



Universidade Federal de Uberlândia - UFU

Faculdade de Matemática - FAMAT

Coordenação dos Cursos de Bacharelado e Licenciatura em Matemática

Trabalho de Conclusão de Curso

O Teorema de Wedderburn

Aluno: João Paulo Guardieiro Sousa

Orientador: Guilherme Chaud Tizziotti

João Paulo Guardieiro Sousa

O Teorema de Wedderburn

Trabalho apresentado à Faculdade de Matemática, como parte dos requisitos para obtenção do título de Bacharel em matemática

Universidade Federal de Uberlândia – UFU

Faculdade de Matemática

Orientador: Prof. Dr. Guilherme Chaud Tizziotti

Uberlândia-MG

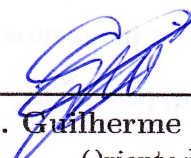
2018

João Paulo Guardieiro Sousa

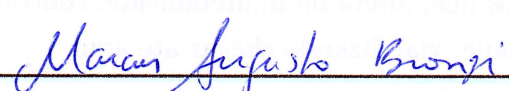
O Teorema de Wedderburn

Trabalho apresentado à Faculdade de Matemática, como parte dos requisitos para obtenção do título de Bacharel em matemática

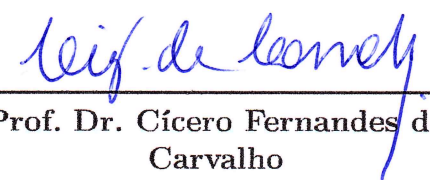
Trabalho aprovado. Uberlândia-MG, 11 de dezembro de 2018:



Prof. Dr. Guilherme Chaud Tizziotti
Orientador



Prof. Dr. Marcus Augusto Bronzi



Prof. Dr. Cícero Fernandes de
Carvalho

Uberlândia-MG

2018

Agradecimentos

Agradeço primeiramente a Deus por ter me dado forças para chegar até esse momento, superar os obstáculos e alcançar tantas graças. Por ter me dado a vida, minha família e meus amigos.

Agradeço também à Universidade Federal de Uberlândia e a todos os professores que dela fazem parte, que contribuíram diretamente para minha formação acadêmica, me ensinando novas formas de enxergar a matemática e sendo exemplo para o profissional o qual quero me tornar.

Em especial, agradeço a meu orientador Guilherme Chaud Tizziotti pelos três anos e meio de iniciação, um período no qual amadureci muito, aprendendo novos assuntos em matemática. Fico profundamente grato aos desafios de cada seminário, que me fizeram repensar meu modo de estudo. Obrigado pelo apoio e incentivo, principalmente por ter me dado um direcionamento.

Não poderia deixar de agradecer à minha família, minha mãe Cláudia, meu pai Valtuir e meu irmão Vinícius com os quais aprendi a ser mais humano e ajudaram a moldar a pessoa que sou hoje. Agradeço ainda a todos os meus tios, primos e avós os quais sempre me acolheram nas dificuldades e me mostraram a beleza de se viver em família.

Aos meus amigos, por transformarem-se em quase irmãos, em especial àqueles com quem compartilhei esses últimos quatro anos, da faculdade e da igreja, apoiando-me em várias decisões e me dando suporte nos momentos mais difíceis.

Também à CAPES e ao CNPq, pelo aporte financeiro e por terem me possibilitado começar uma iniciação científica.

Por fim, a todos que, direta ou indiretamente, contribuíram de alguma forma para me tornar quem sou hoje, viabilizando chegar até aqui.

*Eu tenho uma epígrafe verdadeiramente maravilhosa,
mas essa página é muito pequena para a conter.*

Resumo

“Todo anel de divisão finito é um corpo”. Esse é o enunciado do Teorema de Wedderburn, proposto no início do século XX. A partir de resultados envolvendo corpos finitos e polinômios definidos sobre eles, pode-se provar esse importante resultado, bem como caracterizar e compreender melhor essas estruturas.

Palavras-chave: Álgebra. Teoria de corpos. Polinômios.

Abstract

“Every finite division ring is a field”. This is what the Wedderburn’s Theorem states, proposed at the beginning of the XXth century. Starting by results concerning finite fields and polynomials defined over them, one can prove this result, as well as characterize and understand better those structures.

Keywords: Algebra. Field Theory. Polynomials.

Sumário

	Introdução	9
1	RESULTADOS PRELIMINARES	10
1.1	Estruturas algébricas	10
1.2	Polinômios	15
1.3	Extensões de corpos	18
2	CORPOS FINITOS	23
3	RAÍZES DE POLINÔMIOS IRREDUTÍVEIS E POLINÔMIOS CI- CLOTÔMICOS	29
3.1	Raízes de polinômios irredutíveis	29
3.2	Polinômios ciclotômicos	32
4	TEOREMA DE WEDDERBURN	37
5	CONCLUSÃO	42
	REFERÊNCIAS	43
	APÊNDICE A – REPRESENTAÇÃO DE CORPOS FINITOS . . .	44

Introdução

Os corpos são estruturas algébricas muito importantes em diversos campos da álgebra e até em outras áreas da matemática: o conceito de corpo foi usado implicitamente por Évariste Galois (1811-1832) em seus trabalhos que envolviam buscar soluções para equações e culminaram na importante Teoria de Galois. A Teoria de Corpos é, de certa forma, uma extensão da Teoria de Anéis, afinal, um corpo é um anel comutativo com unidade em que todos os elementos não nulos possuem um inverso multiplicativo.

É importante destacar uma outra estrutura: os anéis de divisão. Esses são simplesmente anéis com unidade em que todos os elementos não nulos possuem um inverso multiplicativo (a comutatividade da multiplicação não é exigida). De certa forma, podemos enxergar os corpos como anéis de divisão comutativos.

Um exemplo de anel de divisão que não é um corpo é o conjunto dos números quaternions

$$\mathbb{H} = \{u + xi + yj + zk, u, x, y, z \in \mathbb{R}\},$$

em que $i^2 = j^2 = k^2 = -1$, $i \cdot j = k$, $j \cdot k = i$, $k \cdot i = j$, $j \cdot i = -k$, $k \cdot j = -i$ e $i \cdot k = -j$. Podemos ver esse anel como uma extensão dos números complexos $\mathbb{C}$. Como no caso complexo, dado um número $q = u + xi + yj + zk \in \mathbb{H}$, definimos seu conjugado por $\bar{q} = u - xi - yj - zk$ e seu módulo por $|q| = \sqrt{u^2 + x^2 + y^2 + z^2}$ e a unidade desse anel é o número real 1. Assim, pode-se provar que $\mathbb{H}$ é um anel, o inverso de um quaternião q é $q^{-1} = \frac{\bar{q}}{|q|^2}$ (donde $\mathbb{H}$ é um anel de divisão) e, como, por exemplo, $ij = k$ e $ji = -k$, vemos que esse anel não é comutativo (logo $\mathbb{H}$ não é um corpo).

O resultado central deste trabalho é o Teorema de Wedderburn, desenvolvido pelo matemático escocês Joseph Wedderburn (1882-1948). Ele nos diz que um anel de divisão finito é um corpo, ou seja, se estamos trabalhando com uma estrutura algébrica que sabemos ser um anel finito com unidade e sabemos que todos os elementos não nulos possuem um inverso multiplicativo, então a multiplicação nesse anel é comutativa.

Nesse trabalho, caracterizaremos corpos finitos, de forma que possamos entender melhor como seus elementos se relacionam e como obter subcorpos e extensões de grau finito. A seguir, apresentaremos alguns resultados fortes sobre polinômios irredutíveis e suas raízes, bem como uma classe importante de tais polinômios: os polinômios ciclotômicos. Por fim, utilizando resultados de álgebra linear e teoremas vistos ao longo do trabalho, daremos duas demonstrações para o Teorema de Wedderburn.

1 Resultados preliminares

Nesse capítulo, começaremos com definições básicas, como grupos, anéis e corpos e finalizaremos com resultados importantes envolvendo polinômios irredutíveis e corpos de decomposição.

1.1 Estruturas algébricas

Definição 1.1. Um **grupo** é um conjunto G munido com uma operação $*$ tal que as seguintes propriedades são válidas:

1. $*$ é associativa, isto é, para quaisquer $a, b, c \in G$,

$$a * (b * c) = (a * b) * c.$$

2. Existe um elemento identidade (ou unidade) e em G tal que, para todo $a \in G$,

$$a * e = e * a = a.$$

3. Para cada $a \in G$, existe um elemento inverso a^{-1} em G tal que

$$a * a^{-1} = a^{-1} * a = e.$$

Se o grupo também satisfizer

4. Para todos $a, b \in G$,

$$a * b = b * a,$$

então o grupo será chamado de **abeliano** (ou **comutativo**).

Por fim, se o conjunto G for finito, o grupo será dito **finito** e o número de elementos de G é chamado **ordem de G** , e denotado por $|G|$.

Em particular, se a operação $*$ é chamada de adição, o grupo será dito aditivo e, se a operação $*$ é chamada de multiplicação, o grupo será dito multiplicativo. Ainda, se $H \subset G$ e a operação $*$ restrita a H conservar as propriedades acima, chamaremos H de **subgrupo** de G .

Vale, ainda, destacar uma importante classe de grupos: os **grupos cíclicos**. Dizemos que um grupo multiplicativo é cíclico se existir $a \in G$ tal que, para todo $b \in G$, existe um inteiro j tal que $b = a^j = a \cdot a \cdots a$, isto é, $G = \{a^m : m \in \mathbb{Z}\}$. O elemento a é chamado **gerador** de G . É simples ver que todo grupo cíclico é abeliano.

Queremos definir um grupo muito importante, denotado por $\mathbb{Z}_n$ e chamado de grupo das classes de restos na divisão por um número n . Para isso, precisamos entender o que é uma classe. Seja S um conjunto. Dizemos que um subconjunto R de $S \times S$ é uma **relação de equivalência** em S se as três seguintes propriedades forem satisfeitas:

1. $(s, s) \in R$ para todo $s \in S$ (reflexiva).
2. Se $(s, t) \in R$, então $(t, s) \in R$ (simétrica).
3. Se $(s, t), (t, u) \in R$, então $(s, u) \in R$ (transitiva).

Se agruparmos todos os elementos de S equivalentes a um elemento $s \in S$ fixado, obteremos o que chamamos de **classe de equivalência** de s , denotada por

$$\bar{s} = \{t \in S : (s, t) \in R\}.$$

Note que $\bar{s} = \bar{t}$ se, e somente se, $(s, t) \in R$.

Definição 1.2. Para inteiros arbitrários a, b e um natural n , dizemos que a é **congruente** a b módulo n , e escrevemos $a \equiv b \pmod{n}$ se $a - b$ for um múltiplo de n .

Pode-se verificar facilmente que a “congruência módulo n ” é uma relação de equivalência no conjunto dos inteiros $\mathbb{Z}$.

Definição 1.3. O grupo formado pelo conjunto $\{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$ de classes de equivalência módulo n com a operação

$$\bar{a} + \bar{b} = \overline{a + b}$$

é chamado **grupo de inteiros módulo n** e denotado por $\mathbb{Z}_n$.

Para finalizar o estudo dos grupos, precisamos definir o que seriam o normalizador de um conjunto, o centro de um grupo e apresentar a equação de classe. Para isso, tomando um subconjunto S de um grupo G e um elemento $a \in G$, denotaremos por aSa^{-1} o conjunto

$$aSa^{-1} = \{asa^{-1} : s \in S\}.$$

Definição 1.4. Seja S um subconjunto não vazio de G . O **normalizador** de S em G é o conjunto $N(S) = \{a \in G : aSa^{-1} = S\}$.

Dizemos que dois elementos $a, b \in G$ são **conjugados** se existir um elemento $g \in G$ tal que $gag^{-1} = b$. Se agruparmos todos os elementos conjugados a um elemento fixado a , obteremos um conjunto chamado de **classe de conjugação** de a . Para certos elementos, essas classes de conjugação são unitárias, e isso vale exatamente para os elementos do centro do grupo G .

Definição 1.5. Para um grupo G , o **centro** de G é o conjunto $C(G) = \{c \in G : ac = ca, \text{ para todo } a \in G\}$.

Nesse caso, um conjugado de $c \in C(G)$ é um elemento $b \in G$ tal que existe $g \in G$ com $gcg^{-1} = b$. Mas, como c comuta com g , $gcg^{-1} = cgg^{-1} = c$. Assim, temos $c = b$ e o único elemento conjugado a c é o próprio c .

Por fim, precisamos apresentar a equação de classe. Sua demonstração pode ser encontrada como corolário do Teorema 2.H de [5].

Teorema 1.6 (Equação de classe). *Seja G um grupo finito com centro $C(G)$. Então,*

$$|G| = |C(G)| + \sum_{i=1}^k |C_G(x_i)|,$$

em que $C_G(x_i)$ percorrem todas as classes de conjugação distintas e não unitárias de G e $|X|$ denota a ordem (ou quantidade de elementos) do conjunto X .

Agora, podemos definir anéis e corpos, uma “generalização” dos grupos. Para essas duas estruturas, porém, precisamos de duas operações.

Definição 1.7. Um **anel** R é um conjunto R munido de duas operações chamadas de adição e multiplicação, e denotadas por $+$ e $\cdot$ respectivamente, tais que

1. R é um grupo abeliano com respeito a $+$.
2. $\cdot$ é associativa, isto é, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, para todos $a, b, c \in R$.
3. A lei distributiva é válida, ou seja, para todos $a, b, c \in R$, temos $a \cdot (b + c) = a \cdot b + a \cdot c$ e $(b + c) \cdot a = b \cdot a + c \cdot a$.

Denotamos por 0 o elemento identidade do grupo abeliano R com respeito à operação de adição e por $-a$ o inverso aditivo de um elemento $a \in R$. Um exemplo bem conhecido de anel é o conjunto dos números inteiros $\mathbb{Z}$. Assim como no caso dos grupos, se tivermos $H \subset R$ e as propriedades acima ainda forem válidas em H , chamaremos H de **subanel** de R .

- Definição 1.8.**
1. Um anel R é chamado **anel com identidade** se R tiver um elemento identidade para a multiplicação, isto é, se existir um elemento e tal que $a \cdot e = e \cdot a = a$ para todo $a \in R$.
 2. Um anel é dito **comutativo** se a operação $\cdot$ for comutativa.
 3. Um anel é chamado um **domínio de integridade** se for um anel comutativo com identidade $e \neq 0$ no qual $a \cdot b = 0$ implica $a = 0$ ou $b = 0$.

4. Um anel é chamado um **anel de divisão** se os elementos não nulos de R formarem um grupo sob a multiplicação.
5. Um anel de divisão comutativo é chamado de **corpo**.

Denotaremos o elemento identidade da multiplicação (quando esse existir) por 1. Um **subcorpo** H do corpo F é um subconjunto H de F tal que H também é um corpo. Um exemplo importante de corpo é o conjunto dos números reais $\mathbb{R}$.

Se um dado anel R não for domínio de integridade, isto é se existirem $a, b \in R \setminus \{0\}$ tais que $ab = 0$, dizemos que R tem divisores de zero e, obviamente, a e b são esses divisores. Pode-se provar que todo corpo é um domínio de integridade e que todo domínio de integridade finito é um corpo.

De fato, sejam F um corpo e $a, b \in F$ tais que $ab = 0$. Suponha $a \neq 0$. Assim, existe $a^{-1} \in F$ tal que $a^{-1}a = 1$. Dessa forma, $a^{-1}(ab) = 0$ implica $b = 0$ e vemos que F é domínio de integridade.

Agora, seja $D = \{0, d_1, \dots, d_n\}$ um domínio de integridade finito e, para cada $i \in \{1, \dots, n\}$ consideremos os produtos $d_i d_1, \dots, d_i d_n$, que são dois a dois distintos (se tivermos $d_i d_j = d_i d_k$, teremos $d_i(d_j - d_k) = 0$ e $d_j = d_k$). Dessa forma, os produtos percorrem todos os elementos não nulos de D . Em particular, existe j tal que $d_i d_j = 1$ (já que 1 é um elemento de D), e vemos que um elemento não nulo arbitrário $d_i \in D$ é invertível.

Usando esse fato, podemos mostrar o seguinte.

Teorema 1.9. $\mathbb{Z}_p$, o anel das classes de restos na divisão por um primo p , é um corpo.

Demonstração. Aqui, as duas operações $+$ e $\cdot$ são definidas da seguinte forma:

$$\bar{a} + \bar{b} = \overline{a + b} \text{ e } \bar{a} \cdot \bar{b} = \overline{a \cdot b}.$$

Como $\mathbb{Z}_p$ é finito, precisamos apenas mostrar que $\mathbb{Z}_p$ é um domínio de integridade. Note que $\bar{1}$ é identidade de $\mathbb{Z}_p$ e $\bar{a}\bar{b} = \overline{ab} = \bar{0}$ se, e somente se, $ab = kp$ para algum inteiro k . Mas, uma vez que p é primo, p divide ab se, e somente se, p dividir a ou p dividir b . Portanto, devemos ter $\bar{a} = \bar{0}$ ou $\bar{b} = \bar{0}$. Logo, $\mathbb{Z}_p$ é um domínio de integridade. $\square$

Esses corpos $\mathbb{Z}_p$ são muito importantes pois, veremos mais adiante, todo corpo finito contém um subcorpo isomorfo a algum $\mathbb{Z}_p$. Precisamos, então, definir isomorfismo entre corpos.

Definição 1.10. Uma aplicação bijetora $\varphi : R \rightarrow S$ de um corpo R em um corpo S é chamada um **isomorfismo** se, para todos $a, b \in R$, tivermos

$$\varphi(a + b) = \varphi(a) + \varphi(b) \text{ e } \varphi(ab) = \varphi(a)\varphi(b).$$

De certa forma, podemos dizer que um isomorfismo φ de R em S induz uma estrutura de corpo em S , pois, tomando $s_1, s_2 \in S$, encontramos únicos $r_1, r_2 \in R$ tais que $\varphi(r_1) = s_1$ e $\varphi(r_2) = s_2$. Definimos, então $s_1 + s_2$ como sendo $\varphi(r_1 + r_2)$ e $s_1 s_2$ como sendo $\varphi(r_1 r_2)$. Esta estrutura em S é chamada **induzida por** φ e isso nos ajudará a representar melhor os corpos $\mathbb{Z}_p$.

Definição 1.11. Para um primo p , seja $\mathbb{F}_p = \{0, 1, \dots, p-1\}$ o conjunto formado por inteiros e considere a aplicação $\varphi : \mathbb{Z}_p \rightarrow \mathbb{F}_p$ dada por $\varphi(\bar{a}) = a$. Então, $\mathbb{F}_p$ com a estrutura induzida por φ é um corpo finito, chamado **corpo de Galois de ordem p** .

Note que, em $\mathbb{F}_p$, $pb = 0$ para todo $b \in \mathbb{F}_p$ e p é o menor inteiro positivo para o qual isso é válido. De forma geral, todo corpo finito terá essa propriedade para algum inteiro q .

Definição 1.12. Se R for um anel arbitrário e existir um inteiro positivo n tal que $nr = 0$ para todo $r \in R$, então o menor tal inteiro positivo é chamado de **característica** de R e R é dito ter característica (positiva) n , em particular, se $n > 0$ for um número primo (e veremos que isso sempre acontece), dizemos que o corpo tem característica prima. Se tal inteiro positivo n não existir, dizemos que R tem característica 0.

Teorema 1.13. *Um anel $R \neq \{0\}$ de característica positiva, com unidade e sem divisores de zero deve ter característica prima.*

Demonstração. Uma vez que R contém elementos não nulos, R tem característica $n \geq 2$. Se n não fosse primo, poderíamos escrever $n = km$ com $k, m \in \mathbb{Z}$, $1 < k, m < n$. Então, $0 = ne = (km)e = (ke)(ne)$, e isso implica $ke = 0$ ou $me = 0$, já que R não tem divisores de zero. Segue, então que ou $kr = (ke)r = 0$ para todo $r \in R$ ou $mr = (me)r = 0$ para todo $r \in R$, contradizendo a definição da característica n . $\square$

Corolário 1.14. *Todo corpo finito tem característica prima.*

Demonstração. Pelo teorema anterior, é suficiente mostrar que a característica de um corpo finito F é positiva. Considere os múltiplos $e, 2e, 3e, \dots$ da unidade. Uma vez que F contém apenas uma quantidade finita de tais elementos que sejam distintos, existe inteiros k e m com $1 \leq k < m$ tal que $ke = me$ ou, $(m-k)e = 0$, e então F tem característica positiva. $\square$

Um fato interessante sobre corpos de característica 2 é que, como $0 = 2a = a + a$ para todos os elementos a do corpo, $a = -a$ para todo a . Uma propriedade muito útil envolvendo a característica p de um corpo F é a seguinte.

Teorema 1.15. *Seja F um corpo de característica prima p . Então,*

$$(a+b)^{p^n} = a^{p^n} + b^{p^n} \text{ e } (a-b)^{p^n} = a^{p^n} - b^{p^n},$$

para todos $a, b \in F$ e $n \in \mathbb{N}$.

Demonstração. Usamos o fato de que

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

para todo $i \in \mathbb{Z}$ com $0 < i < p$, o que segue do fato de que $\binom{p}{i}$ ser um inteiro e da observação de que o fator p do numerador não poder ser cancelado. Então, pelo Teorema do Binômio de Newton,

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

e usando indução sobre n , completamos a prova da primeira identidade. Pelo que já mostramos, obtemos

$$a^{p^n} = ((a-b) + b)^{p^n} = (a-b)^{p^n} + b^{p^n},$$

e a segunda identidade é válida. □

Com isso, temos definida a principal estrutura com a qual trabalharemos na demonstração do Teorema de Wedderburn: os corpos finitos. Também, provamos que todos eles têm característica prima p . Podemos, agora definir polinômios e corpos de decomposição, que nos serão muito úteis.

1.2 Polinômios

Agora, vale destacar alguns resultados importantes sobre polinômios e seus corpos de decomposição, que serão essenciais para a construção de uma classe especial deles: os polinômios ciclotômicos e para a caracterização dos corpos finitos.

Definição 1.16. Um **polinômio** sobre um anel R é uma expressão da forma

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

em que n é um inteiro não negativo e os **coeficientes** a_i , $0 \leq i \leq n$, são elementos de R . Se f for um polinômio com, pelo menos, um coeficiente não nulo, seja n o maior índice tal que $a_n \neq 0$. Então, a_n é chamado de **coeficiente líder** e a_0 é chamado **termo constante**, enquanto n é chamado **grau** e denotado por $n = \text{gr}(f)$. Polinômios com grau 0 são chamados de **polinômios constantes**. Se o anel R tiver unidade 1 e o coeficiente líder de f for 1, chamaremos f de **polinômio mônico**.

Podemos, ainda, escrever os polinômios numa forma “estendida”, observando que $f(x) = a_0 + a_1x + \cdots + a_nx^n = a_0 + a_1x + \cdots + a_nx^n + 0a_{n+1}x^{n+1} + \cdots$. Assim, definimos a soma e o produto de dois polinômios $f(x) = \sum_{i=0}^n a_i x^i$ e $g(x) = \sum_{j=0}^m x^j$ como sendo

$$f(x) + g(x) = \sum_{k=0}^{\max(i,j)} (a_k + b_k)x^k$$

e

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

Com essas operações, é fácil ver que os polinômios formam um anel, chamado de **anel de polinômios**, e denotado por $R[x]$. O elemento nulo de $R[x]$ é o polinômio $f(x) = 0$, em que 0 é o elemento nulo de R e, se o anel tiver unidade 1, então a unidade de $R[x]$ será $f(x) = 1$.

Assim como no caso dos elementos nulo e identidade, o anel $R[x]$ “herda” certas características de R , por exemplo $R[x]$ é comutativo se, e só se, R for comutativo e $R[x]$ é um domínio de integridade se, e só se, R for um domínio de integridade. No que se segue, usaremos polinômios sobre um corpo F . Com isso, $F[x]$ é um domínio de integridade comutativo e com unidade $f(x) = 1$. Vale a pena destacar um resultado bem conhecido: o algoritmo da divisão.

Teorema 1.17 (Algoritmo da divisão). *Seja $g \neq 0$ um polinômio em $F[x]$. Então, para todo $f \in F[x]$, existem polinômios $q, r \in F[x]$ tais que*

$$f = qg + r, \text{ em que } r = 0 \text{ ou } \text{gr}(r) < \text{gr}(g).$$

Agora que definimos uma forma para dividir polinômios, podemos pensar em divisores e múltiplos e, como no caso dos inteiros, procurar o máximo divisor comum e o mínimo múltiplo comum entre dois polinômios não nulos. Isso é sempre possível, como afirma o próximo teorema (cuja demonstração pode ser obtida generalizando-se os Teoremas 4.4 e 4.11 de [6]).

Teorema 1.18. *Sejam $f_1, \dots, f_m \in F[x]$. Então existe um polinômio mônico unicamente determinado $d = \text{mdc}(f_1, \dots, f_m) \in F[x]$ (que chamaremos **máximo divisor comum entre** $f_1, \dots, f_m$) com as seguintes propriedades: (i) d divide cada f_j , $1 \leq j \leq m$; (ii) qualquer polinômio $c \in F[x]$ que divide todos os f_j , $1 \leq j \leq m$ também divide d . Por fim, existem polinômios $b_1, \dots, b_m \in F[x]$ tais que*

$$d = b_1 f_1 + \cdots + b_m f_m.$$

Além disso, existe um polinômio mônico unicamente determinado $e = \text{mmc}(f_1, \dots, f_m) \in F[x]$ (que chamaremos **mínimo múltiplo comum entre** $f_1, \dots, f_m$) com as seguintes propriedades: (i) e é um múltiplo de cada f_j , $1 \leq j \leq m$; (ii) qualquer polinômio $b \in F[x]$ que seja um múltiplo de todos os f_j , $1 \leq j \leq m$ também é múltiplo de e .

Assim como fomos capazes de “estender” o conceito de mdc e mmc dos números inteiros para os polinômios, podemos pensar em estender o conceito de números primos. Para isso, precisamos da definição de um elemento irredutível pois, em certas estruturas algébricas, elementos irredutíveis nem sempre são elementos primos.

Definição 1.19. Um polinômio $p \in F[x]$ será dito **irredutível sobre F** se p tiver grau positivo e $p = bc$ com $b, c \in F[x]$ implica que b ou c é um polinômio constante. Se $p \in F[x]$ não for irredutível, chamaremos p de **redutível**.

Note que a irredutibilidade de um polinômio depende do corpo sob o qual estamos trabalhando. Por exemplo, $x^2 - 2 \in \mathbb{Q}[x]$ é irredutível, mas $x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2}) \in \mathbb{R}[x]$ é redutível. Os polinômios irredutíveis desempenham um papel importante no estudo dos anéis $F[x]$, uma vez que, nessas estruturas, todo elemento irredutível é primo (isto é, se $p \in F[x]$ for irredutível e p dividir o produto $f_1 \cdots f_m$, então p dividirá pelo menos um dos fatores f_i).

Além disso, vale a fatoração única em $F[x]$, ou seja, todo $f \in F[x]$ pode ser escrito de forma única (a menos de reordenação dos fatores) da forma $f = ap_1^{e_1} \cdots p_m^{e_m}$, em que $a \in F$, $p_1, \dots, p_m$ são polinômios mônicos irredutíveis distintos e $e_1, \dots, e_m$ são inteiros não negativos.

Assim como fizemos para construir os corpos $\mathbb{F}_p$, podemos construir um anel $F[x]/(f)$ a partir de um polinômio f . Usaremos a mesma relação de equivalência que nos fornece as classes de restos na divisão por f e a soma e produto de duas classes será feito de modo similar aos elementos de $\mathbb{F}_p$. Dessa forma, $F[x]/(f)$ será o conjunto formado pela união dessas classes. Como os elementos irredutíveis e primos em $F[x]$ são os mesmos, segue que $F[x]/(f)$ é um corpo se, e somente se, f for irredutível. Além disso, se $F = \mathbb{F}_p$ e $\text{gr}(f) = n \geq 0$, então $F[x]/(f)$ terá p^n elementos.

Em breve, definiremos outro corpo que se relaciona com um polinômio irredutível $f \in F[x]$: o corpo de decomposição de f . Antes disso, porém, precisamos definir o que são as raízes de um polinômio e como elas se relacionam com a redutibilidade de f .

Definição 1.20. Um elemento $b \in F$ é chamado uma **raiz** do polinômio $f \in F[x]$ se $f(b) = 0$.

Teorema 1.21. Um elemento $b \in F$ é uma raiz do polinômio $f \in F[x]$ se, e somente se, $x - b$ dividir f .

Demonstração. Usamos o algoritmo da divisão para expressar $f(x) = q(x)(x - b) + c$, com $q \in F[x]$ e $c \in F$. Substituindo b por x , obtemos $c = f(b)$. Logo, $f(x) = q(x)(x - b) + f(b)$ e o resultado segue dessa identidade. $\square$

Definição 1.22. Seja $b \in F$ uma raiz de um polinômio $f \in F[x]$. Se k for um inteiro positivo tal que $f(x)$ é divisível por $(x - b)^k$, mas não por $(x - b)^{k+1}$, então k é chamado de **multiplicidade** de b . Se $k = 1$, então b é chamado **raiz simples** de f e, se $k \geq 2$, b é chamado de **raiz múltipla** de f .

Teorema 1.23. *Seja $f \in F[x]$ com $\text{gr}(f) = n \geq 0$. Se $b_1, \dots, b_m \in F$ forem raízes distintas de f com multiplicidades $k_1, \dots, k_m$ respectivamente, então $(x - b_1)^{k_1} \cdots (x - b_m)^{k_m}$ divide $f(x)$. Consequentemente, $k_1 + \cdots + k_m \leq n$ e f pode ter no máximo n raízes distintas em F .*

Demonstração. Note que cada polinômio $x - b_j$, $1 \leq j \leq m$, é irredutível sobre F , e então $(x - b_j)^{k_j}$ aparece na fatoração de f . Além disso, o fator $(x - b_1)^{k_1} \cdots (x - b_m)^{k_m}$ aparece na fatoração de f e é, portanto, um divisor de f . Comparando graus, encontramos $k_1 + \cdots + k_m \leq n$ e $m \leq k_1 + \cdots + k_m \leq n$ mostra a última afirmação. $\square$

Definição 1.24. Se $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in F[x]$, então a **derivada** f' de f é definida como sendo $f'(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1} \in F[x]$.

Teorema 1.25. *O elemento $b \in F$ é uma raiz múltipla de $f \in F[x]$ se, e somente se, for uma raiz de f e f' simultaneamente.*

Demonstração. Seja b uma raiz de f , então $f(x)$ pode ser escrito da forma $f(x) = (x - b)q(x)$. Usando técnicas de cálculo, sabemos que $f'(x) = q(x) + (x - b)q'(x)$. Note que $f'(b) = q(b)$, ou seja, b é raiz de f' se, e somente se, b for uma raiz de q , se, e somente se, $q(x) = (x - b)g(x)$ e $f(x) = (x - b)^2g(x)$, se, e somente se, b for uma raiz múltipla de f . $\square$

Agora, podemos estudar extensões de corpos e corpos de decomposição. Essas duas estruturas serão muito utilizadas na demonstração do Teorema de Wedderburn.

1.3 Extensões de corpos

Seja F um corpo. Um subconjunto $K \subset F$ que também é um corpo com as operações de F será chamado de **subcorpo** de F . Nesse contexto, F é chamado uma **extensão** de K . Se $K \neq F$, diremos que K é um **subcorpo próprio** de F .

Se K for um subcorpo do corpo finito $\mathbb{F}_p$, p primo, então K deve conter os elementos 0 e 1, e todos os outros elementos de $\mathbb{F}_p$ uma vez que K é fechado pela adição. Segue que $\mathbb{F}_p$ não tem nenhum subcorpo próprio. Um corpo com tal propriedade é chamado de **corpo primo**.

Pelo argumento acima, qualquer corpo finito de ordem p , com p primo, é um corpo primo. Um outro exemplo de um corpo primo, embora seja infinito, é o corpo dos números

racionais $\mathbb{Q}$. A interseção de todos os subcorpos de F nos fornece o **subcorpo primo** de F , que é obviamente um corpo primo.

Teorema 1.26. *O subcorpo primo de um corpo F é isomorfo a $\mathbb{F}_p$ ou $\mathbb{Q}$, conforme a característica de F é um primo p ou 0.*

Definição 1.27. Seja K um subcorpo de F e M qualquer subconjunto de F . O corpo $K(M)$ é obtido pela interseção de todos os subcorpos de F contendo K e M e é chamado de extensão de K obtida pela **adjunção** dos elementos de M . Para um conjunto $M = \{\theta_1, \dots, \theta_n\}$ finito, escrevemos $K(M) = K(\theta_1, \dots, \theta_n)$. Se M consistir de um único elemento $\theta \in F$, então $L = K(\theta)$ é dito uma **extensão simples** de K e θ é chamado um **elemento definidor** de L sobre K .

Definição 1.28. Sejam K um subcorpo de F e $\theta \in F$. Se θ satisfizer uma equação polinomial não trivial, isto é, se $a_n\theta^n + \dots + a_1\theta + a_0 = 0$ com $a_i \in K$ não todos nulos, então θ é dito **algébrico** sobre K . Uma extensão L de K é dita **extensão algébrica** se todo elemento de L for algébrico sobre K .

Definição 1.29. Seja $\theta \in K$ algébrico e tome todos os polinômios $f \in K[x]$ tais que $f(\theta) = 0$. É possível provar que existe um único polinômio mônico irreduzível $g(x) \in K[x]$ de menor grau tal que $g(\theta) = 0$, que será chamado de **polinômio minimal de θ sobre K** e o **grau** de θ é definido como sendo o grau de $g(x)$.

Uma propriedade interessante do polinômio minimal $g(x)$ de $\theta \in K$ é que, para todo $f \in K[x]$, $f(\theta) = 0$ se, e somente se, g dividir f . Note que o polinômio minimal, bem como o grau de um elemento dependem do corpo sobre o qual estamos trabalhando. Por exemplo, $\sqrt{2}$ tem polinômio minimal $x^2 - 2$ e grau 2 em $\mathbb{Q}[x]$, mas tem polinômio minimal $x - \sqrt{2}$ e grau 1 em $\mathbb{R}[x]$.

Se L for uma extensão de K , então L pode ser visto como um espaço vetorial sobre K . Primeiro, note que os elementos de L formam um grupo abeliano com respeito à adição. Além disso, cada “vetor” $\theta \in L$ pode ser multiplicado por um “escalar” $r \in K$ de forma que $r\theta$ pertença a L (basta usar a multiplicação usual do corpo L), e, com isso, os axiomas de multiplicação por escalar serão satisfeitos.

Definição 1.30. Seja L uma extensão de corpos de K . Se L , visto como espaço vetorial sobre K , for de dimensão finita, dizemos que L é uma **extensão finita** de K . A dimensão do espaço vetorial L sobre K é chamado **grau** de L sobre K e denotado por $[L : K]$.

Apresentaremos a seguir três resultados, eles nos serão bem úteis para provar a unicidade (a menos de isomorfismo) de um tipo especial de extensão de corpos: os corpos de decomposição.

Teorema 1.31. *Se L for uma extensão finita de K e M for uma extensão finita de L , então M é uma extensão finita de K com*

$$[M : K] = [M : L][L : K].$$

Demonstração. Sejam $\{v_1, \dots, v_r\}$ uma base de M sobre L e $\{u_1, \dots, u_s\}$ uma base de L sobre K . Vamos provar que

$$B = \{v_i u_j : i = 1, \dots, r, j = 1, \dots, s\}$$

é uma base de M sobre K . Primeiramente, vejamos que B é LI sobre K . De fato, sejam $a_{ij} \in K$, $1 \leq i \leq r$, $1 \leq j \leq s$ e suponha

$$(a_{11}u_1 + \dots + a_{1s}u_s)v_1 + \dots + (a_{r1}u_1 + \dots + a_{rs}u_s)v_r = 0.$$

Como cada u_i está em L , segue, pela independência linear dos v_j que

$$\begin{aligned} a_{11}u_1 + \dots + a_{1s}u_s &= 0 \\ &\vdots \\ a_{r1}u_1 + \dots + a_{rs}u_s &= 0. \end{aligned}$$

Mas, como os a_{ij} estão em K , segue, pela independência linear dos u_i que $a_{ij} = 0$ para todos $i = 1, \dots, r, j = 1, \dots, s$. Logo, B é LI sobre K .

Resta ver que B gera M a partir de K . De fato, seja $\gamma \in M$. Sendo $\{v_1, \dots, v_r\}$ uma base de M sobre L , existem $b_1, \dots, b_r \in L$ tais que

$$\gamma = b_1 v_1 + \dots + b_r v_r.$$

Como $b_i \in L$, para todo $i = 1, \dots, r$ e $\{u_1, \dots, u_s\}$ é uma base de L sobre K , existem $a_{ij} \in K$, $1 \leq i \leq r, 1 \leq j \leq s$, tais que

$$b_i = a_{i1}u_1 + \dots + a_{is}u_s.$$

Daí, segue que

$$\gamma = \sum_{\substack{1 \leq i \leq r \\ 1 \leq j \leq s}} a_{ij} v_i u_j,$$

e B é um conjunto gerador de M sobre K . □

Teorema 1.32. *Toda extensão finita F de K é algébrica sobre K .*

Demonstração. Seja $n = [F : K]$ e $\alpha \in F$. Note que o conjunto $\{1, \alpha, \alpha^2, \dots, \alpha^n\}$ é linearmente dependente sobre K , isto é, existem constantes não todas nulas $a_0, \dots, a_n \in K$ tais que $a_0 + a_1\alpha + \dots + a_n\alpha^n = 0$. Logo, α é algébrico sobre K . □

Teorema 1.33. *Seja $\theta \in F$ algébrico de grau n sobre K e seja g o seu polinômio minimal sobre K . Então:*

- (i) $K(\theta)$ é isomorfo a $K[x]/(g)$.
- (ii) $[K(\theta) : K] = n$ e $\{1, \theta, \dots, \theta^{n-1}\}$ é uma base de $K(\theta)$ sobre K .
- (iii) Todo $\alpha \in K(\theta)$ é algébrico sobre K e seu grau sobre K é um divisor de n .

Demonstração. (i) Seja $\varphi_\theta : K[x] \rightarrow F$ o homomorfismo dado por $\varphi(f(x)) = f(\theta)$. Por definição de polinômio minimal, vemos que $\text{Ker} \varphi = (g)$. Assim, pelo Teorema do Isomorfismo, vale

$$\frac{K[x]}{(g)} \cong K[\theta] := \{f(\theta) : f \in K[x]\}.$$

Como g é irredutível, temos (g) maximal e $\frac{K[x]}{(g)}$ é um corpo, donde $K[\theta]$ também é um corpo (que contém K e θ). Como $K(\theta)$ é o menor corpo contendo K e θ , segue que $K(\theta) = K[\theta]$.

- (ii) Vimos que $K(\theta) = \{f(\theta) : f(x) \in K[x]\}$. Então, dado $f(\theta) \in K(\theta)$, considere o polinômio $f(x) \in K[x]$ a ele associado. Pelo algoritmo da divisão, temos $f(x) = q(x)g(x) + r(x)$, onde o grau de r é menor que n , sendo, portanto, da forma $a_0 + a_1x + \dots + a_{n-1}x^{n-1}$. Assim, $f(\theta) = r(\theta) = a_0 + a_1\theta + \dots + a_{n-1}\theta^{n-1}$ e temos que $\{1, \theta, \dots, \theta^{n-1}\}$ é uma base de $K(\theta)$ sobre K .
- (iii) Como $K(\theta)$ é uma extensão finita de K , segue que todos os seus elementos, em particular α , são algébricos sobre K . Como $K \subset K(\theta)$ e $\alpha \in K(\theta)$, segue que $K \subset K(\alpha) \subset K(\theta)$. Assim, $n = [K(\theta) : K] = [K(\theta) : K(\alpha)][K(\alpha) : K]$ e $[K(\alpha) : K]$ é um divisor de n .

□

Dessa forma, os elementos de uma extensão algébrica simples $K(\theta)$ sobre K podem ser representados de forma única como um polinômio em θ , ou seja, podem ser escritos de forma única como $a_0 + a_1\theta + \dots + a_{n-1}\theta^{n-1}$ com $a_i \in K$ para $0 \leq i \leq n-1$.

Teorema 1.34. *Seja $f \in K[x]$ irredutível sobre o corpo K . Então existe uma extensão algébrica simples de K com uma raiz de f como elemento definidor.*

Demonstração. Considere o anel de classes residuais $L = K[x]/(f)$, que é um corpo pois f é irredutível. Os elementos de L são as classes residuais denotadas por $[h] = h + (f)$ com $h \in K[x]$. Para todo $a \in K$, podemos formar a classe residual $[a]$ determinada pelo polinômio constante igual a a e, se $a, b \in K$ forem distintos, então $[a] \neq [b]$ uma vez que f tem grau positivo. O mapa $a \mapsto [a]$ nos fornece um isomorfismo de K em um subcorpo

K' de L , de modo que K' pode ser identificado com K . Em outras palavras, podemos ver L como uma extensão de K . Para todo $h(x) = a_0 + a_1x + \cdots + a_mx^m \in K[x]$ temos $[h] = [a_0 + a_1x + \cdots + a_mx^m] = [a_0] + [a_1][x] + \cdots + [a_m][x^m] = a_0 + a_1[x] + \cdots + a_m[x]^m$ pelas regras de operações com classes residuais e a identificação $[a_i] = a_i$. Então, todo elemento de L pode ser escrito como uma expressão polinomial em $[x]$ com coeficientes em K . Uma vez que qualquer corpo contendo K e $[x]$ deve conter essas expressões polinomiais, L é uma extensão simples de K obtida pela adjunção de $[x]$. Se $f(x) = b_0 + b_1x + \cdots + b_nx^n$, então $f([x]) = b_0 + b_1[x] + \cdots + b_n[x]^n = [b_0 + b_1x + \cdots + b_nx^n] = [f] = [0]$, logo $[x]$ é uma raiz de f e L é uma extensão algébrica simples de K . $\square$

Teorema 1.35. *Sejam α e β raízes de $f \in K[x]$ que é irredutível sobre K . Então $K(\alpha)$ e $K(\beta)$ são isomorfos sob um isomorfismo que leva α em β e fixa os elementos de K .*

Agora podemos definir os corpos de decomposição, que são estruturas que contêm todas as raízes de um dado polinômio.

Definição 1.36. Seja $f \in K[x]$ de grau positivo e F uma extensão de K . Dizemos que f se **decompõe** em F se f puder ser escrito como produto de fatores lineares em $F[x]$, isto é, se existirem elementos $\alpha_1, \alpha_2, \dots, \alpha_n \in F$ tais que

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

em que a é o coeficiente líder de f . O corpo F é um **corpo de decomposição** de f sobre K se f se decompuser em F e, além disso, $F = K(\alpha_1, \alpha_2, \dots, \alpha_n)$.

É claro que um corpo de decomposição F de f sobre K é, de certa forma, o menor subcorpo contendo todas as raízes de f (nenhum subcorpo próprio de F que seja uma extensão de K contém todas as raízes de f). Aplicando repetidamente o processo usado no Teorema 1.34, pode-se provar a primeira parte do seguinte resultado. A segunda parte é uma extensão do Teorema 1.35.

Teorema 1.37 (Existência e Unicidade de Corpos de Decomposição). *Se K for um corpo e f for um polinômio de grau positivo em $K[x]$, então existe um corpo de decomposição de f sobre K . Além disso, dois corpos de decomposição de f sobre K são isomorfos segundo o isomorfismo que fixa os elementos de K e mapeia as raízes de f umas nas outras.*

Uma vez que corpos de decomposição podem ser identificados uns com os outros, podemos procurar o corpo de decomposição de f sobre K . Ele pode ser obtido adjuntando uma quantidade finita de elementos algébricos sobre K , e, portanto, pode-se provar, tendo como base os Teoremas 1.31 e 1.33(ii), que o corpo de decomposição de f sobre K é uma extensão finita sobre K .

2 Corpos finitos

O Teorema de Wedderburn relaciona anéis de divisão a corpos finitos, por isso faz-se necessário um estudo aprofundado sobre essa última estrutura. Neste capítulo, estamos interessados em caracterizar todas essas estruturas como corpos de decomposição de um polinômio e obter extensões finitas para um dado corpo. Para isso, partiremos de um corpo finito $\mathbb{F}_q$ e buscaremos raízes de polinômios irredutíveis sobre ele.

Lema 2.1. *Seja F um corpo finito contendo um subcorpo K com q elementos. Então, F contém q^m elementos, em que $m = [F : K]$.*

Demonstração. Sabemos que F é um espaço vetorial sobre K , e uma vez que F é finito, ele é um espaço de dimensão finita sobre K . Se $[F : K] = m$, então F tem uma base sobre K consistindo de m elementos, digamos $b_1, b_2, \dots, b_m$. Logo, cada elemento de F pode ser unicamente representado na forma $a_1b_1 + \dots + a_mb_m$, em que $a_1, \dots, a_m \in K$. Como cada a_i pode assumir q valores, F tem exatamente q^m elementos. $\square$

Teorema 2.2. *Seja F um corpo finito. Então, F tem p^n elementos, em que o primo p é a característica de F e n é o grau de F sobre seu subcorpo primo.*

Demonstração. Uma vez que F é finito, sua característica é um primo p . Assim o subcorpo primo K de F é isomorfo a $\mathbb{F}_p$ e, portanto, contém p elementos. O resultado segue do Lema 2.1. $\square$

Começando dos corpos primos $\mathbb{F}_p$, podemos construir outros corpos finitos pelo processo de adjunção de raízes. Se $f \in \mathbb{F}_p[x]$ for um polinômio irredutível sobre $\mathbb{F}_p$ de grau n , então pela adjunção de uma raiz de f a $\mathbb{F}_p$, obtemos um corpo finito com p^n elementos. Além disso, veremos que existe apenas um corpo (a menos de isomorfismo) com uma dada quantidade de elementos.

Lema 2.3. *Se F_q for um corpo finito com q elementos, então todo $a \in F$ satisfaz $a^q = a$.*

Demonstração. A identidade $a^q = a$ é trivial para $a = 0$. Por outro lado, os elementos não nulos de F formam um grupo multiplicativo de ordem $q - 1$. Então, $a^{q-1} = 1$ para todo $a \in F$ com $a \neq 0$, e multiplicando ambos os lados por a , obtemos o resultado desejado. $\square$

Lema 2.4. *Se $F = F_q$ for um corpo finito com q elementos e K for um subcorpo de F , então o polinômio $x^q - x \in K[x]$ se fatora em $F[x]$ como*

$$x^q - x = \prod_{a \in F} (x - a)$$

e F é um corpo de decomposição de $x^q - x$ sobre K .

Demonstração. O polinômio $x^q - x$ de grau q tem, no máximo q raízes em F . Pelo Lema 2.3, conhecemos q tais raízes (todos os elementos de F). Assim, o polinômio dado se divide em F da maneira indicada, e não pode se dividir em nenhum corpo menor. $\square$

Teorema 2.5 (Existência e unicidade de corpos finitos). *Para todo primo p e todo inteiro positivo n , existe um corpo finito com p^n elementos. Qualquer corpo finito com $q = p^n$ elementos é isomorfo ao corpo de decomposição de $x^q - x$ sobre $\mathbb{F}_p$.*

Demonstração. (Existência) Para $q = p^n$, considere $x^q - x$ em $\mathbb{F}_p[x]$ e seja F seu corpo de decomposição sobre $\mathbb{F}_p$. Esse polinômio tem q raízes distintas em F , uma vez que sua derivada é $qx^{q-1} - 1 = -1 \in \mathbb{F}_p[x]$ e, dessa maneira, não tem nenhuma raiz em comum com $x^q - x$. Seja $S = \{a \in F : a^q - a = 0\}$. Então, S é um subcorpo de F , já que:

- (i) S contém 0 e 1;
- (ii) $a, b \in S$ implica $a - b \in S$ ($(a - b)^q = a^q - b^q = a - b$);
- (iii) $a, b \in S, b \neq 0$ implica $ab^{-1} \in S$ ($(ab^{-1})^q = a^q b^{-q} = ab^{-1}$).

Mas, por outro lado, $x^q - x$ deve se dividir em S , uma vez que S contém todas as suas raízes. Logo, $F = S$ e, uma vez que S tem q elementos, F é um corpo finito com q elementos.

(Unicidade) Seja F um corpo finito com $q = p^n$ elementos. Então F tem característica p pelo Teorema 2.2 e, assim, contém $\mathbb{F}_p$ como subcorpo. Segue do Lema 2.4 que F é um corpo de decomposição de $x^q - x$ sobre $\mathbb{F}_p$. Então, o resultado desejado é uma consequência da unicidade (a menos de isomorfismo) dos corpos de decomposição. $\square$

Podemos concluir que o único (a menos de isomorfismo) corpo finito com $q = p^n$ elementos é o corpo de decomposição de $x^q - x$ sobre $\mathbb{F}_p$. A seguir, veremos quais são todos os subcorpos $\mathbb{F}_r$ de um dado corpo $\mathbb{F}_q$. Não basta que $\mathbb{F}_r$ esteja contido em $\mathbb{F}_q$, precisamos que todos os elementos $x \in \mathbb{F}_r$ satisfaçam a condição $x^q = x$ em $\mathbb{F}_r$. Por exemplo,

$$\mathbb{F}_5 = \{0, 1, 2, 3, 4\} \subset \{0, 1, 2, 3, 4, 5, 6\} = \mathbb{F}_7,$$

mas, em $\mathbb{F}_5$, $2^7 = 3$, mostrando que $\mathbb{F}_5$ não é subcorpo de $\mathbb{F}_7$.

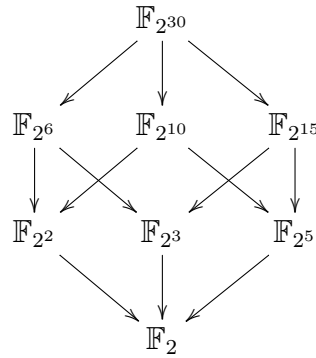
Teorema 2.6 (Critério para subcorpos). *Seja $\mathbb{F}_q$ um corpo finito com $q = p^n$ elementos. Então todo subcorpo de $\mathbb{F}_q$ tem p^m elementos, em que m é um divisor positivo de n . Inversamente, se m for um divisor positivo de n , então existe exatamente um subcorpo de $\mathbb{F}_q$ com p^m elementos.*

Demonstração. É fácil ver que um subcorpo K de $\mathbb{F}_q$ tem ordem p^m para algum inteiro positivo $m \leq n$. O Lema 2.1 mostra que $q = p^n$ deve ser uma potência de p^m , logo m é, necessariamente, um divisor de n .

Inversamente, se m for um divisor positivo de n , então $p^m - 1$ divide $p^n - 1$, e assim $x^{p^m} - 1$ divide $x^{p^n} - 1$ em $\mathbb{F}_p[x]$. Consequentemente, $x^{p^m} - x$ divide $x^{p^n} - x = x^q - x$ em $\mathbb{F}_p[x]$. Logo, toda raiz de $x^{p^m} - x$ é uma raiz de $x^q - x$ e, portanto, pertence a $\mathbb{F}_q$. Segue que $\mathbb{F}_q$ deve conter como subcorpo um corpo de decomposição de $x^{p^m} - x$ sobre $\mathbb{F}_p$, e como vimos na prova do Teorema 2.5, tal corpo de decomposição tem ordem p^m . Se existissem dois tais subcorpos de ordem p^m em $\mathbb{F}_q$, eles conteriam, juntos, mais que p^m raízes de $x^{p^m} - x$ em $\mathbb{F}_q$, uma contradição óbvia. $\square$

A prova do Teorema 2.6 mostra que o único subcorpo de $\mathbb{F}_{p^n}$ de ordem p^m , em que m é um divisor positivo de n , consiste precisamente das raízes do polinômio $x^{p^m} - x \in \mathbb{F}_p[x]$ em $\mathbb{F}_{p^n}$.

Exemplo 2.7. Os subcorpos do corpo finito $\mathbb{F}_{2^{30}}$ podem ser determinados listando todos os divisores positivos de 30. As relações de contingência entre esses vários subcorpos estão dispostas no seguinte diagrama.



Pelo Teorema 2.6, as relações de contingência são equivalentes às relações de divisibilidade entre os divisores positivos de 30.

Para um corpo finito $\mathbb{F}_q$, denotamos por $\mathbb{F}_q^*$ o grupo multiplicativo dos elementos não nulos de $\mathbb{F}_q$. Uma propriedade muito importante de tal grupo é a seguinte:

Teorema 2.8. *Para todo corpo finito $\mathbb{F}_q$, o grupo multiplicativo $\mathbb{F}_q^*$ é cíclico.*

Demonstração. Podemos assumir $q > 3$. Seja $h = p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}$ a decomposição em fatores primos da ordem $h = q - 1$ do grupo $\mathbb{F}_q^*$. Para cada $i, 1 \leq i \leq m$, o polinômio $x^{\frac{h}{p_i}} - 1$ tem, no máximo, $\frac{h}{p_i}$ raízes em $\mathbb{F}_q$. Uma vez que $\frac{h}{p_i} < h$, segue que existem elementos não nulos em $\mathbb{F}_q$ que não são raízes desse polinômio. Seja a_i um tal elemento e defina $b_i = a_i^{\frac{h}{p_i^{r_i}}}$. Então $b_i^{p_i^{r_i}} = 1$, logo a ordem de b_i é um divisor de $p_i^{r_i}$ e é, com isso, da forma $p_i^{s_i}$ com $0 \leq s_i \leq r_i$. Por outro lado,

$$b_i^{p_i^{r_i}-1} = a_i^{\frac{h}{p_i}} \neq 1,$$

e, assim, a ordem de b_i é $p_i^{r_i}$. Afirmamos que o elemento $b = b_1 b_2 \cdots b_m$ tem ordem h . Suponha, do contrário, que a ordem de b é um divisor próprio de h e é, portanto, um divisor de, no mínimo, um dos m inteiros $\frac{h}{p_i}, 1 \leq i \leq m$, digamos de $\frac{h}{p_1}$. Então, temos

$$1 = b^{\frac{h}{p_1}} = b_1^{\frac{h}{p_1}} b_2^{\frac{h}{p_1}} \cdots b_m^{\frac{h}{p_1}}.$$

Agora, se $2 \leq i \leq m$, então $p_i^{r_i}$ divide $\frac{h}{p_1}$, e, assim, $b_1^{\frac{h}{p_1}} = 1$. Isso implica que a ordem de b_1 deve dividir $\frac{h}{p_1}$, o que é impossível, já que a ordem de b_1 é $p_1^{r_1}$. Logo, $\mathbb{F}_q^*$ é um grupo cíclico com gerador b . $\square$

Definição 2.9. Um gerador para o grupo cíclico $\mathbb{F}_q^*$ é chamado um **elemento primitivo** de $\mathbb{F}_q$.

Teorema 2.10. *Seja $\mathbb{F}_q$ um corpo finito e $\mathbb{F}_r$ um corpo finitamente estendido. Então $\mathbb{F}_r$ é uma extensão algébrica simples de $\mathbb{F}_q$ e todo elemento primitivo de $\mathbb{F}_r$ pode servir como um elemento definidor de $\mathbb{F}_r$ sobre $\mathbb{F}_q$.*

Demonstração. Seja ζ um elemento primitivo de $\mathbb{F}_r$. Temos, claramente, $\mathbb{F}_q(\zeta) \subset \mathbb{F}_r$. Por outro lado, $\mathbb{F}_q(\zeta)$ contém 0 e todas as potências de ζ , e, então, todos os elementos de $\mathbb{F}_r$. Logo, $\mathbb{F}_q(\zeta) = \mathbb{F}_r$. $\square$

Corolário 2.11. *Para todo corpo finito $\mathbb{F}_q$ e todo inteiro positivo n , existe um polinômio irredutível em $\mathbb{F}_q[x]$ de grau n .*

Demonstração. Seja $\mathbb{F}_r$ o corpo estendido de $\mathbb{F}_q$ de ordem q^n , então $[\mathbb{F}_r : \mathbb{F}_q] = n$. Pelo Teorema 2.10, temos $\mathbb{F}_r = \mathbb{F}_q(\zeta)$ para algum $\zeta \in \mathbb{F}_r$. Então, o polinômio minimal de ζ sobre $\mathbb{F}_q$ é um polinômio irredutível em $\mathbb{F}_q[x]$ de grau n . $\square$

O resultado anterior nos garante que sempre existe pelo menos um polinômio irredutível em $\mathbb{F}_q[x]$ de grau fixado n , a título de curiosidade apresentaremos uma fórmula para o número exato de tais polinômios. Para isso, precisaremos de alguns resultados, cujas demonstrações são encontradas no Corolário 3.21 e Teorema 3.24 de [1].

Lema 2.12. *Se $N_q(d)$ for o número de polinômios mônicos irredutíveis de grau d sobre $\mathbb{F}_q[x]$, então*

$$q^n = \sum_{d|n} d N_q(d) \text{ para todo } n \in \mathbb{N},$$

em que a soma é estendida sobre todos os divisores positivos d de n .

Para obtermos a fórmula desejada, precisamos definir a função de Moebius e a fórmula da inversão de Moebius.

Definição 2.13. A função de Moebius μ é a função em $\mathbb{N}$ definida por

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

Lema 2.14 (Fórmula da Inversão de Moebius). *Sejam h e H duas funções de $\mathbb{N}$ em um grupo aditivo abeliano G . Então,*

$$H(n) = \sum_{d|n} h(d), \text{ para todo } n \in \mathbb{N} \quad (2.1)$$

se, e somente se,

$$h(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) H(d) = \sum_{d|n} \mu(d) H\left(\frac{n}{d}\right), \text{ para todo } n \in \mathbb{N}. \quad (2.2)$$

Com base nesses resultados, podemos provar o seguinte:

Teorema 2.15. *O número $N_q(n)$ de polinômios mônicos irredutíveis em $\mathbb{F}_q[x]$ de grau n é dado por*

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

Demonstração. Aplicamos o caso aditivo da fórmula de inversão de Moebius ao grupo $G = \mathbb{Z}$. Seja $h(n) = nN_q(n)$ e $H(n) = q^n$, para todo $n \in \mathbb{N}$. Então, (2.1) é satisfeita por causa da identidade apresentada no Lema 2.12, e então (2.2) nos dá a fórmula desejada. $\square$

Observação 2.16. Essa fórmula reforça o fato de que para todo corpo finito $\mathbb{F}_q$ e todo $d \in \mathbb{N}$, existe um polinômio irredutível em $\mathbb{F}_q[x]$ de grau n . De fato, usando $\mu(1) = 1$ e $\mu(d) \geq -1$ para todo $d \in \mathbb{N}$, uma estimativa bruta fornece

$$N_q(n) \geq \frac{1}{n}(q^n - q^{n-1} - q^{n-2} - \dots - q) = \frac{1}{n} \left(q^n - \frac{q^n - q}{q - 1} \right) > 0.$$

Exemplo 2.17. Na tabela a seguir, apresentamos o número de polinômios mônicos irredutíveis sobre $\mathbb{F}_7[x]$ de alguns graus fixados:

n	$N_7(n)$
1	7
2	21
3	112
4	558
5	3.360
10	28.245.840
20	3.989.613.300.756.720

Note como o número de polinômios mônicos irredutíveis aumenta rapidamente com o aumento de n , embora encontrar um tal polinômio “ao acaso” se torne uma questão cada vez mais complicada. Usando a fórmula acima, pode-se estimar que $N_q(n) \rightarrow \frac{q^n}{n}$ quando $n \rightarrow \infty$ e, como o número de polinômios mônicos de grau n em $\mathbb{F}_q[x]$ é q^n , a probabilidade de um polinômio aleatório ser irredutível é $\frac{1}{n}$.

Com os resultados apresentados nesse capítulo, podemos enxergar um corpo finito $\mathbb{F}_q$ de característica p como o corpo de decomposição de $x^q - x$ sobre $\mathbb{F}_p = \mathbb{Z}_p$, temos um critério para subcorpos e sabemos encontrar extensões de corpos de qualquer grau. Essas relações de contingência entre corpos serão fundamentais para uma das demonstrações do Teorema de Wedderburn.

3 Raízes de polinômios irredutíveis e polinômios ciclotômicos

Nesse capítulo, entenderemos melhor como as raízes de polinômios irredutíveis nos fornecem informações sobre os corpos finitos. Além disso, estudaremos uma classe muito importante de polinômios: os ciclotômicos. Embora não seja necessário para a demonstração do Teorema de Wedderburn, o Apêndice A nos mostra de uma forma mais detalhada como todos os elementos de um corpo finito se relacionam aos tópicos estudados nesse capítulo.

3.1 Raízes de polinômios irredutíveis

Lema 3.1. *Seja $f \in \mathbb{F}_q[x]$ um polinômio irredutível sobre um corpo finito $\mathbb{F}_q$ e seja α uma raiz de f em uma extensão de corpos de $\mathbb{F}_q$. Então, para um polinômio $h \in \mathbb{F}_q[x]$, temos $h(\alpha) = 0$ se, e só se, f dividir h .*

Demonstração. Basta usar o algoritmo da divisão em $\mathbb{F}_q$. A partir dele, obtemos

$$h(x) = q(x)f(x) + r(x).$$

Utilizando $x = \alpha$ nessa expressão, encontramos $h(\alpha) = r(\alpha)$ e o resultado segue. $\square$

Lema 3.2. *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 só se, m dividir n .*

Demonstração. Suponha que $f(x)$ divida $x^{q^n} - x$. Seja α uma raiz de f no corpo de decomposição de f sobre $\mathbb{F}_q$. Então $\alpha^{q^n} = \alpha$, logo $\alpha \in \mathbb{F}_{q^n}$. Segue que $\mathbb{F}_q(\alpha)$ é um subcorpo de $\mathbb{F}_{q^n}$. Mas, uma vez que $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$ e $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$, sabemos que m divide n pelo Teorema 1.31.

Inversamente, se m dividir n , o Teorema 2.6 implica que $\mathbb{F}_{q^n}$ contém $\mathbb{F}_{q^m}$ como subcorpo. Se α for uma raiz de f no corpo de decomposição de f sobre $\mathbb{F}_q$, então $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$, e, então, $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$. Consequentemente, temos $\alpha \in \mathbb{F}_{q^n}$, logo $\alpha^{q^n} = \alpha$, e, portanto, α é uma raiz de $x^{q^n} - x \in \mathbb{F}_q[x]$. Nós inferimos então pelo Lema 3.1 que $f(x)$ divide $x^{q^n} - x$. $\square$

Teorema 3.3. *Se f for um polinômio irredutível em $\mathbb{F}_q[x]$ de grau m , então f tem uma raiz α em $\mathbb{F}_{q^m}$. Além disso, todas as raízes de f são simples e são dadas pelos m distintos elementos $\alpha, \alpha^q, \alpha^{q^2}, \dots, \alpha^{q^{m-1}}$ de $\mathbb{F}_{q^m}$.*

Demonstração. Seja α uma raiz de f no corpo de decomposição de f sobre $\mathbb{F}_q$. Então $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$, logo $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$, e, em particular, $\alpha \in \mathbb{F}_{q^m}$. Em seguida, mostraremos que se $\beta \in \mathbb{F}_{q^m}$ for uma raiz de f , então β^q é também uma raiz de f . Escreva $f(x) = a_0 + a_1x + \cdots + a_mx^m$, com $a_i \in \mathbb{F}_q$. Logo, usando o Lema 2.3, temos

$$\begin{aligned} f(\beta^q) &= a_0 + a_1\beta^q + \cdots + a_m\beta^{qm} = a_0^q + a_1^q\beta^q + \cdots + a_m^q\beta^{qm} \\ &= (a_0 + a_1\beta + \cdots + a_m\beta^m)^q = f(\beta)^q = 0. \end{aligned}$$

Portanto, os elementos $\alpha, \alpha^q, \alpha^{q^2}, \dots, \alpha^{q^{m-1}}$ são raízes de f . Resta provar que esses elementos são distintos. Suponha, ao contrário, que $\alpha^{q^j} = \alpha^{q^k}$, para inteiros j e k com $0 \leq j < k \leq m-1$. Elevando essa identidade à potência q^{k-j} , obtemos

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

Segue, então, do Lema 3.1, que $f(x)$ divide $x^{q^{m-k+j}} - x$. Pelo Lema 3.2, isso só é possível se m dividir $m - k + j < m$, e então chegamos em uma contradição. $\square$

Corolário 3.4. *Seja f um polinômio irredutível em $\mathbb{F}_q[x]$ de grau m . Então o corpo de decomposição de f sobre $\mathbb{F}_q$ é dado por $\mathbb{F}_{q^m}$.*

Demonstração. Usando o Teorema 3.3, vemos facilmente que f se decompõe em $\mathbb{F}_{q^m}$. Além disso, $\mathbb{F}_q(\alpha, \alpha^q, \dots, \alpha^{q^{m-1}}) = \mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$ para uma raiz α em $\mathbb{F}_{q^m}$, em que a segunda identidade é tirada da prova do Teorema 3.3. $\square$

Corolário 3.5. *Quaisquer dois polinômios irredutíveis em $\mathbb{F}_q[x]$ de mesmo grau têm corpos de decomposição isomorfos.*

Assim, vimos que o corpo de decomposição de um polinômio irredutível pode ser obtido quando sabemos uma de suas raízes. Além disso, nós conseguimos mostrar que, se soubermos uma raiz α de um polinômio irredutível de grau m , saberemos todas as outras raízes (que são exatamente as potências $\alpha^q, \alpha^{q^2}, \dots, \alpha^{q^{m-1}}$). Essas potências recebem uma nomenclatura especial.

Definição 3.6. Seja $\mathbb{F}_{q^m}$ uma extensão de $\mathbb{F}_q$ e seja $\alpha \in \mathbb{F}_{q^m}$. Então os elementos $\alpha, \alpha^q, \alpha^{q^2}, \dots, \alpha^{q^{m-1}}$ são chamados **conjugados** de α com respeito a $\mathbb{F}_q$.

Os conjugados de $\alpha \in \mathbb{F}_{q^m}$ com respeito a $\mathbb{F}_q$ são distintos se, e só se, o polinômio minimal de α sobre $\mathbb{F}_q$ tiver grau m . De forma inversa, o grau d do polinômio minimal será um divisor próprio de m , e, assim, os conjugados de α com respeito a $\mathbb{F}_q$ serão os elementos distintos $\alpha, \alpha^q, \dots, \alpha^{d-1}$, cada um repetido $\frac{m}{d}$ vezes.

Teorema 3.7. *Os conjugados de $\alpha \in \mathbb{F}_{q^m}^*$ com respeito a qualquer subcorpo de $\mathbb{F}_q$ têm a mesma ordem no grupo $\mathbb{F}_q^*$.*

Demonstração. Seja $\mathbb{F}_d$ um subcorpo de $\mathbb{F}_q$ e a a ordem de α no grupo $\mathbb{F}_q^*$. Sabemos que d é uma potência da característica de $\mathbb{F}_q$ e, portanto, é coprimo com a ordem $q - 1$ de $\mathbb{F}_q^*$. Um outro resultado bem conhecido da teoria de grupos é que a ordem de α^d em $\mathbb{F}_q^*$ é igual a $\frac{a}{\text{mdc}(d, q-1)} = a$. Logo, a ordem de α^d em $\mathbb{F}_q^*$ é igual à ordem de α nesse grupo. Analogamente, prova-se para os outros conjugados e temos o resultado desejado. $\square$

Corolário 3.8. *Se α for um elemento primitivo de $\mathbb{F}_{q^m}$, então todos os seus conjugados com respeito a qualquer subcorpo de $\mathbb{F}_q$ também o são.*

Exemplo 3.9. Seja $\alpha \in \mathbb{F}_{16}$ uma raiz de $f(x) = x^4 + x + 1 \in \mathbb{F}_2[x]$. Então os conjugados de α com respeito a $\mathbb{F}_2$ são $\alpha, \alpha^2, \alpha^4 = \alpha + 1$ e $\alpha^8 = \alpha^2 + 1$, cada um deles é um elemento primitivo de $\mathbb{F}_{16}$. Os conjugados de α com respeito a $\mathbb{F}_4$ são α e $\alpha^4 = \alpha + 1$.

Existe uma relação íntima entre elementos conjugados e certos automorfismos de um corpo finito. Seja $\mathbb{F}_{q^m}$ uma extensão de $\mathbb{F}_q$. Um automorfismo de $\mathbb{F}_{q^m}$ que fixa os elementos de $\mathbb{F}_q$ será chamado de automorfismo de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$. Portanto, em detalhes, nós exigimos que σ seja um mapa injetor de $\mathbb{F}_{q^m}$ nele mesmo com $\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta)$ e $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$ para todos $\alpha, \beta \in \mathbb{F}_{q^m}$ e $\sigma(a) = a$ para todo $a \in \mathbb{F}_q$.

Teorema 3.10. *Os distintos automorfismos de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$ são exatamente os mapas $\sigma_0, \sigma_1, \dots, \sigma_{m-1}$ definidas por $\sigma_j(\alpha) = \alpha^{q^j}$ para $\alpha \in \mathbb{F}_{q^m}$ e $0 \leq j \leq m - 1$.*

Demonstração. Para cada σ_j e todos $\alpha, \beta \in \mathbb{F}_{q^m}$ é simples notar que temos $\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta)$ e $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$, de forma que σ_j é um endomorfismo de $\mathbb{F}_{q^m}$. Além disso, $\sigma_j(\alpha) = 0$ se, e só se, $\alpha = 0$, logo σ_j é injetor. Uma vez que $\mathbb{F}_{q^m}$ é um conjunto finito, σ_j é sobrejetor e, portanto, um automorfismo de $\mathbb{F}_{q^m}$. Além disso, temos $\sigma_j(a) = a$ para todo $a \in \mathbb{F}_q$ pelo Lema 2.3, e, então, cada σ_j é um automorfismo de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$. Os mapas $\sigma_0, \sigma_1, \dots, \sigma_{m-1}$ são distintos, uma vez que atribuem valores distintos aos elementos primitivos de $\mathbb{F}_{q^m}$.

Agora, suponha que σ é um automorfismo arbitrário de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$. Seja β um elemento primitivo de $\mathbb{F}_{q^m}$ e seja $f(x) = x^m + a_{m-1}x^{m-1} + \dots + a_0 \in \mathbb{F}_q[x]$ seu polinômio minimal sobre $\mathbb{F}_q$. Então

$$0 = \sigma(\beta^m + a_{m-1}\beta^{m-1} + \dots + a_0) = \sigma(\beta)^m + a_{m-1}\sigma(\beta)^{m-1} + \dots + a_0,$$

de forma que $\sigma(\beta)$ é uma raiz de f em $\mathbb{F}_{q^m}$. Segue do Teorema 3.3 que $\sigma(\beta) = \beta^{q^j}$ para algum $0 \leq j \leq m - 1$. Uma vez que σ é um homomorfismo, $\sigma(\alpha) = \alpha^{q^j}$ para todo $\alpha \in \mathbb{F}_{q^m}$. $\square$

Assim, finalizamos essa seção ressaltando a importância de se conhecer as raízes de polinômios irredutíveis: a partir de uma dessas raízes, pode-se obter todas as outras tomando seus conjugados e o corpo de decomposição desse polinômio pode ser obtido adjuntando-se ao corpo base uma raiz encontrada.

3.2 Polinômios ciclotômicos

Vimos que as raízes de um polinômio são muito importantes para o estudo da teoria de corpos finitos. Nessa seção, vamos “fabricar” uma classe especial de polinômios escolhendo raízes para eles que satisfaçam a uma condição simples, porém muito importante para a demonstração do Teorema de Wedderburn.

Definição 3.11. Seja n um inteiro positivo. O corpo de decomposição de $x^n - 1$ sobre um corpo K é chamado o **n -ésimo corpo ciclotômico** sobre K e denotado por $K^{(n)}$. As raízes de $x^n - 1$ em $K^{(n)}$ são chamadas as **n -ésimas raízes da unidade** sobre K e o conjunto dessas raízes é denotado por $E^{(n)}$.

Para nossos objetivos, o caso mais importante é aquele sobre um corpo finito K . As propriedades básicas de raízes da unidade podem, no entanto, serem estabelecidas sem essa restrição. A estrutura de $E^{(n)}$ é determinada pela relação entre n e a característica de K . Quando nos referimos à característica p de K , permitimos o caso $p = 0$ também.

Teorema 3.12. *Seja n um inteiro positivo e K um corpo de característica p . Então:*

- (i) *Se p não dividir n , então $E^{(n)}$ é um grupo cíclico de ordem n com respeito à multiplicação em $K^{(n)}$.*
- (ii) *Se p dividir n , escrevendo $n = mp^a$ com inteiros positivos m e a e m não divisível por p , 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 um com multiplicidade p^a .*

Demonstração. (i) O caso $n = 1$ é trivial. Para $n \geq 2$, $x^n - 1$ e sua derivada nx^{n-1} não têm raízes comuns, pois nx^{n-1} só tem a raiz 0 em $K^{(n)}$. Assim, $x^n - 1$ não pode ter raízes múltiplas, e então $E^{(n)}$ tem n elementos. Agora, se $\zeta, \eta \in E^{(n)}$, então $(\zeta\eta^{-1})^n = \zeta^n(\eta^n)^{-1} = 1$, então $\zeta\eta^{-1} \in E^{(n)}$. Segue que $E^{(n)}$ é um grupo multiplicativo. Seja $n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$ a decomposição em fatores primos de n . Então pode-se mostrar por um argumento semelhante ao usado na prova do Teorema 2.8 que, para cada i , $1 \leq i \leq t$, existe um elemento $\alpha_i \in E^{(n)}$ o qual não é raiz do polinômio $x^{\frac{n}{p_i}} - 1$, que $\beta_i = \alpha_i^{\frac{n}{p_i}}$ tem ordem $p_i^{e_i}$ e que $E^{(n)}$ é um grupo cíclico com gerador $\beta = \beta_1 \beta_2 \cdots \beta_t$.

(ii) Segue imediatamente de $x^n - 1 = x^{mp^a} - 1 = (x^m - 1)^{p^a}$ e da parte (i). $\square$

Definição 3.13. Sejam K um corpo de característica p e n um inteiro positivo não divisível por p . Então um gerador do grupo cíclico $E^{(n)}$ é chamado uma **n -ésima raiz primitiva da unidade** sobre K .

Sabemos que, sob as condições da Definição 3.13, existem exatamente $\phi(n)$ n -ésimas raízes primitivas da unidade diferentes sobre K . Se ζ for uma delas, então todas as n -ésimas

raízes primitivas da unidade sobre K são dadas por ζ^s , em que $1 \leq s \leq n$ e $\text{mdc}(s, n) = 1$. O polinômio cujas raízes são precisamente as n -ésimas raízes primitivas da unidade sobre K é de grande interesse.

Definição 3.14. Sejam K um corpo de característica p , n um inteiro positivo não divisível por p e ζ uma n -ésima raiz primitiva da unidade sobre K . Então o polinômio

$$Q_n(x) = \prod_{\substack{s=1 \\ \text{mdc}(s, n)=1}}^n (x - \zeta^s)$$

é chamado o **n -ésimo polinômio ciclotômico** sobre K .

Note que, para todo $n \in \mathbb{N}$, o n -ésimo polinômio ciclotômico $Q_n(x)$ sobre K divide $x^n - 1$ em $K[x]$, já que todas as raízes de $Q_n(x)$ são também raízes de $x^n - 1$. O polinômio $Q_n(x)$ é claramente independente da escolha de ζ . O grau de $Q_n(x)$ é $\phi(n)$ e seus coeficientes obviamente pertencem a $K^{(n)}$. Um simples argumento mostrará que eles, na verdade, estão contidos no subcorpo primo de K . Usamos o símbolo $\prod_{d|n}$ para denotar um produto estendido a todos os divisores positivos d de um inteiro positivo n .

Teorema 3.15. *Seja K um corpo de característica p e n um inteiro positivo não divisível por p , Então:*

- (i) $x^n - 1 = \prod_{d|n} Q_d(x)$;
- (ii) *os coeficientes de $Q_n(x)$ pertencem ao subcorpo primo de K , ou a $\mathbb{Z}$ se o subcorpo primo de K for $\mathbb{Q}$.*

Demonstração. (i) Cada raiz n -ésima da unidade é uma raiz d -ésima primitiva da unidade sobre K para exatamente um divisor positivo d de n . Em detalhes, se ζ for uma raiz n -ésima primitiva da unidade sobre K e ζ^s é uma n -ésima raiz arbitrária da unidade sobre K , então $d = \frac{n}{\text{mdc}(s, n)}$, isto é, d é a ordem de ζ^s em $E^{(n)}$. Uma vez que

$$x^n - 1 = \prod_{s=1}^n (x - \zeta^s),$$

a fórmula em (i) é obtida agrupando-se os fatores $(x - \zeta^s)$ para os quais ζ^s é uma raiz d -ésima primitiva da unidade sobre K .

(ii) Isto é provado por indução sobre n . Note que $Q_n(x)$ é um polinômio mônico. Para $n = 1$, temos $Q_1(x) = x - 1$, e a afirmação é obviamente válida. Agora, seja $n > 1$ e suponha que a proposição é válida para todos $1 \leq d < n$. Então, temos, por (i), $Q_n(x) = \frac{x^n - 1}{f(x)}$, em que $f(x) = \prod_{d|n, d < n} Q_d(x)$. A hipótese de indução implica que $f(x)$ é um polinômio com coeficientes no subcorpo primo de K ou em $\mathbb{Z}$ no caso da característica de K ser 0. Usando o algoritmo da divisão com $x^n - 1$ e o polinômio mônico $f(x)$, vemos que os coeficientes de $Q_n(x)$ pertencem ao subcorpo primo de K ou a $\mathbb{Z}$, respectivamente. $\square$

Exemplo 3.16. Seja r um primo e $k \in \mathbb{N}$. Então

$$Q_{r^k}(x) = 1 + x^{r^{k-1}} + x^{2r^{k-1}} + \cdots + x^{(r-1)r^{k-1}},$$

uma vez que

$$Q_{r^k}(x) = \frac{x^{r^k} - 1}{Q_1(x)Q_r(x) \cdots Q_{r^{k-1}}(x)} = \frac{x^{r^k} - 1}{x^{r^{k-1}} - 1}$$

pelo Teorema 3.15 (i). Para $k = 1$, temos simplesmente $Q_r(x) = 1 + x + x^2 + \cdots + x^{r-1}$.

Teorema 3.17. *O corpo ciclotômico $K^{(n)}$ é uma extensão algébrica simples de K . Além disso,*

- (i) *Se $K = \mathbb{Q}$, então o polinômio ciclotômico Q_n é irredutível sobre K e $[K^{(n)} : K] = \phi(n)$.*
- (ii) *Se $K = \mathbb{F}_q$ com $\text{mdc}(q, n) = 1$, então Q_n se fatora em $\frac{\phi(n)}{d}$ polinômios irredutíveis mônicos distintos em $K[x]$ de mesmo grau d , $K^{(n)}$ é o corpo de decomposição de algum tal fator irredutível sobre K , e $[K^{(n)} : K] = d$, em que d é o menor inteiro positivo tal que $q^d \equiv 1 \pmod{n}$.*

Demonstração. Se existisse uma raiz n -ésima primitiva da unidade ζ sobre K , é claro que $K^{(n)} = K(\zeta)$. Caso contrário, teríamos a situação descrita no Teorema 3.12 (ii); então $K^{(n)} = K^{(m)}$ e o resultado segue novamente. Para o restante da afirmação, provaremos apenas (ii), que é o caso importante para nossos objetivos. Seja η uma raiz primitiva n -ésima da unidade sobre $\mathbb{F}_q$. Então $\eta \in \mathbb{F}_{q^k}$ se, e somente se, $\eta^{q^k} = \eta$, e a última igualdade é equivalente a $q^k \equiv 1 \pmod{n}$. O menor inteiro positivo para o qual isso é válido é $k = d$, e então η pertence a $\mathbb{F}_{q^d}$, mas em nenhum de seus subcorpos próprios. Logo, o polinômio minimal de η sobre $\mathbb{F}_q$ tem grau d , e uma vez que η é uma raiz arbitrária de Q_n , o resultado desejado segue. $\square$

Corolário 3.18. *O N -ésimo polinômio ciclotômico $Q_n(x)$ sobre $\mathbb{F}_q[x]$, em que a característica p do corpo e n são relativamente primos, é irredutível se, e somente se, o menor inteiro d tal que $q^d \equiv 1 \pmod{n}$ for $\phi(n)$.*

Teorema 3.19. *O corpo finito $\mathbb{F}_q$ é o $(q-1)$ -ésimo corpo ciclotômico sobre qualquer um de seus subcorpos.*

Demonstração. O polinômio $x^{q-1} - 1$ se fatora em $\mathbb{F}_q$, uma vez que suas raízes são exatamente os elementos não nulos de $\mathbb{F}_q$. Obviamente, o polinômio não se fatora em nenhum subcorpo próprio de $\mathbb{F}_q$, de forma que $\mathbb{F}_q$ é o corpo de decomposição de $x^{q-1} - 1$ sobre qualquer um de seus subcorpos. $\square$

Uma vez que $\mathbb{F}_q^*$ é um grupo cíclico de ordem $q - 1$ pelo Teorema 2.8, existe, para qualquer divisor positivo n de $q - 1$, um subgrupo cíclico $\{1, \alpha, \dots, \alpha^{n-1}\}$ de $\mathbb{F}_q^*$ de ordem n . Todos os elementos desse subgrupo são raízes n -ésimas da unidade sobre qualquer subcorpo de $\mathbb{F}_q$ e o elemento gerador α é uma raiz n -ésima primitiva da unidade sobre qualquer subcorpo de $\mathbb{F}_q$.

Lema 3.20. *Se d for um divisor do inteiro positivo n com $1 \leq d < n$, então $Q_n(x)$ divide $\frac{x^n - 1}{x^d - 1}$, quando $Q_n(x)$ está definido.*

Demonstração. Do Teorema 3.15 (i), sabemos que $Q_n(x)$ divide $x^n - 1 = (x^d - 1) \cdot \frac{x^n - 1}{x^d - 1}$. Uma vez que d é um divisor próprio de n , os polinômios $Q_n(x)$ e $x^d - 1$ não têm raízes comuns, donde $\text{mdc}(Q_n(x), x^d - 1) = 1$ e a proposição é verdadeira. $\square$

De uma maneira bem resumida, podemos enxergar as n -ésimas raízes primitivas da unidade sobre $\mathbb{F}_q$ como sendo os elementos de ordem n em $\mathbb{F}_{q^n}$ e o n -ésimo polinômio ciclotômico como sendo o polinômio que tem exatamente essas raízes. Esses polinômios serão bem úteis para uma das demonstrações do Teorema de Wedderburn.

Agora, podemos apresentar uma forma explícita para o n -ésimo polinômio ciclotômico usando a versão multiplicativa da fórmula da inversão de Moebius.

Lema 3.21 (Fórmula da Inversão de Moebius). *Sejam h e H duas funções de $\mathbb{N}$ em um grupo multiplicativo abeliano G . Então,*

$$H(n) = \prod_{d|n} h(d), \text{ para todo } n \in \mathbb{N} \quad (3.1)$$

se, e somente se,

$$h(n) = \prod_{d|n} H(d)^{\mu(\frac{n}{d})} = \prod_{d|n} H\left(\frac{n}{d}\right)^{\mu(d)}, \text{ para todo } n \in \mathbb{N}. \quad (3.2)$$

Teorema 3.22. *Para um corpo finito K de característica p e $n \in \mathbb{N}$ não divisível por p , o n -ésimo polinômio ciclotômico Q_n sobre K satisfaz*

$$Q_n(x) = \prod_{d|n} (x^d - 1)^{\mu(\frac{n}{d})} = \prod_{d|n} (x^{\frac{n}{d}} - 1)^{\mu(d)}.$$

Demonstração. Aplicamos o caso multiplicativo da fórmula de inversão de Moebius ao grupo multiplicativo G das funções racionais não nulas sobre K . Seja $h(n) = Q_n(x)$ e $H(n) = x^n - 1$ para todo $n \in \mathbb{N}$. Então o Teorema 3.15 (i) mostra que (3.1) é satisfeita, e então (3.2) nos fornece o resultado desejado. $\square$

Exemplo 3.23. Para corpos K sobre os quais Q_{12} está definido, temos

$$\begin{aligned} Q_{12}(x) &= \prod_{d|12} (x^{\frac{12}{d}} - 1)^{\mu(d)} \\ &= (x^{12} - 1)^{\mu(1)} (x^6 - 1)^{\mu(2)} (x^4 - 1)^{\mu(3)} (x^3 - 1)^{\mu(4)} (x^2 - 1)^{\mu(6)} (x - 1)^{\mu(12)} \\ &= \frac{(x^{12} - 1)(x^2 - 1)}{(x^6 - 1)(x^4 - 1)} = x^4 - x^2 + 1. \end{aligned}$$

Por fim, sabemos uma fórmula para o número de polinômios mônicos irredutíveis sobre $\mathbb{F}_q[x]$ de grau fixado n e, usando os polinômios ciclotômicos, podemos obter a fórmula para o produto de tais polinômios (Teorema 3.31 de [1]). Para isso, sejam q e m dois inteiros positivos relativamente primos. Chamaremos “ordem multiplicativa de q no módulo m ” o menor inteiro a tal que $q^a \equiv 1 \pmod{m}$.

Teorema 3.24. *O produto $I(q, n, x)$ de todos os polinômios mônicos irredutíveis sobre $\mathbb{F}_q[x]$ de grau fixado n é dado por*

$$I(q, n, x) = \prod_m Q_m(x),$$

em que o produto é estendido sobre todos os divisores positivos m de $q^n - 1$ tais que n é a ordem multiplicativa de q no módulo m .

4 Teorema de Wedderburn

Chegamos, enfim, à demonstração do Teorema de Wedderburn. Faremos duas provas para ele, a primeira usando os teoremas e definições apresentadas nos capítulos anteriores e a segunda utilizando resultados simples de álgebra linear. Ambas podem ser encontradas em [1]. A demonstração original de Joseph Wedderburn apresentada à Universidade de Chicago em 1905 pode ser encontrada em [3]. Antes, porém, precisamos fixar algumas notações.

Seja D um anel de divisão e F um subanel que é um corpo. Então D pode ser visto como um espaço vetorial (à esquerda) de F . Se $F = \mathbb{F}_q$ e D for de dimensão finita m sobre $\mathbb{F}_q$, então D tem q^m elementos. Denotaremos por D^* o grupo multiplicativo dos elementos não nulos de D .

Para um grupo G e um subconjunto não vazio S de G , definimos o **normalizador** de S em G como

$$N(S) = \{a \in G : aSa^{-1} = S\}.$$

Se S for um conjunto unitário $\{b\}$, podemos nos referir a $N(\{b\})$ como o normalizador do elemento b em G . Podemos inferir que, se G for finito, o número de elementos na classe de conjugação de b é $\frac{|G|}{|N(\{b\})|}$.

Teorema 4.1 (Teorema de Wedderburn). *Todo anel de divisão finito é um corpo.*

Demonstração. Seja D um anel de divisão finito e seja $Z = \{z \in D : zd = dz, \text{ para todo } d \in D\}$ o **centro** de D . Omitiremos a verificação simples que Z é um corpo. Então $Z = \mathbb{F}_q$ para alguma potência prima q . Agora, D é um espaço vetorial sobre Z de dimensão finita n , e então D tem q^n elementos. Queremos mostrar que $D = Z$ ou, equivalentemente, $n = 1$.

Suponhamos, do contrário, que $n > 1$. Agora, seja $a \in D$ e defina $N_a = \{b \in D : ab = ba\}$ elementos, em que $1 \leq r \leq n$ (podemos usar a justificativa do Lema 2.1 já que N_a também pode ser visto como um espaço vetorial sobre Z). Queremos mostrar que r divide n .

Uma vez que N_a^* é um subgrupo de D^* , sabemos que $q^r - 1$ divide $q^n - 1$. Se $n = rm + t$, com $0 \leq t < r$, então $q^n - 1 = q^{rm}q^t - 1 = q^t(q^{rm} - 1) + (q^t - 1)$. Agora, $q^r - 1$ divide $q^n - 1$ e $q^{rm} - 1 = (q^r - 1)((q^r)^{m-1} + \dots + q + 1)$, donde segue que $q^r - 1$ divide $q^t - 1$. Mas $q^t - 1 < q^r - 1$, e devemos ter $t = 0$. Isso implica que r divide n .

Consideremos agora a equação de classe para o grupo D^* . O centro de D^* é Z^* , que tem ordem $q - 1$. Para $a \in D^*$, o normalizador de a em D^* é exatamente N_a^* . Então, uma classe de conjugação em D^* contendo mais de um membro tem $\frac{q^n - 1}{q^r - 1}$ elementos, em

que r é um divisor de n com $1 \leq r \leq n$. Assim, a equação de classe de D^* (apresentada no Teorema 1.6) é

$$q^n - 1 = q - 1 + \sum_{i=1}^k \frac{q^n - 1}{q^{r_i} - 1}, \quad (4.1)$$

em que $r_1, \dots, r_k$ são divisores não necessariamente distintos de n com $1 \leq r_i < n$ para $1 \leq i \leq k$.

Agora, seja Q_n o n -ésimo polinômio ciclotômico sobre o corpo dos números racionais. Então $Q_n(q)$ é um inteiro, pelo Teorema 3.15 (ii). Além disso, o Lema 3.20 implica que $Q_n(q)$ divide $\frac{q^n - 1}{q^{r_i} - 1}$ para $1 \leq i \leq k$. A observação que segue a Definição 3.14 nos permite concluir que $Q_n(q)$ divide $q^n - 1$, então concluímos, por (4.1), que $Q_n(q)$ divide $q - 1$. Entretanto, isso nos leva a uma contradição pois, por definição, temos

$$Q_n(x) = \prod_{\substack{s=1 \\ \text{mdc}(s,n)=1}}^n (x - \zeta^s),$$

em que o número complexo ζ é uma raiz n -ésima primitiva da unidade sobre $\mathbb{Q}$. Pode-se provar que, como números complexos, $|q - \zeta^s| > |q - 1|$, para todo $1 \leq s \leq n$ com $\text{mdc}(s, n) = 1$. Logo,

$$|Q_n(q)| = \prod_{\substack{s=1 \\ \text{mdc}(s,n)=1}}^n |q - \zeta^s| > \prod_{\substack{s=1 \\ \text{mdc}(s,n)=1}}^n (q - 1) \geq q - 1$$

uma vez que $n > 1$ e $q \geq 2$. Essa desigualdade é incompatível com a afirmação que $Q_n(q)$ divide $q - 1$. Então, devemos ter $n = 1$ e $D = Z$, e o teorema está provado. $\square$

Antes de começarmos a segunda demonstração do Teorema de Wedderburn, estabeleceremos alguns resultados preliminares.

Seja D um anel de divisão finito com centro Z , e F denotará um **subcorpo maximal** de D , ou seja, F é um subcorpo de D tal que o único subcorpo próprio de D contendo F é F . Então F é uma extensão de Z , porque se existisse um elemento $z \in Z$ com $z \notin F$, poderíamos adjuntar z a F e obter um subcorpo de D que contenha propriamente F . Pelo Teorema 2.10, sabemos que $F = Z(\xi)$, em que $\xi \in F^*$ é uma raiz de um polinômio mônico irreduzível $f \in Z[x]$.

Se enxergarmos D como um F -espaço vetorial, então, para cada $a \in D$, a atribuição $T_a(d) = da$ para $d \in D$ define um operador linear T_a nesse espaço vetorial. Consideremos agora o operador linear T_ξ . Se d for um autovetor de T_ξ , então, para algum $\lambda \in F^*$, temos $d\xi = \lambda d$. Isso implica que $d\xi d^{-1} = \lambda$ e, assim, $dF^*d^{-1} = F^*$, logo $d \in N(F^*)$, o normalizador de F^* no grupo D^* . Inversamente, se $d \in N(F^*)$, então $d\xi d^{-1} = \lambda$ para algum $\lambda \in F^*$, e então d é um autovetor de T_ξ . Isso prova o seguinte resultado:

Lema 4.2. *Um elemento $d \in D^*$ é um autovetor de T_ξ se, e somente se, $d \in N(F^*)$.*

Agora, seja λ um autovalor de T_ξ com autovetor d , então $d\xi = \lambda d$ e $\lambda = d\xi d^{-1}$. Suponha que $f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_1x + a_0 \in Z[x]$, então

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

Segue que $f(\lambda) = 0$, então λ deve ser uma raiz de f . Se d_0 for outro autovetor correspondente ao autovalor λ , então $d_0 d^{-1} \lambda d d_0^{-1} = \lambda$, e o elemento $b = d_0 d^{-1}$ comuta com λ e, consequentemente, com todo elemento de $F = Z(\lambda)$.

Seja P o conjunto de todas as expressões polinomiais em b com coeficientes em F . Então, pode-se checar que P forma um domínio de integridade finito (a finitude de P vem do fato de que todas essas expressões polinomiais pertencem a D e D é um conjunto finito), com isso P é um corpo finito. Mas, P contém F , e então $F = P$ pela maximalidade de F . Em particular, temos $b \in F$, e uma vez que $d_0 = bd$, concluímos que todo autoespaço de T_ξ tem dimensão 1. Usamos, agora, o seguinte resultado de álgebra linear, cuja demonstração pode ser encontrada no Teorema 10 do capítulo 6 de [2]:

Lema 4.3. *Seja T um operador linear no espaço vetorial de dimensão finita V sobre o corpo K . Então, V tem uma base consistindo de autovetores de T se, e só se, o polinômio minimal de T se fatorar em K em fatores lineares mônicos distintos.*

Uma vez que $f(\xi) = 0$, o polinômio f anula o operador linear T_ξ . Além disso, f se fatora em F em fatores lineares mônicos distintos pelo Teorema 3.3. O polinômio minimal para T_ξ divide f , e então ele também se fatora em fatores lineares mônicos distintos em F . Segue do Lema 4.3 que D tem uma base como F -espaço vetorial consistindo de autovetores de T_ξ . Uma vez que todo autoespaço de T_ξ tem dimensão 1, a dimensão m de D sobre F é igual ao número de autovalores distintos de T_ξ .

Sejam $\xi = \xi_1, \xi_2, \dots, \xi_m$ os autovalores distintos de T_ξ e sejam $1 = d_1, d_2, \dots, d_m$ os correspondentes autovetores e considere o polinômio $g(x) = (x - \xi_1) \cdots (x - \xi_m)$. Como $g(\xi) = 0$, o Lema 3.1 implica que f divide g . Por outro lado, nós já tínhamos observado que todo autovalor de T_ξ deve ser uma raiz de f , e então $f = g$.

Segue que $[F : Z] = [Z(\xi) : Z] = \text{gr}(f) = m$. Agora, m é também a dimensão de D sobre F , e então a dimensão de D sobre Z é m^2 . Note que a última igualdade não depende do subcorpo F , donde concluímos que todo subcorpo maximal de D tem o mesmo grau sobre Z . Enunciaremos esse resultado na seguinte forma equivalente:

Lema 4.4. *Todo subcorpo maximal de D tem a mesma ordem.*

Podemos, agora, apresentar a segunda demonstração para o Teorema de Wedderburn.

Segunda prova para o Teorema de Wedderburn. Seja D um anel de divisão finito, e sejam $Z, F = Z(\xi)$ e $f \in F[x]$ como acima. Seja E um subcorpo maximal de D arbitrário. Então, pelo Lema 4.4, E e F têm a mesma ordem, digamos q . Em vista do Lema 2.4, tanto E quanto F são corpos de decomposição de $x^q - x$ sobre Z . Segue que existe um isomorfismo de F em E que fixa os elementos de Z . A imagem $\eta \in E^*$ de ξ sob esse isomorfismo é, portanto, uma raiz de f em E , e, então, $E = Z(\eta)$.

Considere o operador T_η no espaço vetorial D sobre F . Uma vez que $f(\eta) = 0$, o polinômio f anula T_η . Mas, f se fatora em F , e, assim, existe uma raiz λ de f em F^* que é um autovalor de T_η . Para um autovetor d correspondente, $d\eta = \lambda d$, e isso implica $E^* = d^{-1}F^*d$. Logo, E^* é um conjugado do subgrupo F^* de D^* .

Para um arbitrário $c \in D^*$, o conjunto de expressões polinomiais em c com coeficientes em Z forma um domínio de integridade finito, logo é um corpo finito (por um argumento similar ao usado para o conjunto P definido acima). Assim, qualquer elemento de D^* está contido em algum subcorpo de D , e, com isso, em algum subcorpo maximal de D . Concluimos, pelo que já foi provado anteriormente, que qualquer elemento de D^* pertence a algum conjugado de F^* . Sabe-se que o número de conjugados distintos de F^* é dado por $\frac{|D^*|}{|N(F^*)|}$, e, então, é no máximo $\frac{|D^*|}{|F^*|}$. Uma vez que todo conjugado de F^* contém o elemento identidade de D^* , a união dos conjugados de F^* tem, no máximo,

$$\frac{|D^*|}{|F^*|}(|F^*| - 1) + 1 = |D^*| - \frac{|D^*|}{|F^*|} + 1$$

elementos. Esse número é menor que $|D^*|$, exceto quando $D^* = F^*$. Logo, $D = F$, e D é um corpo. $\square$

Uma vez que chegamos ao objetivo principal desse trabalho, vale destacar que Nathan Jacobson, um aluno de doutorado de Joseph Wedderburn, foi capaz de generalizar esse teorema que acabamos de demonstrar. A prova original do Teorema de Jacobson pode ser encontrada em [4].

Teorema 4.5 (Teorema de Jacobson). *Seja R um anel tal que, para todo elemento $a \in R$, existe um inteiro $n(a) > 1$ tal que $a^{n(a)} = a$. Então, R é um anel comutativo.*

Esse resultado é, de fato, uma generalização do Teorema de Wedderburn, pois, dado um anel de divisão finito R , o conjunto $R^* = R \setminus \{0\}$ forma um grupo multiplicativo finito. Assim, sabemos que, para todo elemento $a \in R^*$, a ordem de a é finita, isto é, existe um inteiro $o(a) \geq 1$ tal que $a^{o(a)} = 1$.

Portanto, tomando $n(a) = o(a) + 1 > 1$,

$$a^{n(a)} = a^{o(a)+1} = a^{o(a)} * a = 1 * a = a.$$

Para o elemento nulo 0 , podemos tomar $n(0) = 2$ e vemos que o anel R se enquadra nas condições do Teorema de Jacobson. Dessa forma, ele nos garante que R é comutativo, em particular, segue que R é um corpo por definição.

5 Conclusão

Neste trabalho, foi apresentado o Teorema de Wedderburn, um resultado com enunciado simples, mas que demanda vários tópicos de álgebra para sua demonstração: “todo anel de divisão finito é um corpo”. Então, durante o estudo da demonstração desse teorema, tivemos a oportunidade de compreender melhor a estrutura dos corpos finitos e os polinômios definidos sobre eles.

Cumprimos com o cronograma estipulado e estudamos todos os tópicos programados, entendendo em detalhes cada um deles. Embora esse “ciclo” de estudos tenha se encerrado, os resultados auxiliares para a demonstração do Teorema de Wedderburn nos fornecem uma boa base para estudos futuros.

Referências

- [1] LIDL, R.; NIEDERREITER, H. *Introduction to finite fields and their applications*. Cambridge university press, 1994.
- [2] HOFFMAN, K.; KUNZE, R. *Álgebra Linear, 2a. edição*. Livros Técnicos e Científicos Editora, Rio de Janeiro, 1979.
- [3] WEDDERBURN, Joseph H. M. *A theorem on finite algebras*. Transactions of the American Mathematical Society, v. 6, n. 3, p. 349-352, 1905.
- [4] JACOBSON, N. *Structure theory for algebraic algebras of bounded degree*. Annals of Mathematics v. 46 p. 695-707, 1945.
- [5] HERSTEIN, I. N. *Tópicos de álgebra*. Editora Polígono.
- [6] VIEIRA, Ana Cristina. *Fundamentos de Álgebra II*. Coleção EAD - Matemática, Belo Horizonte, 2011.

APÊNDICE A – Representação de corpos finitos

Nesse apêndice, apresentaremos três diferentes maneiras de se representar um elemento de um corpo finito $\mathbb{F}_q$ com $q = p^n$ elementos, em que p é a característica de $\mathbb{F}_q$, usando raízes de polinômios irredutíveis sobre $\mathbb{F}_q$ e os polinômios ciclotômicos sobre essas estruturas.

No primeiro método, notamos que $\mathbb{F}_q$ é uma extensão algébrica simples de $\mathbb{F}_p$ pelo Teorema 2.10. De fato, se f for um polinômio irredutível em $\mathbb{F}_p[x]$ de grau n , então f tem uma raiz α em $\mathbb{F}_q$ de acordo com o Teorema 3.3, e então $\mathbb{F}_q = \mathbb{F}_p(\alpha)$. Logo, todo elemento de $\mathbb{F}_q$ pode ser unicamente representado como um polinômio em α sobre $\mathbb{F}_p$ de grau menor que n . Também podemos enxergar $\mathbb{F}_q$ como sendo o anel residual $\mathbb{F}_p[x]/(f)$.

Exemplo A.1. Para representar os elementos de $\mathbb{F}_9$ dessa maneira, enxergamos $\mathbb{F}_9$ como uma extensão algébrica simples de $\mathbb{F}_3$ de grau 2, a qual é obtida adjuntando-se uma raiz α de um polinômio quadrático irredutível sobre $\mathbb{F}_3$, digamos $f(x) = x^2 + 1 \in \mathbb{F}_3[x]$. Então, $f(\alpha) = \alpha^2 + 1 = 0$ em $\mathbb{F}_9$, e os nove elementos de $\mathbb{F}_9$ são dados na forma $a_0 + a_1\alpha$, em que $a_0, a_1 \in \mathbb{F}_3$. Em detalhes, $\mathbb{F}_9 = \{0, 1, 2, \alpha, \alpha + 1, \alpha + 2, 2\alpha, 2\alpha + 1, 2\alpha + 2\}$.

Se usarmos os Teoremas 3.17 e 3.19, obtemos outra possibilidade para expressar os elementos de $\mathbb{F}_q$. Uma vez que $\mathbb{F}_q$ é o $(q - 1)$ -ésimo corpo ciclotômico sobre $\mathbb{F}_p$, podemos construí-lo encontrando a decomposição do $(q - 1)$ -ésimo polinômio $Q_{q-1}(x) \in \mathbb{F}_p[x]$ em fatores irredutíveis em $\mathbb{F}_p[x]$, os quais são todos de mesmo grau. Uma raiz de qualquer um desses polinômios é então uma raiz $(q - 1)$ -ésima primitiva da unidade sobre $\mathbb{F}_p$ e, portanto, um elemento primitivo de $\mathbb{F}_q$. Logo, $\mathbb{F}_q$ consiste de 0 e potências apropriadas desse elemento primitivo.

Exemplo A.2. Para aplicar isso à construção de $\mathbb{F}_9$, observamos que $\mathbb{F}_9 = \mathbb{F}_3^{(8)}$, o oitavo corpo ciclotômico sobre $\mathbb{F}_3$. Agora, $Q_8(x) = x^4 + 1 \in \mathbb{F}_3[x]$ pelo Exemplo 3.16 e

$$Q_8(x) = (x^2 + x + 2)(x^2 + 2x + 2)$$

é a decomposição de $Q_8(x)$ em fatores irredutíveis em $\mathbb{F}_3[x]$. Seja ζ uma raiz de $x^2 + x + 2$, então ζ é uma raiz oitava primitiva da unidade sobre $\mathbb{F}_3$. Logo, todos os elementos não nulos de $\mathbb{F}_9$ podem ser representados como potências de ζ , e assim $\mathbb{F}_9 = \{0, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5, \zeta^6, \zeta^7, \zeta^8\}$. Podemos organizar os elementos não nulos de $\mathbb{F}_9$ na chamada **tabela de índices**, em que listamos os elementos ζ^i de acordo com seus expoentes i . Para estabelecer a conexão com a representação no Exemplo A.1, observamos que $x^2 + x + 2 \in \mathbb{F}_3[x]$ tem $\zeta = 1 + \alpha$ como raiz, em que $\alpha^2 + 1 = 0$ como no Exemplo A.1. Portanto, a tabela de índices para $\mathbb{F}_9$ é:

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

Vemos que obtemos, obviamente, os mesmos elementos do Exemplo A.1, apenas em uma ordem diferente.

Uma terceira possibilidade para representar os elementos de $\mathbb{F}_q$ é dada por meio de matrizes. No geral, a **matriz companheira** de um polinômio mônico $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ de grau positivo n sobre um corpo é definida como a matriz $n \times n$

$$A = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}.$$

É sabido da álgebra linear que A satisfaz a equação $f(A) = 0$, isto é, $A^n + a_{n-1}A^{n-1} + \cdots + a_1A + a_0I = 0$.

Então, se A é a matriz companheira de um polinômio mônico irredutível sobre $\mathbb{F}_p$ de grau n , então $f(A) = 0$, e portanto A pode fazer o papel de uma raiz de f . Os polinômios em A sobre $\mathbb{F}_p$ de grau menor que n fornecem uma representação para os elementos de $\mathbb{F}_q$.

Exemplo A.3. Como no Exemplo A.1, seja $f(x) = x^2 + 1 \in \mathbb{F}_3[x]$. A matriz companheira de f é

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

O corpo $\mathbb{F}_9$ pode então ser representado na forma $\mathbb{F}_9 = \{0, I, 2I, A, A + I, A + 2I, 2A, 2A + I, 2A + 2I\}$. Explicitamente,

$$0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad 2I = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \quad A = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}, \quad A + I = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix},$$

$$A + 2I = \begin{pmatrix} 2 & 2 \\ 1 & 2 \end{pmatrix}, \quad 2A = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}, \quad 2A + I = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}, \quad 2A + 2I = \begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix}.$$

Com $\mathbb{F}_9$ dado dessa forma, os cálculos nesse corpo seguem as regras usuais da álgebra matricial. Por exemplo,

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

Exemplo A.4. Como no Exemplo A.2, seja $h(x) = x^2 + x + 2 \in \mathbb{F}_3[x]$ um fator irredutível do polinômio ciclotômico $Q_8(x) \in \mathbb{F}_3[x]$. A matriz companheira de h é

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

O corpo $\mathbb{F}_9$ pode ser representada na forma

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

Explicitamente,

$$\begin{aligned} 0 &= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad C = \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}, \quad C^2 = \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}, \quad C^3 = \begin{pmatrix} 2 & 2 \\ 2 & 0 \end{pmatrix}, \quad C^4 = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \\ C^5 &= \begin{pmatrix} 0 & 2 \\ 2 & 1 \end{pmatrix}, \quad C^6 = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, \quad C^7 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \quad C^8 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

Os cálculos seguem as regras da álgebra matricial. Por exemplo,

$$C^6 + C = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 2 & 0 \end{pmatrix} = C^3.$$