração**:*

1. Seja K um subcorpo de $\mathbb{F}_q$. Observe que F_p é subcorpo de K e $[\mathbb{F}_q : \mathbb{F}_p] = n$. Segue do Teorema 1.40 que $n = [F_q : \mathbb{F}_p] = [F_q : K][K : \mathbb{F}_p]$. De acordo com o Teorema 2.1, K contém p^m para algum $m \leq n$ e, novamente pelo Teorema 2.1, vemos que $\mathbb{F}_q$ contém $(p^m)^k$ elementos, para algum k. Mas como $\mathbb{F}_q$ contém $q = p^n$ elementos, então $p^n = p^{mk}$ e portanto m divide n.

2. Seja m um divisor positivo de n. Segue do Lema 1.1 que $p^m - 1$ divide $p^n - 1$, o que por sua vez implica que $x^{p^m-1} - 1$ divide $x^{p^n-1} - 1$ em $\mathbb{F}_p[x]$. Logo, $x^{p^m} - x$ divide $x^{p^n} - x$ em $\mathbb{F}_p[x]$. Assim, toda raiz de $x^{p^m} - x$ é também raiz de $x^{p^n} - x$. Como o corpo de decomposição L do polinômio $x^{p^m} - x$ tem p^m elementos, e pelo Lema 2.2 toda raiz de $x^{p^m} - x$ está em $\mathbb{F}_q$, então L é um subcorpo de $\mathbb{F}_q$ com p^m elementos. Isso mostra a existência de um subcorpo de $\mathbb{F}_q$ contendo p^m elementos. Para verificarmos a unicidade, suponhamos por absurdo que existam dois subcorpos distintos de $\mathbb{F}_q$ com p^m elementos. Então ambos são corpos de decomposição do polinômio $x^{p^m} - x$ e, como os supomos distintos, a união destes subcorpos conterá mais do que p^m elementos, os quais seriam as raízes do polinômio $x^{p^m} - x$, o que constitui um absurdo e portanto $L = \mathbb{F}_{p^m}$ é o único subcorpo de $\mathbb{F}_q$ com p^m elementos.

Exemplo 2.1 *Vamos analisar os subcorpos do corpo $\mathbb{F}_{2^{30}}$. Tendo em vista o Teorema 2.2, a estrutura de subcorpos fica determinada pelos divisores de* 30*. No diagrama abaixo, indicamos as relações entre os subcorpos de $\mathbb{F}_{2^{30}}$ do seguinte modo: se dois corpos estão ligados por uma linha, o corpo que está acima estende o corpo que está abaixo.*



Denotaremos por $\mathbb{F}_q^*$ o conjunto dos elementos não nulos de $\mathbb{F}_q$. Segue da definição de corpo que $\mathbb{F}_q^*$ é um grupo abeliano com respeito à operação de multiplicação de $\mathbb{F}_q$. Entender a estrutura desse grupo é um passo fundamental para a teoria de corpos finitos.

Teorema 2.3 *Para todo corpo finito $\mathbb{F}_q$, o grupo multiplicativo $\mathbb{F}_q^*$ é cíclico.*

***Demonstração**:* Sejam $\mathbb{F}_q$ um corpo finito e $h = p_1^{r_1} \cdots p_m^{r_m}$ uma decomposição em fatores primos da ordem $h = q - 1$ do grupo multiplicativo $\mathbb{F}_q^*$. Para cada i com $1 \leq i \leq m$, o polinômio $x^{h/p_i} - 1$ tem no máximo $h/p_i < h$ raízes, logo existe um elemento $a_i \in \mathbb{F}_q^*$ que não é raiz deste polinômio. Tomando $b_i := a_i^{h/(p_i^{r_i})}$, temos $(b_i)^{p_i^{r_i}} = a_i^h = 1$. Logo, a ordem de b_i é um divisor de $p_i^{r_i}$ e, como p_i é um número primo, segue que a ordem de b_i é da forma $p_i^{s_i}$ com $0 \leq s_i \leq r_i$. Como $b_i^{p_i^{r_i-1}} = (a_i^{h/(p_i^{r_i})})^{p_i^{r_i-1}} = a_i^{h/p_i} \neq 1$ por construção, vemos que a ordem de b_i é $p_i^{r_i}$. Vejamos que $b := b_1 \cdots b_m$ tem ordem h. De fato, suponhamos que a ordem de b é um divisor próprio de h, ou seja, um divisor de pelo menos um dos m inteiros h/p_i com $1 \leq i \leq m$, digamos de h/p_1. Temos $1 = b_1^{h/p_1} \cdots b_m^{h/p_1}$. Agora, observamos que se $2 \leq i \leq m$, então $p_i^{r_i}$ divide h/p_1, logo $b_i^{h/p_1} = 1$ para $2 \leq i \leq m$. Assim, $1 = b_1^{h/p_1}(b_2^{h/p_1} \cdots b_m^{h/p_1}) = b_1^{h/p_1}$ implica que a ordem $p_1^{r_1}$ de b_1 divide h/p_1, o que é absurdo pois $(p_2^{r_2} \cdots p_m^{r_m})/p1$ seria inteiro. Portanto $\mathbb{F}_q^*$ é grupo cíclico com gerador $b = b_1 \cdots b_m$.

Definição 2.1 *Dizemos que $\alpha \in \mathbb{F}_q$ é um **elemento primitivo** de $\mathbb{F}_q$ se α gera $\mathbb{F}_q^*$.*

Observação 2.1 *Pelo Teorema 1.9, existem $\varphi(q-1)$ elementos primitivos de $\mathbb{F}_q$ em $\mathbb{F}_q^*$.*

A existência de elementos primitivos nos permite obter resultados importantes. Uma consequência imediata do resultado a seguir é que podemos olhar para um corpo finito como sendo extensão algébrica simples do seu subcorpo primo.

Teorema 2.4 *Se $\mathbb{F}_q$ é um corpo finito e $\mathbb{F}_r$ é uma extensão finita de $\mathbb{F}_q$, então $\mathbb{F}_r$ é uma extensão algébrica simples de $\mathbb{F}_q$ e $\mathbb{F}_q(\xi) = \mathbb{F}_r$ para todo elemento primitivo ξ de $\mathbb{F}_r$*

***Demonstração**:* Seja $\mathbb{F}_r$ uma extensão finita de $\mathbb{F}_q$ e seja ξ um elemento primitivo de $\mathbb{F}_r$. Temos que $\mathbb{F}_q \subset \mathbb{F}_r$ implica $\mathbb{F}_q(\xi) \subset \mathbb{F}_r(\xi) = \mathbb{F}_r$. Reciprocamente, $\mathbb{F}_q(\xi)$ contém 0 e todas as potências de ξ, e como ξ gera $\mathbb{F}_r^*$, então $\mathbb{F}_r \subseteq \mathbb{F}_q(\xi)$. Portanto, $\mathbb{F}_q(\xi) = \mathbb{F}_r$.

A seguir, provamos a existência de polinômios irredutíveis de qualquer grau.

Corolário 2.2 *Para todo corpo finito $\mathbb{F}_q$ e para todo inteiro positivo $n \geq 2$, existe um polinômio $f \in \mathbb{F}_q[x]$ irredutível sobre $\mathbb{F}_q$ de grau n.*

***Demonstração**:* Seja $\mathbb{F}_r$ uma extensão de $\mathbb{F}_q$ com q^n elementos. Então $[\mathbb{F}_r : \mathbb{F}_q] = n$ e, pelo Teorema 2.4, temos que $\mathbb{F}_r = \mathbb{F}_q(\xi)$ para algum elemento primitivo $\xi \in \mathbb{F}_r$. Logo $[\mathbb{F}_q(\xi) : \mathbb{F}_q] = n$. Sendo $\mathbb{F}_q(\xi)$ uma extensão algébrica de grau n, então o polinômio minimal de ξ sobre $\mathbb{F}_q$ é irredutível sobre $\mathbb{F}_q$ de grau n pelo Teorema 1.45.

Exemplo 2.2 *Consideremos o polinômio $f(x) = x^3+x+1 \in \mathbb{F}_2[x]$. Como $f(1) = f(0) = 1$, vemos que f é irredutível sobre $\mathbb{F}_2$ pelo Teorema 1.38. Seja α uma raiz de f em alguma extensão de $\mathbb{F}_2$. Segue dos Teoremas 1.46 e 2.1 que $\mathbb{F}_2[x]/(f) = \{ax^2+bx+c : a, c, b \in \mathbb{F}_2\}$ é corpo finito com 8 elementos, logo $\mathbb{F}_2/(f)$ é isomorfo a $\mathbb{F}_8$. Usando a relação $\alpha^3+\alpha+1 = 0$, podemos verificar explicitamente que $\mathbb{F}_8^* = \langle\alpha\rangle$. De fato, deduzimos*

$$\alpha^4 = \alpha(\alpha^3) = \alpha(-\alpha - 1) = -\alpha^2 - \alpha = \alpha^2 + \alpha,$$

e, de modo semelhante, vemos que

$$\begin{aligned}
\alpha^0 &= 1\\
\alpha^1 &= \alpha\\
\alpha^2 &= \alpha^2\\
\alpha^3 &= \alpha^3\\
\alpha^4 &= \alpha + \alpha^2\\
\alpha^5 &= 1 + \alpha + \alpha^2\\
\alpha^6 &= 1 + \alpha^2\\
\alpha^6 &= 1 + \alpha^2\\
\alpha^7 &= 1 = \alpha^0.
\end{aligned}$$

Exemplo 2.3 *Lembramos que b é dito uma **raiz quadrada** de a se $b^2 = a$. Vejamos que todo elemento de um corpo finito de característica 2 admite raiz quadrada neste mesmo corpo. De fato, a aplicação $\psi : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ dada por $\psi(x) = x^2$ é injetiva, pois $\psi(x) = \psi(y)$ implica $(x+y)(x-y) = 0$. Mas $y = -y$ em característica 2, logo $0 = (x-y)(x+y) = (x-y)^2$ implica $x = y$. Sendo $\mathbb{F}_{2^m}$ um conjunto finito, temos que f é sobrejetiva, logo é bijetiva. Isso implica que todo elemento de $\mathbb{F}_{2^m}$ admite raiz quadrada em $\mathbb{F}_{2^m}$.*

Dizemos que um corpo K é **algebricamente fechado** se todo polinômio $f \in K[x]$ admite uma - e portanto toda - raiz em K.

Exemplo 2.4 *$\mathbb{Q}$ não é algebricamente fechado, pois o polinômio $f(x) = x^2 + 1 \in \mathbb{Q}[x]$ é irredutível de grau 2 sobre $\mathbb{Q}$, logo se α é raiz de f, então $\alpha \notin \mathbb{Q}$ pelo Teorema 1.38.*

Corolário 2.3 *Nenhum corpo finito é algebricamente fechado.*

***Demonstração**:* Segue do Corolário 2.2 que sempre existe um polinômio $f \in \mathbb{F}_q[x]$ de grau 2 irredutível sobre $\mathbb{F}_q$. Se α é uma raiz de f em alguma extensão de $\mathbb{F}_q$, então $\alpha \notin \mathbb{F}_q$ pelo Teorema 1.38 e portanto $\mathbb{F}_q$ não é algebricamente fechado.

Encerramos esta seção apresentando uma aplicação que transforma soma de elementos primitivos em produto. Esta aplicação é de grande importância em computação.

Definição 2.2 *Sejam ξ um elemento primitivo de $\mathbb{F}_q$ e n um inteiro tal que $\xi^n \neq -1$. Definimos o **logaritmo de Jacobi**, o qual denotaremos por $L(n)$, como sendo o menor inteiro positivo para o qual é válida a igualdade $1 + \xi^n = \xi^{L(n)}$.*

Teorema 2.5 *Seja ξ um elemento primitivo de $\mathbb{F}_q$. Se m e n são inteiros tais que $\xi^{n-m} \neq 1$, então $\xi^m + \xi^n = \xi^{m+L(n-m)}$.*

***Demonstração**:* O logaritmo de Jacobi está bem definido para $n - m$, pois $\xi^{n-m} \neq -1$ equivale a $0 \neq 1 + \xi^{n-m} = \xi^{L(n-m)}$ e, como ξ é elemento primitivo, então existe o menor inteiro positivo $L(n-m)$ tal que vale essa última igualdade. Dados m e n inteiros, temos

$$\xi^{m+L(n-m)} = \xi^m \xi^{L(n-m)} = \xi^m(1 + \xi^{n-m}) = \xi^m + \xi^m \xi^{n-m} = \xi^m + \xi^n.$$

2.2 Polinômios irredutíveis

Dedicamos esta seção ao estudo de polinômios irredutíveis sobre corpos finitos. Isso nos permitirá deduzir mais informações a relacionadas à estrutura desses corpos.

Lema 2.3 *Seja $f \in \mathbb{F}_q[x]$ um polinômio irredutível sobre $\mathbb{F}_q$ e seja α uma raiz de $f(x)$ em uma extensão de $\mathbb{F}_q$. Se $h \in \mathbb{F}_q[x]$, então $h(\alpha) = 0$ se, e somente se f divide h.*

***Demonstração**:* Seja a o coeficiente líder de f e consideremos $g(x) := a^{-1}f(x)$. Como $f(x)$ é irredutível, então $g(x)$ é mônico e irredutível com $g(\alpha) = 0$, pois α é raiz de $f(x)$. Consequentemente, $g(x)$ é o polinômio minimal de α sobre $\mathbb{F}_q$ pelo Teorema 1.44. Assim, se $h \in \mathbb{F}_q[x]$ é tal que $h(\alpha) = 0$, então g divide h por definição de polinômio minimal. Reciprocamente, se $f(x)$ divide $h(x)$, então existe $s \in \mathbb{F}_q[x]$ tal que $h(x) = f(x)s(x)$. Sendo α uma raiz de $f(x)$, temos $h(\alpha) = f(\alpha)s(\alpha) = 0s(\alpha) = 0$.

Lema 2.4 *Seja $f \in \mathbb{F}_q[x]$ um polinômio irredutível sobre $\mathbb{F}_q$ de grau m. Então $f(x)$ divide $x^{q^n} - x$ se, e somente se m divide n.*

***Demonstração**:* Suponhamos que o polinômio irredutível $f(x)$ divide $x^{q^n} - x$ e seja α uma raiz de f no corpo de decomposição de f sobre $\mathbb{F}_q$. Então $\alpha^{q^n} - \alpha = 0$ implica $\alpha \in \mathbb{F}_{q^n}$ pelo Lema 2.2. Logo, F_q é subcorpo de $\mathbb{F}_q(\alpha)$. Sendo $f(x)$ um polinômio irredutível sobre $\mathbb{F}_q$ de grau m e α uma raiz de f, temos que $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$ pois $\mathbb{F}_q(\alpha)$ tem q^m elementos. Segue do Teorema 1.40 que $n = [\mathbb{F}_{q^n} : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_q(\alpha)][\mathbb{F}_q(\alpha) : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_q(\alpha)]m$, portanto m divide n. Reciprocamente, suponhamos que m divide n. Então $\mathbb{F}_{q^m}$ é subcorpo de $\mathbb{F}_{q^n}$ pelo Teorema 2.2. Se α é uma raiz do polinômio f no corpo de decomposição de f sobre $\mathbb{F}_q$, então $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$ pois f é um polinômio irredutível de grau m. Logo $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$ pelo Teorema 2.2. Em particular, $\alpha \in \mathbb{F}_{q^m} \subseteq \mathbb{F}_{q^n}$. Segue do Lema 2.2 que $\alpha^{q^n} = \alpha$, isto é, α é raiz de $x^{q^n} - x \in \mathbb{F}_q[x]$. Sendo α uma raiz qualquer de f, podemos aplicar o Lema 2.3 e concluir que $f(x)$ divide $x^{q^n} - x$.

O resultado a seguir mostra em particular que, se conhecemos uma raiz de um polinômio irredutível, então podemos determinar todas as demais raízes deste polinômio.

Teorema 2.6 *Seja $f \in \mathbb{F}_q[x]$ um polinômio irredutível sobre $\mathbb{F}_q$ de grau m. Então $f(x)$ tem uma raiz α em $\mathbb{F}_{q^m}$. Além disso, todas as raízes de $f(x)$ são simples e são dadas pelos m elementos distintos $\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{m-1}} \in \mathbb{F}_{q^m}$.*

***Demonstração**:* Seja α uma raiz de f no corpo de decomposição de f sobre $\mathbb{F}_q$. Como f é irredutível de grau m, então $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$ pelo Teorema 1.46. Pelo Lema 2.1, $\mathbb{F}_q(\alpha)$ é um corpo finito que contém exatamente q^m elementos, logo $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$ pela unicidade dos corpos finitos. Isso mostra que $\alpha \in \mathbb{F}_{q^m}$. Agora, seja $\alpha \in \mathbb{F}_{q^m}$ uma raiz de $f(x) \in \mathbb{F}_q[x]$, então $f(\alpha^{q^j}) = f(\alpha)^{q^j} = 0$ para $1 \leq j \leq m$ pelo Corolário 2.1. Portanto, os elementos $\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{m-1}} \in \mathbb{F}_{q^m}$ são raízes de f. Para ver que estes elementos são distintos, suponhamos por absurdo que existam j, k com $0 \leq j < k \leq m-1$ e tais que $\alpha^{q^j} = \alpha^{q^k}$. Elevando essa igualdade a q^{m-k}, temos $\alpha^{q^{m-k+j}} = \alpha^{q^m} = \alpha$, o que implica que α é uma raiz de $x^{q^{m-k+j}} - x \in \mathbb{F}_q[x]$. Dessa forma, f divide $x^{q^{m-k+j}} - x$ pelo Lema 2.3. Mas de acordo com o Lema 2.4 esta divisão ocorre se, e somente se o grau m de f divide $m - k + j$ e, como $0 < m - k + j < m$, pois $j - k < 0$, temos um absurdo. Portanto os α^{q^i} são distintos.

O Teorema 2.6 que é de grande importância teórica. Na linguagem de Teoria de Galois, ele nos diz que toda extensão $\mathbb{F}_{q^m}$ de F_q é uma **extensão galoisiana**, isto é, $\mathbb{F}_{q^m}$ é o corpo de decomposição de um polinômio $f \in \mathbb{F}_q[x]$ **separável** sobre $\mathbb{F}_q$ (isto é, cujas raízes são simples) e **normal** (isto é, sempre que uma raiz de $f \in \mathbb{F}_q[x]$ pertence a $\mathbb{F}_{q^m}$, então todas as demais raízes de f também pertencem a $\mathbb{F}_{q^m}$) (MARTIN, 2010).

As potências de α apresentados no Teorema 2.6 recebem um nome especial, o qual faz parte essencial da terminologia básica da teoria de corpos finitos.

Definição 2.3 *Seja $\alpha \in \mathbb{F}_{q^m}$. Os elementos $\alpha, \alpha^q, \cdots, \alpha^{q^{m-1}}$ são chamados os **conjugados** de α em relação a $\mathbb{F}_q$.*

Observação 2.2 *Segue do Teorema 2.6 que os conjugados de α em relação a $\mathbb{F}_q$ são distintos se, e somente se o polinômio minimal de α sobre $\mathbb{F}_q$ tem grau m. De acordo com o Teorema 1.46, se o polinômio minimal de α sobre $\mathbb{F}_q$ tem grau d, então d é um divisor de m. Neste caso, os conjugados de α são $\alpha, \alpha^q, \cdots, \alpha^{q^{d-1}}$, repetidos m/d vezes.*

Apresentamos agora algumas propriedades relacionadas aos elementos conjugados.

Teorema 2.7 *Os conjugados de $\alpha \in \mathbb{F}_{q^m}$ em relação a qualquer subcorpo de $\mathbb{F}_{q^m}$ tem a mesma ordem no grupo $\mathbb{F}_{q^m}^*$.*

***Demonstração**:* Pelo Teorema 2.3, $\mathbb{F}_{q^m}^*$ é grupo cíclico de ordem $q^m - 1$. Pelo Lema 2.1, q^m é uma potência da característica prima p de $\mathbb{F}_{q^m}$. Logo $\text{mdc}(q^m - 1, q^j) = 1$ para $0 \leq j \leq m-1$. Como os conjugados de α são da forma α^{q^j} para $0 \leq j \leq m-1$, então pelo item 2 do Teorema 1.9, os elementos α^{q^j} geram subgrupos de ordem $|\alpha|/\,\text{mdc}(|\alpha|, q^j)$ no grupo $\langle\alpha\rangle$. Como $|\alpha|$ é um divisor de $q^m - 1$, então $|\alpha|$ não divide q^m. Logo $\text{mdc}(|\alpha|, q^j) = 1$, o que implica que a ordem dos subgrupos gerados pelos α^{q^j} é $|\alpha|$.

Corolário 2.4 *Seja ξ um elemento primitivo de $\mathbb{F}_q$. Então todos os conjugados de ξ em relação a qualquer subcorpo de $\mathbb{F}_q$ também são elementos primitivos.*

***Demonstração**:* Seja ξ um elemento primitivo de $\mathbb{F}_q$. Os conjugados de ξ com relação a algum subcorpo de $\mathbb{F}_q$ são da forma ξ^{p^j}, onde p é a característica de $\mathbb{F}_q$ e $j \geq 0$ são inteiros adequados. Como ξ tem ordem $q-1$ no grupo multiplicativo $\mathbb{F}_q^*$, segue do Teorema 2.7 que todos os conjugados de ξ em relação a este subcorpo tem ordem $q-1$.

Seja F uma extensão do corpo K. Um **automorfismo** de F sobre K é um isomorfismo $\sigma : F \to F$ que fixa os elementos de K, isto é, é tal que que $\sigma(c) = c$ para todo $c \in K$. É de fácil verificação que a composição de automorfismos de F sobre K também é um automorfismo de F sobre K, e consequentemente o conjunto dos automorfismos de F sobre K é um grupo com a operação de composição.

Exemplo 2.5 *Consideremos a aplicação $\sigma : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ dada por $\sigma(\alpha) = \alpha^q$. Pelo Teorema 1.23, vemos que σ é um isomorfismo, e pelo Lema 2.2 vemos que σ deixa fixos os elementos de $\mathbb{F}_q$. Portanto, σ é automorfismo de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$.*

Chamamos a aplicação σ do Exemplo 2.5 de **automorfismo de Frobenius**.

Teorema 2.8 *Os automorfismos de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$ são as aplicações $\sigma_j : \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}$ definidas por $\sigma_j(\alpha) = \alpha^{q^j}$ com $0 \leq j \leq m-1$.*

***Demonstração**:* Para qualquer $j \in \{0, \cdots, m-1\}$ e quaisquer $\alpha, \beta \in \mathbb{F}_{q^m}$ temos $\sigma_j(\alpha\beta) = (\alpha\beta)^{q^j} = (\alpha)^{q^j}(\beta)^{q^j} = \sigma_j(\alpha)\sigma_j(\beta)$ e, pelo Teorema 1.23, temos $\sigma_j(\alpha+\beta) = (\alpha+\beta)^{q^j} = \alpha^{q^j} + \beta^{q^j} = \sigma_j(\alpha) + \sigma_j(\beta)$. Além disso, $\sigma_j(\alpha) = 0$ se, e somente se $\alpha = 0$. Logo, sendo σ_j um homomorfismo injetivo e $\mathbb{F}_{q^m}$ um conjunto finito, temos que σ_j é sobrejetiva e portanto σ_j é um automorfismo de $\mathbb{F}_{q^m}$. Agora, se $c \in \mathbb{F}_q$, então $c^{q^j} = c$ para todo j pelo Teorema 2.2, ou seja, σ_j é um automorfismo de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$.

Para ver que as aplicações $\sigma_0, \sigma_1, \cdots, \sigma_{m-1}$ são distintas, tomemos ξ um elemento primitivo de $\mathbb{F}_{q^m}$. Pelo Teorema 2.6, o polinômio minimal de ξ sobre $\mathbb{F}_q$ é irredutível sobre $\mathbb{F}_q$ de grau m e, pelo Teorema 2.6 suas raízes são dadas pelos m elementos distintos $\xi, \xi^q, \cdots, \xi^{q^{m-1}}$. Portanto, $\sigma_s(\xi) = \xi^{q^s} \neq \xi^{q^t} = \sigma_t(\xi)$ sempre que $0 \leq s < t \leq m-1$.

Vejamos agora que qualquer automorfismo de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$ é da forma σ_j para algum j com $1 \leq j \leq m-1$. Seja ξ um elemento primitivo de $\mathbb{F}_{q^m}$ e seja $f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_1x + a_0 \in \mathbb{F}_q[x]$ o polinômio minimal de ξ sobre $\mathbb{F}_q$. Como $f(\xi) = 0$ e σ é um automorfismo de $\mathbb{F}_{q^m}$ que fixa os elementos de $\mathbb{F}_q$, então

$$\begin{aligned} 0 &= \sigma(f(\xi)) \\ &= \sigma(\xi^m + a_{m-1}\xi^{m-1} + \cdots + a_1\xi + a_0) \\ &= (\sigma(\xi))^m + \sigma(a_{m-1})(\sigma(\xi))^{m-1} + \cdots + \sigma(a_1)\sigma(\xi) + \sigma(a_0) \\ &= (\sigma(\xi))^m + a_{m-1}(\sigma(\xi))^{m-1} + \cdots + a_1\sigma(\xi) + a_0. \end{aligned}$$

Isso mostra que $\sigma(\xi)$ é uma raiz de f em $\mathbb{F}_{q^m}$. Mas pelo Teorema 2.6 as m raízes de f em $\mathbb{F}_{q^m}$ são dadas por $\xi, \xi^q \cdots, \xi^{q^{m-1}}$, logo devemos ter $\sigma(\xi) = \xi^{q^j}$ para algum j com $1 \leq j \leq m-1$. Agora, dado $\alpha \in \mathbb{F}_{q^m}^*$, existe um inteiro positivo r tal que $\alpha = \xi^r$ pois ξ é elemento primitivo de $\mathbb{F}_{q^m}$. Portanto $\sigma(\alpha) = \sigma(\xi^r) = (\xi^r)^q = (\xi^q)^r = (\sigma(\xi))^r = (\xi^{q^j})^r = (\xi^r)^{q^j} = \alpha^{q^j}$.

Acabamos de mostrar que o grupo de automorfismos de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$ é um grupo cíclico cujo gerador é o automorfismo de Frobenius associado a extensão. Esse grupo é conhecido como **grupo de Galois** da extensão de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$.

2.3 Traço e norma

Seja $f(x) \in \mathbb{F}_q[x]$ o polinômio minimal de $\alpha \in \mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$. Suponhamos que o grau de f é d. Então $\mathbb{F}_{q^d}$ é subcorpo de $\mathbb{F}_{q^m}$, e daí d divide m. Assim, o polinômio $g(x) := (f(x))^{m/d} \in \mathbb{F}_q[x]$ está bem definido e tem grau m. Este polinômio é chamado o **polinômio característico** de α sobre $\mathbb{F}_q$. Em vista da Observação 2.2, as raízes de f em $\mathbb{F}_{q^m}$ são $\alpha, \alpha^q, \cdots, \alpha^{q^{d-1}}$, todas com multiplicidade m/d. Temos

$$\begin{aligned} g(x) &= x^m + a_{m-1}x^{m-1} + \cdots + a_1x + a_0 \\ &= ((x-\alpha)(x-\alpha^q)\cdots(x-\alpha^{q^{d-1}}))^{m/d} \\ &= (x-\alpha)(x-\alpha^q)\cdots(x-\alpha^{q^{m-1}}). \end{aligned}$$

Expandindo o segundo membro desta igualdade e comparando os coeficientes, temos

$$\begin{cases} \alpha + \alpha^q + \cdots + \alpha^{q^{m-1}} = -a_{m-1} \in \mathbb{F}_q \\ (-1)^m \alpha^{(q^m-1)/(q-1)} = a_0 \in \mathbb{F}_q \end{cases}. \tag{2.1}$$

Assim, a soma e o produto dos conjugados de $\alpha \in \mathbb{F}_{q^m}$ em relação a $\mathbb{F}_q$ pertencem a $\mathbb{F}_q$.

Definição 2.4 *Consideremos $K = \mathbb{F}_q$ e $F = \mathbb{F}_{q^m}$. O **traço** de $\alpha \in F$ sobre K, o qual denotaremos por $\mathrm{Tr}_{F/K}(\alpha)$, é definido por*

$$\mathrm{Tr}_{F/K}(\alpha) = \sum_{i=0}^{m-1} \alpha^{q^i} = \alpha + \alpha^q + \cdots + \alpha^{q^{m-1}}.$$

Observação 2.3 *Consideremos $K = \mathbb{F}_q, F = \mathbb{F}_{q^m}$ e $E = \mathbb{F}_{q^{mn}}$. Segue imediatamente da equação (2.1) que $\mathrm{Tr}_{F/K}(\alpha) \in K$ para qualquer $\alpha \in F$. Além disso,*

$$\mathrm{Tr}_{F/K}(\alpha) = \sum_{i=0}^{m-1} \alpha^{q^i},\ \mathrm{Tr}_{E/F}(\alpha) = \sum_{j=0}^{n-1} \alpha^{q^{mj}},\ \mathrm{Tr}_{E/K}(\alpha) = \sum_{l=0}^{mn-1} \alpha^{q^l}. \tag{2.2}$$

A seguir apresentamos algumas propriedades da aplicação traço.

Teorema 2.9 *Sejam $K = \mathbb{F}_q$ e $F = \mathbb{F}_{q^m}$. A aplicação*

$$\begin{aligned} \mathrm{Tr}\colon F &\longrightarrow K \\ \alpha &\longmapsto \mathrm{Tr}(\alpha) = \mathrm{Tr}_{F/K}(\alpha) \end{aligned}$$

satisfaz as seguintes propriedades:

1. $\mathrm{Tr}(\alpha + c\beta) = \mathrm{Tr}(\alpha) + c\,\mathrm{Tr}(\beta)$ *para quaisquer $\alpha, \beta \in F$ e para qualquer $c \in K$.*
2. $\mathrm{Tr} : F \to K$ *é uma aplicação linear sobrejetiva.*
3. $\mathrm{Tr}(c) = mc$ *para qualquer $c \in K$.*
4. $\mathrm{Tr}(\alpha^q) = \mathrm{Tr}(\alpha)$, *para qualquer $\alpha \in F$.*

***Demonstração**:*

1. Para quaisquer $\alpha, \beta \in F$ e qualquer $c \in K$, temos

$$\begin{aligned} \mathrm{Tr}(\alpha + c\beta) &= \mathrm{Tr}_{F/K}(\alpha + c\beta) \\ &= (\alpha + c\beta) + (\alpha + c\beta)^q + \cdots + (\alpha + c\beta)^{q^{m-1}} \\ &= \alpha + c\beta + \alpha^q + (c\beta)^q + \cdots + \alpha^{q^{m-1}} + (c\beta)^{q^{m-1}} \\ &= \alpha + c\beta + \alpha^q + c^q\beta^q + \cdots + \alpha^{q^{m-1}} + c^{q^{m-1}}\beta^{q^{m-1}} \end{aligned}$$

$$\begin{aligned}
&= \alpha + c\beta + \alpha^q + c\beta^q + \cdots + \alpha^{q^{m-1}} + c\beta^{q^{m-1}} \\
&= \alpha + \alpha^q + \cdots + \alpha^{q^{m-1}} + c\beta + c\beta^q + \cdots + c\beta^{q^{m-1}} \\
&= (\alpha + \alpha^q + \cdots + \alpha^{q^{m-1}}) + c(\beta + \beta^q + \cdots + \beta^{q^{m-1}}) \\
&= \mathrm{Tr}_{F/K}(\alpha) + c\,\mathrm{Tr}_{F/K}(\beta) \\
&= \mathrm{Tr}(\alpha) + c\,\mathrm{Tr}(\beta),
\end{aligned}$$

onde a terceira igualdade segue do Teorema 1.23, e quinta segue do Lema 2.2.

2. Pelo item 1, $\mathrm{Tr} : F \longrightarrow K$ é uma aplicação linear. Vejamos que essa aplicação é sobrejetiva. Temos que $\mathrm{Tr}(\alpha) = 0$ se, e somente se α é uma raiz do polinômio $p(x) = x + x^q + \cdots + x^{q^{m-1}} \in K[x]$ em F. Como $p(x)$ tem no máximo q^{m-1} raízes, então existe $\alpha' \in F$ tal que $\mathrm{Tr}(\alpha') \neq 0$. Logo, a imagem de Tr tem dimensão pelo menos 1 como espaço vetorial sobre K. Portanto $\mathrm{Im}(\mathrm{Tr}) = K$.

3. Para qualquer $c \in K$, temos que $c^{q^j} = c$ para $1 \leq j \leq m-1$. Logo,

$$\mathrm{Tr}(c) = c + c^q + \cdots + c^{q^{m-1}} = c + c + \cdots + c = mc.$$

4. Para qualquer $\alpha \in F$, temos que $a^{q^m} = \alpha$. Logo,

$$\begin{aligned}
\mathrm{Tr}(\alpha^q) &= \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{m-1}} + \alpha^{q^m} \\
&= \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{m-1}} + \alpha \\
&= \alpha + \alpha^q + \cdots + \alpha^{q^{m-1}} \\
&= \mathrm{Tr}(\alpha)
\end{aligned}$$

Classificaremos agora todas as transformações lineares $T : F \to K$, onde K é um corpo finito e F é uma extensão finita de K. Em particular, mostraremos que o número de transformação lineares de F em K é igual ao número de elementos de F.

Teorema 2.10 *Seja F uma extensão finita do corpo finito K. Então as transformações lineares de F em K são caracterizadas pelas aplicações L_β, com $\beta \in F$, definidas por*

$$\begin{aligned}
L_\beta \colon F &\longrightarrow K \\
\alpha &\longmapsto L_\beta(\alpha) = \mathrm{Tr}_{F/K}(\beta\alpha)
\end{aligned}$$

Além disso, temos $L_\beta \neq L_\gamma$ sempre que β e γ forem elementos distintos em F.

***Demonstração**:* Dado $\beta \in F$, seja a aplicação $L_\beta : F \to K$ dada por $L_\beta(\alpha) = \mathrm{Tr}_{F/K}(\beta\alpha)$. Para quaisquer $\alpha, \lambda \in F$ e qualquer $c \in K$, segue do item 1 do Teorema 2.9 que

$$L_\beta(\alpha + c\lambda) = \mathrm{Tr}_{F/K}(\beta(\alpha + c\lambda)) = \mathrm{Tr}_{F/K}(\beta\alpha) + c\,\mathrm{Tr}_{F/K}(\beta\lambda) = L_\beta(\alpha) + cL_\beta(\lambda).$$

Logo, L_β é aplicação linear. Sejam agora $\beta, \gamma \in F$ com $\beta \neq \gamma$. Para qualquer $\alpha \in F$, temos

$$\begin{aligned} L_\beta(\alpha) - L_\gamma(\alpha) &= \mathrm{Tr}_{F/K}(\beta\alpha) - \mathrm{Tr}_{F/K}(\gamma\alpha) \\ &= \mathrm{Tr}_{F/K}(\beta\alpha - \gamma\alpha) \\ &= \mathrm{Tr}_{F/K}((\beta - \gamma)\alpha) \\ &\neq 0 \text{ para algum } \alpha \in F \text{ adequado,} \end{aligned}$$

onde a segunda igualdade segue da linearidade do traço e a quarta igualdade segue da sobrejetividade do traço. Portanto, $L_\beta \neq L_\gamma$ sempre que $\beta \neq \gamma$. Isso mostra que, se $F = \mathbb{F}_{q^m}$ e $K = \mathbb{F}_q$ temos q^m transformações lineares distintas da forma L_β.

Por outro lado, seja $T : \mathbb{F}_{q^m} \to \mathbb{F}_q$ uma transformação linear qualquer. Fixe uma base $B = \{\gamma_1, \cdots, \gamma_m\} \subseteq F$ de F sobre K. Como sabemos, T fica complemente determinada quando aplicamos T nos elementos da base B. Para cada i com $1 \leq i \leq m$, temos que $T(\gamma_i)$ pode assumir q valores distintos. Logo, por combinatória, existem q^m transformações lineares de $\mathbb{F}_{q^m}$ em $\mathbb{F}_q$. Mas já mostramos que existem q^m aplicações distintas da forma L_β com $\beta \in F$. Portanto, devemos ter $T = L_\beta$ para algum $\beta \in \mathbb{F}_q$.

Exemplo 2.6 *Analisemos as transformações de $K = \mathbb{F}_q$ em $F = \mathbb{F}_{q^m}$, ambos vistos como espaço vetorial sobre K. Pelo Teorema de Núcleo e da Imagem, temos duas possibilidades:*

1. $\dim_K \ker(T) = 1$ *e* $\dim_K \mathrm{Im}(T) = 0$*, o que implica que T é identicamente nula.*
2. $\dim_K \ker(T) = 0$ *e* $\dim_K \mathrm{Im}(T) = \dim_K K = 1$*, logo K e $T(K)$ são isomorfos.*

O resultado a seguir caracteriza os elementos cujo traço é nulo.

Teorema 2.11 *Sejam $K = \mathbb{F}_q$, $F = \mathbb{F}_{q^m}$ e seja $\alpha \in F$. Então $\mathrm{Tr}_{F/K}(\alpha) = 0$ se, e somente se $\alpha = \beta^q - \beta$ para algum $\beta \in F$.*

***Demonstração**:* Suponhamos que $\mathrm{Tr}_{F/K}(\alpha) = 0$ com $\alpha \in F$. Considere β uma raiz do polinômio $x^q - x - \alpha \in F[x]$ em alguma extensão de F. Então $\beta^q - \beta - \alpha = 0$, o que implica $\alpha = \beta^q - \beta$. Temos

$$\begin{aligned} 0 &= \mathrm{Tr}_{F/K}(\alpha) \\ &= \alpha + \alpha^q + \cdots + \alpha^{q^{m-2}} + \alpha^{q^{m-1}} \\ &= (\beta^q - \beta) + (\beta^q - \beta)^q + \cdots + (\beta^q - \beta)^{q^{m-2}} + (\beta^q - \beta)^{q^{m-1}} \\ &= (\beta^q - \beta) + (\beta^{q^2} - \beta^q) + \cdots + (\beta^{q^{m-1}} - \beta^{q^{m-2}}) + (\beta^{q^m} - \beta^{q^{m-1}}) \\ &= \beta^{q^m} - \beta, \end{aligned}$$

o que implica $\beta^{q^m} = \beta$ e portanto $\beta \in F$ pelo Lema 2.2.

Reciprocamente, se $\alpha = \beta^q - \beta$ para algum $\beta \in F$, então $\alpha \in F$. Logo,

$$\mathrm{Tr}_{F/K}(\alpha) = \mathrm{Tr}_{F/K}(\beta^q - \beta) = \mathrm{Tr}_{F/K}(\beta^q) - \mathrm{Tr}_{F/K}(\beta) = \mathrm{Tr}_{F/K}(\beta) - \mathrm{Tr}_{F/K}(\beta) = 0,$$

onde a terceira igualdade segue do item 4 do Teorema 2.9. Portanto $\mathrm{Tr}_{F/K}(\alpha) = 0$.

A seguir, verificamos que a aplicação traço é transitiva em relação a composição.

Teorema 2.12 *Seja K um corpo finito, F uma extensão finita de K e E uma extensão finita de F. Então*

$$\mathrm{Tr}_{F/K}(\mathrm{Tr}_{E/F}(\alpha)) = \mathrm{Tr}_{E/K}(\alpha) \text{ para todo } \alpha \in E.$$

***Demonstração**:* Consideremos $K = \mathbb{F}_q, F = \mathbb{F}_{q^m}$ e $E = \mathbb{F}_{q^{mn}}$. Seja $\alpha \in E$. Segue da definição de traço e da equação (2.1) que $\mathrm{Tr}_{E/F}(\alpha) \in F$. Pela equação (2.2), temos

$$\begin{aligned}
\mathrm{Tr}_{F/K}(\mathrm{Tr}_{E/F}(\alpha)) &= \sum_{i=0}^{m-1} (\mathrm{Tr}_{E/F}(\alpha))^{q^i} \\
&= \sum_{i=0}^{m-1} (\alpha + \alpha^{q^m} + \cdots + \alpha^{q^{m(n-1)}})^{q^i} \\
&= \sum_{i=0}^{m-1} (\alpha^{q^i} + \alpha^{q^{m+i}} + \cdots + \alpha^{q^{m(n-1)+i}}).
\end{aligned}$$

Observe que no somatório

$$\sum_{i=0}^{m-1} (\alpha^{q^i} + \alpha^{q^{m+i}} + \cdots + \alpha^{q^{m(n-1)+i}}),$$

cada i com $0 \leq i \leq mn-1$ aparece uma e apenas uma vez como potência de q. De fato, para α^{q^i} as potências de q variam de 0 a $m-1$; para $\alpha^{q^{m+i}}$ as potências de q variam de m a $2m-1$ e assim sucessivamente, até que para $\alpha^{q^{m(n-1)+i}}$ as potências de q variam de $m(n-1)+m-2 = mn-2$ a $m(n-1)+m-1 = mn-1$. Portanto,

$$\mathrm{Tr}_{F/K}(\mathrm{Tr}_{E/F}(\alpha)) = \sum_{i=0}^{m-1} (\alpha^{q^i} + \alpha^{q^{m+i}} + \cdots + \alpha^{q^{m(n-1)+i}}) = \sum_{k=0}^{mn-1} \alpha^{q^k} = \mathrm{Tr}_{E/K}(\alpha).$$

A seguir introduzimos outra aplicação que é de grande interesse para a teoria.

Definição 2.5 *Consideremos $K = \mathbb{F}_q$ e $\alpha \in F = \mathbb{F}_{q^m}$. A **norma** de α sobre K, a qual denotaremos por $\mathrm{N}_{F/K}(\alpha)$, é definida por*

$$\mathrm{N}_{F/K}(\alpha) = \alpha \cdot \alpha^q \cdots \alpha^{q^{m-1}} = \alpha^{(q^m-1)/(q-1)}.$$

A segunda igualdade apresentada na definição 2.5 segue da identidade $(q^m - 1) = (q-1)(q^{m-1} + \cdots + q + 1)$. Pela equação (2.1), temos $\mathrm{N}_{F/K}(\alpha) \in K$ para todo $\alpha \in F$.

Apresentamos agora algumas propriedades da aplicação norma.

Teorema 2.13 *Sejam $K = \mathbb{F}_q$ e $F = \mathbb{F}_{q^m}$. A aplicação*

$$\begin{aligned} \mathrm{N}\colon F &\longrightarrow K \\ \alpha &\longmapsto \mathrm{N}(\alpha) = \mathrm{N}_{F/K}(\alpha) \end{aligned}$$

satisfaz as seguintes propriedades:

1. $\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)N(\beta)$ *para todo* $\alpha, \beta \in F$.
2. N *e* $\bar{N} := \mathrm{N}\,|_{F^*} : F^* \mapsto K^*$ *são aplicações sobrejetivas.*
3. $\mathrm{N}(c) = c^m$ *para todo* $c \in K$.
4. $\mathrm{N}(\alpha^q) = \mathrm{N}(\alpha)$ *para todo* $\alpha \in F$.

***Demonstração**:*

1. Para quaisquer $\alpha, \beta \in F$, temos

$$\begin{aligned} \mathrm{N}(\alpha\beta) &= \mathrm{N}_{F/K}(\alpha\beta) \\ &= (\alpha\beta)^{(q^m-1)/(q-1)} \\ &= (\alpha^{(q^m-1)/(q-1)})(\beta^{(q^m-1)/(q-1)}) \\ &= \mathrm{N}_{F/K}(\alpha)\,\mathrm{N}_{F/K}(\beta) \\ &= \mathrm{N}(\alpha)\,\mathrm{N}(\beta). \end{aligned}$$

2. Segue da definição de norma que $\mathrm{N}(\alpha) = \mathrm{N}_{F/K}(\alpha) = 0$ se, e somente se $\alpha = 0$. Assim, pelo item 1 vemos que $\bar{N} : F^* \to K^*$ é um homomorfismo de grupos. Como

$$\begin{aligned} \ker \bar{N} &= \{\alpha \in F^* : \bar{N}(\alpha) = 1\} \\ &= \{\alpha \in F^* : \alpha^{(q^m-1)/(q-1)} = 1\} \\ &= \{\alpha \in F^* : \alpha^{(q^m-1)/(q-1)} - 1 = 0\}, \end{aligned}$$

   então $\alpha \in \ker \bar{N}$ se, e somente se α é uma raiz do polinômio $x^{(q^m-1)/(q-1)} - 1 \in K[x]$ em F. Mas este polinômio tem no máximo $(q^m - 1)/(q - 1)$ raízes, o que implica

$$|\ker \bar{N}| \leq \frac{(q^m - 1)}{(q - 1)}.$$

   Pelo Teorema de Isomorfismo para grupos, $F^*/\ker \bar{N}$ é isomorfo a $\operatorname{Im} \bar{N}$. Logo,

$$\begin{aligned} |\operatorname{Im} \bar{N}| &= \frac{|F^*|}{|\ker \bar{N}|} \\ &= \frac{(q^m - 1)}{|\ker \bar{N}|} \\ &\geq q - 1. \end{aligned}$$

Como $\operatorname{Im}\bar{N} \subseteq K^*$ e $|K^*| = q-1$, então $\operatorname{Im}\bar{N}$ não pode conter mais do que $q-1$ elementos. Isso implica que $\operatorname{Im}\bar{N} = K^*$ e assim $\bar{N}$ é sobrejetiva. Além disso, sendo $\mathrm{N}(0) = 0$, vemos que N também é sobrejetiva.

3. Para qualquer $c \in K$, temos $c^{q^j} = c$ se $1 \leq j \leq m-1$. Logo, $\mathrm{N}(c) = cc^q \cdots c^{q^{m-1}} = c^m$.

4. Para qualquer $\alpha \in F$, temos $\alpha^{q^m} = \alpha$. Logo,

$$\begin{aligned}\mathrm{N}(\alpha^q) &= \alpha^q \alpha^{q^2} \cdots \alpha^{q^{m-1}} \alpha^{q^m} \\ &= \alpha^q \alpha^{q^2} \cdots \alpha^{q^{m-1}} \alpha \\ &= \alpha \alpha^q \cdots \alpha^{q^{m-1}} \\ &= \mathrm{N}(\alpha).\end{aligned}$$

Assim como o traço, a norma é transitiva em relação a composição.

Teorema 2.14 *Seja K um corpo finito, F uma extensão finita de K e E uma extensão finita de F. Então*

$$N_{E/K}(\alpha) = N_{F/K}(N_{E/F}(\alpha)) \text{ para todo } \alpha \in E.$$

***Demonstração**:* Consideremos $K = \mathbb{F}_q, F = \mathbb{F}_{q^m}$ e $E = \mathbb{F}_{q^{mn}}$. Seja $\alpha \in E$. Pela equação (2.1), $\mathrm{N}_{E/F}(\alpha) \in F$. Portanto,

$$\begin{aligned}N_{F/K}(N_{E/F}(\alpha)) &= N_{F/K}(\alpha^{(q^{mn}-1)/(q^m-1)}) \\ &= (\alpha^{(q^{mn}-1)/(q^m-1)})^{(q^m-1)/(q-1)} \\ &= \alpha^{(q^{mn}-1)/(q-1)} \\ &= N_{E/K}(\alpha).\end{aligned}$$

É possível caracterizar os elementos cuja norma é igual a 1 :

Teorema 2.15 *Sejam $K = \mathbb{F}_q$, $F = \mathbb{F}_{q^m}$ e $\alpha \in F$. Então $\mathrm{N}_{F/K} = 1$ se, e somente se $\alpha = \beta^{q-1}$ para algum $\beta \in K$.*

O resultado a seguir nos diz que podemos olhar o traço e a norma como sendo, respectivamente, o traço e o determinante da matriz associada a uma transformação linear.

Teorema 2.16 *Sejam $K = \mathbb{F}_q$, $F = \mathbb{F}_{q^m}$ e $\beta \in F$ fixo. Considerando F como espaço vetorial sobre K, defina o operador linear $L : F \to F$ dado por $L(\alpha) = \beta\alpha$. Então o polinômio característico g de β sobre K coincide com o polinômio característico da aplicação L, isto é, $g(x) = \det(Ix - L)$, onde I denota a aplicação identidade e L denota a matriz associada a aplicação L. Além disso, $\mathrm{Tr}_{F/K}(\beta)$ é igual ao traço da matriz associada a L e $\mathrm{N}_{F/K}(\beta)$ é igual ao determinante da matriz associada a L.*

2.4 Bases

Nesta seção, investigamos questões relacionadas com álgebra linear para deduzir propriedades do corpo finito F visto como espaço vetorial sobre um subcorpo K.

Iniciamos fixando uma base $\{\alpha_1, \cdots, \alpha_m\} \subseteq F$ de F sobre K. Como sabemos, cada elemento $\gamma \in F$ pode ser escrito de forma única como

$$\gamma = c_1(\gamma)\alpha_1 + \cdots + c_m(\gamma)\alpha_m \text{ com } c_j(\gamma) \in K, \text{ para } 1 \leq j \leq m.$$

É fácil verificar que, para cada j com $1 \leq j \leq m$, a aplicação

$$\begin{aligned} \pi_j \colon F &\longrightarrow K \\ \gamma &\longmapsto \pi_j(\gamma) = c_j(\gamma) \end{aligned}$$

é uma transformação linear. Observemos que cada $c_j(\gamma)$ é o elemento de K que multiplica α_j na representação de γ como combinação linear dos elementos da base. Dessa forma, cada $c_j(\gamma)$ está unicamente determinado. Pelo Teorema 2.10, para cada j com $1 \leq j \leq m$, existe e é único o elemento $\beta_j \in F$ tal que

$$\pi_j(\alpha) = \mathrm{Tr}_{F/K}(\beta_j\alpha) \text{ para todo } \alpha \in F.$$

Além disso, como $\alpha_i = 0\alpha_1 + \cdots 1\alpha_i + \cdots + 0\alpha_m$, então para cada $1 \leq j \leq m$ temos

$$\mathrm{Tr}_{F/K}(\beta_j\alpha_i) = \begin{cases} 0, & \text{se } i \neq j \\ 1, & \text{se } i = j \end{cases}. \tag{2.3}$$

Vejamos agora que o conjunto $\{\beta_1, \cdots, \beta_m\}$ assim obtido é L.I. e portanto é uma base de F sobre K. Suponhamos que

$$d_1\beta_1 + \cdots + d_m\beta_m = 0 \text{ com } d_i \in K \text{ para } 1 \leq i \leq m.$$

Fixando i e multiplicando ambos os lados desta igualdade por α_i temos

$$d_1\beta_1\alpha_i + \cdots + d_i\beta_i\alpha_i + \cdots + \alpha_i d_m\beta_m = 0$$

Segue das relações 2.3 e da linearidade do traço que

$$\begin{aligned} 0 &= \mathrm{Tr}_{F/K}(0) \\ &= \mathrm{Tr}_{F/K}(d_1\beta_1\alpha_i + \cdots + d_i\beta_i\alpha_i + \cdots + \alpha_i d_m\beta_m) \\ &= d_1 \mathrm{Tr}_{F/K}(\beta_1\alpha_i) + \cdots d_i \mathrm{Tr}_{F/K}(\beta_i\alpha_i) + \cdots + d_m \mathrm{Tr}_{F/K}(\beta_m\alpha_i) \\ &= d_1 0 + \cdots + d_i 1 + \cdots + d_m 0 \\ &= d_i. \end{aligned}$$

Como i é arbitrário, concluímos que o conjunto $\{\beta_1, \cdots, \beta_m\}$ é um base de F sobre K.

Definição 2.6 *Seja F uma extensão finita do corpo finito K. Duas bases $\{\alpha_1, \cdots, \alpha_m\}$ e $\{\beta_1, \cdots, \beta_m\}$ de F sobre K são ditas* ***bases duais****, ou* ***complementares****, se para cada i, j com $1 \leq i, j \leq m$, vale*

$$\mathrm{Tr}_{F/K}(\beta_j \alpha_i) = \begin{cases} 0, & \text{se } i \neq j \\ 1, & \text{se } i = j \end{cases}.$$

A discussão anterior à definição 2.6 garante a existência e a unicidade da base dual:

Teorema 2.17 *Seja F uma extensão finita do corpo finito K. Dada uma base $\{\alpha_1, \cdots, \alpha_m\}$ de F sobre K, sua base dual $\{\beta_1, \cdots, \beta_m\}$ existe e é unicamente determinada.*

Dizemos que uma base é **autodual** se ela coincide com sua base dual.

No exemplo a seguir, verificamos que uma base é autodual e encontramos os coeficientes de um elemento para sua representação em termos dessa base. Além disso, ilustramos como as operações ocorrem em um corpo finito diferente dos $\mathbb{Z}_p$'s.

Exemplo 2.7 *Consideremos o polinômio*

$$f(x) = x^3 + x^2 + 1 \in \mathbb{F}_2[x].$$

Como $f(0) = f(1) = 1$, então $f(x)$ é irredutível sobre $\mathbb{F}_2$ pelo Teorema 1.38. Dada uma raiz α de f, temos que $\alpha \in \mathbb{F}_{2^3} = \mathbb{F}_8$ pelo Teorema 2.6. Vejamos que

$$B = \{\alpha, \alpha^2, 1 + \alpha + \alpha^2\}$$

é uma base de $\mathbb{F}_8$ sobre $\mathbb{F}_2$. Como $[\mathbb{F}_8 : \mathbb{F}_2] = 3$, é suficiente mostrarmos que B é um conjunto L.I. Pelo item 2 do Teorema 1.46, temos que $C = \{1, \alpha, \alpha^2\}$ é uma base de $\mathbb{F}_8$ sobre $\mathbb{F}_2$. Sejam $c_1, c_2, c_3 \in \mathbb{F}_2$ tais que

$$c_1\alpha + c_2\alpha^2 + c_3(1 + \alpha + \alpha^2) = 0.$$

Temos

$$c_3 1 + (c_1 + c_3)\alpha + (c_2 + c_3)\alpha^2 = 0.$$

Sendo C um conjunto L.I., temos que $c_3 = c_1 + c_3 = c_2 + c_3 = 0$ e assim $c_1 = c_2 = c_3 = 0$.

Checamos agora que B é uma base autodual. Pelo Teorema 2.17, é suficiente verificarmos as relações dadas na definição 2.6. Vamos verificar algumas, pois a verificação das demais é inteiramente análoga. Sendo α uma raiz de f, temos

$$\alpha^3 + \alpha^2 + 1 = 0 \implies \alpha^3 = -\alpha^2 - 1.$$

Com esta igualdade, podemos calcular potências de α*. Temos*

$$\begin{aligned}\alpha^4 &= \alpha\alpha^3\\ &= \alpha(-\alpha^2-1)\\ &= -\alpha^3-\alpha\\ &= 1+\alpha+\alpha^2,\end{aligned}$$

e

$$\begin{aligned}\alpha^6 &= (\alpha^3)^2\\ &= (-\alpha^2-1)^2\\ &= \alpha^4+2\alpha^2+1\\ &= (1+\alpha+\alpha^2)+1\\ &= \alpha+\alpha^2.\end{aligned}$$

Denotando $F=\mathbb{F}_8$ *e* $K=\mathbb{F}_2$*, devemos mostrar que, para quaisquer* $r,s\in B$ *vale* $\mathrm{Tr}_{F/K}(rs)=1$ *se* $r=s$ *e* $\mathrm{Tr}_{F/K}(rs)=0$ *se* $r\neq s$*. Temos*

$$\begin{aligned}\mathrm{Tr}_{F/K}(\alpha\alpha) &= \mathrm{Tr}_{F/K}(\alpha^2)\\ &= \alpha^2+\alpha^4+\alpha^8\\ &= \alpha^2+(1+\alpha+\alpha^2)+(1+\alpha+\alpha^2)^2\\ &= \alpha^2+(1+\alpha+\alpha^2)+(1^2+\alpha^2+\alpha^4)\\ &= \alpha^2+(1+\alpha+\alpha^2)+\alpha\\ &= 1.\end{aligned}$$

Por outro lado,

$$\begin{aligned}\mathrm{Tr}_{F/K}(\alpha\alpha^2) &= \mathrm{Tr}_{F/K}(\alpha^3)\\ &= \mathrm{Tr}_{F/K}(-1-\alpha^2)\\ &= \mathrm{Tr}_{F/K}(1)-\mathrm{Tr}_{F/K}(\alpha^2)\\ &= 0.\end{aligned}$$

De modo semelhante, podemos verificar que $\mathrm{Tr}_{F/K}(\alpha(\alpha+\alpha^2))=0$ *e assim sucessivamente. Concluímos que* B *é base autodual.*

Como B *uma base, então podemos escrever* $\alpha^5\in F$ *de forma única como*

$$\alpha^5=c_1\alpha+c_2\alpha^2+c_3(1+\alpha+\alpha^2),\ \textit{com}\ c_1,c_2,c_3\in K.$$

Para calcular os coeficientes c_1,c_2,c_3 *sabendo que* B *é uma base autodual, basta observar as relações dadas em 2.6. Ao multiplicar os dois lados da igualdade acima por* α *e tomarmos*

o traço, obtemos

$$\begin{aligned} c_1 &= c_1 \operatorname{Tr}_{F/K}(\alpha\alpha) \\ &= \operatorname{Tr}_{F/K}(c_1\alpha\alpha) \\ &= \operatorname{Tr}_{F/K}(\alpha\alpha^5) \\ &= \operatorname{Tr}_{F/K}((\alpha^3)^2) \\ &= \operatorname{Tr}_{F/K}(\alpha^3) \\ &= 0. \end{aligned}$$

De forma semelhante, obtemos $c_2 = 1$ *e* $c_3 = 1$*. Portanto,*

$$\alpha^5 = \alpha^2 + (1 + \alpha + \alpha^2).$$

A seguir, uma classificação das extensões que admitem base autodual.

Teorema 2.18 (Seroussi e Lempel) $\mathbb{F}_{q^m}$ *admite uma base autodual sobre* $\mathbb{F}_q$ *se, e somente se ou* q *é par, ou* q *e* m *são ímpar.*

O artigo (SEROUSSI; LEMPEL, 1980) contém uma prova do Teorema 2.18. Esse artigo também mostra que todo corpo finito $F = \mathbb{F}_{q^m}$ admite uma base **traço-ortogonal** sobre $K = \mathbb{F}_q$, isto é, uma base $\{\beta_1, \beta_2, \cdots, \beta_m\}$ com $\operatorname{Tr}_{F/K}(\beta_i\beta_j) = 0$ se $i \neq j$.

A seguir, vamos considerar que duas bases são iguais se, e somente se têm os mesmos elementos listados na mesma ordem. Com essa condição, é possível exibir o número bases de um corpo finito como espaço vetorial sobre um seu subcorpo:

Teorema 2.19 *Se a ordem dos elementos de uma base é levada em consideração, então o número de bases distintas de* $\mathbb{F}_{q^m}$ *sobre* $\mathbb{F}_q$ *é*

$$\prod_{k=0}^{m-1} (q^m - q^k) = (q^m - 1)(q^m - q) \cdots (q^m - q^{m-1}).$$

Como o número de bases cresce muito rápido com p e n, é de grande interesse teórico e prático a escolha de uma base com propriedades especiais que facilitem as operações, permitam implementação de algoritmos ou mesmo economizem processamento computacional, por exemplo. Dentre as várias possibilidades para uma base de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$, destacamos duas com propriedades interessantes. A primeira é a chamada **base polinomial** $\{1, \alpha, \cdots, \alpha^{m-1}\}$, a qual de acordo com o Teorema 1.46 pode ser obtida das potências de um elemento $\alpha \in \mathbb{F}_{q^m}$ raiz de um polinômio irredutível sobre $\mathbb{F}_q$ de grau m - ou ainda, de um elemento primitivo de $\mathbb{F}_{q^m}$. Vimos no Exemplo 2.7 a conveniência de se trabalhar com uma base autodual com auxílio da base polinomial. O segundo tipo de base que podemos considerar é a seguinte:

Definição 2.7 *Sejam $K = \mathbb{F}_q$ e $F = \mathbb{F}_{q^m}$. A base $\{\alpha, \alpha^q, \cdots, \alpha^{q^{m-1}}\}$ de F sobre K constituída de conjugados de $\alpha \in F$ sobre K é chamada de* ***base normal*** *de F sobre K.*

A base apresentada no Exemplo 2.7 é uma base normal.

A seguir, resultados necessários para provarmos a existência das bases normais.

Lema 2.5 (Artin) *Seja F um corpo, $\psi_1, \cdots, \psi_m$ homomorfismos distintos do grupo G no grupo multiplicativo F^* e $a_1, \cdots, a_m$ elementos de F não todos nulos. Então*

$$a_1\psi_1(g) + \cdots + a_m\psi_m(g) \neq 0 \text{ para algum } g \in G.$$

***Demonstração**:* Procedemos por indução sobre m. O caso $m = 1$ é imediato pois $0 \neq a_1 \in F$ e $0 \neq \psi(g) \in \mathrm{Im}\,(\psi) \subseteq F^*$ implicam $a_1\psi(g) \neq 0,$ para todo $g \in G$.

Assuma que $m > 1$ e que o resultado está provado para quaisquer $m-1$ homomorfismos distintos de G em F^*. Sejam $\psi_1, \cdots, \psi_m$ homomorfismos distintos de G em F^*, e sejam $a_1, \cdots, a_m$ elementos de F, não todos nulos. Podemos assumir $a_1 \neq 0$, pois se $a_1 = 0$, então o Lema está provado por hipótese de indução. Suponhamos por absurdo que

$$a_1\psi_1(g) + \cdots + a_m\psi_m(g) = 0 \text{ para todo } g \in G. \tag{2.4}$$

Como $\psi_1 \neq \psi_m$ por hipótese, então existe $h \in G$ com $\psi_1(h) \neq \psi_m(h)$. Substituindo g por gh na igualdade (2.4), obtemos

$$\begin{aligned} 0 &= a_1\psi_1(gh) + \cdots + a_m\psi_m(gh) \\ &= a_1\psi_1(g)\psi_1(h) + \cdots + a_m\psi_m(g)\psi_m(h), \text{ para todo } g \in G, \end{aligned}$$

e multiplicando ambos os lados da igualdade acima por $\psi_m^{-1}(h)$, temos

$$b_1\psi_1(g) + \cdots + b_{m-1}\psi_{m-1}(g) + a_m\psi_m(g) = 0 \text{ para todo } g \in G, \tag{2.5}$$

onde $b_i = a_i\psi_i(h)\psi_m^{-1}(h)$ para $1 \leq i \leq m-1$. Subtraindo a equação (2.4) de (2.5), obtemos

$$c_1\psi_1(g) + \cdots + c_{m-1}\psi_{m-1}(g) = 0 \text{ para todo } g \in G, \tag{2.6}$$

onde $c_i = a_i - b_i$ para $1 \leq i \leq m-1$. Em particular, $c_1 = a_1 - b_1 = a_1 - a_1\psi_1(h)\psi_m^{-1}(h) \neq 0$, pois $\psi_1(h)\psi_m^{-1}(h) = 1$ se, e somente se $\psi_1(h) = \psi_m(h)$. Assim, a igualdade (2.6) contraria a hipótese de indução que diz que as ψ_i são distintas. Portanto, a equação (2.4) é absurda.

Recordamos alguns fatos da álgebra linear de que precisaremos a seguir. Seja F um espaço vetorial sobre K de dimensão n. Dizemos que um polinômio $f \in K[x]$ **aniquila** a transformação linear $T : F \to F$ se $f(T) = 0$. O **polinômio minimal** para T é o polinômio mônico de menor grau que aniquila T. O **polinômio característico** para T é dado por $\det(Ix - T)$, onde I é a aplicação identidade. Um vetor $u \in F$ é dito um **vetor T-cíclico** se $\{u, Tu, \cdots T^{n-1}u\}$ gera F como espaço vetorial sobre K (COELHO, 2020).

Lema 2.6 *Seja T um operador linear no espaço vetorial V de dimensão finita. Então T possui um vetor cíclico se, e somente se seu polinômio minimal e característico coincidem.*

Agora, podemos garantir a existência da base normal.

Teorema 2.20 (Base normal) *Seja F uma extensão finita do corpo finito K. Existe uma base normal de F sobre K.*

***Demonstração**:* Sejam $K = \mathbb{F}_q$ e $F = \mathbb{F}_{q^m}$. Pelo Teorema 2.21, os distintos automorfismos de F sobre K são$I, \sigma, \sigma^2, \cdots, \sigma^{m-1}$, onde I é a aplicação identidade, $\sigma(\alpha) := \alpha^q$ para todo $\alpha \in F$ e a potência σ^j indica a composição de σ consigo mesma j vezes. Para quaisquer $\alpha, \beta \in F$ e qualquer $c \in K$, temos $\sigma(\alpha + c\beta) = (\alpha + c\beta)^q = \alpha^q + c\beta^q = \sigma(\alpha) + c\sigma(\beta)$. Logo, σ é um operador linear que age no espaço vetorial F. Como $\sigma^m = I$, então o polinômio $x^m - 1 \in K[x]$ aniquila σ.

Como $\sigma : F^* \to F^*$ homomorficamente, pois $\sigma(\alpha\beta) = (\alpha\beta)^q = \alpha^q\beta^q = \sigma(\alpha)\sigma(\beta)$ para quaisquer $\alpha, \beta \in F^*$, então aplicando o Lema de Artin para os homomorfismos distintos $I, \sigma, \cdots, \sigma^{m-1}$ e m elementos de F^* não todos nulos, vemos que nenhum polinômio não nulo de grau menor do que m aniquila σ. Assim, $x^m - 1$ é o polinômio minimal de σ.

Pelo Teorema de Cayley-Hamilton, o polinômio característico para σ é o polinômio mônico de grau m que é divisível pelo polinômio minimal para σ. Isso implica que os polinômios minimal e característico para σ coincidem. Portanto, segue do Lema 2.6 que existe $\alpha \in F$ tal que $\alpha, \sigma(\alpha) = \alpha^q, \sigma^2(\alpha) = \alpha^{q^2}, \cdots, \sigma^{m-1} = \alpha^{q^{m-1}}$ geram F sobre K.

A definição apresentada a seguir nos auxilia na caracterização de algumas bases.

Definição 2.8 *Seja F uma extensão de grau m do corpo finito K.O **discriminante** dos elementos $\alpha_1, \cdots, \alpha_m \in F$, o qual denotaremos por $\Delta_{F/K}(\alpha_1, \cdots, \alpha_m)$, é definido por*

$$\Delta_{F/K}(\alpha_1, \cdots, \alpha_m) = \begin{vmatrix} \mathrm{Tr}_{F/K}(\alpha_1\alpha_1) & \mathrm{Tr}_{F/K}(\alpha_1\alpha_2) & \dots & \mathrm{Tr}_{F/K}(\alpha_1\alpha_m) \\ \mathrm{Tr}_{F/K}(\alpha_2\alpha_1) & \mathrm{Tr}_{F/K}(\alpha_2\alpha_2) & \dots & \mathrm{Tr}_{F/K}(\alpha_2\alpha_m) \\ \vdots & \vdots & \ddots & \vdots \\ \mathrm{Tr}_{F/K}(\alpha_m\alpha_1) & \mathrm{Tr}_{F/K}(\alpha_m\alpha_2) & \dots & \mathrm{Tr}_{F/K}(\alpha_m\alpha_m) \end{vmatrix}$$

Como cada entrada desse determinante pertence a K, então $\Delta_{F/K}(\alpha_1, \cdots, \alpha_m) \in K$.

Teorema 2.21 *Sejam K um corpo finito, F uma extensão de K de grau m e sejam $\alpha_1, \cdots, \alpha_m \in F$. Então $\{\alpha_1, \cdots, \alpha_m\}$ é uma base de F sobre K se, e somente se*

$$\Delta_{F/K}(\alpha_1, \cdots, \alpha_m) \neq 0.$$

***Demonstração**:* Seja $\{\alpha_1, \cdots, \alpha_m\}$ base de F sobre K. Para que $\Delta_{F/K}(\alpha_1, \cdots, \alpha_m) \neq 0$ é suficiente que os vetores-linha que aparecem na definição 2.8, sejam L.I. Suponhamos que, para $1 \leq j \leq m$,

$$c_1 \operatorname{Tr}_{F/K}(\alpha_j\alpha_1) + \cdots + c_m \operatorname{Tr}_{F/K}(\alpha_j\alpha_m) = 0 \text{ com } c_1, \cdots, c_m \in K.$$

Então, pondo $\beta = c_1\alpha_1 + \cdots + c_m\alpha_m$, temos pela igualdade acima que $\operatorname{Tr}_{F/K}(\beta\alpha_j) = 0$ para $1 \leq j \leq m$ e portanto $\operatorname{Tr}_{F/K}(\beta\alpha) = 0$ para todo $\alpha \in F$, o que só é possível se $\beta = 0$. Assim, $0 = \beta = c_1\alpha_1 + \cdots + c_m\alpha_m$ implica $c_1 = \cdots = c_m = 0$ pois $\{\alpha_1, \cdots, \alpha_m\}$ é base.

Reciprocamente, se $\Delta_{F/K}(\alpha_1, \cdots, \alpha_m) \neq 0$, vejamos que o conjunto $\{\alpha_1, \cdots, \alpha_m\}$ é L.I., e consequentemente uma base de F sobre K. De fato, se $c_1\alpha_1 + \cdots + c_m\alpha_m = 0$ com $c_1, \cdots, c_m \in K$, então $c_1\alpha_1\alpha_j + \cdots + c_m\alpha_m\alpha_j = 0\alpha_j = 0$, para $1 \leq j \leq m$, logo

$$c_1 \operatorname{Tr}_{F/K}(\alpha_j\alpha_1) + \cdots + c_m \operatorname{Tr}_{F/K}(\alpha_j\alpha_m) = \operatorname{Tr}_{F/K}(0) = 0.$$

Mas isso é uma combinação linear dos elementos da j-ésima linha do discriminante, o qual, por hipótese, é não nulo. Portanto, $c_1 = \cdots = c_m = 0$ e daí $\{\alpha_1, \cdots, \alpha_m\}$ é L.I.

Corolário 2.5 *Seja $\alpha_1, \cdots, \alpha_m \in \mathbb{F}_{q^m}$. Então $\{\alpha_1, \cdots, \alpha_m\}$ é uma base de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$ se, e somente se*

$$\begin{vmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_m \\ \alpha_1^q & \alpha_2^q & \dots & \alpha_m^q \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{q^{m-1}} & \alpha_2^{q^{m-1}} & \dots & \alpha_m^{q^{m-1}} \end{vmatrix} \neq 0.$$

***Demonstração**:* Sejam $K = \mathbb{F}_q$ e $F = \mathbb{F}_{q^m}$ e considere a matriz A e sua transposta A^T

$$A = \begin{bmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_m \\ \alpha_1^q & \alpha_2^q & \dots & \alpha_m^q \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{q^{m-1}} & \alpha_2^{q^{m-1}} & \dots & \alpha_m^{q^{m-1}} \end{bmatrix} \quad A^T = \begin{bmatrix} \alpha_1 & \alpha_1^q & \dots & \alpha_1^{q^{m-1}} \\ \alpha_2 & \alpha_2^q & \dots & \alpha_2^{q^{m-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_m & \alpha_m^q & \dots & \alpha_2^{q^{m-1}} \end{bmatrix}.$$

Comparando a definição de discriminante com o produto de A^T com A, vemos que

$$A^TA = \begin{bmatrix} \operatorname{Tr}_{F/K}(\alpha_1\alpha_1) & \operatorname{Tr}_{F/K}(\alpha_1\alpha_2) & \dots & \operatorname{Tr}_{F/K}(\alpha_1\alpha_m) \\ \operatorname{Tr}_{F/K}(\alpha_2\alpha_1) & \operatorname{Tr}_{F/K}(\alpha_2\alpha_2) & \dots & \operatorname{Tr}_{F/K}(\alpha_2\alpha_m) \\ \vdots & \vdots & \ddots & \vdots \\ \operatorname{Tr}_{F/K}(\alpha_m\alpha_1) & \operatorname{Tr}_{F/K}(\alpha_m\alpha_2) & \dots & \operatorname{Tr}_{F/K}(\alpha_m\alpha_m) \end{bmatrix}.$$

Assim, $\Delta_{F/K}(\alpha_1, \cdots, \alpha_m) = \det(A^TA) = \det(A^T)\det(A) = \det(A)^2$. Como $(\det(A))^2 = 0$ se, e somente se $\det(A) = 0$, temos que $\Delta_{F/K}(\alpha_1, \cdots, \alpha_m) \neq 0$ se, e somente se, $\det(A) \neq 0$. Portanto, $\det(A) \neq 0$ é equivalente a $\{\alpha_1, \cdots, \alpha_m\}$ ser base pelo Teorema 2.21.

Corolário 2.6 *A base dual de uma base normal é uma base normal.*

Demonstração: Seja $L = \{\alpha, \alpha^q, \cdots, \alpha^{q^{m-1}}\}$ uma base normal de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$ e seja $L' = \{\beta_1, \beta_2, \cdots, \beta_m\}$ sua base dual. Considere as matrizes

$$A = \begin{bmatrix} \alpha & \alpha^q & \dots & \alpha^{q^m} \\ \alpha^q & \alpha^{q^2} & \dots & \alpha \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{q^{m-1}} & \alpha & \dots & \alpha^{q^{m-2}} \end{bmatrix} \quad B = \begin{bmatrix} \beta_1 & \beta_2 & \dots & \beta_m \\ \beta_1^q & \beta_2^q & \dots & \beta_m^q \\ \vdots & \vdots & \ddots & \vdots \\ \beta_1^{q^{m-1}} & \beta_2^{q^{m-1}} & \dots & \beta_m^{q^{m-1}} \end{bmatrix}.$$

Como a entrada da linha i e coluna j da matriz AB é dada por $\mathrm{Tr}_{F/K}(\alpha^{q^{i-1}}\beta_j)$, então $BA = I$ pois L' é base dual de L. Observe que $(AB)^T = B^T A^T = B^T A = I$ pois A é simétrica. Assim, $BA = I = B^T A$ implica $B = B^T$. Comparando a primeira linha com a primeira coluna de B, vemos que $\beta_i = \beta_1^{q^{m-j}}$ para $i \leq j \leq m$. Portanto, L' é base normal.

Enunciamos um importante resultado relacionado a bases normais e primitivas.

Teorema 2.22 (Base normal primitiva) *Toda extensão finita de corpos finitos admite uma base normal constituída de elementos primitivos.*

2.5 Ciclotomia

Nesta seção, investigamos em detalhes o corpo de decomposição do polinômio $x^m - 1$. Alguns resultados também se aplicam para corpos de característica zero.

Definição 2.9 *Seja n um inteiro positivo e K um corpo. Chamamos de n-**ésimo corpo ciclotômico** sobre K, e denotamos por K^n, ao corpo de decomposição do polinômio $x^n - 1$ sobre K. Chamamos de n-**ésima raiz de unidade** sobre K as raízes de $x^n - 1$.*

Denotaremos por E^n o conjunto de todas as n-ésimas raízes da unidade.

A estrutura de E^n é determinada pela relação entre n e a característica do corpo:

Teorema 2.23 *Seja n um inteiro positivo e K um corpo de característica p. Então,*

1. *Se p não divide n, então E^n é grupo cíclico de ordem n com respeito a operação de multiplicação definida em K.*
2. *Se p divide n, seja $n = mp^e$ onde p não divide m. Então $K^n = K^m$, $E^n = E^m$, e as raízes de $x^n - 1$ em K^n são os m elementos de E^m, cada uma com multiplicidade p^e.*

***Demonstração**:*

1. Se $n = 1$, então $E^n = \{1_F\}$ e o resultado segue. Suponhamos que $n \geq 2$ e que n não é divisível por p. Pelo Teorema 1.37, o polinômio $x^n - 1$ não admite raízes múltiplas Assim, E^n tem n elementos. Note que $E^n \neq \emptyset$ pois $1 \in E^n$. Agora, se $a, b \in E^n$, então $a^n = 1$ e $b^n = 1$, logo $b^{-n} = 1$ e daí $(ab^{-1})^n = a^n b^{-n} = 1$, ou seja, $ab^{-1} \in E^n$. Para verificarmos que E^n é grupo cíclico de ordem finita n, considerando a decomposição em fatores primos $n = p_1^{a_1} \cdots p_k^{a_k}$, e procedemos com o mesmo argumento usado na demonstração do Teorema 2.3.

2. Suponha que p divide n. Podemos escrever $n = mp^e$ onde p não divide m. Segue do item 1 que E^m é grupo cíclico de ordem m. Sendo p a característica de K, temos que $x^n - 1 = x^{mp^e} - 1 = (x^m - 1)^{p^e}$, portanto as raízes de $x^n - 1$ são as m raízes de $x^m - 1$, cada uma com multiplicidade p^e.

Exemplo 2.8 *A notação usual para o grupo multiplicativo das raízes da unidade sobre* $\mathbb{R}$ *é* U_n*, isto é,* $U_n = \{\xi \in \mathbb{C} : \xi^n = 1\}$*. É um resultado conhecido que os elementos do conjunto* U_n *estão dispostos no plano complexo de tal modo que determinam um polígono regular de n lados cujos vértices estão inscritos no círculo de raio 1 centrado na origem.*

Definição 2.10 *Seja* K *um corpo e* n *um inteiro positivo que não é divisível pela característica de* K*. Dizemos que* $\xi \in E^n$ *é uma* n***-ésima raiz primitiva da unidade*** *sobre* K *se* ξ *é um gerador do grupo cíclico* E^n*.*

Segue da Observação 2.1 que o número de n-ésimas raízes primitivas da unidade sobre K é $\varphi(n)$. Além disso, se ξ é um gerador de E^n, então todas as n-ésimas raízes primitivas da unidade são dadas pelos ξ^s tais que $\text{mdc}(s, n) = 1$.

Definição 2.11 *Seja* K *um corpo de característica* p*,* n *um inteiro positivo não divisível por* p *e* ξ *uma* n*-ésima raiz primitiva da unidade. Definimos o* n***-ésimo polinômio ciclotômico*** *sobre* K*, o qual denotaremos por* Φ_n*, como sendo o produto*

$$\Phi_n(x) = \prod_{\substack{s=1 \\ \text{mdc}(s,n)=1}}^{n} (x - \xi^s).$$

O grau de $\Phi_n(x)$ é $\varphi(n)$, e esse produto independe da escolha da raiz primitiva.

Teorema 2.24 *Seja K um corpo de característica p e n um inteiro positivo não divisível por p. Então,*

1. $x^n - 1 = \prod_{d|n} \Phi_d(x)$.
2. *Os coeficiente de $\Phi_n(x)$ pertencem a $\mathbb{F}_p$ se $p > 0$, e pertencem a $\mathbb{Z}$ se $p = 0$.*

***Demonstração**:*

1. Seja $\alpha \in E^n$ uma raiz da unidade de ordem d. Como E^n é grupo cíclico, então d divide n e $x^d = 1$, mas $x^r \neq 1$ para $0 < r < d$. Logo, α é uma d-ésima raiz primitiva da unidade. Agrupando as d-ésimas raízes primitivas para cada divisor d de n, temos

$$x^n - 1 = \prod_{i=1}^{n}(x - \alpha^i) = \prod_{d|n}\left(\prod_{\substack{s=1 \\ \text{mdc}(s,n)=1}}^{d}(x - \xi^s)\right) = \prod_{d|n}\Phi_n(x).$$

2. Seja $F = \mathbb{F}_p$ se $p > 0$, ou $F = \mathbb{Z}$ se $p = 0$. Em qualquer dos casos, $F[x]$ é um anel com a propriedade de que se $f(x), g(x) \in F[x]$ e $g(x) \neq 0$, então $f(x)g(x) \in F[x]$ e, pelo Algoritmo da Divisão, $f(x)/g(x) \in F[x]$. Procedemos por indução sobre n. Para $n = 1$, o polinômio $\Phi_1(x) = x - 1$ tem coeficientes em F. Suponhamos que o resultado está provado para todo $d < n$, isto é, assuma que $\Phi_d(x)$ tem coeficientes em F para todo $d < n$. Logo, $\prod_{d|n} \Phi_d(x)$, com $d < n$, tem coeficientes em F. Segue do item 1 que $\Phi_n(x) = (x^n - 1)/r(x)$, onde $r(x) = \prod_{d|n} \Phi_d$ com $d < n$. Como $x^n - 1$ e $r(x)$ tem coeficientes em F, concluímos que $\Phi_n(x)$ tem coeficientes em F.

Comparando os graus de $x^n - 1 = \prod_{d|n} \Phi_d(x)$ obtemos a igualdade $n = \sum_{d|n} \varphi(d)$.

Exemplo 2.9 *Consideremos r primo e n um inteiro positivo. Vejamos que*

$$\Phi_{r^n}(x) = 1 + x^{r^{n-1}} + x^{2r^{n-1}} + \cdots + x^{(r-1)r^{n-1}}.$$

De fato, sendo r um primo, temos que os únicos divisores de r^n são r^i com $1 \leq i \leq n$. Pelo item 1 do Teorema 2.24,

$$x^{r^n} - 1 = \prod_{d|r^n} \Phi_d(x) = \left(\prod_{i=1}^{n-1} \Phi_{r^i}(x)\right) \Phi_{r^n}(x) = (x^{r^{n-1}} - 1)\Phi_{r^n}(x).$$

Por outro lado,

$$x^{r^n} - 1 = ((x^{r^{n-1}})^r - 1)(1 + x^{r^{n-1}} + x^{2r^{n-1}} + \cdots + x^{(r-1)r^{n-1}}).$$

Comparando estas igualdades, temos $\Phi_{r^n}(x) = 1 + x^{r^{n-1}} + x^{2r^{n-1}} + \cdots + x^{(r-1)r^{n-1}}$.

Exemplo 2.10 *Podemos calcular qualquer polinômio $\Phi_n(x)$ sobre o corpos dos racionais aplicando recursivamente o item 1 do Teorema 2.24. Neste processo, precisamos calcular Φ_d para cada divisor d de n. Como exemplo, vamos calcular $\Phi_8(x)$.*

- $\Phi_1(x) = x - 1$.
- *De* $x^2 - 1 = \Phi_1(x)\Phi_2(x)$, *temos* $\Phi_2(x) = (x^2 - 1)/\Phi_1(x) = (x^2 - 1)/(x - 1) = x + 1$. *Logo* $\Phi_2(x) = x + 1$.
- *De* $x^4 - 1 = \Phi_1(x)\Phi_2(x)\Phi_4(x) = (x-1)(x+1)\Phi_4(x)$, *temos* $\Phi_4(x) = (x^4-1)/(x^2-1) = x^2 + 1$. *Logo,* $\Phi_4(x) = x^2 + 1$.
- *De* $x^8 - 1 = \Phi_1(x)\Phi_2(x)\Phi_4(x)\Phi_8(x) = (x - 1)(x + 1)(x^2 + 1)\Phi_8(x) = (x^4 - 1)\Phi_8(x)$, *temos* $\Phi_8(x) = (x^8 - 1)/(x^4 - 1) = (x^4 - 1)(x^4 + 1)/(x^4 - 1)x^4 + 1$. *Portanto*

$$\Phi_8(x) = x^4 - 1.$$

Dado n um inteiro positivo, consideremos o conjunto $U(\mathbb{Z}_n)$ formado pelos elementos de $\mathbb{Z}_n$ que admitem inverso multiplicativo. Pelo Teorema de Bézout, $a \in U(\mathbb{Z}_n)$ se, e somente se $\text{mdc}(a, n) = 1$, logo $U(\mathbb{Z}_n)$ é grupo com respeito à multiplicação induzida de $\mathbb{Z}_n$.

Dado um inteiro b relativamente primo com n, definimos a **ordem multiplicativa** de b módulo n, a qual denotamos por $\text{ord}_n(b)$, como sendo a ordem de b no grupo $U(\mathbb{Z}_n)$. Em outras palavras, se $\text{mdc}(b, n) = 1$, então $\text{ord}_n(b) = \min_{k>0}\{b^k \equiv 1 \pmod{n}\}$.

Teorema 2.25 *Para todo inteiro positivo n,*

1. *K^n é extensão algébrica simples de K.*
2. *Se $K = \mathbb{Q}$, então $\Phi_n(x)$ é irredutível sobre $\mathbb{Z}$ e $[K^n : K] = \phi(n)$.*
3. *Se $K = \mathbb{F}_q$ e $\text{mdc}(q, n) = 1$, então $\Phi_n(x)$ é fatorado em $K[x]$ como produto de $\varphi(n)/d$ polinômios mônicos irredutíveis sobre K de mesmo grau $d = \text{ord}_n(q)$. Além disso, K^n é o corpo de decomposição de qualquer um destes fatores irredutíveis sobre K e $[K^n : K] = d$.*

***Demonstração**:*

1. Se existe uma $\xi \in K$ n-ésima raiz primitiva da unidade sobre K, então $K^n = K(\xi)$. De fato, $K(\xi)$ contém todas as potências de ξ, que é n-ésima raiz primitiva da unidade, logo $K(\xi)$ contém todos as demais raízes de $x^n - 1$ e daí $K^n \subseteq K \subseteq K(\xi)$. A inclusão $K(\xi) \subseteq K^n$ é imediata pois $\xi \in K^n$. Se, porém, não existe uma raiz n-ésima primitiva da unidade em K, procedemos como no item 2 do Teorema 2.23 e obtemos $K^n = K^m = K(\xi)$ e o resultado segue.

2. Essa demonstração pode ser encontrada em (GALLIAN, 2017), Teorema 33.3.

3. Seja ξ uma n-ésima raiz primitiva da unidade sobre $\mathbb{F}_q$. Pelo Lema 2.2, temos $\xi \in \mathbb{F}_{q^k}$ se, e somente se $\xi^{q^k} = \xi$. Vejamos que essa última igualdade é válida se, e somente se $q^k \equiv 1 \pmod{n}$. De fato, se $\xi^{q^k} = \xi$ então $\xi^{q^k-1} = 1 = \xi^n$ pois ξ também é raiz da unidade, logo $q^k = 1 + n$. Reciprocamente, se vale $q^k \equiv 1 \pmod{n}$, então $q^k = 1 + jn$ com $j \in \mathbb{Z}$, logo $1 = \xi^{q^k} = \xi^{1+jn} = (\xi^n)^j\xi = \xi$. Isso implica que ξ é raiz de $x^{q^k} - x \in \mathbb{F}_q[x]$, logo $\xi \in \mathbb{F}_{q^k}$ para algum k. Devemos tomar o menor inteiro positivo k com esta propriedade, o qual existe já que $\text{mdc}(q, n) = 1$, pois ξ deve pertence ao menor corpo que contém $\mathbb{F}_q$ e todas as raízes de $x^n - 1$. Seja então d o menor k dentre esses k's. Temos $d = \text{ord}_n(q)$ por definição de ordem. Dessa forma, $\xi \in \mathbb{F}_{q^d}$ e ξ não pertence a nenhum subcorpo próprio de $\mathbb{F}_{q^d}$. Agora, o polinômio minimal de ξ tem grau d, e como ξ é uma raiz arbitrária do polinômio $\Phi_n(x)$ de grau $\varphi(n)$, então todos os polinômios irredutíveis na decomposição de $\Phi_n(x)$ tem o mesmo grau d e o número de tais polinômios é $\varphi(n)/d$. Além disso, $\mathbb{F}_{q^d}$ é o corpo de decomposição de qualquer um deles pelo Teorema 2.6.

Exemplo 2.11 *Seja $K = \mathbb{F}_{11}$. De modo análogo ao Exemplo 2.10, podemos deduzir $\Phi_{12}(x) = x^4 - x^2 + 1 \in \mathbb{F}_{11}[x]$. Para aplicar o Teorema 2.25, primeiro verificamos que o grau do polinômio é relativamente primo com a ordem de K:* $\text{mdc}(4, 11) = 1$. *Em seguida, verificamos que $d = 2$ é o menor inteiro positivo tal que* $11^2 \equiv 1 \pmod{4}$. *Portanto, $\Phi_{12}(x)$ se fatora em $\mathbb{F}_{11}[x]$ como produto de $\varphi(4)/2 = 2$ polinômios mônicos de mesmo grau 2. Explicitamente, $\Phi_{12}(x) = (x^2 + 5x + 1)(x^2 - 5x + 1)$. Além disso, o corpo de decomposição de qualquer destes polinômios irredutíveis é $\mathbb{F}_{121}$.*

Podemos olhar para corpos finitos como sendo corpos ciclotômicos.

Teorema 2.26 *$\mathbb{F}_q$ é o $(q-1)$-ésimo corpo ciclotômico sobre qualquer um de seus subcorpos.*

***Demonstração**:* O polinômio $x^{q-1} - 1 \in \mathbb{F}_q$ se decompõe em $\mathbb{F}_q$ pois suas raízes são os elementos não nulos de $\mathbb{F}_q$. Esse polinômio não pode se decompor em nenhum subcorpo próprio K de $\mathbb{F}_q$ pois neste caso o corpo de decomposição de $x^{q-1} - 1$ conteria menos do que suas $q - 1$ raízes. Portanto, $\mathbb{F}_q$ é corpo de decomposição de $x^{m-1} - 1$ sobre K.

Teorema 2.27 *Se d é um divisor próprio de n, então $\Phi_n(x)$ divide $(x^n - 1)/(x^d - 1)$ sempre que $\Phi_n(x)$ está definido.*

***Demonstração**:* Segue do Teorema 2.24 que $x^n - 1 = \prod_{d|n} \Phi_d(x)$. Logo, $\Phi_n(x)$, que está definido por hipótese, divide $x^n - 1$. Note que $x^n - 1 = (x^d - 1)[(x^n - 1)/(x^d - 1)]$. Como d é um divisor próprio de n, então $\Phi_n(x)$ é co-primo com $x^d - 1$ pois toda raiz de $\Phi_n(x)$

tem ordem n e as raízes de $x^d - 1$ tem ordem $1 \leq d < n$. Isso implica que $\Phi_n(x)$ não divide $x^d - 1$, logo $\Phi_n(x)$ deve ser um divisor de $(x^n - 1)/(x^d - 1)$ pelo Teorema 1.32.

Exemplo 2.12 *A soma das n-ésimas raízes da unidade sobre K é igual a zero se $K \neq \mathbb{F}_2$. De fato, seja ξ n-ésima raiz da unidade sobre K. Como $x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1)$ e n é o menor inteiro positivo tal que $\xi^n = 1$, então $0 = \xi^n - 1 = (\xi - 1)(\xi^{n-1} + \xi^{n-2} + \cdots + 1)$. Como $(\xi - 1) \neq 0$, então devemos ter $(\xi^{n-1} + \cdots + \xi + 1) = 0$. Concluímos ao observarmos $1 = \xi^n$, e que esse argumento não vale para $K = \mathbb{F}_2$ já que neste caso a única raiz da unidade é $\xi = 1$.*

Teorema 2.28 *Considerando o corpo dos racionais, para quaisquer $q, n \geq 2$, temos*

$$|\Phi_n(q)| > q - 1.$$

***Demonstração**:* O número complexo $\Phi_n(q)$ é o produto de $\varphi(n)$ números da forma $q - \xi^s$ com ξ raiz primitiva, $|\xi^s| = 1$ e $\xi^s \neq 1$. Logo, $|q - \xi^s| > |q| - |\xi|^s = q - 1 > 1$. Daí,

$$\begin{aligned}
|\Phi_n(q)| &= |\prod_{\substack{s=1 \\ \text{mdc}(s,n)=1}}^{n} (x - \xi^s)| \\
&= \prod_{\substack{s=1 \\ \text{mdc}(s,n)=1}}^{n} |x - \xi^s| \\
&> \prod_{\substack{s=1 \\ \text{mdc}(s,n)=1}}^{n} (q - 1) \\
&= (q-1)^{\varphi(n)} \\
&> q - 1.
\end{aligned}$$

A seguir, uma fórmula explícita para o polinômio ciclotômico sobre corpos finitos:

Teorema 2.29 *Se F é um corpo finito de característica p e n não é divisível por p, então*

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)} = \prod_{d|n} (x^{n/d} - 1)^{\mu(d)},$$

*onde $\mu : \mathbb{N} \to \{-1, 0, 1\}$ é a **função de Möebius** definida por*

$$\mu(n) = \begin{cases} 1 & , \text{ se } n = 1 \\ (-1)^k & , \text{ se } n \text{ é o produto de } k \text{ primos distintos} \\ 0 & , \text{ se } n \text{ é divisível pelo quadrado de um primo} \end{cases}.$$

Uma prova dessa fórmula pode ser encontrada em (LIDL; NIEDERREITER, 1997), Teorema 3.27. Com um pouco mais de teoria dos números e o Teorema 2.25, é possível classificar os polinômios ciclotômicos irredutíveis:

Teorema 2.30 *$\Phi_n(x)$ é irredutível sobre $\mathbb{F}_q$ se, e somente $n = r^k$, $n = 2r^k$, ou $n = 4$, onde r é um primo ímpar e $k \geq 0$, e q é um gerador do grupo multiplicativo $\mathbb{Z}_n^*$.*

2.6 Teorema de Wedderburn

Nesta seção, revisitamos a teoria de anéis para provar que todo anel de divisão finito é um corpo finito - esse resultado é conhecido como Teorema de Wedderburn.

O **centro do anel** A, o qual denotaremos por $Z(A)$, é o conjunto dos elementos de A que comutam com todos os elementos de A com respeito a multiplicação de A.

Teorema 2.31 *O centro de um anel de divisão finito é um corpo finito.*

***Demonstração**:* Seja A um anel de divisão. Temos $Z(A) \neq \emptyset$ pois $1_A, 0_A \in A$ são tais que $1a = a1 = a$ e $0_A a = a0_A = 0_A$ para qualquer $a \in A$, logo $1_A, 0_A \in Z(A)$. Além disso,

- Para quaisquer $r, s \in Z(A)$ temos que $ra = ar$ e $sa = as$ para todo $a \in A$. Assim, $(r-s)a = ra + sa = ar + as = a(r+s)$, o que implica $(r-s) \in Z(A)$.
- Para quaisquer $r, s \in Z(A) \setminus \{0_A\}$, temos que $ra = ar$ e $s^{-1}a = as^{-1}$ para todo $a \in A$, logo $rs^{-1}a = ras^{-1} = ars^{-1}$, o que implica $rs^{-1} \in Z(A)$.

Isso mostra que $Z(A)$ é subgrupo com respeito a soma, e $A \setminus \{0_A\}$ é subgrupo com respeito ao produto. Além disso, como A é anel divisão, então vale a comutatividade do produto e a distributividade em $Z(A)$. Portanto, $Z(A)$ é corpo finito.

Teorema 2.32 *Seja A um anel de divisão finito e $a \in A$ fixo. O conjunto*

$$N_a = \{b \in A : ab = ba\}$$

é um anel de divisão finito.

***Demonstração**:* Devemos mostrar que N_a é um subanel com identidade e que todo elemento de A admite inverso multiplicativo em A. Temos $A \neq \emptyset$ pois $0_A, 1_A \in A$ são tais que $a1_A = a1_A = a$ e $0_A a = a0_A = 0_A$, logo $0_A, 1_A \in N_a$. Além disso,

- Para quaisquer $r, s \in N_a$ temos que $ra = ar$ e $sa = as$. Assim, $(r-s)a = ra - sa = ar - as = a(r-s)$, o que implica $(r-s) \in N_a$.

- Para quaisquer $r, s \in N_a$, temos que $ra = ar$ e $sa = as$, logo $rsa = ras = ars$, o que implica $rs \in N_a$.

Logo A é subanel. Como A é anel de divisão, dado $b \in N_a \subseteq A$, existe $b^{-1} \in A$. Assim, $ba = ab$ implica $ab^{-1} = b^{-1}a$ e portanto $b^{-1} \in N_a$.

Teorema 2.33 (Wedderburn) *Todo anel de divisão finito é um corpo finito.*

***Demonstração**:* Seja A um anel de divisão finito. Pelo Teorema 2.31, $Z(A)$ é um corpo finito, digamos $Z(A) = \mathbb{F}_q$. Tomando vetores em A e escalares em $\mathbb{F}_q$, podemos verificar que A é um espaço vetorial de dimensão finita $n \geq 1$ sobre $\mathbb{F}_q$. Por combinatória, vemos que A tem exatamente q^n elementos. Basta mostrar que $n = 1$, pois daí $A = \mathbb{F}_q$.

Suponhamos por absurdo que $n > 1$. Denotando $N_a = \{b \in A : ab = ba\}$, temos

$$Z(A) = \bigcap_{a \in A} N_a,$$

pois $x \in Z(A)$ se, e somente se $xa = ax$ para todo $a \in A$, o que equivale a afirmar que $x \in N_a$ para todo $a \in A$. Dessa forma, $Z(A) \subset N_a$ para todo $a \in A$. Mas pelo Teorema 2.32, N_a é anel de divisão finito que contido em A, logo N_a tem q^r elementos, com $1 \leq r \leq n$, pois N_a é subespaço vetorial de A. Vejamos que r divide n.

Como A é anel de divisão, então $A^* := A \setminus \{0_A\}$ é grupo com a operação de multiplicação de A, e $N_a^* := N_a \setminus \{0_A\}$ é o normalizador de $a \in A^*$ em A^*. Como N_a^* é subgrupo de A^*, então $|N_a^*| = q^r - 1$ divide $|A^*| = q^n - 1$, daí r divide n pelo Lema 1.1.

O centro do grupo A^* é $Z^* := Z(A) \setminus \{0_A\}$ e tem ordem $q - 1$, o normalizador de $a \in A^*$ em A^* é N_a^* e tem ordem $q^r - 1$ com r dividindo n. Tendo em vista o Teorema 1.13, as classes de conjugação em A^* que contém mais de um elemento contém $(q^n - 1)/(q^r - 1)$ elementos, com r dividindo n e $1 \leq r < n$. Portanto, a equação das classes de A^* é

$$q^n - 1 = (q - 1) + \sum_{i=1}^{k} \frac{q^n - 1}{q^{r_i} - 1} \text{ com } r_i \text{ divisor de } n \text{ e } 1 \leq r_i < n \text{ para } 1 \leq i \leq k. \quad (2.7)$$

Agora, considere $\Phi_n(x)$ o n-ésimo polinômio ciclotômico sobre o corpo dos racionais. Segue do Teorema 2.24 que $\Phi_n(x)$ tem coeficientes inteiros, logo $\Phi_n(q) \in \mathbb{Z}$. Como cada r_i é um divisor próprio de n, então pelo Lema 2.27 temos que $\Phi_n(q)$ divide $(q^n - 1)/(q^{r_i} - 1)$ para $1 \leq i \leq k$. Isso e a equação (2.7) implicam que $\Phi_n(q)$ divide $(q - 1)$. Logo $|\Phi_n(q)| \leq q - 1$ e o Lema 2.28 implica que $n = 1$.

Uma importante generalização do Teorema de Wedderburn (JACOBSON, 1945) é uma condição suficiente para que um anel seja um corpo:

Teorema 2.34 (Jacobson) *Se R é um anel tal que para todo $a \in R$, existe um inteiro $n(a) > 1$ que depende de a, tal que $a^{n(a)} = a$, então R é um corpo.*

2.7 Representação

Existem objetos matemáticos Γ que satisfazem alguns dos axiomas do corpo finito. Sob certas condições, eles cumprem todos os axiomas. Assim, faz sentido estudar aplicações injetivas $\mathbb{F}_q \to \Gamma$ que preservem as operações de $\mathbb{F}_q$ pois, a partir disso podemos olhar para $\mathbb{F}_q$ do ponto de vista da estrutura algébrica de Γ, bem como outras eventuais estruturas que Γ possua (MARTIN, 2010). Essa ideia é conhecida por **representação**, e é objeto de nosso estudo nessa seção. Vamos descrever três formas de se representar um corpo finito qualquer e em seguida vemos como usar essas ideias para analisar o corpo $\mathbb{F}_9$.

A primeira forma de representação é utilizando a base polinomial. Nesse tipo de base, as operações ocorrem de modo semelhante ao que apresentamos no exemplo 2.7.

Exemplo 2.13 *Podemos olhar para $\mathbb{F}_{q^m}$ como o conjunto dos polinômios com coeficientes em $\mathbb{F}_q$ de grau $\leq m-1$ na variável α, onde α é uma raiz de um polinômio $f \in \mathbb{F}_{q^m}$ irredutível sobre $\mathbb{F}_q$. De fato, pelo Teorema 2.4, $\mathbb{F}_{q^m}$ é extensão algébrica simples de $\mathbb{F}_q$. Pelo Corolário 2.2, existe um polinômio $f \in \mathbb{F}_q[x]$ de grau m irredutível sobre $\mathbb{F}_q$. Fixada uma raiz α de f, temos que f é o polinômio minimal de α pelo Teorema 1.44 e consequentemente $\mathbb{F}_{q^m} = \mathbb{F}_q(\alpha)$. Portanto, pelo Teorema 1.46 todo elemento de $\mathbb{F}_q(\alpha)$ pode ser escrito como $a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{m-1}\alpha^{m-1}$ com $a_i \in \mathbb{F}_q$ para $0 \leq i \leq m-1$.*

Vejamos como isso ocorre no corpo $\mathbb{F}_9$. Pelo Teorema 1.38, $f(x) = x^2 + 1 \in \mathbb{F}_3[x]$ é irredutível pois $f(0) = 1$, $f(1) = 2$ e $f(2) = 2$. Se α uma raiz de f em $\mathbb{F}_9$, então todo elemento de $\mathbb{F}_9$ é da forma $a + b\alpha$ com $a, b \in \mathbb{F}_3$. Temos

$$\mathbb{F}_9 = \mathbb{F}_3(\alpha) = \{0, 1, 2, \alpha, 1+\alpha, 2+\alpha, 2\alpha, 1+2\alpha, 2+2\alpha\}. \tag{2.8}$$

As operações entre esses elementos ocorrem forma usual, e a igualdade $0 = f(\alpha) = \alpha^2 + 1$ implica $\alpha^2 = -1$, o que nos permite operar com potências α^k, $k \geq 2$. Por exemplo, temos

$$(1+\alpha)\alpha = \alpha + \alpha^2 = \alpha - 1 = \alpha + 2. \tag{2.9}$$

Essas observações são suficientes para construir a tabela de operações em termos de (2.8).

A segunda forma de representar um corpo finito é através dos elementos primitivos.

Exemplo 2.14 *Podemos olhar para $\mathbb{F}_q$ através das potências de um elemento primitivo de $\mathbb{F}_q$. Para isso, seja* $\operatorname{char} \mathbb{F}_q = p$. *De acordo com o Teorema 2.26, $\mathbb{F}_q$ é o $(q-1)$-ésimo corpo ciclotômico sobre seu subcorpo primo $\mathbb{F}_p$. Pelo Teorema 2.24, $\Phi_{q-1}(x)$ tem coeficientes em $\mathbb{F}_p$. Como* $\operatorname{mdc}(q-1, q) = 1$, *então segue do Teorema 2.25 que $\Phi_{q-1}(x)$ pode ser fatorado como produto de certos polinômios irredutíveis de mesmo grau. Qualquer raiz de um destes fatores irredutíveis é uma n-ésima raiz primitiva da unidade, pois é raiz de $\Phi_{q-1}(x)$. Portanto, se $f(x)$ é um fator irredutível de $\Phi_{q-1}(x)$ e ξ é raiz $f(x)$, então ξ*

tem ordem $\varphi(n)$ no grupo $\mathbb{F}_q^*$, logo ξ é um elemento primitivo de $\mathbb{F}_q$. Neste caso, temos $\mathbb{F}_q^* = \{1, \xi, \xi^2, \cdots, \xi^{n-1}\}$. Em resumo, basta determinar um fator irredutível $f(x)$ de Φ_{q-1}, pois uma raiz de $f(x)$ é um gerador do grupo $\mathbb{F}_q^*$.

Vejamos como aplicar isso novamente no caso do corpo $\mathbb{F}_9$. Temos que $\mathbb{F}_9$ é o 8-ésimo corpo ciclotômico sobre $\mathbb{F}_3$. Pelo exemplo 2.10, temos que $\Phi_8(x) = x^4 + 1 \in \mathbb{F}_3[x]$. É possível mostrar que a fatoração canônica de $\Phi_8(x)$ em $\mathbb{F}_3[x]$ é

$$\Phi_8(x) = (x^2 + x + 2)(x^2 + 2x + 2). \tag{2.10}$$

Se ξ é uma raiz de $r(x) = x^2 + x + 2$, então ξ um elemento primitivo de $\mathbb{F}_9$ e assim

$$\mathbb{F}_9 = \{0, 1, \xi, \xi^2, \xi^3, \xi^4, \xi^5, \xi^6, \xi^7\}. \tag{2.11}$$

Vamos estabelecer a relação entre as tabelas de operações de (2.8) e (2.11). Para isso, observamos que $r(x)$ tem $\xi = 1 + \alpha$ como raiz, onde α é raiz de $f(x) = x^2 + 1$:

$$r(\xi) = (\alpha + 1)^2 + (\alpha + 1) + 2 = (\alpha^2 + 2\alpha + 1) + (\alpha + 1) + 2 = \alpha^2 + 1 = 0.$$

Para ξ e α assim associados, a relação que buscamos é dada pela seguinte tabela:

i	ξ^i
1	$1 + \alpha$
2	2α
3	$1 + 2\alpha$
4	2
5	$2 + 2\alpha$
6	α
7	$2 + \alpha$
8	1

(2.12)

Observamos, por exemplo, a relação entre as igualdades (2.9) e $\xi\xi^6 = \xi^7$.

Definição 2.12 *Sejam $p = \operatorname{char} \mathbb{F}_q$ e $f(x) = a_0 + a_1 x + \cdots + x_{n-1}x^{n-1} + x^n \in \mathbb{F}_q[x]$ um polinômio mônico irredutível sobre $\mathbb{F}_p$. Definimos a* ***matriz companheira*** *de f por*

$$A := \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -a_{n-1} \end{bmatrix}$$

É possível mostrar que $f(A) = 0$ [Seção 5.4 de (COELHO, 2020)]. Vamos explorar isso para ver a terceira forma de representar um corpo finito, que é através de matrizes.

Exemplo 2.15 *A matriz companheira de* $f(x) = x^2 - 1 \in \mathbb{F}_9[x]$ *é*

$$A = \begin{bmatrix} 0 & 2 \\ 1 & 0 \end{bmatrix}.$$

Como f *é irredutível e* $f(A) = 0$*, então pelo Teorema 1.46 podemos escrever*

$$\mathbb{F}_9 = \{0, I, 2I, A, I + A, 2I + A, 2A, I + 2A, 2I + 2A\}. \tag{2.13}$$

As operações entre os elementos de $\mathbb{F}_9$ *em (2.13) ocorrem como no exemplo 2.13, no entanto agora estamos somando e multiplicando matrizes com entradas em* $\mathbb{F}_3$*. Assim, valem as propriedades das operações de matrizes e, em cada entrada da matriz resultante valem as propriedade de* $\mathbb{F}_3$*. Por exemplo, observamos a relação entre a equação (2.9) e a igualdade:*

$$(I + A)A = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 0 & 2 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 2 & 2 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} + \begin{bmatrix} 0 & 2 \\ 1 & 0 \end{bmatrix} = 2I + A.$$

Podemos combinar a representação matricial com elementos primitivos.

Exemplo 2.16 *Pelo Exemplo 2.14, o polinômio* $r(x) = x^2 + x + 2 \in \mathbb{F}_3[x]$ *é um fator irredutível de* Φ_8*. A matriz companheira de* r *é*

$$C = \begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix}.$$

Como r *é irredutível com* $0 = h(C) = C^2 + C + 2I$*, então podemos deduzir que*

$$\mathbb{F}_9 = \{0, C, C^2, C^3, C^4, C^5, C^6, C^7, C^8\}. \tag{2.14}$$

Vemos facilmente que (2.13) e (2.14) estão relacionados por uma tabela análoga a (2.12).

2.8 Ordem

Nesta última seção, definimos e investigamos a ordem de um polinômio. Assim como o grau, trata-se de um inteiro positivo associado a um polinômio. Esse número aparece naturalmente no estudo do polinômio $x^n - 1$ e constitui mais um importante conceito na teoria de corpos finitos.

Teorema 2.35 *Seja* $f \in \mathbb{F}_q[x]$ *um polinômio de grau* $m \geq 1$ *com* $f(0) \neq 0$*. Existe um inteiro positivo* $e \leq q^m - 1$ *tal que* $f(x)$ *divide* $x^e - 1$*.*

***Demonstração**:* Pelo exemplo 1.16, o anel quociente $\mathbb{F}_q[x]/(f)$ contém $q^m - 1$ classes não nulas. Vejamos que as q^m classes $x^j + (f)$ são não nulas, para cada $0 \leq j \leq q^m - 1$. De

fato, se fosse $x^j + (f) = (f)$ para algum j, então $x^j = p(x)f(x)$ para algum $p(x) \in \mathbb{F}_q[x]$. Como $x = 0$ não é uma raiz de f, então x^j divide $p(x)$. Por outro lado, $p(x)$ divide x^j, logo $x^j = \alpha p(x)$ com α constante. Podemos assumir que $\alpha = 1$ e $p(x)$ é mônico, pois x^j é mônico e daí α deve ser o inverso multiplicativo do coeficiente líder de $p(x)$. Assim, $p(x) = x^j$ e daí $x^j = p(x)f(x) = x^j f(x)$ implica $1 = f(x)$, absurdo pois $\deg(f) \geq 1$. Sendo as classes $x^j + (f)$ não nulas, existem $0 \leq r < s \leq q^m - 1$ tais que $x^r + (f) = x^s + (f)$, isto é, $x^r \equiv x^s \pmod f$. Como a única raiz do polinômio x é $x = 0$, e $x = 0$ não é raiz de f, então x e $f(x)$ são relativamente primos. Logo $x^{s-r} \equiv 1 \pmod f$, ou seja, $f(x)$ divide $x^e - 1$ com $e = s - r > 0$. Concluímos tomando o menor e com esta propriedade.

Definição 2.13 *Seja $f \in \mathbb{F}_q[x]$ um polinômio não nulo com $f(0) \neq 0$. Chamamos de* ***ordem*** *de f, e denotamos por* $\mathrm{ord}(f)$*, o menor inteiro positivo $\mathfrak{e}$ tal que $f(x)$ divide $x^{\mathfrak{e}} - 1$.*

Observação 2.4 *Seja $f \in \mathbb{F}_q[x]$ um polinômio com $f(0) = 0$ e seja h a multiplicidade da raiz $x = 0$. Podemos escrever f de modo único como $f(x) = x^h g(x)$, com $g(0) \neq 0$. Neste caso, definimos* $\mathrm{ord}(f) := \mathrm{ord}(g)$.

Pelo Teorema 2.35, se $f \in \mathbb{F}_q[x]$ tem grau m e $f(0) = 0$, então $\mathrm{ord}(f) \leq q^m - 1$.

Quando o polinômio é irredutível, temos o seguinte resultado:

Teorema 2.36 *Seja $f \in \mathbb{F}_q[x]$ um polinômio irredutível sobre $\mathbb{F}_q$ de grau m. A ordem de f é igual a ordem de qualquer raiz de f no grupo multiplicativo $\mathbb{F}_{q^m}^*$.*

***Demonstração**:* Seja α uma raiz arbitrária de f. Segue do Teorema 2.6 que $\alpha \in \mathbb{F}_{q^m}$. Pelo Teorema 2.35, existe o menor inteiro positivo $\mathfrak{e}$ tal que $f(x)$ divide $x^{\mathfrak{e}} - 1$. Então $\mathfrak{e}$ é raiz de $x^{\mathfrak{e}} - 1$, isto é, $\alpha^{\mathfrak{e}} = 1$, o que implica que $|\alpha|$ divide $\mathfrak{e}$. Se $|\alpha|$ fosse um divisor próprio de $\mathfrak{e}$, teríamos $\alpha^{|\alpha|} = 1$ e, sendo α uma raiz do polinômio irredutível f, segue do Lema 2.3 que $f(x)$ divide $x^{|\alpha|} - 1$, absurdo pois $|\alpha| < \mathfrak{e} = \mathrm{ord}(f)$. Portanto, $\mathrm{ord}(f) = |\alpha|$.

Corolário 2.7 *Se $f \in \mathbb{F}_q[x]$ é um polinômio irredutível sobre $\mathbb{F}_q$ de grau m, então*

$$\mathrm{ord}(f) \text{ divide } q^m - 1.$$

***Demonstração**:* Se α é uma raiz $f(x)$, então $\alpha \in \mathbb{F}_{q^m}$, o que implica que $|\alpha|$ divide $|\mathbb{F}_q^*| = q^m - 1$. Segue do Teorema 2.36 que $\mathrm{ord}(f) = |\alpha|$, portanto $\mathrm{ord}(f)$ divide $q^m - 1$.

A seguir, uma fórmula para o número polinômios irredutíveis em termos da ordem.

Teorema 2.37 *O número de polinômios mônicos irredutíveis sobre $\mathbb{F}_q$ de grau m e ordem $\mathfrak{e}$ é igual a $\varphi(\mathfrak{e})/m$, se $\mathfrak{e} \geq 2$ e $m = \mathrm{ord}_{\mathfrak{e}}(q)$; é igual a 1, se $m = \mathfrak{e} = 1$; e é igual a 0 em todos os outros casos. Em particular, o grau de um polinômio mônico irredutível sobre $\mathbb{F}_q$ de ordem $\mathfrak{e}$ é igual a $\mathrm{ord}_e(q)$.*

***Demonstração**:* Seja $f \in \mathbb{F}_q$ irredutível de grau m com $f(0) \neq 0$. Afirmamos que $\text{ord}(f) = \mathfrak{e}$ se, e somente se toda raiz de f é uma $\mathfrak{e}$-ésima raiz primitiva da unidade sobre $\mathbb{F}_{q^m}$. De fato, suponhamos que $\mathfrak{e} = \text{ord}\, f$. Então $\mathfrak{e}$ é o menor inteiro positivo tal que f divide $x^{\mathfrak{e}} - 1$. Isso implica que toda raiz $\alpha \in \mathbb{F}_{q^m}$ de f cumpre $\alpha^{\mathfrak{e}} - 1 = 0$. Reciprocamente, suponhamos que toda raiz $\alpha \in \mathbb{F}_{q^m}$ de f é também uma $\mathfrak{e}$-ésima raiz primitiva da unidade sobre $\mathbb{F}_{q^m}$. Pelo Teorema 2.36, $\mathfrak{e}$ é o menor inteiro positivo tal que $\alpha^{\mathfrak{e}} - 1 = 0$, e como α é raiz do polinômio irredutível f, então pelo Lema 2.3 temos que $f(x)$ divide $x^{\mathfrak{e}} - 1$.

Segue da afirmação que, se $\mathfrak{e} = \text{ord}(f)$ com f irredutível, então $f(x)$ é um fator irredutível de $\Phi_{\mathfrak{e}}(x)$. Pelo Teorema 2.25, qualquer fator mônico irredutível de $\Phi_{\mathfrak{e}}(x)$ tem o mesmo grau $m = \text{ord}_{\mathfrak{e}}(q)$, e o número de tais fatores é $\varphi(\mathfrak{e})/m$ desde que $\text{mdc}(\mathfrak{e}, q^m) = 1$. Mas isso sempre vale pois qualquer divisor comum d de $\mathfrak{e}$ e q^m é da forma $d = p^j$ com p primo, e como $\mathfrak{e}$ divide $q^m - 1 = |\mathbb{F}_{q^m}^*|$ pela afirmação, então d deve dividir $q^m - 1$, o que só é possível se $d = 1$. Quando $m = \mathfrak{e} = 1$, o único polinômio mônico irredutível é $p(x) = x$. A demonstração está concluída pois analisamos todos os casos possíveis.

Exemplo 2.17 *Seja $f \in \mathbb{F}_q[x]$ um polinômio mônico irredutível sobre $\mathbb{F}_q$. Pelo Teorema 2.37, f tem grau $m = \text{ord}_{\mathfrak{e}}(q)$, onde $\mathfrak{e} = \text{ord}(f)$. Para q e $\mathfrak{e}$ convenientes, podemos usar isso para obter o grau se a ordem for dada, ou obter a ordem se o grau for dado. Por exemplo, a ordem de qualquer polinômio mônico irredutível de grau 3 sobre $\mathbb{F}_2$ é dada por $3 = ord_{\mathfrak{e}}(2)$, o que equivale a $2^3 \equiv 1 \pmod{\mathfrak{e}}$, o que é possível apenas para $\mathfrak{e} = 7$. Assim, o número de polinômios mônicos irredutíveis sobre $\mathbb{F}_2$ de grau 3 e ordem 7 é $\varphi(7)/3 = 2$.*

Os resultados a seguir nos permitem calcular a ordem de um polinômio qualquer.

Teorema 2.38 *Seja c um inteiro positivo. O polinômio $f \in \mathbb{F}_q[x]$ com $f(0) \neq 0$ divide $x^c - 1$ se, e somente se $\text{ord}(f)$ divide c.*

***Demonstração**:* Seja $\mathfrak{e} = \text{ord}(f)$. Se $f(x)$ divide $x^c - 1$, então $c \geq \mathfrak{e}$. Pelo Algoritmo da Divisão, temos $c = m\mathfrak{e} + r$ com $0 \leq r < \mathfrak{e}$. Logo, $x^c - 1 = x^{m\mathfrak{e}+r} - 1 = (x^{m\mathfrak{e}} - 1)x^r + (x^r - 1)$. Pelo Lema 2.4, $x^{\mathfrak{e}} - 1$ divide $x^{m\mathfrak{e}} - 1$. Como $f(x)$ divide $x^c - 1$ e $x^{\mathfrak{e}} - 1$, então $f(x)$ divide $x^r - 1$ com $r < \mathfrak{e}$. Mas isso só é possível se $r = 0$ e portanto $\mathfrak{e} = \text{ord}(f)$ divide c. Reciprocamente, se $\mathfrak{e} = \text{ord}(f)$ divide c, então $x^{\mathfrak{e}} - 1$ divide $x^c - 1$ pelo Lema 2.4. Como f divide $x^{\mathfrak{e}} - 1$, concluímos que f divide $x^c - 1$.

Teorema 2.39 *Seja $g \in \mathbb{F}_q[x]$ um polinômio irredutível sobre $\mathbb{F}_q$ de grau m com $g(0) \neq 0$ e ordem $\mathfrak{e}$. Considere $f(x) = (g(x))^b$, onde b é um inteiro positivo. Se t é o menor inteiro positivo tal que $p^t \geq b$, onde p é a característica de $\mathbb{F}_q$, então $\text{ord}(f) = \mathfrak{e}p^t$.*

***Demonstração**:* Seja $c = \text{ord}(f)$. Como g é um fator irredutível de f, e $f(x)$ divide $x^c - 1$, então $g(x)$ divide $x^c - 1$. Logo, $\mathfrak{e} = \text{ord}(g)$ divide c pelo Teorema 2.38. Seja t o

menor inteiro positivo tal que $p^t \geq b$, onde p é a característica de $\mathbb{F}_q$ e b é um inteiro positivo qualquer. Podemos escrever $p^t = b + s$ para algum $s \geq 0$. Pelo Teorema 1.23, temos

$$(x^{\mathfrak{e}p^t} - 1) = (x^{\mathfrak{e}} - 1)^{p^t} = (x^{\mathfrak{e}} - 1)^b (x^{\mathfrak{e}} - 1)^s.$$

Como $g(x)$ divide $x^{\mathfrak{e}} - 1$, então $f(x) = (g(x))^b$ divide $(x^{\mathfrak{e}} - 1)^b$. Logo $f(x)$ divide $x^{\mathfrak{e}p^t} - 1$. Pelo Teorema 2.38, c divide $\mathfrak{e}p^t$. Sendo $\mathfrak{e}$ mínimo, então c é da forma $c = \mathfrak{e}p^u$ com $0 \leq u \leq t$.

Pelo Corolário 2.7, $\mathfrak{e}$ divide $q^m - 1$. Logo $\mathfrak{e}$ não é múltiplo de q^m, o que implica que todas as raízes de $x^{\mathfrak{e}} - 1$ são simples pelo Teorema 1.37. Assim, $(x^{\mathfrak{e}p^u} - 1) = (x^{\mathfrak{e}} - 1)^{p^u}$ tem $\mathfrak{e}$ raízes de multiplicidade p^u. Como $(g(x))^b$ divide $(x^{\mathfrak{e}p^u} - 1) = (x^{\mathfrak{e}} - 1)^{p^u}$, então comparando a multiplicidade das raízes vemos que $p^u \geq b$, logo $t \leq u$. Portanto, $t = u$ e $\text{ord}(f) = \mathfrak{e}p^t$.

Teorema 2.40 *Seja $f(x) = g_1(x)g_2(x)\cdots g_k(x)$, com $g_1, g_2, \cdots, g_k \in \mathbb{F}_q[x]$ primos em pares. Então* $\text{ord}(f) = \text{mmc}(\text{ord}(g_1), \text{ord}(g_2), \cdots, \text{ord}(g_k))$.

***Demonstração**:* Sejam $\mathfrak{e} = \text{ord}(f)$, $e_i = \text{ord}(g_i)$ para $1 \leq i \leq k$ e $c = \text{mmc}(e_1, e_2, \cdots, e_k)$. Por definição de ordem, $g_i(x)$ divide $x^{e_i} - 1$ para cada i. Como e_i divide c, então $x^{e_i} - 1$ divide $x^c - 1$ pelo Lema 2.4. Logo g_i divide $x^c - 1$ para cada i. Como os polinômios $g_1, g_2, \cdots, g_k$ são primos em pares, isto é, $\text{mdc}(g_i, g_j) = 1$ sempre que $i \neq j$, então $f(x) = g_1(x), g_2(x), \cdots, g_k(x)$ divide $x^c - 1$. Consequentemente, $\mathfrak{e}$ divide c pelo Corolário 2.7. Por outro lado, $f(x)$ divide $x^{\mathfrak{e}} - 1$ e, como cada $g_i(x)$ divide $f(x)$, então $g_i(x)$ divide $x^{\mathfrak{e}} - 1$ para cada $1 \leq i \leq k$. Pelo Corolário 2.7, isso implica que e_i divide $\mathfrak{e}$ para cada i. Logo, $c = \text{mmc}(e_i, e_2, \cdots, e_k)$ divide $\mathfrak{e}$. Portanto, $c = \mathfrak{e}$.

Podemos calcular a ordem de um polinômio redutível arbitrário.

Exemplo 2.18 *Vamos calcular a ordem do polinômio*

$$f(x) = x^{10} + x^9 + x^3 + x^2 + 1 \in \mathbb{F}_2[x].$$

Passo 1. Escrevemos a fatoração canônica de f:

$$f(x) = (x^2 + x + 1)^3 (x^4 + x + 1).$$

Se denotarmos $g(x) = (x^2 + x + 1)$ e $h(x) = (x^4 + x + 1)$, então temos $f(x) = (g(x))^3 h(x)$ com $g(x)$ e $h(x)$ polinômios irredutíveis.

Passo 2. Calculamos a ordem dos fatores primos em pares na decomposição de f, que são $\text{ord}(g^3)$ *e* $\text{ord}(h)$*. Para calcular* $\text{ord}(g^3)$*, é suficiente calcular* $\text{ord}(g)$ *e aplicar o Teorema 2.39: Temos que* $\text{ord}(g) = 3$ *e 2 é o menor inteiro tal que $2^2 = 4 \geq 3$, logo* $\text{ord}(g^3) = 3 \cdot 4 = 12$*. Por sua vez,* $\text{ord}(h) = 15$*.*

Passo 3. Aplicamos o Teorema 2.40 para calcular $\text{ord}(f)$ *desde que as ordem dos fatores primos em pares de f sejam conhecidas. Pelo passo 2, temos* $\text{ord}(g^3) = 12$ *e* $\text{ord}(h) = 15$*, logo* $\text{ord}(f) = \text{mmc}(12, 15) = 60$*.*

Observação 2.5 *Seja a, b, r, s, p inteiros positivos com p primo. Vale o seguinte:*

$$\text{mmc}(ap^r, bp^s) = \text{mmc}(a, b) \cdot p^u \text{ com } u = max\{r, s\}.$$

Temos uma fórmula para o cálculo da ordem a partir da fatoração canônica.

Corolário 2.8 *Seja $f \in \mathbb{F}_q[x]$ um polinômio de grau positivo com $f(0) \neq 0$. Se*

$$f(x) = a(f_1(x))^{n_1}(f_2(x))^{n_2} \cdots (f_k(x))^{n_k} \text{ com } a \in \mathbb{F}_q \text{ e } n_i \in \mathbb{N}$$

é a fatoração canônica de f em $\mathbb{F}_q$, então

$$\text{ord}(f) = cp^t,$$

onde $c = \text{mmc}(\text{ord}(f_1), \text{ord}(f_2), \cdots, \text{ord}(f_k))$, $p = \text{char}\,\mathbb{F}_q$ e t é o menor inteiro positivo tal que $p^t \geq \max\{n_1, n_2, \cdots, n_k\}$.

***Demonstração**:* Tomando $g_i(x) = (f_i(x))^{n_i}$ para $1 \leq i \leq k$, temos pelo Teorema 2.39 que $\text{ord}(g_i) = e_i p^{t_i}$, onde $e_i = \text{ord}(f_i)$ e t_i é o menor inteiro positivo tal que $p^{t_i} \geq n_i$. Como os g_i são primos em pares, segue do Teorema 2.40 que $\text{ord}(f) = \text{mmc}(e_1 p^{t_1}, e_2 p^{t_2}, \cdots, e_k p^{t_k})$ e o resultado segue da obervação 2.5.

Conclusão

O conteúdo do capítulo introdutório foi selecionada de modo a ser ao mesmo tempo abstrato e aplicável ao estudo dos corpos finitos. Detalhes omitidos e resultados relacionados a estruturas algébricas gerais podem ser encontrados nos livros (HUNGERFORD, 1980) e (GALLIAN, 2017); já o livro (ENDLER, 2006) se concentra de forma mais profunda na teoria dos anéis e ideias. Os livros (MARTIN, 2010) e (GONÇALVES, 1979) abordam de forma mais direta os corpos em característica prima e zero, respectivamente. Para aplicações de corpos finitos em criptografia e teoria dos códigos, indicamos o livro (PANARIO, 2007).

O capítulo principal é baseado principalmente no segundo capítulo do livro (LIDL; NIEDERREITER, 1997). Esse livro é uma referência clássica da teoria de corpos finitos. Ele contém uma exposição de diversos conceitos básicos da teoria, com demonstrações e exemplos detalhados. Além disso, ele traz uma extensa lista de artigos e livros contendo resultados mais profundos.

Fazemos agora alguns comentários sobre o capítulo principal. O Teorema 2.6 garante a aplicabilidade do bem conhecido Teorema Fundamental da Teoria de Galois para o caso de extensões finitas de corpos finitos. Esse resultado diz que, em certo sentido, a estrutura de subgrupos do grupo de automorfismos de corpos F sobre um subcorpo K está em bijeção com a estrutura de subcorpos de F. A classificação de todas as aplicações lineares entre corpos finitos em termos do traço dá uma ideia da importância do conceito de traço; a aplicação norma não é menos relevante para a teoria. Ambas são amplamente usadas, por exemplo, na Teoria dos Números Algébricos, como pode ser constatado no livro (ENDLER, 2006). O Teorema 2.11 é um caso particular de um importante resultado mais geral conhecido como Teorema 90 de Hilbert. Além das que apresentamos, existem outros tipos de bases e representações de corpos finitos de grande interesse. Uma dessas representações é o fato de que corpos finitos podem ser vistos como classe residuais de certos anéis quocientes.

Sem dúvidas, a Teoria dos Corpos Finitos constitui uma área rica de investigações teóricas e aplicações. Esperamos que este trabalho contribua para estudos futuros dessa teoria, bem como da álgebra e matemática em geral.

Referências

COELHO, M. L. L. F. U. *Um Curso de Álgebra Linear*. 2. ed. [S.l.]: Editora da Universidade de São Paulo, 2020. ISBN 978-85-314-0594-5. Citado 2 vezes nas páginas 51 e 63.

ENDLER, O. *Teoria do Números Algébricos*. [S.l.]: Instituto de Matemática Pura e Aplicada, 2006. Citado na página 69.

GALLIAN, J. A. *Contemporary Abstract Algebra*. 9. ed. [S.l.]: Cecange Learning, 2017. ISBN 978-1-305-65796-0. Citado 2 vezes nas páginas 58 e 69.

GONÇALVES, A. *Introdução à Álgebra*. [S.l.]: Instituto de Matemática Pura e Aplicada, Rio de Janeiro, 1979. v. 7. xiv+194 p. (Projeto Euclides [Euclid Project], v. 7). Citado 3 vezes nas páginas 1, 11 e 69.

HUNGERFORD, T. W. *Algebra*. [S.l.]: Springer-Verlag, New York-Berlin, 1980. v. 73. xxiii+502 p. (Graduate Texts in Mathematics, v. 73). Reprint of the 1974 original. ISBN 0-387-90518-9. Citado 3 vezes nas páginas 1, 4 e 69.

JACOBSON, N. Structure theory for algebraic algebras of bounded degree. *Annals of Mathematics*, v. 46, p. 695–707, 1945. Citado na página 61.

LIDL, R.; NIEDERREITER, H. *Finite Fields*. Second. [S.l.]: Cambridge University Press, Cambridge, 1997. v. 20. xiv+755 p. (Encyclopedia of Mathematics and its Applications, v. 20). With a foreword by P. M. Cohn. ISBN 0-521-39231-4. Citado 5 vezes nas páginas 9, 1, 32, 60 e 69.

MARTIN, P. A. *Grupos, Corpos e Teoria de Galois*. 1. ed. [S.l.]: Livraria da Física, 2010. ISBN 978-8578610654. Citado 3 vezes nas páginas 38, 62 e 69.

PANARIO, A. M. M. D. *Tópicos de Corpos Finitos com Aplicações em Criptografia e Teoria de Códigos*. 1. ed. [S.l.]: Impa, 2007. ISBN 978-85-244-0261-6. Citado 2 vezes nas páginas 9 e 69.

SEROUSSI, G.; LEMPEL, A. Factorization of symmetric matrices and trace-orthogonal bases in finite fields. *SIAM Journal on Computing*, v. 9, n. 4, p. 758–767, Nov 1980. Citado na página 50.

Índice