SMA - 306 - Álgebra II

Teoria de Anéis - Notas de Aulas

Professora Ires Dias - Segundo Semestre de 2001

1 Definição e Exemplos

Definição 1 Um conjunto não vazio R, juntamente com duas operações binárias $+$ e $\cdot$, é dito ser um ***anel*** quando:

(i) $(R, +)$ é um grupo abeliano, ou seja;

- $a + (b + c) = (a + b) + c$, para todo $a, b, c \in R$;
- $\exists\ 0 \in R;\ a + 0 = 0 + a = a$, para todo $a \in R$;
- Para todo $a \in R,\ \exists\ -a \in R;\ a + (-a) = 0 = (-a) + a$;
- $a + b = b + a$; para todo $a, b \in R$.

(ii) $\cdot$ é associativa, ou seja,

$a \cdot (b \cdot c) = (a \cdot b) \cdot c$, para todo $a, b, c \in R$.

(iii) Valem as leis distributivas:

$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$,

$(b + c) \cdot a = (b \cdot a) + (c \cdot a)$, para todo $a, b, c \in R$.

Notação: $(R\,,\,+\,,\,\cdot)$ denotará um anel R com as operações $+$ e $\cdot$.

Exemplo 1 $(\mathbb{Z}\,,\,+\,,\,\cdot)$ é um anel, onde $+$ e $\cdot$ são a adição e a multiplicação usuais dos inteiros. A operação $\cdot$ é comutativa e 1 é o elemento neutro para esta operação.

Exemplo 2 $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ e $(\mathbb{C}, +, \cdot)$ são anéis, onde $+$ e $\cdot$ são a adição e a multiplicação usuais. Em cada caso, a operação $\cdot$ é comutativa e 1 é o elemento neutro para esta operação.

Exemplo 3 Para todo $n \geq 0$, seja $n\mathbb{Z} = \{na;\ a \in \mathbb{Z}\}$. Com as operações induzidas pelas operações de $\mathbb{Z}$, temos que $(n\mathbb{Z}, +, \cdot)$ é um anel, onde a operação $\cdot$ é comutativa e não tem elemento neutro para esta operação, se $n \neq 1$.

Exemplo 4 Sejam $R = \mathbb{Z}_n = \left\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\right\}$, $n \geq 0$, $+$ e $\cdot$ operações em $\mathbb{Z}_n$, definidas por:

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

$\overline{a} \cdot \overline{b} = \overline{ab}$, para todo $\overline{a}, \overline{b} \in \mathbb{Z}_n$.

$(\mathbb{Z}_n, +, \cdot)$ é um anel, onde a operação $\cdot$ é comutativa e tem elemento neutro $\overline{1}$. Este anel é chamado o ***anel dos inteiros módulo*** n**.**

Lembrete: Para todo $\overline{a}, \overline{b} \in \mathbb{Z}_n$, temos: $\overline{a} = \overline{b} \iff a \equiv b \bmod n \iff n \,/\, (a + b) \iff a$ e b deixam o mesmo resto quando divididos por n.

Definição 2 Um anel $(R, +, \cdot)$, onde a operação $\cdot$ é comutativa é dito ser um **anel comutativo**. Um anel $(R, +, \cdot)$ onde $\cdot$ tem elemento neutro é dito ser um ***anel com elemento identidade*** ou simplesmente, um ***anel com*** 1. Tal elemento neutro será indicado por 1 ou 1_R.

Exemplo 5 Seja $R = \{f : \mathbb{R} \to \mathbb{R};\ f \text{ é função}\}$. Para todo $f, g \in R$, definimos $(f + g) \in R$ e $(f \cdot g) \in R$, por:

$(f + g)(x) = f(x) + g(x), \quad \forall\ x \in \mathbb{R}$

$(f \cdot g)(x) = f(x) \cdot g(x), \quad \forall\ x \in \mathbb{R}.$

$(R, +, \cdot)$ é um anel comutativo com 1 .

Exemplo 6 $(M_2(\mathbb{Z}), +, \cdot)$ é um anel com $1_R = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ que não é comutativo,

pois

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Exemplo 7 Seja $R = \mathbb{Z}[X] = \{a_0 + a_1X + \cdots + a_nX^n;\ a_i \in \mathbb{Z}\,,\ n \in \mathbb{N}\}$. Para todo $p(X) = \sum_{i=0}^{n} a_iX^i$ e $q(X) = \sum_{i=1}^{m} b_iX^i$, em R, com $m \leq n$ definimos as operações $+$ e $\cdot$ por:

$$p(X) + q(X) = \sum_{i=0}^{n} (a_i + b_i)X^i,$$

$$p(X) \cdot q(X) = \sum_{k=0}^{n+m} c_kX^k, \text{ onde } c_k = \sum_{j=0}^{k} a_j\, b_{k-j}, \text{ para todo } k = 0, 1, \cdots, n+m.$$

$(\,\mathbb{Z}[X],\, +\,,\, \cdot\,)$ é um anel comutativo, com 1, chamado o **anel dos polinômios sobre** $\mathbb{Z}$.

Exemplo 8 Seja $\mathbb{Z}_n[X] = \{\overline{a_0} + \overline{a_1}X + \cdots + \overline{a_m}X^m;\ \overline{a_i} \in \mathbb{Z}_n\,,\ m \geq 0\}$. Com as operações induzidas pelas operações $+$ e $\cdot$ de $\mathbb{Z}_n$, temos que $(\,\mathbb{Z}_n[X], +, \cdot)$ é anel comutativo com $1 = \overline{1}$.

Por exemplo, para $n = 6$ e $f(X) = \overline{2} + \overline{3}X + \overline{1}X^2$, $g(X) = \overline{4} + \overline{2}X^2 \in \mathbb{Z}_6[X]$, temos $f(X)+g(X) = (\overline{2}+\overline{4})+\overline{3}X+\overline{3}X^2 = \overline{3}X+\overline{3}X^2$ e $f(X)\cdot g(X) = \overline{2}+\overline{2}X^2+\overline{2}X^4$.

Exemplo 9 Seja $G = \{a + bi;\ a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$. Usando as operações induzidas pelas operações de $\mathbb{C}$, temos $(a + bi) + (c + di) = (a + c) + (b + d)i$ e $(a + bi)(c + di) = (ac + bd) + (ad + bc)i$, para todo $a + bi, c + di \in G$.

$(\,G\,,\, +\,,\, \cdot\,)$ é um anel comutativo com 1 $(1 = 1 + 0i)$, chamado o **anel dos inteiros de Gauss.**

2 Tipos de Anéis e suas Propriedades

Em $R = M_2(\mathbb{Z})$, temos que $a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ e $b = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ são elementos de R tais que $a \neq 0$, $b \neq 0$ mas

$$a \cdot b = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

ou seja, o zero tem fatores não nulos, o que implica que não vale a lei do cancelamento para o produto. Por exemplo,

$$\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 2 & 4 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{e} \quad \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 2 & 4 \end{pmatrix}.$$

Definição 3 Seja $(R\,,+,\cdot)$ um anel. Um elemento $a \in R,\ a \neq 0$ é um **divisor de zero à esquerda de** R se existe $b \neq 0$ em R, tal que $a \cdot b = 0$. Analogamente, $a \neq 0$ é um **divisor de zero à direita** se existe $b \neq 0$ tal que $b \cdot a = 0$.

Por exemplo, $\begin{pmatrix} 0 & 1 \\ 0 & 2 \end{pmatrix}$ é um divisor de zero à esquerda de $R = M_2(\mathbb{Z})$ pois $\begin{pmatrix} 0 & 1 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ mas $\begin{pmatrix} 2 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 4 \\ 0 & 0 \end{pmatrix} \neq 0$. Isso não implica que $\begin{pmatrix} 0 & 1 \\ 0 & 2 \end{pmatrix}$ não é divisor de zero à direita, pois $\begin{pmatrix} 2 & -1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

Exercício 1 Todo divisor de zero à esquerda é também divisor de zero à direita?

Definição 4 Um **domínio**, ou um **anel de integridade** é um anel comutativo, com 1, sem divisores de zero, ou seja um anel $(R\,,+,\cdot)$ comutativo com 1 é domínio $\Leftrightarrow$ (para todo $a, b \in \mathbb{R},\ ab = 0 \Rightarrow a = 0$ ou $b = 0$).

Um anel $(R\,,+,\cdot)$ é um **anel com divisão**, ou um **quase corpo** se $(R - \{0\}\,,\cdot)$ é um grupo, ou seja $1 \in R$ e para todo $a \in R,\ a \neq 0$, existe $b \in R$, tal que $a \cdot b = b \cdot a = 1$, este elemento b é dito ser o inverso de a e é denotado por a^{-1}.

Um **corpo** é um anel com divisão comutativo.

Exemplo 10 Com as operações usuais, o anel dos inteiros $\mathbb{Z}$ é um domínio que não é corpo. $\mathbb{R}\,,\ \mathbb{Q}\,,\ \mathbb{C}$ são corpos.

Se n é um inteiro positivo que não é primo, então $\mathbb{Z}_n$ não é domínio. Mas, $\mathbb{Z}_p$, com p primo é corpo.

De fato, seja $\overline{a} \in \mathbb{Z}_p$, $\overline{a} \neq \overline{0}$, ou seja $a \in \mathbb{Z}$ tal que $p \nmid a$. Assim, mdc $(p, a) = 1$, o que implica que existem $r, s, \in \mathbb{Z}$; $rp + sa = 1$. Logo $\overline{rp} + \overline{sa} = \overline{1} \Rightarrow \overline{sa} = \overline{1} \Rightarrow \overline{s} = (\overline{a})^{-1}$, o que mostra que $\mathbb{Z}_p$ é corpo.

Exercício 2 Mostre que $\mathbb{Z}_n$ é corpo $\Leftrightarrow$ n é primo.

Exemplo 11 Um exemplo de um anel com divisão que não é corpo, chamado o **anel dos quatérnios de Hamilton.**

Seja $\mathbb{H} = \mathbb{R} \cdot 1 \oplus \mathbb{R} \cdot i \oplus \mathbb{R} \cdot j \oplus \mathbb{R} \cdot k = \{\alpha + \beta i + \gamma j + \sigma k\,;\ \alpha, \beta, \gamma, \sigma \in \mathbb{R}\}$, o espaço vetorial real, com base $\{1, i, j, k\}$.

Com relação a + temos que $(\mathbb{H}, +)$ é um grupo abeliano, pois por definição de espaço vetorial, a + é associativa, comutativa, tem elemento neutro (o vetor nulo) e, todo vetor $\vec{v}$ tem um inverso com relação a adição, que é o vetor $-\vec{v}$.

Com relação ao produto, temos:

$$\begin{cases} i^2 = j^2 = k^2 = -1 \\ ij = k\,,\ jk = i\,,\ ki = j \\ ji = -k\,,\ kj = -i\,,\ ik = -j \end{cases} .$$

Assim, $(\alpha_1 + \alpha_2 i + \alpha_3 j + \alpha_4 k) \cdot (\beta_1 + \beta_2 i + \beta_3 j + \beta_4 k) = (\alpha_1\beta_1 + \alpha_1\beta_2 i + \alpha_1\beta_3 j + \alpha_1\beta_4 k) + (\alpha_2\beta_1 i - \alpha_2\beta_2 + \alpha_2\beta_3 k - \alpha_2\beta_4 j) + (\alpha_3\beta_1 j - \alpha_3\beta_2 k - \alpha_3\beta_3 + \alpha_3\beta_4 i) + (\alpha_4\beta_1 k + \alpha_4\beta_2 j - \alpha_4\beta_3 i - \alpha_4\beta_4) = (\alpha_1\beta_1 - \alpha_2\beta_2 - \alpha_3\beta_3 + \alpha_4\beta_4) + (\alpha_1\beta_2 + \alpha_2\beta_1 + \alpha_3\beta_4 - \alpha_4\beta_3)i + (\alpha_1\beta_3 - \alpha_2\beta_4 + \alpha_3\beta_1 + \alpha_4\beta_2)j + (\alpha_1\beta_4 + \alpha_2\beta_3 - \alpha_3\beta_2 + \alpha_4\beta_1)k$.

É facil ver que $(\mathbb{H}, +, \cdot)$ é uma anel com 1, não comutativo. Mais ainda, se $x = a + bi + cj + dk \in \mathbb{H}$, $x \neq 0$, então $a^2 + b^2 + c^2 + d^2 \neq 0$ e $x^{-1} = \dfrac{a - bi - cj - dk}{a^2 + b^2 + c^2 + d^2} \in \mathbb{H}$ é tal que $x \cdot x^{-1} = 1 = x^{-1} \cdot x$. Assim, tomando $\overline{x} = a - bi - cj - dk$, temos que $x \cdot \overline{x} = a^2 + b^2 + c^2 + d^2 = N(x)$ e $x^{-1} = \dfrac{\overline{x}}{N(x)}$. Logo, $\mathbb{H}$ é um anel com divisão e não é corpo, pois não é comutativo.

O próximo teorema apresenta as primeiras propriedades básicas de um anel.

Teorema 1 *Seja* $(R, +, \cdot)$ *um anel. Então:*

(i) *O elemento neutro da $+$, denotado por $0(=0_R)$, é único.*

(ii) *Para todo $a \in R$, o* **oposto** *de a (o inverso com relação $a+$), $-a$, é único.*

(iii) *Valem as leis do cancelamento para $a+$.*

(iv) *Para todo $a \in R$, $a \cdot 0 = 0 \cdot a = 0$.*

(v) *Para todo $a, b \in R$, $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$ e $(-a) \cdot (-b) = a \cdot b$.*

(vi) *Se R é um anel com 1, então 1_R é único.*

(vii) *Se R tem mais que um elemento e R tem 1, então $1 \neq 0$.*

(viii) *Se R é um anel no qual vale a lei do cancelamento à esquerda (respectivamente, à direita) para o produto, então R não tem divisores de zero à esquerda (resp., à direita).*

Dem.: *(i)* Se existem 0 e $0'$ em R tais que $a + 0 = 0 + a = a$ e $a + 0' = 0' + a = a$, para todo $a \in R$, então, em particular, $0 = 0 + 0' = 0'$, ou seja, o elemento neutro da $+$ é único.
(ii) Para $a \in R$, sejam $b, c \in R$ tais que $0 = a + b = b + a$ e $0 = a + c = c + a$. Então $b = b + 0 = b + (a + c) = (b + a) + c = 0 + c = c$, logo o oposto é único.
(iii) Mostremos somente que vale a lei do cancelamento à esquerda, o caso à direita é análogo.

Se $a, b, c \in R$ são tais que $a+b = a+c$, então $(-a)+(a+b) = (-a)+(a+c)$, o que implica que $((-a)+a)+b = ((-a)+a)+c$. Logo $0+b = 0+c$ e, consequentemente $b = c$.
(iv) Para $a \in R$, temos $a \cdot 0 = a \cdot (0+0) = a \cdot 0 + a \cdot 0$. Usando *(iii)*, temos $a \cdot 0 = 0$. Mostrar que $0 \cdot a = 0$, para todo $a \in R$, é análogo.
(v) Mostremos inicialmente que $a \cdot (-b) = -(a \cdot b)$. Pela unicidade do oposto, é suficiente mostrar que $a \cdot (-b) + a \cdot b = 0 = a \cdot b + a \cdot (-b)$. Mas, $a \cdot (-b) + a \cdot b = a \cdot ((-b) + b) = a \cdot 0 = 0$. A outra igualdade é análoga.

De maneira análoga mostra-se que $(-a) \cdot b = -(a \cdot b)$.

Agora, usando as igualdades acima, temos $(-a) \cdot (-b) = -(a \cdot (-b)) = a \cdot (-(-b)) = a \cdot b$.

(vi) Se 1 e 1' são elementos neutros para $\cdot$. então $1 = 1 \cdot 1' = 1'$. Portanto $1 = 1'$.

(vii) Se $1 = 0$ em R, então para todo $a \in R$ temos $a = a \cdot 1 = a \cdot 0 = 0$, ou seja, $R = \{0\}$,o que é uma contradição, portanto $1 \neq 0$ em R.

(viii) Se $a \in R$, $a \neq 0$ e $a \cdot b = 0$, então $a \cdot b = a \cdot 0$ e $a \neq 0$. Por hipótese temos $b = 0$, ou seja, R não possui divisores de zero à esquerda. ■

Corolário 1 *Todo corpo é domínio, mais ainda, todo anel com divisão não tem divisores de zero.*

Dem.: Se F é um corpo, então F é um anel comutativo com 1 onde todo elemento não nulo tem inverso com relação a multiplicação, ou seja, $(F - \{0\}, \cdot)$ é um grupo abeliano.

Se $a, b \in F$ são tais que $a \cdot b = 0$ e $a \neq 0$, então $a^{-1} \in F$ e $b = 1 \cdot b = (a^{-1} \cdot a) \cdot b = a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 = 0$. ■

A recíproca do corolário anterior não vale. O anel dos inteiro $\mathbb{Z}$ é um domínio que não é corpo.

Corolário 2 *Se R é um anel comutativo com 1 no qual valem as leis do cancelamento, então R é um domínio.*

Dem.: Segue de (v) do Teorema anterior. ■

Vale a volta do corolário acima, ou seja, se R é um domínio, então valem as leis do cancelamento para o produto em R.

De fato, sejam R um domínio e $a, b, c \in \mathbb{R}$, $a \neq 0$ tais que $a \cdot b = a \cdot c$. Então $0 = a \cdot b - (a \cdot c)a \cdot b + a(-c) = a \cdot (b + (-c)) = a \cdot (b - c)$. Como $a \neq 0$ e R é um domínio, temos $b - c = 0$, ou seja $b = c$. Portanto valem a lei do cancelamento à

esquerda e, como R é comutativo, vale também o cancelamento à direita. Com isso obtemos:

Teorema 2 *Um anel comutativo com 1 é um domínio se, e somente se, valem as leis do cancelamento (para o produto).*

Os anéis $\mathbb{Z}$, $\mathbb{Z}[x]$, $\mathbb{Z}_p[x]$ (p primo) são domínios, mas não são corpos e são infinitos.

Existem domínios finitos que não são corpos? **Não**.

Teorema 3 *Todo domínio finito com mais de um elemento é corpo.*

Dem.: Seja R um domínio finito com $1 \neq 0$. Desde que R é corpo se todo elemento não nulo tem inverso multiplicativo, para todo $a \in R$, $a \neq 0$, temos que $\{a, a^2, a^3, \ldots, a^k, \ldots\} \subseteq R$. Como R é finito, temos que $\{a, a^2, a^3, \ldots, a^k, \ldots\}$ é finito.

Seja s o menor inteiro positivo tal que $a^s = a^r$, para algum $r \neq s$ $(r > s)$.

Como $r > s$, podemos escrever $r = s+t$, com $t > 0$ e $0 = a^s - a^{s+t} = a^s \cdot (1 - a^t)$.

Como R é domínio e $a \neq 0$, temos $a^s \neq 0$. o que implica que $a^t = 1$, para algum $t > 0$.

Se $t = 1 \Rightarrow a = 1 \Rightarrow a^{-1} = a = 1 \in R$.

Se $t > 1 \Rightarrow 1 = a \cdot a^{t-1} \Rightarrow a^{-1} = a^{t-1} \in R$.

Portanto, para todo $a \in R$, $a \neq 0$, temos que $a^{-1} \in R$, i.é., R é corpo. ■

Observação: Também vale: *Todo anel com divisão finito é corpo.*

3 Exercícios

1. Sejam $(R, +, .)$ um anel com 1 e R^* o conjunto de todas as unidades (elementos inversíveis com relação ao produto $(.)$) de R. Mostre que $(R^*, .)$ é um grupo.

2. Encontre R^* quando:
   (a) $R = \mathbb{Z}$; **(b)** $R = \mathbb{Z}_6$;
   (c) $R = \mathbb{Z}[x]$; **(d)** $R = \mathbb{Z}_7$;
   (e) R é o anel dos quatérnios reais.

3. No anel dos inteiros de Gauss G, mostre que um elemento é uma unidade se, e somente se ele tem norma 1(onde a norma é a norma dos números complexos), ou seja $G^* = \{a + bi \in G;\ a^2 + b^2 = 1\}$. Determine G^*.

4. No anel $\mathbb{Z}_5[x]$, calcule:
   (a) $(\bar{2} + \bar{3}x + \bar{4}x^2) + (\bar{1} + \bar{2}x + \bar{4}x^2)$;
   (b) $(\bar{2} + \bar{3}x + \bar{4}x^2).(\bar{1} + \bar{2}x + \bar{4}x^2)$;
   (c) $(\bar{1}x + \bar{1}x^3).(\bar{1} + \bar{1}x^2 + \bar{2}x^3)$.

5. Se R é um conjunto e $*$ é uma operação binária em R tal que $(R, *, *)$ é um anel, mostre que R tem somente um elemento.

6. Seja $R = \mathbb{Z} \times \mathbb{Z}$. Defina em R as operações $+$ e $.$ por:
   $(a, b) + (c, d) = (a + c, b + d)$; $(a, b).(c, d) = (ac, bd)$
   para todo a, b, c, $d \in R$. Mostre que R é um anel comutativo com 1.

7. Seja $R = \{f : \mathbb{R} \to \mathbb{R};\ f \text{ é função }\}$. Para todo f, $g \in R$, definimos:
   $(f + g)(x) = f(x) + g(x)$ $(f.g)(x) = f(g(x))$,
   para todo $x \in \mathbb{R}$. $(R, +, .)$ é um anel???

8. Seja $R = \mathbb{Z}$. Defina $\odot$ em R por: $a \odot b = a + b - ab$, para todo a, $b \in \mathbb{Z}$. Se $+$ é a adição usual dos inteiros, é $(R, +, \odot)$ um anel comutativo com 1???

9. Seja R um anel. Um elemento $e \in R$ é *idempotente* se $e^2 = e$; um elemento $k \in R$ é *quadrado nilpotente* se $k^2 = 0$; se R tem 1, então um elemento $v \in R$ é *involutório* se $v^2 = 1$. Seja R um anel com 1 e $e \in R$ um idempotente. Mostre que:

   (a) $1 - e$ é idempotente.

   (b) para cada $x \in R$, $ex(1 - e)$ é quadrado nilpotente.

   (c) para cada $x \in R$, $e + ex(1 - e)$ é idempotente.

   (d) para cada $x \in R$, $1 + ex(1 - e)$ é uma unidade(inversível) em R.

   (e) $2e - 1$ é involutório.

10. Encontre todos os elementos idempotentes do anel $\mathbb{Z}_8$.

11. Mostre que em um domínio, os únicos elementos idempotentes são o 0 e o 1.

12. Um anel R, com 1, é dito ser um *anel Booleano* se todo elemento de R é idempotente. Mostre que, neste caso, temos:

    (a) $a = -a$, $\forall a \in R$; **(b)** R é comutativo.

13. De exemplos de não triviais elementos idempotentes, quadrado nilpotentes e involutório no anel $M_2(\mathbb{Z})$.

14. Mostre que o subconjunto de $M_2(\mathbb{Z})$ consistindo de todas as matrizes cujas entradas são números inteiros pares, $M_2(2\mathbb{Z})$, é um anel não comutativo, sem 1.

15. Sejam $(R, +, .)$ e $(S, \oplus, \odot)$ anéis. Mostre que o conjunto $R \times S = \{(r, s);\ r \in R, s \in S\}$, com as operações coordenada à coordenada, ou seja:
    $(r_1, s_1) \mp (r_2, s_2) = (r_1 + r_2, s_1 \oplus s_2)$ e
    $(r_1, s_1) \bullet (r_2, s_2) = (r_1.r_2, s_1 \odot s_2)$
    é um anel, chamado o *produto direto externo* de R e S.

16. Se R e S são domínios, então $R \times S$ é também um domínio???

17. Como são os elementos inversíveis de $R \times S$ en termos das unidades de R e de S??

18. Seja R o conjunto de todas as matrizes de $M_2(\mathbb{Z})$, da forma $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$.

    (a) Mostre que, com as operações induzidas pelas operações de $M_2(\mathbb{Z})$, R é um anel.

    (b) Mostre que $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ é um divisor de zero à direita de R mas não é divisor de zero à esquerda.

19. Encontre todos os divisores de zero dos seguintes anéis:

    (a) $\mathbb{Z}_4$; **(b)** $\mathbb{Z}_8$;

    (c) $\mathbb{Z} \times \mathbb{Z}$; **(d)** $\mathbb{Z}_4 \times \mathbb{Z}_6$;

    (e) $M_2(\mathbb{Z}_2)$, **(f)** G, o anel dos inteiros de Gauss.

20. Mostre que se R é um domínio e $a \in R$ é tal que $a^2 = 1$, então $a = 1$ ou $a = -1$.

4 Subanéis

Definição 5 Um subconjunto não vazio S de um anel $(R, +, \cdot)$ é dito ser um **subanel** de R se, com as operações induzidas pelas operações de R (restrições), S é um anel.

Teorema 4 *Um subconjunto $S \neq \emptyset$ de um anel $(R, +, \cdot)$ é um subanel de R se, e somente se valem as seguinte afirmações:*

(i) Para todo $a, b \in S \Rightarrow a - b = a + (-b) \in S$.

(ii) Para todo $a, b \in S \Rightarrow a \cdot b \in S$.

Dem.: ($\Rightarrow$) Se $S \subseteq R$ é um subanel, então para todo $a, b \in S$, temos que $-b \in S$ e $a \in S$. Logo $a - b \in S$, pois $+$ é uma operação binária em S e, $a \cdot b \in S$, pois $\cdot$ é uma operação em S.

($\Leftarrow$) Sejam $+|_S : S \times S \to R$ e $\cdot|_S : S \times S \to R$, as restrições de $+$ e $\cdot$ à S. A condição *(ii)* implica que $\Rightarrow \cdot|_S : S \times S \to S$, i.é, $\cdot|_S$ é uma operação em S. Mais ainda:

- $0 \in S$, pois $S \neq \emptyset \Rightarrow \exists\, a \in S \stackrel{(i)}{\Longrightarrow} 0 = a - a \in S$.
- Para todo $b \in S \Rightarrow -b \in S$, pois para $b \in S$, como $0 \in S \stackrel{(i)}{\Longrightarrow} -b = 0 - b \in S$.
- Para todo $a, b \in S \Rightarrow a + b \in S$, pois $a + b = a - (-b)$ e $-b \in S \stackrel{(i)}{\Longrightarrow} a + b \in S$,

o que implica que $+|_S$ é uma operação em S.

Como a associatividade de $+$, a comutatividade de $+$, a associatividade de $\cdot$ e a distributividade valem em R, temos que também valem em S. Assim, $(S, +, \cdot)$ é uma anel, o que mostra que S é um subanel de R. ■

Exemplo 12 $2\mathbb{Z}$ é um subanel de $\mathbb{Z}$. Mais geralmente, $n\mathbb{Z} \subseteq \mathbb{Z}$ são subanéis, para todo $n \geq 0$.

De fato, para todo $a, b \in n\mathbb{Z} \Rightarrow a = nk_1$, $b = nk_2$, com $k_1, k_2 \in \mathbb{Z}$. Assim, $a - b = n(k_1 - k_2) \in n\mathbb{Z}$ e $a \cdot b = n(k_1\, k_2\, n) \in n\mathbb{Z}$.

Exemplo 13 Seja $R = \mathbb{Z}_6$.

$S_1 = \{\overline{0}, \overline{2}, \overline{4}\}$ e $S_2 = \{\overline{0}, \overline{3}\}$ são subanéis de $\mathbb{Z}_6$, pois $\overline{2} \cdot \overline{4} = \overline{2}$, $-\overline{2} = \overline{4}$; $\overline{3} = -\overline{3}$, $\overline{3} \cdot \overline{3} = \overline{3}$.

Observe que $1_R = \overline{1}$, $1_{S_1} = \overline{4}$, $1_{S_2} = \overline{3}$. Assim, $Si \subseteq R$ são subanéis com 1 tais que $1_{S_i} \neq 1_R$, para $i = 1, 2$.

Exemplo 14 $M_2(n\,\mathbb{Z}) \subseteq M_2(\mathbb{Z})$, para todo $n \geq 0$ são subanéis de $M_2(\mathbb{Z})$.

Exemplo 15 $\{0\}$ e R são sempre subanéis de R, chamados os **subanéis triviais.**

Exemplo 16 $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ é uma cadeia de subanéis.

Exemplo 17 Sejam $R = M_2(\mathbb{Z})$, $S = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} ; \ a, b \in \mathbb{Z} \right\}$ e $A = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} ; \ a \in \mathbb{Z} \right\}$.

S é um subanel de R, A é um subanel de R e de S, com $1_R = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$; $1_A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, pois $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$; para todo $a \in \mathbb{Z}$.

Assim, $A \subseteq R$, é um subanel de R, com 1, mas $1_A \neq 1_R$.

Mais ainda, S não tem 1. De fato, suponhamos por absurdo, que $1_S = \begin{pmatrix} a_0 & b_0 \\ 0 & 0 \end{pmatrix}$, para algum a_0, $b_0 \in \mathbb{Z}$. Então, em particular,

$$\begin{pmatrix} a_0 & b_0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a_0 & b_0 \\ 0 & 0 \end{pmatrix},$$

o que implica que $a_0 = 1$ e $b_0 = 0$, ou seja $1_S = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$.

Mas $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \cdot 1_S = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$, para algum $b \in \mathbb{Z}$. Portanto S não tem 1.

Assim, $S \subseteq R$, é um subanel com S sem 1 e R com 1 e $A \subseteq S$, com S sem 1 e A com 1.

Exemplo 18 Nem todo subgrupo é subanel. Por exemplo, para $R = M_2(\mathbb{Z})$, temos $H = \left\{ \begin{pmatrix} a & b \\ c & 0 \end{pmatrix};\ a,b,c \in \mathbb{Z} \right\}$ é um subgrupo de $(R,+)$, mas H não é um subanel de R, pois $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \in H$ e $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \notin H$.

Todo anel contém um subanel comutativo.

Definição 6 *Se $(R, +, \cdot)$ é um anel, então o* ***centro de*** *R é o conjunto:*

$$C(R) = \{a \in R;\ a \cdot b = b \cdot a, \quad \forall\, b \in R\}.$$

Se R é um anel comutativo, então claramente $C(R) = R$.

Teorema 5 *Para todo anel R, o centro de R, $C(R)$ é um subanel comutativo de R.*

Dem.: Como $0 \cdot a = a \cdot 0 = 0$, para todo $a \in R$, temos que $0 \in C(R) \Rightarrow C(R) \neq \emptyset$.

Para $a, b \in C(R)$ e $r \in R$, temos $(a-b)\cdot r = a\cdot r + (-b)\cdot r = a\cdot r - (b\cdot r) = r\cdot a - r\cdot b = r\cdot a + r\cdot(-b) = r\cdot(a-b)$, ou seja $a - b \in C(R)$. Mais ainda, $(a\cdot b)\cdot r = a\cdot(b\cdot r) = a\cdot(r\cdot b) = (a\cdot r)\cdot b = (r\cdot a)\cdot b = r\cdot(a\cdot b)$, o que implica que $a \cdot b \in C(R)$.

Portanto $C(R)$ é um subanel de R, claramente comutativo. ■

Exemplo 19 Para $R = M_2(\mathbb{Z})$, $C(R) = ?$

Se $x = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in C(R)$, então, em particular $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, ou seja $\begin{pmatrix} a & 0 \\ c & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$, o que implica que $b = c = 0$. Logo $x = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$.

Mas, $\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$, ou seja $\begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & d \\ 0 & 0 \end{pmatrix} \Rightarrow a = d \Rightarrow x = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$, com $a \in \mathbb{Z}$. Assim, $C(R) \subseteq \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix};\ a \in \mathbb{Z} \right\}$; a inclusão contraria é trivial.

Portanto, $C(R) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix};\ a \in \mathbb{Z} \right\}$.

5 Homomorfismo de Anéis e Ideais

Definição 7 Sejam $(R, +, \cdot)$ e $(S, \oplus, \odot)$ anéis. Uma função $\varphi : R \to S$ é um **homomorfismo de anéis** se, para todo $a, b \in R$, temos:

(i) $\varphi(a+b) = \varphi(a) \oplus \varphi(b)$, (i.é, φ é um homomorfismo de grupos)

(ii) $\varphi(a \cdot b) = \varphi(a) \odot \varphi(b)$.

Se, além disso, φ é bijetora, dizemos que φ é um **isomorfismo de anéis** e, neste caso, dizemos tamém que os anéis R e S são isomorfos e denotamos por $R \cong S$ ou $R \overset{\varphi}{\cong} S$.

Se $(R, +, \cdot) = (S, \oplus, \odot)$, dizemos que φ é um **endomorfismo** de anéis.

Se $\varphi : R \to R$ é um isomorfismo, então φ é um **automorfismo** do anel R.

Exemplo 20 Seja $\varphi : \mathbb{Z} \to \mathbb{Z}_n$, definida por $\varphi(a) = \overline{a}$, para todo $a \in \mathbb{Z}$.

- φ é um homomorfismo de anéis. De fato, para todo $a, b \in \mathbb{Z}$,

$\varphi(a+b) = \overline{a+b} = \overline{a} + \overline{b} = \varphi(a) \oplus \varphi(b)$

$\varphi(a \cdot b) = \overline{a \cdot b} = \overline{a} \cdot \overline{b} = \varphi(a) \odot \varphi(b)$.

φ é sobrejetor mas não é injetor, pois $\varphi(a) = \varphi(a+n)$, para todo $a \in \mathbb{Z}$.

Exemplo 21 Seja $\varphi : \mathbb{Z} \to M_2(\mathbb{Z})$, definido por

$\varphi(a) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$, $\forall\, a \in \mathbb{Z}$.

φ é um homomorfismo de anéis, injetor mas não sobrejetor.

Exemplo 22 Seja $\varphi : \mathbb{Z} \to C(M_2(\mathbb{Z}))$, definido por

$\varphi(a) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$, para todo $a \in \mathbb{Z}$.

φ é um isomorfismo de anéis, ou seja, $C(M_2(\mathbb{Z})) \cong \mathbb{Z}$.

Exemplo 23 Todo homomorfismo de anéis é também um homomorfismo de grupos, mas não vale a recíproca. Por exemplo, $\varphi : \mathbb{Z} \to \mathbb{Z}$, definida por $\varphi(a) = 2a$, para todo $a \in \mathbb{Z}$, é um homomorfismo de grupos e não é homomorfismo de anéis, pois $\varphi(ab) = 2(ab) \neq \varphi(a)\,\varphi(b) = (2a)(2b)$, para todo $a, b \in \mathbb{Z}$.

Teorema 6 *Seja* $\varphi : (R, +, \cdot) \to (S, \oplus, \odot)$ *um homomorfismo de anéis. Então:*

(i) $\varphi(O_R) = O_S$,

(ii) $\varphi(-a) = -\varphi(a)$, $\forall\ a \in R$,

(iii) $\varphi(R) = \{\varphi(a);\ a \in R\}$ *é um subanel de* S.

(iv) Se R *tem 1, então* $\varphi(1_R) = 1_{\varphi(R)}$.

(v) Se $a \in R$ *é inversível, ou seja, tem inverso multiplicativo, então* $\varphi(a^{-1}) = \varphi(a)^{-1}$ *em* $\varphi(R)$.

Dem.: *(i)* Como $\varphi(O_R) \oplus O_S = \varphi(O_R) = \varphi(O_R + 0_R) = \varphi(O_R) \oplus \varphi(O_R)$, do cancelamento da operação $\oplus$, temos $\varphi(O_R) = O_S$.
(ii) Para todo $a \in R$, temos $O_S = \varphi(O_R) = \varphi(a + (-a)) = \varphi(a) \oplus \varphi(-a)$, o que implica que $\varphi(-a) = -\varphi(a)$.
(iii) $\varphi(R)$ é um subanel de S, pois para todo $\varphi(a), \varphi(b) \in \varphi(R)$, temos:

- $\varphi(a) - \varphi(b) = \varphi(a) \oplus \varphi(-b) = \varphi(a + (-b)) = \varphi(a - b) \in \varphi(R)$.
- $\varphi(a) \odot \varphi(b) = \varphi(a \cdot b) \in \varphi(R)$.

(iv) Para todo $\varphi(a) \in \varphi(R)$,

$\varphi(a) \odot \varphi(1_R) = \varphi(a \cdot 1_R) = \varphi(a) = \varphi(1_R \cdot a) = \varphi(1_R) \odot \varphi(a) \Rightarrow \varphi(1_R) = 1_{\varphi(R)}$.

(v) Se $a \in R$ tem inverso, então $1_R = a \cdot a^{-1} = a^{-1} \cdot a$, o que implica que $1_{\varphi(R)} = \varphi(1_R) = \varphi(a \cdot a^{-1}) = \varphi(a) \odot \varphi(a^{-1}) = \varphi(a^{-1}) \odot \varphi(a) \Rightarrow \varphi(a^{-1}) = \varphi(a)^{-1}$. ■

Exemplo 24 Exemplo de um homomorfismo de anéis $\varphi : R \to S$, com $\varphi(1_R) \neq 1_S$.

Seja $\varphi : \mathbb{Z}_2 \to \mathbb{Z}_6$ o homomorfismo de anéis definido por $\varphi(\overline{0}) = \overline{0}$ e $\varphi(\overline{1}) = \overline{3}$. Temos então que $\varphi(\mathbb{Z}_2) = \{\overline{0}, \overline{3}\} \subseteq \mathbb{Z}_6$ é um subanel, com $\varphi(\overline{1}) = \overline{3} = 1_{\varphi(\mathbb{Z}_2)} \neq 1_{\mathbb{Z}_6}$.

Se $\varphi : R \to S$ é uma função e $S' \subseteq S$, então definimos a **imagem inversa** de S' por φ, por $\varphi^{-1}(S') = \{r \in R;\ \varphi(r) \in S'\}$.

Teorema 7 *Se* $\varphi : (R, +, \cdot) \to (S, \oplus, \odot)$ *é um homomorfismo de anéis e* S' *é um subanel de* S*, então* $\varphi^{-1}(S')$ *é um subanel de* R*, ou seja, a imagem inversa, por homomorfismo, de subanel é subanel.*

Dem.: De fato:

- $\varphi^{-1}(S') \neq \emptyset$, pois como $\varphi(O_R) = O_S \in S' \Rightarrow O_R \in \varphi^{-1}(S')$;
- Para todo $a, b \in \varphi^{-1}(S') \overset{\text{def}}{\Longrightarrow} \varphi(a), \varphi(b) \in S'$.

Como S' é subanel, $\varphi(a) - \varphi(b) \in S' \Rightarrow \varphi(a - b) \in S'$. Daí, $a - b \in \varphi^{-1}(S')$.

Novamente, como S' é subanel, $\varphi(a) \odot \varphi(b) \in S' \Rightarrow \varphi(a \cdot b) \in S'$. Logo, $a \cdot b \in \varphi^{-1}(S')$. Portanto, $\varphi^{-1}(S')$ é um subanel de R. ■

Corolário 3 *Se* $\varphi : R \to S$ *é um homomorfismo de anéis, então* Ker $(\varphi) = \varphi^{-1}(\{O_s\})$ *é um subanel de* R*, chamado o* **núcleo do homomorfismo** φ*. Note que* Ker $(\varphi) = \{a \in R;\ \varphi(a) = O_S\}$.

Teorema 8 *Se* $\varphi : R \to S$ *é um homomorfismo de anéis e* $a \in$ Ker (φ) *então* $a \cdot r \in$ Ker (φ) *e* $r \cdot a \in$ Ker (φ)*, para todo* $r \in R$*.*

Dem.: Se $a \in$ Ker (φ) e $r \in R$, então temos $\varphi(a \cdot r) = \varphi(a) \odot \varphi(r) = O_S \odot \varphi(r) = O_S$. Logo, $a \cdot r \in$ Ker (φ). ■

As propriedades que Ker (φ) satisfaz no teorema anterior são as propriedades que caracterizam certos subconjuntos especiais de um anel.

Definição 8 Um subanel I de um anel R é:

- um ***ideal*** de R, se $\forall\, a \in I$ e $r \in R \Rightarrow a \cdot r \in I$ e $r \cdot a \in I$.
- um ***ideal à direita*** de R se, $\forall\, a \in I$ e $r \in R \Rightarrow a \cdot r \in I$.
- um ***ideal à esquerda*** de R se, $\forall\, a \in I$ e $r \in R \Rightarrow r \cdot a \in I$.

O próximo teorema caracteriza um ideal.

Teorema 9 *Sejam R um anel e $I \neq \emptyset$ um subconjunto de R. I é um ideal de R se, e somente se para todo $a, b \in I$ e $r \in R$, temos:*

(i) $a - b \in I$.

(ii) $a \cdot r \in I$ *e* $r \cdot a \in I$.

Dem.: Imediata. ■

Exemplo 25 $\{0\}$ e R são os **ideais triviais** de R.

Exemplo 26 Se $\varphi : R \to S$ é um homomorfismode anéis, então $I = \text{Ker}\ (\varphi)$ é um ideal de R.

Exemplo 27 Ideal $\underset{\not\Leftarrow}{\Rightarrow}$ subanel

Por exemplo, para $R = \mathbb{Z}[X]$, temos que $\mathbb{Z} \subseteq R$ é um subanel mas não é um ideal, pois $a = 1 \in \mathbb{Z}$ e $r = X \in R \Rightarrow a \cdot r \notin \mathbb{Z}$.

Exemplo 28 Para $R = \mathbb{Z}$, temos $I = n\mathbb{Z}$, com $n \geq 0$ são todos os ideais de $\mathbb{Z}$. Mais ainda, todos são núcleos de homomorfismos de anéis. De fato, $n\mathbb{Z} = \text{Ker}\ (\varphi)$, onde $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ é o homomorfismo canônico dado por $\varphi(a) = \overline{a}$, para todo $a \in \mathbb{Z}$, e, neste caso, $\text{Ker}\ (\varphi) = \{a \in \mathbb{Z};\ \overline{a} = \overline{0}\} = n\mathbb{Z}$.

Exemplo 29 Para $R = M_2(\mathbb{Z})$, temos $I = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix};\ a, b \in \mathbb{Z} \right\}$ é um subgrupo aditivo de $(R, +)$ tal que para todo $x = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \in I$ e $r = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in R$,

$x \cdot r = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa' + bc' & ab' + bd' \\ 0 & 0 \end{pmatrix} \in I$, ou seja, I é um ideal à direita de R, mas não é um ideal à esquerda pois

$r \cdot x = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} aa' & a'b \\ c'a & c'b \end{pmatrix} \notin I$ em geral.

Exemplo 30 Para $R = M_2(\mathbb{Z})$, $I = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} ;\ a, b \in \mathbb{Z} \right\}$ é um ideal à esquerda, mas não é à direita.

Exemplo 31 $J = M_2(n\mathbb{Z})$, com $n \geq 0$ são todos ideais bilaterais de R.

Exemplo 32 Se $S \subseteq R$ é subanel e $I \subseteq S$ é um ideal $\Rightarrow I \subseteq R$ é um ideal? Não.

Para $R = M_2(\mathbb{Z})$,

$S = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} ;\ a, b, d \in \mathbb{Z} \right\}$ e

$I = \left\{ \begin{pmatrix} 0 & c \\ 0 & 0 \end{pmatrix} ;\ c \in \mathbb{Z} \right\}$, temos que

$S \subseteq R$ é subanel, I é ideal de S e não é ideal de R, pois

$$\left.\begin{array}{l} \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} \begin{pmatrix} b & c \\ 0 & d \end{pmatrix} = \begin{pmatrix} 0 & ad \\ 0 & 0 \end{pmatrix} \in I \\ \\ \begin{pmatrix} b & c \\ 0 & d \end{pmatrix} \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & ba \\ 0 & 0 \end{pmatrix} \in I \end{array}\right\} \Rightarrow I \text{ é um ideal de } S \text{ e}$$

I não é ideal de R

$$x \cdot r = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \notin I\,.$$

Proposição 1 *Se R é um anel e $a \in R$ então:*

(i) $a \cdot R = \{a \cdot r;\ r \in R\}$ *é um ideal à direita de* R.

(ii) $R \cdot a = \{r \cdot a;\ r \in R\}$ *é um ideal à esquerda de* R.

(iii) Se R é comutativo $\Rightarrow a \cdot R = R \cdot a$ *é um ideal de* R.

(iv) Se R é comutativo com 1, então $a \cdot R$ é o menor ideal de R que contém a.

Dem.: A demonstração dos itens *(i)*, *(ii)* e *(iii)* ficam como exercício.

(iv) Mostremos que se $I \subseteq R$ é um ideal e $a \in I \Rightarrow a \cdot R \subseteq I$.

De fato, se $a \in I \Rightarrow a \cdot r \in I$, para todo $r \in R$, pois I é ideal $\Rightarrow a \cdot R \subseteq I$. Mais ainda, se $1 \in R \Rightarrow a = a \cdot 1 \in a \cdot R$. ■

Exemplo 33 Um anel R sem 1 e $a \in R$ com $a \notin a \cdot R$.

Para $R = 2\mathbb{Z}$, $a = 2$, temos $2R = 4\mathbb{Z}$ e $2 \notin 4\mathbb{Z} = 2R$.

Definição 9 *Sejam R um anel comutativo e $a \in R$. A intersecção de todos os ideais de R que contém a é o* ***ideal principal gerado por*** *a e denotado por (a).*

Proposição 2 *Se R é comutativo com 1, então $(a) = a \cdot R$. Se R é comutativo sem 1, então $(a) = \{a \cdot r + m \cdot a;\ r \in R \text{ e } m \in \mathbb{Z}\}$.*

Dem.: Demonstremos o caso em que R não tem 1.

Seja $J = \{a \cdot r + m \cdot a\,;\, r \in R,\ m \in \mathbb{Z}\}$. Mostre, como exercício, que J é um ideal de R.

Agora, $a = a \cdot O_R + 1 \cdot a \in J$, ou seja, J é um ideal que contém a. Assim, $(a) = \bigcap_{a \in I} I \subseteq J$.

Resta mostrar que se I é um ideal de R e $a \in I$, então $J \subseteq I$, pois assim, teremos $J \subseteq \bigcap_{a \in I} I$.

Se $a \in I$, então $a \cdot r \in I$, para todo $r \in R$ e $m \cdot a \in I$, para todo $m \in \mathbb{Z}$. Logo, $ar + ma \in I$, para todo $r \in R$ e $m \in \mathbb{Z}$, o que mostra que $J \subseteq I \Rightarrow J \subseteq \bigcap_{a \in I} I = (a)$.

Logo, $J = (a)$, como queríamos. ■

Exemplo 34 Para $R = 2\mathbb{Z}$, $a = 2$, temos $2R = 4\mathbb{Z}$ e $(2) = \{2 \cdot r + m \cdot 2;\ r \in 2\,\mathbb{Z} \text{ e } m \in \mathbb{Z}\} = 4\,\mathbb{Z} + 2\,\mathbb{Z} = 2\,\mathbb{Z} = R$.

6 Anéis Quocientes e o Primeiro Teorema do Isomorfismo

Sejam R um anel e I um ideal (bilateral) de R. Definimos uma relação $\sim$ em R por:

$$x \sim y \Leftrightarrow x - y \in I,$$

para todo $x, y \in R$. É facil ver que $\sim$ define uma relação de equivalência em R. Mais ainda, para todo $a \in R$, temos que $\overline{a} = \{x \in R;\ x - a \in I\} = a + I$.

Seja R/I o conjunto das classes de equivalência de $\sim$, ou seja,

$$R/I = \{a + I;\ a \in R\}.$$

Observe que $a + I = b + I$ se, e somente se $a - b \in I$.

Em R/I definimos as operações $+$ e $\cdot$ por:

$(a + I) + (b + I) = (a + b) + I$,

$(a + I) \cdot (b + I) = (a \cdot b) + I$,

para todo $a, b \in R$.

Vejamos que $+$ e $\cdot$ estão bem definidas, ou seja, não dependem da escolha dos representantes das classes de equivalência.

Se $a + I = a' + I$ e $b + I = b' + I$, então existem $x_1, x_2 \in I$ tais que $a = a' + x_1$ e $b = b' + x_2$.

Assim,

$$\begin{aligned}(a + I) + (b + I) &= (a + b) + I = ((a' + x_1) + (b' + x_2)) + I = \\ &= (a' + b') + (x_1 + x_2) + I = (a' + b') + I + (x_1 + x_2) + I = \\ &= (a' + b') + I + 0 + I = (a' + b' + 0) + I = \\ &= (a' + I) + (b' + I),\end{aligned}$$

e

$$
\begin{aligned}
(a+I)\cdot(b+I) &= a\cdot b+I \;= (a'+x_1)(b'+x_2)+I = \\
&= (a'b'+a'x_2+x_1b'+x_1x_2)+I \;= \\
&= (a'b'+I)+((\underbrace{a'x_2+x_1b'+x_1x_2}_{\in I})+I) = \\
&= (a'b'+I)+(0+I) = \\
&= (a'b'+0)+I = a'b'+I = (a'+I)(b'+I).
\end{aligned}
$$

Exercício 3 Mostre que $(\, R/I,\, +\,,\, \cdot\,)$ é um anel. Tal anel é chamado o **anel quociente de R por I.**

Observe que no anel quociente, $0_{R/I} = I$ e $-(a+I) = (-a)+I$, para todo $a \in R$.

Com a noção de anel quociente, podemos mostrar que, de fato, todo ideal é o núcleo de um homomorfismo, ou seja:

Teorema 10 *Sejam R um anel e I um ideal de R. A função $\pi : R \to R/I$, definida por $\pi(a) = a+I$, para todo $a \in R$, é um homomorfismo sobrejetor de anéis com núcleo I, ou seja, todo ideal de R é núcleo de um homomorfismo de anéis com domínio R.*

Dem.: Que π é um homomorfismo de anéis é imediato, pois

$\pi(a+b) = (a+b)+I = (a+I)+(b+I) = \pi(a)+\pi(b)$,

$\pi(ab) = (ab)+I = (a+I)+(b+I) = \pi(a)\cdot\pi(b)$, para todo $a, b \in R$.

Agora, Ker $(\pi) = \{a \in R;\ \pi(a) = 0_S\} = \{a \in R;\ a+I = 0+I\} = \{a \in R;\ a \in I\} = I$. ■

Exemplo 35 Dado o ideal $n\,\mathbb{Z}$, com $n \geq 0$ do anel $\mathbb{Z}$, temos

$\mathbb{Z}/n\,\mathbb{Z} = \{a + n\,\mathbb{Z}\,;\ a \in \mathbb{Z}\}$.

Dado $a \in \mathbb{Z}$, pelo Algoritmo da Divisão, temos que existem $q, r \in \mathbb{Z}$ tais que $a = qn + r\,,$ com $0 \leq r \leq n-1$. Assim,

$$\begin{aligned} a+n\mathbb{Z} &= (nq+r)+n\mathbb{Z} = (nq+n\mathbb{Z})+(r+n\mathbb{Z}) = \\ &= (0+n\mathbb{Z})+(r+n\mathbb{Z}) = r+n\mathbb{Z}. \end{aligned}$$

Então $\mathbb{Z}/n\,\mathbb{Z} = \{r+n\mathbb{Z};\ r=0,1,\ldots,n-1\}$, onde $r+n\,\mathbb{Z} = \{r+n\,k;\ k\in\mathbb{Z}\} = \{b\in\mathbb{Z};\ b\equiv r \bmod n\} = \overline{r}\in\mathbb{Z}_n$, ou seja, $\mathbb{Z}/n\,\mathbb{Z} = \mathbb{Z}_n$.

Teorema 11 - Primeiro Teorema do Isomorfismo - *Sejam $(R,+,\cdot)$ e $(S,\hat{+},\hat{\cdot})$ anéis. O anel S é uma* **imagem homomórfica** *do anel R (ou seja, existe um homomorfismo sobrejetor de anéis $\varphi: R\to S$) se, e somente se, existe um ideal I de R tal que $R/I\cong S$.*

Dem.: ($\Leftarrow$) Se I é um ideal de R, com $R/I \overset{\psi}{\cong} S$ então, compondo com o homomorfismo canônico $\pi: R\to R/I$, temos que $\varphi = \psi\circ\pi : R\to S$ é um homomorfismo sobrejetor de anéis. Portanto S é uma imagem homomórfica de R.
($\Rightarrow$) Se $\varphi: R\to S$ é um homomorfismo sobrejetor, então $I = \text{Ker }(\varphi)$ é um ideal de R e $\psi: R/I\to S$, definido por $\psi(a+I) = \varphi(a)$, para todo $a\in R$ é um isomorfismo de anéis.

De fato,

- ψ está bem definido, pois se $a+I = b+I$, então $a-b\in I = \text{Ker }(\varphi) \Rightarrow \varphi(a-b) = 0 \Rightarrow \varphi(a) = \varphi(b) \Rightarrow \psi(a+I) = \psi(b+I)$.
- ψ é homomorfismo, pois φ o é.
- ψ é bijetor, pois dado $s\in S$, desde que φ é sobrejetor, existe $a\in R$, tal que $\varphi(a) = s$. Logo $\psi(a+I) = \varphi(a) = s$, o que mostra que ψ é sobrejetor.

Agora, se $\varphi(a) = \varphi(b)$, então $\varphi(a-b) = 0$, ou seja $(a-b)\in \text{Ker }(\varphi) = I$. Assim, $a+I = b+I$, o que mostra que ψ é injetor. ■

Em muitos textos, o próximo resultado é conhecido como o primeiro teorema do isomorfismo.

Corolário 4 *Se $\varphi: R\to S$ é um homomorfismo de anéis, então*

$$R/\text{Ker }(\varphi) \cong \varphi(R) = \text{Im }(\varphi).$$

Corolário 5 *Um homomorfismo sobrejetor de anéis $\varphi : R \to S$ é um isomorfismo se, e somente se* Ker $(\varphi) = \{0_R\}$.

Exemplo 36 $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$, pois $\varphi : \mathbb{Z} \to \mathbb{Z}_n$, definida por $\varphi(a) = \overline{a}$, é um homomorfismo sobrejetor com Ker $(\varphi) = n\mathbb{Z}$.

Exemplo 37 $\dfrac{M_2(\mathbb{Z})}{M_2(n\mathbb{Z})} \cong M_2(\mathbb{Z}_n)$, pois $\varphi : M_2(\mathbb{Z}) \to M_2(\mathbb{Z}_n)$ definido por

$$\varphi \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix},$$

é um homomorfismo de anéis sobrejetor, com

$$\text{Ker } (\varphi) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z});\ \begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix} = \begin{pmatrix} \overline{0} & \overline{0} \\ \overline{0} & \overline{0} \end{pmatrix} \right\}.$$

Agora, $\begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix} = \begin{pmatrix} \overline{0} & \overline{0} \\ \overline{0} & \overline{0} \end{pmatrix} \Leftrightarrow \overline{a} = \overline{b} = \overline{c} = \overline{d} = \overline{0}$, ou seja, $a, b, c, d \in n\mathbb{Z}$, o que implica que $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(n\mathbb{Z})$.

Portanto, Ker $(\varphi) \subseteq M_2(n\mathbb{Z})$ e, a inclusão contrária é obvia. O que mostra que $\dfrac{M_2(\mathbb{Z})}{M_2(n\mathbb{Z})} \cong M_2(\mathbb{Z}_n)$.

Exercício 4 Mostre que $\dfrac{\mathbb{Z} \times \mathbb{Z}}{\mathbb{Z} \times n\mathbb{Z}} \cong \mathbb{Z}_n$ e $\dfrac{\mathbb{Z} \times \mathbb{Z}}{n\mathbb{Z} \times m\mathbb{Z}} \cong \mathbb{Z}_n \times \mathbb{Z}_m$.

Teorema 12 *Se R é um anel com 1, então R contém um subanel que é isomorfo a $\mathbb{Z}$ ou a $\mathbb{Z}_n$ para algum $n > 0$.*

Dem.: Seja $A = \{n \cdot 1_R;\ n \in \mathbb{Z}\} \subseteq R$.

A é um subanel de R, pois $n \cdot 1_R - m \cdot 1_R = (n-m) \cdot 1_R \in A$ e $(n \cdot 1_R) \cdot (m \cdot 1_R) = (n \cdot m) \cdot 1_R \in A$.

Agora, se $n \cdot 1_R \neq m \cdot 1_R$, para todo $m \neq n$, então $\varphi : \mathbb{Z} \to A$, definido por $\varphi(n) = n \cdot 1_R$, para todo $n \in \mathbb{Z}$, é um isomorfismo de anéis e, neste caso, R contém um subanel isomorfo a $\mathbb{Z}$.

Se $n \cdot 1_R = m \cdot 1_R$, para algum $n > m$, então $(n-m) \cdot 1_R = 0$, com $n - m > 0$. Assim, $T = \{k \in \mathbb{Z};\ k > 0 \ \text{ e } \ k \cdot 1_R = 0\} \neq \emptyset$.

Pelo princípio da boa ordem, existe um menor inteiro positivo n, tal que $n \cdot 1_R = 0$ ($n = \min T$). Neste caso, $\varphi : \mathbb{Z} \to A$, definido por $\varphi(k) = k \cdot 1_R$, para todo $k \in \mathbb{Z}$, é um homomorfismo sobrejetor e, pelo Primeiro Teorema do Isomorfismo, temos que $A \cong \mathbb{Z}/\text{Ker }(\varphi)$.

Agora, para mostrarmos que $A \cong \mathbb{Z}_n$, é suficiente mostrarmos que Ker $(\varphi) = n\mathbb{Z}$.

Desde que Ker $(\varphi) = \{k \in \mathbb{Z};\ k \cdot 1_R = 0\}$, temos que $n \in$ Ker (φ). Logo, para todo $s \in \mathbb{Z}$, temos que $n \cdot s \in$ Ker (φ), pois $(n \cdot s) \cdot 1_R = s \cdot (n \cdot 1_R) = s \cdot 0 = 0$, o que mostra que $n\mathbb{Z} \subseteq$ Ker (φ).

Dado $k \in$ Ker (φ), temos que $-k \in$ Ker (φ), assim, podemos supor que existe $k \in$ Ker (φ) com $k > 0$, o que implica que $k \in T$.

Como $n = \min T$, temos que $k \geq n$. Logo, $k = rn + s$, para algum $r, s \in \mathbb{Z}$, com $0 \leq s < n$. Assim, $0 = k \cdot 1_R = (rn+s) \cdot 1_R = (rn) \cdot 1_R + s \cdot 1_R = r \cdot (n \cdot 1_R) + s \cdot 1_R = s \cdot 1_R$, e $0 \leq s < \min T$, o que implica que $s = 0$. Portanto $k = rn \in n\mathbb{Z}$, o que mostra que Ker $(\varphi) \subseteq n\mathbb{Z}$.

Então Ker $(\varphi) = n\mathbb{Z}$ e, neste caso, R contém um subanel $A \cong \mathbb{Z}/\text{Ker }(\varphi) = \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$. ■

Definição 10 Se R é um anel com 1, dizemos que R tem **característica** n ($Car\,(R) = n$), se existe $n \in \mathbb{Z}$, tal que R contém um subanel isomorfo a $\mathbb{Z}_n$. Caso contrário, dizemos que $Car\,(R) = 0$, ou seja, $Car\,(R) = 0$ quando R contém um subanel isomorfo a $\mathbb{Z}$.

Assim temos

$Car\,(R) = n \Leftrightarrow n$ é o menor inteiro positivo tal que $n \cdot 1_R = 0$.

$Car\,(R) = 0 \Leftrightarrow \nexists\ n \in \mathbb{Z} - \{0\}$, tal que $n \cdot 1_R = 0$.

$Car\,(R) = n \Rightarrow n \cdot a = 0$, para todo $a \in R$, pois $n \cdot a = n \cdot (1_R \cdot a) = (n \cdot 1_R) \cdot a = 0 \cdot a = 0$.

Exemplo 38 $Car(\mathbb{Z}) = 0$.

$Car(\mathbb{Z}_n) = n$

$Car(M_2(\mathbb{Z})) = 0$

$Car(\mathbb{Z}_4 \times \mathbb{Z}_8) = 8$

$Car(\mathbb{Z}_4 \times \mathbb{Z}_6) = 12$ (mmc (4,6)=12)

Exemplo 39 Se R é um domínio e $Car(R) \neq 0$, então $Car(R) = p$, para algum número primo p.

De fato, se $Car(R) = n$, com n composto, então $n = n_1 \cdot n_2$ com $1 < n_1, n_2 < n$. Logo, $0 = n \cdot 1_R = (n_1 \cdot n_2) \cdot 1_R = (n_1 \cdot 1_R) \cdot (n_2 \cdot 1_R)$. Como R é domínio, temos $n_1 \cdot 1_R = 0$ ou $n_2 \cdot 1_R = 0$, o que fura a minimalidade de n. Portanto $Car(R) = p$, para algum número p primo.

7 Ideais Primos e Maximais

Teorema 13 *Seja R um anel comutativo com 1. Se I é um ideal próprio de R, isto é, não trivial, então I não contém unidades de R, ou seja, $I \cap R^* = \emptyset$.*

Dem.: Se $I \cap R^* \neq \emptyset$, então para $a \in I \cap R^*$, temos que $1 = a \cdot a^{-1} \in I \Rightarrow R \subseteq I \subseteq R \Rightarrow R = I$. ■

Definição 11 Seja R um anel. Um ideal M de R é dito ser um **ideal maximal** de R se:

(i) $M \neq R$;

(ii) Se I é um ideal de R com $M \subseteq I \subseteq R$, então $I = M$ ou $I = R$.

Exemplo 40 Os ideais $p\mathbb{Z}$, com p primo, são todos os ideais maximais de $\mathbb{Z}$.

De fato, se p é um número primo, então $p\mathbb{Z}$ é maximal, pois

(i) $p\mathbb{Z} \neq \mathbb{Z}$.

(ii) Se I é um ideal de $\mathbb{Z}$ tal que $p\,\mathbb{Z} \subseteq I \subseteq \mathbb{Z}$, então, como I é um ideal de $\mathbb{Z}$, temos que existe $n \in \mathbb{Z}$ tal que $I = n\mathbb{Z}$. Logo, $p\,\mathbb{Z} \subseteq n\mathbb{Z} \Rightarrow p \in n\mathbb{Z} \Rightarrow p = \alpha \cdot n$, para algum $\alpha \in \mathbb{Z}$. Desde que p é primo, temos que $n = 1$ ou $n = p$.

$$\left.\begin{array}{l} \text{Se } \; n = 1 \Rightarrow n\mathbb{Z} = \mathbb{Z} \\ \text{Se } \; n = p \Rightarrow n\mathbb{Z} = p\,\mathbb{Z} \end{array}\right\} I = \mathbb{Z} \;\text{ ou }\; I = p\,\mathbb{Z},$$

o que mostra que $p\,\mathbb{Z}$ é maximal.

Estes são todos os ideais maximais de $\mathbb{Z}$, pois se $n\mathbb{Z}$ é um ideal de $\mathbb{Z}$ e n não é primo, então $n = n_1 \cdot n_2$, com $1 < n_1,\ n_2 < n$ e, neste caso, $n\mathbb{Z} \subsetneq n_1\mathbb{Z} \subsetneq \mathbb{Z}$, o que implica que $n\mathbb{Z}$ não é maximal.

Exemplo 41 Sejam $R = M_2(\mathbb{Z})$ e p um número primo. O ideal $M = M_2(p\,\mathbb{Z})$ é um ideal maximal de R.

De fato, é imediato que $M \neq R$. Seja I um ideal de R com $M \subseteq I \subseteq R$ e $I \neq R$. Vamos mostrar que $I = M$.

Seja $I_{11} = \left\{ a_{11} \in \mathbb{Z};\ \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in I \right\} \subseteq \mathbb{Z}$.

Verifique que I_{11} é um ideal de $\mathbb{Z}$.

Então existe $t \in \mathbb{Z}$, tal que $I_{11} = t\,\mathbb{Z}$. Afirmamos que $t > 1$, pois, se $t = 1$, temos que $1 \in I_{11}$ e, consequentemente existe $x = \begin{pmatrix} 1 & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in I$.

Assim, $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in I.$

Logo, $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \in I$ e $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \in I.$

Consequentemente, $1_R = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \in I \Rightarrow I = R$, o que é uma contradição. Assim, $I_{11} = t\,\mathbb{Z}$, para algum $t > 1$.

Vamos agora mostrar que $I \subseteq M_2(t\mathbb{Z})$.

Se $x \in I$, então $x = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, com $a \in I_{11} = t\,\mathbb{Z}$. Logo $a = t\,a'$, para algum $a' \in \mathbb{Z}$.

Mais ainda,

$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot x = \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} \in I \Rightarrow c = t\,c'$, para algum $c' \in \mathbb{Z}$;

$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} b & 0 \\ d & 0 \end{pmatrix} \in I \Rightarrow b = t\,b'$, para algum $b' \in \mathbb{Z}$;

$\begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} d & 0 \\ 0 & 0 \end{pmatrix} \in I \Rightarrow d = t\,d'$, para algum $d' \in \mathbb{Z}$.

Assim, $x = \begin{pmatrix} ta' & tb' \\ tc' & td' \end{pmatrix} \in M_2(t\,\mathbb{Z})\,.$

Logo, $M_2(p\,\mathbb{Z}) \subseteq I \subseteq M_2(t\mathbb{Z}) \neq R$, o que implica que $p\,\mathbb{Z} \subseteq t\,\mathbb{Z} \neq \mathbb{Z}$. Mas, $p\,\mathbb{Z}$ é maximal, então $\Rightarrow p\,\mathbb{Z} = t\mathbb{Z}$, ou seja $I = M_2(p\,\mathbb{Z})$, e, portanto $M_2(p\,\mathbb{Z})$ é maximal, como queríamos mostrar.

No próximo teorema usaremos resultados sobre ideais que deixaremos como exercício

Exercício 5 Sejam R um anel e I, J ideais de R. Mostre que $I + J = \{a+b \in R;\ a \in I, b \in J\}$ é um ideal de R, ou seja, a soma de ideais é também ideal.

Exercício 6 Sejam R um anel e J um ideal de R. Mostre que os ideais do anel quociente R/J são da forma I/J, com I ideal de R tal que $J \subseteq I$.

Teorema 14 *Sejam R um anel e M um ideal de R. São equivalentes:*

(i) M *é maximal.*

(ii) R/M *não tem ideais (bilaterais) não triviais.*

(iii) Para todo $x \in R - M$, *temos* $(x) + M = R$.

Dem.: *(i)* $\Rightarrow$ *(ii)*. Seja I/M um ideal de R/M. Então I é um ideal de R e $M \subseteq I \subseteq R$. Desde que M é maximal, temos que $I = M$ ou $I = R$. Consequentemente, $I/M = M/M$ ou $I/M = R/M$, ou seja I/M é trivial, o que mostra *(ii)*.

(ii) $\Rightarrow$ *(iii)*. Para todo $x \in R - M$, temos que $I = (x) + M$ é um ideal de R que contém M e é diferente de M. Assim, I/M é um ideal de R/M não nulo, pois $x + M \in I/M$ e $x + M \neq M$. De *(ii)*, temos que $I/M = R/M$, ou seja, $R = I = (x) + M$.

(iii) $\Rightarrow$ *(i)*. Se $M \subseteq I \subseteq R$ e $I \neq M$, então existe $x \in I - M$ e, de *(iii)*, temos que $(x) + M = R$, o que implica que $I = R$. ■

Corolário 6 *Se R é um anel comutativo com 1, então M é um ideal maximal de R se, e somente se, R/M é corpo.*

Dem.: ($\Leftarrow$) Como um corpo não tem ideais não triviais, temos que se R/M é corpo, então de *(ii)* $\Leftrightarrow$ *(i)*, temos que M é maximal.
($\Rightarrow$) Se R é comutativo com 1 e M é um ideal maximal de R, então R/M é um anel comutativo com $1_{R/M} = 1_R + M$.

Agora, dado $a + M \neq M$ em R/M, temos que $a \notin M$ e, de *(i)* $\Leftrightarrow$ *(iii)*, obtemos $(a) + M = R$. Logo, existem $b \in R$ e $m \in M$ tais que $1 = ab + m$. O que implica que $1 + M = (ab + m) + M = (ab + M) + (m + M) = (ab + M) = (a + M) \cdot (b + M)$. Como R/M é comutativo, temos que $(a + M)^{-1} = (b + M) \in R/M$, o que mostra que R/M é corpo. ■

Definição 12 *Um anel R que não admite ideais (bilaterais) não triviais é dito ser um* ***anel simples****.*

Sobre anéis simples temos:

Teorema 15 *Todo anel com divisão é simples.*

Dem.: Imediata. ■

Teorema 16 *Se R é um anel simples, com 1, então $M_n(R)$, com $n \geq 1$, é simples.*

Dem.: Segue imediatamente do teorema seguinte. ■

Teorema 17 *Se R é um anel com 1 e $n \geq 1$, então os ideais de $M_n(R)$ são da forma $M_n(I)$, com I ideal de R.*

Dem.: Sejam e_{ij}, com $i, j = 1, \ldots, n$, as matrizes unitárias elementares, isto é, para cada $i, j = 1, \ldots, n$, e_{ij} é a matriz que possui 1_R na posição ij e zero nas demais posições. Cada elemento de $M_n(R)$ é da forma $(a_{ij}) = \sum_{i,j} a_{ij}\, e_{ij}$, com $a_{ij} \in R$.

Seja A um ideal de $M_n(R)$.

Considere $I = \{a_{11} \in R;\ \sum_{ij}\ a_{ij}\ e_{ij} \in A\}$.

Mostremos primeiramente que I é um ideal de R.

De fato, para todo $a_{11}, b_{11} \in I$ e $r \in R$, existem $x = \sum_{ij}\ a_{ij}\, e_{ij} \in A$ e $y = \sum_{ij}\ b_{ij}\ e_{ij} \in A$.

Então $\sum_{ij}(a_{ij} - b_{ij})e_{ij} \in A$, o que implica que $a_{11} - b_{11} \in I$. Mais ainda, $r \cdot x = \sum_{ij} r(a_{ij}\, e_{ij}) = \sum_{ij}\ r\, a_{ij}\, e_{ij} \in A$, ou seja $r \cdot a_{11} \in I$.

Vamos mostrar agora que $A = M_n(I)$.

(i) $A \subseteq M_n(I)$

Seja $x \in A$, $x = \sum_{ij}\ a_{ij}\, e_{ij}$. Queremos mostrar que $a_{sk} \in I$, para cada $s, k = 1, \ldots, n$.

Observe que $e_{1s} \cdot x \cdot e_{k1} = \sum_{ij}\ a_{ij} \cdot (e_{1s} \cdot e_{ij} \cdot e_{k1}) = \sum_{j}\ a_{sj}\, e_{1j}\, e_{k1} = a_{sk}\, e_{11} \in A$, o que implica que $a_{sk} \in A$. Portanto $A \subseteq M_n(I)$.

(ii) $M_n(I) \subseteq A$

Se $y = \sum_{i,j} b_{ij}\, e_{ij} \in M_n(I)$, então $b_{ij} \in I$, para todo $i, j = 1, \ldots, n$. Assim, para cada $i, j = 1, \ldots, n$, existe uma matriz $\alpha_{ij} = \sum a_{ks}\, e_{ks} \in A$, tal que $a_{11} = b_{ij}$. Então, $e_{i1}\, \alpha_{ij}\, e_{1j} = \sum a_{ks}\, e_{i1}\, e_{ks}\, e_{1j} = a_{11}\, e_{ij} \in A$. Consequentemente,

$b_{ij}\, e_{ij} \in A$ para cada $i, j = 1, \ldots, n$, o que mostra que $y = \sum b_{ij}\, e_{ij} \in A$. Portanto $A = M_n(I)$.

■

Outra classe de ideais, que contém a classe dos ideais maximais de um anel, é a classe dos ideais primos.

Definição 13 Um ideal P de um anel comutativo R é um **ideal primo** de R se:

(i) $P \neq R$;

(ii) Para todo $a, b \in R$, se $ab \in P$, então $a \in P$ ou $b \in P$.

Exemplo 42 Para todo número primo p, os ideais $p\,\mathbb{Z}$, são ideais primos de $\mathbb{Z}$. Desde que $ab \in p\,\mathbb{Z} \Leftrightarrow p/ab$, temos que p/a ou p/b. Assim, $a \in p\,\mathbb{Z}$ ou $b \in p\,\mathbb{Z}$.

Exemplo 43 O ideal (0) é primo em $\mathbb{Z}$.

Pois, $ab \in (0) \Leftrightarrow ab = 0 \Rightarrow a = 0$ ou $b = 0 \Rightarrow a \in (0)$ ou $b \in (0)$.

Exercício 7 Um anel comutativo com 1 é um domínio $\Leftrightarrow (0)$ é um ideal primo.

Teorema 18 *Em um anel comutativo com 1, todo ideal maximal é primo.*

Dem.: Sejam R um anel comutativo com 1 e $M \subseteq R$ um ideal maximal.

Se $a, b \in R$ são tais que $ab \in M$, então $ab + M = M$ em R/M, ou seja $(a+M)(b+M) = M$ em R/M. Desde que R/M é corpo, temos que $(a+M) = M$ ou $(b+M) = M$, o que implica que $a \in M$ ou $b \in M$. Portanto M é primo. ■

($\not\Leftarrow$) pois (0) é primo em $\mathbb{Z}$ e não é maximal. De fato, $\dfrac{\mathbb{Z}}{(0)} \cong \mathbb{Z}$, que não é corpo.

Exemplo 44 É necessária a condição de R ter 1, pois $R = 2\,\mathbb{Z}$ é um anel comutativo sem 1 e $M = 4\,\mathbb{Z}$ é um ideal maximal que não é primo, pois $a = 2 = b \in R$, são tais que $ab \in M$ com $a \notin M$ e $b \notin M$.

Teorema 19 *Sejam R um anel comutativo com 1 e $I \subseteq R$ um ideal. Então I é primo se, e somente se R/I é domínio.*

Dem.: ($\Rightarrow$) Se R é comutativo com 1, então R/I é comutativo com 1.

Desde que I é primo, temos que $I \neq R$ e, consequentemente, $1 + I \neq I$, ou seja, $1 \neq 0$ no anel R/I.

Se $a, b \in R$ são tais que $(a + I) \cdot (b + I) = I$, então $ab + I = I$. Logo, $ab \in I$ e desde que I é primo, temos que $a \in I$ ou $b \in I$. Assim, $a + I = I$ ou $b + I = I$, o que mostra que R/I é um domínio.

($\Leftarrow$) Se R/I é domínio, então R/I tem 1, o que implica que $I \neq R$.

Se $a, b \in R$ são tais que $ab \in I$, então $I = ab + I = (a + I)(b + I)$ em R/I. Como R/I é domínio, temos que $a + I = I$ ou $b + I = I$, o que implica que $a \in I$ ou $b \in I$, ou seja I é um ideal primo de R. ■

8 Exercícios

1. **(a)** Mostre que $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2};\ a,\ b \in \mathbb{Z}\}$ é um subanel de $\mathbb{R}$.
   (b) Se $a + b\sqrt{2}$ é uma unidade com $mdc\,(a, b) = 1$, então $a^2 - 2b^2 = \pm 1$.
   (c) Encontre $(\mathbb{Z}[\sqrt{2}])^*$.

2. **(a)** Mostre que se S_1 e S_2 são subanéis de um anel R, então $S_1 \cap S_2$ é também um subanel de R.
   (a) A união de subanéis é também um subanel? Justifique.

3. Mostre que se F é um corpo e R é um subanel de F com $1_R \neq 0_R$, então R é um domínio e $1_R = 1_F$.

4. Um anel comutativo pode ter uma imagem homomórfica não comutativa?? Justifique.

5. Sejam R um domínio e $\phi : R \to R$ um homomorfismo de anéis. Se $\phi(1) \neq 0$, então $\phi(1) = 1$ e, a imagem de unidade é também unidade.

6. Seja $\phi : R \to S$ um homomorfismo sobrejetor de anéis com $K = Ker(\phi)$. Se S é um anel com divisores de zero, mostre que existem elementos $a, b\ \in R$ tais que $ab \in K$, mas $a \notin K$ e $b \notin K$.

7. Seja $\phi : R \to S$ um homomorfismo sobrejetor de anéis com $K = Ker(\phi)$. Se S é um anel comutativo, mostre que $ab - ba\ \in K$, para todo $a, b\ \in R$.

8. Seja $\phi : R \to S$ um homomorfismo sobrejetor de anéis. Mostre que $\phi(C(R)) \subseteq C(S)$.

9. Sejam R um anel com 1 e $I \subseteq R$ um ideal. Mostre que são equivalentes:
   (a) $I = R$
   (b) $1 \in I$
   (c) I contém alguma unidade de R.

10. Seja $\phi : R \to S$ um homomorfismo de anéis. Mostre que:

    (a) Se I é um ideal de R, então $\phi(I)$ é um ideal de $\phi(R)$.

    (b) É $\phi(I)$ um ideal de S? Justifique.

    (c) Se ϕ é sobrejetor e J é um ideal de S, então $\phi^{-1}(J)$ é um ideal de R que contém $Ker(\phi)$.

11. **(a)** Sejam I, J ideais de um anel R. Mostre que $I \cap J$ é um ideal de R.

    (b) Se Γ é um conjunto não vazio de ideais de um anel R, então $\bigcap_{I \in \Gamma} I$ é também um ideal de R.

    (c) Para qualquer subconjunto S do anel R, a intersecção de todos os ideais de R que contém S é também um ideal de R (chamado o *ideal gerado por* S e denotado por (S). Se $S = \{a\}$, então denotamos $(S) = (a)$ e dizemos *o ideal principal gerado por* a).

12. Mostre que o ideal de $M_2(\mathbb{R})$ gerado por qualquer matriz não nula é o anel todo.

13. Sejam R um anel comutativo com 1, e $a,\ b\ \in R$. Prove que o ideal de R gerado pelo conjunto $\{a, b\}$ é igual ao conjunto $aR + bR = \{ax + by;\ x,\ y \in R\}$.

14. Sejam a, b números inteiros primos entre si. Mostre que $a\mathbb{Z} \cap b\mathbb{Z} = ab\mathbb{Z}$ e $a\mathbb{Z} + b\mathbb{Z} = (1) = \mathbb{Z}$.

15. Use o Teorema Fundamental do Isomorfismo para Anéis, para mostrar que:

    (a) $3\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z}$

    (b) $M_n(\mathbb{Z}/k\mathbb{Z}) \simeq M_n(\mathbb{Z})/M_n(k\mathbb{Z})$, para todo k, n inteiros positivos maiores que 1.

16. No corpo $\mathbb{Z}/7\mathbb{Z}$, encontre o inverso (multiplicativo) de $7\mathbb{Z} - 237$.

17. No anel $M_2(\mathbb{Z})/M_2(7\mathbb{Z})$, determine se o elemento $\begin{pmatrix} 2 & 5 \\ 6 & 8 \end{pmatrix} + M_2(7\mathbb{Z})$ é uma unidade.

18. **(a)** Para $k > 1$ em $\mathbb{Z}$, mostre que o anel $\mathbb{Z}/k\mathbb{Z}$ não tem divisores de zero se, e somente se k é primo.

    (b) Mostre que $M_2(\mathbb{Z})/M_2(k\mathbb{Z})$ tem divisores de zero para cada $k > 1$ em $\mathbb{Z}$.

    (c) É verdade que se R tem divisores de zero, então R/I tem divisores de zero para cada ideal $I \neq R$? Justifique.

19. Seja $I = (x^2 + 1)$ o ideal principal do anel $R = \mathbb{Z}[x]$. Mostre que R/I é isomorfo ao anel dos inteiros de Gauss. É I maximal? Justifique.

20. Para um inteiro $n > 1$, mostre que, se I é um ideal maximal de $M_n(\mathbb{Z})$, então $I = M_n(p\mathbb{Z})$, onde p é um número primo.

21. Sejam $M_1 \neq R$ e $M_2 \neq R$ ideais de um anel R. Se $M_1 \cap M_2$ é maximal, mostre que $M_1 = M_2$.

22. Sejam R um anel comutativo, com 1, e F um corpo. Se $\phi : R \to F$ é um homomorfismo não nulo de anéis com $K = Ker(\phi)$, mostre que K é um ideal primo de R. Este ideal é maximal?

9 Corpo Quociente

O objetivo desta seção é mostrar que todo dominio pode ser imerso em um corpo e, que existe um único menor corpo com esta propriedade.

Teorema 20 *Todo domínio é isomorfo a um subanel de um corpo.*

Para a demonstração deste teorema, à partir de um domínio dado, contruiremos um corpo satisfazendo o requerido. Para tanto consideremos $(D, +, \cdot)$ um domínio e tomemos $S = D \times (D - \{0\}) = \{(a, b);\ a, b \in D \ \text{ e } \ b \neq 0\}$.

Definimos em S a relação $\sim$ por:

$(a, b) \sim (c, d) \Leftrightarrow ad = bc$, para todo $(a, b) \in S$.

Lema 1 *A relação $\sim$ é uma relação de equivalência sobre S.*

Dem.: Devemos mostrar que $\sim$ é reflexiva, simétrica e transitiva.

(i) $\sim$ é reflexiva, pois para todo $(a, b) \in S$, desde que D é comutativo, temos que $ab = ba$ e, assim, $(a, b) \sim (a, b)$.

(ii) $\sim$ é simétrica, pois se $(a, b),\ (c, d) \in S$ são tais que
$(a, b) \sim (c, d) \Rightarrow ad = bc \Rightarrow cb = da \Rightarrow (c, d) \sim (a, b)$.

(iii) $\sim$ é transitiva, pois se (a, b), (c, d) e $(e, f) \in S$ são tais que
$(a, b) \sim (c, d) \ \text{ e } \ (c, d) \sim (e, f) \Rightarrow ad = bc \ \text{ e } \ cf = de \Rightarrow (ad)f = (bc)f$ e $(cf)b = (de)b \Rightarrow (af)d = (be)d$. Como D é domínio e $d \neq 0$, temos que $af = bc \Rightarrow (a, b) \sim (e, f)$.

■

Seja F o conjunto das classes de equivalência dos elementos de S, ou seja $F = \left\{(\overline{a, b});\ (a, b) \in S\right\}$. Usando a notação $\dfrac{a}{b} = (\overline{a, b})$, temos que

$$\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc.$$

Lembremos também que $(\overline{a,b}) = (\overline{c,d}) \Leftrightarrow (a,b) \sim (a,b)$.

Assim, $F = \left\{ \frac{a}{b};\ a \in D,\ b \in D - \{0\} \right\}$ é o nosso candidato a corpo procurado. O nosso próximo passo é definirmos uma estrutura de corpo em F.

Definimos em F, duas operações binarias, $\oplus$ e $\odot$, por:

$$\frac{a}{b} \oplus \frac{c}{d} = \frac{(ad+bc)}{bd},$$

$$\frac{a}{b} \odot \frac{c}{d} = \frac{ac}{bd},$$

para todo $\frac{a}{b}, \frac{c}{d} \in F$.

Lema 2 *As operações $\oplus$ e $\odot$ estão bem definidas.*

Dem.: Mostraremos somente que $\oplus$ está bem definida, ficando a outra parte para o leitor.

Se $\frac{a}{b} = \frac{e}{f}$ e $\frac{c}{d} = \frac{s}{t}$ em F, então $af = be$ e $ct = ds$ em D. Queremos mostrar que

$$\frac{a}{b} \oplus \frac{c}{d} = \frac{e}{f} \oplus \frac{s}{t},$$

ou seja, que $(ft)(ad+bc) = (bd)(et+fs)$ em D.

Usando as propriedades do anel D temos, $(ft)(ad+bc) = (af)td + (ct)bf = (be)td + (ds)bf = bd(et+fs)$, como queríamos. ■

Mostremos agora que, as operações definidas acima dão uma estrutura de corpo em F.

Lema 3 $(F, \oplus, \odot)$ *é um corpo chamado* ***o corpo quociente, ou corpo de frações*** *de D.*

Dem.: Fica como exercício mostrar que as operações $\oplus$ e $\odot$ são associativas, comutativas e distributivas.

Mostremos que:

(i) Existe o elemento neutro para $\oplus$.

De fato, $0_F = \dfrac{0}{1}$, pois para todo $\dfrac{a}{b} \in F$, temos que $\dfrac{a}{b} \oplus \dfrac{0}{1} = \dfrac{a \cdot 1 + b \cdot 0}{b \cdot 1} = \dfrac{a}{b}$.

(ii) Existência do oposto.

Para todo $\dfrac{a}{b} \in F$, temos que $-\left(\dfrac{a}{b}\right) = \dfrac{(-a)}{b}$, pois

$$\frac{a}{b} \oplus \frac{(-a)}{b} = \frac{ab + b(-a)}{b^2} = \frac{0}{b^2} = \frac{0}{1},$$

desde que $0 \cdot 1 = b^2 \cdot 0 = 0$.

(iii) Existência do elemento neutro de $\odot$.

Temos que $1_F = \dfrac{1}{1}$, pois $\dfrac{a}{b} \odot \dfrac{1}{1} = \dfrac{a \cdot 1}{b \cdot 1} = \dfrac{a}{b}$, para todo $\dfrac{a}{b} \in F$.

Observe que $\dfrac{1}{1} = \dfrac{b}{b}$, para todo $b \neq 0$ em D.

(iv) Existência do inverso.

Se $\dfrac{a}{b} \in F - \{0_F\}$, então $\frac{a}{b} \neq \frac{0}{1} \Longrightarrow a \cdot 1 \neq b \cdot 0 = 0 \Longrightarrow a \neq 0$. Assim, $\dfrac{b}{a} \in F$ e $\dfrac{a}{b} \odot \dfrac{b}{a} = \dfrac{ab}{ba} = \dfrac{1}{1}$, ou seja, $\left(\dfrac{a}{b}\right)^{-1} = \dfrac{b}{a}$.

Do descrito acima temos que F é corpo. ■

Agora, mostrar que D é isomorfo a um subanel de F é equivalente a mostrar que existe um homomorfismo injetor de anéis $\varphi : D \to F$.

Teorema 21 *A aplicação $\varphi : D \to F$, definida por $\varphi(a) = \dfrac{a}{1}$, para todo $a \in D$ é um homomorfismo injetor de anéis.*

Dem.: φ é um homomorfimo, pois para todo $a, b \in D$, temos :

$\varphi(a + b) = \dfrac{a + b}{1} = \dfrac{a}{1} \oplus \dfrac{b}{1} = \varphi(a) \oplus \varphi(b)$, e

$\varphi(a \cdot b) = \dfrac{a \cdot b}{1} = \dfrac{a}{1} \odot \dfrac{b}{1} = \varphi(a) \odot \varphi(b)$.

O núcleo de φ é Ker $(\varphi) = \left\{a \in D;\ \varphi(a) = \dfrac{0}{1}\right\} = \left\{a \in D;\ \dfrac{a}{1} = \dfrac{0}{1}\right\} = \{0\}$, o que implica que φ é injetora. ■

Identificando $a \in D$ com $\dfrac{a}{1} \in F$, diremos que D é um subanel de F, e consideraremos que $D \subseteq F$. No próximo resultado mostraremos que F, como construido

acima, é o menor corpo que contém D, donde segue que o corpo quociente de um domínio é único a menos de isomorfismos.

Teorema 22 *Se K é um corpo com $D \subseteq K \subseteq F$, então $K = F$.*

Dem.: Desde que $D = \left\{\frac{a}{1};\ a \in D\right\}$, temos que para todo $b \in D,\ b \neq 0,\ \frac{b}{1} \in K$ e, como K é corpo, obtemos $\frac{1}{b} \in K$. Assim, $\frac{a}{b} = \frac{a}{1} \odot \frac{1}{b} \in K$, para todo $a \in D$ e $b \in D - \{0\}$. Consequentemente $F = K$. ■

Corolário 7 *Se $\varphi : D \to K$ é um homomorfismo injetor de anéis e K é um corpo, então K contém um subcorpo isomorfo a F.*

Dem.: Defina $\varphi^* : F \to K$ por $\varphi^*\left(\frac{a}{b}\right) = \frac{\varphi(a)}{\varphi(b)}$, para todo $\frac{a}{b} \in F$.

Usando que φ é um homomorfismo injetor, é facil mostrar que φ^* é também um homomorfismo injetor. ■

Exercício: Mostre que o corpo de frações de um corpo é o próprio corpo.

10 Teorema Chinês do Resto

Como consequência de um isomorfismo de anés, obteremos o teorema Chinês do resto.

Lembremos que:

Lema 4 *Se* $a, b \in \mathbb{Z}$ *e* $d = \text{mdc}\,(a, b)$ *então existem* $r, s \in \mathbb{Z}$, *tais que* $d = a \cdot r + b \cdot s$.

Usando este resultado mostraremos que:

Lema 5 *Se* $a, b \in \mathbb{Z}$ *são primos entre si, i.é,* $\text{mdc}\,(a, b) = 1$, *então* $\mathbb{Z}_a \times \mathbb{Z}_b \cong \mathbb{Z}_{ab}$.

Dem.: Desde que $\mathbb{Z}_{ab} \cong \dfrac{\mathbb{Z}}{(ab)\mathbb{Z}}$ e $\mathbb{Z}_a \times \mathbb{Z}_b \cong \dfrac{\mathbb{Z}}{a\mathbb{Z}} \times \dfrac{\mathbb{Z}}{b\mathbb{Z}}$, é suficiente mostrarmos que $\dfrac{\mathbb{Z}}{(ab)\mathbb{Z}} \cong \dfrac{\mathbb{Z}}{a\mathbb{Z}} \times \dfrac{\mathbb{Z}}{b\mathbb{Z}}$.

Seja $\varphi : \mathbb{Z} \to \dfrac{\mathbb{Z}}{a\mathbb{Z}} \times \dfrac{\mathbb{Z}}{b\mathbb{Z}}$, definida por $\varphi(x) = (x + a\mathbb{Z},\, x + b\mathbb{Z})$, para todo $x \in \mathbb{Z}$. Claramente temos que φ é um homomorfismo de anéis. Mais ainda, $\text{Ker}\,(\varphi) = \{x \in \mathbb{Z};\ \varphi(x) = 0\} = \{x \in \mathbb{Z};\ \varphi(x) = (a\mathbb{Z},\, b\mathbb{Z})\}$.

Se $x \in \text{Ker}\,(\varphi)$, então $x \in a\mathbb{Z}$ e $x \in b\mathbb{Z}$. Logo, $a \mid x$ e $b \mid x$, o que implica que $\text{mmc}\ (a, b) \mid x$.

Mas, $\text{mmc}\,(a, b) = \dfrac{a \cdot b}{\text{mdc}\,(a, b)} = a \cdot b$. Assim, $x \in ab\,\mathbb{Z}$, ou seja $\text{Ker}\,(\varphi) \subseteq ab\,\mathbb{Z}$. A inclusão contrária é imediata.

Logo, pelo 1º Teorema do isomorfismo para anéis temos $\dfrac{\mathbb{Z}}{ab\,\mathbb{Z}} \cong \text{Im}\,(\varphi) \subseteq \mathbb{Z}_a \times \mathbb{Z}_b$ e $\#(\mathbb{Z}_{ab}) = ab = \#(\mathbb{Z}_a \times \mathbb{Z}_b)$, o que implica que φ é sobrejetora. ■

Teorema 23 *Se* $n \in \mathbb{Z}$, $n > 0$ *e* $n = p_1^{\alpha_1}, \ldots, p_k^{\alpha_k}$, *com* p_i*'s primos distintos, então* $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}}$.

Dem.: Seque diretamente do lema anterior e indução. ■

Observemos que na demonstração do lema anterior, mostramos que φ é sobrejetora sem exibirmos a pré-imagem de um elemento genérico. Assim cabe a seguinte pergunta:

- Se $(c + a\,\mathbb{Z},\, d + b\,\mathbb{Z}) \in \mathbb{Z}_a \times \mathbb{Z}_b$, então qual é o $x \in \mathbb{Z}$ tal que $\varphi(x) = (c + a\mathbb{Z}\,,\, d + b\mathbb{Z})$?

Observe que

$$\begin{cases} x + a\mathbb{Z} = c + a\mathbb{Z} \\ x + b\mathbb{Z} = d + b\mathbb{Z} \end{cases} \Rightarrow \begin{cases} x \equiv c \bmod a \\ x \equiv d \bmod b \end{cases} \Rightarrow \begin{cases} x = c + a \cdot n_1, & n_1 \in \mathbb{Z} \\ x = d + b \cdot n_2, & n_2 \in \mathbb{Z} \end{cases}$$

Por exemplo $\mathbb{Z}_{15} = \mathbb{Z}_3 \times \mathbb{Z}_5$, qual é o elemento $x \in \mathbb{Z}$, tal que $\varphi(x) = (\overline{2}, \overline{4})$?

Temos que

$x \equiv 2 \mod 3$

$x \equiv 4 \mod 5$.

Assim, $x = 2 + 3n_1$, com $n_1 \in \mathbb{Z}$ e $x \equiv 4 \mod 5$.

$$\begin{aligned} \Rightarrow \quad 2 + 3n_1 &\equiv 4 \bmod 5 \\ \Rightarrow \quad 3n_1 &\equiv 2 \bmod 5 \\ \Rightarrow \quad 2 \cdot 3n_1 &\equiv 2 \cdot 2 \bmod 5 \\ \Rightarrow \quad n_1 &= 4 + 5n_2, \text{ para algum } n_2 \in \mathbb{Z}. \end{aligned}$$

Então, $x = 2 + 3(4 + 5n_2) = 14 + 15n_2$, ou seja $x = 14 \bmod 15$.

Corolário 8 (Teorema Chinês dos Restos) *Seja $\{m_i\}_{i=1}^k$ um conjunto de k inteiros primos entre si 2 a 2, ou seja, mdc $(m_i, m_j) = 1$, para todo $i \neq j$. Então o sistema de congruências lineares:*

$$\begin{cases} x \equiv a_1 \ mod\ m_1 \\ \vdots \\ x \equiv a_k \ mod\ m_k \end{cases}$$

onde $a_i \in \mathbb{Z}$, possui uma única solução módulo $n = m_1\, m_2 \cdots m_k$.

Dem.: Basta observar que $\mathbb{Z}_n \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$. ■

Exemplo 45 *Encontrar o menor inteiro $a > 2$ tal que $2 \mid a$, $3 \mid (a+1)$, $4 \mid (a+2)$ e $5 \mid (a+3)$.*

Solução - o problema pode ser equacionado pelo seguinte sistema de congruências lineares:

$$\begin{cases} a \equiv 0 \bmod 2 \\ a \equiv 2 \bmod 3 \\ a \equiv 2 \bmod 4 \\ a \equiv 2 \bmod 5 \end{cases}$$

Da primeira congruência temos que $a = 2t$, com $t \in \mathbb{Z}$. Substituindo na segunda obtemos $2t \equiv 2 \bmod 3$; donde $t = 1+3s$, com $s \in \mathbb{Z}$ e, então $a = 2+6s$. Substituindo na terceira congruência temos $2+6s \equiv 2 \bmod 4$ que é equivalente a $3s \equiv 0 \bmod 2$; e daí $s = 2k$, com $k \in \mathbb{Z}$. Logo $a = 2+12k$ e substituindo na última equação obtemos $2 + 12k \equiv 2 \bmod 5$, o que implica que $12k \equiv 0 \bmod 5$, ou seja $k = 5r$, com $r \in \mathbb{Z}$. Assim $a = 2 + 60r,\ r \in \mathbb{Z}$ e a resposta é $a = 62$.

Exemplo 46 (Problema Chinês do Resto) *Um bando de 17 bandidos Chineses capturaram uma caravana do imperador. Dentre os objetos roubados estava uma quantidade de ovos sólidos de ouro. Ao tentar dividir os ovos em partes iguais eles observaram que sobrariam 3 ovos, os quais eles concordaram que deveriam ser dados ao cozinheiro do bando, Foo Yun. Mas 6 dos bandidos foram mortos em uma batalha e, agora dividindo o total dos ovos de ouro em partes iguais entre os bandidos sobravam 4 ovos que, novamente, de comum acordo eles concordaram que seriam dados para o cozinheiro. No próximo ataque, somente 6 bandidos, os ovos de ouro e o cozinheiro foram salvos. Nesta fase, uma divisão em partes iguais deixava um resto de 5 ovos para o cozinheiro. No jantar da noite seguinte o cozinheiro envenenou a comida e ficou com todos os ovos de ouro. Com quantos ovos Foo Yun ficou?*

Solução - Seja x o número de ovos de ouro roubados. Então temos que $x \equiv 3 \bmod 17$, pois repartindo em 17 bandidos sobraram 3 ovos. Mas morreram 6 bandidos e, na nova divisão sobravam 4 ovos, ou seja, $x \equiv 4 \bmod 11$. Na próxima

fase temos 6 bandidos e uma sobra de 5 ovos, ou seja, temos $x \equiv 5 \bmod 6$. Assim, queremos a solução do sistema de congruências

$$\begin{cases} x \equiv 3 \bmod 17 \\ x \equiv 4 \bmod 11 \\ x \equiv 5 \bmod 6 \end{cases}$$

Da primeira equação temos $x = 3 + 17n_1$, com $n_1 \in \mathbb{Z}$. Substituindo na segunda equação obtemos $3 + 17n_1 \equiv 4 \bmod 11 \Rightarrow 17n_1 \equiv 1 \bmod 11 \Rightarrow 6n_1 \equiv 1 \bmod 11 \Rightarrow 2.6n_1 \equiv 2 \bmod 11 \Rightarrow n_1 = 2 \bmod 11 \Rightarrow n_1 = 2 + 11n_2$, com $n_2 \in \mathbb{Z}$.

Assim, $x = 3 + 17(2 + 11n_2) = 37 + 187n_2$ e, substituindo na terceira equação obtemos

$$\begin{aligned} \Rightarrow \quad 37 + 187n_2 &\equiv 5 \bmod 6 \\ \Rightarrow \quad 1 + n_2 &\equiv 5 \bmod 6 \\ \Rightarrow \quad n_2 &\equiv 4 \bmod 6, \end{aligned}$$

ou seja, $n_2 = 4 + 6k$, com $k \in \mathbb{Z}$. Assim, $x = 37 + 187(4 + 6k) = 785 + 6 \cdot 11 \cdot 17\,k$, ou seja, $x \equiv 785 \bmod 1122$. Consequentemente, o problema tem infinitas soluções.

11 Domínios de Ideais Principais

Definição 14 Sejam R um domínio e $a, b \in R$. Dizemos que a **divide** b, ou que a é um divisor de b, e escrevemos $a \mid b$ se existe $x \in R$ tal que $b = a\,x$. Caso contrário, escrevemos $a \nmid b$ e dizemos que a não é um divisor de b, ou que a não divide b. Dizemos que a e b são **associados** ou que a é associado de b se existe $u \in R^*$, tal que $a = bu$ e neste caso, escrevemos $a \sim b$.

Observe que $u \in R$ é uma unidade se, e somente se $u \mid 1$, ou seja

$$R^* = \{a \in R;\, a \mid 1\} = \{a \in R;\, a \sim 1\}.$$

As primeiras propriedades sobre divisibilidade em domínios são:

Teorema 24 *Seja R um domínio. Então, para todo a, b, $c \in R$ temos:*

(1) $a \sim a$, *ou seja,* $\sim$ *é reflexiva;*

(2) $a \sim b \Rightarrow b \sim a$, *ou seja,* $\sim$ *é simétrica;*

(3) $a \sim b$ *e* $b \sim c \Rightarrow a \sim c$, *ou seja,* $\sim$ *é transitiva;*

(4) $a \mid a$;

(5) $a \mid b$ *e* $b \mid a \Leftrightarrow a \sim b$;

(6) $a \mid b$ *e* $b \mid c \Rightarrow a \mid c$.

Dem.: **(1)** $a \sim a$ pois $a = 1 \cdot a$ e $1 \in R^*$.

(2) Se $a \sim b$, então $a = b \cdot u$, com $u \in R^*$. Logo $b = a \cdot u^{-1}$, com $u^{-1} \in R^*$, ou seja, $b \sim a$.

(3) Se $a \sim b$ e $b \sim c$, então $a = b \cdot u$ e $b = c \cdot t$, com $u, t \in R^*$. Logo $a = c \cdot t \cdot u$, com $t \cdot u \in R^*$, o que implica que $a \sim c$.

(4) Desde que $a = 1 \cdot a$, temos que $a \mid a$.

(5) Se $a \sim b$, então $a = b \cdot u$, com $u \in R^*$ e $b = a \cdot u^{-1}$, com $u^{-1} \in R^*$, o que implica que $a \mid b$ e $b \mid a$.

Reciprocamente, se $a \mid b$ e $b \mid a$, então existem $x, y \in R$ tais que $b = a \cdot x$ e $a = b \cdot y$. Assim, $b = b \cdot y \cdot x$.

Se $b = 0$, então $a = b \cdot y = 0$ e $a \sim b$.

Se $b \neq 0$, como R é um domínio, temos $1 = x \cdot y$, ou seja, $x, y \in R^*$ e $a = b \cdot y$. Logo $a \sim b$.

(6) Se $a \mid b$ e $b \mid c$, então $b = a \cdot x$ e $c = b \cdot y$, com $x, y \in R$. Então $c = a \cdot x \cdot y$, com $x \cdot y \in R$, o que implica que $a \mid c$. ■

Observação: Para todo $a \in R$, temos que $1 \mid a$ e $a \mid 0$. Mais ainda $R^* = \{a \in R;\ a \sim 1\}$ e, para todo $a \in R$, a classe de equivalência $\overline{a} = \{b \in R;\ a \sim b\} = \{u \cdot a;\ u \in R^*\}$. Em particular, em $\mathbb{Z}$, $\overline{n} = \{\pm n\}$ pois $\mathbb{Z}^* = \{\pm 1\}$.

Definição 15 Sejam R um domínio e $a, b \in R$. Dizemos que a é um **divisor próprio** de b se $a \mid b$, com $a \notin R^*$ e $a \not\sim b$, ou seja $b = a \cdot x$, com $a \notin R^*$ e $x \notin R^*$.

Um elemento $q \in R$ é um **elemento irredutível** de R se $q \neq 0$, $q \notin R^*$ e q não tem divisores próprios em R (i.é., se $a \mid q$, então $a \in R^*$ ou $a \sim q$).

Um elemento $p \in R$ é um **elemento primo** de R se $p \neq 0$, $p \notin R^*$ e, se $a, b \in R$ são tais que $p \mid a \cdot b$, então $p \mid a$ ou $p \mid b$.

Proposição 3 *Em $\mathbb{Z}$, os conceitos de elemento irredutível e elemento primo coincidem, ou seja $p \in \mathbb{Z}$, $p \neq 0$ e $p \neq \pm 1$ é irredutível se, e somente se p é primo.*

Dem.: Se p é irredutível e $a, b \in R$ são tais que $p \mid a \cdot b$ e $p \nmid a$, então mdc $(p, a) = 1$. Logo existem $r, s \in \mathbb{Z}$ tais que $p \cdot r + a \cdot s = 1$. Então $b = p \cdot b \cdot r + a \cdot b \cdot s$ e como $p \mid a \cdot b$, temos que $a \cdot b = p \cdot x$ e, consequentemente $b = p \cdot b \cdot r + p \cdot x \cdot s = p \cdot (b \cdot r + x \cdot s)$, o que implica que $p \mid b$, mostrando assim que p é primo.

Reciprocamente, se p é primo e $a \in \mathbb{Z}$ é tal que $a \mid p$, então existe $b \in Z$ tal que $p = a \cdot b$. Logo $p \mid ab$ e como p é primo, temos que $p \mid a$ ou $p \mid b$.

Se $p \mid a$, como $a \mid p$, temos que $a \sim p$.

Se $p \mid b$, então $b = p \cdot x$, com $x \in \mathbb{Z}$. Logo $p = a \cdot x \cdot p$ e, como $p \neq 0$ e $\mathbb{Z}$ é um domínio, temos que $a \cdot x = 1$, ou seja $a \in \mathbb{Z}^*$, mostrando assim que p é irredutível. ■

Observe que na demonstração acima, mostramos que se R é domínio e $p \in R$ é primo, então p é irredutível. Em geral, **não** vale a volta.

Exemplo 47 Seja $R = \{a + b\sqrt{-5};$ tal que $a, b \in \mathbb{Z}\} = \mathbb{Z}[\sqrt{-5}\,]$, com $+$ e $\cdot$ induzidas pelas oporações usuais de $\mathbb{C}$. R é um anel comutativo com 1 e portanto um domínio, pois está contido num corpo. Vamos mostrar que $3 \in R$ é um elemento irredutível e não é primo.

Para tanto definimos $N : R \to \mathbb{N}$ por $N(a+b\sqrt{-5}) = (a+b\sqrt{-5})(a-b\sqrt{-5}) = a^2 + 5b^2$, para todo $a, b \in \mathbb{Z}$. Desde que N é a restrição da norma de um número complexo, temos que $N(x) \cdot N(y) = N(x \cdot y)$, para todo $x, y \in R$.

Mais ainda, $R^* = \{a + b\sqrt{-5};\ a^2 + 5b^2 = 1\}$. De fato, se $x \in R^*$, então existe $y \in R$ tal que $x \cdot y = 1$, o que implica que $N(x) \cdot N(y) = 1 = N(1)$. Logo $N(x) = 1$, mostrando assim que $R^* \subseteq \{x \in R;\ N(x) = 1\}$.

Se $x \in R$ é tal que $N(x) = 1$, então $x \cdot \overline{x} = 1$. Logo $\overline{x} = x^{-1}$. Portanto $R^* = \{x \in R;\ N(x) = 1\}$.

Mostremos que $3 \in R$ é irredutível.

Desde que $N(3) = 9 \neq 1$, temos que $3 \notin R^*$.

Se $3 = x \cdot y$ com $x, y \in R$ e x é um divisor próprio de 3, então $x \notin R^*$ e $x \not\sim 3$.

Se $x \notin R^*$, então $N(x) > 1$ e $9 = N(3) = N(x) \cdot N(y)$, o que implica que $N(x) = 3$ ou $N(x) = 9$.

Se $N(x) = 9$, então $N(y) = 1$ e, consequentemente $x \sim 3$, o que é uma contradição. Mas, $N(x) \neq 3$, pois não existem inteiros a e b com $a^2 + b^2 \cdot 5 = 3$.

Portanto 3 não admite divisor próprio em R, i.é., 3 é irredutível.

Mostremos que $3 \in R$ não é primo. Observe que $9 = 3 \cdot 3 = (2+\sqrt{-5}) \cdot (2-\sqrt{-5})$

e $3 \mid (2+\sqrt{-5}) \cdot (2-\sqrt{-5})$ com $3 \nmid (2+\sqrt{-5})$ e $3 \nmid (2-\sqrt{-5})$. Portanto 3 não é primo.

Definição 16 *Um domínio R é dito ser um* **domínio de ideais principais** *(DIP) se cada ideal de R é principal, isto é, gerado por um único elemento.*

O próximo resultado relaciona divisibilidade com ideais principais.

Lema 6 (Dicionário) *Sejam R um domínio e $a, b \in R$. Então:*

(i) $a \mid b \Leftrightarrow (b) \subseteq (a)$*;*

(ii) $a \sim b \Leftrightarrow (b) = (a)$*;*

(iii) a *é um divisor próprio de* $b \Leftrightarrow (a) \neq R$ *e* $(b) \subsetneq (a)$*;*

(iv) $a \in R^* \Leftrightarrow (a) = R$.

Dem.: **(i)** $a \mid b$ se, e somente se exiate $c \in R$ tal que $b = c \cdot a \Leftrightarrow b \in (a) \Leftrightarrow (b) \subseteq (a)$;

(ii) $a \sim b \Leftrightarrow a \mid b$ e $b \mid a \Leftrightarrow (b) \subseteq (a)$ e $(a) \subseteq (b) \Leftrightarrow (a) = (b)$;

(iii) a é um divisor próprio de $b \Leftrightarrow a \mid b$, $a \notin R^*$ e $a \not\sim b \Leftrightarrow (a) \neq R$ e $(a) \neq (b)$ e $(b) \not\subseteq (a)$;

(iv) $a \in R^* \Leftrightarrow a \sim 1 \Leftrightarrow (a) = (1) = R$. ■

Teorema 25 *Sejam R um DIP e $I \subseteq R$ um ideal não nulo. Então I é maximal se, e somente se $I = (q)$, onde q é um elemento irredutível de R.*

Dem.: Se $I = (q)$, com $q \in R$ irredutível, então $q \neq 0$ e $q \notin R^*$, o que implica que $I \neq (0)$ e $I \neq R$.

Se M é um ideal de R com $I \subseteq M \subseteq R$, então, como R é DIP, temmos que $M = (a)$ para algum $a \in R$. Logo $(q) \subseteq (a) \subseteq (1)$. Do lema do dicionário temos que $a \mid q$ e, como q é irredutível, obtemos $a \in R^*$ ou $a \sim q$. Novamente usando o lema do dicionário temos que $(a) = R$ ou $(a) = (q)$, o que implica que I é maximal.

Reciprocamente, se I é um ideal maximal de R, então $I \neq R$ e, por hipótese $I \neq (0)$. Logo $I = (q)$, com $q \in R$ tal que $q \notin R^*$ e $q \neq 0$.

Se $a \in R$ é tal que $a \mid q$, então, pelo lema do dicionário temos que $(q) \subseteq (a) \subseteq R$. Como (q) é maximal, temos que $(a) = (q)$ ou $(a) = R$. Novamente do lema do dicionário obtemos $a \sim q$ ou $a \in R^*$, o que mostra que q é irredutível. ■

Como consequência temos o seguinte resultado

Corolário 9 *Se R é DIP e $I \neq (0)$ é um ideal de R, então R/I é corpo se, e somente se $I = (q)$ com $q \in R$ irredutível.*

O próximo resultado mostra que em um DIP as noções de elemento irredutível e elemento primo coincidem.

Teorema 26 *Sejam R um DIP e $p \in R$, $p \neq 0$ e $p \notin R^*$. Então p é um elemento irredutível de R se, e somente se p é um elemento primo de R.*

Dem.: Se $p \in R$ é irredutível e $a,\ b \in R$ são tais que $p \mid a \cdot b$, então $a \cdot b \in (p)$ que é um ideal maximal de R. Como todo ideal maximal é primo, temos que $a \in (p)$ ou $b \in (p)$ e, usando o lema do dicionário obtemos $p \mid a$ ou $p \mid b$. Portanto p é um elemento primo de R.

Reciprocamente, se $p = a \cdot b$, com $a,\ b \in R$, então $p \mid a \cdot b$ e, como p é primo, temos que $p \mid a$ ou $p \mid b$. Por outro lado, $a \mid p$ e $b \mid p$. Logo $a \sim p$ ou $b \sim p$, mostrando assim que p é um elemento irredutível de R. ■

Observação: Do último exemplo e do teorema acima temos que $\mathbb{Z}[\sqrt{-5}\,]$ não é um DIP.

Teorema 27 *Seja R um anel comutativo com 1. Então $p \in R$ é um elemento primo de R se, e somente se (p) é um ideal primo não nulo de R.*

Dem.: Se p é um elemento primo de R, então $p \neq 0$ e $p \notin R^*$, o que implica que $(p) \neq (0)$ e $(p) \neq R$.

Se $a, b \in R$ são tais que $a \cdot b \in (p)$, então $p \mid a \cdot b$ e, como p é primo, temos que $p \mid a$ ou $p \mid b$. Do lema do dicionário obtemos $(a) \subseteq (p)$ ou $(b) \subseteq (p)$, ou seja, $a \in (p)$ ou $b \in (p)$, o que mostra que (p) é um ideal primo não nulo de R.

Reciprocamente, se (p) é um ideal primo não nulo de R, então $(p) \neq (0)$ e $(p) \neq R$. Logo $p \neq 0$ e $p \notin R^*$. Se $p \mid a \cdot b$, então $a \cdot b \in (p)$. Como (p) é um ideal primo, temos que $a \in (p)$ ou $b \in (p)$, o que implica que $p \mid a$ ou $p \mid b$. Portanto p é um elemento primo de R. ■

Corolário 10 *Se R é DIP e I é um ideal não nulo de R, então I é um ideal maximal se, e somente se I é um ideal primo.*

Definição 17 *Sejam R um domínio e $a, b \in R$. Então $d \in R$ é* ***um máximo divisor comum*** *de a e b se:*
(i) $d \mid a$ e $d \mid b$;
(ii) *se $c \in R$ é tal que $c \mid a$ e $c \mid b$, então $c \mid d$.*

Proposição 4 *Sejam R um domínio e $a, b \in R$. Se existe um máximo divisor comum de $a, b \in R$, então ele é único a menos de associados.*

Dem.: Se d_1 e d_2 são m.d.c. de a e b em R, então $d_1 \mid a$ e $d_1 \mid b$ e, como d_2 é um m.d.c. de a e b, temos que $d_1 \mid d_2$. Por outro lado, $d_2 \mid a$ e $d_2 \mid b$ e, como d_1 é um m.d.c. de a e b, temos que $d_2 \mid d_1$. Logo $d_1 \sim d_2$.

Agora, se d_1 é um m.d.c. de a e b e $d_2 \sim d_1$, então $d_2 = u \cdot d_1$, com $u \in R^*$. Como $d_1 \mid a$ e $d_1 \mid b$, temos que $(u \cdot d_1) \mid a$ e $(u \cdot d_1 \mid b$. Se $c \in R$ é tal que $c \mid a$ e $c \mid b$, então $c \mid d_1$, o que implica que $c \mid (u \cdot d_1)$, mostrando assim que $u \cdot d_1$ é um m.d.c. de a e b. ■

Escrevemos $d = \text{mdc}\,(a, b)$ para denotar a classe de equivalência representada por um m.d.c., d, de a e b.

O próximo resultado mostra que em um DIP quaisquer dois elementos admitem um m.d.c.

Teorema 28 *Seja R um DIP. Se $a, b \in R - \{0\}$, então a e b admitem um m.d.c., ou seja, existe* $\text{mdc}\,(a, b)$ *e pode ser expresso na forma* $\text{mdc}\,(a, b) = a \cdot r + b \cdot s$, *para algum $r, s \in R$.*

Dem.: Basta mostrar que $I = \{a \cdot x + b \cdot y;\ x, y \in R\}$ é um ideal de R e que se $I = (d)$, então $d = \text{mdc}\,(a, b)$. ■

Corolário 11 *Se* $a, b \in \mathbb{Z}$ *e* d *é o menor inteiro positivo tal que* $d = a \cdot x + b \cdot y$, *então* $d = \text{mdc}\,(a, b)$.

O próximo exemplo mostra que a hipótese de R ser DIP é necessária.

Exemplo 48 Seja $R = 2\,\mathbb{Z}$, que não é um DIP pois R não tem 1. Neste anel não existe $\text{mdc}\,(2, 4)$, pois se existisse $\text{mdc}\,(2, 4)$ então este seria o 2, mas $2 \nmid 2$ em R.

Para finalizar essa seção, daremos um exemplo de um domínio que não é DIP.

Exemplo 49 Sejam $R = \mathbb{Z}[x]$ e

$$I = (2, x) = 2R + xR = \{2 \cdot f(x) + x \cdot g(x);\ f, g \in R\}.$$

Vamos mostrar que I não é um ideal principal.

De fato, se esistir $h \in \mathbb{Z}[x]$ tal que $I = (h(x))$, então desde que $2 \in I$, temos que $2 = h \cdot h_1$, com $h_1 \in R$. Calculando o grau temos $0 = \partial(2) = \partial(h \cdot h_1) = \partial(h) + \partial(h_1)$, o que implica que $\partial(h) = 0$, ou seja $h = c \in \mathbb{Z}$. Mais ainda, $h \mid 2$, o que implica que $h = 1$ ou $h = 2$.

Mas, $x \in I$, ou seja $x = h \cdot h_2$, com $h_2 \in R$. Se $h = 2$, então $x = 2 \cdot h_2$, o que é um absurdo.

Se $h = 1$, então $I = R$ e $1 = 2 \cdot f(x) + x \cdot g(x)$, o que é um absurdo.

Portanto, não existe $h \in R$ tal que $I = (h)$, ou seja $\mathbb{Z}[x]$ não é um DIP.

12 Domínio de Fatoração Única

Definição 18 *Sejam R um domínio $a \in R$, $a \neq 0$, $a \notin R^*$. Duas fatorações $a = p_1\, p_2 \ldots p_r = q_1\, q_2 \ldots q_s$, onde p_i's e os q_i's são elementos irredutíveis de R, são ditas **fatorações equivalentes** de a se $r = s$ e existe σ e S_r tal que para cada $i = 1, \ldots, r$, $p_i \sim q_{\sigma(i)}$.*

$(S_r = \{$permutações de $\{1, 2, \ldots, r\}\})$

Definição 19 *Um domínio R é dito um **domínio de fatoração única** (DFU) se cada $a \in R$, $a \neq 0$, $a \notin R^*$, pode ser representado como um produto de elementos irredutíveis de R e, quaisquer duas tais representações de um mesmo elemento são equivalentes.*

Exemplo 50 Em $\mathbb{Z}[\sqrt{-5}]$, $9 = 3 \cdot 3 = (2 + \sqrt{-5}) \cdot (2 - \sqrt{-5})$ são duas fatorações não equivalentes de 9. Portanto $\mathbb{Z}[\sqrt{-5}]$ não é um DFU.

Proposição 5 *Em um DFU, todo elemento irredutível é primo.*

Dem.: Sejam R um DFU e $q \in R$ um elemento irredutível. Então $q \neq 0$ e $q \notin R^*$.

Se $a, b \in R$ são tais que $q \mid a \cdot b$, escrevendo $a = p_1 \ldots p_r$ e $b = q_1 \ldots q_s$, com p_i e q_j elementos irredutíveis de R, temos que uma fatoração para $a \cdot b$ é $a \cdot b = p_1 \ldots p_r \cdot q_1 \ldots q_s$. Como $q \mid a \cdot b$, temos que $a \cdot b = q \cdot c$, para algum $c \in R$.

Pela unicidade da fatoração de $a \cdot b$, temos que $q \sim p_i$ ou $q \sim q_j$, para algum índice i, j. Agora, $q \mid p_i$ e $p_i \mid a$, implica que $q \mid a$ ou $q \mid q_j$ e $q_j \mid b$, implica que $q \mid b$, o que mostra que q é primo. ■

O próximo passo é mostrarmos que todo DIP é um DFU. Para tanto usaremos dois resultados auxiliares.

Lema 7 *Se R é um DIP e $I_1 \subseteq I_2 \subseteq \ldots \subseteq I_k \subseteq I_{k+1} \subseteq \ldots$ é uma cadeia crescente de ideais de R, então existe $n > 0$ tal que $I_n = I_{n+i}$, para todo $i \geq 0$.*

Dem.: Seja $I = \bigcup_{i=1}^{\infty} I_i$. Verifique que I é um ideal de R. Como R é um DIP, temos que existe $d \in R$ tal que $I = (d)$.

Como $d \in I = \bigcup_{i=1}^{\infty} I_i$, temos que existe $n > 0$ tal que $d \in I_n$. Logo $(d) \subseteq I_n$, o que implica que $I_n \subseteq I = (d) \subseteq I_n$, ou seja $I = I_n$. Assim, para todo $i > 0$, temos $I_n \subseteq I_{n+i} \subseteq I = I_n$, o que mostra que $I_n = I_{n+i}$. ■

Lema 8 *Se R é um DIP e $(a_i)_{i>0}$ é uma sequência de elementos de R tais que $a_{i+1} \mid a_i$ para todo $i > 0$, então existe um inteiro $n > 0$ tal que $a_i \sim a_n$ para todo $i \geq n$.*

Dem.: Seque diretamente do lema anterior e do lema do dicionário. ■

Teorema 29 *Todo DIP é um DFU.*

Dem.: Sejam R um DIP e $a \in R$, $a \neq 0$ e $a \notin R^*$. Queremos mostrar que existe uma fatoração de a comoum produto de elementos irredutíveis de R e que esta fatoração é única à menos de equivalências. Mostraremos separadamente a existência e a unicidade.

Existência: Suponhamos que a não admite uma fatoração como um produto de elementos irredutíveis de R, então, em particular, a não é irredutível. Logo temos uma fatoração $a = a_1 \cdot b_1$, com a_1 e b_1 divisores próprios de a tais que a_1 ou b_1 não admite fatoração. Suponhamos que a_1 não admita fatoração. Então $a_1 = a_2 \cdot b_2$, com a_2 e b_2 divisores próprios de a_1 e a_2 ou b_2 não admite fatoração. Repetindo esse raciocínio, obtemos uma sequência (a_i) de elementos de R, infinita, com a_{i+1} divisor próprio de a_i, o que contradiz o lema anterior. Portanto, a admite uma fatoração.

Unicidade: Se $a = p_1 \dots p_r = q_1 \dots q_s$, com $r \leq s$, p_i e q_j irredutíveis de R, devemos mostrar que estas fatorações são equivalentes. Faremos isso por indução sobre r.

Se $r = 1$, então $a = p_1 = q_1 \dots q_s$. Logo a é irredutível, o que implica que $s = 1 = r$ e $p_1 = q_1$.

Suponhamos que o resultado vale para $r-1$, ou seja, se $p_1 \dots p_{r-1} = q_1 \dots q_t$, então estas fatorações são equivalentes.

Como $a = p_1 \dots p_r = q_1 \dots q_s$, temos que $p_r \mid a = q_1 \dots q_s$. Mas R é um DIP, o que implica que p_r é um elemento primo de R. Consequentemente $p_r \mid q_j$ para algum $j = 1, \dots, s$.

Renomeando, se necessário, podemos supor $j = s$. Assim, $p_r \mid q_s$ e, como q_s irredutível, temos que $p_r \sim q_s$, ou seja, $q_s = u \cdot p_r$, para algum $u \in R^*$. Logo $a = p_1 \dots p_{r-1} \cdot p_r = q_1 \dots q_{s-1} \cdot (u \cdot p_r)$ e, como R é um domínio, temos que $p_1 \dots p_{r-1} = q_1 \dots (u \cdot q_{s-1})$.

Então, por hipótese de indução, $r-1 = s-1$, o que implica que $r = s$ e existe $\sigma \in S_{r-1}$ tal que $p_i \sim q_{\sigma(i)}$, o que mostra a unicidade da fatoração, pois se $p_i \sim u \cdot q_{s-1}$, , como $u \cdot q_{s-1} \sim q_s \Rightarrow p_i \sim q_s$ e $p_r \sim q_s$. ■

Não vale a volta do teorema acima, ou seja nem todo DFU é DIP. Por exemplo, já vimos que $\mathbb{Z}[x]$ não é um DIP, e veremos que é DFU, ou seja veremos que se R é um DFU, então $R[x]$ também o é.

Como consequência imediata deste teorema temos

Corolário 12 (Teorema Fundamental da Aritmética) *Para todo número natural $n > 1$, existem primos positivos distintos $p_1, \dots, p_m$ e números naturais $e_1, \dots, e_m$ tais que*

$$n = p_1^{e_1} \cdots p_m^{e_m}.$$

Dem.: Basta observar que $\mathbb{Z}$ é um DIP, o que implica que é um DFU e $\mathbb{Z}^* = \{\pm 1\}$. ■

Teorema 30 *Se R é um DFU, então quaisquer dois elementos de R admitem um m.d.c.*

Dem.: Sejam $a, b \in R$, não nulos e não unidades. Usando o fato que R é um DFU, podemos encontrar $p_1, p_2, \dots, p_r$ irredutíveis distintos de R e $\alpha_1, \alpha_2, \dots, \alpha_r$, $\beta_1, \beta_2, \dots, \beta_r \in \mathbb{N} \cup \{0\}$ tais que

$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}$

$b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdots p_r^{\beta_r}$.

Agora é fácil verificar que $d = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdots p_r^{\gamma_r}$, onde $\gamma_i = \max\{\alpha_i, \beta_i\}$, é um m.d.c. de a e b. ■

13 Domínios Euclidianos

Nesta seção estudaremos outra classe de anéis contida na classe dos DFU.

Definição 20 Seja R um domínio. Uma função $N : R - \{0\} \to \mathbb{N}$ é dita ser uma **norma euclidiana** se, para todo $a, b \in R$, $b \neq 0$, temos:
(i) se $b \mid a$ e $a \neq 0$ então $N(b) \leq N(a)$;
(ii) existem $q, r \in R$ tais que $a = q \cdot b + r$, com $r = 0$ ou $N(r) < N(b)$.
Se existe uma norma euclidiana N em R, então dizemos que R é um **domínio euclidiano** com respeito a N.

Exemplo 51 O anel dos inteiros $\mathbb{Z}$ é um domínio euclideano com respeito a norma $N : \mathbb{Z} - \{0\} \to \mathbb{N}$, onde $N(a) = |a|$, para todo $a \in \mathbb{Z} - \{0\}$.

Teorema 31 *Todo domínio euclidiano é um DIP.*

Dem.: Sejam R um domínio euclideano com norma euclideana N e I um ideal de R. Queremos mostrar que I é principal.

Se $I = \{0\} = (0)$, então I é principal. Se $I \neq (0)$, consideramos o conjunto $\{N(a);\ a \in I, a \neq 0\} \subseteq \mathbb{N}$. Pelo princípio da boa ordenação, este conjunto tem um mínimo s_0.

Seja $a_0 \in I$ tal que $N(a_0) = s_0$. Então $a_0 \neq 0$ e $(a_0) \subseteq I$.

Se $a \in I$, desde que $a_0 \neq 0$ e R é um domínio euclideano, temos que existem q, $r \in R$ tais que $a = q \cdot a_0 + r$, com $r = 0$ ou $N(r) < N(a_0)$. Logo $r = a - q \cdot a_0 \in I$. Então, pela minimalidade de a_0, temos que $r = 0$, ou seja, $a = q \cdot a_0 \in (a_0)$. Mostramos assim que $I \subseteq (a_0)$, e consequentemente $I = (a_0)$. Portanto R é um DIP. ■

Desde que todo DIP é um DFU, temos:

Corolário 13 *Todo domínio euclideano é um DFU.*

No próximo teorema apresentamos um exemplo importante de domínio euclideano.

Teorema 32 *O anel dos inteiros de Gauss, $\mathbb{Z}[i]$ é um domínio euclideano.*

Dem.: Desde que $\mathbb{Z}[i] \subseteq \mathbb{C}$ e $\mathbb{C}$ é corpo, temos que $\mathbb{Z}[i]$ é um domínio. Vamos mostrar que a norma induzida pela norma dos números complexos é uma norma euclideana, ou seja, $N : \mathbb{Z}[i] \to \mathbb{N}$, definida por $N(a+bi) = a^2 + b^2$, para todo $a, b \in \mathbb{Z}$, é uma norma euclideana.

(i) Se $x, y \in R = \mathbb{Z}[i]$ e $x \mid y$, então $y = x \cdot z$ para algum $z \in R$ e $N(y) = N(x) \cdot N(z)$, o que implica que $N(x) \leq N(y)$.

(ii) Dados $x, y \in R$ com $x \neq 0$, temos que mostrar que existem q, $r \in \mathbb{Z}[i]$ tais que $y = q \cdot x + r$, com $r = 0$ ou $N(r) < N(x)$.

Como $x \neq 0$, temos que $x^{-1} \in \mathbb{C}$ e $y \cdot x^{-1} = \alpha + \beta i$, com $\alpha, \beta \in Q$. Então existem $\alpha_0, \beta_0 \in \mathbb{Z}$ tais que $|\alpha - \alpha_0| \leq \dfrac{1}{2}$ e $|\beta - \beta_0| \leq \dfrac{1}{2}$.

Assim,

$$\begin{aligned} y &= (\alpha + \beta i) \cdot x = [(\alpha - \alpha_0) + (\beta - \beta_0)i + \alpha_0 + \beta_0\, i] \cdot x = \\ &= (\alpha_0 + \beta_0\, i) \cdot x + [(\alpha - \alpha_0) + (\beta - \beta_0)i] \cdot x, \end{aligned}$$

com $q = (\alpha_0 + \beta_0\, i) \in \mathbb{Z}[i]$ e $r = [(\alpha - \alpha_0) + (\beta - \beta_0)i] \cdot x = y - q \cdot x \in \mathbb{Z}[i]$ tal que

$$\begin{aligned} N(r) &= N[(\alpha - \alpha_0) + (\beta - \beta_0)i] \cdot N(x) = \\ &= [(\alpha - \alpha_0)^2 + (\beta - \beta_0)^2] \cdot N(x) = \\ &= (|\alpha - \alpha_0|^2 + |\beta - \beta_0|^2) \cdot N(x) \leq \\ &\leq \left(\frac{1}{4} + \frac{1}{4}\right) \cdot N(x) < N(x). \end{aligned}$$

Portanto, $\mathbb{Z}[i]$ é um domínio euclideano. ■

Exemplo 52 O anel $R = \mathbb{Z}\left[\sqrt{-5}\right]$ não é um domínio euclideano com a norma induzida pela norma dos números complexos $N(a + b\sqrt{-5}) = a^2 + 5b^2$, para todo $a, b \in \mathbb{Z}$, pois já vimos que R não é um DFU. Isso implica que nao vale o algoritmo de Euclides para elementos de R.

14 Exercícios

1. Mostre que se D e D' são domínios isomorfos, então seus corpos de frações também são isomorfos.

2. Mostre que se R é um anel com divisores de zero, então R não pode ser imerso em um corpo, ou seja não existe um homomorfismo de anéis injetor de R em um corpo.

3. Seja $R^* = \mathbb{N} \times \mathbb{N} = \{(a, b);\ a,\ b \in \mathbb{N}\}$. Defina em R^* uma relação $\sim$ por

$$(a, b) \sim (c, d) \Leftrightarrow a + d = b + d$$

(a) Mostre que $\sim$ é uma relação de equivalência em R^*.

(b) Seja $a - b$ a classe de equivalência de (a, b) e R o conjunto das classes de equivalência. Defina $\oplus$ e $\odot$ em R por

$(a - b) \oplus (c - d) = (a + c) - (b + d)$

$(a - b) \odot (c - d) = (ac + bd) - (ad + bc)$

Mostre que $\oplus$ e $\odot$ estão bem definidas.

(c) Mostre que $(R, \oplus, \odot)$ é um anel comutativo com 1.

(d) Mostre $(R, \oplus, \odot)$ é um domínio.

(e) Se $a > b$, então $a = b + h$ para algum $h > 0$ e $(a, b) = (b + h, b)$. Se $a < b$, então $b = a + h$ para algum $h > 0$ e $(a, b) = (a, a + h)$. Mostre que a função $\phi : \mathbb{Z} \to R$, definido por

$$\phi(h) = \begin{cases} (1 + h, 1) & \text{se } h \geq 0 \\ (1, 1 - h) & \text{se } h < 0 \end{cases}$$

é um isomorfismo de anéis.

4. Qual é o corpo quociente de um corpo???

5. Qual é o corpo quociente de $\mathbb{Z}[\sqrt{2}]$?? e de $\mathbb{Z}[i]$, o anel dos inteiros de Gauss??? Justifique sua resposta.

6. Mostre que se $\text{mdc}\,(a,b) = 1$ e $as + bt = 1$, então a congruência linear $ax \equiv c \bmod b$ é equivalente à $x \equiv sc \bmod b$.

7. Resolva, se possível as seguintes congruências. Quando não for possível resolver, justifique porque.

(**a**) $\begin{cases} x \equiv 1 \bmod 7 \\ x \equiv 3 \bmod 5 \\ x \equiv 2 \bmod 8 \end{cases}$ (**b**) $\begin{cases} x \equiv 1 \bmod 2 \\ x \equiv 3 \bmod 4 \\ x \equiv 9 \bmod 11 \end{cases}$

(**c**) $\begin{cases} 3x \equiv 1 \bmod 5 \\ 2x \equiv 3 \bmod 7 \\ x \equiv 3 \bmod 4 \end{cases}$ (**d**) $\begin{cases} 2x \equiv 3 \bmod 4 \\ x \equiv 3 \bmod 5 \\ x \equiv 5 \bmod 7 \end{cases}$

8. Ache o menor inteiro $a > 2$ tal que $2 \mid a;\ 3 \mid (a+1),\ 4 \mid (a+2)$ e $5 \mid (a+3)$.

9. Em um domínio R qualquer, mostre que $\text{mdc}\,(a,b) = \text{mdc}\,(-a,-b)$.

10. Seja $R = \{a + b\sqrt{-5};\ a, b \in \mathbb{Z}\}$.

(a) Mostre que R é um domínio.

(b) Defina $N : R \to \mathbb{Z}$ por $N(a + b\sqrt{-5}) = a^2 + 5b^2$, para todo $a, b \in \mathbb{Z}$. Mostre que $N(x \cdot y) = N(x) \cdot N(y)$, para todo $x, y \in R$.

(c) Mostre que $x \in R^*$ se, e somente se $N(x) = 1$.

(d) Encontre R^*.

(e) Mostre que $3,\ 2 + \sqrt{-5},\ 2 - \sqrt{-5},\ 2,\ 1 + \sqrt{-5},\ 1 - \sqrt{-5}$ são elementos irredutíveis de R.

(f) Quais os elementos do item anterior são primos???

(g) Quais são associados???

(h) Voce tem idéia de como é a norma de um elemento irredutível??? e de um primo??? Existe alguma equivalência análoga ao item (c)????

(i) R é um DIP????

11. Seja R um domínio. Para $a,\ b,\ c \in R$, responda juntificando sua resposta.

    (a) Se a divide b e a divide c, entao a divide $b+c$??

    (b) Se a divide $b+c$, então a divide b e a divide c??

    (c) Se a e b são unidades, então eles são associados??

    (d) Se a divide bc, a divide b e a divide c, então a não é irredutível ??

12. Encontre todos os associados de $2+3i$ em $\mathbb{Z}[i]$, e em $\mathbb{C}$.

13. Mostre que $a+bi$ é um elemento primo em $\mathbb{Z}[i]$ se, e somente se $a-bi$ é primo em $\mathbb{Z}[i]$.

14. Sejam R um domínio e $a \in R$. Mostre que a é irredutível (resp. primo) se, e somente se cada associado de a é irredutível (resp. primo).

15. Mostre que o número 2 é respectivamente irredutível, redutível e inversível em $\mathbb{Z}$, $\mathbb{Z}[i]$ e $\mathbb{C}$.

16. Em cada caso, determine se os elementos $a,\ b$, do domínio R, são associados.

    (a) $a=3,\ \ b=7,\ \ R=\mathbb{Q}$.

    (b) $a=2x-2,\ \ b=-3x+3,\ \ R=\mathbb{Q}[x]$.

    (c) $a=2x-3,\ \ b=-4x+6,\ \ R=\mathbb{Z}[x]$.

    (d) $a=\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix},\ \ b=\begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix},\ \ R=M_2(\mathbb{Q})$.

    (e) $a=\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix},\ \ b=\begin{pmatrix} 1 & 2 \\ 3 & 0 \end{pmatrix},\ \ R=M_2(\mathbb{Z})$.

    (f) $a=\begin{pmatrix} 4 & 3 \\ 2 & 6 \end{pmatrix},\ \ b=\begin{pmatrix} 13 & 16 \\ 4 & 12 \end{pmatrix},\ \ R=M_2(\mathbb{Z}_5)$.

17. Seja $I=\{(2m,3n);\ m,n \in \mathbb{Z}\}$. I é um ideal principal de $\mathbb{Z}\times\mathbb{Z}$???

18. Prove que todo corpo é um DIP.

19. Mostre que em $\mathbb{Z}_n$ cada ideal é principal, para todo $n \geq 1$.

20. É a imagem homomórfica de um DIP um DIP???

21. Seja $R = \mathbb{Z}[i]$ o anel dos inteiros de Gauss.

    (a) Mostre que $a + bi \in R$ é irredutível se $a^2 + b^2$ é um número primo de $\mathbb{Z}$.

    (b) Vale a volta do item **(a)**??

    (c) Se $z = a + bi$ é primo em R, mostre que existe um número inteiro primo p tal que $p = zz'$, para algum $z' \in R$.

    (d) Mostre que 2 não é irredutível em R, mas 3 é.

    (e) Encontre todos os associados de 3 em R.

    (f) Encontre o máximo divisor comum de $3 - 5i$ e $4 + 6i$ em R.

22. Mostre que $1 + 2\sqrt{2}$ e $\sqrt{2}$ são irredutíveis em $\mathbb{Z}[\sqrt{2}]$.

23. Mostre que se R é um DFU, então a intersecção de dois ideais principais de R é ainda um ideal principal.

24. Mostre que o ideal $(3) \cap (2 + \sqrt{-5})$ não é um ideal principal do anel $\mathbb{Z}[\sqrt{-5}]$.

25. Mostre que $\mathbb{Z}_n$ é um DFU. Quem são os elementos primos de $\mathbb{Z}_5$, $\mathbb{Z}_9$ e $\mathbb{Z}_{12}$??

26. Mostre que $\mathbb{Z}[\sqrt{-6}]$ não é DFU.

27. Seja I um ideal não nulo de $\mathbb{Z}[i]$. Mostre que $\mathbb{Z}[i]/I$ é um anel finito.

28. Mostre que $\mathbb{Z}[\sqrt{-2}]$ é um domínio euclideano com respeito a norma $N(a + b\sqrt{-2}) = a^2 + 2b^2$, para todo $a, b \in \mathbb{Z}$.

15 Anéis de Polinômios

Seja R um anel comutativo. Escrevemos $(a_i)_{i\geq 0}$ para indicar uma sequência infinita de elementos de R, ou seja $(a_i)_{i\geq 0} = (a_0, a_i, a_2, \ldots)$ com $a_i \in R$.

Seja $R[x]$ o conjunto de todas as sequências $(a_i)_{i\geq 0}$ tais que $a_i = 0$ quase sempre, isto é, $a_i = 0$ à menos de um número finito de índices. Daí

$R[x] = \{\, (a_i)_{i\geq 0};\ a_i \in R \ \text{ e } \ a_i = 0 \ \text{ quase sempre} \,\}$.

Toda sequência $(a_i)_{i\geq 0}$ pode ser vista como uma função $f : \mathbb{N} \to R$, onde $f(i) = a_i$, para todo $i \in \mathbb{N}$. Da igualdade de funções, temos que $(a_i)_{i\geq 0} = (b_i)_{i\geq 0}$ se, e somente se $a_i = b_i$, para todo $i = 0, 1, \ldots$.

Em $R[x]$ definimos duas operações $+$ e $\cdot$ por:

$(a_i)_{i\geq 0} + (b_i)_{i\geq 0} = (a_i + b_i)_{i\geq 0}$

$(a_i)_{i\geq 0} \cdot (b_i)_{i\geq 0} = (c_i)_{i\geq 0}$, onde, para cada $i \geq 0$, $c_i = \displaystyle\sum_{\substack{r+s=i \\ r,s\geq 0}} a_r \cdot b_s$.

Proposição 6 *$(R[x],\ +,\ \cdot)$ é um anel comutativo, onde $-(a_i)_{i\geq 0} = (-a_i)_{i\geq 0}$, chamado o* **anel de polinômios** *em uma variável com coeficientes no anel R.*

Dem.: Exercício. ■

- Como identificar $R[x]$ com $\{a_0 + a_1 x + \cdots + a_n x^n,\ n \geq 0,\ a_i \in R\}$?

A função $\varphi : R \to R[x]$, definida por $\varphi(a) = (a, 0, 0, \ldots)$, para todo $a \in R$, é um homomorfismo injetor de anéis. De fato, para todo $a, b \in R$, temos:

$\varphi(a + b) = \varphi(a) + \varphi(b)$, pois $(a + b, 0, 0, \ldots) = (a, 0, 0, \ldots) + (b, 0, 0, \ldots)$.

$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$, pois $(a \cdot b, 0, 0, \ldots) = (a, 0, 0, \ldots) \cdot (b, 0, 0, \ldots) = (c_0, c_1, \ldots)$, onde $c_0 = a \cdot b$, $c_1 = a \cdot 0 + 0 \cdot b = 0$ e $c_i = 0$, para todo $i \geq 1$ pois $c_i = \displaystyle\sum_{r+s=i} a_r \cdot b_s$ e, $r + s \geq 1$ implica que $r \geq 1$ ou $s \geq 1$, ou seja $a_r = 0$ ou $b_s = 0$. Portanto $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.

Logo, podemos identificar os elementos $a \in R$ com as sequências $(a, 0, 0, \ldots)$ de $R[x]$, e com isso podemos assumir que $R \subseteq R[x]$.

Observe que

$$(0, a_1, 0, \ldots) \cdot (0, b_1, 0, \ldots) = (0, 0, a_1 \cdot b_1, 0, \ldots), \quad \text{para todo } \ a_1,\, b_1 \in R$$

$$(0, a_1, 0, \ldots) \cdot (0, 0, b_2, 0, \ldots) = (0, 0, 0, a_1 \cdot b_2, 0, \ldots), \quad \text{para todo } \ a_1,\, b_2 \in R$$

$$\vdots$$

$$(0, \ldots, 0, a_i, 0, \ldots) \cdot (0, \ldots, 0, b_j, 0, \ldots) = (0, \ldots, 0, a_i \cdot b_j, 0, \ldots), \text{ para todo } \ a_i,\, b_j \in R$$

Assim, com as identificações

$$(a_0, 0, \ldots) \longleftrightarrow a_0 = a_0 x^0$$

$$(0, a_1, 0, \ldots) \longleftrightarrow a_1 x$$

$$\vdots$$

$$(0, \ldots, 0, a_i, 0, \ldots) \longleftrightarrow a_i x^i$$

obtemos para $(a_i)_{i\geq 0} \in R[x]$ que

$$(a_i)_{i\geq 0} = (a_0, 0, \ldots) + (0, a_1, 0, \ldots) + \cdots (0, \ldots, 0, a_i, 0, \ldots) = \sum_{i=0}^{\infty} (0, \ldots, 0, a_i, 0, \ldots) = \sum_{i=0}^{\infty} a_i x^i.$$

Como $a_i = 0$ quase sempre, temos que existe $n \geq 0$, tal que $a_i = 0$, para todo $i > n$. Assim $(a_i)_{i\geq 0} = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + \ldots + a_n x^n$, obtendo a identificação de $R[x]$ com $\{a_0 + a_1 x + \cdots + a_n x^n,\ n \geq 0,\ a_i \in R\}$, como queríamos.

Note que $x \in R[x]$ se, e somente se $1 \in R$ e, neste caso, temos a identificação $x = (0, 1, 0, \ldots)$, pois

$$\begin{aligned}
\underbrace{(0, a_1, 0, \ldots)}_{a_1 x} &= \underbrace{(a_1, 0, \ldots)}_{a_1} \cdot \underbrace{(0, 1, 0, \ldots)}_{x} \\
\underbrace{(0, 0, a_2, 0, \ldots)}_{a_2 x^2} &= \underbrace{(a_2, 0, \ldots)}_{a_2} \cdot \underbrace{(0, 1, 0, \ldots)}_{x} \cdot \underbrace{(0, 1, 0, \ldots)}_{x} \\
&\vdots \\
\underbrace{(0, \ldots, 0, a_i, 0, \ldots)}_{a_i x^i} &= \underbrace{(a_i, 0, \ldots)}_{a_i} \cdot \underbrace{(0, \ldots, 0, 1, 0, \ldots)}_{x^i}
\end{aligned}$$

Com as identificações acima, temos que

$$R[x] = \{a_0 + a_1x + \ldots + a_nx^n;\ a_i \in R,\ n \geq 0\},$$

com as operações $+$ e $\cdot$ definidas por:

$(a_0+a_1x+\cdots+a_nx^n)+(b_0+b_1x+\cdots+b_mx^m) = (a_0+b_0)+(a_1+b_1)x+\cdots+(a_m+b_m)x^m$

se $n \leq m$ e $(a_0 + \cdots + a_nx^n) \cdot (b_0 + \cdots + b_mx^m) = \sum_{i=0}^{m+n} c_ix^i$, com $c_i = \sum_{r+s=i} a_r \cdot b_s$.

Definição 21 *Sejam R um anel comutativo e $R[x]$ o anel de polinômios com coeficientes em R. Se $f \in R[x]$, $f \neq 0$, $f = a_0 + a_1x + \cdots + a_nx^n$, com $a_n \neq 0$, então o **grau** de f é definido por $\partial(f) = n$ e a_n é dito ser o **coeficiente dominante** de f.*

Teorema 33 *Se $f, g \in R[x]$ são não nulos, então $\partial(f + g) \leq \max\{\partial(f), \partial(g)\}$ e $\partial(f \cdot g) \leq \partial(f) + \partial(g)$. Se R é domínio, então $\partial(f \cdot g) = \partial(f) + \partial(g)$.*

Dem.: Se $f = a_0 + a_1x + \cdots + a_nx^n$, com $a_n \neq 0$, e $g = b_0 + b_1x + \cdots + b_mx^m$, com $b_m \neq 0$ e $n \leq m$, temos

$f + g = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n + b_{n+1}x^{n+1} + \cdots + b_mx^m$,

o que implica que $\partial(f + g) \leq m = \max\{n, m\}$ e

$f \cdot g = c_0 + c_1x + \cdots + c_{n+m}x^{n+m}$, onde $c_{n+m} = \sum_{r+s=n+m} a_r \cdot b_s = a_n \cdot b_m$, ou seja, $\partial(f \cdot g) \leq n + m$.

Se R é um domínio, como $a_n \neq 0$ e $b_m \neq 0$, temos que $c_{n+m} = a_n \cdot b_m \neq 0$, o que mostra que $\partial(f \cdot g) = n + m = \partial(f) + \partial(g)$. ■

Em particular, da demonstração do teorema acima temos que se $f \neq 0$ e $g \neq 0$, então $f \cdot g \neq 0$. Temos então

Corolário 14 *Se R é um domínio, então $R[x]$ também é um domínio.*

- Se R é corpo, então $R[x]$ também é corpo?

Não, pois se $f \in R[x]^*$, então existe $g \in R[x]$ tal que $f \cdot g = 1$. Logo $0 = \partial(1) = \partial(f \cdot g) = \partial(f) + \partial(g) = 0$, o que implica que $f, g \in R$. Como $f \cdot g = 1$, temos

que $f \in R^*$, o que mostra que $R[x]^* \subseteq R^*$. A outra inclusão é imediata, portanto $R[x]^* = R^* \neq R[x] - \{0\}$.

Teorema 34 *Sejam R um domínio; f e $g \in R[x]$ polinômios não nulos com $\partial(f) = m$ e $\partial(g) = n$. Sejam $k = \max\{m - n + 1, 0\}$ e $b = b_n \neq 0$ o coeficiente dominante de g. Então existem únicos polinômios q, $r \in R[x]$ tais que*

$$b^k \cdot f(x) = q(x) \cdot g(x) + r(x),$$

onde $r(x) = 0$ ou $\partial(r) < \partial(g) = n$.

Dem.: Mostraremos separadamente a existência e a unicidade.

Existência - Se $m < n$, basta tomar $q(x) = 0$ e $r(x) = f(x)$. Logo, podemos assumir que $m \geq n$.

Por indução sobre m assumiremos que o resultado vale para todo polinômio de grau menor do que m e mostraremos que vale para f.

Seja $a = a_m \neq 0$ o coeficiente dominante de f. Então $a \cdot X^{m-n} \cdot g(x)$ é um polinômio de grau m com coeficiente dominante $a \cdot b$. Logo $b \cdot f(x) - a \cdot X^{m-n} \cdot g(x) = f_1(x)$ é um polinômio de grau $< m$.

Por hipótese de indução, existem q_1, $r_1 \in R[x]$ tais que

$b^{k'} \cdot f_1(x) = q_1 \cdot g(x) + r_1(x)$, com $r_1 = 0$ ou $\partial(r_1) < n = \partial(g)$, onde $k' = \max\{(m-1) - n + 1, 0\} = \max\{m - n, 0\}$.

Assim, $b^{k'} \cdot (b \cdot f(x)) = (b^{m-n} \cdot a \cdot X^{m-n} + q_1(x)) \cdot g(x) + r_1(x)$, ou seja

$b^k \cdot f(x) = q(x) \cdot g(x) + r(x)$, onde $b^k = b^{k'} \cdot b$.

Unicidade - Se $b^k \cdot f = q \cdot g + r = q_1 \cdot g + r_1$, com $r = 0$ ou $\partial(r) < n$ e $r_1 = 0$ ou $\partial(r_1) < n$, então, temos $(q - q_1) \cdot g = r_1 - r$.

Se $q_1 \neq q$, então $\partial[(q_1 - q) \cdot g] = \partial(q_1 - q) + \partial(g) \geq n$ e $\partial(r_1 - r) \leq \max\{\partial(r), \partial(r_1)\} < n$, o que é uma contradição. Assim, $q_1 = q$ e $r_1 = r$. ■

Corolário 15 *Se F é um corpo, então $F[x]$ é um domínio euclideano com respeito à norma euclidiana*

$$\begin{array}{rcl} \partial : F[x] - \{0\} & \to & \mathbb{N} \\ f & \mapsto & \partial(f) \end{array}$$

Dem.: Segue imediatamente do teorema anterior e de propriedades da função grau. ■

Exemplo 53 Sabemos que $\mathbb{Z}[x]$ não é um domínio euclideano, pois não é um DIP. Logo a função grau não satisfaz o item (ii) da definição de norma euclideana. Por exemplo os elementos $f = x^2 + x$, $g(x) = 2x$ de $\mathbb{Z}[x]$ são tais que não existem $q, r \in \mathbb{Z}[x]$, com $f = q \cdot g + r$ e $r = 0$ ou $\partial(r) = 0$.

Corolário 16 *Se F é um corpo, então $F[x]$ é um DIP (o que implica que é também um DFU) e, cada ideal I de $F[x]$ é gerado por um polinômio de grau mínimo em I.*

Definição 22 *Sejam R um anel comutativo, $f = a_0 + a_1x + \cdots + a_nx^n \in R[x]$ e $d \in R$. Escrevemos $f(d) = a_0 + a_1d + \cdots + a_nd^n \in R$, que é o* ***valor do polinômio*** *f no elemento $d \in R$, ou seja, cada polinômio $f \in R$, define uma função polinomial $f : R \to R$ por $a \mapsto f(a)$.*

Dizemos que $a \in R$ é uma **raiz** *de f se $f(a) = 0$. Um polinômio $f \in R[x]$ é dito ser* **irredutível sobre** *R se f é um elemento irredutível do anel $R[x]$, ou seja, se $f(x) = r(x) \cdot s(x)$ em $R[x]$ implicar qye $r \in R^*$ ou $s \in R^* = R[x]^*$. Se $f(x) = r(x) \cdot s(x)$ com $r(x)$ e $(s(x)$ não unidades, então f é dito ser um polinômio* **redutível sobre** *R e $r(x)$ e $s(x)$ são* **fatores** *de f.*

Exemplo 54 O polinômio $2x^2 + 2 = 2(x^2 + 1)$ é redutível sobre $\mathbb{Z}$, irredutível sobre $\mathbb{Q}$, irredutível sobre $\mathbb{R}$ e redutível sobre $\mathbb{C}$.

Teorema 35 (Teorema do Resto) *Se R é um domínio e $f(x) \in R[x]$, então o resto da divisão de $f(x)$ por $g(x) = x - a$, para cada $a \in R$ é $f(a)$.*

Dem.: Dado $a \in R$, temos que $x - a$ é um polinômio não nulo de $r[x]$ e dividindo f por $(x - a)$ obtemos que existem $q, r \in R[x]$ tais que $f(x) = q(x) \cdot (x - a) + r(x)$ com $r(x) = 0$ ou $\partial(r) < 1$, o que implica que $r(x)$ é constante. Mas $f(a) = q(a) \cdot (a - a) + r$, ou seja, $r = f(a)$. ■

Teorema 36 (Teorema do Fator) *Sejam R um domínio e $f(x) \in R[x]$. Dado $a \in R$, temos que a é uma raiz de $f(x)$ se, e somente se $(x-a)$ é um fator de $f(x)$.*

Dem.: Dividindo $f(x)$ por $(x-a)$, do teorema do resto, temos que existe $q \in R[x]$ tal que $f(x) = q(x) \cdot (x-a) + f(a)$. Assim, a é uma raiz de f se, e somente se $f(a) = 0$ e, isso ocorre se, e somente se $(x-a) \mid f(x)$. ■

Definição 23 *Dizemos que $a \in R$ é uma* **raiz de multiplicidade** $m \geq 1$ *de $f(x) \in R[x]$ se $(x-a)^m \mid f(x)$ e $(x-a)^{m+1} \nmid f(x)$.*

O análogo ao Teorema Fundamental da Álgebra para anéis é:

Teorema 37 *Se R é um domínio e $f(x) \in R[x]$ tem grau n, então f tem no máximo n raízes distintas em R.*

Dem.: Se $n = 0$, então f é constante e não tem raiz.

Se $n = 1$, então $f(x) = a \cdot x + b$, com $a, b \in R$ e $a \neq 0$. Se $x_1, x_2 \in R$ são raízes de f, então $a \cdot x_1 + b = a \cdot x_2 + b = 0$, o que implica que $a \cdot x_1 = a \cdot x_2$ e, como R é um domínio, obtemos que $x_1 = x_2$, mostrando que f tem no máximo uma raiz em R.

Suponhamos que o resultado vale para todo polinômio de grau $k < n$ e vamos mostrar que o resultado vale para f.

Se $a \in R$ é uma raiz de f, então $f(x) = (x-a) \cdot g(x)$ para algum $g \in R[x]$ com $\partial(g) = n - 1$. Por hipótese de indução temos que g tem no máximo $n-1$ raízes distintas em R.

Agora, se $b \in R$ é tal que $g(b) = 0$, então é imediato que $f(b) = 0$, ou seja, toda raiz de g é também raiz de f. Por outro lado, se b é uma raiz de f com $b \neq a$, temos $0 = f(b) = (b-a) \cdot g(b)$. Como R é um domínio, temos que $g(b) = 0$, mostrando assim que f tem no máximo n raízes distintas. ■

Exemplo 55 A hipótese de R ser um domínio é excencial, pois para $R = \mathbb{Z}_6$, temos que $f(x) = x^2 - x \in \mathbb{Z}_6[x]$ é tal que $f(\overline{0}) = f(\overline{1}) = f(\overline{3}) = f(\overline{4}) = \overline{0}$, ou seja, f tem mais que $n = 2$ raízes.

Definição 24 *Sejam R um DFU e $f(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$, com $n \geq 1$. O* **conteúdo** *de $f(x)$ é o máximo divisor comum de seus coeficientes e será denotado por $c(f)$, ou seja, $c(f) = \text{mdc}\,(a_0, a_1, \ldots, a_n)$. Se $c(f) = 1$, dizemos que f é um polinômio* **primitivo**.

Observemos que o conteúdo de um polinômio é definido à menos de associados.

Exemplo 56 Dado $f(x) = 2x^2 + 4x + 6 \in \mathbb{Z}[x]$, temos que $c(f) = 2$. Se vemos $f(x)$ como um elemento de $\mathbb{Q}[x]$, temos que $c(f) = 2 \sim 1$, pois $1 = \dfrac{1}{2} \cdot 2$ em $\mathbb{Q}$. Dado $g(x) = 2x^2 + 5x + 6 \in \mathbb{Z}[x]$, temos que $c(g) = 1$.

Lema 9 (Lema de Gauss) *Sejam R um DFU e $f(x), g(x) \in R[x]$. Então $f(x) \cdot g(x)$ é um polinômio primitivo se, e somente se $f(x)$ e $g(x)$ são primitivos.*

Dem.: Sejam $f(x) = a_0 + a_1x + \cdots + a_nx^n$ e $g(x) = b_0 + b_1x + \cdots + b_mx^m$, com $a_n \neq 0$ e $b_m \, neq 0$. Escrevemos $h(x) = f(x) \cdot g(x) = \displaystyle\sum_{k=0}^{n+m} c_kx^k$, onde $c_k = \displaystyle\sum_{i+j=k} a_i \cdot b_j$.

Se f e g são primitivos e h não é primitivo, então $c(h) = a \notin R^*$ e, como R é um DFU, temos que existe um elemento primo $p \in R$ tal que $p \mid a$. Então $p \mid c_k$, para todo $k = 0, \ldots, n + m$. Como f e g são primitivos, existem i, j tais que $p \nmid a_i$ e $p \nmid b_j$. Sejam r e s os menores índices tais que $p \nmid a_r$ e $p \nmid b_s$. Então $p \mid a_0,\ p \mid a_1, \ldots, p \mid a_{r-1}$ e $p \nmid a_r$; $p \mid b_0,\ p \mid b_1, \ldots, p \mid b_{s-1}$ e $p \nmid b_s$.

Temos então $c_{r+s} = a_{r+s} \cdot b_0 + \cdots + a_{r+1} \cdot b_{s-1} + a_r \cdot b_s + a_{r-1} \cdot b_{s+1} + \cdots + a_0 \cdot b_{r+s})$, de onde obtemos $a_r \cdot b_s = c_{r+s} - (a_{r+s} \cdot b_0 + \cdots + a_{r+1} \cdot b_{s-1}) - (a_{r-1} \cdot b_{s+1} + \cdots + a_0 \cdot b_{r+s})$. Assim, p divide o lado direito da igualdade e como $p \nmid a_r$ e $p \nmid b_s$, temos uma contradição, pois p é primo. Logo, $h = f \cdot g$ é primitivo.

Reciprocamente, se h é primitivo e f não é primitivo, então existe um elemento primo $p \in R$ tal que $p \mid a_i$, para todo $i = 0, \ldots, n$, o que implica que $p \mid a_i \cdot b_j$, para

todo i, j. Logo $p \mid \sum_{k=i+j} a_i \cdot b_j$, para todo k. Assim, $p \mid c(h) = 1$, o que contradiz o fato de h ser primitivo. Logo, f e g são primitivos. ■

Lema 10 *Se R é um DFU e $f(x) \in R[x]$ é não nulo, então existem $a \in R$ e $f_1(x) \in R[x]$ primitivo, tais que $f(x) = a \cdot f_1(x)$ e, esta decomposição é única, a menos de associados.*

Dem.: Escrevendo $f(x) = a_0 + a_1x + \cdots + a_nx^n$ e $a = c(f) = \text{mdc}\ (a_0, \ldots, a_n)$, temos que existem $b_0, b_1, \ldots, b_n \in R$ tais que $a_i = a \cdot b_i$, para todo $i = 1, \ldots, n$, com mdc $(b_0, b_1, \ldots, b_n) = 1$. Logo $f(x) = a(b_0 + b_1x + \ldots + b_nx^n) = a \cdot f_1(x)$, com f_1 primitivo.

Se $f(x) = a_0 \cdot f_0(x)$ com $a_0 \in R$ e f_0 primitivo, temos $c(f) = a_0$ e $c(f) = a$, o que implica que $a_0 \sim a$, pois quaisquer dois máximos divisores comuns são associados. Logo $a = u \cdot a_0$, com $u \in R^*$ e $a_0 \cdot f_0(x) = a \cdot f_1(x) = a_0 \cdot (u \cdot f_1(x))$ e, como R é um domínio, temos $f_0(x) = u \cdot f_1(x)$, com $u \in R^*$, ou seja $f_0 \sim f_1$. ■

Teorema 38 *Se R é um DFU e $f \in R[x]$ é não nulo, então f pode ser escrito como um produto finito de elementos irredutíveis de $R[x]$.*

Dem.: Do lema anterior escrevemos $f(x) = a \cdot f_0(x)$, com $a \in R$ e $f_0(x) \in R[x]$ primitivo. Faremos a demonstração por indução sobre o $\partial(f) = \partial(f_0)$.

Se $\partial(f) = \partial(f_0) = 0$, então $f = a$ e, como R é um DFU, temos que f se fatora como um produto de irredutíveis de R.

Se $\partial(f) \geq 1$ e f_0 é irredutível, então $f = p_1 \cdots p_k \cdot f_0$ é uma fatoração em irredutíveis de f, onde $a = p_1 \cdots p_k$ é uma fatoração em irredutíveis de a. Se f_0 é redutível sobre R, então $f_0 = f_1 \cdot f_2$, com $f_1, f_2 \notin R[x]^*$ e, pelo Lema de Gauss, f_1 e f_2 são também primitivos, o que implica que $0 < \partial(f_1) < \partial(f)$ e $0 < \partial(f_2) < \partial(f)$. Por hipótese de indução temos que f_1 e f_2 se fatoram como produto de irredutíveis, o que implica que f também se fatora. ■

Lema 11 *Sejam R um DFU, K seu corpo de frações e $p(x) \in R[x]$ primitivo. Então $p(x)$ é irredutível em $R[x]$ se, e somente se $p(x)$ é irredutível em $K[x]$.*

Dem.: Se $p(x)$ é redutível em $R[x]$, desde que p é primitivo, temos que $p(x) = f_1(x) \cdot f_2(x)$, com $0 < \partial(f_1) < \partial(p)$ e $0 < \partial(f_2) < \partial(p)$, o que implica que $p(x)$ é redutível em $K[x]$.

Reciprocamente, se $p(x)$ é redutível em $K[x]$, então $p(x) = f(x) \cdot g(x)$, onde $f, g \in K[x]$, com $\partial(f) > 0$ e $\partial(g) > 0$.

Escrevemos $f(x) = \sum_{i=0}^{n} \left(\frac{a_i}{b_i}\right) x^i$ e $g(x) = \sum_{j=0}^{m} \left(\frac{c_j}{d_j}\right) x^j$, com a_i, b_i, c_j, $d_j \in R$. Se $b = b_0 \cdot b_1 \cdots b_n$ e $d = d_0 \cdot d_1 \cdots d_m$, então $b \cdot f(x) = \sum_{i=0}^{n} a_i' \, x^i = f_1(x) \in R[x]$ e $d \cdot g(x) = g_1(x) \in R[x]$.

Do último lema temos que existem $a, c \in R$ e $f_2, g_2 \in R[x]$ primitivos tais que $b \cdot d \cdot p(x) = f_1(x) \cdot g_1(x) = a \cdot f_2(x) \cdot c \cdot g_2(x)$. Do Lema de Gauss e da unicidade da decomposição do último lema, temos que $b \cdot d \sim a \cdot c$ e $p(x) \sim f_2(x) \cdot g_2(x)$. Logo existe $u \in R^*$ tal que $p(x) = (u \cdot f_2(x)) \cdot g_2(x)$, o que mostra que p é redutível em $R[x]$. ■

Teorema 39 *Se R é um DFU, então $R[x]$ também o é.*

Dem.: Seja $f \in R[x]$ uma não unidade. Do teorema anterior, é suficiente mostrarmos a unicidade da fatoração. Se $\partial(f) = 0$, então $f = a \in R$ e a fatoração em iredutíveis é única pois R é um DFU.

Se $\partial(f) \geq 1$, então $f = a \cdot p(x)$, com $a \in R$ e $p(x)$ primitivo. Desde que R é um DFU, é suficiente mostrarmos a unicidade da fatoração de $p(x)$.

Seja K o corpo de frações do domínio R. Desde que $p(x) \in K[x]$ e $K[x]$ é um DFU, temos que existem únicos $f_1(x), \ldots, f_m(x) \in K[x]$ tais que $p(x) = f_1(x) \cdots f_m(x)$. Cada $f_i = \dfrac{q_i(x)}{b_i}$, com $b_i \in R$ e $q_i \in R[x]$ e cada $q_1(x) = a_i \cdot p_i(x)$, com $a_i \in R$ e $p_i(x) \in R[x]$ primitivo.

Assim, $p(x) = \dfrac{a_1 \cdots a_m}{b_1 \cdots b_m} \cdot p_1(x) \cdots p_m(x)$. Calculando o conteúdo em ambos os lados e usando o lema de Gauss, obtemos que $b_1 \cdots b_m = u \cdot (a_1 \cdots a_m)$, para algum $u \in R^*$. Consequentemente, $p(x) = u^{-1} \cdot p_1(x) \cdots p_m(x)$, onde os p_i's são únicos a menos de associados. ■

16 Critérios de Irredutibilidade

Nosso próximo passo é apresentarmos alguns resultados que nos auxiliam a determinar se um dado polinômio é ou não irredutível sobre um DFU. Todos os resultados apresentados sobre $\mathbb{Z}$ e/ou $\mathbb{Q}$ valem, com demonstrações análogas, também sobre um DFU R e/ou seu corpo de frações K.

Teorema 40 *Seja* $f(x) = a_n\,x^n + a_{n-1}x^{n-1} + \cdots + a_1\,x + a_0 \in \mathbb{Z}[x]$, *com* $a_n \neq 0$. *Se* $\dfrac{r}{s} \in \mathbb{Q}$ *é uma raiz de* $f(x)$, *com* $\text{mdc}\,(r,s) = 1$, *então* $r \mid a_0$ *e* $s \mid a_n$.

Dem.: Temos $0 = f\left(\dfrac{r}{s}\right) = a_n \cdot \left(\dfrac{r}{s}\right)^n + a_{n-1} \cdot \left(\dfrac{r}{s}\right)^{n-1} + \cdots + a_1 \cdot \left(\dfrac{r}{s}\right) + a_0$. Multiplicando por s^n, temos $0 = a_n \cdot r^n + a_{n-1} \cdot r^{n-1} \cdot s + \cdots + a_1 \cdot r \cdot s^{n-1} + a_0 \cdot s^n$, o que implica que $-a_n \cdot r^n = (a_{n-1} \cdot r^{n-1} + \cdots + a_1 \cdot r \cdot s^{n-2} + a_0 \cdot s^{n-1}) \cdot s$. Logo $s \mid a_n \cdot r^n$ e, como $\text{mdc}\,(r,s) = 1$, temos que $\text{mdc}\,(s, r^n) = 1$ e, consequentemente $s \mid a_n$.

De maneira análoga obtemos $-a_0 \cdot s^n = (a_n \cdot r^{n-1} + \cdots + a_1 \cdot s^{n-1}) \cdot r$, o que implica que $r \mid a_0 \cdot s^n$ e, como $\text{mdc}\,(r, s^n) = 1$, temos que $r \mid a_0$. ■

Exemplo 57 *Dado* $f(x) = 2x^3 - x^2 + 4x - 2 \in \mathbb{Z}[x]$, *determine se* f *é irredutível em* $\mathbb{Q}[x]$.

Sabemos que se $\dfrac{r}{s}$ é uma raiz de f, então $r \mid 2$ e $s \mid 2$. Logo, $r, s \in \{\pm 1\,,\ \pm 2\}$. Assim o conjunto dos números racionais candidatos a raiz de f é $\{\pm 1\,,\ \pm\dfrac{1}{2}\,,\ \pm 2\}$. Testando cada um deles temos $f(1) \neq 0$; $f(-2) \neq 0$; $f(2) \neq 0$; $f(-1) \neq 0$; $f(-\dfrac{1}{2}) \neq 0$ e $f(\dfrac{1}{2}) = 0$. Portanto $f(x) = (2x-1)(x^2+2)$, ou seja, f é redutível sobre $\mathbb{Q}$.

Exemplo 58 *Seja* $g(x) = x^4 + 2x^2 + 1 \in \mathbb{Z}[x]$. *Verifique se* g *é irredutível sobre* $\mathbb{Q}$.

Notemos que g não tem raizes racionais, pois se r/s é raiz de g, então $r/s = \pm 1$, pois $r \mid 1$ e $s \mid 1$. Mas $g(1) = g(-1) = 4 \neq 0$. Apesar disso $g(x)$ é redutível sobre $\mathbb{Q}$, pois $g(x) = (x^2+1) \cdot (x^2+1)$.

Para polinômios de grau ≤ 3, temos o seguinte critério de irredutibilidade que pode ser útil em muitos casos.

Teorema 41 *Seja $f(x) \in \mathbb{Z}[x]$ um polinômio primitivo com $\partial(f) = 2$ ou $\partial(f) = 3$. Então f é redutível sobre $\mathbb{Z}$ se, e somente se f tem raiz em $\mathbb{Q}$.*

Dem.: Desde que f é primitivo, temos que f é redutível se, e somente se $f(x) = g(x) \cdot h(x)$, com g, $h \in \mathbb{Z}[x]$ com $\partial(g) > 1$ e $\partial(h) > 1$. Como $\partial(g \cdot h) = \partial(g) + \partial(h)$, temos que $\partial(g) = 1$ ou $\partial(h) = 1$, e o resultado segue. ■

Outro famoso critério de irredutibilidade é:

Teorema 42 (Critério de Eisenstein) *Seja $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. Se existe um número primo $p \in \mathbb{Z}$ tal que $p \nmid a_n$, $p \mid a_{n-1}, \cdots, p \mid a_0$ e $p^2 \nmid a_0$, então f é irredutível sobre $\mathbb{Q}$.*

Dem.: Se existe um número primo $p \in \mathbb{Z}$ tal que $p \mid a_i$, para todo $i = 0, \cdots, n-1$, $p \nmid a_n$ e $p^2 \nmid a_0$ e $f(x)$ é redutível sobre $\mathbb{Q}$, então

$$f(x) = (c_0 + c_1 x + \cdots + c_r x^r) \cdot (b_0 + b_1 x + \cdots + b_s x^s),$$

com c_i, $b_i \in \mathbb{Z}$, $0 < r < n$ e $0 < s < n$. Como $a_0 = c_0 \cdot b_0$, $p \mid a_0$ e $p^2 \nmid a_0$, temos que $p \mid c_0$ ou $p \mid b_0$, mas não ambos.

Suponhamos que $p \mid c_0$ e $p \nmid b_0$. Desde que $p \nmid a_n$, temos que existe $i > 0$ tal que $p \nmid c_i$. Seja $0 < j \leq r < n$ o menor índice tal que $p \nmid c_j$.

Logo $a_j = (c_0 \cdot b_j + c_1 \cdot b_{j-1} + \cdots + c_{j-1} \cdot b_1) + c_j \cdot b_0$ e, como $p \mid c_i$, para todo $i < j$, temos que $p \mid (c_0 \cdot b_j + c_1 \cdot b_{j-1} + \cdots + c_{j-1} \cdot b_1)$ e $p \mid a_j$, o que é uma contradição pois $p \nmid c_j \cdot b_0$. Portanto, f é irredutível sobre $\mathbb{Q}$. ■

Exemplo 59 *Verifique se $f(x) = x^{201} - 6x^{107} + 21$ é irredutível sobre $\mathbb{Q}$.*

Tomando $p = 3$, temos que $p \mid 6$, $p \mid 21$, $p \mid 0$ e $p^2 \nmid 21$. Então pelo critério de Eisenstein, f é irredutível sobre $\mathbb{Q}$.

Exemplo 60 *Verifique se* $f(x) = x^4 + 10x^3 - 25x^2 + 15x + 30$ *é irredutível sobre* $\mathbb{Q}$.

Aplicando o critério de Eisenstein para $p = 5$, obtemos que f é irredutível sobre $\mathbb{Q}$.

Exemplo 61 *Usando o critério de irredutibilidade de Eisenstein determine se* $f(x) = x^2 - 4x + 9$ *é irredutível sobre* $\mathbb{Z}$

Desde que f é um polinômio primitivo, é suficiente mostrarmos que f é irredutível sobre $\mathbb{Q}$.

Note que não existe um número primo p satisfazendo as hipóteses do critério de Eisenstein para f, mas para $g(x) = f(x+1) = (x+1)^2 - 4(x+1) + 9 = x^2 + 2x + 1 - 4x - 4 + 9 = x^2 - 2x + 6$, temos que $p = 2$ satisfaz.

Logo pelo critério de Eisenstein, temos que $g(x) = f(x+1)$ é irredutível sobre $\mathbb{Q}$. Então $f(x)$ também é irredutível sobre $\mathbb{Q}$, pois se $f(x) = k(x) \cdot h(x)$, então $f(x+1) = k(x+1) \cdot h(x+1)$.

A mesma técnica pode ser aplicada para o próximo exemplo.

Exemplo 62 *Determine se* $f(x) = x^4 + x^3 + x^2 + x + 1$ *é irredutível sobre* $\mathbb{Q}$, *ou mais geralmente se* $g(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$, *com p primo é irredutível sobre* $\mathbb{Q}$.

Observe que $g(x) = \dfrac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$. Logo

$$\begin{aligned} g(x+1) &= \frac{(x+1)^p - 1}{x} = \frac{x^p + px^{p-1} + px^{p-2} + \cdots + px + 1 - 1}{x} \\ &= x^{p-1} + px^{p-2} + \cdots + p. \end{aligned}$$

Aplicando o critério de Eisenstein para p, temos que $g(x+1)$ é irredutível sobre $\mathbb{Q}$. Portanto $g(x)$ também o é.

O próximo exemplo é uma aplicação do critério de Eisenstein para polinômios sobre um DFU.

Exemplo 63 *Sejam* $R = \mathbb{Z}[i]$ *e* $f(x) = (1-i)x^3+(3+6i)x^2+(2-i)x-1+3i \in R[x]$. *Decida se* f *é irredutível sobre* $\mathbb{Q}(i)$.

Para $p = 1 + 2i$, temos que $N(p) = 5$ que é um número primo de $\mathbb{Z}$ e, como R é um DFU, temos que p é um elemento primo de R. Mais ainda $p \nmid (1 - i)$, pois se $(1 - i) = p \cdot x$, então $2 = N(1 - i) = 5 \cdot N(x)$, o que é uma contradição; $p \mid 3 + 6i = 3 \cdot p$; $p \mid (2 - i) = i \cdot p$; $p \mid (-1 + 3i) = (1 + i) \cdot p$ e $p^2 \nmid (-1 + 3i)$. Portanto f é irredutível pelo Critério de Eisenstein.

Exemplo 64 *Determine se* $f(x) = x^3 + 2x^2 + 3x + 5$ *é irredutível sobre* $\mathbb{Q}$.

Observe que não podemos aplicar o critério de Eisenstein para f. Mas, $\overline{f}(x) = \overline{1}x^3 + \overline{2}x^2 + \overline{3}x + \overline{5} = x^3 + x + 1 \in \mathbb{Z}_2[x]$. Como $\partial(\overline{f}) = 3$ e $\overline{f}(\overline{0}) = \overline{f}(\overline{1}) = \overline{1} \neq \overline{0}$ em $\mathbb{Z}_2$, temos que $\overline{f}$ é irredutível em $\mathbb{Z}_2[x]$, o que implica que $\overline{f}$ é irredutível sobre $\mathbb{Z}$, como veremos no próximo critério de irredutibilidade.

Teorema 43 *Sejam* $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$ *e* $\overline{f}(x) = x^n + \overline{a_{n-1}}x^{n-1} + \cdots + \overline{a_1}x + \overline{a_0} \in \mathbb{Z}_p[x]$, *com* $p \in \mathbb{Z}$ *um número primo. Se* $\overline{f}$ *é irredutível em* $\mathbb{Z}_p[x]$ *então* f *é irredutível em* $\mathbb{Z}[x]$.

Dem.: Se f é redutível sobre $\mathbb{Z}$, desde que o coeficiente dominante de f é 1, temos que $f = g \cdot h$, onde $g, h \in \mathbb{Z}[x]$ são tais que $0 < \partial(g), \partial(h) < \partial(f) = n$. Então $\overline{f} = \overline{g} \cdot \overline{h}$, com $\partial(g) = \partial(\overline{g})$ e $\partial(h) = \partial(\overline{h})$, o que implica que $\overline{f}$ é redutível sobre $\mathbb{Z}_p$. ■

17 Extensões de Corpos

Definição 25 *Se um subanel E de um corpo F é um corpo, então E é dito ser um* **subcorpo** *de F ou F é uma* **extensão** *do corpo E. Mais geralmente, dizemos que o corpo F é uma* **extensão** *do corpo E se F contém um subcorpo isomorfo a E, ou seja , se existe um homomorfismo injetor de anéis $\varphi : E \to F$. Neste caso, usaremos a notação $F \supseteq E$.*

Exemplo 65 Todo corpo F é uma extensão dele mesmo. Temos também as extensões naturais $\mathbb{R} \supseteq \mathbb{Q}$, $\mathbb{C} \supseteq \mathbb{Q}$ e $\mathbb{C} \supseteq \mathbb{R}$. Também temos que $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2};\ a, b \in \mathbb{Q}\}$ é uma extensão do corpo $\mathbb{Q}$.

Observe que se F é um corpo e R é um subanel não nulo de F com 1_R, então R é domínio e $1_R = 1_F$, pois $1_R \cdot 1_F = 1_R = 1_R \cdot 1_R$ e, como F é corpo, podemos cancelar 1_R em ambos os lados e obtemos $1_R = 1_F$.

Definição 26 *Sejam F um corpo e $S \subseteq F$ um subconjunto. O* **subanel de F gerado** *por S é a intersecção de todos os subaneis de F que contém S. O* **subcorpo de F gerado por** *S é a intersecção de todos os subcorpos de F que contém S.*

Exemplo 66 Sejam $F = \mathbb{R}$ e $S = \{1\}$. O subanel de F gerado por S é $\mathbb{Z}$ e o subcorpo de F gerado por S é $\mathbb{Q}$.

Para $S' = \{\sqrt{2}\}$, se A é o subanel de F gerado por S' e K é o subcorpo de F gerado por S', então temos que $\sqrt{2} \in A \subseteq K$, o que implica que $\mathbb{Z}\sqrt{2} \subseteq A \subseteq K$. Mais ainda, $2 = (\sqrt{2})^2 \in A$. Logo $2\mathbb{Z} \subseteq A$ e $\mathbb{Z} \subseteq K$. Assim,

$$\{2a + b\sqrt{2};\ a, b, \in \mathbb{Z}\} \subseteq A$$

e $\mathbb{Z}[\sqrt{2}] \subseteq K$. Como $\{2a + b\sqrt{2};\ a, b, \in \mathbb{Z}\}$ é um anel temos que $\{2a + b\sqrt{2};\ a, b, \in \mathbb{Z}\} = A$ e, $\mathbb{Z}[\sqrt{2}] \subseteq K$, implica que $\mathbb{Q}[\sqrt{2}] = K$.

Note que neste caso A não tem 1_A e K não é o corpo de frações de A.

Lema 12 *Sejam F um corpo, $S \subseteq F$ um subconjunto com $1_F \in S$. Se R é o subanel de F gerado por S, então R é um domínio e K, o subcorpo de F gerado por S, é o corpo de frações de R.*

Dem.: É imediato que $R \subseteq K$, pois todo subcorpo é subanel. Agora, como $1_F \in S \subseteq R$, temos que $1_R = 1_F = 1$. Mais ainda, como $R \subseteq F$, temos que R é um domínio.

Seja $K' = \{a \cdot b^{-1};\ \ a, b \in R,\ b \neq 0\}$ o corpo de frações de R. Desde que $R \subseteq K$ e K' é o menor corpo que contém R, temos que $K' \subseteq K$. Mas $S \subseteq R \subseteq K' \subseteq F$, ou seja, K' é um subcorpo de F que contém S. Então, por definição, $K \subseteq K'$ e, consequentemente $K' = K$. ■

Teorema 44 *Seja F um corpo. temos então:*

(i) *O subanel de F gerado por 1_F, isto é gerado por $\{1_F\}$ é $\mathbb{Z} \cdot 1_F = \{a \cdot 1_F;\ a \in \mathbb{Z}\}$ e o subcorpo de F gerado por 1_F é o corpo de frações de $\mathbb{Z} \cdot 1_F$.*

(ii) *Se $\varphi : \mathbb{Z} \to F$ definida por $\varphi(a) = a \cdot 1_F$, para todo $a \in \mathbb{Z}$, então φ é um homomorfismo de anéis com $\text{Im}\ (\varphi) = \mathbb{Z} \cdot 1_F$ e $\text{Ker}\ (\varphi) = \{0\}$ ou $\text{Ker}\ (\varphi) = p\,\mathbb{Z}$, para algum primo $p \in \mathbb{Z}$.*

(iii) *Se $\text{Ker}\ (\varphi) = \{0\}$, então $\mathbb{Z} \cdot 1_F \cong \mathbb{Z}$ e o subcorpo de F gerado por 1_F é isomorfo a $\mathbb{Q}$.*

(iv) *Se $\text{Ker}\ (\varphi) = p\,\mathbb{Z}$ com p primo, então $\mathbb{Z} \cdot 1_F \cong \mathbb{Z}_p$ e o subcorpo de F gerado por 1_F é também isomorfo a $\mathbb{Z}_p$.*

Dem.: **(i)** Todo subanel de F que contém 1_F contém $\mathbb{Z} \cdot 1_F$ e, $\mathbb{Z} \cdot 1_F$ é um subanel de F que contém 1_F. Então $\mathbb{Z} \cdot 1_F$ é o subanel de F gerado por 1_F e, do lema anterior, seu corpo de frações é o subcorpo de F gerado por 1_F.

(ii) É fácil ver que φ é um homomorfismo de anéis com $\text{Im}\ (\varphi) = \mathbb{Z} \cdot 1_F$. Do primeiro Teorema do Isomorfismo para Anéis, temos: $\mathbb{Z}/\text{Ker}\ (\varphi) \cong \text{Im}\ (\varphi) = \mathbb{Z} \cdot 1_F$ que é um domínio, pois é um subanel du um corpo com 1. Assim, $\text{Ker}\ (\varphi)$ é um

ideal primo de $\mathbb{Z}$, o que implica que Ker $(\varphi) = \{0\}$ ou Ker $\varphi = p\mathbb{Z}$ para algum número primo p.

(iii) Se Ker $(\varphi) = \{0\}$, então φ é injetor e $\mathbb{Z} \cong \mathbb{Z}/\text{Ker }(\varphi) \cong \text{Im }(\varphi) = \mathbb{Z} \cdot 1_F$. E, o subcorpo de F gerado por 1_F é o corpo de frações de $\mathbb{Z} \cdot 1_F$ que é isomorfo ao corpo de frações de $\mathbb{Z}$, que é $\mathbb{Q}$.

(iv) Se Ker $(\varphi) = p\mathbb{Z}$, com p um número primo de $\mathbb{Z}$, então $\mathbb{Z} \cdot 1_F = \text{Im }(\varphi) \cong \mathbb{Z}/\text{Ker }(\varphi) = \mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}_p$, que é corpo e portanto igual ao seu corpo de frações. ■

Observação: O subcorpo de F gerado por 1_F é a intersecção de todos os subcorpos de F.

Definição 27 *A intersecção de todos os subcorpos de F é chamado o* **corpo primo** *de F.*

Como consequência imediata do teorema acima temos

Corolário 17 *Seja F um corpo e $\varphi : \mathbb{Z} \to F$ o homomorfismo de anéis tal que $\varphi(a) = a \cdot 1_F$, para todo $a \in \mathbb{Z}$. Se* Ker $(\varphi) = \{0\}$*, então o corpo primo de F é isomorfo a $\mathbb{Q}$. Se* Ker $(\varphi) = p\mathbb{Z}$*, com p primo, então o corpo primo de F é isomorfo a $\mathbb{Z}_p$.*

Definição 28 *Dizemos que o corpo F tem* **característica zero** *$(Car\,(F) = 0)$ se o corpo primo de F é isomorfo a $\mathbb{Q}$ e F tem* **característica** *p $(Car\,(F) = p)$ se o corpo primo de F é isomorfo a $\mathbb{Z}_p$.*

Esta noção de característica para corpos deriva da noção de característica para anéis, pois:

Corolário 18 *Seja F um corpo. Então:*

(i) $Car\,(F) = 0 \Leftrightarrow Car\,(\mathbb{Z} \cdot 1_F) = 0$;

(ii) $Car\,(F) = p \Leftrightarrow Car\,(\mathbb{Z} \cdot 1_F) = p$.

Exemplo 67 Para os corpos canônicos temos $Car(\mathbb{Q}) = 0$; $Car(\mathbb{C}) = 0$ e $Car(\mathbb{R}) = 0$.

Para o corpo $\mathbb{Q}[\sqrt{2}]$ temos $Car(\mathbb{Q}[\sqrt{2}]) = 0$. Mais geralmente, se F é uma extensão do corpo dos números racionais $\mathbb{Q}$, então $Car(F) = 0$. Por exemplo, se

$$\mathbb{Q}(x) = \left\{ \frac{f(x)}{g(x)};\ f, g \in \mathbb{Q}[x] \ \text{ e } \ g \neq 0 \right\},$$

então $\mathbb{Q}(x)$ é o corpo de frações do domínio $\mathbb{Q}[x]$ e $Car(\mathbb{Q}(x)) = 0$.

Note que se F é um corpo com $Car(F) = 0$, então F é um corpo infinito, pois contém uma cópia de $\mathbb{Z}$. Assim, se F é finito, então $Car(F) = p$, para algum primo p. Mas existem corpos infinitos de característica p, por exemplo $\mathbb{Z}_p(x)$ o corpo de frações do anel de polinômios $\mathbb{Z}_p[x]$ é um corpo de característica p infinito.

Finalizaremos esta seção com um exemplo de um corpo com 4 elementos.

Exemplo 68 Seja $F = \{0, 1, \alpha, 1 + \alpha\}$, com as operações dadas pelas tabelas abaixo:

$+$	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

$\cdot$	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

Das tabelas é fácil ver que F é um corpo com 4 elementos de $Car(F) = 2$.

18 Elementos Algébricos e Transcendentes

Sejam $K \supseteq F$ uma extensão de corpos e $\alpha \in K$. Escrevemos $F(\alpha)$ para denotar o subcorpo de K gerado por F e α, ou seja, $F(\alpha)$ é o menor subcorpo de K que contém F e α. Claramente $F(\alpha) \supseteq F$ é uma extensão de corpos, dita ser uma **extensão simples** de F por α e, é dita ser obtida de F pela **adjunção do elemento** α.

Exemplo 69 Para $F = \mathbb{R}$ e $\alpha = i \in \mathbb{C}$, temos que $F(\alpha) = \mathbb{C}$.

Para $F = \mathbb{Q}$ e $\alpha = \sqrt{2} \in \mathbb{C}$, temos que $F(\alpha) = \mathbb{Q}[\sqrt{2}]$.

Definição 29 *Sejam $K \supseteq F$ uma extensão de corpos e $\alpha \in K$. Dizemos que α é* **algébrico** *sobre F se existe $f(x) \in F[X]$, $f \neq 0$, tal que $f(\alpha) = 0$. Se não existe um polinômio não nulo $f \in F[x]$ tal que $f(\alpha) = 0$, então dizemos que α é* **transcendente** *sobre F.*

Exemplo 70 O número real $\alpha = \sqrt{2}$ é algébrico sobre $\mathbb{Q}$, pois α é raiz de $f(x) = x^2 - 2 \in \mathbb{Q}[x]$. Observe que $\alpha \notin \mathbb{Q}$, o que implica que $\mathbb{Q} \subsetneqq \mathbb{Q}(\sqrt{2}) \subsetneqq \mathbb{R}$.

Já, pode-se mostrar que o elemento $\beta = \pi \in \mathbb{R}$ é transcendente sobre $\mathbb{Q}$. Mas π é algébrico sobre $\mathbb{Q}(\pi^2)$, pois β é raiz de $g(x) = x^2 - \pi^2 \in \mathbb{Q}(\pi^2)[x]$.

O elemento $\gamma = \dfrac{3 - \sqrt[6]{2}}{9} \in \mathbb{R}$ é algébrico sobre $\mathbb{Q}$, pois $9\gamma - 3 = -\sqrt[6]{2}$, o que implica que $(9\gamma - 3)^6 = 2$. Logo γ é raiz de $f(x) = (9x - 3)^6 - 2 \in \mathbb{Q}[x]$.

Sejam $K \supseteq F$ uma extensão de corpos e $\alpha \in K$. É fácil verificar que $\varphi_\alpha : F[x] \to K$, definida por $\varphi_\alpha(f) = f(\alpha) \in K$ é um homomorfismo de anéis. Observe que se $f(x) = a_0 + a_1 x + \cdots + a_n x^n;$, com $a_i \in F$, então $f(\alpha) = a_0 + a_1 \cdot \alpha + \cdots + a_n \cdot \alpha^n \in K$. Com estas noções temos:

Proposição 7 *$\alpha \in K$ é algébrico sobre $F \Leftrightarrow$ Ker $(\varphi_\alpha) \neq \{0\}$;*

$\alpha \in K$ é transcendente sobre $F \Leftrightarrow$ Ker $(\varphi_\alpha) = \{0\}$.

Dem.: Imediata. ■

Teorema 45 *Sejam $K \supseteq F$ uma extensão de corpos e $\alpha \in K$. São equivalentes*

(i) *α é algébrico sobre F;*

(ii) $\text{Ker}\ (\varphi_\alpha) = p(x) \cdot F[x] = (p(x))$ *para algum polinômio irredutível $p \in F[x]$;*

(iii) $\text{Im}\ (\varphi_\alpha) = F[\alpha] = \{f(\alpha);\ f(x) \in F[x]\}$ *é um corpo e portanto igual ao seu corpo de frações $F(\alpha)$.*

Dem.: Se α é algébrico sobre F, então $\text{Ker}\ (\varphi_\alpha) \neq \{0\}$ e $\dfrac{F[x]}{\text{Ker}\ (\varphi_\alpha)} \cong \text{Im}\ (\varphi_\alpha) \subseteq K$. Desde que K é corpo, temos que $\dfrac{F[x]}{\text{Ker}\ (\varphi_\alpha)}$ é um domínio, o que implica que $\text{Ker}\ (\varphi_\alpha)$ é um ideal primo não nulo de $F[x]$. Como $F[x]$ é um DIP, temos que $\text{Ker}\ (\varphi_\alpha)$ é gerado por um elemento irredutível de $F[x]$, ou seja $\text{Ker}\ (\varphi_\alpha) = (p(x))$, com $p(x)$ irredutível sobre F. Com isso mostramos que **(i)** $\Rightarrow$ **(ii)**.

Para mostrarmos que **(ii)** $\Rightarrow$ **(iii)**, suponhamos que $\text{Ker}\ (\varphi_\alpha) = (p(x))$ onde $p(x)$ é irredutível em $F[x]$. Desde que em um DIP todo ideal gerado por um elemento irredutível é primo e, que todo ideal primo não nulo é maximal, temos que $\text{Ker}\ (\varphi_\alpha)$ é um ideal maximal de $F[x]$. Assim, $\dfrac{F[x]}{\text{Ker}\ (\varphi_\alpha)} \cong \text{Im}\ (\varphi_\alpha)$ é um corpo, o que implica que $\text{Im}\ (\varphi_\alpha) = F[\alpha]$ é um corpo. Logo, seu corpo de frações $F(\alpha)$ é igual a $F[\alpha]$.

Finalmente, para mostrarmos que **(iii)** $\Rightarrow$ **(i)**, suponhamos que $\text{Im}\ (\varphi_\alpha)$ é um corpo. Então $\dfrac{F[x]}{\text{Ker}\ (\varphi_\alpha)}$ é um corpo, o que implica que $\text{Ker}\ (\varphi_\alpha) \neq \{0\}$, pois $F[x]$ é um domínio que não é corpo. Assim, α é algébrico sobre F. ■

O resultado análogo ao teorema anterior para elementos transcendentes é:

Teorema 46 *Sejam $K \supseteq F$ uma extensão de corpos e $\alpha \in K$. São equivalentes*

(i) *α é transcendente sobre F;*

(ii) $\text{Ker}\ (\varphi_\alpha) = \{0\}$;

(iii) $\text{Im}\ (\varphi_\alpha) = F[\alpha] = \{f(\alpha);\ f(x) \in F[x]\}$ *é isomorfo ao anel de polinômios $F[x]$.*

Dem.: Imediata. ■

Definição 30 *Um polinômio com coeficiente dominante igual a 1 é dito ser um* **polinômio mônico**.

Corolário 19 *Sejam $K \supseteq F$ uma extensão de corpos e $\alpha \in K$ algébrico sobre F. Então existe um único polinômio mônico irredutível $q(x) \in F[x]$ tal que $q(\alpha) = 0$.*

Dem.: Se α é algébrico sobre F, então de teorema anterior, temos que Ker $(\varphi_\alpha) = (p(x))$, com $p(x)$ irredutível sobre F tal que $p(\alpha) = 0$. Seja $q(x)$ o único polinômio mônico associado a $p(x)$. Então $q(x)$ também é irredutível e pelo teorema do dicionário, temos que Ker $(\varphi_\alpha) = (p(x)) = (q(x))$, o que implica que $q(\alpha) = 0$. ■

Definição 31 *Se $K \supseteq F$ é uma extensão de corpos e $\alpha \in K$ algébrico sobre F, então o único polinômio mônico irredutível sobre F tal que α é raiz é dito ser o* **polinômio minimal de α sobre** *F e será denotado por* $\min(\alpha, F)$.

Com esta noção, temos o seguinte resultado:

Corolário 20 *Sejam $K \supseteq F$ uma extensão de corpos e $\alpha \in K$ algébrico sobre F. Então* $\min(\alpha, F)$ *satisfaz as seguintes propriedades:*

(i) $\min(\alpha, F)$ *é o único polinômio mônico irredutível de menor grau em $F[x]$ tendo α como raiz.*

(ii) *Para $f(x) \in F[x]$, temos que $f(\alpha) = 0$ se, e somente se* $\min(\alpha, F) \mid f(x)$.

(iii) $F(\alpha) \cong F[x]/(\min(\alpha, F))$.

(iv) $F(\alpha) = \{f(\alpha);\ f \in F[x]$ *com* $\partial f < \partial\ (\min(\alpha, F))$ *ou* $f = 0\} = F[x]/(\min(\alpha, F))$.

Exemplo 71 Dado $\alpha = \sqrt{2} \in \mathbb{R}$, temos que $\min(\alpha, \mathbb{Q}) = x^2 - 2$ e $\min(\alpha, \mathbb{R}) = x - \sqrt{2}$.

Do item **(iv)** do corolário acima temos

$$\mathbb{Q}(\sqrt{2}) = \left\{ f(\sqrt{2});\ f \in \mathbb{Q}[x] \text{ e } \partial(f) < 2 \text{ ou } f = 0 \right\}.$$

Assim, $\mathbb{Q}(\sqrt{2}) = \left\{ a + b\sqrt{2};\ a, b \in \mathbb{Q} \right\} = \mathbb{Q}[\sqrt{2}]$.

Exemplo 72 Dado $i \in \mathbb{C}$, temos $\min(i, \mathbb{R}) = \min(i, \mathbb{Q}) = x^2 + 1$.

Mais ainda, $\mathbb{Q}(i) = \{a + b_i;\ a, b \in \mathbb{Q}\}$ e $\mathbb{R}(i) = \{a + b_i;\ a, b \in \mathbb{R}\} = \mathbb{C}$.

Temos também $\dfrac{\mathbb{R}[x]}{(x^2+1)} \cong \text{Im}\ (\varphi_\alpha) = \mathbb{C}$.

Nosso próximo passo é mostrar que dado um polinômio irredutível sobre um corpo F, sempre existe uma extensão de F que contém uma raiz deste polinômio.

Primeiro observamos que para F um corpo e $p(x) \in F[x]$ irredutível sobre F, temos que se $K \supseteq F$ é uma extensão de corpos e $\alpha \in K$ é uma raiz de $p(x)$, então $F[\alpha] = F(\alpha) \supseteq F$, ou seja $K \supseteq F(\alpha) \supseteq F$ são extensões de corpos, com $F(\alpha) \cong \dfrac{F[x]}{(p(x))}$.

Teorema 47 *Sejam F um corpo e $p(x) = \sum_{i=0}^{n} a_i x^i \in F[x]$ irredutível de grau n. Então existe um corpo E e um homomorfismo injetor $\sigma : F \to E$ tais que $\sigma(p) = \sum_{i=0}^{n} \sigma(a_i) \cdot x^i \in \sigma(F)[x]$ tem uma raiz em E.*

Dem.: Sejam $E = \dfrac{F[x]}{(p(x))}$, que é um corpo e $\pi : F[x] \to E$ a projeção canônica, ou seja, $\pi(f(x)) = f(x) + (p(x))$, para todo $f(x) \in F[x]$.

Para $\sigma = \pi\ |_F$: $F \to E$, temos que σ é um homomorfismo injetor, pois se $\sigma(a) = 0$, então $a + (p(x)) = (p(x))$, o que implica que $a \in (p(x))$, ou seja $a = 0$. Logo Ker $(\sigma) = \{0\}$.

Desde que $p \in (p(x))$, temos que $\pi(p) = 0 \in E$. Logo $0 = \pi(p) = \sum_{i=0}^{n} \pi(a_i) \cdot (\pi(x))^i = \sum_{i=0}^{n} \sigma(a_i) \cdot (\pi(x))^i = \sigma(p)(\pi(x))$, ou seja, $\alpha = \pi(x) \in E$ é uma raiz de $\sigma(p)$. ■

Da demonstração acima temos

$$E = \frac{F[x]}{(p(x))} = \pi(F[x]) = \{\pi(f(x));\ f(x) \in F[x]\} = \{\sigma(f)(\pi(x));\ f \in F[x]\} =$$

$$= \{\sigma(f)(\alpha);\ f \in F[x]\} = \{g(\alpha);\ g \in \sigma(F)[x]\} = \sigma(F)(\alpha)\,.$$

que é identificado com $F(\alpha)$.

Exemplo 73 Para $F = \mathbb{Z}_2$ e $p(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$, temos que

$E = \dfrac{\mathbb{Z}_2[x]}{(x^2+x+1)} = \sigma(\mathbb{Z}_2)(\alpha)$, onde $\alpha^2 + \alpha + 1 = 0$ que é identificado com $\mathbb{Z}_2(\alpha) = \{a + b\alpha;\ a, b \in \mathbb{Z}_2\} = \{0, 1, \alpha, 1 + \alpha\}$, onde $\alpha^2 + \alpha + 1 = 0$ que é o corpo com 4 elementos do exemplo da seção anterior.

Usando o teorema do fator, o teorema anterior e indução sobre o grau do polinômio obtemos:

Teorema 48 *Sejam F um corpo e $p(x) \in F[x]$ um polinômio de grau $n > 0$. Então existe uma extensão E do corpo F tal que $p(x) = a_n(x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n)$; com os $\alpha_i \in E$ não necessariamente distintos, para $i = 1, \ldots, n$.*

Definição 32 *Sejam F um corpo, $p(x) \in F[x]$ um polinômio de grau $n > 0$ e $E \supseteq F$ uma extensão de corpos tal que p se fatora em um produto de fatores lineares em $E[x]$ (como no teorema anterior). Se S é o conjunto de todas as raízes de p, então $S \subseteq E$ e o subcorpo de E gerado por $F \cup S$, $F(S)$ é dito ser* **um corpo de raízes** *de p sobre F.*

Corolário 21 *Se F é um corpo e $f \in F[x]$ tem grau $n > 0$, então existe um corpo de raízes de f sobre F. Mais ainda, se $K \supseteq F$ é um corpo de raízes de f sobre F e $E \subseteq K$ é um subcorpo de K tal que f se fatora completamente em $E[x]$, então $E = K$, ou seja, o corpo de raizes de um polinômio é único.*

Exemplo 74 Para $f(x) = x^2 - 2 \in \mathbb{Q}[x]$, temos que $\mathbb{Q}(\sqrt{2})$ é o corpo de raízes de f sobre $\mathbb{Q}$, pois $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(S)$, onde $S = \{\pm\sqrt{2}\})$ é o conjunto das raizes de f.

Desde que $S \subseteq \mathbb{R}$, temos que $\mathbb{R}(S) = \mathbb{R}$ é o corpo de raízes de $f(x) = x^2 - 2$ sobre $\mathbb{R}$.

Para $g(x) = x^2 + x + 1 \in \mathbb{Q}[x]$, temos que as raizes de g são
$\dfrac{-1 \pm \sqrt{-3}}{2} = \dfrac{-1 \pm \sqrt{3}\,i}{2}$.
Assim, $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\sqrt{3}i)$ é o corpo de raízes de f sobre $\mathbb{Q}$.

Definição 33 *Sejam $K \supseteq F$ uma extensão de corpos. Dizemos que K é uma* **extensão algébrica** *de F se cada elemento de K é algébrico sobre F. Caso contrário, dizemos que K é uma* **extensão transcendente** *de F.*

Observe que se $K \supseteq F$, então K tem a estrutura de espaço vetorial sobre F. A dimensão de K como espaço vetorial sobre F é o **grau da extensão** *e é denotada por $[K : F]$. Dizemos que $K \supseteq F$ é uma* **extensão finita** *se $[K : F] < \infty$. Se $[K : F] = \infty$, dizemos que $K \supseteq F$ é uma* **extensão infinita**.

Exemplo 75 Para a extensão $\mathbb{Q}(\sqrt{2}) \supseteq \mathbb{Q}$, temos que $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 = \partial(\min(\sqrt{2}, \mathbb{Q}))$. Mais ainda, $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2};\ a, b \in \mathbb{Q}\}$ e $\{1, \sqrt{2}\}$ é uma base de $\mathbb{Q}(\sqrt{2})$ sobre $\mathbb{Q}$.

Teorema 49 *Toda extensão finita de corpos é algébrica.*

Dem.: Seja $K \supseteq F$ uma extensão de corpos com $[K : F] = n$.

Então, para todo $\alpha \in K$, temos que o conjunto $\{1, \alpha, \alpha^2, \ldots, \alpha^n\} \subseteq K$ é linearmente dependente sobre F. Logo existem $a_0, a_1, \ldots, a_n \in F$, não todos nulos, tais que $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$, o que implica que α é raiz do polinômio não nulo $f(x) = a_0 + a_1x + \cdots + a_nx^n \in F[x]$, ou seja, α é algébrico sobre F. Portanto, $K \supseteq F$ é uma extensão algébrica. ■

Obs: não vale a recíproca deste teorema. Pode-se mostrar que $\{x \in \mathbb{R};\ x$ é algébrico sobre $Q\} = \overline{Q}$ é um corpo e $[\overline{Q} : Q] = \infty$.

Corolário 22 *Seja $K \supseteq F$ uma extensão de corpos e $\alpha \in K$ um elemento algébrico sobre F. Se $\min(\alpha, F) \in F[x]$ tem com grau $n > 0$, então $[F(\alpha) : F] = n$.*

Dem.: Sabemos que $F(\alpha) = \{r(\alpha);\ r(x) \in F[x]$ com $r = 0$ ou $\partial(r) < n\}$ que é gerado como espaço vetorial sobre F por $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$. Vamos mostrar que este conjunto é uma base para $F(\alpha)$ sobre F.

O conjunto $\{1, \alpha, \ldots, \alpha^{n-1}\}$ é linearmente independente sobre F pois se $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = 0$, com $a_i \in F$, então temos que $f(\alpha) = 0$, onde $f(x) = \sum_{i=0}^{n-1} a_i x^i \in F[x]$.

Se $f \neq 0$, então $\partial(f) \leq n-1 < \partial(\min(\alpha, F))$ e α é raiz de f, o que é uma contradição. Portanto, $f = 0$ e $a_i = 0$, para todo $i = 0, \ldots, n-1$.

Assim, $\Rightarrow [F(\alpha) : F] = n$, como queríamos. ■

Obs: $[F(\alpha) : F] = \partial(\min(\alpha, F))$.

Do corolário, temos que se $\alpha \in K$ é algébrico sobre F, então, $F(\alpha)$ é uma extensão algébrica de F, chamada a **extensão algébrica simples gerada por α.**

O próximo resultado é uma consequência imediata de resultados de álgebra linear.

Teorema 50 *Se $K \supseteq E \supseteq F$ são extensões de corpos, com $[E : F] < \infty$ e $[K : E] < \infty$, então $[K : F] < \infty$ e $[K : F] = [K : E] \cdot [E : F]$.*

Dem.: Sejam $[K : E] = n$ e $[E : F] = m$. É suficiente mostrar que se $\{x_1, \ldots, x_n\}$ é uma base de K sobre E e $\{y_1, \ldots, y_n\}$ é uma base de E sobre F, então $\{x_i \cdot y_j;\ i \leq 1 \leq n \text{ e } j \leq 1 \leq m\}$ é uma base de K sobre F. A demonstração deste fato é feita com argumentos de álgebra linear e, fica para o leitor. ■

Exemplo 76 Sejam $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ e α é uma raiz de $f(x)$ em alguma extensão de $\mathbb{Q}$.

Desde que $f(x)$ é irredutível sobre $\mathbb{Q}$, temos que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$.

As raizes de $f(x)$ são $\alpha_1 = \sqrt[3]{2}$, $\alpha_2 = \sqrt[3]{2}\,\omega$, onde ω é uma raiz cúbica primitiva da unidade, ou seja, $\omega^3 = 1$ e $\omega \neq 1$, e $\alpha_3 = \sqrt[3]{2}\,\omega^2$.

Seja E o corpo de raizes de $f(x)$ sobre $\mathbb{Q}$. Queremos calcular $[E : F]$.

Note que E é o menor corpo que contém $\mathbb{Q}$ e $\{\alpha_1, \alpha_2, \alpha_3\}$. É fácil verificar que $E = \mathbb{Q}(\sqrt[3]{2}\,, \omega)$.

Desde que ω é uma raiz cúbica primitiva da unidade, temos que $\min(\omega, \mathbb{Q}) = x^2 + x + 1$, que tem como raizes ω e ω^2, que não são reais. Como $K = \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$, temos que $\min(\omega, K) = x^2 + x + 1$. Portanto, $[K(\omega) : K] = 2$.

Assim, $[E, \mathbb{Q}] = \big[E, \mathbb{Q}(\sqrt[3]{2})\big] \cdot \big[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}\big] = 2 \cdot 3 = 6\,.$

Exemplo 77 *Dado $\alpha = \sqrt{2}+\sqrt{3} \in \mathbb{R}$, mostre que α é algébrico sobre $\mathbb{Q}$ e encontre* $\min(\alpha, \mathbb{Q})$.

Desde que $\alpha^2 = (5 + 2\sqrt{6})$, temos que $\dfrac{\alpha^2 - 5}{2} = \sqrt{6}$. Logo $\left(\dfrac{\alpha^2 - 5}{2}\right)^2 = 6\,.$ Assim, α é raiz do polinômio $f(x) = x^4 - 10x + 1 \in \mathbb{Q}[x]$, o que mostra que α é algébrico sobre $\mathbb{Q}$.

Para mostrar que $\min(\alpha, \mathbb{Q}) = f(x)$, é suficiente mostrar que $f(x)$ é irredutível.

Sabemos que não é fácil provar que um polinômio de grau 4 é irredutível, então mostraremos que $\min(\alpha, \mathbb{Q}) = f(x)$, usando grau de extensão.

Seja $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Então $\mathbb{Q}(\alpha) \subseteq E$ e, consequentemente $[\mathbb{Q}(\alpha) : \mathbb{Q}] \mid [E : \mathbb{Q}]$.

Agora, $[E : \mathbb{Q}] = [E : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2.2$, pois $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$.

Então $[\mathbb{Q}(al) : \mathbb{Q}] = 1, 2$ ou 4.

$[\mathbb{Q}(\alpha) : \mathbb{Q}] \neq 1$ pois $\alpha \notin \mathbb{Q}\,.$

$[\mathbb{Q}(\alpha) : \mathbb{Q}] \neq 2$ pois $\alpha^2 \notin \mathbb{Q}$, $[\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha^2)] = 2$ e

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha^2)] \cdot [\mathbb{Q}(\alpha^2) : \mathbb{Q}] = 2.[\mathbb{Q}(\alpha^2) : \mathbb{Q}] > 2.$$

Portanto $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ e, como consequência disso, temos que $\min(\alpha, \mathbb{Q}) = x^4 - 10x + 1$ que é irredutível sobre $\mathbb{Q}$.

19 Exercícios

1. Seja R um anel. Defina $\phi : R \to R[x]$ por $\phi(a) = ax$, para todo $a \in R$. Então ϕ é um homomorfismo de anéis? Justifique.

2. Representar cada um dos seguintes polinômios como um produto de uma constante de K por um polinômio primitivo de $R[x]$, onde K é o corpo de frações do domínio R:

   (a) $3x^2 + 6x + 6, \quad R = \mathbb{Z}$;

   (b) $2x^2 + 2x + 1, \quad R = \mathbb{R}$;

   (c) $2x^2 + (1+i)x + (1-i), \quad R = \mathbb{Z}[i]$;

   (d) $2x^2 + (2-\sqrt{2})x + 4, \quad R = \mathbb{Z}[\sqrt{2}]$;

   (e) $\frac{1}{3}x^2 + \frac{1}{2}x + 6, \quad R = \mathbb{Z}$;

   (f) $\frac{1}{2}x^2 - \frac{5}{1-i}x + 2, \quad R = \mathbb{Z}[i]$;

   (g) $\frac{1}{4}x^2 + \frac{1}{2}x + \frac{1}{4-2\sqrt{2}}, \quad R = \mathbb{Z}[\sqrt{2}]$.

3. Mostre que um elemento primo de um DFU R, também é primo em $R[x]$.

4. De um exemplo para mostrar que não vale a volta do lema de Gauss.

5. Verifique se os seguintes polinômios são irredutíveis em $R[x]$.

   (a) $2x^4 + 14x^3 + 28x^2 + 42x + 70, \quad R = \mathbb{Q}$;

   (b) $x^3 + 4x^2 + 2x + 2, \quad R = \mathbb{Z}$;

   (c) $x^5 - 7, \quad R = \mathbb{Z}$;

   (d) $x^4 + 3x^3 + 9x^2 + 9x + 18, \quad R = \mathbb{Q}$;

   (e) $14x^3 + 280x^2 - 420x + 15, \quad R = \mathbb{Q}$;

   (f) $\frac{2}{3}x^5 + 4x^4 - 12x^3 + 6x^2 + 2x + 14, \quad R = \mathbb{Q}$;

   (g) $x^4 - 2ix^3 + (1+i)x^2 + 4x + (1-i), \quad R = \mathbb{Z}[i]$;

(h) $x^3 + (2y+2)x + (y+1), \;\; R = \mathbb{Z}[y]$.

6. Mostre que os seguintes polinômios são irredutíveis em $\mathbb{Z}[x]$:

   (a) $x^4 + 6x^2 + 11x + 8$;

   (b) $x^4 + x^3 + x^2 + x + 1$;

   (c) $3x^3 + x^2 + 1$;

   (d) $2x^5 + 3x^4 - 2x^3 + 5x^2 + 1$;

   (e) $2x^7 + 1$.

7. Mostre que o polinômio

$$x^2 + (2+\sqrt{-3})x + (-2+\sqrt{-3}) \;\in\; \mathbb{Z}[\sqrt{-3}][x]$$

   é irredutível mas não é primo. É $\mathbb{Z}[\sqrt{-3}]$ um DFU?

8. Se $Car\,(F) = p$, com p primo, mostre que $(x+y)^p = x^p + y^p$, para todo $x,\; y \in F$.

9. Encontre o polinômio minimal de α sobre F, onde:

   (a) $\alpha = \dfrac{1+\sqrt{2}}{3};\; F = \mathbb{Q}$.

   (b) $\alpha = \dfrac{1+\sqrt{2}}{3};\; F = \mathbb{Q}(\sqrt{2})$.

   (c) $\alpha = e^{2\pi i/3};\; F = \mathbb{R}$.

   (d) $\alpha = e^{2\pi i/3};\; F = \mathbb{C}$.

   (a) $\alpha = \sqrt{2} + \sqrt{3};\; F = \mathbb{Q}$.

10. Mostre que $\mathbb{Q}(i\sqrt{3}) = \mathbb{Q}(e^{2\pi i/3})$.

11. Mostre que $\mathbb{Q}(e^3)$ é isomorfo à $\mathbb{Q}(1+\pi^2)$.

12. Mostre que $\mathbb{Q}(\sqrt{2})$ não é isomorfo à $\mathbb{Q}(\sqrt{3})$.

13. Se $F = \mathbb{Q}[x]/(x^2+x+1)$, mostre que F contém um elemento $\alpha \neq 1$ tal que $\alpha^3 = 1$.

14. Encontre um corpo com

    (a) 9 elementos.

    (b) 25 elementos.

    (c) 8 elementos.

    (d) 5^4 elementos.

15. Encontre:

    (a) $[\mathbb{Q}(\sqrt[4]{2}); \mathbb{Q}]$.

    (b) $[\mathbb{Q}(\sqrt[4]{2}); \mathbb{Q}(\sqrt{2})]$.

    (c) $[\mathbb{Q}(\sqrt[4]{2}, \sqrt{3}); \mathbb{Q}(\sqrt{2}, \sqrt{3})]$.

    (d) $[\mathbb{Q}(\sqrt{2}, \sqrt{3}); \mathbb{Q}]$.

    (e) $[\mathbb{Q}(\sqrt{2} + \sqrt{3}); \mathbb{Q}]$.

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

17. Encontre uma base para:

    (a) $\mathbb{Q}(\sqrt{2})$ sobre $\mathbb{Q}$.

    (b) $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ sobre $\mathbb{Q}$.

    (c) $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ sobre $\mathbb{Q}$.