CORPOS FINITOS

César Polcino Milies

Sumário

Capítulo 1

Introdução à Teoria de Corpos

1.1 Conceitos básicos

Começaremos lembrando algumas definições que devem ser já conhecidas do leitor.

Se, para todo par de elementos a e b de um anel R, tem-se que

$$ab = ba$$

então diz-se que R é um anel é **comutativo** .

Os conjuntos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, com as operações usuais, são exemplos de anéis comutativos. Também o anel $\mathbb{Z}_m$ dos inteiros módulo m, com as operações nele definidas a partir das operações de $\mathbb{Z}$, é um anel comutativo.

O conjunto $M_2(\mathbb{Q})$ das matrizes 2×2 com coeficiente racionais, com as operações usuais de soma e de produto de matrizes, é um anel mas *não é* comutativo. Por exemplo, se consideramos as matrizes;

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

temos que

$$AB = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \quad \text{e} \quad BA = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix},$$

logo $AB \neq BA$.

Se existem elementos não nulos a, b num anel R tais que $ab = 0$ então esses elementos dizem-se **divisores de zero**.

Por exemplo, no anel $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$ temos que $\overline{3} \cdot \overline{4} = \overline{0}$, logo $\overline{3}$ e $\overline{4}$ são divisores de zero em $\mathbb{Z}_6$.

Um anel sem divisores de zero chama-se um **domínio**.

Um anel R que contém um elemento 1 tal que

$$1 \cdot a = a \cdot 1 = a, \text{ para todo } a \in R$$

diz-se um **anel com unidade** *e esse elemento chama-se o* **elemento unidade** *de R.*

Note que, se num anel com unidade R tem-se que $1 = 0$, então necessáriamente $R = \{0\}$. Por causa disso, ao falar em anéis com unidade, iremos assumir sempre que $1 \neq 0$.

Um anel com unidade, que é também um domínio comutativo chama-se um **domínio de integridade**; *em outras palavras, um domínio de integridade é um anel comutativo, com unidade, sem divisores de zero.*

Num anel com unidade, pode-se distinguir uma outra classe de elementos importantes:

Um elemento a de um anel R diz-se **inversível** *se existe um elemento, que denotaremos por $a^{-1} \in R$, e chamaremos seu* **inverso**, *tal que $a \cdot a^{-1} = a^{-1} \cdot a = 1$. O conjunto*

$$\mathcal{U}(R) = \{a \in R \mid a \text{ é inversível}\}$$

chama-se o **grupo de unidades** *de R.*

Note que $\mathcal{U}(R)$ é, de fato, um grupo em relação à operação de multiplicação de R.

Definição 1.1.1. *Um anel comutativo, com identidade, em que todo elemento não nulo é inversível diz-se um* **corpo**.

O termo *corpo* foi usado por primeira vez em alemão, na expressão *Zahlenkörper* (corpo de números) por Richard Dedekind (1831-1916), em 1858, mas só passou a ser usado mais extensamente, a partir da década de 1890. Antes disso, a expressão comumente usada era "domínio de racionalidade".

Proposição 1.1.2. *Um elemento inversível não é um divisor de zero.*

Demonstração. Seja a um elemento inversível de um anel com unidade R. Suponhamos que a é um divisor de zero. Então, existe um elemento $b \neq 0$ em R tal que $ab = 0$. Então temos que:

$$0 = a^{-1}(ab) = (a^{-1}a)b = 1.b$$

logo $b = 0$, uma contradição. □

Proposição 1.1.3. *Seja m um inteiro positivo e seja $\overline{a} \neq 0$ um elemento de $\mathbb{Z}_m$. Então, são equivalentes:*
(i) $\overline{a}$ é inversível.
(ii) $\overline{a}$ não é divisor de zero.
(iii) $mdc(a, m) = 1$.

Demonstração.
O fato de que (i) ⇒ (ii) segue diretamente do Lema 1.1.1.

(ii) ⇒ (iii). Para demonstrar esta implicação assumumimos que $mdc(a, m) = d \neq 1$ para mostrar que isso nos leva a uma contradição. De fato, como $d \mid a$ e $d \mid m$, existem a' e m' em $\mathbb{Z}$ tais que $a = da'$ e $m = dm'$. Como $m' < m$ obviamente $\overline{m'} \neq \overline{0}$ em $\mathbb{Z}_m$. Porém, temos que:

$$\overline{a}\overline{m'} = (\overline{a'}\overline{d})\overline{m'} = \overline{a'}(\overline{d}\overline{m'}) = \overline{am} = \overline{0},$$

uma contradição.

(iii) ⇒ (i) Se $mdc(a, m) = 1$ então existem inteiros r e s tais que $ra+sm = 1$. Logo, em $\mathbb{Z}_m$ temos que

$$\overline{ra} + \overline{sm} = \overline{1}$$

donde

$$\overline{r}\,\overline{a} = \overline{1}.$$

Como consequência imediata da proposição acima, temos os seguinte resultado.

Proposição 1.1.4. *O anel $\mathbb{Z}_p$ dos inteiros módulo p é um corpo se e somente se p é um inteiro primo.*

Como veremos adiante, estes corpos irão desempenhar um papel central na teoria.

EXERCÍCIOS

---

1. Provar que, num corpo $\mathbb{F}$ vale a propriedade cancelativa: sa a, b, c são elementos de $\mathbb{F}$, $c \neq 0$ e $ac = bc$ então $a = b$.

2. Provar que todo domínio de integridade finito, é um corpo.

3. Dado um anel comutativo R, chama-se **grupo das unidades** de R ao conjunto
$$\mathcal{U}(R) = \{a \in R \mid (\exists a' \in R)\ aa' = a'a = 1\}$$
dos elementos inversíveis de R.

   (*i*) Provar que $\mathcal{U}(R)$ é um grupo abeliano.

   (*ii*) Determinar $\mathcal{U}(\mathbb{Z}_{15})$ e $\mathcal{U}(\mathbb{Z}_{30})$.

   (*iii*) Mostrar que, em geral $\mathcal{U}(R)$ não é um corpo.

4. (i) Provar que $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$ é um corpo.

   (ii) Provar que $\mathbb{Z}_5(i) = \{a + bi \mid a, b \in \mathbb{Z}_5, i^2 = -1\}$ não é um corpo, mostrando que contém divisores de zero e elementos idempotentes não triviais.

5. Provar que, se $d \in \mathbb{Z}$ não é um quadrado perfeito, então $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$ é um corpo.

6. Provar que o subconjunto $\mathbb{K} = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}\} \subset \mathbb{Z}_{10}$ é um corpo.

7. Considere o seguinte conjunto de matrizes de $M_2(\mathbb{Z}_2)$:
$$F = \left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \right\}.$$
Provar que, com as operações usuais de $M_2(\mathbb{Z}_2)$, F é um corpo.

8. Dar um exemplo de corpo onde a equação $X^2 + Y^2 = 0$ tem solução não trivial.

9. Sejam $\mathbb{F}$ um corpo e $e \in \mathbb{F}$ um elemento idempotente; i.e., um elemento tal que $e^2 = e$. Provar que $e = 0$ ou $e = 1$.

10. Seja $\mathbb{F}$ um corpo. Provar que $\mathbb{F} \setminus \{0\}$ é um grupo, em relação à multiplicação de $\mathbb{F}$.

11. Seja $\mathbb{F}$ um corpo que tem n elementos. Provar que para todo elemento $\alpha \in \mathbb{F}$ tem-se que $\alpha^{n-1} = 1$.

12. . Sejam $\mathbb{F}$ e $\mathbb{E}$ corpos e seja $\varphi : \mathbb{F} \to \mathbb{E}$ um homomorfismo não nulo. Provar que φ é injetora.

1.2 Corpos primos

Tal como acontece ao estudar outras estruturas algébricas, será de nosso interesse considerar subconjuntos de um corpo que são, eles próprios, corpos.

Definição 1.2.1. *Um subconjunto $\mathbb{K}$ de um corpo $\mathbb{F}$ diz-se um* **subcorpo** *de $\mathbb{F}$ se $\mathbb{K}$ é fechado em relação aos operações de $\mathbb{F}$ e em relação à inversão; isto é, se para todo par de elementos $x, y \in \mathbb{K}$ tem-se que:*

(i) $x \pm y \in \mathbb{K}$.

(ii) $xy \in \mathbb{K}$.

(iii) $x^{-1} \in \mathbb{K}$.

e se $\mathbb{K}$, com a restrição das operações de $\mathbb{F}$, é, ele próprio, um corpo.

Na verdade, é possível determinar se um subconjunto $\mathbb{K}$ de um corpo $\mathbb{F}$ é um subcorpo, apenas com um número pequeno de verificações; veja o exercício 1.

Uma observação simples, mas muito importante, é a seguinte. Sejam $\mathbb{F}$ um corpo e $\mathbb{K}$ um subcorpo de $\mathbb{F}$. Denotaremos, como sempre, por 1 o

elemento unidade de $\mathbb{F}$. Como $\mathbb{K}$ também é um corpo, ele tem um elemento unidade, que denotaremos por e e que, em princípio, poderia ser diferente de 1. Porém, se $e \in \mathbb{K}$ é unidade, em particular ele deve verificar que $e.e = e$. Logo. temos que:

$$e^2 - e = 0,$$

donde

$$e(e-1) = 0.$$

Como $\mathbb{K}$ não contém divisores de 0, temos que $e = 0$ ou $e = 1$ e, como por definição, o elemento unidade de um corpo é diferente de 0, temos que $e = 1$. Isto prova que *o elemento unidade de qualquer subcorpo de* $\mathbb{F}$ *é sempre igual a* 1*, o elemento unidade de* $\mathbb{F}$.

Seja $m > 0$ um inteiro. Dado um elemento a de um corpo $\mathbb{F}$, podemos definir o produto ma por

$$ma = \underbrace{a + a + \cdots + a}_{m \text{ vezes}} \in \mathbb{F},$$

ou, equivalentemente, de modo mais formal, podemos definir $1.a = a$ e, indutivamente, $ma = (m-1)a + a$.

Esta definição pode se estender a todos os inteiros da seguinte forma:
Se $m = 0$ definimos $ma = 0$ para todo $a \in \mathbb{F}$.
Se $m < 0$ definimos

$$ma = |m|(-a) = \underbrace{(-a) + (-a) + \cdots + (-a)}_{|m| \text{ vezes}}.$$

Note que, se $\mathbb{K}$ é um subcorpo de $\mathbb{F}$, como $1 \in K$, temos que $m.1 \in \mathbb{K}$, para todo inteiro m. Assim, todo subcorpo $\mathbb{K}$ de $\mathbb{F}$ contém o subconjunto:

$$S = \{m.1 \mid m \in \mathbb{Z}\}.$$

Podemos agora definir uma função $\varphi : \mathbb{Z} \to \mathbb{F}$ por $\varphi(m) = m.1$, para todo $m \in \mathbb{Z}$.

O leitor poderá verificar facilmente que φ é um homomorfismo de anéis e que $Im(\varphi)$ (que é precisamente S) está contido em todo subcorpo $\mathbb{K}$ de $\mathbb{F}$. Do Teorema do Homomorfismo para anéis, temos que $Im(\varphi) \cong \mathbb{Z}/Ker(\varphi)$.

Vamos considerar separadamento, dois casos possíveis.

(i) Se $Ker(\varphi) \neq 0$, como $\mathbb{Z}$ é um domínio principal e $Ker(\varphi)$ é um ideal de $\mathbb{Z}$, existe um inteiro $m > 0$ tal que $ker(\varphi) = m\mathbb{Z}$. Note que, em particular, m é o menor inteiro positivo que pertence a $Ker(\varphi)$.

Afirmamos que m é um inteiro primo. De fato, se $m = rs$, com r e s inteiros positivos, temos que:

$$0 = \varphi(m) = \varphi(rs) = \varphi(r)\varphi(s).$$

Como $\mathbb{F}$ não contém divisores de zero, deve ser $\varphi(r) = 0$ ou $\varphi(s) = 0$ donde $r \in Ker(\varphi)$ ou $s \in Ker(\varphi)$. Como tanto r quanto s são inteiros positivos menores do que m, qualquer uma das possibilidades acima implica numa contradição.

Assim, temos que $S = Im(\varphi) \cong \mathbb{F}/p\mathbb{Z})$. Como p é primo, $p\mathbb{Z}$ é um ideal maximal e, portanto, $\mathbb{Z}/p\mathbb{Z}$ é um corpo. Como, S está contido em todo subcorpo $\mathbb{K}$ de $\mathbb{F}$, temos que S *é o menor subcorpo de* $\mathbb{F}$.

(ii) Se $Ker(\varphi) = (0)$ então $Im(\varphi) \cong \mathbb{Z}$ e, diferentemente do caso anterior, não é um corpo. Note que, neste caso, podemos estender φ a um homomorfismo $\overline{\varphi} : \mathbb{Q} \to \mathbb{F}$ da seguinte forma. Cada elemento $\alpha \in \mathbb{Q}$ pode-se escrever de modo único como $\alpha = a/b$ com $a, b \in \mathbb{Z}, b \neq 0$ e $mdc(a, b) = 1$. Definimos então

$$\overline{\varphi}(\alpha) = \overline{\varphi}(a/b) = \varphi(a)\varphi(b)^{-1}.$$

Note que esta função está bem definida porque, como $b \neq 0$ e $Ker(\varphi) = (0)$, temos que $\varphi(b) \neq 0$. Ainda, como $\mathbb{F}$ é um corpo, nestas condições sempre existe $\varphi(b)^{-1}$.

Agora, é muito fácil provar que também $Ker(\overline{\varphi}) = (0)$. Portanto temos que

$$\mathbb{Q} \cong Im(\overline{\varphi}) = \{\varphi(a)\varphi(b)^{-1} \mid a, b \in \mathbb{Z}, b \neq 0\}.$$

Logo, $Im(\overline{\varphi})$ é um corpo. Ainda, como $\varphi(b) \in \mathbb{K}$, temos também que $\varphi(b)^{-1} \in \mathbb{K}$. Como isto vale para todos os subcorpos $\mathbb{K}$ de $\mathbb{F}$ temos que $Im(\overline{\varphi})$ é *o menor subcorpo de* $\mathbb{K}$ *pois, como no caso anterior, ele está contido em todos os subcorpos de* $\mathbb{F}$.

Definição 1.2.2. *Seja $\mathbb{F}$ um corpo. Chama-se* **subcorpo primo** *de $\mathbb{F}$ ao menor subcorpo de $\mathbb{F}$, em relação à inclusão.*

Um corpo diz-se **primo** *se coincide com seu subcorpo primo; isto é, se não existe nenhum subcorpo própriamente contido nele.*

Note que as considerações acima mostram que todo corpo $\mathbb{F}$ contém um subcorpo primo. Mais ainda, temos provado o seguinte.

Teorema 1.2.3. *Seja $\mathbb{F}$ um corpo primo. Então $\mathbb{F}$ é isomorfo a $\mathbb{Q}$, o corpo dos números racionais ou $\mathbb{F}$ é isomorfo a $\mathbb{Z}_p$, o anel dos inteiros módulo p, para algum primo p.*

Lembramos que chama-se **característica** de um corpo $\mathbb{F}$ ao menor inteiro positivo m, tal que $m.a = 0$, para todo elemento $a \in F$, se esse inteiro existe. Em caso contrário, diz-se que $\mathbb{F}$ é um **corpo de característica** 0. Note que, do teorema anterior, segue imediatamente o seguinte.

Corolario 1.2.4. *Seja $\mathbb{F}$ um corpo. Então a característica de $\mathbb{F}$ é 0 se e somente se o corpo primo de $\mathbb{F}$ é isomorfo a $\mathbb{Q}$ e a característica de $\mathbb{F}$ é um primo $p > 0$ se e somente se o corpo primo de $\mathbb{F}$ é isomorfo a $\mathbb{Z}_p$.*

A noção de *corpo primo*, que estudamos nesta seção, é devida a Ernst Steinitz (1871-1928) que a define num artigo de 1910 onde introduz também várias outras noções importantes da teoria de corpos, que estudaremos ao longo deste capítulo.

Este texto de Steinitz contém ainda a primeira definição abstrata de *corpo* e a construção, hoje tão familiar, dos números racionais como classes de equivalência de pares ordenados de inteiros (com segunda componente não nula), e a relação $(a, b) \equiv (c, d)$ se e só se $ad = bc$.

Esta memória veio a se tornar tão importante que N. Bourbaki, no seu livro sobre história de matemática a descreeve como um dos dois pilares sobre os quais se levantou todo o edifício da álgebra moderna. A outra memória a que este autor se refere, é o trabalho de E. Noether (1882-1935) sobre anéis, módulos e representações publicado em 1929.

Em 1930, vinte anos depois da primeira publicação, o trabalho de Steinitz foi re-editado, com um prólogo escrito por Reinhold Baer (1902-1979) e Helmut Hesse (1898-1979), dois destacados algebristas do século XX, onde escrevem que a memória

... tornou-se o ponto de partida de muitas análises profundas no campo da álgebra e da aritmética. Na clássica beleza e perfeição na forma de apresentação de todos seus detalhes não é somente uma ponto alto no desenvolvimento do conhecimento algébrico, mas é, ainda hoje, uma extraordinária e até indispensável introdução para qualquer um que deseja se dedicar ao campo de estudos mais detalhados da álgebra moderna.

EXERCÍCIOS

---

1. Seja $\mathbb{K}$ um subconjunto de um corpo $\mathbb{F}$. Provar que $\mathbb{K}$ é um subcorpo de $\mathbb{F}$ se e somente se para todo par de elementos $x, y \in \mathbb{K}$ tem-se que $x \pm y$ e xy^{-1} estão em $\mathbb{K}$.

2. (i) Seja $\mathcal{F}$ uma família de subcorpos de um corpo $\mathbb{F}$. Provar que $\bigcap_{\mathbb{K}\in\mathcal{F}} \mathbb{K}$ é um subcorpo de $\mathbb{F}$.

   (ii) Provar que, se $\mathcal{F}$ é a família de todos os subcorpos de $\mathbb{F}$, então $\mathbb{P} = \bigcap_{\mathbb{K}\in\mathcal{F}} \mathbb{K}$ é o corpo primo de $\mathbb{F}$.

3. Sejam m um inteiro e a um elemento de um corpo $\mathbb{F}$. Provar que $ma = (m1)a$.

4. Sejam r e s inteiros positivos e $\mathbb{F}$ um corpo . Provar que $(rs)1 = (r1)(s1)$ em $\mathbb{F}$. Mostrar que esta igualdade vale também quando r e s são inteiros quaisquer.

5. Seja F um corpo cujo corpo primo é isomorfo a $\mathbb{Z}_p$. Provar que para todo inteiro m e para todo elemento não nulo $a \in \mathbb{F}$ tem-se quue $ma = 0$ se e somente se $p \mid m$.

6. Sejam a e b elementos de um corpo de característica $p \neq 0$.

   (i) Provar que $(a+b)^p = a^p + b^p$.

   (ii) Mostrar que, para todo inteiro positivo m tem-se que

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

7. Seja $\mathbb{E}$ um corpo finito, de característica $p \neq 2$. Provar que a soma de todos os elementos de $\mathbb{E}$ é igual a 0.

8. Seja $\mathbb{E}$ um corpo finito. Provar que o produto de todos os elementos de $\mathbb{E}$ é igual a -1.

1.3 Elementos algébricos e transcendentes

Na seção anterior, estudamos corpos que estão contidos num corpo dado $\mathbb{F}$. Nesta seção vamos mudar o ponto de vista e estudar corpos que *contém* $\mathbb{F}$.

Definição 1.3.1. *Seja $\mathbb{F}$ um corpo e seja $\mathbb{E}$ um corpo tal que $\mathbb{F} \subset \mathbb{E}$. Neste caso, diz-se que $\mathbb{E}$ é uma* **extensão** *de $\mathbb{F}$.*

Esta terminologia está intimamente relacionada com a que foi introduzida na seção anterior. Naturalmente, $\mathbb{E}$ é uma extensão de $\mathbb{F}$ se e somente se $\mathbb{F}$ é um subcorpo de $\mathbb{E}$. Às vezes, descreveremos esta situação dizendo, simplesmente que $\mathbb{F} \subset \mathbb{E}$ é uma **extensão de corpos**.

Definição 1.3.2. *Seja $\mathbb{F} \subset \mathbb{E}$ uma extensão de corpos e seja X um subconjunto de elementos de $\mathbb{E}$. Denotaremos por $\mathbb{F}(X)$ o menor subcorpo de $\mathbb{E}$ que contém $\mathbb{F}$ e contém X.*

A definição acima da significado para a notação $\mathbb{F}(X)$. Porém, em princípio, nada garante a existência de um tal corpo. Consideremos então a família

$$\mathcal{F} = \{\mathbb{E}_i \mid \mathbb{E}_i \text{ é subcorpo de } \mathbb{E}, X \subset \mathbb{E}_i,\ \mathbb{F} \subset \mathbb{E}_i\}.$$

Esta família é não vazia pois o próprio corpo $\mathbb{E}$ pertence a $\mathcal{F}$.
Consideramos agora o conjunto

$$\mathbb{K} = \bigcap_{E_i \in \mathcal{F}} E_i.$$

Claramente, $\mathbb{K}$ é um corpo e, como tanto $\mathbb{F}$ quanto X estão contidos em todos os corpos $\mathbb{E}_i \in \mathcal{F}$, temos que $\mathbb{F} \subset \mathbb{K}$ e $X \subset \mathbb{K}$. Ainda, qualquer corpo nestas condições é um dos membros da família $\mathcal{F}$, logo $\mathbb{K}$, que é a interseção de todos, está contido nele. Desta forma, temos provado que $\mathbb{F}(X)$ existe, pois é, precisamente, o corpo $\mathbb{K}$ construído acima.

Quando X é um conjuto finito $\{a_1, a_2, \ldots, a_n\}$ denotaremos a extensão $\mathbb{F}(X)$ simplesmente por $\mathbb{F}(a_1, a_2, \ldots, a_n)$. Um caso particularmente interessante é quando X consiste num único elemento. Neste caso, a extensão recebe um nome particular.

Definição 1.3.3. *Seja $\mathbb{F} \subset \mathbb{E}$ uma extensão de corpos e seja a um elemento de E. O corpo $\mathbb{F}(a)$ diz-se uma* **extensão simples** *de $\mathbb{F}$.*

A estrutura do corpo $\mathbb{F}(a)$ depende de propriedades do elemento a; mais explicitamente, depende fortemente do fato de a ser, ou não, raiz de um polinômio com coeficientes em $\mathbb{F}$. Para estudar esta situação, precisamos introduzir ainda alguns conceitos.

Definição 1.3.4. *Seja $\mathbb{F} \subset \mathbb{E}$ uma extensão de corpos. Um elemento $a \in \mathbb{E}$ diz-se* **algébrico** *sobre $\mathbb{F}$ se existe um pólinômio $f \in \mathbb{F}[X]$ tal que $f(a) = 0$. Neste caso, diz-se que a é uma* **raiz** *de f.*

Um elemento $a \in E$ que não é algébrico sobre $\mathbb{F}$ diz-se **transcendente**.

Note que, de acordo com esta definição, um elemento $a \in \mathbb{E}$ é transcendente sobre $\mathbb{F}$ se a não é raiz de nenhum polinômio com coeficientes em $\mathbb{F}$.

A expressão *elemento transcendente* foi usada por Leonhard Euler (1707-1783) em 1744 para indicar que números que são transcendentes sobre os racionais, *"transcendem o poder dos métodos algébricos"*.

Somente um século depois, em 1844, Joseph Liouville (1809-1882) provou a existência de números transcendentes. Em 1873 Charles Hermite (1822-1901) provou que a constante de Euler, e, é transcendente sobre os racionais

e, em 1873, C.L. Ferdinand von Lindemann (1852-1939) provou que também π é transcendente.

Seja então $\mathbb{F} \subset \mathbb{E}$ uma extensão de corpos e seja a um elemento de $\mathbb{E}$. Se a é algébrico sobre $\mathbb{F}$, então o conjunto de polinômios

$$I = \{f \in \mathbb{F}[X] \mid f(a) = 0\}$$

não é vazio.

É fácil verificar diretamente que I é um ideal de $\mathbb{F}[X]$. Como $\mathbb{F}[X]$ é um anel principal, existe um polinômio f que é gerador de I; isto é, tal que todo elemento de I é um múltiplo de f. O ideal dos múltiplos de f_0 é denotado por (f); assim, podemos escrever que $I = (f)$. Ainda, se multiplicamos f por uma constante $a \in \mathbb{F}$ temos que af é outro gerador do mesmo ideal I.

Escrevendo $f = a_0 + a_1X + + \cdots + a_{n-1}X^{n-1} + a_nX^n$ temos que o polinômio

$$f_0 = a_n^{-1}f = a_n^{-1}a_0 + a_n^{-1}a_1X + \cdots + a_n^{-1}a_{n-1}X^{n-1} + X^n$$

é outro gerador de I que é *mônico* (isto é, um polinomio em que o coeficiente do termo de maior grau é igual a 1).

Note que, se $g \in F[X]$ é qualquer outro polinômio que tem raiz a, então $g \in I$; portanto $f_0 \mid g$, donde $gr(f_0) \leq gr(g)$.

Definição 1.3.5. *O polinômio de $\mathbb{F}[X]$, mônico, de menor grau, que tem raiz a chama-se o* **polinômio minimal** *de a sobre $\mathbb{F}$.*

Daqui por diante, denotaremos o polinômio minimal de a sobre $\mathbb{F}$ por m_a. Note que, da própria definição, segue que m_a divide todo polinômio de $\mathbb{F}[X]$ que tem raiz a. Este fato será repetidamente usado adiante.

Proposição 1.3.6. *Seja a um elemento algébrico sobre um corpo $\mathbb{F}$. Então m_a é um polinômio irredutível em $\mathbb{F}[X]$.*

Demonstração. De fato, suponhamos que $m_a = gh$ com $g, h \in \mathbb{F}[X]$. Então temos que $0 = m_a(a) = g(a)h(a)$ e, como $\mathbb{F}$ não contém divisores de 0, temos que $g(a) = 0$ ou $h(a) = 0$.

Seja novamente I o ideal de $\mathbb{F}[X]$ formado por todos os polinômios que tem raiz a. Então, conforme nossa definição, temos que $I = (m_a)$.

Se $g(a) = 0$ tem-se que $g \in I$, donde $m_a \mid g$. Como estamos assumindo que também $g \mid m_a$ segue que $gr(m_a) = gr(g)$ e, portanto, $h \in \mathbb{F}$. Se $h(a) = 0$ obtém-se, de forma análoga, que $g \in \mathbb{F}$. Em ambos os casos, a decomposição de m_a não é em produto de divisores próprios, donde m_a é irredutível. □

Definição 1.3.7. *Seja a um elemento algébrico sobre um corpo F e seja m_a o seu polinômio minimal sobre $\mathbb{F}$. O grau do polinômio m_a diz-se o* **grau** *de a sobre $\mathbb{F}$.*

Podemos dar agora uma caracterização das extensões simples, por elementos algébricos.

Proposição 1.3.8. *Sejam $\mathbb{F} \subset \mathbb{E}$ corpos e seja $a \in \mathbb{E}$ um elemento algébrico com polinômio minimal m_a. Então,*

$$\mathbb{F}(a) \cong \frac{\mathbb{F}[X]}{(m_a)}.$$

Demonstração. Seja $\varphi : \mathbb{F}[X] \to \mathbb{F}(a)$ a função que a cada polinômio $f \in \mathbb{F}[X]$ associa $f(a)$, o valor de f em a.

É fácil verificar, diretamene, que φ é um homomorfismo de anéis. Portanto, temos que

$$Im(\varphi) \cong \frac{\mathbb{F}[X]}{Ker(\varphi)}.$$

Note que $Ker(\varphi)$ está formado, precisamente, pelos polinômios que têm raiz a; logo $Ker(\varphi) = (m_a)$. Como m_a é irredutível, $\mathbb{F}[X]/(m_a)$ é um corpo.

Ainda, como $Im(\varphi) \subset \mathbb{F}(a)$, contém a e é um corpo, segue que

$$\frac{\mathbb{F}[X]}{Ker(\varphi)} \cong Im(\varphi) = \mathbb{F}(a).$$

□

Note que a demonstração do teorema acima nos dá informação adicional sobre a natureza de $\mathbb{F}(a)$. Com efeito, no decorrer da prova mostramos que

$\mathbb{F}(a) = Im)\varphi)$. Isto significa que todo elemento de $\mathbb{F}(a)$ é da forma $f(a)$, com $f \in \mathbb{F}[X]$.

Seja então $\alpha = f(a)$ um elemento de $\mathbb{F}(a)$. Dividindo f pelo polinômio minimal m_a temos que existem $q, r \in \mathbb{F}[X]$ tais que $f = m_a q + r$ onde $r = 0$ ou $gr(r) < gr(m_a)$. Calculando valores em a temos que $f(a) = m_a(a)q(a) + r(a)$ e, como $m_a(a) = 0$, segue que $f(a) = r(a)$.

Assim, se n indica o grau de m_a temos que qualquer elemento $\alpha \in \mathbb{F}(a)$ é da forma

$$\alpha = x_0 + x_1 a + x_2 a^2 + \cdots + a_{n-1} a^{n-1}.$$

Logo, temos provado o seguinte.

Corolario 1.3.9. *Se a é um elemento algébrico de grau n sobre um corpo $\mathbb{F}$, então:*

$$\mathbb{F}(a) = \{x_0 + x_1 a + x_2 a^2 + \cdots + x_{n-1} a^{n-1} \mid x_i \in \mathbb{F},\ 1 \leq i \leq n-1\}.$$

Também é possível descrever as extensões simples, por elementos transcendentes. Para isso precisamos de mais uma definição. Lembramos que, dado um corpo $\mathbb{F}$, denota-se por $\mathbb{F}(X)$ o corpo de frações do anel $\mathbb{F}[X]$; isto é:

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

Definição 1.3.10. *O corpo $\mathbb{F}(X)$ chama-se o* **corpo das funções racionais** *sobre $\mathbb{F}$.*

Proposição 1.3.11. *Sejam $\mathbb{F} \subset \mathbb{E}$ corpos e seja $a \in \mathbb{E}$ um elemento transcendente sobre $\mathbb{F}$. Então,*

$$\mathbb{F}(a) \cong \mathbb{F}(X).$$

Demonstração. Seja novamente $\varphi : \mathbb{F}[X] \to \mathbb{F}(a)$ a função que a cada polinômio $f \in \mathbb{F}[X]$ associa $f(a)$, o valor de f em a.

Como na Proposição 1.3.6, fácil verificar que φ é um homomorfismo de anéis. Note que, como a é transcendente, temos que $f(a) \neq 0$, para todo $f \in \mathbb{F}[X]$. Logo, $Ker(\varphi) = (0)$. Do Teorema do Homorfismo para anéis segue agora que $Im(\varphi) \cong \mathbb{F}[X]$.

Podemos estender φ a uma função $\overline{\varphi} : \mathbb{F}(X) \to F(a)$ de forma natural, definindo:

$$\overline{\varphi}\left(\frac{f}{g}\right) = \frac{f(a)}{g(a)}.$$

O leitor pode verificar facilmente que $\overline{\varphi}$ também é um homomorfismo e que $Ker(\overline{\varphi}) = 0$. Logo

$$\mathbb{F}(X) \cong Im(\overline{\varphi}).$$

Como $\mathbb{F}(X)$ é um corpo, temos que $Im(\overline{\varphi})$ também é um corpo e, como $Im(\overline{\varphi}) \subset \mathbb{F}(a)$ e $\mathbb{F}(a)$ é o menor corpo que contém $\mathbb{F}$ e contém a, temos que $Im(\overline{\varphi}) = \mathbb{F}(a)$. Logo:

$$\mathbb{F}(X) \cong \mathbb{F}(a).$$

□

Logo, temos provado o seguinte.

Corolario 1.3.12. *Se a é um elemento transcendente sobre um corpo $\mathbb{F}$, então:*

$$\mathbb{F}(a) = \left\{ \frac{f(a)}{g(a)} \mid f, g \in \mathbb{F}[X],\ g \neq 0 \right\}.$$

EXERCÍCIOS

---

1. Achar o polinômio minimal, sobre $\mathbb{Q}$, dos seguintes elementos:

   (i) $\sqrt{5}$.

   (ii) $\sqrt{2} + \sqrt{5}$.

   (iii) $\sqrt{1 + \sqrt{2}}$.

2. Provar que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

3. Sejam a e b elementos de uma extensão de $\mathbb{Z}_5$ tais que $a^2 = \overline{2}$ e $b^2 = \overline{3}$ (assuma, por enquanto, que tais elementos existem). Achar o polinômio minimal de $a + b$ sobre $\mathbb{Z}_5$.

4. Seja t um símbolo. Considere o conjunto de todos os elementos da forma $\mathbb{Z}_2(t) = \{a + bt \mid a, b \in \mathbb{Z}_2\}$. Mostre que, definindo a soma de dois elementos de $\mathbb{Z}_2(t)$ coeficiente a coeficiente e o produto do dois destes elementos distributivamente, com a convenção de que $t^2 = t + 1$, tem-se que $\mathbb{Z}_2(t)$ é um corpo com quatro elementos.

5. Mostre que o polinômio $f = X^2 + X + 1 \in Z_2[X]$ tem uma raiz no corpo $\mathbb{Z}_2(t)$ definido no exercício anterior.

6. Provar que o polinômio $X^2 + X + 1$ é irredutível em $\mathbb{Z}_2[X]$ e deduzir que o anel $\mathbb{Z}_2[X]/(X^2 + X + 1)$ é um corpo. Provar que este corpo é isomorfo ao corpo $\mathbb{Z}_2(t)$ definido no exercício 4.

7. Seja a uma raiz do polinômio $X^3 + X + 1 \in Z_2[X]$ em alguma extensão de $\mathbb{Z}_2$. Provar que o polinômio $X^3 + X^2 + 1 \in Z_2[X]$ tem uma raiz em $\mathbb{Z}_2(a)$.

8. Determinar a, b em $\mathbb{Q}$ tais que $(2 + \sqrt{3})^{-1} = a + b\sqrt{3}$.

9. Determinar a, b, c em $\mathbb{Q}$ tais que $(1 + \sqrt[3]{4})^{-1} = a + b\sqrt[3]{2} + c\sqrt[3]{4}$.

10. Determinar a, b, c em $\mathbb{Q}$ tais que $(1 + \sqrt[3]{2})(2 + \sqrt[3]{4})^{-1} = a + b\sqrt[3]{2} + c\sqrt[3]{4}$.

11. Calcular o grau de $\sqrt{2} + \sqrt{3}$ e de $\sqrt{2}\sqrt{3}$ determinando os respectivos polinômios minimais.

12. Determinar o grau de $\sqrt{3} + \sqrt[3]{5}$ sobre $\mathbb{Q}$.

13. Provar que $\mathbb{Q}(\sqrt{2})$ não é isomorfo a $\mathbb{Q}(\sqrt{3})$.

14. Determinar todos os automorfismos de $\mathbb{Q}(\sqrt{2})$ e de $\mathcal{Q}_8(\sqrt[3]{2})$.

15. Determinar todos os automorfismos de $\mathbb{Q}(\sqrt[3]{3})$ e de $\mathbb{Q}(\sqrt[3]{7})$.

16. (i) Provar que $\mathbb{R}(2 + i) = \mathbb{R}(5 + 2i)$.

    (ii) Provar que, se α é qualquer número complexo, então $\mathbb{R}(\alpha) = \mathbb{C}$.

17. Seja $\mathbb{F} \subset \mathbb{E}$ uma extensão de corpos e seja α um elemento de $\mathbb{E}$. Provar que, para todo elemento não nulo $a \in \mathbb{F}$, tem-se que $\mathbb{F}(\alpha) = \mathbb{F}(a + \alpha) = \mathbb{F}(a\alpha)$. Deduzir que, se $a \neq 0$ e b são elementos de $\mathbb{F}$ então $\mathbb{F}(\alpha) = \mathbb{F}(a\alpha + b)$.

18. Sejam $\mathbb{F} \subset \mathbb{E}$ corpos e sejam a e b elementos de $\mathbb{E}$. Provar que $\mathbb{F}(a)(b) = \mathbb{F}(b)(a) = \mathbb{F}(a, b)$.

19. Seja α um elemento algébrico sobre um corpo $\mathbb{F}$. Provar que α é algébrico sobre toda extensão $\mathbb{K}$ de $\mathbb{F}$.

20. Seja $f = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + a_nX^n$ um polinômio. Chama-se **recíproco** deste polinômio ao polinômio

$$f_R = X^n f(1/X) = a_0X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n.$$

(i) Provar que f é irredutível se e somente se f_R é irredutível.

(ii) Usar (i) para provar que um elemento α é algébrico sobre um corpo $\mathbb{F}$ se e somente se α^{-1} é algébrico sobre $\mathbb{F}$.

21. Um número complexo α diz-se um **número algébrico** se α é algébrico sobre $\mathbb{Q}$ e diz-se um **inteiro algébrico** se é raiz de um polinômio mônico, com coeficientes em $\mathbb{Z}[X]$. Provar que:

(i) O conjunto de todos os números algébricos é um subcorpo de $\mathbb{C}$.

(ii) Se α é um número algébrico, então existe um inteiro m tal que $m\alpha$ é um inteiro algébrico.

(iii) Se um número racional α é um inteiro algébrico, então α é um número inteiro.

Capítulo 2

Extensões de Corpos

2.1 Um pouco de Álgebra Linear

Seja $\mathbb{F} \subset \mathbb{E}$ uma extensão de corpos. Naturalmente, está definida uma operação de soma em $\mathbb{E}$. Por outro lado, também está definido o produto em $\mathbb{E}$ e, como $\mathbb{F} \subset E$, podemos nos restringir a considerar apenas o produto de elementos de $\mathbb{F}$ por elementos de $\mathbb{E}$. Pode-se afirmar então que está definido o produto de elementos de $\mathbb{E}$ por "escalares" de $\mathbb{F}$. Desta forma, pode-se considerar $\mathbb{E}$ como espaço vetorial sobre $\mathbb{F}$.

Esta simples observação nos permitirá fazer uso de idéias da álgebra linear para estudar extensões de corpos. Esta é, talvez, a ideia principal da memória de Steinitz [?] que citamos no capítulo anterior. Aliás, muitas das idéias hoje comuns em álgebra linear foram desenvolvidos por Steinitz para trabalhar com corpos e essa memória é hoje leitura obrigatória para os estudiosos da história da álgebra linear.

Para dar apenas um exemplo, mencionamos que Steinitz prova dois resultados que são hoje muito familiares para quem estuda esta área[1]:

(i) Se um espaço vetorial tem uma base com n elementos, então todo conjunto com mais de n elementos é linearmente dependente.

(ii) Todo conjunto de geradores de um espaço vetorial contém uma base.

Ele utiliza estes resultados para provar que todas as bases de um espaço vetorial (de dimensão finita) têm o mesmo número de elementos. Este último

[1] O leitor interessado na relevância do trabalho de Steinitz para a álgebra linear, pode consultar o interessante a artigo de Jean-Luc Dorier [?]

resultado apareceu antes num trabalho de Richard Dedekind (1831-1916), de 1893, onde estudava também extensões de corpos, mas os enunciados (i) e (ii) aparecem por primeira vez, explicitamente, na obra de Steinitz.

Definição 2.1.1. *Sejam $\mathbb{F} \subset \mathbb{E}$ corpos. Diz-se que $\mathbb{E}$ é uma* **extensão finita** *de $\mathbb{F}$ se $\mathbb{E}$, considerado como espaço vetorial sobre $\mathbb{F}$, é de dimensão finita.*

Neste caso, denotaremos a dimensâo de $\mathbb{E}$ sobre $\mathbb{F}$ por $[\mathbb{E} : \mathbb{F}]$.

No Corolário 1.3.9 do capítulo anterior, provamos que, se a é um elemento algébrico de grau n sobre um corpo $\mathbb{F}$, então:

$$\mathbb{F}(a) = \{x_0 + x_1 a + x_2 a^2 + \cdots + x_{n-1} a^{n-1} \mid x_i \in \mathbb{F},\ 1 \leq i \leq n-1\}.$$

Isto mostra que o conjunto de elementos $\{1, a, a^2, \ldots, a^{n-1}\}$ é um conjunto de geradores de $\mathbb{F}(a)$ sobre $\mathbb{F}$. Vamos provar que é, também, um conjunto linearmente independente.

De fato, suponha que existem elementos $\lambda_0, \lambda_1, \ldots, \lambda_{n-1}$ de $\mathbb{F}$, não todos nulos, tais que $\lambda_0 + \lambda_1 a + \lambda_2 a^2 + \cdots + \lambda_{n-1} a^{n-1} = 0$. Isto significa que a é raiz do polinômio $f = \lambda_0 + \lambda_1 X + \lambda_2 X^2 + \cdots + \lambda_{n-1} X^{n-1} \in \mathbb{F}[X]$.

Como f tem raiz a, tem-se que $m_a \mid f$ e, como $gr(m_a) = n > gr(f)$, deve ser $f = 0$, uma contradição.

Assim, temos mostrado o seguinte.

Teorema 2.1.2. *Sejam $\mathbb{F} \subset \mathbb{E}$ corpos e seja $a \in \mathbb{E}$ um elemento algébrico de grau n sobre $\mathbb{E}$. Então, o conjunto $\{1, a, a^2, \ldots, a^{n-1}\}$ é uma base de $\mathbb{F}(a)$ sobre $\mathbb{F}$ e*

$$[\mathbb{F}(a) : \mathbb{F}] = n.$$

Também podemos considerar elementos transcendentes desde este ponto de vista.

Teorema 2.1.3. *Sejam $\mathbb{F} \subset \mathbb{E}$ corpos e seja $a \in \mathbb{E}$ um elemento transcendente sobre $\mathbb{E}$. Então $\mathbb{F}(a)$ é de dimensão infinita sobre $\mathbb{F}$.*

Demonstração. Para provar nossa afirmação basta mostrar que o conjunto $A = \{1, a, a^2, \ldots, a^n, \ldots\}$ é linearmente independente. Como se trata de um conjunto infinito, a tese seguirá imediatamente.

Suponha, então, que existe a um subconjunto finito $\{1, a, \ldots, a^m\}$ de A, que é linearmente dependente. Então, existem elementos $\lambda_0, \lambda_1, \ldots, \lambda_m$ de $\mathbb{F}$, não todos nulos, tais que $\lambda_0 + \lambda_1 a + \lambda_2 a^2 + \cdots + \lambda_m a^m = 0$. Como acima, isto significa que a é raiz de $f = \lambda_0 + \lambda_1 X + \lambda_2 X^2 + \cdots + \lambda_m X^m$ que é um polinômio não nulo de $\mathbb{F}[X]$.

Consequentemente, a é algébrico sobre $\mathbb{F}$, uma contradição. □

Note que, juntos, os Teoremas 2.1.2 e 2.1.4 implicam o seguinte.

Corolario 2.1.4. *Sejam $\mathbb{F} \subset \mathbb{E}$ corpos e seja a um elemento de $\mathbb{E}$. Então a é algébrico sobre $\mathbb{F}$ se e somente se $\mathbb{F}(a)$ é uma extensão finita de $\mathbb{F}$.*

Definição 2.1.5. *Uma extensão de corpos $\mathbb{F} \subset \mathbb{E}$ diz-se uma* **extensão algébrica** *se todo elemento de $\mathbb{E}$ é algébrico sobre $\mathbb{F}$.*

O próximo resultado é relativamente simples, mas extremamente útil para estudar extensões de corpos.

Teorema 2.1.6. *Sejam $\mathbb{F} \subset \mathbb{K} \subset \mathbb{E}$ corpos. Então, $\mathbb{E}$ é uma extensão finita de $\mathbb{F}$ se e somente se $\mathbb{E}$ é uma extensão finita de $\mathbb{K}$ e $\mathbb{K}$ uma extensão finita de $\mathbb{F}$. Neste caso, tem-se que*

$$[\mathbb{E} : \mathbb{F}] = [\mathbb{E} : \mathbb{K}][\mathbb{K} : \mathbb{F}].$$

Demonstração. Num sentido, a demonstração é muito fácil. Se $[\mathbb{E}; \mathbb{F}]$ é finita, como $\mathbb{K}$ é um $\mathbb{F}$-subespaço de $\mathbb{E}$, também $[\mathbb{K} : \mathbb{F}]$ é finita. Ainda, qualquer base de $\mathbb{E}$ sobre $\mathbb{F}$ é, certamente, um conjunto de geradores de $\mathbb{E}$ sobre $\mathbb{K}$ (pois todo escalar de $\mathbb{F}$ é um escalar de $\mathbb{K}$. Como ela deve conter uma base de $\mathbb{E}$ sobre $\mathbb{F}$, segue que também $[\mathbb{E} : \mathbb{K}]$ é finita.

Para demonstrar a recíproca, exibiremos explicitamente uma base de $\mathbb{E}$ sobre $\mathbb{F}$.

Sejam

$$X = \{x_1, x_2, \ldots, x_n\} \quad \text{e} \quad Y = \{y_1, y_2, \ldots, y_m\}$$

uma base de $\mathbb{E}$ sobre $\mathbb{K}$ e uma base de $\mathbb{K}$ sobre $\mathbb{F}$ respectivamente.

Mostraremos que o conjunto de todos os produtos de elementos destas bases

$$YX = \{y_j x_i \mid 1 \leq j \leq m,\ 1 \leq i \leq n\}$$

é uma base de $\mathbb{E}$ sobre $\mathbb{F}$.

Provaremos inicialmente que este é um conjunto de geradores. De fato, dado $\alpha \in \mathbb{E}$, como Y é uma base de $\mathbb{E}$ sobre $\mathbb{K}$, existem elementos $b_1, b_2, \ldots, b_n$ em $\mathbb{K}$ tais que

$$\alpha = b_1 x_1 + b_2 x_2 + \cdots + b_n x_n.$$

Ainda, para cada índice $i,\ 1 \leq i \leq n$, como $b_i \in \mathbb{K}$ e Y é uma base de $\mathbb{K}$ sobre $\mathbb{F}$, existem elementos $a_{i1}, a_{i2}, \ldots, a_{im} \in \mathbb{F}$ tais que

$$b_i = a_{i1} y_1 + a_{i2} y_2 + \cdots + a_{im} y_m.$$

Logo, temos que

$$\alpha = \sum_{i=1}^{n} b_i x_i = \sum_{i=1}^{n} \left(\sum_{j=1}^{m} a_{ij} y_j \right) x_i = \sum_{ij} a_{ij} y_j x_i.$$

Consequentemente, YX é um conjunto gerador.

Provaremos finalmente que o conjunto também é linearmente independente sobre $\mathbb{F}$. Para isso, suponha que existem elementos $c_{ij} \in \mathbb{F}$ tais que

$$\sum_{ij} c_{ij} y_j x_i = 0.$$

Colocando em evidência cada elemento $x_i,\ 1 \leq i \leq n$, em todos os termos da soma em ele que comparece, podemos escrever

$$0 = \sum_{i=1}^{n} \left(\sum_{j_1}^{m} c_{ij} y_j \right) x_i.$$

Note agora que cada soma da forma $\left(\sum_{j=1}^{m} c_{ij} y_j \right)$ é um elemento de $\mathbb{K}$. Como X é uma base de $\mathbb{E}$ sobre $\mathbb{K}$, os elementos de X são linearmente independentes sobre $\mathbb{K}$. Logo, deve-se ter que

$$\sum_{j_1}^{m} c_{ij} y_j = 0 \quad \text{para cada índice } i \ \ 1 \leq i \leq m.$$

Finalmente, como os elementos de Y são linearmente independentes sobre $\mathbb{F}$. deve-se ter também que

$$c_{ij} = 0, \text{ para cada índice } i \text{ e par cada índice } j, 1 \leq i \leq n,\ 1 \leq j \leq m.$$

Logo, YX é um conjunto linearmente independente sobre $\mathbb{F}$ e, consequentemente, uma base de $\mathbb{E}$ sobre $\mathbb{F}$.

Note ainda que

$$[\mathbb{E} : \mathbb{F}] = |YX| = mn = [\mathbb{E} : \mathbb{K}][\mathbb{K} : \mathbb{F}].$$

□

Proposição 2.1.7. *Toda extensão finita $\mathbb{F} \subset \mathbb{E}$ é uma extensão algébrica.*

Demonstração. Seja $n = [\mathbb{E} : \mathbb{F}]$. Vamos provar que todo elemento $a \in \mathbb{E}$ é algébrico sobre $\mathbb{F}$. Seja $n = [\mathbb{E} : \mathbb{F}]$. Considere o conjunto

$$\{1, a, a^2, \ldots, a^n\}.$$

Como este conjunto tem $n + 1$ elementos, ele é linearmente dependente. Logo, existem elementos $\lambda_0, \lambda_1, \ldots, \lambda_n$ de $\mathbb{F}$, não todos nulos, tais que

$$\lambda_0 + \lambda_1 a + \lambda_2 a^2 + \cdots + \lambda_n a^n = 0.$$

Isto significa que a é raiz de $f = \lambda_0 + \lambda_1 X + \lambda_2 X^2 + \cdots + \lambda_n X^n$ que é um polinômio não nulo de $\mathbb{F}[X]$.

Consequentemente, a é algébrico sobre $\mathbb{F}$. □

Este resultado permite estabelecer um fato interessante.

Proposição 2.1.8. *Sejam $\mathbb{F} \subset \mathbb{E}$ corpos e sejam $a, b \in \mathbb{E}$ elementos algébricos sobre $\mathbb{F}$. Então $a \pm b$ e ab são algébricos sobre $\mathbb{F}$. Ainda, se $a \neq 0$, então a^{-1} também é algébrico sobre $\mathbb{F}$.*

Demonstração.

Sejam m_a e m_b os polinomios minimais de a e b sobre $\mathbb{F}$ e sejam r e s seus graus respectivos. Então $[\mathbb{F}(a) : \mathbb{F}] = r$. Ainda, como m_b é um polinômio de $\mathbb{F}[X] \subset \mathbb{F}(a)[X]$ e tem raiz b, o polinômio minimal de b sobre $\mathbb{F}(a)$ é um divisor de m_b. Se denotamos por t o seu grau, temos que $t \leq s$ e, portanto, $[\mathbb{F}(a, b); \mathbb{F}(a)] \leq s$. Consequentemente

$$[\mathbb{F}(a, b) : \mathbb{F}] = [\mathbb{F}(a, b) : \mathbb{F}(a)][\mathbb{F}(a) : \mathbb{F}] \leq rs.$$

Este argumento mostra que $\mathbb{F}(a,b)$ é uma extensão algébrica de $\mathbb{F}$. Pelo teorema anterior tanto $a \pm b$ quanto ab, que são elementos de $\mathbb{F}(a,b)$, são algébricos sobre $\mathbb{F}$.

Ainda, como $\mathbb{F}(a)$ é um corpo que contém a, temos que $a^{-1} \in \mathbb{F}$. □

Da proposição acima segue imediatamente o seguinte.

Corolario 2.1.9. *Sejam $\mathbb{F} \subset \mathbb{E}$ corpos. O conjunto de todos os elementos de $\mathbb{E}$ que são algébricos sobre $\mathbb{F}$ é um subcorpo de $\mathbb{E}$.*

Definição 2.1.10. *Sejam $\mathbb{F} \subset \mathbb{E}$ corpos. O subcorpo de $\mathbb{E}$ formado por todos os elementos que são algébricos sobre $\mathbb{F}$ chama-se o* **fecho algébrico de** $\mathbb{F}$ *em* $\mathbb{E}$.

Em particular, os números complexos que são algébricos sobre $\mathbb{Q}$ chamam-se **números algébricos** *e o conjunto de todos eles diz-se o* **corpo dos números algébricos**.

EXERCÍCIOS

---

1. Provar que $\{1, \sqrt{2}, \sqrt{5}, \sqrt{10}\}$ é uma base de $\mathbb{Q}(\sqrt{2}, \sqrt{5})$ sobre $\mathbb{Q}$.
2. Determinar uma base de $\mathbb{Q}(\sqrt{3} + \sqrt{5})$ sobre $\mathbb{Q}$.
3. Provar que $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \ldots, \sqrt[n]{2}, \ldots)$ é uma extensão algébrica de $\mathbb{Q}$, mas não é uma extensão finita.
4. Determinar uma base de $\mathbb{Q}(\sqrt{3} + \sqrt{5})$ sobre $\mathbb{Q}(\sqrt{15})$.
5. Sejam $\mathbb{F} \subset \mathbb{E}$ corpos tais que $[\mathbb{E} : \mathbb{F}] = p$, onde p é um inteiro primo. Provar que, para todo elemento $\alpha \in \mathbb{E}$ tem-se que $\alpha \in \mathbb{F}$ ou $\mathbb{F}(\alpha) = \mathbb{E}$.
6. Seja $\mathbb{F} \subset \mathbb{E}$ uma extensão de corpos e sejam α e β elementos de $\mathbb{E}$, algébricos sobre $\mathbb{F}$, de graus n e m respectivamente. Provar que, se $mdc(m,n) = 1$ então $[\mathbb{F}(a,b) : \mathbb{F}] = mn$.

7. Dar um exemplo elementos α e β de graus n e m sobre $\mathbb{Q}$ tais que $[\mathbb{Q}(\alpha,\beta] : \mathbb{Q}] \neq mn$.

8. Provar que se α é um elemento algébrico sobre um corpo $\mathbb{F}$ e β é uma raiz n-ésima de α em alguma extensão de $\mathbb{F}(\alpha)$, então β é algébrico sobre $\mathbb{F}$.

9. Sejam $\mathbb{F} \subset \mathbb{K} \subset \mathbb{E}$ corpos e seja $\alpha \in \mathbb{E}$ um elemento que é raiz de um polinômio de $\mathbb{K}[X]$. Provar que, se $\mathbb{K}$ é algébrico sobre $\mathbb{F}$ então também α é algébrico sobre $\mathbb{F}$.

10. Sejam α e β elementos de uma extensão de um corpo $\mathbb{F}$. Provar que α e β são algébricos sobre $\mathbb{F}$ se e somente se $\alpha+\beta$ e $\alpha\beta$ são algébricos sobre $\mathbb{F}$.

11. Um inteiro diz-se *livre de quadrados* se não é divisível pelo quadrado de nenhum número inteiro.

    (i) Seja $m = p_1^{n_1} p_2^{n_2} \cdots p_t^{n_t}$ a decomposição de um inteiro m como produto de primos, diferentes dois a dois. Provar que m é livre de quadrados se e somente se $n_i = 1, 1 \leq i \leq t$.

    (ii) Seja $\mathbb{E} \subset \mathbb{C}$ um corpo tal que $[\mathbb{E} : \mathbb{C}] = 2$. Provar que existe um inteiro m, livre de quadrados, tal que $\mathbb{E} = \mathbb{Q}(\sqrt{m})$.

12. Sejam $\mathbb{F} \subset \mathbb{E}$ corpos tais que $[\mathbb{E} : \mathbb{F}] = 2$. Prove que existe um elemento $\alpha \in \mathbb{E}$ tal que $\alpha^2 \in \mathbb{F}$ e $\mathbb{E} = \mathbb{F}(\alpha)$.

13. Sejam $\mathbb{F} \subset \mathbb{E}$ corpos. Provar que $\mathbb{E}$ é uma extensão finita de $\mathbb{F}$ se e somente se existem elementos $\alpha_1, \alpha_2, \ldots, \alpha_n$ em $\mathbb{E}$ tais que $\mathbb{E} = \mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

14. Seja $\mathbb{F}$ um corpo. Provar que o conjunto $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$ é um grupo abeliano em relação ao produto de $\mathbb{F}$. Provar que, se este grupo é cíclico, então $\mathbb{F}$ é um corpo finito.

15. Sejam $\mathbb{F}, \mathbb{K}$ e $\mathbb{E}$ subcorpos de um corpo Ω e suponha que $\mathbb{E}$ e $\mathbb{K}$ contém $\mathbb{F}$. Mostre que, se $\mathbb{E}$ é uma extensão finita de $\mathbb{F}$ então $\mathbb{EK} = \mathbb{E}(\mathbb{K}) = \mathbb{K}(\mathbb{E})$ é uma extensão finita de $\mathbb{K}$ e que $[\mathbb{EK} : \mathbb{K}] \leq [\mathbb{E} : \mathbb{F}]$. (Sugestão: mostre que se $\{b_1, b_2, \ldots, b_n\}$ é uma base de $\mathbb{E}$ sobre $\mathbb{F}$, então também é um conjunto de geradores de $\mathbb{EK}$ sobre $\mathbb{K}$.)

16. Seja $\mathbb{F} \subset \mathbb{E}$ uma extensão algébrica. Prove que, se a família

$$\{\mathbb{K} \mid \mathbb{F} \subset \mathbb{K} \subset \mathbb{E},\ \mathbb{K} \text{ é um corpo } \}$$

    é finita, então a dimensão de $\mathbb{E}$ sobre $\mathbb{F}$ é finita.

17. Seja $\mathbb{F}$ um corpo de característica $p > 0$ e seja α um elemento de uma extensão de $\mathbb{F}$. Provar que $\mathbb{F}(\alpha) = \mathbb{F}$ se e somente se existe um inteiro positivo n tal que $\alpha^{p^n} = \alpha$.

18. Sejam $\mathbb{F}, \mathbb{K}$ e $\mathbb{E}$ corpos. Provar que se $\mathbb{E}$ é uma extensão algébrica de $\mathbb{K}$ e $\mathbb{K}$ é uma extensão algébrica de $\mathbb{F}$, então $\mathbb{E}$ é uma extensão algébrica de $\mathbb{F}$.

2.2 Raízes de polinômios

A teoria de polinômios demorou a se tornar clara para os matemáticos. Um fato interessante é que, embora o fato se suspeitasse de longa data, não havia uma prova convincente de que um polinômio de grau n tem, no máximo, n raizes. Como veremos, isto segue facilmente de nosso próximo teorema, devido a René Descartes (1596-1650) de 1637. Naturalmente, nós o enunciamos em termos mais atuais.

Teorema 2.2.1. (Teorema do Resto) *Seja $\mathbb{F} \subset \mathbb{E}$ corpos e seja f um polinômio com coeficientes em $\mathbb{F}$. Dado um elemento $\alpha \in \mathbb{E}$, o resto de dividir f por $X - \alpha$, em $\mathbb{E}[X]$ é $f(\alpha)$.*

Demonstração. De fato, pelo Algoritmo de Euclides temos que existem $q, r \in \mathbb{E}[X]$ tais que $f = (X - \alpha)q + r$, com $r = 0$ ou $gr(r) = 0$, uma vez que o grau do divisor, $X - \alpha$, é igual a 1. Logo;

$$f(\alpha) = (\alpha - \alpha)q(\alpha) + r = r.$$

□

Como consequência imediata deste resultado temos o seguinte.

Corolario 2.2.2. *Seja $\mathbb{F} \subset \mathbb{E}$ corpos e seja f um polinômio com coeficientes em $\mathbb{F}$. Dado um elemento $\alpha \in \mathbb{E}$ é raiz de f se e somente se f é divisível por $X - \alpha$.*

Se α é uma raiz de f, então $(x - \alpha)$ divide f . Logo, existe o maior iteiro positivo m tal que $(X - \alpha)^m$ que divide f, já que, necessariamente $m \leq gr(f)$. Esta observação permite definir a *multiplicidade* de uma raiz. O fato de que um polinômio pode ter raízes múltiplas foi notado, por primeira vez, por Girólamo Cardano (1501-1576) na sua *Ars Magna*, de 1545, uma das obras de importância fundamental para o desenvolvimento da álgebra.

Definição 2.2.3. *Seja $\mathbb{F}$ um corpo e seja f polinômio com coeficientes em $\mathbb{F}$. Um elemento α numa extensão $\mathbb{E}$ de $\mathbb{F}$ diz-se uma* **raiz múltipla** *de f se existe um inteiro $n > 1$ tal que $(X-\alpha)^n$ divide f e $(X-\alpha)^{n+1}$ não divide f. Neste caso, o inteiro n diz-se a* **multiplicidade** *de α como raiz de f.*

Uma raiz de multiplicidade 1, diz-se uma **raíz simples** *de f.*

Teorema 2.2.4. *Sejam $\mathbb{F}$ um corpo e f polinômio de grau n com coeficientes em $\mathbb{F}$. Então, f possui, no máximo, n raízes (contadas com suas respectivas multiplicidades) em qualquer extensão $\mathbb{E}$ de $\mathbb{F}$; isto é, f se decompoe em $\mathbb{E}[X]$ na forma*

$$f = (X-\alpha_1)^{m_1}(X-\alpha_2)^{m_2}\cdots(X-\alpha_t)^{m_t}h,$$

onde $m_1 + m_2 + \cdots m_t \leq n$ e h não tem raízes em $\mathbb{E}$.

Demonstração. Provaremos o enunciado por indução em n, o grau do polinômio f.

Se $n = 1$ então $f = aX + b$ com $a, b \in \mathbb{F}$ e $\alpha = -b/a$ é a única raiz de f, em qualquer extensão $\mathbb{E}$ de $\mathbb{F}$.

Suponha então que o enunciado vale para qualquer polinômio de grau menor que f. Seja $\mathbb{E}$ uma extensão qualquer de $\mathbb{F}$ e sejam $\alpha_1, \alpha_2, \ldots \alpha_t$ as raízes distintas de f em $\mathbb{E}$. Seja m_1 a multiplicidadae de α_1 como raiz de f. Então podemos escrever

$$f = (X-\alpha_1)^{m_1}g, \quad \text{com} \quad g \in \mathbb{E}[X], \tag{2.1}$$

onde $gr(g) = n - m < n$.

Afirmamos que α_1 não é raiz de g. De fato, se $g(\alpha_1) = 0$, pelo Corolário 2.2.2 podemos escrever $g = (X-\alpha_1)g_1$, com $g_1 \in \mathbb{E}[X]$ donde $f = (x-\alpha_1)^{m+1}g_1$, contradizendo o fato de que a multiplicidade de α_1 é m_1.

Dada qualquer outra raiz α_i, $2 \leq i \leq t$ de f, temos que $0 = f(\alpha_i) = (\alpha_i - \alpha_1)g(\alpha_i)$ donde α_i é raiz de g. Por outro lado, a equação (2.1) mostra que toda raiz de g é raiz de f. Assim, as raizes de g em $\mathbb{E}$ são precisamente os elementos $\alpha_2, \ldots \alpha_t$. Sejam $m_2, \ldots, m_t$ as respectivas multiplicidades.

Pela hipótese de indução temos que

$$g = (X - \alpha_2)^{m_2} \cdots (X - \alpha_t)^{m_t} h, \quad \text{onde } m_2 + \cdots + m_t < n - m_1,$$

e h não tem raízes em $\mathbb{E}$.

Logo:

$$f = (X - \alpha_1)^{m_1} (X - \alpha_2)^{m_2} \cdots (X - \alpha_t)^{m_t} h,$$

onde $m_1 + m_2 + \cdots + m_t = n + gr(g) < m_1 + n - m_1 = n$. □

Definição 2.2.5. *Sejam $\mathbb{F}$ um corpo e $f \in \mathbb{F}[X]$ um polinômio não constante. Um corpo $\mathbb{E}$ diz-se um* **corpo de decomposição** *para f se este polinômio se decompõe como um produto de fatores lineares em $\mathbb{E}[X]$; isto é, se*

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

com $a_i \in \mathbb{E}$, $1 \leq i \leq n$.

Note que, quando isto acontece, n é o grau de f, a é o coeficiente do termo de maior grau de f e $\alpha_1 \ldots, \alpha_n$ são n raízes de f (não necessariamente diferentes dois a dois). Neste caso, diz-se que f tem todas suas raízes em $\mathbb{E}$.

Definição 2.2.6. *Sejam $\mathbb{F}$ um corpo e $f \in \mathbb{F}[X]$ um polinômio não constante. Um corpo $\mathbb{E}$ diz-se um* **corpo de raízes** *de f sobre $\mathbb{F}$ se $\mathbb{E}$ é um corpo de decomposição para f e para todo corpo $\mathbb{K}$ tal que $\mathbb{F} \subset \mathbb{K} \subset \mathbb{E}$ que é um corpo de decomposição para f, tem-se que $\mathbb{K} = \mathbb{E}$.*

Lema 2.2.7. *Sejam $\mathbb{F}$ um corpo e $f \in \mathbb{F}[X]$ um polinômio não constante. Seja ainda $\mathbb{E}$ um corpo que contém $\mathbb{F}$. Se $\mathbb{E}$ é um corpo de decomposição para f, então $\mathbb{K} = \mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_n) \subset \mathbb{E}$ é um corpo de raízes de f sobre $\mathbb{F}$.*

Demonstração. Se $\mathbb{E}$ é um corpo de decomposição para f então podemos escrever

$$f = a(X - \alpha_1)(x - \alpha_2)\cdots(X - \alpha_n), \quad \text{com} \quad \alpha_i \in \mathbb{E},\ 1 \leq i \leq n.$$

Então, o corpo $\mathbb{K} = \mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ é um corpo de decomposição para f e, claramente, $\mathbb{K} \subset \mathbb{E}$.

Por outro lado, se $\mathbb{K}' \subset \mathbb{K}$ é um corpo de decomposição para f, então $\mathbb{K}'$ contém $\mathbb{F}$ e, necessáriamente, contém todas as raízes $a_1,\ 1 \leq i \leq n$ de f. Portanto $\mathbb{K}' \supset \mathbb{K}$ e segue a igualdade. □

Podemos utilizar os resultados desta seção para caracterizar corpos que não tem nenhuma extensão algébrica própria.

Definição 2.2.8. *Um corpo $\mathbb{F}$ diz-se* **algebricamente fechado** *se todo polinômio não constante $f \in \mathbb{F}[X]$ tem uma raiz em $\mathbb{F}$.*

Teorema 2.2.9. *Seja $\mathbb{F}$ um corpo. As seguintes afirmações são equivalentes:*

(i) $\mathbb{F}$ é algébricamente fechado.

(ii) Todo polinômio não constante $f \in \mathbb{F}[X]$ se decompõe como produto de fatores lineares em $\mathbb{F}[X]$.

(iii) Todo polinômio irredutível em $\mathbb{F}[X]$ tem grau 1.

Demonstração.

$(i) \Rightarrow (ii)$.

Faremos a demonstração por indução no grau do polinômio considerado. Si o polinômio tem grau 1, então ele próprio é linear e o resultado é trivialmente válido.

Seja f
$in\mathbb{F}[X]$ um polinômio não constante. Então $gr(f) = n > 1$ e vamos admitir, como hipótese de indução, que o resultado vale para polinomios de grau $n - 1$. Como $\mathbb{F}$ é algébricamente fechado, ele tem uma raiz $a \in \mathbb{F}$. Pelo Corolário 2.2.2, podemos escrever

$$f = (X - a)g, \quad \text{com } g \in \mathbb{F}[X],\ gr(g) = n - 1.$$

Pela hipótes de indução, g é um produto de fatores lineares e, como $X - a$ também é linear, segue a tese.

$(ii) \Rightarrow (iii)$ é imediata.
$(iii) \Rightarrow (i)$
Sabe-se que, se $\mathbb{F}$ é um corpo, então $\mathbb{F}[X]$ é um anel fatorial; i.e., todo polinômio não constante de $\mathbb{F}[X]$ é um produto de polinômios irredutíveis. Como estamos assumindo que vale (ii), todo polinômio não constante f é um produto de fatores lineares. Cada fator linear tem uma raiz em $\mathbb{F}$, que é também raiz de f, donde a tese segue imediatamente. □

Corolario 2.2.10. *Seja $\mathbb{F}$ um corpo algébricamente fechado. Se $\mathbb{E}$ é uma extensão algébrica de $\mathbb{F}$, então $\mathbb{E} = \mathbb{F}$.*

Demonstração. De fato, seja $\mathbb{E}$ uma extensão algébrica de $\mathbb{F}$. Dado um elemento $\alpha \in E$, ele é algébrico sobre $\mathbb{F}$. Seja $f \in \mathbb{F}[X]$ o polinômio minimal de α e seja n o grau de f. Pelo teorema acima, f é da forma:

$$f = a(X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_n) \quad \text{com} \quad \alpha_i, \in \mathbb{F},\ 1 \leq i \leq n.$$

Como $f(a) = 0$, existe um índice i tal que $\alpha - \alpha_i = 0$ donde $\alpha = \alpha_i \in \mathbb{F}$. Assim, todo elemento α de $\mathbb{E}$ pertence a $\mathbb{F}$, o que implica que $\mathbb{E} = \mathbb{F}$. □

O corpo $\mathbb{C}$ dos números complexos é algébricamente fechado. Este fato foi provado por Carl Frederich Gauss em 1799, na sua tese de doutoramento, quando ele tinha apenas 22 anos de idade. Ao longo de sua vida, Gauss deu outras três provas diferentes deste resultado, que se tornou conhecido como o *Teorema Fundamental da Álgebra*. Hoje em dia, existem mais de 100 provas conhecidas deste teorema.

EXERCÍCIOS

---

1. Seja f um polinômio com coeficientes reais. Provar que, se um número complexo $\alpha = a + bi$ é raiz de f então o conjugado $\overline{\alpha} = a - bi$ também é raiz de f. Mostrar que $(X - \alpha)(X - \overline{\alpha}) \in \mathbb{R}[X]$.

2. Provar que se $f \in \mathbb{R}[X]$ é um polinômio irredutível, então $gr(f) = 1$ ou $gr(f) = 2$.

3. Determinar todas as raízes do polinômio $X^4 + X^2 + 1$ em $\mathbb{Q}(i\sqrt{3})$.

4. Sejam $\mathbb{F} \subset \mathbb{E}$ corpos e $f \in \mathbb{F}[X]$ um polinômio não constante. Provar que, se $\alpha \in \mathbb{E}$ é uma raiz de multiplicidade m de f, então f pode-se escrever em $\mathbb{E}[X]$ na forma $f = (X - \alpha)^m g$, onde $g(\alpha) \neq 0$.

5. Seja $f = a_0 + a_1X + a_2X^4 + \cdots + a_{n-1}X^{n-1} + a_nX^n$ um polinômio com coeficientes reais. Na sua obra extraordinária, *La Geometrie*, de 1637, Descartes deu uma regra, sem demonstração, de como calcular o número de raízes positivas e negativas da equação $f = 0$. Este resultado é conhecido hoje como *regra dos sinais de Descartes* e pode ser enunciado da seguinte forma:

   > *Seja t o número de trocas de sinal na sequência dos coeficentes de f e seja p o número de raizes reais positivas de f. Então $t - r$ é um inteiro positivo, par.*
   >
   > *Em particular, se todas as raízes de f são reais, então $p = t$.*

   (i) Prove esta afirmação, diretamente, para polinômios de grau 1 e 2.

   (ii) Prove a regra de Descartes em geral, usando indução. (Sugestão: considere primeiro o caso em que $a_0 < 0$ e use o teorema de Bolzano para concluir que f tem uma raiz real e positiva. No caso em que $a_0 > 0$ considere separadamente os casos em que $p = 0$ e $p > 0$.)

6. Prove que o fecho algébrico de $\mathbb{Q}$ em $\mathbb{C}$ é o corpo dos números algébricos.

7. Seja $\mathbb{F}$ um corpo finito. Provar que $\mathbb{F}$ não é algébricamente fechado.

8. Seja $\mathbb{K}$ o fecho algébrico de $\mathbb{Q}$ em $\mathbb{R}$. Provar que $\mathbb{K}$ tem dimensão infinita sobre $\mathbb{Q}$.

2.3 O corpo de raízes de um polinômio

Os números complexos foram introduzidos por Rafael Bombelli (1526-1573) em 1572, para resolver equações de terceiro grau. Logo encotraram

aplicações em diversos ramos da ciência, mas as dúvidas quanto a sua legitimidade permaneceram até que William Rowan Hamilton apresentou, em 1833, a fundamentação, hoje bem conhecida, de considerar os números complexos como pares ordenados de números reais com as operações entre pares definidas por

$$\begin{aligned}(a,b)+(c,d) &= (a+b,c+d),\\ (a,b)\cdot(c,d) &= (ac-bd,ad+bc).\end{aligned}$$

Em 1847, Agustin Cauchy (1789-1857) deu outra construção, usando apenas congruências entre polinômios. Na linguagem atual, sua idéia foi a seguinte. Primeiro observou que o polinômio X^2+1 é irredutível em $\mathbb{R}[X]$, pois é de segundo grau e não tem raízes nesse corpo. Considerou então o anel quociente

$$R=\frac{\mathbb{R}[X]}{(X^2+1)}.$$

Dado um polinômio qualquer $f\in\mathbb{R}[X]$ dividindo por X^2+1 tem-se um quociente q é um resto da forma $r=a+bX$ (pois gr(r)$<$2). Como $f=(X^2+1)q+r$ temos que $\overline{f}=\overline{a+bX}$ em R.

Desta forma, temos que $R=\{a+b\overline{X}\mid a,b\in\mathbb{R}\}$.

Ainda, como $\overline{X^2+1}=0$ em R temos que $\overline{X}^2=-1$ e R é isomorfo ao corpo $\mathbb{C}$ dos números complexos.

Anos mais tarde, em 1887, Leopold Kroneker (1832-1891) generalizou está técnica para mostrar como construir uma raiz de um polinômio qualquer com coeficientes num corpo arbitrário.

Teorema 2.3.1. *Seja $\mathbb{F}$ um corpo e seja f um polinômio não constante, com coeficientes em $\mathbb{F}$. Então, existe uma extensão $\mathbb{E}$ de $\mathbb{F}$ tal que f tem uma raiz em $\mathbb{E}$.*

Demonstração. Inicialmente, observamos que é suficiente provar o teorema para polinômios irredutíveis. De fato, se o teorema vale para irredutíveis e f não o é, tomamos um fator irredutível de f. Este fator tem uma raiz que, naturalmente, é também raiz de f.

Assim, daqui em diante, vamos assumir que $f=a_0+a_1X+\cdots+a_nX^n\in\mathbb{F}[X]$ é um polinônio irredutível.

Consideramos então o anel quociente

$$\mathbb{E} = \frac{\mathbb{F}[X]}{(f)}.$$

Note que, como f é irredutível, $\mathbb{E}$ é um corpo.

Ainda, se $i : \mathbb{F} \to \mathbb{F}[X]$ indica a inclusão natural e $\omega : \mathbb{F}[X] \to \frac{\mathbb{F}[X]}{(f)}$ indica o homomorfismo canônico, a função $\phi = \omega \circ i$ leva $\mathbb{F}$ num subcorpo $\mathbb{F}'$ de $\mathbb{E}$, que é isomorfo a $\mathbb{F}$ e tem-se que $\mathbb{F}' \subset \mathbb{E}$. Daqui em diante, vamos identificar $\mathbb{F}$ com sua imagem isomorfa $\mathbb{F}'$, em $\mathbb{E}$.

Seja agora $\alpha = \overline{x}$, a classe do polinômio X no quociente $\mathbb{F}[X]/(f)$.

Como $\overline{f} = 0$ em $\mathbb{E} = \mathbb{F}[X]/(f)$, tem-se que

$$\begin{aligned} 0 = \overline{f} &= \overline{a_0 + a_1 X + \cdots + a_n X^n} \\ &= a_0 + a_1 \overline{X} + \cdots + a_n \overline{X}^n \\ &= a_0 + a_1 \alpha + \cdots + a_n \alpha^n. \end{aligned}$$

Esta igualdade mostra que $\alpha \in \mathbb{E}$ é uma raiz de f. □

Nas condições do teorema acima, se α é ume raiz de f então, necessáriamente, f deve ser o polinômio minimal de α sobre $\mathbb{F}$. De fato, o polinômio f tem raiz α e é irredutível; logo, é o seu polinômio minimal.

Do Corolário 1.3.9 segue que

$$\mathbb{E} = \frac{\mathbb{F}[X]}{(f)} \cong \mathbb{F}(\alpha).$$

Ainda, tem-se que

$$\mathbb{F}(\alpha) = \{x_0 + x_1 a + x_2 a^2 + \cdots + x_{n-1} a^{n-1} \mid x_i \in \mathbb{F},\ 1 \leq i \leq n-1\},$$

e, como $f(\alpha) = 0$ temos que

$$\alpha^n = -a_0 - a_1 X - \cdots - a_n X^n.$$

Naturalmente, é fácil somar elementos de $\mathbb{F}(\alpha)$, coeficiente a coeficiente. A observação acima permite também multiplicar facilmente elementos de $\mathbb{F}(\alpha)$.

Exemplo 2.3.2.

Considere o polinômio $X^3 + X + 1$ que é irredutível em $\mathbb{F}_2[X]$. De fato, note que, se fosse redutível teria, necessariamente, um factor de primeiro grau e, portanto, uma raiz em $\mathbb{F}_1$. É fácil verificar, diretamente, que nenhum dos dois elementos de $\mathbb{F}_2$ é raiz de f. Seja α é uma raiz de f. Temos que

$$\mathbb{F}(\alpha) = \{a_0 + a_1\alpha + a_2\alpha^2 \mid a_i \in \mathbb{F}_2,\ 0 \leq i \leq 2\}.$$

Vamos multiplicar os elemento: $\gamma_1 = 1 + \alpha + \alpha^2$ e $\gamma_2 = 1 + \alpha^2$.

Temos

$$\gamma_1.\gamma_2 = (1 + \alpha + \alpha^2)(1 + \alpha^2) = 1 + \alpha + \alpha^2 + \alpha^2 + \alpha^3 + \alpha^4 = 1 + \alpha + \alpha^3 + \alpha^4.$$

Como $\alpha^3 = 1 + \alpha$ e $\alpha^4 = \alpha\alpha^3 = \alpha + \alpha^2$ temos:

$$\gamma_1.\gamma_2 = 1 + \alpha + 1 + \alpha + \alpha + \alpha^2 = \alpha + \alpha^2.$$

O leitor particularmente cuidadoso deve ter notado que, na verdade, não provamos que existe uma extensão de $\mathbb{F}$ em que f tem raízes, mas uma extensão de uma cópia isomorfa de $\mathbb{F}$. Para provar o enunciado, ao pé da letra, veja o Exercício 2.

Agora estamos em condições de provar a existência do corpo de raiízes de um polinômio dado.

Teorema 2.3.3. *Seja $\mathbb{F}$ um corpo e seja f um polinômio não constante, com coeficientes em $\mathbb{F}$. Então, existe uma extensão $\mathbb{E}$ de $\mathbb{F}$ que é um corpo de raízes para f.*

Demonstração. Faremos a demonstração ppor indução no grau de f. Se $gr(f) = 1$ então $F = aX + b$ com$a, b \in \mathbb{F}$ e $\alpha = -b/a \in \mathbb{F}$ é a única raiz de f, Logo, o próprio $\mathbb{F}$ é um corpo de raízes de f sobre $\mathbb{F}$,

Suponhamos então $gr(f) = n > 1$ e que o teorema vale para polinômios de grau menor. Pelo Teorema 2.3.1, existe uma extensão $\mathbb{K}$ de $\mathbb{F}$ tal que f tem uma raiz α_1 em $\mathbb{K}$. Então, podemos escrever f na forma

$$f = (X - \alpha_1)h,$$

onde $h \in E[X]$ com $gr(h) = n - 1 < gr(f)$. Pela hipótese de indução, existe uma extensão $\mathbb{E}$ de $\mathbb{K}$ tal que h é um produto de fatores lineares

$$h = (X - \alpha_2) \cdots (X - \alpha_n)$$

em $\mathbb{E}[X]$. Portanto,

$$f = (X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_n)$$

em $\mathbb{E}[X]$.

Conforme vimos na demonstração do Lema 2.2.6, o corpo $\mathbb{F}9\alpha_1, \alpha_2, \ldots, \alpha_n)$ é um corpo de raízes de f sobre $\mathbb{F}$. □

Nossa intenção, daqui em diante, é demonstrar que dois corpos de raízes de um polinômio f sobre um corpo $\mathbb{F}$ são isomorfos. Para isso, vamos introduzir ainda alguns conceitos.

Definição 2.3.4. *Sejam $\mathbb{E}_1$ e $\mathbb{E}_2$ duas extensões de um corpo K. Uma função $\varphi : \mathbb{E}_1 \to \mathbb{E}_2$ diz se um* **$\mathbb{F}$-isomorfismo** *se φ é um isomorfismo de corpos e φ, restrito a $\mathbb{F}$, é a função identidade; isto é, se $\varphi(x) = x$ para todo $x \in \mathbb{F}$.*

Podemos definir também um conceito levemente mais geral.

Definição 2.3.5. *Sejam $\mathbb{F}_1 \subset \mathbb{E}_1$ e $\mathbb{F}_2 \subset \mathbb{E}_2$ corpos e seja $\varphi : \mathbb{F}_1 \to \mathbb{F}_2$ um isomorfismo de corpos. Diz-se que φ pode se* **estender** *a um isomorfismo de $\mathbb{E}_1$ em $\mathbb{E}_2$ se existe uma função $\psi : \mathbb{E}_1 \to \mathbb{E}_2$ que é um isomorfismo de corpos e tal que, restrita a $\mathbb{E}_1$ coincide com φ; isto é, se $\psi(x) = \varphi(x)$ para todo $x \in \mathbb{F}_1$.*

Dado um isomorfismo de corpos $\varphi : \mathbb{F}_1 \to \mathbb{F}_2$, para cada polinômio $f = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{F}_1[X]$ definimos o polinômio

$$f^* = \varphi(a_0) + \varphi(a_1)X + \cdots + \varphi(a_n)X^n \in F_2[X].$$

É fácil verificar diretamente que, se $f, g \in \mathbb{F}_1[X]$, então:

$$(fg)^* = f^* g^*.$$

Em particular, isto implica que, se f é irredutível em $\mathbb{F}_1[X]$, então f^* é irredutível em $\mathbb{F}_2[X]$.

Sejam $\mathbb{F}_1 \subset \mathbb{E}_1$ e $\mathbb{F}_2 \subset \mathbb{E}_2$ corpos. Dado um polinômio irredutível $f = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{F}_1[X]$, consideramos $f^* = \varphi(a_0) + \varphi(a_1)X + \cdots + \varphi(a_n)X^n$ como acima.

Sejam $\alpha_1 \in \mathbb{E}_1$ e $\alpha_2 \in \mathbb{E}_2$ raízes de f e f^* respectivamente. Então, como mostramos no Teorema 2.1.2, o conjunto $\{1, a_1, a_1^2, \ldots, a_1^{n-1}\}$ é uma base de $\mathbb{F}_1(\alpha_1)$ sobre $\mathbb{F}_1$ e, da mesma forma, $\{1, a_2, a_2^2, \ldots, a_2^{n-1}\}$ é uma base de e $\mathbb{F}_2(\alpha_2)$ sobre $\mathbb{F}_2$.

Podemos definir uma função $\Phi : \mathbb{F}_1(\alpha_1) \to \mathbb{F}_2(\alpha_2)$ da seguinte forma:

Dado um elemento

$$x = \lambda_0 + \lambda_1 a_1 + \lambda_2 a_1^2 + \cdots \lambda_{n-1} a_1^{n-1} \in \mathbb{F}_1(\alpha_1),$$

definimos:

$$\Phi(x) = \varphi(\lambda_0) + \varphi(\lambda_1)a_2 + \varphi(\lambda_2)a_2^2 + \cdots + \varphi(\lambda_{n-1})a_2^{n-1} \in \mathbb{F}_2(\alpha_2).$$

Lema 2.3.6. *Com as notações acima, a função $\Phi : \mathbb{F}_1(\alpha_1) \to \mathbb{F}_2(\alpha_2)$ é um isomorfismo de corpos que estende φ.*

Demonstração. O fato de que Φ é um homomorfismo segue diretamente da definição e deixamos esta verificação a cargo do leitor.

Como o kernel de um homomorfismo é um ideal e como $\mathbb{F}_1$ não contém ideais próprios porque é um corpo, resulta imediatamente ker)Φ) deve ser igual a (0) ou a $\mathbb{F}_1$. Mas ker($\Phi \neq \mathbb{F}_1$ porque Φ não é a função nula; logo $kar(\Phi) = (0)$ e segue que Φ é injetora.

Finalmente, dado um elemento qualquer $y \in \mathbb{F}_2(\alpha_2)$, ele é da forma

$$y = \mu_0 + \mu_1\alpha_2 + \mu_2\alpha_2^2 + \cdots + \mu_{n-1}\alpha_2^{n-1}.$$

Consideramos então os elementos $\lambda_i = \varphi^{-1}(\mu_i) \in F_1, 0 \leq i \leq n-1$. É fácil ver que o elemento

$$y = \lambda_0 + \lambda_1\alpha_1 + \lambda_1\alpha_1^2 + \cdots + \lambda_{n-1}\alpha_1^{n-1} \in \mathbb{F}_1(\alpha_1)$$

é tal que $\Phi(x) = y$. Portanto, Φ também é sobrejetora e, claramente, $\Phi(\lambda) = \varphi(\lambda)$ para todo $\lambda \in \mathbb{F}_1$. □

Agora estamos em condições de provar a unicidade (a menos de isomorfismos) do corpo de raízes de um polinômio. Para isso, demonstraremos um resultado levemente mais geral.

Teorema 2.3.7. *Seja $\varphi : \mathbb{F}_1 \to \mathbb{F}_2$ um isomorfismo de corpos. Dado um polinômio não constante $f \in \mathbb{F}_1[X]$ seja $f^* \in \mathbb{F}_2[X]$ como definido acima. Sejam $\mathbb{E}_1$ um corpo de raízes de f sobre $\mathbb{F}_1$ e $\mathbb{E}_2$ um corpo de raízes de f^* sobre $\mathbb{F}_2$. Então existe um isomorfismo $\Psi : \mathbb{E}_1 \to \mathbb{E}_2$ que estende φ; i.e., tal que $\varphi(x) = \Psi(x)$, para todo elemento $x \in \mathbb{F}_1$.*

Demonstração. Provaremos o resultado por indução no grau de f.

Se f é um polinômio de primeiro grau, então $\mathbb{E}_1 = \mathbb{F} = \mathbb{E}_2$ e o resultado é trivialmente verdadeiro.

Seja então $gr(f) = n$ e suponha que o resultado vale para polinômios de grau menor que n.

Seja h um divisor irredutível de f em $\mathbb{F}_1[X]$ e seja α uma raiz de h em $\mathbb{E}_1$. Escrevendo $f = hq$ temos que $f^* = h^*g^*$ e temos que h^* é um divisor de f^*.

Sejam $\alpha_1 \in \mathbb{E}_1$ e $\alpha_2 \in \mathbb{E}_2$ raízes de f e f^* respectivamente. Então $\mathbb{F}_1 \subset \mathbb{F}_1(\alpha_1) \subset \mathbb{E}_1$ e $\mathbb{F}_1 \subset \mathbb{F}_2(\alpha_2) \subset \mathbb{E}_2$.

$$\begin{array}{ccc} \mathbb{E}_1 & \xrightarrow{\Psi} & \mathbb{E}_2 \\ | & & | \\ \mathbb{F}_1(\alpha_1) & \xrightarrow{\Phi} & \mathbb{F}(\alpha_2) \\ | & & | \\ \mathbb{F}_1 & \xrightarrow{\varphi} & \mathbb{F}_2 \end{array}$$

Em $\mathbb{F}_1(\alpha_1)$ podemos escrever $f = (X - \alpha_1)g$ com $gr(g) = n - 1$ e, da mesma forma, $f^* = (X - \alpha_2)g^*$ com $gr(g^*) = n - 1$. Note que segue direta-

mente do Lema 2.2.7 que $\mathbb{E}_1$ e $\mathbb{E}_2$ são corpos de raízes de g e g^* sobre $\mathbb{F}(_1(\alpha_1)$ e $\mathbb{F}_2(\alpha_2)$ respectivamente.

Pelo Lema 2.3.6 existe um isomorfismo de corpos $\Phi : \mathbb{F}_1(\alpha_1) \to \mathbb{F}_2(\alpha_2)$ que estende ϕ e, pela hipótese de indução, existe um isomorfismo de corpos $\Psi : \mathbb{E}_1 \to \mathbb{E}_2$ que estende φ que estende Φ. Logo Ψ é também uma extensão de φ, como requerido pelo enunciado. □

Como consequência imediata do Teorema acima temos o seguinte.

Corolario 2.3.8. *Sejam $\mathbb{F}$ um corpo e $f \in \mathbb{F}[X]$ um polinômio não constante. Então, dois corpos de raízes de f sobre $\mathbb{F}$ são $\mathbb{F}$-isomorfos.*

Demonstração. Basta tomar, no teorema acima, $\mathbb{F} = \mathbb{F}_1 = \mathbb{F}_2$ e escolher como isomorfismo φ a função identidade. □

EXERCÍCIOS

---

1. Achar a decomposição em fatores irredutíveis do polinômio $f = 2X^4 + 2X^3 + 2X + 1$ em $\mathbb{F}_3[X]$ e achar dois corpos não isomorfos tais que f tem uma raiz em cada um deles.

2. Sejam $\mathbb{F}$, $\mathbb{F}'$ e $\mathbb{E}$ como na demonstração do Teorema 2.3.1. Seja A qualquer conjunto finito com o mesmo número de elementos que $\mathbb{E}\backslash\mathbb{F}$. Então $X = A \cup \mathbb{F}$ tem o mesmo número de elementos que $\mathbb{E}$. Portanto, existe uma bijeção $\Phi : X \to \mathbb{E}$. Pode-se introduzir operações em X da seguinte forma:

   Dados $x, y \in X$ sejam $a, b \in E$ tais que $\Phi(x) = a$ e $\Phi(y) = b$, defina:

   $$\begin{aligned} x + y &= \Phi^{-1}(a) + \Phi^{-1}(b), \\ x.y &= \Phi^{-1}(a).\Phi^{-1}(b). \end{aligned}$$

   Provar que, com estas operações, X é um corpo que contém $\mathbb{F}$ e que f tem uma raiz em X.

3. Seja $\mathbb{F} \subset \mathbb{E}$ corpos. Provar que o conjunto $Gal(\mathbb{E}; \mathbb{F})$ de todos os $\mathbb{F}$ automorfismos de $\mathbb{E}$ é um grupo em relação à operação de composição de funçãoes.

4. Provar que o polinômio $f = X^2 - 2$ é irredutível em $\mathbb{Q}[X]$. Seja ω uma raiz de f em $\mathbb{C}$. Determinar o grupo $Gal(\mathbb{Q}(\omega) : \mathbb{Q})$.

5. Provar que o polinômio $f = X^2 - 2$ é irredutível em $\mathbb{Q}[X]$ e seja ω uma raiz de f em $\mathbb{C}$. Seja ainda $\zeta \in \mathbb{C}$ uma raiz do polinômio $X^2 + X + 1$.

   (i) Provar que $\mathbb{E} = \mathbb{Q}(\omega, \zeta)$ é um corpo de raízes de f sobre $\mathbb{Q}$.

   (ii) Determinar $Gal(\mathbb{E} : \mathbb{Q})$.

6. (i) Determinar o subcorpo $\mathbb{E}$ de $\mathbb{C}$ que é o corpo de raízes de $f = X^3 - 3$ sobre $\mathbb{Q}$.

   (ii) Idem, para o polnômio $g = X^3 - 1$.

   (iii) Em ambos os casos, determinar $Gal(\mathbb{E}, \mathbb{Q})$.

7. Sejam a e b dos inteiros que não são quadrados perfeitos. Seja $\mathbb{E} \subset \mathbb{C}$ o corpo de raízes do polinômio $f = (X^2 - a)(X^2 - b)$ sobre $\mathbb{Q}$. Determinar $\mathbb{E}$ e determinar o grupo $Gal(\mathbb{E} : \mathbb{Q})$.

8. Um elemento ζ de um corpo $\mathbb{E}$ diz-se um **raiz primitiva n-ésima da unidade** se $\zeta^n = 1$ e $\zeta^m \neq 1$ para todo inteiro positivo $m < n$. Provar que, se $\zeta \in \mathbb{C}$ é uma raiz primitiva n-ésima da unidade, então $\mathbb{Q}(\zeta)$ é o corpo de raízes do polinômio $X^n - 1$ sobre $\mathbb{Q}$.

9. Seja $\mathbb{F}_2$ o corpo com dois elementos e seja ζ uma raiz do polinômio $X^3 + X^2 + 1 \in \mathbb{F}_2[X]$. Provar que $\mathbb{Z}_2(\zeta)$ é um corpo de raízes para f sobre $\mathbb{F}_2$.

10. Sejam a um inteiro, $\alpha \in \mathbb{C}$ uma raiz do polinômio $f = X^n - a$ e ζ uma raiz primitiva n-ésima da unidade. Provar que $\mathbb{Q}(\alpha, \zeta)$ é o corpo de raízes de f sobre $\mathbb{Q}$.

11. Seja Sejam $\mathbb{F}$ um corpo e f um polinômio não constante de $\mathbb{F}[X]$. Seja ainda $\mathbb{E}$ um corpo de decomposição para f sobre $\mathbb{F}$. Provar que a interseção de todos os subcorpos de $\mathbb{E}$ que são corpos de decomposição para f sobre $\mathbb{F}$ é um corpo de raízes fe f,

12. Provar que o isomorfismo construído no Lema 2.3.6 é o único isomorfismo de $\mathbb{F}_1(\alpha_1)$ em $\mathbb{F}_2(\alpha_2)$ que estende φ e que leva α_1 em α_2.

13. Sejam $\mathbb{F}$ um corpo e f um polinômio não constante de $\mathbb{F}[X]$. Provar que, se α e β são raízes de f em alguma extensão de $\mathbb{F}$, então existe um $\mathbb{F}$-isomorfismo de $\mathbb{F}(\alpha)$ em $\mathbb{F}(\beta)$.

14. Seja $\varphi : \mathbb{F}_1 \to \mathbb{F}_2$ um isomorfismo de corpos. Provar que a função $\overline{\varphi} : \mathbb{F}_1[X] \to \mathbb{F}_2[X]$ definida por

$$f = a_0 + a_1X + \cdots + a_nX^n \ \mapsto \ f^* = \varphi(a_0) + \varphi(a_1)X + \cdots + \varphi(a_n)X^n$$

é um isomorfismo de anéis.

Provar que, se $\alpha \in \mathbb{F}_1$ é uma raiz de f então $\varphi(\alpha) \in \mathbb{F}_2$ é uma raiz de f^*.

2.4 Extensões Separáveis

Lembramos que, ena Definição 2.2.3 dizemos que, dado um corpo $\mathbb{F}$ e um polinômio $f \in \mathbb{F}[X]$ um elemento α numa extensão $\mathbb{E}$ de $\mathbb{F}$ diz-se uma **raiz múltipla** de f se existe um inteiro $n > 1$ tal que $(X - \alpha)^n$ divide f e $(X-\alpha)^{n+1}$ não divide f. Neste caso, o inteiro n diz-se a **multiplicidade** de α como raiz de f.

Nossa intenção agora é determinar um critério para decidir quando um polinômio tem raízes múltiplas. O leitor provavelmente lembra que, nos cursos de Cálculo, isto podia ser feito usando a noção de derivada. No presente contexto, trabalhando em corpos quaisquer, não dispomos da noções de distância, limite, etc. Porém, como estamos trabalhando apenas com polinômios, pde se introduzir esta noção de um modo puramente formal.

Definição 2.4.1. *Seja $\mathbb{F}$ um corpo. Dado um polinômio $f = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{F}[X]$, chama-se* **derivada** *ao polinômio*

$$f' = a_1 + a_2X + \cdots + a_nX^{n-1};$$

ou, equivalentemente, se $f = \sum_{i=0}^{n} a_iX^i$ então

$$f' = \sum_{i=1}^{n} ia_iX^{i-1}.$$

O próximo lema mostra que as propriedades familiares das derivadas, no Cálculo, também valem neste contexto.

Lema 2.4.2. *Seja $\mathbb{F}$ um corpo, f, g polinomios de $\mathbb{F}[X]$ e a um elemento de $\mathbb{F}$. Então:*
(i) $(f+g)' = f' + g'$.
(ii) $(af)' = af'$.
(iii) $(fg)' = fg' + f'g$.

Demonstração. Os itens (i) e (ii) seguem diretamente da aplicação da definição.

Para demonstrar (iii) escrevemos $f = \sum_{i=0}^{n} a_i X^i$ e faremos indução no grau de f. Se $gf(f) = 0$ a afirmação se reduz ao caso (ii).

Suponhamos então que $f = \sum_{i=0}^{n} a_i X^i$, com $a_n \neq 0$ e que (iii) vale para polinômios de grau menor que n. Escrevendo $f_1 = \sum_{i=0}^{n-1} a_i X^i$ temos que $f = f_1 + a_n X_n$ donde

$$fg = (f_1 + a_n X_n)g = f_1 g + a_n X^n g$$

e, applicando (i)

$$(fg)' = (f_1 g)' + (a_n X^n g)'.$$

Pela hipótese de indução temos que $(f_1 g)' = f_1 g' + f_1' g$.

Agora, é fácil provar que

$$(a_n X^n g)' = a_n X^n g' + a_n X^{n-1} g$$

através de um cálculo direto, usando a definição. Logo

$$\begin{aligned} (fg)' &= (f_1 g' + f_1' g) + (a_n X^n g' + a_n X^{n-1} g) \\ &= (f_1 + a_n X^n) g' + (f_1' + a_n X^{n-1}) g = fg' + f'g. \end{aligned}$$

□

Podemos agora der um critério para decidir quando um polinômio tem raízes multiplas em algum corpo.

Lema 2.4.3. *Sejam $\mathbb{F} \subset \mathbb{E}$ corpos e seja $f \in \mathbb{F}[X]$ um polinômio não constante. Um elemento $\alpha \in \mathbb{E}$ é uma raiz múltipla de f se e somente se*

$$f(\alpha) = 0 \quad e \quad f'(\alpha) = 0.$$

Demonstração. Obviamente, α é raiz de f se e somente se $f(\alpha) = 0$. Neste caso, podemos escrever $f = (X-\alpha)^n g$ em $\mathbb{E}[X]$, com $n \geq 1$ e $g(\alpha) \neq 0$.

Temos então que

$$f' = (X-\alpha)^n g' + n(X-\alpha)^{n-1} g.$$

Se $n > 1$ temos $f'(\alpha) = 0$. Por outro lado, se $n = 1$ temos $f'(\alpha) = g(\alpha) \neq 0$ (veja o Exercício 4 de seção §2), o que prova nossa afirmação.

□

Na verdade, é possível decidir quando um polinômio tem raízes múltiplas em alguma extensão, sem necessidade de conhecer explicitamente essa extensão ou as raízes de f.

Lema 2.4.4. *Seja $\mathbb{F}$ um corpo e seja $f \in \mathbb{F}[X]$ um polinômio não constante. Então f tem raízes múltiplas em alguma extensão $\mathbb{E}$ de $\mathbb{F}$ se e somente se $mdc(f, f') \neq 1$ em $\mathbb{F}[X]$.*

Demonstração. De fato, note que, do Lema acima, temos que f tem raíz múltipla se e somente se $(X - \alpha)$ é um divisor de f e também de f'. Portanto $mdc(f, f') \neq 1$ em $\mathbb{E}[X]$.

Ainda, é fácil ver que, como f e f' pertencem a $\mathbb{F}[X]$, então seu máximo comum divisor também pertence a $\mathbb{F}[X]$ (por exemplo, lembrando que $mdc(f, f')$ pode se calcular usando o algoritmo de Euclides e observando que todas as operações implicadas nesse cálculo acontecem em $\mathbb{F}[X]$.

□

Polinômios que têm só raízes simples são tão importantes que eles recebem um nome particular.

Definição 2.4.5. *Seja $\mathbb{F}$ um corpo. Um polinômio irredutível f em $\mathbb{F}[X]$ diz-se* **separável** *se todas suas raízes são simples.*

Um polinômio f de $\mathbb{F}[X]$ diz-se **separável** *se todos seus fatores irredutíveis são separáveis.*

Um elemento α numa extensão $\mathbb{E}$ de $\mathbb{F}$ diz-se **separável** *sobre $\mathbb{F}$ se o seu polinômio minimal em $\mathbb{F}[X]$ é um polinômio separável.*

Uma extensão $\mathbb{E}$ de um corpo $\mathbb{F}$ diz-se **separável** *se todo elemento de $\mathbb{E}$ é separável sobre $\mathbb{F}$.*

Nos próximos capítulos, resultará muito útil saber quando um polinômio irredutível é separável. Os próximos resultados proporcionam critérios para reconhecer esta situação.

Lema 2.4.6. *Um polinômio irredutível $f \in \mathbb{F}[X]$ é separável se e somente se $f' \neq 0$.*

Demonstração. Como vimos no Lema 2.4.4, f tem raízes multiplas (isto é, não é separável) se e somente se $mdc(f, f') \neq 1$. Como f é irredutível, temos que seu único divisor mônico não trivial é da forma af, para algum $a \in F$, logo $mdc(f, f') = af$ donde $af \mid f'$ e consequentemente também $f \mid f'$. Como $gr(f') < gr(f)$ isto acontece se e so se $f' = 0$.

Por tanto, f é separável se e so se $f' \neq 0$. □

Teorema 2.4.7. *Sejam $\mathbb{F}$ um corpo f um polinômio irredutível de $\mathbb{F}x$. Então:*

(i) Se $car(\mathbb{F}) = 0$ então f é sempre separável.

(ii) Se $car(\mathbb{F}) = p > 0$ então f não é separável se e somente se ele é da forma $f = g(X^p)$ para algum polinômio $g \in \mathbb{F}[X]$.

Demonstração. Seja $f = \sum_{i=0}^{n} a_i X^i$. Então

$$f' = \sum_{i=1}^{n} i a_i X^{i-1}.$$

(i) Se $car(\mathbb{F}) = 0$, como $a_n \neq 0$ temos que o coeficiente do termo de maior grau de f' é $na_n \neq 0$, donde $f' \neq 0$. Pelo lema acima, f é separável.

(ii) Se $car(\mathbb{F})p > 0$ temos que $f' = 0$ se e so se, para cada índice i que não é multiplo de p, tem-se que $a_i = 0$. Consequentemente, $f' = 0$ se e somente se f é da forma

$$f = a_0 + a_p X^p + a_{2p} X^{2p} + \cdots a_{kp} X^{kp}.$$

□

Corpos onde todo polinômio irredutível é separável recebem um nome especial.

Definição 2.4.8. *Um corpo diz-se* **perfeito** *se todo polinômio irredutível de* $\mathbb{F}[X]$ *é separável.*

Do teorema acima, segue imediatamente que todo corpo de característica 0 é perfeito. Veremos, no próximo capítulo (no Teorema **??**) que todo corpo finito também é perfeito.

EXERCÍCIOS

---

1. Mostre que o polinômio $f = (X^2 + 1)(X^4 - 1) \in \mathbb{R}[X]$ é separável, mas tem raízes múltiplas.

2. Provar que, se $\mathbb{F}$ é um corpo e $f \in \mathbb{F}[X]$ é um polinômio irredutível mônico, então as seguintes afirmações são equivalentes:

   (i) f é separável.

   (ii) as raízes de f em qualquer extensão $\mathbb{E}$ de $\mathbb{F}$ são simples.

   (iii) Existe uma extensão $\mathbb{E}$ de $\mathbb{F}$ tal que $f = (X - \alpha_1)(X - \alpha_2) \cdots (x - \alpha_n)$ em $\mathbb{E}[X]$.

3. Prove que, se $\mathbb{F}$ é um corpo de característica 0, então todo polinômio $f \in \mathbb{F}[x]$ é separável.

4. Sejam $\mathbb{F} \subset \mathbb{E}$ corpos e seja f um polinômio de $\mathbb{F}[X]$. Provar que, f é separável em $\mathbb{E}[X]$, se e somente se é separável em $\mathbb{E}[X]$.

5. Sejam $\mathbb{F} \subset \mathbb{K} \subset \mathbb{E}$ corpos. Prova que $\mathbb{E}$ é uma extensão separável de $\mathbb{F}$ se e somente se $\mathbb{E}$ é uma extensão separável de $\mathbb{K}$ e $\mathbb{K}$ é uma extensão separável de $\mathbb{F}$.

6. Sejam $\mathbb{F} \subset \mathbb{E}$ corpos, e sejam α e β elementos de $\mathbb{E}$, separáveis sobre $\mathbb{F}$. Provar que $\alpha \pm \beta$, $\alpha\beta$ e α/β são separáveis sobre $\mathbb{F}$.

7. Seja $\mathbb{E}$ uma extensão algébrica de um corpo $\mathbb{F}$. Provar que o subconjunto dos elementos de $\mathbb{E}$ que são separáveis sobre $\mathbb{F}$ é um subcorpo de $\mathbb{E}$ (chamado o **fecho separável** de $\mathbb{F}$ em $\mathbb{E}$).

8. Provar que todo corpo algébricamente fechado é perfeito.

9. Seja $\mathbb{F}$ um corpo perfeito. Provar que toda extensão algébrica de $\mathbb{F}$ é separável.

10.* Sejam p um inteiro primo e $\mathbb{F}$ o corpo com p elementos. Seja ainda t um elemento transcendente sobre $\mathbb{F}$. Provar que o corpo $\mathbb{F}(t)$ não é perfeito.

Capítulo 3

Corpos Finitos

3.1 Introdução

O conceito de *corpo finito* é devido a Evariste Galois (1811-1832) que o introduziu em 1830. Ele considerou um polinômio irredutível $f \in \mathbb{Z}[X]$, de grau n. Chamando de i uma de suas raízes (note que, neste contexto, i não tem nada a ver com a unidade imaginária dos números complexos), ele considerou expressões do tipo

$$a_0 + a_1 i + a_2 i^2 + \cdots + a_{n-1} i^{n-1},$$

com $a_i \in \mathbb{Z}$, $1 \leq i \leq n-1$. Tomando estes coeficientes inteiros em módulo um primo p, o conjunto $\mathbb{E}$ de todas as expressões da forma acima, tem p^n elementos. Galois prova, a seguir, que $\mathbb{E}$ é um corpo - naturalmente, na linguagem própria da época. O leitor notará que esta descrição coincide com a construção do corpo $\mathbb{Z}_p(i)$, que vimos em capítulos anteriores.

Por causa disso, os corpos finitos também são chamados de **Corpos de Galois** e um corpo com p^n elementos se representa, às vezes, pelo símbolo $GF(p^n)$ (do inglês: Galois Field with p^n elements). Para indicar que $\mathbb{F}$ é um corpo finito, *com q elementos*, nós empregaremos a notação $\mathbb{F}_q$.

Nosso primeiro passo, neste capítulo, será determinar todos os corpos finitos.

Note, em primeiro lugar, que se $\mathbb{F} \subset \mathbb{E}$ são corpos finitos, quando consideramos $\mathbb{E}$ como espaço vetorial sobre $\mathbb{F}$, ele deve ser de dimensão finita. Seja n essa dimensão e seja $\{b_1, b_2, \ldots, b_n\}$ uma base de $\mathbb{E}$ sobre $\mathbb{F}$. Então $\mathbb{E}$

é o conjunto de todas as combinações lineares da forma

$$\alpha = x_1 b_1 + x_2 b_2 + \cdots + x_n b_n \quad \text{com} \quad x_i \in \mathbb{F}_p,\ 1 \leq i \leq n.$$

Se $\mathbb{F}$ é um corpo com q elementos, cada um dos coeficientes x_i, $1 \leq i \leq n$, pode assumir exatamente q valores distintos (cada um dos elementos de $\mathbb{F}$); portanto, o número total de combinações lineares possíveis é q^n. Estas considerações demonstram o seguinte.

Teorema 3.1.1. *Sejam $\mathbb{F} \subset \mathbb{E}$ corpos finitos. Se $\mathbb{F}$ é um corpo com q elementos, então o número de elementos de $\mathbb{E}$ é uma potência de q.*

Por outro lado, se $\mathbb{E}$ é um corpo finito, do Teorema 1.2.3 vem imediatamente que seu corpo primo é isomorfo a $\mathbb{Z}_p$, para algum primo p e, consequentemente, $car(\mathbb{E}) = p$. Este argumento mostra, em particular, que todos os corpos com p elementos são isomorfos entre si (pois são todos isomorfos a $\mathbb{Z}_p$). Daqui em diante denotaremos um tal corpo por $\mathbb{F}_p$. Como $\mathbb{F}_p \subset \mathbb{E}$ o teorema acima implica o seguinte.

Teorema 3.1.2. *Seja $\mathbb{E}$ um corpo finito com q elementos. Então, existem um inteiro positivo n e um primo p tal que $q = p^n$.*

É interessante considerar também os corpos finitos desde outro ponto de vista.

Teorema 3.1.3. *Seja $\mathbb{E}$ um corpo finito com p^n elementos. Então, para todo elemento $a \in \mathbb{E}$, tem-se que*

$$a^{p^n} = a.$$

Consequentemente, $\mathbb{E}$ é o corpo de raízes do polinômio $f = X^{p^n} - X$ sobre $\mathbb{F}_p$ e

$$X^{p^n} - X = (X - a_1)(X - a_2) \cdots (X - a_q),$$

onde $a_1, a_2, \ldots, a_q$ são todos os elementos de $\mathbb{F}_q$.

Demonstração. O conjunto $\mathbb{E}^* = \mathbb{E} \setminus \{0\}$ é um grupo de ordem $p^n - 1$. Por tanto, para todo elemento $a \in \mathbb{E}^*$, tem-se que $a^{p^n - 1} = 1$ donde $a^{p^n} = a$. Como esta relação vale também para o elemento 0, ela vale para todos os elementos de $\mathbb{E}$.

Este argumento mostra que o conjunto dos elementos de $\mathbb{E}$ é também o conjunto das raízes do polinômio $f = X^{p^n} - X$ e, como $gr(f) = p^n$, estas são todas as raízes deste polinômio. Portanto

$$X^{p^n} - X = (X - a_1)(X - a_2) \cdots (X - a_q).$$

Finalmente, f tem todas suas raízes em $\mathbb{E}$ e, claramente, um subcorpo estritamente menor não contém, necessariamente, alguma das raízes de f. Isto prova que $\mathbb{E}$ é o corpo de raízes de f, como queríamos demonstrar. $\square$

No Teorema 3.1.2 mostramos que, se $\mathbb{E}$ é um corpo finito, então o número de elementos de $\mathbb{E}$ é da forma p^n, para algum primo p e um inteiro positivo n. Mostraremos agora que vale a recíproca deste resultado.

Teorema 3.1.4. (Existência e Unicidade de Corpos Finitos) *Sejam p um primo e n um inteiro positivo. Então, existe um corpo $\mathbb{E}$ com p^n elementos, que é único a menos de isomorfismos e todo corpo finito é desta forma. O corpo $\mathbb{E}$ é o corpo de decomposição do polinômio $X^{p^n} - X$ sobre $\mathbb{F}_p$.*

Demonstração. Dados p e n como no enunciado, consideramos o polinômio $f = X^{p^n} - X \in \mathbb{F}_p[X]$. Pelo Teorema 2.3.3 sabemos que existe um corpo $\mathbb{E} \supset \mathbb{F}_p$ que é corpo de decomposição para f. Seja A o conjunto das soluções de f em $\mathbb{E}$.

Como $f' = -1$, segue que f e f' não tem raízes comuns; portanto, todas as raízes de f são simples, o que implica que $|A| = p^n$. Mostraremos que $A = \mathbb{E}$.

Note que, dados α e β em A, tem-se que $(\alpha \pm \beta)^{p^n} = \alpha^{p^n} \pm \beta^{p^n} = \alpha \pm \beta$. Da mesma forma, $(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta$.

Finalmente, se $\alpha^{p^n} = \alpha$ então também $(1/\alpha)^{p^n} = 1/\alpha$. Todas estas observações mostram que A é um subcorpo de $\mathbb{E}$. Como $\mathbb{E}$ é um corpo de raízes de f e todas as raízes de f pertencem a A temos que $\mathbb{E} = A$, donde $|\mathbb{E}| = |A| = p^n$.

Como corpos de raízes são únicos, a menos de isomorfismo, a unicidade resulta imediatamente.

O fato de que todo corpo finito é desta forma foi estabelecido no Teorema 3.1.2. $\square$

A classificação dos corpos finitos é devida a Eliakim Hastings Moore (1862-1932), em 1893, [**?**]. Moore foi um dos pioneiros da matemática americana e um dos fundadores do Departamento de Matemática da Universidade de Chicago.

Nossa intenção agora é estudar o conjunto $\mathbb{E}^*$ dos elementos não nulos de um corpo finito. Como todo elemento não nulo é inversível, segue imediatamente que $\mathbb{E}^*$ é um grupo em relação à operação de multiplicação de $\mathbb{E}$. Da própria definição de corpo, segue que este grupo é comutativo. Na

verdade, provaremos que é um grupo cíclico. Para isso precisamos de alguns resultados preliminares.

EXERCÍCIOS

---

1. Exibir exemplos de corpos com 8 e com 16 elementos.

2. Provar que $\mathbb{E} = \mathbb{F}_3[X]/(X^2+1)$ é o corpo de decomposição do polinômio $f = X^9 - X$ sobre $\mathbb{F}_3$.

3. Provar que $\mathbb{E}_1 = \mathbb{F}_3[X]/(X^2+X+2)$ é isomorfo a $\mathbb{E} = \mathbb{F}_3[X]/(X^2+1)$.

4. Seja $\alpha = \frac{-1+\sqrt{5}}{2} \in \mathbb{C}$. Seja $I = 2\mathbb{Z}[\alpha]$. Prove que $\mathbb{E}_2 = \mathbb{Z}[a]/I$ é um corpo isomorfo a
$$\mathbb{E} = \frac{\mathbb{Z}_2[X]}{(x^2+X+1)}.$$
.

5. Construir um exemplo de corpo finito com 27 elementos.

6. Dar um exemplo de corpo finito com 25 elementos.

7. Seja $q = p^n$ onde p é um primo ímpar. Provar que:

   (i) A função $\psi : F_q \to \mathbb{F}_q$ definida por $\psi(x) = x^2$, para todo $x \in \mathbb{F}_q$ não é injetora.

   (ii) Existe um elemento $c \in \mathbb{F}_q$ que não é o quadrado de nenhum elemento de $\mathbb{F}_q$.

   (iii) O polinômio $f = X^2 - c$ é irredutível em $\mathbb{F}_q[X]$.

   (iv) Se t denota uma raiz de f numa extensão de $\mathbb{F}_q$, então $\mathbb{F}_q(t)$ é um corpo com q^2 elementos.

8. Seja $\mathbb{E}$ um corpo finito com p^n elementos e seja a um elemento de $\mathbb{E}$. Provar que $a^p = a$ se e somente se a pertence ao corpo primo de $\mathbb{E}$.

9. Provar que um corpo finito $\mathbb{F}$ não é algébricamente fechado. Sugestão: considere o polinômio $f = 1 + \prod_{a\in\mathbb{F}}(X-a)$.

10. Seja $\mathbb{F}$ um corpo finito, com q elementos. Prova que o polinômio $f = X^q - X + 1$ não tem raízes em $\mathbb{F}$.

11. Sejam $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$ corpos finitos. Mostrar que, $m \mid n$.

12. Prove que todo polinômio irredutível de segundo grau em $\mathbb{F}_q[X]$ pode se escrever como o produto de dois polinômios de primeiro grau em $\mathbb{F}_{q^2}[X]$.

13. Seja $\mathbb{E}$ um corpo finito com p^n elementos. Provar que, para todo elemento $a \in \mathbb{E}$ tem-se que $a^{p^n} = a$.

14. Seja $\mathbb{E} = \mathbb{F}_{2^n}$ um corpo finito, de característica 2. Provar que a soma de todos os elementos de $\mathbb{E}$ é igual a 0 se e somente se $\mathbb{E} \neq \mathbb{F}_2$. (Sugestão: usar indução em n).

3.2 Grupos cíclicos

Lembramos que um grupo A diz-se **cíclico** se existe um elemento $a \in A$ tal que A é o grupo gerado por A; i.e., se

$$A = \{\ldots, a^{-2}, a^{-1}, 1,\ a,\ a^2, \ldots\} = \{\ a^i \mid i \in \mathbb{Z}\ \}.$$

O grupo cíclico gerado por a se representa frequentemente por $\langle a \rangle$.

Lembramos que, dado um elemento a num grupo G, se $a^n = 1$ para algum inteiro positivo n, então chama-se **ordem** de a ao inteiro

$$m = min\{h \in \mathbb{Z}^+ \mid a^h = 1\}.$$

Costuma-se denotar a ordem de um elemento a pelo símbolo $o(a)$.

Se a é um elemento de ordem finita n então tem-se que

$$\langle a \rangle = \{\ 1,\ a,\ a^2, \ldots, a^{n-1}\ \}.$$

Neste caso, temos que

$$|A| = o(a).$$

Note que, da própria definição temos que, se $m = o(a)$ então $a^m = 1$.

Lema 3.2.1. *Seja a um elemento de um grupo, de ordem finita m. Se h é um inteiro positivo tal que $a^h = 1$ então $m \mid h$.*

Demonstração. Dado um inteiro h nas condições do enunciado, dividindo h por m obtemos um quociente q e um resto r tais que $h = mq + r$, com $0 \leq r < m$ donde $a^h = a^{mq} + a^r$.

Como $a^h = a^m = 1$ temos que $a^r = 1$. Se $r \neq 0$ temos que $r < m$ (que é o menor elemento com a propriedade de que $a^m = 1$), uma contradição.

Logo, $r = 0$ e segue que $m \mid h$. □

Como consequência destas observações temos:

Corolario 3.2.2. *Seja a um elemento de um grupo G de ordem finita m. Então, dado um inteiro n, tem-se que $a^n = 1$ se e somente se $m \mid n$.*

Se a é um elemento de ordem m, então todo elemento de $\alpha a\rangle$ é da forma a^h, com $0 \leq h \leq m - 1$. Como veremos, é possível determinar a ordem de qualquer elemento desta forma.

Lema 3.2.3. *Seja a um elemento de um grupo G de ordem finita n. Então, um elemento da forma $a^h \in G$, com $h \in \mathbb{Z}$, tem ordem*

$$o(a^h) \;=\; \frac{n}{mdc(n,h)}.$$

Demonstração. Seja $d = mdc(h, n)$. Escrevemos $h = dh'$, $n = dn'$ com $mdc(h', n') = 1$ e seja $t = o(a^h)$. Devemos provar que $t = n/d$.

Temos que:

$$(a^h)^{n/d} = a^{hn/d} = a^{h'n} = (a^n)^h = 1,$$

donde segue que $t \mid n/d$.

Por outro lado, temos também que $1 = (a^h)^t = a^{ht}$; logo $n \mid (ht)$, ou seja $(dn') \mid (dh't)$ o que implica que n' divide $h't$. Como $mdc(n', h') = 1$ temos então que $n' = n/d$ divide t. Conseqüentemente, $n/d = t$, como queriamos demonstrar. □

Agora podemos descrever todos os subgrupos de um grupo cíclico finito.

Teorema 3.2.4. *Seja A um grupo cíclico de ordem finita m. Então, tem-se que:*
(i) Todo subgrupo de A é cíclico.
(ii) Para cada divisor d de m, o grupo A contém um <u>único</u> subgrupo de ordem d.

Demonstração.
(i) Seja $G = \langle a \rangle$ um grupo cíclico de ordem m e seja H um subgrupo de A. Queremos provar que H é cíclico. Se $H = \{1\}$, então ele é um grupo cíclico. Suponhamos então que $H \neq 1$. Neste caso, o conjunto $\{x \in \mathbb{Z} \mid a^x \in H,\ 1 \leq x \leq n-1\ \}$ não é vazio. Seja então:

$$m \ = \ min\{x \in \mathbb{Z} \mid a^x \in H,\ 1 \leq x \leq n-1\ \}.$$

Mostraremos que $H = \langle a^m \rangle$. De fato, como $a^m \in H$, vem imediatamente que $\langle a^m \rangle \subset H$. Devemos ainda provar que vale a inclusão contrária.

Para isso, consideramos um elemento arbitrário $h \in H$. Como $h \in G$, existe algum inteiro t tal que $h = a^t$. Dividindo t por m obtemos dois inteiros q e r tais que $t = mq + r$, e $0 \leq r < m$. Então:

$$h \ = \ a^t \ = \ a^{mq+r} \ = \ a^{mq}a^r,$$

donde

$$a^r \ = \ a^{-mq}h \in H.$$

Como $r < m$, deve ser $r = 0$. Isto implica que $t = mq$, donde $h = a^t = (a^m)^q \in \langle a^m \rangle$ o que mostra que $H \subset \langle a^m \rangle$. Isto completa a demonstração da nossa primeira afirmação.

(ii) Seja d um divisor de n e seja $t = n/d$. Considere o subgrupo $H = \langle a^t \rangle$. De acordo com lema 3.2.3 a ordem de H é:

$$|H| = o(a^t) = \frac{n}{mdc(n,t)} = \frac{n}{mdc(n,n/d)} = \frac{n}{n/d} = d.$$

Para mostrar que este é o único subgrupo dessa ordem, suponhamos que existe $K = \langle a^s \rangle$ tal que $|K| = d$. Então temos que $o(a^s) = n/mdc(n,s) = d$ donde $mdc(n,s) = n/d$ e podemos escrever $s = s_1(n/d)$. Logo

$$K = \langle a^s \rangle = \langle (a^{n/d})^{s_1} \rangle = \langle (a^t)^{s_1} \rangle \subset H.$$

Como ambos conjuntos são finitos, da mesma ordem, segue que $K = H$, como queríamos demonstrar. □

Mais adiante, precisaremos conhecer a ordem de um produto de elementos, pelo menos num caso particular, interessante.

Lema 3.2.5. *Seja A um grupo abeliano e sejam a e b elementos de A de ordens r e s respectivamente.*

(i) Se $mdc(r,s)=1$, então $o(ab)=rs$.

(ii) Em qualquer caso, A contém um elemento de ordem $mmc(r,s)$.

Demonstração.

(i) Seja $t=o(ab)$. Como $(ab)^{rs}=(a^r)^s(b^s)^r=1$ temos que $t \mid (rs)$.

Por outro lado, temos que $1=(ab)^{tr}=a^{tr}b^{tr}=b^{tr}$ donde $s \mid (tr)$ e, como $mdc(s,r)=1$, do Teorema de Euclides temos que $s \mid t$. De forma análoga, considerando $(ab)^{ts}$ segue que $r \mid t$ e, como r e s são relativamente primos, temos também que $(rs) \mid t$.

Desta forma, segue que $t=rs$, como queriamos demonstrar.

(ii) Sejam $r=p_1^{n_1}\cdots p_t^{n_t}$ e $s=p_1^{m_1}\cdots p_t^{m_t}$ as decomposições em fatores primos de r e s, com $n_i, m_i \geq 0, 1 \leq i \leq t$. Definimos

$$\gamma_i = max(n_i, m_i), \quad 1 \leq i \leq t.$$

Note que $p_i^{\gamma_i}$ é um divisor de r ou um divisor de s, pois concide com $p_i^{n_i}$ ou com $p_i^{m_i}$. No primeiro caso, o subgrupo $\langle a \rangle$ contém um elemento de ordem $p_i^{\gamma_i}$; no segundo caso, $\langle b \rangle$ contém um tal elemento, $1 \leq i \leq t$.

Em qualquer caso, para cada índice i existe um elemento $g_i \in A$ tal que $o(g_i)=\gamma_i$, $1 \leq i \leq t$. Seja $g \in A$ o produto $g=g_1g_2\cdots g_t$.

Como $mdc(o(g_i), o(g_j))=1$ sempre que $i \neq j$, conforme à parte (i), temos que

$$o(g)=p_1^{\gamma_1}p_2^{\gamma_2}\cdots p_t^{\gamma_t}=mmc(r,s).$$

□

Do Lema 3.1.4 temos imediatamente o seguinte.

Corolario 3.2.6. *Seja $A=\langle a \rangle$ um grupo cíclico gerado por um elemento a. Se a é de ordem finita m então um elemento da forma a^h é um gerador de A se e somente se $mdc(m,h)=1$.*

Lembramos que chama-se **função de Euler** à função que a cada inteiro positivo n associa o *número de inteiros positivos que são menores do que n e relativamente primos com ele.* Por exemplo, os inteiros positivos menores que 12 e relativamente primos com 12 são 1, 5, 7 e 11, logo $\varphi(12)=4$. Já os inteiros positivos menores que 14 e relativamente primos com 14 são 1, 3, 5, 9, 11, 13, donde $\varphi(14)=6$.

Do resultado acima, vem imediatamente o seguinte.

Corolario 3.2.7. *Seja $A = \langle a \rangle$ um grupo cíclico gerado por um elemento a. Se a é de ordem finita m então o número de geradores de A; i,e, o número de elementos de A que têm ordem precisamente igual a m é $\varphi(m)$.*

Na próxima seção veremos como calcular os valores desta função.

EXERCÍCIOS

---

1. Determinar todos os geradores dos grupos aditivos $\mathbb{Z}_6$, $\mathbb{Z}_8$, $\mathbb{Z}_{10}$, $\mathbb{Z}_{12}$ e $\mathbb{Z}_{24}$.

2. Determinar todos os geradores do grupo cíclico (multiplicativo) $G = \langle a \rangle$ quando $o(a) = 6,\ 8,\ 10,\ 12$ e 24, respectivamente.

3. Seja $G = \langle a \rangle$ um grupo cíclico de ordem 24. Determine todos os elementos do subgrupo de ordem 12. Identifique todos os geradores deste grupo.

4. Determinar qual dos seguintes grupos é cíclico, achando um gerador: $\mathcal{U}(\mathbb{Z}_8)$, $\mathcal{U}(\mathbb{Z}_9), \mathcal{U}(\mathbb{Z}_{10})$ e $\mathcal{U}(\mathbb{Z}_{12})$.

5. Determine todos os elementos de ordem 3 e todos os elementos de ordem 5 do grupo $G = \langle a \rangle$, sabendo que $o(a) = 15$.

6. Prove que todo grupo de ordem prima é cíclico.

7. Provar que um grupo cíclico finito, de ordem par, contém um único elemento de ordem 2.

8. Seja $G = \langle a \rangle$ um grupo cíclico de ordem n e seja t um inteiro tal que $1 \leq t \leq n-1$. Determine a ordem do grupo quociente $\langle a \rangle / \langle a^t \rangle$.

9. Seja $G = \langle a \rangle$ um grupo cíclico finito, de ordem n. Determine condições necessárias e suficientes sobre os inteiros r e s para que $\langle a^r \rangle \subset \langle a^s \rangle$ e também para que $\langle a^r \rangle = \langle a^s \rangle$.

10. De um grupo G sabe-se que ele contém somente dois subgrupos. Provar que G é cíclico, de ordem prima.

11. De um grupo cíclico G sabe-se que ele contém exatamente três subgrupos: o próprio G, o subgrupo $\{e\}$ e um subgrupo de ordem prima p. Determine G.

12. Sejam G um grupo e p um número primo. Mostre que se G contém mais que $p-1$ elementos de ordem p, então G não é cíclico.

13. Seja G um grupo cíclico cuja ordem é divisível por 8. Quantos elementos de ordem 8 há em G?

14. Mostre que o grupo

$$TU(2,\mathbb{Z}_7) = \left\{ \begin{pmatrix} \overline{1} & \overline{a} \\ \overline{0} & \overline{1} \end{pmatrix} \mid \overline{a} \in \mathbb{Z}_7 \right\}$$

é cíclico, achando um gerador.

3.3 A Função de Euler

Note inicialmente que, se n é um inteiro da forma $n = p^m$, com p primo, então é fácil calcular o valor de $\varphi(n)$. De fato, o número de inteiros menores que n é $n-1 = p^m - 1$.

Por outro lado, os números menores que n que são múltiplos de p são: $p,\ 2p,\ 3p,\ \ldots, p^m - p$; isto é, existem exatamente $p^{m-1} - 1$ números nestas condições. Logo:

$$\varphi(p^m) = p^m - 1 - (p^{m-1} - 1) = p^m - p^{m-1}$$

i.e.

$$\varphi(p^m) = p^{m-1}(p-1).$$

Nossa intenção agora é provar que, se m e n são inteiros relativamente primos, então $\varphi(mn) = \varphi(m)\varphi(n)$. Há várias formas de chegar a este resultado. Nós o obteremos como consequência do próximo resultado, que é uma versão do Teorema Chinez do Resto (veja o Exercício 2 desta seção).

Teorema 3.3.1. *Seja m e n inteiros positivos relativamente primos. Então:*

$$\mathbb{Z}_{mn} \cong \mathbb{Z}_m \oplus \mathbb{Z}_n.$$

Demonstração. Como vamos trabalhar em três anéis diferentes, precisamos tomar certos cuidados com a notação. Dado um inteiro a, denotaremos por $\overline{a}$ a sua classe em $\mathbb{Z}_{mn}$ e por $[a]_n, [a]_m$ sua classe em $\mathbb{Z}_n$ e $\mathbb{Z}_m$ respectivamente.

Definimos uma função $\phi : \mathbb{Z}_{mn} \to \mathbb{Z}_n \oplus Z_m$ por

$$\overline{a} \;\mapsto\; ([a]_n, [a]_m).$$

Nossa primeira providência será provar que ela está bem definida, uma vez que parece depender do representante. Sejam então $a, b \in \mathbb{Z}$ tais que $\overline{a} = \overline{b}$. Isto implica que $a \equiv b \pmod{mn}$. Conseqüentemente, temos também que

$$a \equiv\ b \pmod{m} \quad \text{e} \quad a \equiv b \pmod{n},$$

o que significa que

$$[a]_m = [b]_m \quad \text{e} \quad [a]_n = [b]_n.$$

Logo, nossa definição independe do representante e ϕ está bem definida.

Um cálculo simples mostra que ϕ é um homomorfismo. Para verificar que ϕ também é injetora, devemos mostrar que se $\phi(\overline{a}) = \phi(\overline{b})$; isto é, se $([x]_m, [x]_n) = ([y]_m, [y]_n)$ então $\overline{a} = \overline{b}$.

De fato, $[x]_m = [y]_m$ implica que $m|(y - x)$. Da mesma forma, como $[x]_n = [y]_n$, temos que $n|(y - x)$. Ainda, como $mdc(m, n) = 1$ segue que $(mn)|(y - x)$ donde $\overline{x} = \overline{y}$, como queriamos demonstrar.

Finalmente, como $\mathbb{Z}_{mn}$ e $\mathbb{Z}_m \oplus \mathbb{Z}_n$ são conjuntos finitos com a mesma cardinalidade mn, segue imediatamente que ϕ também é sobrejetora. □

Corolario 3.3.2. *Sejam m e n inteiros positivos, relativamente primos. Então*

$$\varphi(mn) = \varphi(m)\varphi(n).$$

Demonstração. Como $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \oplus \mathbb{Z}_n$, o número de elementos inversíveis em $\mathbb{Z}_{mn}$ deve ser igual ao número de elementos inversíveis em $\mathbb{Z}_m \oplus \mathbb{Z}_n$.

Como um elemento $\overline{a} \in \mathbb{Z}_{mn}$ é inversível se e somente se $mdc(a, mn) = 1$, temos que o número de inversíveis em $\mathbb{Z}_{mn}$ é $\varphi(mn)$.

Por outro lado, um par $([x]_n, [y]_m) \in \mathbb{Z}_m \oplus \mathbb{Z}_n$ é inversível se e somente se $[x]_n$ é inversível em $\mathbb{Z}_m$ e $[y]_n$ é inversível em $\mathbb{Z}_n$. Logo, o número de elementos inversíveis em $\mathbb{Z}_m \oplus \mathbb{Z}_n$ é $\varphi(m)\varphi(n)$.

Consequentemente, $\varphi(mn) = \varphi(m)\varphi(n)$, como queríamos demonstrar. □

Este resultado pode-se estender facilmente, usando indução, ao seguinte.

Corolario 3.3.3. *Sejam $m_1, m_2 \ldots, m_t$ inteiros Sejam $m_1, m_2 \ldots, m_t$ inteiros relativamente primos e seja $m = m_1 m_2 \cdots m_t$. Então:*

$$\mathbb{Z}_m \;\cong\; \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_t}.$$

Finalmente, podemos calcular o valor de φ em qualquer inteiro positivo n.

Teorema 3.3.4. *Seja n um inteiro positivo e seja $n = p_1^{n_1} p_2^{n_2} \cdots p_t^{n_t}$ a decomposição de n como produto de primos distintos. Então;*

$$\varphi(n) = p_1^{n_1-1}(p_1 - 1)p_2^{n_2-1}(p_2 - 1)\cdots p_t^{n_t-1}(p_t - 1),$$

ou, equivalentemente,

$$\varphi(n) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

Demonstração. Do Corolário 3.3.3 temos que

$$\varphi(n) = \varphi(p_1^{n_1})\varphi(p_2^{n_2})\cdots\varphi(p_t^{n_t})$$

e, calculando φ em cada potência de primo:

$$\varphi(n) = p_1^{n_1-1}(p_1 - 1)p_2^{n_2-1}(p_2 - 1)\cdots p_t^{n_t-1}(p_t - 1).$$

Note ainda que

$$\begin{aligned} \varphi(n) &= p_1^{n_1}\left(1 - \frac{1}{p_1}\right) p_2^{n_2}\left(1 - \frac{1}{p_2}\right)\cdots p_t^{n_t}\left(1 - \frac{1}{p_t}\right) \\ &= \varphi(n) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right). \end{aligned}$$

□

Concluímos esta seção com uma observação simples, mas extremamente útil.

Proposição 3.3.5. *Para todo inteiro positivo n tem se que*

$$\varphi(n) = \sum_{d \mid n} \varphi(d).$$

Demonstração.

Seja A um grupo cíclico de ordem n e seja d um divisor de n. Pelo Teorema 3.2.4 sabemos que A contém um único grupo cíclico de ordem d e, pelo Corolário 3.2.7 este subgrupo contém exatamente $\varphi(d)$ elementos de ordem d.

Estes são , necessariamente, os únicos elementos de ordem d em A pois, caso contrário, A teria mais de um subgrupo de ordem d, o que não pode acontecer por causa da parte (ii) do Teorema 3.2.4.

Como cada elemento de A tem ordem divisor de d, contando todos os elementos de A temos que

$$\varphi(n) = \sum_{d \mid n} \varphi(d).$$

□

EXERCÍCIOS

---

1. Calcular $\varphi(36), \varphi(81)$ e $\varphi(120)$.

2. Mostre que, o fato da função ϕ definida na demonstração do Teorema 3.3.1 ser sobrejetora significa que, se m e n são inteiros relativamente primos, dados inteiros positicos c_1, c_2 o sistema

$$\begin{aligned} X &\equiv c_1 \pmod{m} \\ X &\equiv c_2 \pmod{m} \end{aligned}$$

   sempre tem solução em $\mathbb{Z}$.

   Mostre que esta solução é única, módulo mn,

3. Provar que, se n é um inteiro positivo ímpar, então $\varphi(2n) = \varphi(n)$ e $\varphi(4n) = 2\varphi(n)$.

4. Determinar todos os inteiros positivos n tais que $\varphi(n) = 2$.

5. Mostrar que, para todo inteiro positivo n tem-se que $\varphi(n^k) = n^{k-1}\varphi(n)$.

6. Mostrar que, se $mdc(m, n) = 2$ então $\varphi(mn) = 2\varphi(n)\varphi(m)$.

7. Provar que

   (i) $\varphi(3n) = 3\varphi(n)$ se e somente se $3 \mid n$.

(ii) $\varphi(3n) = 2\varphi(n)$ se e somente se $3 \nmid n$.

8. Provar que $\varphi(n) = n/2$ se e somente se $n = 2^m$, com $m \geq 1$.

9. Provar que

   (i) Se p e $p+2$ são ambos primos, então $\varphi(p+2) = \varphi(p) + 2$.

   (ii) Se $p > 2$ e $2p+1$ são ambos primos, então $\varphi(4p+2) = \varphi(4p) + 2$.

10. Sejam d e n inteiros positivos tais que $d \mid n$. Provar que

$$n - \varphi(n) > d - \varphi(d).$$

11. Sejam p um primo e n um inteiro positivo. Provar que

$$\sum_{d|(p^n-1)} \varphi(d) = p^n - 1.$$

12. Seja $\mathbb{F}$ um corpo. Provar que um polinômio irredutível $f \in \mathbb{F}[X]$ e seu recíproco, tem a mesma ordem.

3.4 O grupo multiplicativo de um corpo

Como observamos no fim da seção 3.1, nossa intenção agora é mostrar que o grupo multiplicativo $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$ de um corpo finito $\mathbb{F}$ é cíclico.

Lema 3.4.1. *Seja G um grupo finito de ordem n tal que, para todo divisor d de n a equação $X^d = 1$ tem, no máximo, d soluções em G. Então G é um grupo cíclico.*

Demonstração. Seja $\psi(d)$ o número de elementos de ordem d em G. Se $a \in G$ é um elemento de ordem d, então os elementos $1, a, a^2, \ldots a^{d-1}$ são soluções da equação $X^d = 1$ em G e, pela hipótese do teorema, são todas as soluções. Dentre estas, existem $\varphi(d)$ elementos que são de ordem d. Portanto, se existe um elemento de ordem d em G temos que $\psi(d) = \varphi(d)$.

Por outro lado, se não há elementos de ordem d em G, temos $\psi(d) = 0 \leq \varphi(d)$. Consequentemente, para todo divisor d de n tem-se que $\psi(d) \leq \varphi(d)$.

Como todo elemento de G tem ordem divisor de n temos que $\sum_{d|n} \psi(d) = n$. Da Proposição 3.3.5 segue então que

$$n = \sum_{d|n} \psi(d) \leq \sum_{d|n} \varphi(d) = n.$$

Logo, deve ser $\psi(d) = \varphi(d) \geq 1$, para todo divisor d de n. Em particular. $\psi(n) = \varphi(n) \neq 0$, o que mostra que G contém algum elemento a de ordem n. Logo, $G = \{1, a, a^2, \ldots, a^{n-1}\}$, é cíclico. □

Agora estamos em condições de provar o resultado principal desta seção.

Teorema 3.4.2. *Seja $\mathbb{F}$ um corpo. Todo subgrupo finito do grupo multiplicativo $\mathbb{F}^*$ é cíclico.*

Demonstração. Com efeito, seja G um subgrupo finito de $\mathbb{F}^*$. Do Teorema 2.2.4 temos que, para cada divisor d de n, o número de raizes da equação $X^d - 1 = 0$ é no máximo d. Pelo Lema 3.2.1, segue diretamente que G é cíclico. □

Um caso particularmente importante é o seguinte.

Corolario 3.4.3. *Seja $\mathbb{F}$ um corpo finito. Então, o grupo multiplicativo $\mathbb{F}^*$ é cíclico.*

Este resultado permite mostrar que o Teorema do Elemento Primitivo **??**, vale também para corpos finitos.

Teorema 3.4.4. *Sejam $\mathbb{F} \subset \mathbb{E}$ corpos finitos. Então, existe um elemento $\alpha \in \mathbb{E}$ tal que $\mathbb{E} = \mathbb{F}(\alpha)$.*

Demonstração. Seja $\alpha \in \mathbb{E}$ é um gerador do grupo multiplicativo $\mathbb{E}^*$. Então todos os elementos não nulos de $\mathbb{E}$ são potências de α; portanto, eles pertencem ao corpo $\mathbb{F}(\alpha)$. Como também $0 \in \mathbb{F}(\alpha)$ segue que $\mathbb{E} \subset \mathbb{F}(\alpha)$. A inclusão contrária é obviamente válida; logo, $\mathbb{E} = \mathbb{F}(\alpha)$. □

Definição 3.4.5. *Sejam $\mathbb{F} \subset \mathbb{E}$ corpos. Um elemento $\alpha \in \mathbb{E}$ tal que $\mathbb{E} = \mathbb{F}(\alpha)$ diz-se um* **elemento primitivo** *de $\mathbb{E}$ sobre $\mathbb{F}$.*

Provamos, no Teorema 3.1.4, que $\mathbb{F}_{q^n}$ é o corpo de decomposição do polinômio $x^{q^n} - X$ sobre $\mathbb{F}_q$. Portanto, $\mathbb{F}_{q^n}$ é uma extensão normal de $\mathbb{F}_q$.

Seja $f \in \mathbb{F}_q[X]$ um polinômio irredutível que tem uma raiz α em $\mathbb{F}_{q^n}$. Pelo Teorema **??**, como f tem uma raiz em $\mathbb{F}_{q^n}$, f tem todas suas raízes em $\mathbb{F}_{q^n}$.

Seja $f \in \mathbb{F}[X]$ é um polinômio mônico, irredutível. Se uma das raízes de f é um elemento primitivo de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ (e portanto, todas suas raízes o são) então necessáriamente f tem grau igual a n. Recíprocamente, se $gr(f) = n$ então cada uma de suas raízes é um elemento primitivo de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$.

Definição 3.4.6. *Um polinômio mônico, irredutível, $f \in \mathbb{F}_q[X]$, com de $gr(f) = n$ diz-se um* **polinômio primitivo** *para $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$.*

Exemplo 3.4.7.

O polinômio $X^3 + X + 1$ é irredutível em $\mathbb{F}_2[X]$, como observamos no Exemplo 2.3.2. Logo

$$\mathbb{E} = \frac{\mathbb{F}_2[X]}{(X^3 + X + 1)}$$

é um corpo com 8 elementos e $X^3 + X + 1$ é um polinômio primitivo de grau 3 sobre $\mathbb{F}_2$.

Se denotamos por t uma raiz de f podemos realizar este corpo na forma

$$\mathbb{E} = \{a_0 + a_1 t + a_2 t^2 \mid a_0, a_1, a_2 \in \mathbb{F}_2\}$$

levando em consideração que $t^3 = 1 + t$.

Calculando as potências de t temos:

$$\begin{array}{llll} t^0 = 1, & t^1, = t & t^2 = t^2, & t^3 = 1 + t, \\ t^4 = t + t^2, & t^5 =^1 + t + t^2, & t^6 = 1 + t^2, & t^7 = t + t^3 = 1. \end{array}$$

Logo, t é um gerador de $\mathbb{E}^*$.

Sejam $\mathbb{F} \subset \mathbb{E}$ corpos finitos. Se $\alpha \in \mathbb{E}$ é um gerador do grupo multiplicativo $\mathbb{E}^*$, então todos os elementos não nulos de $\mathbb{E}$ são potências de α; portanto, eles pertencem ao corpo $\mathbb{F}(\alpha)$. Como também $0 \in \mathbb{F}(\alpha)$ segue que $\mathbb{E} \subset \mathbb{F}(\alpha)$. Como a inclusão contrária é obviamente válida, tem-se que que $\mathbb{E} = \mathbb{F}(\alpha)$.

Exemplo 3.4.8.

Considere o polinômio $X^2 - 2 \in \mathbb{F}_5[X]$ que é irredutível, pois não tem raízes em $\mathbb{F}_5$. Então

$$\mathbb{F}_{25} = \frac{\mathbb{F}_5[X]}{(x^2-2)} \cong \mathbb{F}_5(t) = \{a_0 + a_1 t \mid t^2 = 2\}.$$

Vamos procurar um elemento primitivo deste corpo osbre $\mathbb{F}_5$; i.e. um elemento cuja ordem multiplicativa seja 24. Para isso calculamos:

$t^0 = 1$, $t^1 = t$, $t^2 = 2$, $t^3 = 2t$,
$t^4 = 2t^2 = 4$, $t^5 = 4t$, $t^6 = 4t^2 = 3$, $t^7 = 3t$, $t^8 = 1 = t^0$.

Logo, $o(t) = 8$. Nenhum dos elementos listados acima pode ser primitivo, pois todos eles pertencem a um subgrupo de ordem 8.

Tentamos então outro elemento. Escolhemos $\alpha = 1 + t$. Calculando, obtemos:

$$\alpha^1 = 1 + t, \quad \alpha^2 = 1 + 2t + t^2 = 3 + 2t, \quad \alpha^3 = (3 + 2t)(1 + t) = 2,$$
$$\alpha^4 = 2 + 2t, \quad \alpha^5 = (2 + 2t)(1 + t) = 1 + 4t, \quad \alpha^6 = (1 + 4t)(1 + t) = 4.$$

Neste ponto, notamos que $\alpha^{12} = (\alpha^6)^2 = 1$. Consequentemente, $o(\alpha)$ é um divisor de 12, e nossos cálculos mostraram que é maior que seis. Logo, $o(\alpha) = 12$.

Note que $o(\alpha^4) = 12/4 = 3$. Então, $mmc(o(t), o(\alpha^4)) = 1$ e, pelo Lema 3.2.5, temos que $o(t.\alpha^4) = o(t)o(\alpha^4) = 8 \times 3 = 24$. Como $\alpha^4 = 2 + 2t$ temos que

$$\gamma = t(2 + 2t) = t + 2t^2 = 2 + 2t$$

é um elemento primitivo de $\mathbb{F}_{25}$.

A técnica usada no exemplo acima para determinar um elemento gerador é, na verdade, um caso particular de um método, devido a Gauss, para determinar o gerador de um grupo cíclico.

Seja A um grupo cíclico de ordem n e seja α_1 um elemento qualquer de A. Seja α_2 outro elemento de A que não pertence a $\langle \alpha_1 \rangle$. Sejam m_1 e m_2 as respectivas ordens. Escrevemos a desomposição em fatores primos de ambas ordens, de tal forma que compareçam os mesmos primos em ambas. Para isso, basta completar as decomposições, adicionando primos, elevados

ao expoente 0, quando necessário. Mais ainda, podemos reordenar os primos de modo que compareçam primeiro os primos que têm expoente maior em m_1 e depois os que têm expoente maior em m_2. Mais precisamente, escrevemos:

$$\begin{aligned} \alpha_1 &= p_1^{a_1} \cdots p_r^{a_r}.p_{r+1}a_{r+1} \cdots p_k^{a_k}, \\ \alpha_2 &= p_1^{b_1} \cdots p_r^{b_r}.p_{r+1}b_{r+1} \cdots p_k^{b_k}, \end{aligned}$$

onde assumimos que $b_i \leq a_i$ para $1 \leq i \leq r$ e $b_i > a_i$ para $r+1 \leq i \leq k$.

Tomamos então:

$$d_1 = p_1^{a_1} \cdots p_r^{a_r} \quad \text{e} \quad d_2 = p_{r+1}b_{r+1} \cdots p_k^{b_k},$$

e definimos $\alpha_3 = d_1.d_2$

Note que $mdc(d_1, d_2) = 1$ e que $o(\alpha_3) = mmc(d_1, d_2)$. Como $\alpha_2 \notin \langle \alpha_1 \rangle$ segue que m_1 não pode ser um divisor de m_2 e, consequentemente, $o(\alpha_2) < o(\alpha_3)$.

Se α_3 não é um gerador de A, repetimos o processo.

Desta forma, obtemos uma sequência de elementos tal que $o(\_2) < o(\alpha + 3) < \cdots \leq |A|$.

Como esta sequência está limitada por $|A|$, deve terminar. O último elemento achado é um gerador de A. Este processo da orígem a um algoritmo, que pode ser implementado para achar um elemento primitivo de um corpo $\mathbb{F}_q$, com q elementos.

Algoritmo de Gauss.

(1) Escreva $i = 1$ e determine um um elemento α_i de $\mathbb{F}_q^*$. Calcule $o(\alpha_i) = m_i$.

(2) Se $o(\alpha_i) = q - 1$, pare.

(3) Se $o(\alpha_i) \neq q - 1$, escolha um elemento $\gamma \in (\mathbb{F}_q^* \setminus \langle \alpha_i \rangle)$. Calcule $o(\gamma) = m$.

(4) Se $o(\gamma) = q - 1$ pare; γ é um gerador de $\mathbb{F}^*$.

(5) Se $o(\gamma) \neq q - 1$ determine divisores d_i e d de m_i e m respectivamente tais que $mdc(d_1, d_2) = 1$.

(6) Calcule $\alpha_{i+1} = \alpha_i^{m_i/d_i}.\gamma^{m/d}$.

(7) Se $d_i.d = q-1$ pare; α_{i+1} é um gerador de $\mathbb{F}^*$.

(8) Caso contrário, escreva $\alpha_i = \alpha_{i+1}$ e volte a (3).

EXERCÍCIOS

---

1. Seja p um inteiro primo. Provar que o grupo multiplicativo $\mathbb{Z}_p^*$ é cíclico. Determinar um gerador de cada um dos seguintes grupos: $\mathbb{Z}_5, \mathbb{Z}_{17}$ e $\mathbb{Z}_{31}$.

2. Provar que o corpo $\mathbb{F} = \mathbb{Z}_3[X]/(X^2+2X+2)$ tem nove elementos e determinar todos os geradores do grupo cíclico $\mathbb{F}^*$.

3. Provar que X^2-1 é irredutível sobre $\mathbb{F}_3$ e, se $\mathbb{E} = \mathbb{F}_3[X]/(X^2-1)$, determinar todos todos os geradores de $\mathbb{E}^*$.

4. Determinar os polinômios minimais dos elementos de $\mathbb{F}_{16}$ sobre $\mathbb{F}_4$.

5. Seja $\mathbb{F}$ um corpo finito com q elementos. Provar que o grupo aditivo $(\mathbb{F},+)$ é cíclico se e somente se q é primo.

6. Seja p um inteiro primo. Provar que $\mathbb{Z}_{p^2}$ não é um corpo e mostrar que, mesmo assim, o conjunto $\mathcal{U}(\mathbb{Z}_{p^2})$ dos elementos inversíveis de $\mathbb{Z}_{p^2}$ é um grupo cíclico de ordem $p(p-1)$.

7. Determinar todos os subgrupos finitos do corpo $\mathbb{C}$ dos números complexos.

8. Achar todos os elementos primitivos dos corpos $\mathbb{F}_7$, $\mathbb{F}_{11}$, $\mathbb{F}_{13}$ e $\mathbb{F}_{17}$.

9. Provar que 3 e 5 são elementos primitivos em $\mathbb{F}_7$. Escrever 2 como potência de 3 e de 5 e, $\mathbb{F}_7$.

10. Provar que 2 é um elemento primitivo em $\mathbb{F}_3$ e $\mathbb{F}_5$, mas não em $\mathbb{F}_7$.

11. Determinar o menor inteiro primo $p > 7$ tal que 2 não é um elemento primitivo de $\mathbb{F}_p$.

12. Provar que o polinômio $X^3 + X^2 + 1$ é irredutível em $\mathbb{F}_2[X]$, determinar um gerador de
$$\frac{\mathbb{F}_2[X]}{(X^3 + X^2 + 1)}$$
e exibir um isomorfismo
$$\phi : \frac{\mathbb{F}_2[X]}{(X^3 + X + 1)} \longrightarrow \frac{\mathbb{F}_2[X]}{(X^3 + X^2 + 1)}.$$

13. Provar que o polinômio $X^4 + X + 1$ é irredutível em $\mathbb{F}_2[X]$ e determinar um gerador do corpo
$$\mathbb{F}_{16} = \frac{\mathbb{F}_2[X]}{(X^4 + X + 1)}.$$

14. Seja $\mathbb{F}$ um corpo qualquer. Provar que, se $\mathbb{F}^*$ é cíclico, então $\mathbb{F}$ é um corpo finito. (Sugestão: mostre que $\mathbb{F}^*$ não pode ser um grupo cíclico infinito.)

15. Mostre que
$$\mathbb{E} = \frac{\mathbb{F}_5[X]}{(X^2 + 2)}$$
é um corpo. Construa explicitamente um isomorfismo $\phi : \mathbb{E} \to \mathbb{F}_{25}$ onde $\mathbb{F}_{25}$ denota o corpo construido no Exemplo 3.4.8

3.5 Subcorpos de um corpo finito

Pretendemos agora determinar todos os subcorpos de um corpo finito dado. Para isso, precisaremos de um lema sobre divisibilidade de polinômios que, embora simples, nos dará todas a informação necessária para resolver esta questão.

Lema 3.5.1. *Sejam $m < n$ inteiros positivos. Então $X^m - 1$ divide $X^n - 1$ se e somente se m divide n.*

Demonstração. Sejam q e r o quociente e resto de dividir n por m. Então $n = mq + r$, com $0 \leq r < m$.

Temos então

$$\begin{aligned} X^n - 1 &= X^{mq+r} - 1 \\ &= X^{mq+r} - X^{mq+(r-1)} + X^{mq+(r-1)} - X^{mq+(r-2)} + \cdots + X^r - 1 \\ &= (X^m - 1)X^{m(q-1)+r} + (X^m - 1)X^{m(q-2)+r} + \cdots + (X^r - 1) \end{aligned}$$

Desta igualdade segue que $x^m - 1$ divide $X^n - 1$ se e somente se $x^m - 1$ divide $X^r - 1$. Como $r < m$, isto acontece se e somente se $r = 0$. □

Note que o mesmo argumento, substituíndo X por um primo p permite provar o seguinte.

Lema 3.5.2. *Sejam p um inteiro primo e $m < n$ inteiros positivos. Então $p^m - 1$ divide $p^n - 1$ se e somente se m divide n.*

Temos agora uma consequência interessante.

Proposição 3.5.3. *Sejam p um inteiro primo e $m < n$ inteiros positivos. Então $X^{p^m-1} - 1$ divide $X^{p^n-1} - 1$ se e somente se m divide n.*

Equivalentemente, $(X^{p^m} - X) \mid (X^{p^n} - X)$ se e somente se $m \mid n$.

Demonstração. Pelo Lema 3.5.1, $X^{p^m-1} - 1 \mid X^{p^n-1} - 1$ se e somente se $p^m - 1 \mid p^n - 1$ e, pelo Lema 3.5.2, isto acontece se e somente se $m \mid n$.

A segunda afirmação seque imediatamente da anterior. □

Note que, dado um corpo finito $\mathbb{F}_{p^n}$, seu corpo primo é $\mathbb{F}_p$. Todo subcorpo de $\mathbb{F}_{p^n}$ deve ser uma extensão de $\mathbb{F}_p$, portanto, da forma $\mathbb{F}_{p^m}$, para algum inteiro positivo m. Podemos agora descrever todos os subcorpos de um corpo finito.

Teorema 3.5.4. *Seja $\mathbb{E} = \mathbb{F}_{p^n}$ um corpo finito. Então $\mathbb{E}$ contém um subcorpo com p^m elementos se e somente se $m \mid n$. Neste caso, $\mathbb{E}$ contém um único subcorpo desta ordem.*

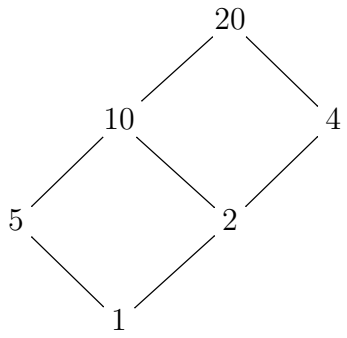
Demonstração. Seja $\mathbb{E} = \mathbb{F}_{p^n}$ e seja $\mathbb{K} = \mathbb{F}_{p^m}$ um subcorpo de $\mathbb{E}$. Então $\mathbb{K}^*$ é um subgrupo multiplicativo de $\mathbb{E}^*$. Logo $|\mathbb{K}^*| = p^m - 1$ é um divisor de $\mathbb{E}^* = p^n - 1$. Do Lema 3.5.1 vem imediatamente que $m \mid n$.

Reciprocamente, se $m \mid n$ então $X^{p^m} - X \mid X^{p^n} - X$. Todo elemento de $\mathbb{K}$ é raiz de $X^{p^m} - X$ e, portanto, também de $X^{p^n} - 1X$. Como $\mathbb{E}$ é o corpo de raízes deste polinômio, todo elemento de $\mathbb{K}$ pertence a $\mathbb{E}$.

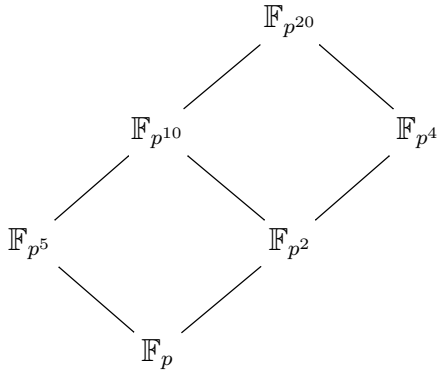
Como um grupo cíclico contém um único subgrupo de uma dada ordem, $\mathbb{K}$ é o único subcorpo de $\mathbb{E}$ de ordem p^m. □

Exemplo 3.5.5.

Seja $\mathbb{E} = \mathbb{F}_{20}$. Os divisores de 20 são $1, 2, 4, 5, 10$ e 20. Podemos representá-los num reticulado, ordenado pela relação "divide".



Consequentemente, o reticulado de subcorpos de $\mathbb{F}_{q^{20}}$ é



O conhecimento dos subcorpos de um corpo finito permite construir explicitamente o fecho algébrico de um corpo finito, veja o Exercício 4.

EXERCÍCIOS

1. Determinar o reticulado de subgrupos de $\mathbb{F}_{2^{30}}$, $\mathbb{F}_{3^{30}}$ e $\mathbb{F}_{5^{32}}$.

2. Sejam n e m inteiros positivos. Provar que, se $d = mdc(n, m)$, então
$$\mathbb{F}_{q^n} \cap \mathbb{F}_{q^m} = \mathbb{F}_{q^d}.$$

3. Prove que os seguintes conjuntos, com as obvias relações de ordem em cada um deles, são isomorfos como retivulados:

   (i) Divisores de n.

   (ii) Divisores de $x^{p^n-1}-1$.

   (iii) Subcorpos de $\mathbb{F}_{p^n}$.

4. Seja $\mathbb{F}_q$ um corpo finito.

   (i) Provar que, para todo inteiro positivo n tem-se que $\mathbb{F}_{q^{n!}} \subset \mathbb{F}_{q^{(n+1)!}}$.

   (ii) Provar que $\Gamma(q) = \bigcup_{n=1}^{\infty} F_{q^{n!}}$ é um corpo.

   (iii) Provar que $\Gamma(q)$ é o fecho algébrico de $\mathbb{F}_q$.

5. Provar que $\Gamma(q)$ não contém subcorpos maximais.

6. Provar que, se $\mathbb{K}$ é um subcorpo próprio de $\Gamma(q)$, então $[\Gamma(q) : \mathbb{K}]$ não é finita.

7. Mostre que, para todo par de inteiros positivos m e n, tem-se que $\Gamma(q^m) = \Gamma(q^n)$.

3.6 Apêndice: o grupo das unidades de $\mathbb{Z}_m$

Nosso objetivo, agora é descrever a estrutra do grupo $\mathcal{U}(\mathbb{Z}_n)$ das unidades do anel dos inteiros módulo m . Para isso vamos proceder por etapas. Primeiro mostraremos que o problema pode ser reduzido a estudar grupos de unidades da forma $\mathcal{U}(\mathbb{Z}_{p^m})$, com p primo.

Se $p \neq 2$, não é difícil descrever a estrutura do grupo de unidades correspondente. Já no caso em que $p = 2$ será necessário um pouco mais de cuidado, mas argumentos razoavelmente elemetares permitirão descrever também a estrutura deste grupo.

De posse de todas estas informações, será fácil descrever $\mathcal{U}(\mathbb{Z}_n)$ e decidir, em particular, quando este grupo é cíclico.

Lembramos que provemos no Corolário 3.3.3 que, se $m_1, m_2 \ldots, m_t$ inteiros dois a dois relativamente primos, então denotando $m = m_1 m_2 \cdots m_t$ temos que:

$$\mathbb{Z}_m \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_t}.$$

Notamos ainda que, como se trata de um isomorfismo de anéis, elementos inversíveis de $\mathbb{Z}_m$ se correspondem com elementos inversíveis de $\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_t}$ e que um elemento é inversível nessa soma direta se cada uma de suas componentes é inversível no anel correspondente. Desta forma obtemos, por restrição um isomorfismo de grupos multiplicativos:

$$\mathcal{U}(\mathbb{Z}_m) \cong \mathcal{U}(\mathbb{Z}_{m_1}) \times \mathcal{U}(\mathbb{Z}_{m_2}) \times \cdots \times \mathcal{U}(\mathbb{Z}_{m_t}). \tag{3.1}$$

Um caso particularmente interessante é o seguinte. Dado um número m, consideramos sua decomposição em fatores primos:

$$m = p_1^{m_1} p_2^{m_2} \cdots p_t^{m_t}.$$

Aplicando o resultado acima, neste caso, obtemos que:

$$\mathcal{U}(\mathbb{Z}_m) \cong \mathcal{U}(\mathbb{Z}_{p_1^{m_1}}) \times \mathcal{U}(\mathbb{Z}_{p_2^{m_2}}) \times \cdots \times \mathcal{U}(\mathbb{Z}_{p_t^{m_t}})$$

e, como o número de elementos em cada um desses grupos pode ser calculado utilizando a função de Euler, isto é uma nova demonstração de que, dado $m = p_1^{m_1} p_2^{m_2} \cdots p_t^{m_t}$ tem-se que:

$$\varphi(m) = \varphi(p_1^{m_1})\varphi(p_2^{m_2}) \cdots \varphi(p_t^{m_t}).$$

Portanto, para descrever $\mathcal{U}(\mathbb{Z}_m)$ precisamos conhecer a estrutura de cada um dos fatores da forma $\mathcal{U}(\mathbb{Z}_{p^{m_i}})$.

Precisamos demonstrar um resultado de natureza técnica, que será necessário adiante.

Lema 3.6.1. *Sejam m um inteiro positivo, p um primo ímpar e k um inteiro qualquer. Então:*

$$(1 + kp)^{p^{m-1}} \equiv 1 + kp^m \pmod{\mathrm{p}^{m+1}}.$$

Demonstração. Vamos demonstrar o resultado por indução. Para $m = 1$ o enunciado afirma que

$$(1 + kp)^{p^0} \equiv 1 + kp \pmod{\mathrm{p}^2},$$

o que é obviamente verdadeiro.

Supomos então que $(1 + kp)^{p^{m-1}} \equiv 1 + kp^m \pmod{\mathrm{p}^{m+1}}$ é verdadeiro e vamos demonstrar que

$$(1 + kp)^{p^m} \equiv 1 + kp^{m+1} \pmod{\mathrm{p}^{m+2}}.$$

Da nossa hipótese de indução temos que existe algum $t \in \mathbb{Z}$ tal que

$$(1+kp)^{p^{m-1}} = 1 + kp^m + tp^{m+1}$$

Logo,

$$\begin{aligned}(1+kp)^{p^m} &= \left((1+kp)^{p^{m-1}}\right)^p = \left(1+kp^m+tp^{m+1}\right)^p \\ &= (1+p^m(k+tp))^p \\ &= 1+p^m.\binom{p}{1}(k+tp) + \sum_{i=2}^{p}\binom{p}{i}(p^m)^i(k+tp)^i.\end{aligned}$$

Note que, quando $i \geq 2$ tem-se que $mi \geq m+2$ donde todos os termos da somatória acima são múltiplos de p^{m+2} e existe um inteiro t' tal que

$$\sum_{i=2}^{p}\binom{p}{i}(p^m)^i(k+tp)^i = t'p^{m+2}.$$

Ainda, como $\binom{p}{1} = p$ temos que

$$(1+kp)^{p^m} = 1 + kp^{m+1} + tp^{m+2} + t'p^{m+2},$$

donde

$$(1+kp)^{p^m} \equiv 1 + kp^{m+1} \pmod{p^{m+2}},$$

como queriamos demonstrar. □

Lema 3.6.2. *Sejam p um primo ímpar e m um inteiro positivo. O grupo $\mathcal{U}(\mathbb{Z}_{p^m})$ contém um elemento de ordem $p-1$.*

Demonstração. Como $\mathbb{Z}_p$ é um corpo, o grupo $\mathcal{U}(\mathbb{Z}_p)$ é cíclico; logo, exite um inteiro positivo b tal que $o(\bar{b}) = p-1$.

Seja $a = b^{p^{m-1}}$ e seja α a classe de a em $\mathbb{Z}_{p^m}$. Afirmamos que α é um elemento de ordem $p-1$ em $\mathcal{U}(\mathbb{Z}_{p^m})$.

Com efeito, calculamos:

$$a^{p-1} = \left(b^{p^{m-1}}\right)^{p-1} = \left(b^{p-1}\right)^{p^{m-1}} = (1+kp)^{p^{m-1}}.$$

Do lema anterior vem imediatamente que

$$a^{p-1} \equiv 1 + kp^m \pmod{p^{m+1}},$$

então

$$a^{p-1} \equiv 1 \pmod{p^m},$$

donde, tomando classes, segue que $\alpha^{p-1} = 1$ em $\mathcal{U}(\mathbb{Z}_{p^m})$. Logo

$$o(\alpha) \mid p-1. \tag{3.2}$$

Por outro lado, temos que

$$a^{o(\alpha)} = b^{o(\alpha)p^{m-1}}$$

e, como $\alpha^{o(\alpha)} = 1$ em $\mathcal{U}(\mathbb{Z}_{p^m})$, temos que $a^{o(\alpha)} \equiv 1 \pmod{p^m}$ donde $b^{o(\alpha)p^{m-1}} \equiv 1 \pmod{p^m}$.

Se p^m divide $b^{o(\alpha)p^{m-1}} - 1$, em particular temoq também que p divide $b^{o(\alpha)p^{m-1}} - 1$ donde

$$\overline{b}^{o(\alpha)p^{m-1}} = \overline{1} \quad \text{em} \quad \mathbb{Z}_p.$$

Como b tem ordem $p-1$ em $\mathbb{Z}_p$, segue que

$$(p-1) \mid o(\alpha). \tag{3.3}$$

De (3.2) e (3.3) vem que $o(\alpha) = p-1$, como queríamos demonstrar. □

Lema 3.6.3. *Seja β a classe do inteiro $1+p$ em $\mathcal{U}(\mathbb{Z}_{p^m})$. Então $o(\beta) = p^{m-1}$.*

Demonstração. Mais uma vez, do Lema 3.6.1, vem que

$$(1+p)^{p^{m-1}} \equiv 1 \pmod{p^m}.$$

Isto significa que $\beta^{p^{m-1}} = 1$ em $\mathbb{Z}_{m^m}$, donde $o(\beta) \mid p^{m-1}$. Portanto, $o(\beta)$ deve ser da forma $o(\beta) = p^s$, com $0 \leq s \leq m-1$.

Queremos provar que $s = m-1$. Por absurdo, se fosse $s < m-1$ ter-se-ia que $\beta^{p^s} = \overline{1}$ em $\mathbb{Z}_{p^m}$; isto é, que

$$(1+p)^{p^s} \equiv 1 \pmod{p^m}. \tag{3.4}$$

Por outro lado, aplicando novamente o Lema 3.6.1 temos que

$$(1+p)^{p^s} = 1 + p^{s+1} \pmod{p^{s+2}}. \tag{3.5}$$

Como $s < m-1$ temos que $s+2 \leq m$, portanto a equação (3.4) implica também que

$$(1+p)^{p^s} \equiv 1 \pmod{p^s}$$

e, em (3.5) resulta que

$$1 \equiv 1 + p^{s+1} \pmod{p^{s+2}},$$

o que implica que $p^{s+2} \mid p^{s+1}$, uma contradição. □

Estamos agora em condições de descrever o grupo $\mathcal{U}(\mathbb{Z}_{p^m})$, quando $p \neq 2$.

Teorema 3.6.4. *Seja p um primo ímpar e sejam α e β os elementos definidos nos lemas 3.6.2 e 3.6.3 respectivamente. Então o grupo $\mathcal{U}(\mathbb{Z}_{p^m})$ é cíclico e o elemento $\alpha\beta$ é um gerador deste grupo.*

Demonstração. Lembramos que $|\mathcal{U}(\mathbb{Z}_{p^m}| = \varphi(p^m) = p^{m-1}(p-1)$.

Por outro lado, como $o(\alpha) = p-1$ e $o(\beta) = p^{m-1}$ e estes inteiros são relativamente primos, o produto destes elementos tem ordem

$$o(\alpha\beta) = (p-1)p^{m-1}.$$

Isto implica que $\langle \alpha\beta \rangle = \mathcal{U}(\mathbb{Z}_{p^m})$ e segue a tese. □

Nosso interesse agora é descrever também o grupo de unidades $\mathcal{U}(\mathbb{Z}_{2^m})$. Claramente, $\mathcal{U}(\mathbb{Z}_2) = \{1\}$ e é fácil verificar diretamente que $\mathcal{U}(\mathbb{Z}_4) = \{\overline{1}, \overline{3}\}$ é um grupo cíclico de ordem 2. Veremos que estes são os únicos casos em que $\mathcal{U}(\mathbb{Z}_{2^m})$ é cíclico.

Como antes, precisaremos provar alguns resultados técnicos.

Lema 3.6.5.

(*i*) *Para todo inteiro b ímpar e todo inteiro $m \geq 2$ tem-se que*

$$b^{2^{m-2}} \equiv 1 \pmod{2^m}.$$

(*ii*) *Para todo inteiro positivo t tem-se que*

$$5^{2^t} \equiv 1 + 2^{t+2} \pmod{2^{t+3}}.$$

Demonstração.

(i) Vamos provar a validade da fórmula por indução. Para $m = 2$, como b é impar, podemos escrevê-lo na forma $b = 2t + 1$, com $t \in Z$ e temos que

$$b^2 = (2t+1)^2 = 4t^2 + 4t + 1, \quad \text{donde} \quad b^2 \equiv 1 \pmod{2^2}.$$

Vamos supor que a fórmula vale para $m = k \geq 0$ e vamos demonstra que vale para $m = k+1$. Nossa hipótese de indução implica que existe um inteiro λ tal que

$$b^{2^{k-2}} \equiv 1 + \lambda 2^k.$$

Calculamos então

$$\begin{aligned} b^{2^{k-1}} &= \left(b^{2^{k-2}}\right)^2 = \left(1 + \lambda 2^k\right)^2 \\ &= 1 + \lambda 2^{k+1} + \lambda^2\, 2^{2k} = 1 + 2^{k+1}\left(\lambda + \lambda^2\, 2^{k-1}\right) \end{aligned}$$

o que implica que

$$b^{2^{k-1}} \equiv 1 \pmod{2^{k+1}}$$

como queríamos demonstrar.

(ii) É imediato que a fórmula vale para $t = 0$. Mais uma vez, usando indução, vamos supor que a fórmula vale para $t = k$ e vamos provar que também vale para $t = k + 1$. Novamente, a hipótese de indução implica que existe um inteiro λ tal que

$$5^{2^k} = 1 + 2^{k+2} + \lambda 2^{k+3}.$$

Calculamos

$$\begin{aligned} 5^{2^{k+1}} &= \left(5^{2^k}\right)^2 = \left(1 + 2^{k+2} + \lambda 2^{k+3}\right)^2 = \left(1 + 2^{k+2}(1+2\lambda)\right)^2 \\ &= 1 + 2^{k+3}(1+2\lambda) + 2^{2k+4}(1+2\lambda)^2 \\ &= 1 + 2^{k+3} + 2^{k+4}\left(\lambda + 2^k(1+2\lambda)^2\right) \end{aligned}$$

o que mostra que

$$5^{2^{k+1}} \equiv 1 + 2^{k+3} \pmod{2^{k+4}}$$

e segue a tese. □

Corolario 3.6.6. *Se $m > 2$, então todo elemento de $\mathcal{U}(\mathbb{Z}_{2^m})$ tem ordem menor o igual a 2^{m-2}.*

Demonstração. De fato, dado um elemento $\overline{b} \in \mathcal{U}(\mathbb{Z}_{2^m})$, parte (i) do lema anterior temos que

$$b^{2^{m-2}} \equiv 1 \pmod{2^m}.$$

Isto significa que $\overline{b}^{2^{m-2}} = \overline{1}$ em $\mathcal{U}(\mathbb{Z}_{2^m})$ e, portanto, sua ordem é um divisor de 2^{m-2}, isto é, da forma 2^t, com $t \leq m-2$. □

Como a ordem de $\mathcal{U}(\mathbb{Z}_{2^m})$ é $\varphi(2^m) = 2^{m-1}$, o resultado acima implica o seguinte.

Corolario 3.6.7. *Se $m > 2$ então grupo $\mathcal{U}(\mathbb{Z}_{2^m})$ não é cíclico.*

Capítulo 4

Polinômios irredutíveis sobre corpos finitos

4.1 O número de polinômios irredutíveis em $\mathbb{F}_q[X]$

Provamos, na seção 3.4, que se $\mathbb{F}_q \subset \mathbb{F}_{q^n}$ são corpos finitos, então existe um elemento primitivo α de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$. Se f é o seu polinômio minimal sobre $\mathbb{F}_q$, então f é irredutível em $\mathbb{F}_q[X]$.

Sabemos que $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$. Como $\mathbb{F}_{q^n} = \mathbb{F}_q(\alpha)$, também temos que $[\mathbb{F}_{q^n}(\alpha) : \mathbb{F}_q] = gr(f)$; logo $n = gr(f)$. Esta observação simples mostra que vale o seguinte.

Lema 4.1.1. *Dado um inteiro positivo n, sempre existe pelo menos um polinômio irredutível f, de grau n, sobre $\mathbb{F}_q$.*

Corolario 4.1.2. *Se $f \in F_q[X]$ é um polinômio irredutível, de grau n, então $f \mid (X^{q^n} - X)$.*

Demonstração. De fato, seja α uma raiz de f. Como observamos acima, f é o polinômio minimal de α. Por outro lado, $\alpha \in \mathbb{F}_{p^n}$ e todo elemento de $\mathbb{F}_{p^n}$ é raiz de $X^{p^n} - X$. Logo, $f \mid (X^{p^n} - X)$. □

Corolario 4.1.3. *Seja $f \in F_q[X]$ é um polinômio irredutível, de grau d. Então $d \mid n$ se e somente se $f \mid (X^{q^n} - X)$.*

Demonstração. Seja $d = gr(f)$. Pelo corolário acima, $f \mid (X^{q^d} - X)$ e, se $d \mid n$, pelo Lema 3.5.3, tem-se que $(X^{p^d} - X) \mid (X^{p^n} - X)$; logo, $f \mid (X^{p^n} - X)$.

Reciprocamente, se $f \mid (X^{q^n} - X)$ e α é uma raiz de f, então $\mathbb{F}_q(\alpha) \subset \mathbb{F}_{q^n}$. Logo $[\mathbb{F}(\alpha) : \mathbb{F}_q] = d$ é um divisor de $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$. □

Na verdade, pode-se provar um resultado mais interessante.

Teorema 4.1.4. *Seja $\mathbb{F}_q$ um corpo finito e seja n um inteiro positivo. O produto de todos os polinômios mônicos, irredutíveis, de $\mathbb{F}_q[X]$ cujo grau é um divisor de n é, precisamente, $(X^{q^n} - X)$.*

Demonstração. Provamos acima que todo polinômio irredutível cujo grau divide n é um divisor de $X^{p^n} - X$. Como polinômios irredutíveis são relativamente primos, o produto de todos eles também dicide $(X^{p^n} - X)$.

Por outro lado, $(X^{p^n} - X)$, como todo polinômio, é o produto de divisores irredutíves em $\mathbb{F}_q[X]$, donde segue a tese. □

Queremos determminar quantos polinômios mômicos, irredutíveis, de um determinado grau m existem em $\mathbb{F}_q[X]$. Para isso, vamos denotar por $N_q(m)$ esse número.

Seja d um divisor de n. Então, o grau do produto de todos os polinômios irredutíveis de grau d que dividem $(X^{p^n} - X)$ é precisamente $d.N_q(d)$. Do Teorema acima vem imediatamente que

$$\sum_{d \mid n} d.N_q(d) = q^n. \tag{4.1}$$

A partir desta fórmula vamos obter o número que desejamos calcular. Porém, para isso será necessário introduzir primeiro uma função bem conhecida em teoria dos números.

Denotaremos por $\mathbb{Z}^+$ o conjunto dos inteiros estritamente positivos. Lembramos que um inteiro $a \in \mathbb{Z}^=$ diz-se **livre de quadrados** se não é divisível pelo quadrado de nenhum número inteiro. É fácil ver que a é livre de quadrados se e somente se sua decomposição como produto de primos é da forma $a = p_1 p_2 \cdots p_r$; i.e. se todos os primos distintos que comparecem na decomposição de a têm expoente igual a 1.

Definição 4.1.5. *A função* $\mu : \mathbb{Z}^+ \to \{-1, 0.1\}$ *definida por:*

$$\mu(a) \;=\; \begin{cases} 1 & \text{se } a = 1. \\ 0 & \text{se } a \text{ não é livre de quadrados.} \\ (-1)^r & \text{se } a = p_1 p_2 \cdots p_r \text{ é a decomposição em primos de } a. \end{cases}$$

chama-se a **função de Möbius**.

Lema 4.1.6. *Para todo inteiro positivo* n *tem-se que*

$$\sum_{d \mid n} \mu(d) = \begin{cases} 1 & \text{se } a = 1. \\ 0 & \text{se } a > 1. \end{cases}$$

Demonstração. Quando $n = 1$ claramente temos $\mu(1)$, da própria definição.

Seja agora $n > 1$ e seja $n = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$ a decomposição em fatores primos de n. Então, entre os divisores de n temos, o número 1, os primos $p_1, p_2, \ldots, p_r$, todos os produtos de dois primos diferentes $p_i p_j$, $1 \leq i, j \leq n$, $i \neq j$, de três primos diferentes, até o produto de todos os primos $p_1 \xi_2 \cdots p_r$. Além destes, há produtos em que pelo menos um dos primos aparece repetido mas, nestes divisores, o valor de μ é 0. Então temos:

$$\begin{aligned} \sum_{d \mid n} \mu(d) &= \mu(1) + \sum_{i=1}^{r} p_i + \sum_{i,j} \mu(p_i p_j) + \sum_{i,j,k} \mu(p_i p_j p_k) + \cdots + \mu(p_1 p_2 \cdots p_r) \\ &= 1 + \binom{r}{1}(-1) + \binom{r}{2}(-1)^2 + \binom{r}{3}(-1)^3 + \cdots + \binom{r}{r}(-1)^r \\ &= (1-1)^r = 0. \end{aligned}$$

□

O próximo resultado é conhecido como a **fórmula de inversão e Möbius**.

Teorema 4.1.7. *Seja* f *uma função definida em* $\mathbb{Z}^+$*, com valores num grupo aditivo, e seja* g *a função definida por*

$$g(n) = \sum_{d \mid n} f(d).$$

Então:

$$f(n) = \sum_{d \mid n} g(d)\mu\left(\frac{n}{d}\right)$$

donde temos também que

$$f(n) = \sum_{d \mid n} g\left(\frac{n}{d}\right)\mu(d).$$

Demonstração. Usando a hipótes sobre g temos:

$$\begin{aligned}\sum_{d \mid n} g(d)\mu\left(\frac{n}{d}\right) &= \sum_{d \mid n} \mu\left(\frac{n}{d}\right)\sum_{\ell \mid d} f(\ell) \\ &= \sum_{\ell \mid d} f(\ell)\sum \mu\left(\frac{n}{d}\right),\end{aligned}$$

onde a última somatória é tomada sobre todos os divisores d de n, que são múltiplos de ℓ. Note que isto é o mesmo que dizer que d/ℓ divide n/ℓ. Logo, podemos escrever:

$$\sum_{d \mid n} g(d)\mu\left(\frac{n}{d}\right) = \sum_{\ell \mid d} f(\ell) \sum_{(d/\ell) \mid (n/\ell)} \mu\left(\frac{n}{d}\right).$$

Pelo Lema 4.1.6 temos que $\sum_{(d/\ell) \mid (n/\ell)} \mu\left(\frac{n}{d}\right) = 0$ se $d/\ell \neq n/\ell$. Logo.

$$\sum_{d \mid n} g(d)\mu\left(\frac{n}{d}\right) = f(n),$$

ou, equivalentemente,

$$\sum_{d \mid n} g\left(\frac{n}{d}\right)\mu(d) = f(n).$$

A última igualdade decorre do fato de que d é um divisor de n se e somente se n/d também é um divisor de n. □

Agora, estamos em condições de provar o seguinte.

Teorema 4.1.8. *O número de polinômios irredutíveis de grau n em $\mathbb{F}_q[X]$ é*

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

Demonstração. Aplicando a fórmula de inversão de Möbius à fórmula (4.1), com $f(d) = N_q(d)$ e $g(n) = p^n$, temos

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

donde

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

□

Exemplo 4.1.9.

Vamos determinar o número de polinômios mônicos, irredutíveis, de grau 12 em $\mathbb{F}_q[X]$.

Aplicando a fórmula do Teorema 4.1.8 acima, temos:

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

Exemplo 4.1.10.

Vamos determinar o número de polinômios mônicos, irredutíveis, de grau 4 em $\mathbb{F}_2[X]$ e em $\mathbb{F}_3[X]$.

$$\begin{aligned} N_2(4) &= \frac{1}{4}\left[\mu(1)2^4 + \mu(2)2^2 + \mu(4)2\right] \\ &= \frac{1}{4}\left[2^4 - 2^2\right] = 3. \end{aligned}$$

$$\begin{aligned} N_3(4) &= \frac{1}{4}\left[\mu(1)3^4 + \mu(2)3^2 + \mu(4)3\right] \\ &= \frac{1}{4}\left[3^4 - 3^2\right] = 8. \end{aligned}$$

EXERCÍCIOS

1. Seja f uma função definida em $\mathbb{Z}^+$, com valores num grupo aditivo, e seja g a função definida por
$$g(n) = \prod_{d \mid n} f(d).$$
Prove que
$$f(n) = \prod_{d \mid n} g(d)^{\mu(n/d)}.$$

2. Provar que, para a função μ de Möbius, tem-se que:
   (i) $\mu(n)\mu(n+1)\mu(n+2)\mu(n+3) = 0$, para todo $n \in \mathbb{Z}^+$.
   (ii) Se $n \geq 3$ então $\mu(1!) + \mu(2!) + \cdots + \mu(n!) = 1$

3. Para um inteiro n denotamos por $\nu(n)$ e $\sigma(n)$ o número de divisores de n e a soma de todos os divisores de n, respectivamente. Provar que, se $n = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$ a decomposição em fatores primos de n, então
$$\begin{aligned} \nu(n) &= (n_1+1)(n_2+1)\cdots(n_r+1) \\ \sigma(n) &= \frac{p_1^{n_1+1}-1}{p_1-1} \cdot \frac{p_2^{n_2+1}-1}{p_2-1} \cdots \frac{p_r^{n_r+1}-1}{p_r-1}. \end{aligned}$$

4. (i) Seja n um inteiro positivo. Provar que, se $\mu(n) \neq 0$ então $\sigma(n)$ é da forma $\sigma(n) = (p_1+1)(p_2+1)\cdots(p_t+1)$ com p_i primo, $1 \leq i \leq t$.
   (ii) Determinar todos os inteiros n tais que $\mu(n) = 1$ e $\sigma(n) = 8$.

5. Aplicando a fórmula de inversão de Möbius á formula
$$\sum_{d \mid n} \varphi(d) = n$$
obtida na Proposição 3.3.5, prove que, se $n = p_1^{n_1} \cdots p_t^{n_t}$ é a decomposição em fatores primos de n, então
$$\varphi(n) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

6. Prove que:
   (*i*) Dois polinômios irredutíveis diferentes em $\mathbb{F}_q[X]$ não podem ter uma raiz comum.
   (*ii*) O número de elementos primitivos de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ é $\varphi(q^n - 1)$.
   (*iii*) O número de polinômios primitivos de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$ é $\varphi(q^n - 1)/n$.

7. Num corpo finito $\mathbb{F}_q$ vamos denotar por Q o conjunto dos elementos não nulos de $\mathbb{F}$ que são quadrados de elementos de $\mathbb{F}$ e por NQ o conjunto dos que não o são; i.e.:

$$\begin{aligned} Q &= \{a \in \mathbb{F}^* \mid (\exists b \in \mathbb{F}) a = b^2\}, \\ NQ &= \{a \in \mathbb{F} \mid a \neq b^2, \forall\, b \in \mathbb{F}\}. \end{aligned}$$

Define-se o **símbolo de Legendre** $\left[\begin{array}{c} a \\ p \end{array}\right]$ de um elemento $a \in \mathbb{F}_p$ por:

$$\left[\begin{array}{c} a \\ p \end{array}\right] = \begin{cases} 0 & \text{se } a = 0 \\ 1 & \text{se } a \in Q \\ -1 & \text{se } a \in NQ \end{cases}$$

(i) Provar que a função $\psi : \mathbb{F}_p^* \to \{\pm 1\}$ definida por $a \mapsto \left[\begin{array}{c} a \\ p \end{array}\right]$ é um homomorfismo de grupos.

(ii) Mostrar que $a^{\frac{p-1}{2}} = \left[\begin{array}{c} a \\ p \end{array}\right]$, para todo $a \in \mathbb{F}_p$.

(iii)Provar que

$$X^{\frac{p-1}{2}} - 1 = \prod_{a \in Q} (X - a)$$

$$X^{\frac{p-1}{2}} + 1 = \prod_{a \in NQ} (X - a)$$

e que

$$X_p - 1 = X \left(\prod_{a \in Q} (X - a) \right) \left(\prod_{a \in NQ} (X - a) \right).$$

4.2 A ordem de um polinômio irredutível

Já observamos, na seção 3.4 que se $f \in \mathbb{F}_q[X]$ é um polinômio irredutível que tem uma raiz α em $\mathbb{F}_{q^n}$, então f tem todas suas raízes em $\mathbb{F}_{q^n}$.

Se β é outra raiz de f, existe um automorfismo $\Phi : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ tal que $\Phi(\alpha) = \beta$. Como ambos elementos se correspondem num automorfismo de $\mathbb{F}_{q^n}$, eles têm a mesma ordem multiplicativa. Estas considerações provam o seguinte.

Lema 4.2.1. *Seja $f \in \mathbb{F}_q[X]$ um polinômio irredutível. Então, todas as raízes de f numa extensão $\mathbb{F}_{q^n}$ de $\mathbb{F}$ tem a mesma ordem multiplicativa.*

Este resultado justifica nossa próxima definição.

Definição 4.2.2. *Seja $f \in \mathbb{F}_q[X]$ um polinômio irredutível. O ordem de qualque uma de suas raízes nema extensão $\mathbb{F}_{q^n}$ de $\mathbb{F}_q$ diz-se a* **ordem** *do polinômio f, que denotaremos por $o(f)$.*

Lema 4.2.3. *Seja $f \in \mathbb{F}_q[X]$ um polinômio irredutível. Então f é um polinômio primitivo, de grau n sobre $\mathbb{F}_q$ se e somente se f é um polinômio de ordem $q^n - 1$.*

Demonstração. Note que, se $f \in \mathbb{F}_q[X]$ é um polinômio irredutível de ordem $q^n - 1$ se e somente se qualquer uma de suas raízes tem ordem multiplicativa igual a $q^n - 1$, o que significa que é um gerador do grupo multiplicativo de $\mathbb{F}_{q^n}$; isto é, a ordem de f é $= q^n - 1$ se e somente se qualquer uma de suas raízes é um elemento primitivo de $\mathbb{F}_{q^n}$; i.e., se f é um polinômio primitivo para $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$. □.

Existe uma relação interessante entre o grau de um plonômio irredutível e sua ordem.

Proposição 4.2.4. *Seja $f \in \mathbb{F}_q[X]$ um polinômio irredutível de grau n e ordem r. Então n é a ordem de $\overline{q}$ no grupo multiplicativo $\mathcal{U}(\mathbb{Z}_r)$.*

Demonstração. Seja α uma raiz de f. Como $gr(f) = n$ temos que $\alpha \in \mathbb{F}_{q^n}$. Portanto, α verifica que $a^{q^n-1} = 1$. Para qualquer inteiro m tal que $n \mid m$ também tem-se que $a^{q^m-1} = 1$.

Note que

$$a^{q^m-1} = 1 \Leftrightarrow r \mid (q^m - 1) \Leftrightarrow q^m \equiv 1 \pmod{r} \Leftrightarrow \overline{q}^m = 1 \text{ em } \mathcal{U}(\mathbb{Z}_r).$$

Como n é o menor inteiro positivo para o qual isto ocorre, temos que $o(\overline{q}) = n$ em $\mathcal{U}(\mathbb{Z}_r)$. □

O cálculo da ordem de um polinômio irredutível

Seja $f \in \mathbb{F}_q$ um polinômio irredutível e seja α uma raiz de f. Notamos inicialmente que se $r = o(f)$ e e $f \mid (X^n - 1)$, para algum inteiro positivo n, então então α é raiz de $X^n - 1$, donde $a^n = 1$. Como $o(\alpha) = r$, tem-se que $r \mid n$.

Reciprocamente, se $r \mid n$ então α é raiz de $X^n - 1$ e, como f é o polinômio minimal de α, temos que $f \mid (X^n - 1)$.

Logo:

$$f \mid (X^n - 1) \Longleftrightarrow r \mid n. \tag{4.2}$$

Por outro lado, como $\alpha \in \mathbb{F}_{q^n}$ temos que $\alpha^{q^n - 1} = 1$ donde

$$r \mid (q^n - 1). \tag{4.3}$$

Utilizaremos as obserfações (4.2) e (4.3) para dar um método para calcular a ordem r de f.

Seja

$$q^n - 1 = p_1^{n_1} \cdots p_t^{n_t}$$

a decomposição de $q^n - 1$ em produto de fatores primos distintos.

Como $r \mid (q^n - 1)$, deve ser da forma

$$r = p_1^{k_1} \cdots p_t^{k_t}$$

com $k_i \leq n_1,\ 1 \leq i \leq t$.

Usando agora a observação (4.2), temos que r é o menor número da forma $p_1^{k_1} \cdots p_t^{k_t}$ tal que

$$f \mid (X^{p_1^{k_1} \cdots p_t^{k_t}} - 1).$$

Exemplo 4.2.5.

O polinômio $f = X^6 + X^4 + X^2 + X_1$ é irredutível sobre $\mathbb{F}_2$ (Prove!). Vamos calcular a sua ordem.

Neste caso $q = 2,\ n = q$ donde $q^n - 1 = 2^6 - 1 = 63$.

A decomposição em fatores primos de 63 é $63 = 3^2.9$. Logo r deve ser da forma $r = 2^k 7\ \ell$ onde $k = 0, 1$ ou 2 e $\ell = 0$ ou 1.
Verificamos então que

$$f \nmid (X^7 - 1), \quad f \mid (X^{21} - 1), \quad f \nmid (X^3 - 1), \quad f \mid (X^{3^2.7} - 1).$$

Logo, $r = 21$.

EXERCÍCIOS

---

1. Provar que os seguintes polinômios são irredutíveis nos anéis de polinômios indicados e calcular a sua ordem.

   (i) $X^4 + X + 1 \in \mathbb{F}_2[X]$.

   (ii) $X^8 + X^7 + X^5 + X + 1 \in \mathbb{F} + 2[X]$.

   (iii) $X^4 + X + 2 \in \mathbb{F}_3[X]$.

   (i) $XX^5 + 2X + 1 \in \mathbb{F}_3[X]$.

2. Seja $f \in \mathbb{F}_q[X]$ um polinômio irredutível e seja f_R o seu polinômio recíproco. Provar que, se α é raiz de f, então α^{-1} é raiz de f_R. Deduzir que f e f_R tem a mesma ordem.

Capítulo 5

Automorfismos de Corpos Finitos

5.1 O automorfismo de Frobenius

Sejam $\mathbb{F} \subset \mathbb{E}$ corpos finitos. Como vimos no Teorema 3.1.2, existem um primo p e inteiros positivos m e n tais que $\mathbb{F}$ tem p^m elementos e $\mathbb{E}$ tem p^n elementos. Mais ainda, $\mathbb{F}$ e $\mathbb{E}$ são os corpos de decomposição dos polinômios $x^{p^m} - X$ e $X^{p^n} - X$ respectivamente. Consequentemente, todos os elementos $\alpha \in \mathbb{E}$ verificam $\alpha^{p^n} = \alpha$. Estas observações nos permitem caracterizar os elementos de $\mathbb{F}$.

Lema 5.1.1. *Sejam $\mathbb{F} \subset \mathbb{E}$ corpos finitos com p^m e p^n elementos, respectivamente. Um elemento $\alpha \in \mathbb{E}$ pertence a $\mathbb{F}$ se e somente se $\alpha^{p^m} = \alpha$.*

Em símbolos, podemos escrever:

$$\mathbb{F} = \{\alpha \in \mathbb{E} \mid \alpha^{p^m} = \alpha\}.$$

Vamos considerar agora a função $\sigma : \mathbb{E} \to \mathbb{E}$ definida por $\sigma(x) = x^{p^m}$, para todo $x \in \mathbb{E}$.

Do lema acima, vem que os elementos fixos por σ; i.e., os elementos tais que $\sigma(x) = x$, são precisamente os elementos de $\mathbb{F}$, de modo que também podemos caracterizar $\mathbb{F}$ como:

$$\mathbb{F} = \{x \in \mathbb{E} \mid \sigma(x) = x\}.$$

.

Ainda, como $\mathbb{E}$ é um corpo de característica p temos que

$$(\alpha + \beta)^{p^m} = \alpha^{p^m} + \beta^{p^m} \quad \text{ou, equivalentemente, } \sigma(\alpha + \beta) = \sigma(a) + \sigma(b).$$

Da mesma forma, como $\mathbb{E}$ é comutativo, segue imediatamente que

$$\sigma(\alpha.\beta) = \sigma(\alpha).\sigma(\beta).$$

Portanto, $\sigma\mathbb{E} \to \mathbb{E}$, que fixa $\mathbb{F}$. Isto implica que σ é um automorfismo de $\mathbb{E}$ (veja o Exercício 1).

Definição 5.1.2. *Sejam $\mathbb{F} \subset \mathbb{E}$ corpos. Um automorfismo $\theta : \mathbb{E} \to \mathbb{E}$ diz-se um F-***automorfismo** *de $\mathbb{E}$ se θ fixa todos os elementos de $\mathbb{F}$.*

Note que, se $\theta : \mathbb{E} \to \mathbb{E}$ é um $\mathbb{F}$ automorfismo de $\mathbb{E}$ então, dados $\ell \in \mathbb{F}$ e $\alpha \in \mathbb{E}$ tem-se que:

$$\theta(\ell\alpha) = \theta(\ell)\theta(\alpha) = \ell\theta(\alpha);$$

portanto, um $\mathbb{F}$ automorismo de $\mathbb{E}$ é, em particular, uma funçaõ F-linear, isto é, também um automorfismo de $\mathbb{E}$ como espaço vetorial sobre $\mathbb{F}$.

Definição 5.1.3. *Sejam $\mathbb{F} \subset \mathbb{E}$ corpos finitos com p^m e p^n elementos, respectivamente. O $\mathbb{F}$-automorfismo $\sigma : \mathbb{E} \to \mathbb{E}$ definido por*

$$\sigma(x) = x^{p^m}, \quad \forall x \in \mathbb{E},$$

chama-se o **automorfismo de Frobenius** *de $\mathbb{E}$ sobre $\mathbb{F}$,*

Como é usual, se denotamos por q o número de elementos de $\mathbb{F}$, vamos denotar $\mathbb{F}$ por $\mathbb{F}_q$. Existe então um inteiro positivo r tal que o número de elementos de $\mathbb{E}$ é q^r e o automorfismo de Frobenius de $\mathbb{E}$ sobre $\mathbb{F}$ é a função

$$\sigma(x) = x^q, \quad \forall x \in \mathbb{E}.$$

Note que, para todo elemento $x \in \mathbb{E}$, tem-se que $\sigma^2(x) = \sigma \circ \sigma(x) = x^{q^2}$ e é muito fácil verificar, usando indução, que

$$\sigma^k(x) = \sigma \circ \sigma^{k-1}(x) = x^{q^k}, \quad \text{para todo inteiro positivo } k.$$

Consequentemente, se $\mathbb{E}$ tem dimensão n sobre $\mathbb{F}_q$ então $\mathbb{E} = \mathbb{F}_{q^n}$ e

$$\sigma^{q^n}(x) = x^{q^n} = x, \quad \forall x \in \mathbb{F}_{q^n}.$$

Este argumento mostra que $\sigma^{q^n} = I$, a função indentidade de $\mathbb{F}_{q^n}$. Afirmamos ainda que as potências

$$\{I = \sigma^0, \sigma^1, \ldots, \sigma^{n-1}\}$$

são diferentes dois a dois;

De fato, suponha que $\sigma^i = \sigma^j$ com $i > j$. Então, para todo $x \in \mathbb{F}_{q^n}$, ter-se-ia:

$$\sigma^i(x) = \sigma^j(x) \iff \sigma^{i-j}(x) = \sigma^{q^{i-j}}(x) = x \iff x^{qi-j} = x,$$

e isto acontece para todo elemento $x \in \mathbb{F}_{q^n}$. Como este corpo contém q^n elementos, isso implicaria que o polinômio $X^{q^{i-j}} - X$ tem mais raizes que o seu grau, uma contradição.

Estas considerações provam o seguinte.

Lema 5.1.4. *O automorfismo de Frobenius de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}q$ tem ordem n.*

Sejam $\mathbb{F} \subset \mathbb{E}$ corpos. O conjunto de todos os $\mathbb{F}$-automorfismos de $\mathbb{E}$ é um grupo

Definição 5.1.5. *Sejam $\mathbb{F} \subset \mathbb{E}$ corpos. O conjunto de todos os $\mathbb{F}$-automorfismos de $\mathbb{E}$ é um grupo em relação à operação de composição de funções, chamado o* **grupo de Galois** *de $\mathbb{E}$ sobre $\mathbb{F}$, que se denota por $Gal(\mathbb{E} : \mathbb{F})$.*

Nossa intenção agora é mostrar que, no caso de extensões de corpos finitos, é muito fácil determinar o grupo de Galois da extensão. Para isso, precisamos do seguinte resultado, cuja demonstração é imediata.

Lema 5.1.6. *Seja $\theta : \mathbb{F} \to \mathbb{F}$ um automorfismo. A função $\overline{\theta} : \mathbb{F}[X] \to \mathbb{F}[X]$ definida por*

$$f = a_0 + a_1X + \cdots + a_kX^k \mapsto \overline{\theta}(f) = \theta(a_0) + \theta(a_1)X + \cdots + \theta(a_k)X^k,$$

é um automorfismo de $\mathbb{F}[X]$ (chamado o **automorfismo estendido** de θ).

Lema 5.1.7. *Sejam $\mathbb{F} \subset \mathbb{E}$ corpos e seja σ o automorfismo de Frobenius de $\mathbb{E}$ sobre $\mathbb{F}$. Dado um polinômio $f \in \mathbb{E}[X]$ tem-se que $f \in \mathbb{F}[X]$ se e somente se $\overline{\sigma}(f) = f$.*

Demonstração. Seja $f = a_0 + a_1X + \cdots + a_kX^k \in \mathbb{E}[X]$. Basta observar que $\overline{\sigma}(f) = f$ se e somente se $\sigma(a_i) = a_i$ para todo índice i, $1 \leq i \leq k$. Isto ocorre se e somente se $a_i \in \mathbb{F}, 1 \leq i \leq k$, e segue a tese. □

Agora estamos em consições de provar que o automorfismo de Frobenius determina completamente o grupo de Galois de uma extensão de corpos finitos.

Teorema 5.1.8. *Sejam $\mathbb{F}_q \subset \mathbb{F}_{q^n}$ corpos e seja σ o automorfismo de Frobenius de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$. Então:*

$$Gal(\mathbb{F}_{q^n} : \mathbb{F}_q) = \langle \sigma \rangle = \{I, \sigma, \ldots, \sigma^{n-1}\}.$$

Demonstração. Seja α um gerador de $\mathbb{F}^*$ e considere o polinômio

$$f = (X - \alpha)(X - \sigma(\alpha)) \cdots (X - \sigma^{n-1}(\alpha)).$$

Note que

$$\overline{\sigma}(f) = (X - \sigma(\alpha))(X - \sigma^2(\alpha)) \cdots (X - \alpha) = f.$$

Pelo lema aacima, temos que $f \in \mathbb{F}_q[X]$e, obviamente, $f(\alpha) = 0$.

Queremos mostrar que todo automorfismo $\gamma \in Gal(\mathbb{F}_{q^n} : \mathbb{F}_q)$ pertence a $Gal(\mathbb{F}_{q^n} : \mathbb{F}_q)$. Seja então γ um elemento qualquer de $Gal(\mathbb{F}_{q^n} : \mathbb{F}_q)$. Como γ fixa todos os elementos de $\mathbb{F}$, temos que $0 = \gamma(f(\alpha)) = f(\gamma(\alpha))$. Mas, da própria definição de f temos

$$0 = f(\gamma(\alpha)) = (\gamma(\alpha) - \alpha)(\gamma(\alpha) - \sigma(\alpha)) \cdots (\gamma(\alpha) - \sigma^{n-1}(\alpha)).$$

Logo, deve existir um índice i, $1 \leq i \leq k$ tal que $\gamma(\alpha) = \sigma^i(\alpha)$. Como α é um gerador de $\mathbb{F}^*_{q^n}$, temos que $\mathbb{F}_{q^n} = \mathbb{F}_q(\alpha)$ e, como γ e σ^i coincidem em elementos de $\mathbb{F}$ e em α, segue que $\gamma = \sigma^i \in \langle \sigma \rangle$, como queríamos demonstrar. □

Note que o teorema acima mostra que o grupo de Galois de uma extensão de corpos finitos é sempre um grupo cíclico. O próximo resultado diz respeito à relação entre subcorpos de uma extensão e subgrupos do grupo de Galois.

Teorema 5.1.9. *Sejam n um inteiro positivo e d um divisor positivo de n. Então:*
(i) $Gal(\mathbb{F}_{q^n} : \mathbb{F}_{q^d})$ *é um grupo cíclico de ordem n/d.*
(ii) Se $\sigma : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ *denota o automorfismo de Frobenius de* $\mathbb{F}_{q^n}$ *sobre* $\mathbb{F}_q$, *então a restrição de* σ

$$\sigma|_d : \mathbb{F}_{q^d} \to \mathbb{F}_{q^d}$$

é o automorfismo de Frobenius de $\mathbb{F}_{q^d}$ *sobre* $\mathbb{F}_q$ *e, consequentemente,*

$$Gal(\mathbb{F}_{q^d} : \mathbb{F}_q) = \langle \sigma|_d \rangle.$$

Demonstração.
(i) Note que $\sigma^q(a) = a^{q^d}$; logo, o subcorpo de $\mathbb{F}_{q^n}$ fixo por σ^q é precisamente $\mathbb{F}_{q^d}$. Isto mostra que σ^d é o automorfismo de Frobenius de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_{q^d}$. Portanto:

$$Gal(\mathbb{F}_{q^n} : \mathbb{F}_{q^d}) = \langle \sigma^d \rangle,$$

que é um grupo cíclico de ordem n/d.

(ii) A restrição $\sigma|_d : \mathbb{F}_{q^d} \to \mathbb{F}_{q^d}$ está bem definida e, diretamenta da definição, segue que é o automorfismo de Frobenius de $\mathbb{F}_{q^d}$ sobre $\mathbb{F}_q$. □

EXERCÍCIOS

---

1. Seja $\mathbb{E}$ um corpo e seja $\sigma : \mathbb{E} \to \mathbb{E}$ um homomorfismo de corpos.

   (i) Provar que σ é um monomorfismo.

   (ii) Provar que se $\mathbb{E}$ é uma extensão finita de um subcorpo $\mathbb{F}$ e σ fixa os elementos de $\mathbb{F}$, então σ é um automorfismo de $\mathbb{E}$.

2. Sejam $\mathbb{F} \subset \mathbb{K} \subset \mathbb{E}$ corpos.

   (i) Provar que todo $\mathbb{K}$-automorfismo de $\mathbb{E}$ é um $\mathbb{F}$-automorfismo.

   (ii) Seja $\varphi : \mathbb{E} \to \mathbb{E}$ um F-automorfismo de E. Definimos:

   $$\mathbb{E}^{\varphi} = \{x \in \mathbb{E} \mid \varphi(x) = x.,$$

e, mais geralmente, se G é um grupo de $\mathbb{F}$ automorfismos de $\mathbb{E}$, definimos:

$$\mathbb{E}^G = \{x \in E \mid \varphi(x) = x,\ \forall \varphi \in G\}.$$

Provar que $\mathbb{E}^\varphi$ e $\mathbb{E}^G$ são subcorpos de $\mathbb{E}$ que contém $\mathbb{F}$ e mostrar que

$$\mathbb{E}^G = \bigcup_{\varphi \in G} \mathbb{E}^\varphi.$$

5.2 O polinômio característico, normas e traços

Nesta seção, vamos assumir que o leitor está familiarizado com alguns conceitos levemente mais avançados de álgebra linear; explicitamente: com os conceitos de polinômio característico e polinômio minimal de uma matriz e com o famoso Teorema de Cayley-Hamilton. Sejam $\mathbb{F} \subset \mathbb{E}$ corpos quaisquer. Dado um elemento $\alpha \in \mathbb{E}$, vamos associar a ele uma função $\mathbb{F}$-linear $t_\alpha : \mathbb{E} \to \mathbb{E}$ definida por

$$T_\alpha(x) = \alpha x, \quad \forall x \in \mathbb{E}.$$

É muito fácil verificar diretamente que T_α é, de fato, uma função linear.

Costuma-se denotar por $Hom_{\mathbb{F}}(\mathbb{E}, \mathbb{E})$ o conjunto de todas as funções $\mathbb{F}$-lineares de $\mathbb{E}$ em $\mathbb{E}$. A função $\Phi : \mathbb{E} \to Hom_{\mathbb{F}}(\mathbb{E}, \mathbb{E})$ que a cada elemento $\alpha \in \mathbb{E}$ associa a função linear T_α, chama-se a **representação regular** de $\mathbb{E}$. Nos exercícicos 1 e 2 damos algumas propriedades desta representação.

Vamos assumir, daqui em diante, que α é algébrico sobre $\mathbb{F}$ e vamos considerar a função T_α restrita ao subcorpo $\mathbb{F}(\alpha)$, que vamos continuar representando pelo mesmo símbolo, para não sobrecarregar a notação. Vamos denotar por

$$m_\alpha = a_0 + a_1 X + \cdots + \alpha_{m-1} X^{m-1} + X^m$$

o polinômio minimal de α sobre $\mathbb{F}$. É fácil verificar que m_α é também o polinômio minimal da função linear T_α. Veja o Exercício 3.

O corpo $\mathbb{F}(\alpha)$ tem base $\{1, \alpha, \alpha^2, \ldots, \alpha^{m-1}\}$ sobre $\mathbb{F}$. Vamos determinar a matriz de T_α nessa base. Para isso, precisamos calcular os valores de T_α em cada um dos elementos da base. Temos:

$$\begin{array}{ll} T_\alpha(1) & = \alpha, \\ T_\alpha(\alpha) & = \alpha^2, \\ & \cdots \\ T_\alpha(\alpha^{m-2}) & = \alpha^{m-1}, \\ T_\alpha(\alpha^{m-1}) & = \alpha^m = \alpha_0 - a_1\alpha - \cdots - a_{m-1}\alpha^{m-1}. \end{array}$$

Logo, a matriz de T_α nessa base é

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

Uma matriz com esta forma especial, aparce em vários contextos em álgebra e recebe um nome particular.

Definição 5.2.1. *Sejam $\mathbb{F}$ um corpo e*

$$f = a_0 + a_1X + \cdots + \alpha_{m-1}X^{m-1} + X^m$$

um polinômio de $\mathbb{F}[X]$. A matriz da forma acima, diz-se a **matriz companheira** *do polinômio f e se denota por $\mathcal{C}(f)$.*

Mesmo no contexto geral, esta matriz tem algumas propriedades interessantes.

Proposição 5.2.2. *Sejam $\mathbb{F}$ um corpo, $f = a_0+a_1X+\cdots+\alpha_{m-1}X^{m-1}+X^m$ um polinômio de $\mathbb{F}[X]$ e $\mathcal{C}$ a matriz companheira de f. Então:*

(i) O polinômio característico da matriz $\mathcal{C}$ é f ou $-f$.
(ii) Se f é irredutível então o polinômio minimal de $\mathcal{C}$ também é f.

Demonstração.
(i)O polinômio característico de uma matriz $\mathcal{C}$ é $\chi_\mathcal{C} = det[\mathcal{C} - X.I]$ onde I indica a matriz identidade da mesma ordem que $\mathcal{C}$. Consequentemente, temos:

$$\chi_{\mathcal{C}} = det[\mathcal{C} - X.I] = \begin{bmatrix} -X & & & \cdots & 0 & -a_0 \\ 1 & -X & & \cdots & 0 & -a_1 \\ 0 & 1 & -X & \cdots & 0 & -a_2 \\ & & & \cdots & & \\ 0 & & & \cdots & 1 & -a_{m-1} - X \end{bmatrix} \qquad (5.1)$$

Desenvolvendo este determinante pela última coluna, temos:

$\chi_{\mathcal{C}} =$

$$= (-1)^m[(-a_0)+(-1)(-a_1)(-X)+(-1)^2(-a_2)X^2+\cdots+(-1)^{m-1}(-a_{m-1}-X)X^{m-1}]$$

$$= \pm f.$$

(ii) Sabe-se, do Teorema de Cayley-Hamilton, que toda matriz é raiz do seu polinômio característico. Se m indica o polinômo minimal de $\mathcal{C}$ então $m \mid \chi_{\mathcal{C}}$. Se f é irredutível, temos que $m = \chi_{\mathcal{C}}$ e segue a tese. □

Como consequência imediata destes resultados, temos o seguinte.

Corolario 5.2.3. *Sejam $\mathbb{F} \subset \mathbb{E}$ corpos e seja $\alpha \in \mathbb{E}$ um elemento algébrico sobre $\mathbb{F}$. Seja ainda $T_\alpha : \mathbb{F}(\alpha) \to \mathbb{F}(\alpha)$ a representação regular de α considerada como função linear em $\mathbb{F}(\alpha)$. Então $\chi_{T(\alpha)} = m_\alpha$.*

Se α é um elemento primitivo de $\mathbb{E}$ sobre $\mathbb{F}$, então $\mathbb{F}(\alpha) = \mathbb{E}$ e este resultado vale para a extensão $\mathbb{F} \subset \mathbb{E}$. Caso contrário, se $[\mathbb{E} : \mathbb{F}] = n$ e $[\mathbb{F}(\alpha) : \mathbb{F}] = m = gr(m_\alpha)$, temos que $m \mid n$. Seja $t = n/m$.

Note que, se $\beta \in \mathbb{E}$ é um elemento que não pertence a $\mathbb{F}(\alpha)$, então $\mathbb{F}(a) \cap \beta\mathbb{F}(\alpha) = (0)$. De fato, se existe $x \in \mathbb{F}(a) \cap \beta\mathbb{F}(\alpha)$ não nulo, então existem $\theta, \gamma \in \mathbb{F}(\alpha)$ não nulos, tais que $x = \theta = \beta\gamma$, donde $\beta = \theta.\gamma^{-1} \in \mathbb{F}(\alpha)$, uma contradição.

Isto implica que o conjunto $\{1, \alpha, \alpha^2, \ldots, \alpha^{m-1}, \beta.1, \beta\alpha, \beta\alpha^2, \ldots, \beta\alpha^{m-1}\}$ é linermente independente. Com efeito, se existe uma combinação linear

$$\lambda_0.1+\lambda_1\alpha+\lambda_2\alpha^2+\ldots+\lambda_{m-1}\alpha^{m-1}+\mu_0.\beta.1+\mu_1\beta\alpha+\mu_2\beta\alpha^2,\ldots+\mu_{m-1}\beta\alpha^{m-1} = 0$$

temos que

$$\lambda_0.1+\lambda_1\alpha+\lambda_2\alpha^2+\ldots+\lambda_{m-1}\alpha^{m-1} = -\mu_0.\beta.1+\mu_1\beta\alpha+\mu_2\beta\alpha^2,\ldots+\mu_{m-1}\beta\alpha^{m-1}.$$

Como o primeiro membro desta igualdade está em $\mathbb{F}(\alpha)$ e o segundo em $\beta\mathbb{F}(\alpha)$ e ambos são iguais, ambos estão na interseção; logo, cada um deles é 0.

Como $\mu_0.\beta.1+\mu_1\beta\alpha+\mu_2\beta\alpha^2,\ldots+\mu_{m-1}\beta\alpha^{m-1} = \beta(\mu_0.1+\mu_1\alpha+\mu_2\alpha^2,\ldots+\mu_{m-1}\alpha^{m-1})$ e $\{1,\alpha,\alpha^2,\ldots,\alpha^{m-1}\}$ é um conjunto linearmente independente, vem imediatamente que

$$\lambda_0 = \lambda_1 = \cdots = \lambda_{m-1} = \mu_0 = \mu_1 = \cdots - \mu_{m-1} = 0.$$

Tomando $\beta_1 = 1$, $\beta_2 = \beta$ e repetindo este processo, podemos determinar, inductivamente, elementos $\beta_1, \beta_2, \ldots, \beta_t$ tais que o conjunto

$$\{\beta_1 1, \beta_1\alpha, \ldots, \beta_1\alpha^{m-1}, \beta_2 1, \beta_2\alpha, \ldots, \beta_2\alpha^{m-1}, \ldots, \beta_t 1, \beta_t\alpha, \ldots, \beta_t\alpha^{m-1}\}$$

é uma base de $\mathbb{E}$ sobre $\mathbb{F}$.

Agora, é fácil ver que a matriz de T_α, nesta base, é uma matriz por blocos da forma:

$$A = \begin{bmatrix} \mathcal{C} & & & \\ & \mathcal{C} & & \\ & & \cdots & \\ & & & \mathcal{C} \end{bmatrix} \tag{5.2}$$

onde $\mathcal{C}$ representa a matriz companheira do polinômio minimal de α e todos os elementos não escritos são iguais a 0.

Como o polinômio característico de uma função linear é o polinômio característico de sua matriz, em qualquer base do espaço, temos que

$$\chi_{T_\alpha} = \chi_A = (\chi_{\mathcal{C}})^t = (m_{T_\alpha})^t = (m_\alpha)^t = (m_\alpha)^{[\mathbb{E}:\mathbb{F}(\alpha)]}.$$

Nesta situação particular, o polinômio característico é uma potência do polinômio minimal.

No que segue, vamos voltar a considerar apenas extensões de corpos finitos $\mathbb{F}_q \subset \mathbb{F}_{q^n}$ e nos utilizaremos do automorfismo de Frobenius da extensão para dar uma descrição dos polinômios minimal e caracterísico. Lembramos que, se $\alpha \in \mathbb{F}_{q^n}$, então $\alpha^{q^n} = \alpha$ mas a igualdade deve acontecer para inteiros menores que q^n. Seja então:

$$m = min\{d \in \mathbb{Z}^+ \mid \alpha^d = 1\}.$$

Teorema 5.2.4. *Com as notações acima, tem-se que*

$$\begin{aligned} m_\alpha &= (X-\alpha)\,(X-\sigma(a))\cdots\left(X-\sigma^{m-1}(\alpha)\right) && (5.3)\\ &= (X-\alpha)\,(X-\alpha^q)\cdots\left(X-\alpha^{q^{m-1}}\right). && (5.4)\end{aligned}$$

Demonstração. Afirmamos inicialmente que os elementos $\alpha, \sigma(\sigma), \ldots, \sigma^{m-1}(\alpha)$ são diferentes dois a dois. De fato, se dentre estes elementos temos $\sigma^i(\alpha) = \sigma^j(\alpha)$, com $i > j$, então $\sigma^{i-j}(\alpha) = \alpha$ com $i - j < m$, uma contradição.

Seja $f = (X-\alpha)\,(X-\sigma(a))\cdots(X-\sigma^{m-1}(\alpha))$. Claramente $f(\alpha) = 0$, donde $m_\alpha \mid f$. Por outro lado, como α é raiz de m_α, como observamos acima, resulta que $\sigma(\alpha)$ também é raiz de m_α. Isto significa que $(x - \sigma^i(\alpha)) \mid m_\alpha$, $0 \leq i \leq m-1$. Como estes polinômios são relativamente primos dois a dois, o seu produto também divide m_α; isto é, $f \mid m_\alpha$. Consequentemente, $f = m_\alpha$. □

Observamos agora que, como $\alpha^{q^m} = \alpha$, para qualquer inteiro positivo j temos que $\alpha^{q^{jm}} = \alpha$ e, mais geralmente, dados inteiros poisitos i e j temos que $\alpha^{q^{jm+i}} = \alpha^{q^i}$; portanto:

$$m_\alpha = (X-\alpha)\,(X-\alpha^q)\cdots\left(X-\alpha^{q^{m-1}}\right)$$

implica que

$$m_\alpha = \left(X-\alpha^{q^{jm}}\right)\left(X-\alpha^{q^{jm+1}}\right)\cdots\left(X-\alpha^{q^{jm+(m-1)}}\right), \quad 0 \leq j \leq t-1.$$

Consequentemente, temos que

$$\begin{aligned} \chi_{T_\alpha} &= (X-\alpha)\,(X-\alpha^q)\left(X-\alpha^{q^2}\right)\cdots\left(X-\alpha^{q^{n-1}}\right) && (5.5)\\ &= (X-\alpha)\,(X-\sigma(\alpha))\left(X-\sigma^2(\alpha)\right)\cdots\left(X-\sigma^{n-1}(\alpha)\right). && (5.6)\end{aligned}$$

Definição 5.2.5. *Sejam $\mathbb{F}_q \subset \mathbb{F}_{q^n}$ corpos e α um elemento de $\mathbb{F}_{q^n}$. Chama-se* **polinômio característico** *do elemento α ao polinômio caractrísitco da função linear T_α, acima.*

Exemplo 5.2.6.

Considere

$$\mathbb{F}_8 = \frac{\mathbb{F}_2[X]}{(X^3 + X + 1)}.$$

Se denotamos por t uma raiz de X^3+X+1, podemos escrever $\mathbb{F}_8 = \mathbb{F}_2(t)$, onde $t^3 = t+1$. Prova-se facilmente que t é um gerador de $\mathbb{F}_8^*$; logo, podemos escrever explicitamente

$$\mathbb{F}_8 = \{0, 1, t, t^2, t^3, t^4, t^5, t^6, t^7\}.$$

Vamos calcular o polinômio minimal de cada um dos elementos deste corpo.

Naturalmente temos que $m_0 = X$ e $m_1 = X + 1$.

Usando a fórmula do teorema acima, aplicada a t, temos:

$$m_t = (X - t)(X - t^2)(X - t^4) = X^3 + X + 1.$$

Como $m_t(t^2) = m_t(t^4) = 0$ segue que $m_t = m_{t^2} = m_{t^4}$.

Da mesma forma, $m_{t^3} = (X - t^3)(X - (t^3)^2)(X - (t^3)^4)$. Podemos fazer os cálculos diretamente, mas também podemos observar que t^3 é raiz de $X^3 + X^2 + 1$ que é irredutível; logo, esse é seu polinômio minimal.

Assim, temos

$$m_{t^3} = m_{t^6} = m_{t^5} = X^3 + X^2 + 1.$$

Note que isso implica que

$$X^8 - X = X(X + 1)(X^3 + X + 1)(X^3 + X^2 + 1).$$

Dado um elemento $\alpha \in \mathbb{E}$, podemos definir a **norma** e o **traço** de α, relativo à extensão $\mathbb{F}_q \subset \mathbb{F}_{q^n}$, respectivamente por:

$$\begin{aligned} Tr_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) &= Tr(T_\alpha), \\ N_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) &= det(T_\alpha). \end{aligned}$$

Escrevendo o polinômio característico de T_α na forma:

$$\chi_\alpha = a_0 + a_1 X + a_2 X^2 + \cdots + a_{n-1} X^{n-1} = X^n,$$

sabemos, da álgebra linear (veja, por exemplo,) que $Tr(T_\alpha) = -a_{n-1}$ e $det(T_\alpha) = (-1)^n a_0$. Como conhecemos, na expressão 5.5 todas as raízes de χ_α, obtemos diretamente, que

$$\begin{aligned} Tr_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) &= \alpha + \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{n-1}}, \\ N_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) &= \alpha.\alpha^q.\alpha^{q^2} \cdots \alpha^{q^{n-1}}. \end{aligned}$$

Seguindo a prática usual na maioria dos textos sobre o assunto, vamos utilizar este resultado para dar uma definição formal de normas e traços.

Definição 5.2.7. *Sejam $\mathbb{F}_q \subset \mathbb{F}_{q^n}$ corpos finitos e seja σ o automorfismo de Frobenius de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$. Dado um elemento $\alpha \in \mathbb{F}_{q^n}$, definimos o* **traço** *e a* **norma** *de α respectivamente por:*

$$\begin{aligned} Tr_{\mathbb{F}_{q^n}|\mathbb{F}_q} &= \sum_{i=0}^{n} \sigma^i(\alpha) = \sum_{i=0}^{n} \alpha^{q^i}, \\ N_{\mathbb{F}_{q^n}|\mathbb{F}_q} &= \prod_{i=0}^{n-1} \sigma^i(\alpha) = \prod_{i=0}^{n-1} \alpha^{q^i} \end{aligned}$$

Observe que as definições não dependem apenas do elemento α considerado mas também da extensão com que estamos trabalhando. Quando a extensão estiver clara do contexto e não for necessario enfatiza-la, representaremos o traço e a norma de α apenas por $tr(\alpha)$ e $N(\alpha)$.

Proposição 5.2.8. *Nas condições da definição, valem as seguintes propriendades:*

Para o traço.

(i) $Im(Tr) \subset \mathbb{F}_q$.
(ii) $Tr(\alpha + \beta) = Tr(\alpha) + Tr(\beta)$.
(iii) Se $\lambda \in \mathbb{F}_q$ *então* $Tr(\lambda\alpha) = \lambda Tr(\alpha)$.
(iv) Se $\alpha \in \mathbb{F}_q$, *então* $Tr(\alpha) = n\alpha$.

(v) $Tr(\alpha^q) = Tr(\sigma(\alpha)) = Tr(\alpha)$.

Para a norma.

(i) $Im(N) \subset \mathbb{F}_q$.
(ii) $N(\alpha\beta) = N(\alpha)N(\beta)$.
(iii) Se $\lambda \in \mathbb{F}_q$ *então* $N(\lambda\alpha) = \lambda^n N(\alpha)$.
(iv) Se $\alpha \in \mathbb{F}_q$ *então* $N(\alpha) = \alpha^n$
(v) $N(\alpha^q) = Tr(\alpha)$.

Demonstração. Demonstraremos,a seguir, as propriedades do traço. As propriedades da norma resultam de forma inteiramente análoga e deixamos sua demonstração como exercício para o leitor.

(i) Segue de observar que

$$\sigma(Tr(\alpha) = \sigma\left(\sum_{i=0}^{n-1} \sigma^i(\alpha)\right) = \sum_{i=0}^{n-1} \sigma^{i+1}(\alpha) = Tr(\alpha).$$

A último igualdade vale porque na soma $\sum_{i=0}^{n-1} \sigma^{i+1}(\alpha)$ aparecem todos os termos da forma $\sigma^i(\alpha)$. O resultado segue agora do Lema 5.1.1.

(ii) Basta calcular: $tr(\alpha + \beta) =$

$$\sum_{i=0}^{n} \sigma^i(\alpha+\beta) = \sum_{i=0}^{n}(\sigma^i(\alpha)+\sigma^i(\beta)) = \sum_{i=0}^{n} \sigma^i(\alpha) + \sum_{i=0}^{n} \sigma^i(\beta) = Tr(\alpha)+Tr(\beta).$$

(iii) Temos:

$$Tr(\lambda\alpha) = \sum_{i=0}^{n} \sigma^i(\lambda\alpha) = \sum_{i=0}^{n} \sigma^i(\lambda)\sigma^i(\alpha) = \sum_{i=0}^{n} \lambda\sigma^i(\alpha) = \lambda \sum_{i=0}^{n} \sigma^i(\alpha) = Tr(\alpha).$$

(iv) Se $a \in \mathbb{F}_q$ temos $Tr(a) = \sum_{i=0}^{n-1} \sigma^i(a) = \sum_{i=0}^{n-1} a = na$.

(iv) Como $\alpha^q = \sigma(\alpha)$, temos:

$$Tr(\alpha^q) = Tr(\sigma(\alpha)) = \sum_{i=0}^{n-1} \sigma^i(\sigma(\alpha)) = \sum_{i=0}^{n-1} \sigma^{i+1}(\alpha) = Tr(\alpha).$$

□

Exemplo 5.2.9.

Considere $\mathbb{F}_8 = \mathbb{F}_2(t)$ onde $t^3 = t + 1$, como no Exemplo 3.4.7.

Dado um elemento $\alpha \in \mathbb{F}_8$, ele pode se escrever na forma $\alpha = a_0 1 + a_1 t + a_2 t^2$. Das propriedades do traço, temos que

$$Tr(\alpha) = a_0 + a_1 Tr(t) + a_2 Tr(t^2).$$

Portanto, é suficiente calcular os valores de $Tr(1), Tr(t)$ e $Tr(t^2)$. Temos que $Tr(1) = 3 = 1$.

Calculando $\sigma(t) = t^2$ e $\sigma^2(t) = t^4 = t^2 + t$ temos que

$$Tr(t) = t + t^2 + t + t^2 = 0.$$

Ainda, $\sigma(t^2) = t^4 = t + t^2$ e $\sigma^2(t^2) = \sigma(t + t^2) = t^2 + t^4 = t$, donde

$$Tr(t^2) = t^2 + t + t^2 + t = 0.$$

Consequentemente, para um elemento α da foram acima temos que

$$Tr(\alpha) = a_0.$$

Vamos calcular $N(t)$. Temos

$$N(t) = t\sigma(t)\sigma^2(t) = t.t^2.t^4 = t^3(t + t^2) = (1 + t)(t + t^2) = t.$$

De modo análogo, podemos calcular

$$N(1 + t) = (1 + t)\sigma(1 + t)\sigma^2(1 + t) = (1 + t)(1 + t^2)(1 + t^4) = 1 + t + t^2.$$

Seja agora d um divisor de n, Então, $\mathbb{F}_{q^d}$ é um subcorpo de $\mathbb{F}_{q^n}$ e temos as seguintes inclusões: $\mathbb{F}_q \subset \mathbb{F}_{q^d} \subset \mathbb{F}_{q^n}$. Veremos que, tal como acontece com as respecticas dimensões, as normas e traços destas extensôes estão relacionadas de uma forma natural.

Teorema 5.2.10. *Seja d um divisor positivo de n. Então, par todo elementos $\alpha \in \mathbb{F}_{q^n}$ tem-se que*

$$Tr_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) = Tr_{\mathbb{F}_{q^d}|\mathbb{F}_q}\left(Tr_{\mathbb{F}_{q^n}|\mathbb{F}_{q^d}}(\alpha)\right).$$

$$N_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha) = N_{\mathbb{F}_{q^d}|\mathbb{F}_q}\left(N_{\mathbb{F}_{q^n}|\mathbb{F}_{q^d}}(\alpha)\right).$$

Demonstração. Novamente, vamos provar o resultado para o traço, e deixaremos a cargo do leitor a demonstração da fórmula para a norma, que é inteiramente análoga.

Lembramos que, se σ denota o automorfismo de Frobenius de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$, então $\sigma(\alpha) = \alpha^q$ e que o automorfismo de Frobenius de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_{q^d}$, que denotaremos por σ_1, está dado por $\sigma_1(\alpha) = \alpha^{q^d}$.

Observamos ainda que, conforme à parte (i) da Proposição 5.2.8, $Im(\sigma_1) \subset \mathbb{F}_{q^d}$, de modo que a expressão $Tr_{\mathbb{F}_{q^d}|\mathbb{F}^q}\left(Tr_{\mathbb{F}_{q^n}|\mathbb{F}_{q^d}}(\alpha)\right)$ está bem definida.

Então, calculamos:

$$Tr_{\mathbb{F}_{q^n}|\mathbb{F}_{q^d}}\left(Tr_{\mathbb{F}_{q^n}|\mathbb{F}_{q^d}}(\alpha)\right) =$$

$$= Tr_{\mathbb{F}_{q^n}|\mathbb{F}_{q^d}}\left(\sum_{j=0}^{(n/d)-1} \sigma_1 j(\alpha)\right) = Tr_{\mathbb{F}_{q^n}|\mathbb{F}_{q^d}}\left(\sum_{j=0}^{(n/d)-1} \alpha^{q^{dj}}\right)$$

$$= \sum_{i=0}^{n-1} \sigma^i \left(\sum_{j=0}^{(n/d)-1} \alpha^{dj}\right) = \sum_{j=0}^{(n/d)-1} \sum_{i=0}^{n-1} \sigma^i(\alpha^{dj})$$

$$= \sum_{j=0}^{(n/d)-1} \sum_{i=0}^{n-1} (\alpha^{dj})^{q^i} = \sum_{j=0}^{(n/d)-1} \sum_{i=0}^{n-1} \alpha^{q^{dj+i}}$$

$$= \sum_{h=0}^{n-1} \alpha^{q^h} = Tr_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\alpha).$$

□

EXERCÍCIOS

1. Sejam $\mathbb{F} \subset \mathbb{E}$ corpos quaisquer e $\alpha \in \mathbb{E}$. Seja T_α a função $\mathbb{F}$-linear $T_\alpha : \mathbb{E} \to \mathbb{E}$ definida por
$$T_\alpha(x) = \alpha x, \quad \forall x \in \mathbb{E}.$$
Dados α e $\beta \in \mathbb{E}$, provar que:
(i) $T_{\alpha+\beta} = T_\alpha + T_\beta$.
(ii) $T_{\alpha\beta} = T_\alpha \circ T_\beta$.
(i) Se $\alpha \neq 0$ então T_α é inversível.

2. Nas condições do exercício anterior, provar que
(i) A função $\Phi : \mathbb{E} \to Hom_{\mathbb{F}}(\mathbb{E}, \mathbb{E})$ é um homomorfismo de álgebras e que esta função é injetora.
(ii) Se denotamos por $GL(\mathbb{E})$ o conjunto das transformações lineares inversíveis de $\mathbb{E}$ em $\mathbb{E}$, com a operação de composição, então $\Phi : \mathbb{E}^* \to GL(\mathbb{E})$ é um homomorfismo de grupos.

3. Dado um polinômio $f = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \in \mathbb{F}[X]$ e uma função linear $T : \mathbb{E} \to \mathbb{E}$ definie-se o **valor** de f em T como sendo a função linear $f = a_0I + a_1T + a_2T^2 + \cdots + a_nT^n \in \mathbb{F}[X]$.
Nas condições do Exarcício 1 acima, dado $f \in \mathbb{F}[X]$, provar que $f(\alpha) = 0$ se e somente se $f(T_\alpha) = 0$. Deduzir que α e T_α têm o mesmo polinômio minimal.

4. Sejam $\mathbb{F} \subset \mathbb{E}$ corpos finitos e seja α um elemento de $\mathbb{F}$. Prove que
$$\begin{aligned} Tr_{\mathbb{E}|\mathbb{F}}(\alpha) &= [\mathbb{E} : \mathbb{F}]\alpha, \\ N_{\mathbb{E}|\mathbb{F}}(\alpha) &= \alpha^{[\mathbb{E}:\mathbb{F}]}. \end{aligned}$$

5. Sejam $\mathbb{F} \subset \mathbb{E}$ e $\mathbb{F} \subset \mathbb{K}$ corpos finitos e seja $\varphi : \mathbb{E} \to \mathbb{K}$ um $\mathbb{F}$-homomorfismo. Provar que
$$N_{\varphi(\mathbb{E})|\mathbb{F}}(\varphi(\alpha)) = \varphi(N_{\mathbb{E}|\mathbb{F}}(\alpha)).$$
Enuncie e demonstre um resultado similar para o traço.

6. Seja $\alpha \in \mathbb{F}_{q^n}$ e seja $m_\alpha = a_0 + a_1X + \cdots + \alpha_{m-1}X^{m-1} + X^m$ o polinômio minimal de α sobre $\mathbb{F}_q$. Provar que
$$\begin{aligned} Tr_{\mathbb{F}_{q^n}|\mathbb{F}_q} &= -\frac{n}{m}\, a_{m-1}, \\ N_{\mathbb{F}_{q^n}|\mathbb{F}_q} &= (-1)^n a_m^{-n/m}. \end{aligned}$$

7. Seja α um elemento de $\mathbb{F}_{q^n}$. Provar que, se $\beta = \alpha - \sigma(\alpha)$, então

$$Tr_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\beta) = 0.$$