unesp

UNIVERSIDADE ESTADUAL PAULISTA

Domínios Euclidianos e Inteiros Gaussianos

Simone Regina Guiselini Degrecci

INSTITUTO DE GEOCIÊNCIAS E CIÊNCIAS EXATAS

RIO CLARO/SP

2019

Universidade Estadual Paulista "Júlio de Mesquita Filho"
Instituto de Geociências e Ciências Exatas
Câmpus de Rio Claro

Domínios Euclidianos e Inteiros Gaussianos

Simone Regina Guiselini Degrecci

Dissertação apresentada como parte dos requisitos para obtenção do título de Mestre em Matemática, junto ao Programa de Pós-Graduação em Matemática, mestrado profissional, do Instituto de Geociências e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", Câmpus de Rio Claro.

Orientadora
Profa. Dra. Elíris Cristina Rizziolli

Rio Claro
2019

D321d

Degrecci, Simone Regina Guiselini
Domínios Euclidianos e Inteiros Gaussianos / Simone Regina Guiselini Degrecci. -- Rio Claro, 2019
63 p. + 1 CD-ROM

Dissertação (mestrado) - Universidade Estadual Paulista (Unesp), Instituto de Geociências e Ciências Exatas, Rio Claro
Orientadora: Elíris Cristina Rizziolli

1. Álgebra. 2. Domínio de Fatoração Única. 3. Domínio Euclidiano. 4. Inteiros Gaussianos. 5. Norma. I. Título.

Sistema de geração automática de fichas catalográficas da Unesp. Biblioteca do Instituto de Geociências e Ciências Exatas, Rio Claro. Dados fornecidos pelo autor(a).

Essa ficha não pode ser modificada.

TERMO DE APROVAÇÃO

Simone Regina Guiselini Degrecci

Domínios Euclidianos e Inteiros Gaussianos

Dissertação APROVADA como requisito parcial para a obtenção do grau de Mestre no Curso de Pós-Graduação em Matemática, mestrado profissional, do Instituto de Geociências e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", pela seguinte banca examinadora:

Profa. Dra. Elíris Cristina Rizziolli
Orientadora

Prof. Dr. Examinador I
Departamento - Universidade

Prof. Dr. Examinador II
Departamento - Universidade

Rio Claro, 2 de maio de 2019

Dedico este trabalho ao meu marido, meu porto seguro, companheiro de todas as horas, pela sua compreensão, respeito, tolerância e por continuar acreditando em nossa família.

Aos meus pais por me mostrarem que o estudo sempre vai me proporcionar algo melhor.

Agradecimentos

Primeiramente a Deus que me deu coragem e forças para enfrentar os desafios e permitiu a realização desse sonho.

Ao meu marido Junior Degrecci que esteve ao meu lado apoiando e compreendendo minhas angustias e ausências.

Aos meus pais e meus irmãos que sempre torceram por essa conquista.

A todos os amigos que me acompanharam e me incentivaram na caminhada até aqui.

Para minha orientadora Elíris pelos ensinamentos, por seu exemplo de profissional e pessoa humana. Por ser tão prestativa e atenciosa, pela enorme ajuda, por me motivar e acreditar em minha capacidade. Muito obrigada.

Todos os nossos sonhos podem se realizar, se tivermos a coragem de persegui-los.
Walt Disney

Resumo

A proposta deste trabalho é aprofundar os estudos sobre a estrutura algébrica dos anéis. Neste sentido tratamos dos Domínios de Fatoração Única (UFD), Domínios Euclidianos e do anel dos Inteiros Gaussianos, bem como resultados pertinentes neste contexto.

Palavras-chave: Álgebra, Domínio de Fatoração Única, Domínio Euclidiano, Inteiros Gaussianos, Norma.

Abstract

The purpose of this paper is to further study the algebraic structure of the rings. In this sense we deal with the Unique Factorization Domains Euclidean Domains and the Ring of the Gaussian Integers, as well as pertinent results in this context.

Keywords: Algebra, Unique Factorization Domains, Euclidean Domains, Gaussian Integers, Norms.

Sumário

Introdução

Nessa dissertação pretendemos aprofundar o estudo sobre a estrutura algébrica dos anéis. Trabalharemos com um tipo interessante de domínio de integridade, a saber, domínio euclidiano. O anel dos inteiros gaussianos será um exemplo importante de domínio euclidiano.

Usaremos como referência básica o livro [2] e será provado que todo domínio euclidiano é um domínio de ideais principais (PID) e também um domínio de fatoração única (UFD) e ainda estabeleceremos um algoritmo da divisão para este tipo de anel. Definiremos norma multiplicativa para um domínio de integridade e a partir desta definição mostraremos um exemplo interessante de um domínio de integridade que não é um domínio de fatoração única.

Para o desenvolvimento do texto admitimos conhecimento básico da estrutura algébrica: grupo.

No capítulo 1 apresentamos noções sobre a estrutura algébrica Anel. No capítulo 2 mostramos que todo domínio de ideais principais (PID) é um domínio de fatoração única. No capítulo 3 tratamos de domínios de integridade em que é possível estabelecer um algoritmo de divisão. E finalmente, no capítulo 4, apresentamos um exemplo não usual de domínio euclidiano.

1 Estrutura algébrica: anel

1.1 Noções de anel

Definição 1.1. *Uma terna $(A, +, .)$ em que A é um conjunto não vazio, $(+)$ e $(.)$ são operações binárias sobre A, é um anel, quando:*

1. *$(A, +)$ é um grupo abeliano;*
2. *Para quaisquer $a, b, c \in A : a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (associativa da multiplicação);*
3. *Para quaisquer $a, b, c \in A$, $a \cdot (b + c) = a \cdot b + a \cdot c$ e $(a + b) \cdot c = a \cdot c + b \cdot c$ (distributividade de $\cdot$ em relação $a +$ à esquerda e à direita).*

Ainda, dizemos que um anel $(A, +, .)$ é comutativo quando para todo $a, b \in A$ temos $a \cdot b = b \cdot a$. E dizemos que o anel A tem identidade (ou podemos dizer unidade) quando $\exists\ 1 \in A$: $a \cdot 1 = a = 1 \cdot a$, para todo $a \in A$.

Além disso, se $(A, +, .)$ é um anel com unidade 1, denotamos por $U(A)$, o conjunto dos elementos invertíveis em A, ou seja,

$$U(A) = \{a \in A \text{ tal que } \exists\ a^{-1} \in A, a \cdot a^{-1} = 1 = a^{-1} \cdot a\}$$

Observação 1.2. Quando necessário (para que fique mais claro no texto) denotaremos as operações de um anel A por $+_A$ e $\cdot_A$. Ainda, para a notação multiplicativa, denotaremos, por vezes $a \cdot b$ simplesmente por ab.

Exemplo 1.3.

1. $(\mathbb{Z}, +, .)$ é anel comutativo com unidade e $U(\mathbb{Z}) = \{-1, 1\}$.
2. $(\mathbb{Q}, +, .)$ é anel comutativo com unidade e $U(\mathbb{Q}) = \mathbb{Q}^* = \mathbb{Q} - \{0\}$.
3. $(\mathbb{R}, +, .)$ é anel comutativo com unidade e $U(\mathbb{R}) = \mathbb{R}^* = \mathbb{R} - \{0\}$.
4. $(\mathbb{C}, +, .)$ é anel comutativo com unidade e $U(\mathbb{C}) = \mathbb{C}^* = \mathbb{C} - \{0\}$.

Para tratar do próximo exemplo (e do lema 1.40), no qual apresentaremos a relação mod m com $m \in \mathbb{Z}_+$, recordemos a definição de relação de equivalência sobre um conjunto A: uma relação $\sim\ \subset A \times A$ é de equivalência quando satisfaz as seguintes propriedades:

1. Reflexiva: $\forall a \in A : a \sim a$.

2. Simétrica: $\forall a, b \in A$: se $a \sim b$ então $b \sim a$.

3. Transitiva: $\forall a, b, c \in A$: se $a \sim b$ e $b \sim c$ então $a \sim c$.

Exemplo 1.4. Seja $m \in \mathbb{Z}$, $m \geq 2$, e considere em $\mathbb{Z}$ a seguinte relação: $\forall a, b \in \mathbb{Z}$,

$$a \sim b \Leftrightarrow m \mid (a - b) \tag{1.1}$$

Ou seja,

$$a \sim b \Leftrightarrow \exists\, k \in \mathbb{Z} : a - b = km$$

Veja que tal relação é uma relação de equivalência. De fato:

(i) Reflexiva. Para qualquer $a \in \mathbb{Z}$, temos $a - a = 0$. Consequentemente, $a - a = 0.m$ Logo, $m \mid (a - a)$, ou seja, $a \sim a$. Portanto, $\forall a \in \mathbb{Z} : a \sim a$.

(ii) Simétrica. Sejam a, $b \in \mathbb{Z}$ tais que: $a \sim b$. Como $a \sim b$ segue que existe $k \in \mathbb{Z}$ tal que $a - b = km$. Assim, $b - a = -(-b + a) = -(a - b) = -(km) = (-k)m$. Ou seja, existe $l = -k \in \mathbb{Z}$ tal que $b - a = lm$. Consequentemente $b \sim a$. Portanto, mostramos que se $a \sim b$ então $b \sim a$.

(iii) Transitiva. Sejam a, b, $c \in \mathbb{Z}$ tais que: $a \sim b$ e $b \sim c$. Como $a \sim b$ existe $k \in \mathbb{Z}$ tal que $a - b = km$ e do fato que $b \sim c$ existe $l \in \mathbb{Z}$ tal que $b - c = lm$. Logo, $a - c = a + ((-b) + b) - c = (a - b) + (b - c) = km + lm = (k + l)m$, com $k + l \in \mathbb{Z}$. Ou seja, existe $j = k + l \in \mathbb{Z}$ tal que $a - c = jm$. Logo, $a \sim c$. Portanto mostramos que se $a \sim b$ e $b \sim c$ então $a \sim c$.

Pelos itens (i), (ii) e (iii) segue que $\sim$ é uma relação de equivalência. Neste caso denotamos $a \sim b$ por $a \equiv b \ mod\ m$ e lemos "a côngruo a b módulo m". Além disso, o conjunto quociente obtido por essa relação é denotado por $\mathbb{Z}_m$. Consequentemente, $\mathbb{Z}_m = \{\overline{a} : a \in \mathbb{Z}\}$, em que cada $\overline{a}$ é a classe de equivalência de a com a relação (1.1). Observe que $a \equiv b \bmod m$ implica em

$$a - b = km \Rightarrow a = b + km.$$

Mais ainda, se $a = b + km$ então $a = r + km$ com $0 \leqslant r < m$. Ou seja, para qualquer $a \in \mathbb{Z}$ temos $a \equiv r \bmod m$, com $0 \leq r < m$.
Assim, as classes de equivalência são: $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}$. Note que todas essas classes são distintas, pois se $\overline{s}_1 = \overline{s}_2$, com $0 \leq \overline{s}_1$, $\overline{s}_2 < m$, temos:

$$\overline{s}_1 = \overline{s}_2 \Leftrightarrow s_1 \equiv s_2 \bmod m \Leftrightarrow m \mid (s_1 - s_2).$$

Mas como $0 < s_1 - s_2 < m$ é impossível de se obter $m \mid (s_1 - s_2)$.
Portanto,

$$\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\}.$$

Em $\mathbb{Z}_m$ podemos definir a seguinte operação binária

$$\begin{array}{rccc} +_m : & \mathbb{Z}_m \times \mathbb{Z}_m & \to & \mathbb{Z}_m \\ & (\overline{a}, \overline{b}) & \mapsto & \overline{a} +_m \overline{b} := \overline{a + b} \end{array}$$

Veja que esta operação está bem definida pois: se $(\overline{a}, \overline{b}) = (\overline{c}, \overline{d})$ temos $\overline{a} = \overline{c}$ e $\overline{b} = \overline{d} \Rightarrow a - c = km$ e $b - d = lm$, para determinados k, $l \in \mathbb{Z}$.

Assim, $(a+b)-(c+d) = (a-c)+(b-d) = km+lm = (k+l)m \Rightarrow (a+b)-(c+d) = jm$, com $j = k + l \in \mathbb{Z}$. Ou seja, $a + b \equiv c + d \bmod m$, logo: $\overline{a + b} = \overline{c + d}$.
Tal operação dá a $\mathbb{Z}_m$ uma estrutura de grupo pois:

1. Associativa. $\forall \overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_m$.
   Segue que $\overline{a}+_m(\overline{b}+_m\overline{c}) = \overline{a}+_m\overline{(b+c)} = \overline{a+(b+c)} = \overline{(a+b)+c} = \overline{(a+b)}+_m\overline{c} = (\overline{a}+_m\overline{b})+_m c$, já que $a+(b+c) = (a+b)+c$ em $\mathbb{Z}$.

2. Elemento neutro. Considere $\overline{0} \in \mathbb{Z}_m$.
   Veja que para qualquer $\overline{a} \in \mathbb{Z}_m$ temos: $\overline{a}+_m\overline{0} = \overline{a+0} = \overline{a}$ e $\overline{0}+_m\overline{a} = \overline{0+a} = \overline{a}$, já que $a+0 = a = 0+a$ em $\mathbb{Z}$. Logo, $\overline{0}$ é o elemento de $\mathbb{Z}_m$.

3. Elemento simétrico. Seja $\overline{a} \in \mathbb{Z}_m$, qualquer.
   Veja que para $\overline{b} := \overline{m-a} \in \mathbb{Z}_m$, temos $\overline{a}+_m\overline{b} = \overline{a+b} = \overline{a+(m-a)} = \overline{(a-a)+m} = \overline{0+m} = \overline{m} = \overline{0}$ e $\overline{b}+_m\overline{a} = \overline{b+a} = \overline{(m-a)+a} = \overline{m+(-a+a)} = \overline{m+0} = \overline{m} = \overline{0}$, já que $a+(-a) = 0 = (-a)+a$ em $\mathbb{Z}$.

4. Comutativa. Sejam $\overline{a}, \overline{b} \in \mathbb{Z}_m$.
   Veja que $\overline{a}+_m\overline{b} = \overline{a+b} = \overline{b+a} = \overline{b}+_m\overline{a}$, já que $a+b = b+a$ em $\mathbb{Z}$.

Portanto, pelos itens verificados anteriormente, segue que $(\mathbb{Z}_m,+_m)$ é um grupo aditivo abeliano. Ainda em $\mathbb{Z}_m$ podemos definir outra operação binária, a saber:

$$\begin{array}{rccc} .{}_m: & \mathbb{Z}_m \times \mathbb{Z}_m & \to & \mathbb{Z}_m \\ & (\overline{a},\overline{b}) & \mapsto & \overline{a} \ .{}_m \ \overline{b} := \overline{ab} \end{array}$$

De modo análogo ao caso de $+_m$, segue que $(.{}_m)$ está bem definida. Veja agora que: $\forall\ \overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_m$, $\overline{a} \ .{}_m \ (\overline{b} \ .{}_m \ \overline{c}) = \overline{a(bc)} = \overline{(ab)c} = \overline{ab} \ .{}_m \ \overline{c} = (\overline{a} \ .{}_m \ \overline{b}) \ .{}_m \ \overline{c}$, já que $a(bc) = (ab)c$ em $\mathbb{Z}$.

Logo a operação $.{}_m$ é associativa.

Além disso: $\forall \overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_m$,
$\overline{a} \ .{}_m \ (\overline{b}+_m\overline{c}) = \overline{a} \ .{}_m \ \overline{(b+c)} = \overline{a(b+c)} = \overline{ab+ac} = \overline{ab}+_m\overline{ac} = \overline{a} \ .{}_m \ \overline{b} + \overline{a} \ .{}_m \ \overline{c}$, já que $a(b+c) = ab+ac$ em $\mathbb{Z}$.

Também, $(\overline{a}+_m\overline{b}) \ .{}_m \ \overline{c} = \overline{(a+b)} \ .{}_m \ \overline{c} = \overline{(a+b) \ . \ c} = \overline{ac+bc} = \overline{ac}+_m\overline{bc} = \overline{a} \ .{}_m \ \overline{c}+_m\overline{b} \ .{}_m \ \overline{c}$, já que $(a+b)c = ac+bc$ em $\mathbb{Z}$.

Portanto, valem as distributivas à direita e à esquerda para as operações $+_m$ e $.{}_m$. Com isso provamos que $(\mathbb{Z}_m, +_m, .{}_m)$ é um anel.

Mais ainda, $\mathbb{Z}_m$ é um anel comutativo pois: $\forall \overline{a}, \overline{b} \in \mathbb{Z}_m$, $\overline{a} \ .{}_m \ \overline{b} = \overline{ab} = \overline{ba} = \overline{b} \ .{}_m \ \overline{c}$, já que $ab = ba$ em $\mathbb{Z}$.

Além disso, $\overline{1} \in \mathbb{Z}_m$ é tal que: $\forall\ \overline{a} \in \mathbb{Z}_m$, $\overline{a} \ .{}_m \ \overline{1} = \overline{a1} = \overline{a} = \overline{1a} = \overline{1} \ .{}_m \ \overline{a}$, já que $a1 = a = 1a$ em $\mathbb{Z}$.

Consequentemente, pelo exposto, podemos concluir finalmente que $(\mathbb{Z}_m, +_m, .{}_m)$ é um anel comutativo com unidade.

Definição 1.5. *Dizemos que um anel $(A,+,.)$ é um corpo quando: A é comutativo com unidade e $U(A) = A - \{0\} = A^*$, em que $\{0\}$ representa o conjunto formado pelo elemento neutro de $(A,+)$, ou seja, quando: $(A,+)$ e $(A^*,.)$ são grupos abelianos e valem as distributivas à esquerda e à direita.*

Exemplo 1.6.

1. $(\mathbb{R},+,.)$ com as operações usuais é um corpo.

2. $(\mathbb{Z}_p,+,.)$ em que p é um número primo, é um corpo finito, como veremos mais adiante.

Definição 1.7. *Sejam A um anel $(A,+,.)$ e $L \subset A$, $L \neq \varnothing$. Dizemos que L é um subanel de A quando:*

1. *L é subgrupo de $(A,+)$. Notação: $L \leqslant (A,+)$.*
2. *Para todos $a,b \in L : ab \in L$.*

Exemplo 1.8.

1. $\mathbb{Z}[i] := \{a+bi : a,b \in \mathbb{Z}\}$ é um subanel de $\mathbb{C}$ e consequentemente $\mathbb{Z}[i]$ é um anel comutativo com unidade, a qual é igual a unidade de $\mathbb{C}$.
2. $\mathbb{Z}[\sqrt{-5}] = \{a+ib\sqrt{5} \mid a,b \in \mathbb{Z}\}$ é um subanel de $\mathbb{C}$ e consequentemente $\mathbb{Z}[\sqrt{-5}]$ é um anel comutativo com unidade, a qual é igual a unidade de $\mathbb{C}$.

Definição 1.9. *Dizemos que um anel comutativo com unidade $(A,+,.)$ é um domínio de integridade quando: para todo $a,b \in A : ab = 0 \Rightarrow a = 0$ ou $b = 0$.*

Exemplo 1.10.

1. $(\mathbb{Z}_6,+,.)$ é anel comutativo com unidade, porém não é domínio de integridade pois: $\overline{2} \neq \overline{0}$ e $\overline{3} \neq \overline{0}$ mas $\overline{2}.\overline{3} = \overline{6} = \overline{0}$ ou seja, $\overline{2}$ e $\overline{3}$ são divisores do zero.
2. $(\mathbb{Z},+,.)$, $(\mathbb{Q},+,.)$ são domínios de integridade, pois: $\forall a,\ b \in R$, $ab = 0 \Rightarrow a = 0$ ou $b = 0$, para $R = \mathbb{Z}$ ou $R = \mathbb{Q}$.

Definição 1.11. *Sejam $(A,+_A,.{}_A)$ e $(B,+_B,.{}_B)$ anéis, quaisquer. Definimos como produto direto entre A e B, o produto cartesiano $A \times B$ munido das operações:*
Para quaisquer $(a_1,b_1),(a_2,b_2) \in A \times B$:

1. $(a_1,b_1) + (a_2,b_2) := (a_1 +_A a_2, b_1 \ +_B \ b_2)$,
2. $(a_1,b_1).(a_2,b_2) := (a_1 \ ._A \ a_2, b_1 \ ._B \ b_2)$.

Veja que se A e B forem anéis comutativos então $A \times B$ é comutativo. Ainda, se A e B tem unidades 1_A e 1_B, respectivamente, então o anel $A \times B$ também tem unidade a saber: $1 := (1_A, 1_B)$.

Entretanto, se A e B são domínios de integridade não podemos garantir que $A \times B$ é domínio, pois se $(a,0),(0,b) \in A \times B$, com $a \neq 0$ e $b \neq 0$, temos:

$$(a,0) \neq (0,0) \text{ e } (0,b) \neq (0,0) \text{ tais que } (a,0).(0,b) = (a0,b0) = (0,0).$$

Proposição 1.12. *Seja $(A,+,.)$ anel comutativo com unidade, qualquer.*

$$A \text{ é domínio de integridade} \Leftrightarrow \forall a,b \in A, a \neq 0 : ab = ac \Rightarrow b = c.$$

Demonstração.

($\Rightarrow$) Suponha $ab = ac$, com $a \neq 0$. Veja que $ab = ac \Rightarrow ab - ac = 0 \Rightarrow a(b-c) = 0$, como A é um domínio de integridade e $a \neq 0$ segue que, necessariamente, $b-c = 0$ e consequentemente que $b = c$.

($\Leftarrow$) Suponha: $\forall a,b \in A,\ ab = 0$. Se $a = 0$ está provado. Se $a \neq 0$, $ab = 0 = a0 \Rightarrow ab = a0 \Rightarrow b = 0$. Logo A é um domínio de integridade.

□

Corolário 1.13. *Todo corpo K é um domínio de integridade.*

Demonstração.

Sendo K um corpo, segue que em particular é um anel comutativo com unidade. Além disso, veja que se $a, b, c \in K$ com $a \neq 0$, temos:

$$ab = ac \Rightarrow a^{-1}(ab) = a^{-1}(ac) \Rightarrow (a^{-1}a)b = (a^{-1}a)c \Rightarrow 1b = 1c \Rightarrow b = c.$$

Pela proposição 1.12 K é domínio de integridade. □

Teorema 1.14. *Todo domínio de integridade finito é um corpo.*

Demonstração.

Seja A um domínio de integridade finito. Logo, A é um anel comutativo com unidade e para A ser um corpo resta mostrar que $U(A) = A^*$. Seja $a \in A, a \neq 0$, qualquer. Provemos que existe $b \in A$ tal que $ab = 1$, ou seja, $b = a^{-1}$. Como A é finito, suponha que A tenha n elementos, digamos: $A = \{a_1, \ldots, a_n\}$ e considere o conjunto $J = \{aa_1, aa_2, \ldots, aa_n\}$.

Veja que a aplicação

$$\begin{array}{rccc} f: & A & \to & J \\ & a_i & \mapsto & f(a_i) = aa_i \end{array}$$

para todo $i \in \{1, \ldots, n\}$, é injetora, pois: $f(a_i) = f(a_j)$ então $aa_i = aa_j$ implica que $a_i = a_j$ visto que $a \neq 0$ e A é domínio de integridade (veja proposição 1.12).

Logo, Imf e A têm o mesmo número de elementos. Além disso, f é sobrejetora, pois para qualquer $y = aa_i \in J$ temos que $f(a_i) = aa_i = y$, com $a_i \in A$. Portanto, $Imf = J$, ou seja, A e J têm o mesmo número de elementos e como $J \subseteq A$, segue que, necessariamente, $J = A$. Em particular, $1 \in A = J$ logo, $1 \in J$ e então existe $a_i \in A$ tal que $1 = aa_i$. Ou seja, existe $a_i \in A$ tal que $aa_i = 1$ então a_i é inverso de a. Portanto, $U(A) = A^*$. □

Lema 1.15. *$\mathbb{Z}_m$ é domínio de integridade se, e somente se, m é primo.*

Demonstração.

($\Rightarrow$) Suponha que $\mathbb{Z}_m$ é um domínio de integridade e que m não é primo.
Se m não é primo, existem $r, s \in \mathbb{Z}$ com $1 < r, s < m$ tais que $m = rs$.
Assim, temos: $\overline{r} \neq \overline{0}$ e $\overline{s} \neq \overline{0}$ e $\overline{r}\ \overline{s} = \overline{rs} = \overline{m} = \overline{0}$, ou seja, existem $\overline{r} \neq \overline{0}$ e $\overline{s} \neq \overline{0}$ em $\mathbb{Z}_m$ com $\overline{r}\ \overline{s} = \overline{0}$ o que é absurdo pois, supomos que $\mathbb{Z}_m$ é domínio de integridade. Portanto, m é primo.

($\Leftarrow$) Já sabemos que $\mathbb{Z}_m$ é um anel comutativo com unidade pelo exemplo 1.4. Além disso, veja que $\mathbb{Z}_m$, com m primo, não tem divisores de zero, pois: para quaisquer $\overline{a}, \overline{b} \in \mathbb{Z}_m$ tais que $\overline{a}\overline{b} = \overline{0}$, segue que $\overline{ab} = \overline{0}$, ou seja, $m \mid ab$. Logo, $m \mid a$ ou $m \mid b$. Então $\overline{a} = \overline{0}$ ou $\overline{b} = \overline{0}$.
Portanto, $\mathbb{Z}_m$ é domínio de integridade.

□

Corolário 1.16. *$\mathbb{Z}_m$ é corpo se, e somente se, m é primo.*

Demonstração. ($\Rightarrow$) Se $\mathbb{Z}_m$ é corpo então $\mathbb{Z}_m$ é um domínio de integridade pelo corolário 1.13 . Sendo assim, pelo lema 1.15 segue que m é primo.

($\Leftarrow$) Se m é primo então $\mathbb{Z}_m$ é um domínio de integridade pelo lema 1.15. Como $\mathbb{Z}_m$ é finito, segue do teorema 1.14 que $\mathbb{Z}_m$ é um corpo.

□

Seja D um domínio de integridade qualquer. Considere em $D \times D^*$ a seguinte relação

$$(a,b) \sim (c,d) \Leftrightarrow ad = bc. \tag{1.2}$$

Veja que tal relação é de equivalência pois:

(i) Reflexiva. Para qualquer $(a,b) \in D \times D^*$ temos $ab = ba$, pois D é, em particular, anel comutativo, logo por (1.2): $(a,b) \sim (a,b)$.

(ii) Simétrica. Para quaisquer $(a,b),(c,d) \in D \times D^*$, se $(a,b) \sim (c,d)$ então

$$ad = bc. \tag{1.3}$$

Mas como D é, em particular, anel comutativo, de (1.3) segue que:

$$da = cb \Rightarrow cb = da \Rightarrow (c,d) \sim (a,b).$$

Ou seja, se $(a,b) \sim (c,d)$ então $(c,d) \sim (a,b)$.

(iii) Transitiva. Para quaisquer $(a,b),(c,d),(e,f) \in D \times D^*$, se $(a,b) \sim (c,d)$ e $(c,d) \sim (e,f)$ então:

$$ad = bc \tag{1.4}$$

e

$$cf = de. \tag{1.5}$$

Multiplicando (1.4) por f e (1.5) por b temos: $adf = bcf$ e $cfb = deb$. Assim, $adf = bcf = deb \Rightarrow afd = ebd \Rightarrow af = eb \Rightarrow (a,b) \sim (e,f)$.

Para cada $(a,b) \in D \times D^*$ denotamos a classe de equivalência $\overline{(a,b)}$ por $\frac{a}{b}$. É possível munir o conjunto quociente $K = \left\{\frac{a}{b}, a \in D \text{ e } b \in D^*\right\}$ com as seguintes operações: $\forall\ \frac{a}{b}, \frac{c}{d} \in K$:

$$\frac{a}{b} + \frac{c}{d} := \frac{ad + bc}{bd}$$

e

$$\frac{a}{b} . \frac{c}{d} := \frac{ac}{bd}.$$

É possível mostrar que tais operações estão bem definidas e ainda que $(K, +, .)$ é um corpo, para mais detalhes veja [1], páginas $256 - 259$.

Definição 1.17. *Tal corpo $(K, +, .)$ definido acima é denominado Corpo das Frações de D.*

Definição 1.18. *Sejam $(A, +, .)$ e $(B, +, .)$ anéis, quaisquer. Dizemos que uma aplicação $f : A \to B$ é um homomorfismo de anéis quando: $\forall a, b \in A$:*

1. $f(a + b) = f(a) + f(b)$;
2. $f(a \cdot b) = f(a) \cdot f(b)$.

Se f é uma bijeção e homomorfismo, dizemos que f é um isomorfismo. Além disso, A e B são anéis isomorfos, $A \simeq B$, quando existe um isomorfismo f de A em B.

Definição 1.19. *Seja $f : A \to B$ um homomorfismo de anéis, qualquer. Definimos o núcleo de f, $N(f)$, como sendo:*

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

Teorema 1.20. *Se $f : A \to B$ é um homomorfismo de anéis, então:*

$$f \text{ é injetora se, e somente se, } N(f) = \{0_A\}.$$

Demonstração.

($\Rightarrow$) Suponha que f seja injetora. Se $a \in N(f)$ então $f(a) = 0 = f(0)$. Ou seja, $f(a) = f(0)$. Pela injetividade de f segue que $a = 0$. Portanto, $N(f) = \{0\}$.

($\Leftarrow$) Suponha que $N(f) = \{0\}$. Mostremos que f é injetora. Para tanto consideremos $x, y \in A$ tais que $f(x) = f(y)$ ou equivalentemente $f(x) - f(y) = 0$. Sendo f um homomorfismo, temos que $f(x) - f(y) = 0$ implica $f(x - y) = 0$ de onde podemos concluir que $x - y \in N(f) = \{0\}$. Logo, $x - y = 0$ ou seja, $x = y$.

□

Lema 1.21. *Se $f : A \to B$ é homomorfismo qualquer, de anéis, então são válidas:*

1. $f(0_A) = 0_B$;
2. *Se A tem elemento unidade, 1_A, e f é sobrejetora então B tem unidade a saber:* $1_B = f(1_A)$;
3. $f(-a) = -f(a)$, $\forall a \in A$;
4. *Se $a \in A$ é invertível e f é sobrejetora, então $f(a) \in B$ é invertível e ainda* $(f(a))^{-1} = f(a^{-1})$.

Demonstração.

1. $f(0_A) = 0_B$, pois:
   $f(0_A) = f(0_A + 0_A) = f(0_A) + f(0_A) \Rightarrow f(0_A) - f(0_A) = f(0_A) + (f(0_A) - f(0_A)) \Rightarrow$
   $0_B = f(0_A)$.

2. 1_A é unidade de A. Para cada $y \in B$, como f é sobrejetora, existe $x \in A$ tal que $y = f(x)$. Assim:

$$f(1_A)y = f(1_A)f(x) = f(1_A x) = f(x) = y$$

e

$$yf(1_A) = f(x)f(1_A) = f(x1_A) = f(x) = y.$$

Portanto, $f(1_A) = 1_B$.

3. $f(-a) = -f(a)$, de fato: $f(a) + f(-a) = f(a-a) = f(0_A) = 0_B$. Além disso: $f(-a) + f(a) = f(-a+a) = f(0_A) = 0_B$. Portanto, $-f(a) = f(-a)$.

4. $a \in A$ é invertível, logo existe $a^{-1} \in A$ tal que $aa^{-1} = 1_A = a^{-1}a$. Daí:
$f(a) \cdot f(a^{-1}) = f(a \cdot a^{-1}) = f(1_A) = 1_B$ e $f(a^{-1}) \cdot f(a) = f(a^{-1} \cdot a) = f(1_A) = 1_B$.
Portanto, $f(a^{-1}) = (f(a))^{-1}$.

□

Definição 1.22. *Sejam A um anel comutativo e $I \subset A$, $I \neq \varnothing$. Dizemos que I é um ideal de A, quando:*

1. *I é subgrupo de $(A, +)$ (Notação: $I \leqslant A$);*
2. *$\forall a \in A, \forall x \in I : ax \in I$.*

Observação 1.23. $\{0\}$ e A são ideais de A chamados ideais triviais. Veja ainda que como A é comutativo; $\forall a \in A$, $\forall x \in I : xa \in I$.

Lema 1.24. *Sejam A um anel comutativo com unidade e I um ideal de A. Se existe $u \in U(A)$ tal que $u \in I$ então $I = A$. Em particular, se $1_A \in I$ então $I = A$.*

Demonstração.
Mostremos primeiramente que se $1_A \in I$ então $I = A$. De fato,

- $I \subset A$ pela definição.
- $A \subset I$, pois: $\forall a \in A$, $a = a1_A \in I$, o que implica $a \in I$. Portanto, $I = A$.

Provemos agora que se u é um elemento invertível de A tal que $u \in I$ então $I = A$. Com efeito, seja $u^{-1} \in A$ o inverso de u, assim: $1_A = u^{-1}u \in I \Rightarrow 1_A \in I \Rightarrow I = A$. □

Lema 1.25. *Sejam A um anel comutativo e $a_1, a_2, ..., a_n \in A$, quaisquer. O subconjunto de A dado por:*

$$\langle a_1, a_2, ..., a_n \rangle = \left\{ \sum_{i=1}^{n} \alpha_i a_i : \alpha_i \in A \right\}$$

é um ideal de A, denominado ideal gerado por $a_1, a_2, ..., a_n$.
Em particular, chamamos $\langle a \rangle = \{\alpha a : \alpha \in A\}$ de ideal principal de A gerado por a.

Demonstração.

- Sabemos que $\langle a_1, ..., a_n\rangle \leq (A, +)$;
- $\forall a \in A, \forall x \in \langle a_1, ..., a_n\rangle$: $ax = a\sum_{i=1}^{n} \alpha_i a_i = \sum_{i=1}^{n} (a\alpha_i)a_i \in \langle a_1, ..., a_n\rangle$.

□

Lema 1.26. *Se $f : A \to B$ é um homomorfismo de anéis, com A comutativo, então o núcleo de f, $N(f)$, é um ideal de A.*

Demonstração.

- $N(f) \leqslant (A, +)$ pois $\forall x, y \in N(f) : (-x) + y \in N(f)$, já que $f((-x) + y) = f(-x) + f(y) = -f(x) + f(y) = -0 + 0 = 0 \Rightarrow f((-x) + y) = 0$.
- $\forall a \in A$, $\forall x \in N(f)$ temos $ax \in N(f)$, pois: $f(ax) = f(a)f(x) = f(a)0 = 0$, logo, $f(ax) = 0$ e consequentemente $ax \in N(f)$.

□

Exemplo 1.27.
Sejam $A = \mathbb{Z}$ e $I = \langle n\rangle$. Veja que I é ideal de A, pois: $\forall a \in \mathbb{Z}, \forall x \in \langle n\rangle$: $ax = a(kn) = (ak)n \in \langle n\rangle = I$, para algum $k \in A$.

Proposição 1.28. *Seja $(A, +, .)$ um anel comutativo com unidade, qualquer.*

A é um corpo se, e somente se, os únicos ideais de A são os triviais: $\{0\}$ e A.

Demonstração.

($\Rightarrow$) Se $I = \{0\}$, I é um ideal trivial de A. Se $I \neq \{0\}$ é um ideal de A, existe $x \in I$, $x \neq 0$. Daí, $0 \neq x \in I \subset A$. Como A é corpo e $x \neq 0$ segue que $x \in U(A)$. Logo, pelo lema 1.24 temos $I = A$. Portanto, os únicos ideais de A são: $\{0\}$ e A.

($\Leftarrow$) Como A é comutativo com unidade resta mostrar que todo elemento $a \in A$, $a \neq 0$ é invertível. Para isso, considere o ideal $\langle a\rangle \subset A$.
Por hipótese, $\langle a\rangle = \{0\}$ ou $\langle a\rangle = A$, mas $a \neq 0$, logo $\langle a\rangle = A$.
Daí, como $1 \in A = \langle a\rangle = \{\alpha a : \alpha \in A\}$ segue que $1 = \alpha a$ para algum $\alpha \in A$.
Portanto, $a \in U(A)$.

□

Lema 1.29. *Seja $f : A \to B$ um homomorfismo de anéis comutativos.*

1. *Se $I \subset A$ é um ideal de A então $f(I)$ é um ideal de Imf.*
2. *Se J é um ideal de imagem f então a imagem inversa $f^{-1}(J)$ é um ideal de A.*

Demonstração. 1. Sabemos que $f(I) \leqslant (Imf, +)$. Além disso, para qualquer $b \in Imf$, existe $a \in A$ tal que $f(a) = b$. Para todo $y \in f(I)$ tem-se que $y = f(x)$, $x \in I$. Assim, $by = f(a)f(x) = f(ax) \in f(I)$, pois sendo I um ideal de A tem-se que $ax \in I$. Portanto, $by \in f(I)$.

2. $f^{-1}(J) \leqslant (A,+)$. De fato: $\forall a_1, a_2 \in f^{-1}(J)$ tem-se $f(a_1)$, $f(a_2) \in J$. Segue que $-f(a_1) + f(a_2) \in J$, pois J é um ideal da imagem de f. Mas, $f((-a_1) + a_2) = f(-a_1) + f(a_2) = -f(a_1) + f(a_2)$. Portanto, $f((-a_1) + a_2) \in J \Rightarrow (-a_1) + a_2 \in f^{-1}(J)$. Além disso, $\forall a \in A$, $\forall x \in f^{-1}(J) : ax \in f^{-1}(J)$, pois, como $x \in f^{-1}(J), f(x) \in J$, e $f(a) \in Imf$. Assim, $f(ax) = f(a)f(x) \in J \Rightarrow f(ax) \in J \Rightarrow ax \in f^{-1}(J)$.

□

Proposição 1.30. *Se I e J são ideais de um anel comutativo A então:*

1. *$I \cap J$ é ideal de A.*

2. *$I + J = \{x +_A y : x \in I, y \in J\}$ é um ideal de A.*

Demonstração.

1. $I \cap J \leqslant (A,+)$: $\forall u, v \in I \cap J$, então, $u, v \in I \cap J \Rightarrow u \in I$ e $u \in J$; $v \in I$ e $v \in J$. Como I e J são subgrupos com $u, v \in I$ e $u, v \in J$ temos $-u + v \in I$ e $-u + v \in J$, logo, $-u + v \in I \cap J$. Além disso, $\forall a \in A$, $\forall u \in I \cap J$, temos $u \in I \cap J \Rightarrow u \in I$ e $u \in J$. Como I e J são ideais de A, temos: $au \in I$ e $au \in J \Rightarrow au \in I \cap J$.

2. $I + J \leqslant (A,+)$, pois $\forall u, v \in I + J : -u + v \in I + J$ já que sendo $u \in I + J$ então $u = x_1 + y_1$, $x_1 \in I, y_1 \in J$ e $v \in I + J$, logo, $v = x_2 + y_2$, $x_2 \in I$, $y_2 \in J$.
Daí: $(-u) + v = -(x_1 + y_1) + (x_2 + y_2) = -y_1 - x_1 + x_2 + y_2 = (-x_1 + x_2) + (-y_1 + y_2) \in I + J$. Além disso, $\forall a \in A, \forall u \in I + J : au \in I + J$. De fato: temos $u = x + y$, $x \in I$ e $y \in J$. Logo: $au = a(x + y) = ax + ay \in I + J$, pois I e J são ideais de A.

□

Observação 1.31.

1. $I \cap J$ é o maior ideal contido em I e em J.

2. I + J é o menor ideal que contém I e J.

Definição 1.32. *Sejam A um anel comutativo e P ideal de A, $P \neq A$. Dizemos que P é ideal primo quando: $\forall a, b \in A : ab \in P \Rightarrow a \in P$ ou $b \in P$.*

Exemplo 1.33.

1. $A = \mathbb{Z}$, $P = \langle p \rangle$, p número primo, $A \neq P$, $1 \notin P$.
Sejam $ab \in \mathbb{Z}$ tais que $ab \in P = \langle p \rangle$. Como $ab \in \langle p \rangle = \{kp : k \in \mathbb{Z}\}$ então $ab = kp$, para algum $k \in \mathbb{Z}$. Então, $p \mid (ab) \Rightarrow p \mid a$ ou $p \mid b \Rightarrow a = k_1 p$ ou $b = k_2 p \Rightarrow a \in \langle p \rangle$ ou $b \in \langle p \rangle \Rightarrow a \in P$ ou $b \in P$. Assim, $ab \in P \Rightarrow a \in P$ ou $b \in P$. Portanto, P é primo.

2. Se A é um domínio de integridade, então $P = \{0\}$ é um ideal primo. De fato, $\forall a, b \in A : ab \in P = \{0\} \Rightarrow ab = 0 \Rightarrow a = 0$ ou $b = 0 \Rightarrow a \in P = \{0\}$ ou $b \in P = \{0\}$.

Definição 1.34. *Sejam A anel comutativo e $M \subset A$, $M \neq A$, ideal. Dizemos que M é ideal maximal quando: se $J \subset A$ é um ideal, tal que $J \neq M$ e $M \subsetneqq J \subset A$ então $J = A$.*

Observação 1.35. Se A é anel comutativo com unidade 1, para mostrar que M é um ideal maximal supomos $J \subset A$ ideal, $J \neq M$ tal que $M \subsetneqq J \subset A$ e mostramos que: $1 \in J$, já que $1 \in J$, implica $J = A$.

Exemplo 1.36.
Sejam $A = \mathbb{Z}$ e $M = \langle 2 \rangle$. Mostremos que M é um ideal maximal de A. Veja que: $M = \langle 2 \rangle$ e $M \neq A$ pois $1 \notin M$. Suponha agora J ideal de $\mathbb{Z}$ tal que $J \neq M$ e $M \subsetneqq J \subset \mathbb{Z}$. Então existe $x \in J$ tal que $x \notin M$.
Agora: $x \notin M = \langle 2 \rangle \Rightarrow x$ não é par $\Rightarrow x$ é ímpar $\Rightarrow x = 2k + 1$, $k \in \mathbb{Z}$. Assim, $1 = (2k + 1) - 2k \Rightarrow 1 \in J \Rightarrow J = A$.

Teorema 1.37. *Seja A um anel comutativo com unidade 1. Se M é um ideal maximal de A então M é um ideal primo.*

Demonstração. Suponha M ideal maximal e que $a, b \in A$ sejam tais que $ab \in M$ e $a \notin M$. Como $a \notin M$, temos que $\langle a \rangle + M \neq M$ e portanto,

$$M \subsetneqq \langle a \rangle + M \subset A. \tag{1.6}$$

Como M é maximal, segue de (1.6), segue que: $\langle a \rangle + M = A$. Como $1 \in A = \langle a \rangle + M$, segue que $1 = u+v$, em que $u \in \langle a \rangle$ e $v \in M$. Podemos, então, escrever $1 = ka+v$, para algum $k \in A$ com $v \in M$. Daí, $b1 = b(ka + v)$ implica $b = b(ka) + bv = k(ab) + bv = k(ab) + bv \in M$.
Ou seja, se $ab \in M$ e $a \notin M$ então $b \in M$. Logo, M é ideal primo. □

Definição 1.38. *Seja A domínio de integridade, qualquer. Dizemos que A é domínio de ideais principais (denotado PID) quando todo ideal I de A é um ideal principal, isto é, quando existe $a \in A$ tal que $I = \langle a \rangle$.*

Exemplo 1.39.
$\mathbb{Z}$ é um PID. Já sabemos que $\mathbb{Z}$ é domínio de integridade. Mostremos que todo ideal é principal. Seja $I \subset \mathbb{Z}$, ideal qualquer. Vamos determinar $a_0 \in \mathbb{Z}$ tal que $I = \langle a_0 \rangle$.

- Se $I = \{0\}$ então $I = \langle 0 \rangle$.
- $I \neq \{0\}$ existe um $b \in I$, $b \neq 0$ ($b > 0$ ou $b < 0$).

Considere o conjunto: $S = \{x \in I : x > 0\}$. Segue que $S \neq \emptyset$ pois $b \in S$ ou $(-b) \in S$ e S é limitado inferiormente por $0 \in \mathbb{Z}$. Logo, nestas condições, pelo Princípio do Menor Inteiro[1] segue que S tem elemento minimal, digamos $a_0 \in S$, logo $a_0 \in I$ e $a_0 > 0$.

Afirmação: $I = \langle a_0 \rangle$. De fato,

1. $\langle a_0 \rangle \subset I$:
   $\forall x \in \langle a_0 \rangle \Rightarrow x = ka_0$ e como $a_0 \in I$, então $x \in I$, pois I é um ideal.

[1]Princípio do Menor Inteiro: "Seja $S \neq \emptyset$ um subconjunto do conjunto dos números inteiros, $\mathbb{Z}$. Se S admite alguma cota inferior em $\mathbb{Z}$ então S possui elemento mínimo, ou seja, existe $a_0 \in S$ tal que $a_0 \leq s$, $\forall\, s \in S$".

2. $I \subset \langle a_0 \rangle$: seja $x \in I$, qualquer, pelo algorítmo da divisão em $\mathbb{Z}$, temos que existem $q, r \in \mathbb{Z}, 0 \leqslant r < a_0$ tais que $x = a_0 q + r \Rightarrow r = x - a_0 q \in I$, pois I é ideal e $x, a_0 \in I$, e ainda $0 \leqslant r < a_0$. Se $r \in I$ e $r > 0$ então $r \in S$, com $r < a_0$, o que é absurdo pois a_0 é o elemento minimal de S. Logo, necessariamente: $r = 0$ e $x = a_0 q + r = a_0 q + 0 = a_0 q \in \langle a_0 \rangle$.

   Por (1) e (2) temos $I = \langle a_0 \rangle$.

O objetivo agora é definir anel quociente e para isso precisamos estabelecer primeiramente a seguinte relação de equivalência.

Lema 1.40. *Se A é um anel comutativo e $I \subset A$ um ideal então a seguinte relação $(\sim)$: $\forall a, b \in A$*

$$a \sim b \Leftrightarrow a - b \in I$$

é uma relação de equivalência.

Demonstração. Veja que,

1. Reflexiva: $\forall a \in A : a - a = 0 \in I \Rightarrow a - a \in I \Leftrightarrow a \sim a$.

2. Simétrica: $\forall a, b \in A$
   $a \sim b \Rightarrow a - b \in I \Rightarrow -(a - b) \in I \Rightarrow b - a \in I \Rightarrow b \sim a$.

3. Transitiva: $\forall a, b, c \in A$
   $a \sim b$ e $b \sim c \Rightarrow a - b \in I$ e $b - c \in I$, Daí: $a - c = a + (-b + b) - c = (a - b) + (b - c) \in I$ e, portanto $a \sim c$.

Portanto, $(\sim)$ é relação de equivalência. □

Observação 1.41. Cada classe de equivalência $\overline{a}$ é tal que: $\overline{a} := \{b \in A : b \sim a\} = \{b \in A : b - a \in I\} = \{b \in A : b - a = r, r \in I\} = \{b \in A : b = a + r, r \in I\} = a + I$ e obtemos o conjunto quociente $\frac{A}{\sim} = \{\overline{a}, a \in A\} = \{a + I, a \in A\}$, que será denotado por $\frac{A}{I}$.

Proposição 1.42. *Sejam $(A, +, .)$ um anel comutativo e I um ideal de A. A terna $\left(\frac{A}{I}, +, \cdot\right)$ em que $(+)$ e $(\ \cdot\ )$ são operações:*

$$\forall a + I,\ b + I \in \frac{A}{I},$$

$(+) : (a + I) + (b + I) := (a +_A b) + I$
$(\ \cdot\ ) : (a + I) \cdot (b + I) := (a \cdot_A b) + I$
é um anel comutativo, denominado anel quociente de A por I.

Demonstração.

$(+)$: Temos $(A, +)$ grupo abeliano e $I \leqslant (A, +)$, logo I é subgrupo normal de A. Então $\left(\frac{A}{I}, +\right)$ é grupo abeliano, em particular, $(+)$ está bem definida. Mostremos que $(\ \cdot\ )$ está bem definida: $\forall (a + I), (b + I), (c + I), (d + I) \in \frac{A}{I}$ tais que:

$$(a+I, b+I) = (c+I, d+I) \Rightarrow a+I = c+I \text{ e } b+I = d+I.$$

Agora, mostremos que: $(a+I).(b+I) = (c+I).(d+I)$, ou seja, $(ab)+I = (cd)+I$, equivalentemente $(ab-cd) \in I$. Queremos mostrar então que $(ab-cd) \in I$. Temos: $a+I = c+I$ e $b+I = d+I \Rightarrow (a-c) \in I$ e $(b-d) \in I$, $b(a-c) \in I$ e $c(b-d) \in I \Rightarrow b(a-c)+c(b-d) \in I \Rightarrow (ba-bc+cb-cd) \in I \Rightarrow (ab-cd) \in I$.

Verifiquemos as propriedades; em cada uma delas usamos fortemente o fato de que $(A, +, .)$ é um anel comutativo e I é um ideal de A :

1. Associativa: $\forall (a+I), (b+I), (c+I) \in \dfrac{A}{I}$,
   $((a+I)(b+I))(c+I) = (ab+I)(c+I) = (ab)c+I = a(bc)+I = (a+I)(bc+I) = (a+I)((b+I)(c+I))$.

2. Comutativa: $\forall (a+I), (b+I), (c+I) \in \dfrac{A}{I}$,
   $(a+I)(b+I) = ab+I = ba+I = (b+I)(a+I)$.

3. Distributiva: $\forall (a+I), (b+I), (c+I) \in \dfrac{A}{I}$,

   - $[(a+I)+(b+I)](c+I) = [(a+b)+I](c+I) = (a+b)c+I = (ac+bc)+I = (ac+I)+(bc+I) = (a+I)(c+I)+(b+I)(c+I)$.

   - $(a+I)[(b+I)+(c+I)] = (a+I)[(b+c)+I] = a(b+c)+I = (ab+ac)+I = (ab+I)+(ac+I) = (a+I)(b+I)+(a+I)(c+I)$.

Portanto, $\left(\dfrac{A}{I}, +, .\right)$ é um anel comutativo. □

Exemplo 1.43. Sejam A anel comutativo e $I \subset A$ ideal, qualquer.

$$\begin{array}{rccc} f: & A & \to & \dfrac{A}{I} \\ & a & \mapsto & f(a) := a+I \end{array}$$

é um homomorfismo de anéis pois:

1. $f(a+b) = (a+b)+I = (a+I)+(b+I) = f(a)+f(b)$;

2. $f(ab) = (ab)+I = (a+I)(b+I) = f(a)f(b)$.

   Tal homomorfismo f é chamado homomorfismo canônico ou natural.

Observação 1.44. Veja que se A é comutativo com unidade 1_A e $I \subset A$ ideal, então $\dfrac{A}{I}$ é anel comutativo com unidade, a saber $1 = 1_A + I$.
De fato,

$$\forall a \in \frac{A}{I},\ (a+I)1 = (a+I)(1_A+I) = a1_A + I = a+I.$$

Teorema 1.45. *(1º Teorema do Isomorfismo de Anéis) Sejam A, B anéis comutativos, quaisquer.*
Se $f : A \to B$ é um homomorfismo de anéis, então $\dfrac{A}{N(f)} \simeq Imf$.

Demonstração. Defina a seguinte aplicação:

$$\begin{array}{rccc} \delta: & \dfrac{A}{N} & \to & Imf \\ & a+N & \mapsto & \delta(a+N) := f(a), \text{ com } N := N(f) \end{array}$$

Afirmação: δ é um isomorfismo.

1. δ está bem definida, pois: se $a+N = b+N$ então $a-b \in N = N(f)$, logo $f(a-b) = 0$ e então, como f é um homomorfismo, $f(a) - f(b) = 0$, assim $f(a) = f(b)$, ou seja, $\delta(a+N) = \delta(b+N)$.

2. δ é homomorfismo de anéis.

   - $\delta((a+N)+(b+N)) = \delta((a+b)+N) = f(a+b) = f(a)+f(b) = \delta(a+N)+\delta(b+N)$.
   - $\delta((a+N)(b+N)) = \delta(ab+N) = f(ab) = f(a)f(b) = (a+N)(b+N)$.

3. δ é injetora.

   Mostremos que $N(\delta) = \{0_A + I\}$. Para tanto seja $a+N \in N(\delta)$, qualquer. Disso implica que $\delta(a+N) = 0_B$ e então, pela definição de δ, $f(a) = 0_B$, logo $a \in N(f) = N$ e consequentemente $a+N = 0_A+N$. Portanto $N(\delta) = \{0_A+N\}$.

4. δ é sobrejetora.

   Seja $b \in Imf$, qualquer. Como $b \in Imf$, existe $a_0 \in A$ tal que $f(a_0) = b$. Tomando a classe $a_0 + N \in \dfrac{A}{N}$ tem-se: $\delta(a_0+N) = f(a_0) = b$. Portanto, δ é sobrejetora.

□

Teorema 1.46. *Seja A um anel comutativo com unidade, qualquer. Um ideal $I \subset A$ é primo se, e somente se, o anel quociente $\dfrac{A}{I}$ é um domínio de integridade.*

Demonstração.

($\Rightarrow$) Suponha $I \subset A$ primo e mostremos que $\dfrac{A}{I}$ é um domínio de integridade. Como A é comutativo com unidade sabemos que $\dfrac{A}{I}$ é anel comutativo com unidade. Resta mostrar que $\dfrac{A}{I}$ não tem divisores do zero. Para tanto, sejam $(a+I)(b+I) = 0_{\frac{A}{I}} = I \Rightarrow ab+I = 0+I \Rightarrow ab \in I \Rightarrow a \in I$ ou $b \in I$ pois I é um ideal primo. Então $a+I = I$ ou $b+I = I \Rightarrow a+I = 0_{\frac{A}{I}}$ ou $b+I = 0_{\frac{A}{I}}$. Portanto, $\dfrac{A}{I}$ é domínio de integridade.

($\Leftarrow$) Suponha $\dfrac{A}{I}$ é domínio de integridade e provemos que I é ideal primo. Suponha, $\forall a, b \in A : ab \in I$. Então, $ab + I = I \Rightarrow (a+I)(b+I) = I = 0_{\frac{A}{I}}$, como $\dfrac{A}{I}$ é domínio de integridade, segue que $(a+I) = I$ ou $(b+I) = I$, consequentemente, $a \in I$ ou $b \in I$. Portanto, I é um ideal primo.

□

Teorema 1.47. *Seja A um anel comutativo com unidade, qualquer. Um ideal $I \subset A$ é maximal se, e somente se, o anel quociente $\dfrac{A}{I}$ é um corpo.*

Demonstração.

($\Rightarrow$) Suponha que I seja maximal. Mostremos que $\dfrac{A}{I}$ é corpo. Temos que $\dfrac{A}{I}$ é um anel comutativo com unidade pois A é comutativo e com unidade.
Mostremos que todo elemento $(a+I) \neq 0_{\frac{A}{I}} = I$ tem inverso.

Suponha por absurdo que: $(a+I) \in \dfrac{A}{I}$, com $a + I \neq 0_{\frac{A}{I}}$, não tem inverso.
Desta forma, segue que:

$$1 + I \notin \langle a+I \rangle = \left\{ (b+I)(a+I) : (b+I) \in \frac{A}{I} \right\}$$

pois se: $1 + I \in \langle a+I \rangle \Rightarrow \exists (b+I) \in \dfrac{A}{I}$ tal que $(b+I)(a+I) = 1 + I = 1_{\frac{A}{I}}$, o que é absurdo.

Assim, $\{0\} \neq \langle a+I \rangle \neq \dfrac{A}{I}$, ou,

$$\{0_{\frac{A}{I}}\} \subsetneqq \langle a+I \rangle \subsetneqq \frac{A}{I}. \tag{1.7}$$

Assim, se $f : A \to \dfrac{A}{I}$ é homomorfismo natural de (1.7) segue que:
$f^{-1}(\{0_{\frac{A}{I}}\}) \subsetneqq f^{-1}(\langle a+I \rangle) \subsetneqq f^{-1}\left(\dfrac{A}{I}\right) \Rightarrow I \subsetneqq f^{-1}(\langle a+I \rangle) \subsetneqq A$, ou seja, $J = f^{-1}(\langle a+I \rangle)$ é um ideal de A tal que $I \subsetneqq J \subsetneqq A$ o que é absurdo pois I é maximal.
Portanto, $\forall (a+I) \in \dfrac{A}{I}$, $a + I \neq 0_{\frac{A}{I}}$, é invertível.

($\Leftarrow$) Suponha que $\dfrac{A}{I}$ é corpo.
Provemos que I é maximal. Para tanto suponha que J é um ideal de A tal que:

$$I \subsetneqq J \subset A \tag{1.8}$$

Logo, sendo $f : A \to \dfrac{A}{I}$ o homomorfismo natural, obtemos de (1.8):

$$f(I) \subsetneqq f(J) \subset f(A) \Rightarrow \{0_{\frac{A}{I}}\} \subsetneqq f(J) \subset \frac{A}{I}.$$

Então, como $\frac{A}{I}$ é corpo e $f(J)$ é diferente do elemento neutro é ideal de $\frac{A}{I}$, segue da proposição 1.28 que o ideal $f(J)$ é igual $\frac{A}{I}$ isso implica então que J é igual a A.

□

Exemplo 1.48.

Pelo corolário 1.16 sabemos que $\mathbb{Z}_p$, p primo, é corpo. Por outro lado $\mathbb{Z}_p = \frac{\mathbb{Z}}{\langle p\rangle}$ pois $\frac{\mathbb{Z}}{\langle p\rangle} = \{a + \langle p\rangle : a \in \mathbb{Z}\}$ e $a + \langle p\rangle = \{b \in \mathbb{Z} : a - b \in \langle p\rangle\} = \{b \in \mathbb{Z} : p \mid (a-b)\} = \overline{b}$, com b o resto da divisão de a por p, tal que $0 \leqslant b < 0$ ou seja, $\frac{\mathbb{Z}}{\langle p\rangle} = \{\overline{0}, \overline{1}, \ldots, \overline{(p-1)}\}$ $= \mathbb{Z}_p$. Logo, pelo teorema 1.47, se p primo, $\frac{\mathbb{Z}}{\langle p\rangle}$ é corpo e $\langle p\rangle \subset \mathbb{Z}$ é ideal maximal.

Definição 1.49. *Sejam A um anel e $m \in \mathbb{Z}$, $\forall a \in A$. Definimos múltiplos de a, m.a, da seguinte maneira:*

$$\begin{cases} m = 0: & 0 \cdot a & := & 0_A \\ m > 0: & m \cdot a & := & (m-1)a + a \\ m < 0: & m \cdot a & := & -((-m) \cdot a) \end{cases}.$$

Pode-se mostrar que: $\forall a \in A$, $\forall m$, $n \in \mathbb{Z}$:

1. $(mn) \cdot a = m \cdot (n \cdot a)$;
2. $(m+n) \cdot a = m \cdot a +_A n \cdot a$;
3. $(-m) \cdot a = -m \cdot a = m \cdot (-a)$;
4. $(mn) \cdot 1_A = (m \cdot 1_A) \cdot_A (n \cdot 1_A)$.

Definição 1.50. *Seja A um anel. Considere o seguinte subconjunto de $\mathbb{Z}_+^*$:*

$$S = \{n \in \mathbb{Z}_+^* : na = 0_A, \forall a \in A\} \subset \mathbb{Z}_+^*.$$

Temos duas possibilidades:

- *$S = \varnothing$: neste caso dizemos que A tem característica zero, ou seja, $C(A) = 0$.*
- *$S \neq \varnothing$: veja que S é limitado inferiormente pelo $0 \in \mathbb{Z}$, assim pelo Princípio do Menor Inteiro, S tem um elemento minimal, digamos $d \in S$.*
  Nesse caso dizemos que A tem característica d, ou seja, $C(A) = d$.

Exemplo 1.51.

1. $\mathbb{Z}_n$ tem característica n pois: $n\overline{a} = \overline{0}$, $\forall \overline{a} \in \mathbb{Z}_n$, já que

$$n\overline{a} = \underbrace{\overline{a} + \ldots + \overline{a}}_{n-parcelas} = \overline{na} = \overline{0}$$

2. $\mathbb{Z}$ tem característica zero, pois $\forall a \in \mathbb{Z}^*$: $na = 0 \Leftrightarrow n = 0$.

Lema 1.52. *A característica de um domínio de integridade, A, é zero ou é um número primo.*

Demonstração. Suponha que $C(A) = d \neq 0$ onde d é um número inteiro não primo. Logo, $d = rs$, $1 < r, s < d$. Assim, para $1_A \in A$ temos: $0_A = d1_A = (rs)1_A = (r1_A)(s1_A) = 0_A \Rightarrow r1_A = 0_A$ ou $s1_A = 0_A$ e $0 < r, s < d$, o que é absurdo pois d é menor inteiro com esta propriedade.
Portanto, d é primo. □

1.2 Anel de polinômios

Nesta seção definimos o anel de polinômios e resultados necessários para o desenvolvimento dos demais capítulos.

Definição 1.53. *Considere R um anel. Um polinômio $f(X)$ com coeficientes em R, e variável indeterminada X, é uma soma formal infinita*

$$\sum_{i=0}^{\infty} a_i X^i = a_0 + a_1 X + \ldots + a_n X^n + \ldots \tag{1.9}$$

em que $a_i \in R$ e $a_i = 0$ para uma quantidade finita de valores de i. Cada a_i é chamado coeficiente de $f(X)$.

Definição 1.54. *Sejam R um anel e $f(X)$ um polinômio com coeficientes em R. Chamamos de grau de f, ∂f, ao índice n tal que $a_n \neq 0$ e $a_j = 0$ para todo $j > n$. Se, para todo $i\{1, \ldots, n\}$, $a_i = 0$ o grau de $f(X)$ não está definido.*

Observação 1.55. No que segue, se $\partial f = n$ podemos denotar $f(X)$ por $a_0 + a_1 X + \ldots + a_n X^n = \sum_{i=0}^{n} a_i X^i$, isto é, $f(X) = \sum_{i=0}^{n} a_i X^i$, já que como $a_i = 0$, para todo $i > n$, $i\{1, \ldots, n\}$, podemos omitir a parcela $\sum_{i=n+1}^{\infty} a_i X^i$ de (1.9).

Além disso, se R é um anel com unidade $1 \neq 0$, escreveremos o termo $1X^k$ em (1.9) como X^k.

Exemplo 1.56. Em $\mathbb{Z}$, escrevemos o polinômio $2 + 1X$ como $2 + X$. Assim, $0, 2, X$, e $2 + X^2$ são polinômios com coeficientes em $\mathbb{Z}$.

Observação 1.57. Cada elemento de R é um polinômio, o qual chamamos: polinômio constante, isto é, $\forall a \in R, f(X) = a$, é um polinômio constante.
Em particular, quando $f(X) = 0$, chamamos $f(X)$ de polinômio nulo. Veja que todo polinômio constante e não nulo tem grau igual a zero.

A seguir definimos duas operações binárias para o conjunto dos polinômios com coeficientes em um anel R. A partir de agora denotamos tal conjunto por $R[X]$. Para a adição em $R[X]$ considere $f(X), g(X) \in R[X]$ dados por

$$f(X) = a_0 + a_1 X + \ldots + a_n X^n + \ldots$$

e

$$g(X) = b_0 + b_1X + \ldots + b_nX^n + \ldots.$$

Definimos a adição de $f(X)$ e $g(X)$, por

$$f(X) + g(X) := c_0 + c_1X + \ldots + c_nX^n + \ldots$$

em que

$$c_n = a_n + b_n.$$

Enquanto que a multiplicação de $f(X)$ e $g(X)$ é definida por

$$f(X)g(X) := d_0 + d_1X + \ldots + d_nX^n + \ldots$$

em que

$$d_n = \sum_{i=0}^{n} a_i b_{n-i}.$$

Com tais operações $(R[X], +, \cdot)$ é um anel. Além disso, se R é um anel com unidade $1_R \neq 0_R$ então $R[X]$ é um anel com unidade em que tal unidade é o polinômio constante igual a 1. Ainda se R é um anel comutativo então $R[X]$ é um anel comutativo. Mais ainda, se R é um domínio de integridade, $R[X]$ também é um domínio de integridade. Em particular, se R é um corpo não podemos garantir que $R[X]$ é um corpo, já que neste caso os únicos elementos invertíveis de $R[X]$ são os polinômios constantes não nulos, ou seja, $U(R[X]) = \{f(X) \in R[X] : f(X)$ é um polinômio constante não nulo$\}$, consequentemente $U(R[X]) \neq R[X] - \{0\}$. Entretanto veremos no teorema 1.71 que se R é um corpo então $R[X]$ é um Domínio de Ideais Principais (PID). Para mais detalhes vide p. 200, Teorema 2.22 em [2].

Exemplo 1.58. Em $\mathbb{Z}_2[X]$ temos

$$(X + \overline{1})^2 = (X + \overline{1})(X + \overline{1}) = X^2 + (\overline{1} + \overline{1})X + \overline{1} = X^2 + \overline{1}.$$

Enquanto que:

$$(X + \overline{1}) + (X + \overline{1}) = (\overline{1} + \overline{1})X + (\overline{1} + \overline{1}) = \overline{0}X + \overline{0} = \overline{0}.$$

Definição 1.59. *Se R é um anel e X e Y são variáveis indeterminadas, podemos formar o anel $(R[X])[Y]$, isto é, o anel de polinômios em Y cujos coeficientes pertencem a $R[X]$.*
Denotamos $(R[X])[Y] = R[X, Y]$. De modo indutivo podemos definir o anel $R[X_1, \ldots, X_n]$ de polinômios com n variáveis indeterminadas X_i com coeficientes em R.

Teorema 1.60. *Sejam F um corpo e α qualquer elemento de F.*
A apliacação $\phi_\alpha : F[X] \to F$ definida por

$$\phi_\alpha(f(X)) = \phi_\alpha(a_0 + a_1X + \ldots + a_nX^n) := a_0 + a_1\alpha + \ldots + a_n\alpha^n$$

para qualquer $f(X) \in F[X]$ é um homomorfismo de $F[X]$ em F.

Além disso, $\phi_\alpha(a) = a$ para $a \in F$.

O homomorfismo ϕ_α é chamado de homomorfismo de valoração em α.

Demonstração. A aplicação ϕ_α está bem definida, isto é, independente da representação de $f(X) \in F[X]$ como uma soma finita

$$a_0 + a_1X + \ldots + a_nX^n,$$

uma vez que tal soma finita representando $f(X)$ pode ser alterada somente pela inserção ou exclusão dos termos $0x^i$, o que não afeta o valor de $\phi_\alpha(f(X))$.
Agora se $f(X) = a_0 + a_1X + \ldots + a_nX^n$, $g(X) = b_0 + b_1X + \ldots + b_mX^m$ e $h(X) := f(X) + g(X) = c_0 + c_1X + \ldots + c_rX^r$, então

$$\phi_\alpha(f(X) + g(X)) = \phi_\alpha(h(X)) = c_0 + c_1\alpha + \ldots + c_r\alpha^r,$$

enquanto que

$$\phi_\alpha(f(X)) + \phi_\alpha(g(X)) = (a_0 + a_1\alpha + \ldots + a_n\alpha^n) + (b_0 + b_1\alpha + \ldots + b_m\alpha^m).$$

Como por definição de adição polinomial temos $c_i = a_i + b_i$, vemos que

$$\phi_\alpha(f(X) + g(X)) = \phi_\alpha(f(X)) + \phi_\alpha(g(X)) \tag{1.10}$$

Para a multiplicação, temos

$$f(X)g(X) = d_0 + d_1X + \ldots + d_sX^s,$$

logo

$$\phi_\alpha(f(X)g(X)) = d_0 + d_1\alpha + \ldots + d_s\alpha^s,$$

enquanto que

$$[\phi_\alpha(f(X))][\phi_\alpha(g(X))] = (a_0 + a_1\alpha + \ldots + \alpha_n\alpha^n)(b_0 + b_1\alpha + \ldots + b_m\alpha^m).$$

Já que por definição de multiplicação polinomial é dada $d_j = \sum_{i=0}^{j} a_ib_{j-i}$ vemos que

$$\phi_\alpha(f(X)(g(X)) = [\phi_\alpha(f(X))][\phi_\alpha(g(X))]. \tag{1.11}$$

Por (1.10) e (1.11) segue que ϕ_α é um homomorfismo. A própria definição de ϕ_α aplicada a um polinômio constante $a \in R[X]$, em que $a \in R$, dá $\phi_\alpha(a) = a$.

E, por definição de ϕ_α, temos $\phi_\alpha(X) = \phi_\alpha(1X) = 1\alpha = \alpha$. □

Exemplo 1.61. Seja $F = \mathbb{Q}$. Pelo teorema 1.60, temos que o homomorfismo de valoração $\phi_0 : \mathbb{Q}[X] \to \mathbb{R}$ é dado por

$$\phi_0(a_0 + a_1X + \ldots + a_nX^n) = a_0 + a_10 + \ldots + a_n0^n = a_0.$$

Exemplo 1.62. Seja $F = \mathbb{Q}$. Pelo teorema 1.60, temos que o homomorfismo de valoração $\phi_2 : \mathbb{Q}[X] \to \mathbb{R}$ é dado por

$$\phi_2(a_0 + a_1X + \ldots + a_nX^n) = a_0 + a_12 + \ldots + a_n2^n.$$

Observe que

$$\phi_2(X^2 + X - 6) = 2^2 + 2 - 6 = 0.$$

Assim, $(X^2 + X - 6)$ está no núcleo de ϕ_2 .

Definição 1.63. *Sejam F um corpo e α um elemento de F, $f(X) = a_0 + a_1X + \ldots + a_nX^n \in F[X]$, e $\phi_\alpha : F[X] \to F$ o homomorfismo de valoração do teorema 1.60. Denotamos*

$$f(\alpha) := \phi_\alpha(f(X)) = a_0 + a_1\alpha + \ldots + a_n\alpha^n.$$

Se $f(\alpha) = 0$ dizemos que α é um zero de $f(X)$.

Definição 1.64. *Seja F um corpo. Dizemos que $f(X) \in F[X]$, polinômio não nulo, se fatora em $F[X]$ quando existem polinômios $g(X)$, $h(X) \in F[X]$, tais que $f(X) = g(X)h(X)$. Ainda $g(X)$ e $h(X)$ são chamados fatores de $f(X)$.*

Observação 1.65. Suponha que $f(X) \in F[X]$ se fatora em $f(X) = g(X)h(X)$ com $g(X)$, $h(X) \in F[X]$ e seja $\alpha \in F$. Veja que

$$f(\alpha) = \phi_\alpha(f(X)) = \phi_\alpha(g(X)h(X)) = \phi_\alpha(g(X))\phi_\alpha(h(X)) = g(\alpha)h(\alpha).$$

Assim, $\alpha \in F$ é tal que $f(\alpha) = 0$ se, e somente se, $g(\alpha) = 0$ ou $h(\alpha) = 0$, já que $g(\alpha)$, $h(\alpha) \in F$ e F é, em particular, um domínio de integridade.

A seguir apresentamos uma ferramenta importante ao longo deste trabalho.

Teorema 1.66. *(Algoritmo da divisão para $F[X]$)*
Se $f(X) = a_nX^n + a_{n-1}X^{n-1} + \ldots + a_0$ e $g(X) = b_mX^m + b_{m-1}X^{m-1} + \ldots + b_0$ são elementos de $F[X]$, com a_n e b_m, não nulos, elementos diferentes de zero em F e $m > 0$ então existem, e são únicos, polinômios $q(X)$ e $r(X) \in F[X]$ tais que $f(X) = g(X)q(X) + r(X)$, em que $r(X) = 0$ ou o grau de $r(X)$ é menor que o grau de $g(X)$. Denominamos $q(X)$ de quociente e $r(X)$ o resto da divisão de $f(X)$ por $g(X)$.

Demonstração. Considere o conjunto $S = \{f(X) - g(X)s(X) \mid s(X) \in F[X]\}$. Se $0 \in S$ então existe um $s(X) \in F[X]$ tal que $f(X) - g(X)s(X) = 0$. Logo, $f(X) = g(X)s(X)$. Assim, tomando $q(X) = s(X)$ e $r(X) = 0$, temos provado o teorema.
Caso contrário, isto é, se $0 \notin S$ seja $r(X)$ elemento de grau mínimo em S, que existe pelo Princípio do Menor Inteiro. Assim,

$$f(X) = g(X)q(X) + r(X)$$

para algum $q(X) \in F[X]$. Resta-nos mostrar que o grau de $r(X)$ é menor que $m = \partial g$. Para tanto, suponha que

$$r(X) = c_tX^t + c_{t-1}X^{t-1} + \ldots + c_0,$$

com $c_t \in F$ e $c_t \neq 0$. Se $t \geq m$, então

$$f(X) - q(X)g(X) - \left(\frac{c_t}{b_m}\right)X^{t-m}g(X) = r(X) - \left(\frac{c_t}{b_m}\right)X^{t-m}g(X). \tag{1.12}$$

Veja que: $r(X) - \left(\frac{c_t}{b_m}\right)X^{t-m}g(X) = r(X) - (c_tx^t + \text{termos de grau menor})$, que é um polinômio de grau menor que $t = \partial r(X)$. No entanto, o polinômio em 1.12 pode ser escrito na forma

$$f(X) - g(X)[q(X) + \left(\frac{c_t}{b_m}\right)X^{t-m}] \tag{1.13}$$

logo (1.13) é um elemento em S, contradizendo o fato de que $r(X)$ foi selecionado para ter grau mínimo em S.

Com isso, o grau de $r(X)$ é necessariamente menor que o grau m de $g(X)$.
Para unicidade do quociente e do resto de tal divisão, suponha

$$f(X) = g(X)q_1(X) + r_1(X) \tag{1.14}$$

e

$$f(X) = g(X)q_2(X) + r_2(X). \tag{1.15}$$

Subtraindo (1.15) de (1.14) obtemos: $g(X)q_1(X) + r_1(X) - g(X)q_2(X) - r_2(X) = 0 \Rightarrow g(X)q_1(X) - g(X)q_2(X) = r_2(X) - r_1(X) \Rightarrow$

$$g(X)[q_1(X) - q_2(X)] = r_2(X) - r_1(X). \tag{1.16}$$

Como $r_2(X) - r_1(X) = 0$ ou o grau de $(r_2(X) - r_1(X))$ é menor que o grau de $g(X)$, (1.16) só pode acontecer se $q_1(X) - q_2(X) = 0$, ou seja, se $q_1(X) = q_2(X)$. Com isso, devemos ter $r_2(X) - r_1(X) = 0$, e então $r_1(X) = r_2(X)$. □

Exemplo 1.67. Consideremos os seguintes polinômios em $\mathbb{Z}_5[X]$, $f(X) = X^4 - \overline{3}X^3 + \overline{2}X^2 + \overline{4}X - \overline{1}$ e $g(X) = X^2 - \overline{2}X + \overline{3}$. Veja que dividindo $f(X)$ por $g(X)$, obtemos: $q(X) = X^2 - X - \overline{3}$ e $r(X) = X + \overline{3}$.

Corolário 1.68. *Um elemento $a \in F$ é um zero de $f(X) \in F[X]$ se, e somente se, $X - a$ é um fator de $f(X) \in F[X]$.*

Demonstração. ($\Rightarrow$) Suponha que para $a \in F$ temos $f(a) = 0$. Pelo teorema 1.66 dividindo $f(X)$ por $(X - a)$, existem $q(X)$, $r(X) \in F[X]$ tais que

$$f(X) = (X - a)q(X) + r(X),$$

em que $r(X) = 0$ ou o grau de $r(X)$ é menor que $1 = \partial(X - a)$.
Assim necessariamente $r(X) = c$ para algum $c \in F$, logo:

$$f(X) = (X - a)q(X) + c.$$

Aplicando o homomorfismo de valoração $\phi_a : F[X] \to F$ temos

$$0 = f(a) = 0q(a) + c,$$

consequentemente $c = 0$. Logo $f(X) = (X - a)q(X)$, ou seja, $X - a$ é um fator de $f(X)$.

($\Leftarrow$) Se $X - a$ é um fator de $f(X) \in F[X]$, onde $a \in F$, temos $f(X) = (X - a)q(X)$ para algum $q(X) \in F[X]$; aplicando o homomorfismo de valoração temos $f(a) = 0q(a) = 0$.

□

Exemplo 1.69. Em $\mathbb{Z}_5[X]$, note que $\overline{1}$ é um zero de

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

pois $f(\overline{1}) = \overline{0}$. Assim, pelo corolário 1.68, podemos fatorar $X^4 + \overline{3}X^3 + \overline{2}X + \overline{4}$ como $(X - \overline{1})q(X)$ em $\mathbb{Z}_5[X]$.
Assim, $X^4 + \overline{3}X^3 + \overline{2}X + \overline{4} = (X - \overline{1})(X^3 + \overline{4}X^2 + \overline{4}X + \overline{1})$ em $\mathbb{Z}_5[X]$. Mas $\overline{1}$ também é um zero de $X^3 + \overline{4}X^2 + \overline{4}X + \overline{1}$ e podemos dividir este polinômio por $X - \overline{1}$ e obter $(X^2 + \overline{4})$. Mas $\overline{1}$ também é zero de $(X^2 + \overline{4})$ e podemos dividir novamente por $X - \overline{1}$ e obter $X + \overline{1}$.
Assim, $X^4 + \overline{3}X^3 + \overline{2}X + \overline{4} = (X - \overline{1})^3(X + \overline{1})$ em $\mathbb{Z}_5[X]$.

Definição 1.70. *Um polinômio não constante $f(X) \in F[X]$ é irredutível sobre F (ou um polinômio irredutível em $F[X]$) se $f(X)$ não pode ser expresso como um produto $g(X)h(X)$, de dois polinômios $g(X)$ e $h(X) \in F[X]$, ambos de menor grau que o grau de $f(X)$. Se $f(X) \in F[X]$ é um polinômio não constante que não é irredutível sobre F, então dizemos que $f(X)$ é redutível sobre F.*

Teorema 1.71. *Se F é um corpo, então em $F[X]$ é um PID.*

Demonstração. Precisamos mostrar que todo ideal N de $F[X]$ é um ideal principal, ou seja, que existe $g(X) \in F[X]$ tal que $N = \langle g(X) \rangle$. Seja N um ideal de $F[X]$. Se $N = \{0\}$, então $N = \langle 0 \rangle$. Suponha que $N \neq \{0\}$ e seja $g(X) \neq 0$ e $g(X) \in N$ de grau mínimo, que existe pelo Princípio do Menor Inteiro. Se o grau de $g(X)$ é 0, então $g(X) \in F$, e $g(X) \in U(F[X])$. Logo $N = \langle 1 \rangle = F[X]$, nessa igualdade usa o lema 1.24 então N é principal. Se $\partial g(X) \geqslant 1$, seja $f(X)$ qualquer elemento de N. Então, pelo teorema 1.66, existem $q(X)$ e $r(X) \in F[X]$ tais que $f(X) = g(X)q(X) + r(X)$, onde $r(X) = 0$ ou $\partial r < \partial g$.

Agora $f(X) \in N$ e $g(X) \in N$ implicam que $f(X) - g(X)q(X) \in N$ por definição de ideal. Como $g(X)$ é um elemento não nulo de grau mínimo em N, necessariamente $r(X) = 0$. Assim $f(X) = g(X)q(X) \in \langle g(X) \rangle$. Portanto $N \subset \langle g(X) \rangle$. Ainda, como $g(X) \in N$ temos $\langle g(X) \rangle \subset N$. Portanto, $N = \langle g(X) \rangle$. □

Teorema 1.72. *Seja F um corpo, um ideal $\langle p(X) \rangle \neq 0$ de $F[X]$ é ideal maximal se, e somente se, $p(X)$ é irredutível sobre F.*

Demonstração. ($\Rightarrow$) Suponha que $\langle p(X) \rangle \neq 0$ seja um ideal maximal de $F[X]$. Então $\langle p(X) \rangle \neq F[X]$, logo $p(X) \notin F$.

Agora seja $p(X) = f(X)g(X)$ uma fatoração de $p(X)$ em $F[X]$. Como $\langle p(X) \rangle$ é um ideal maximal pelo teorema 1.37 e, portanto, também um ideal primo, $(f(X)g(X)) \in \langle p(X) \rangle$ implica que $f(X) \in \langle p(X) \rangle$ ou $g(X) \in \langle p(X) \rangle$; isto é, $f(X)$ ou $g(X)$ tem $p(X)$ como um fator. Mas então não podemos ter os graus de ambos $f(X)$ e $g(X)$ estritamente menores que o grau de $p(X)$. Isso mostra que $p(X)$ é irredutível sobre F, pela definição.

($\Leftarrow$) Se $p(X)$ é irredutível sobre F, suponha que N seja um ideal tal que $\langle p(X)\rangle \subseteq N \subseteq F[X]$. Agora N é um ideal principal pelo teorema 1.71, então $N = \langle g(X)\rangle$ para algum $g(X) \in N$. Logo se $p(X) \in N$ então $p(X) = g(X)q(X)$ para algum $q(X) \in F[X]$. Mas $p(X)$ é irredutível, o que implica que $g(X)$ ou $q(X)$ é de grau 0. Se $g(X)$ é de grau 0, isto é, uma constante diferente de zero em F, então $g(X)$ é uma unidade em $F[X]$, consequentemente $N = \langle g(X)\rangle = F[X]$. Se $q(X)$ é de grau 0, então $q(X) = c$, onde $c \in F$ e $g(X) = (1/c)p(X) \in \langle p(X)\rangle$, então $N = \langle p(X)\rangle$. Assim $\langle p(X)\rangle \subset N \subset F[X]$ é impossível, então $\langle p(X)\rangle$ é ideal maximal.

□

Teorema 1.73. *Seja $p(X)$ um polinômio irredutível em $F[X]$. Se $p(X)$ divide $r(X)s(X)$, com $r(X)$, $s(X) \in F[X]$, então $p(X) \mid r(X)$ ou $p(X) \mid s(X)$.*

Demonstração. Primeiro veja que como $p(X)$ é irredutível temos, pelo teorema 1.72 que $\langle p(X)\rangle$ é ideal maximal e consequentemente por 1.37 é um ideal primo. Assim, se $p(X) \mid r(X)s(X)$ então $r(X)s(X) \in \langle p(X)\rangle$, mas $\langle p(X)\rangle$ é ideal primo logo $r(X) \in \langle p(X)\rangle$ ou $s(X) \in \langle p(X)\rangle$, ou seja, $p(X) \mid r(X)$ ou $p(X) \mid s(X)$. □

Corolário 1.74. *Se $p(X)$ é irredutível em $F[X]$ e $p(X)$ divide o produto $r_1(X)\dots r_n(X)$, com $r_i(X) \in F[X]$, $\forall i \in \{1,\dots,n\}$, então $p(X)$ divide $r_i(X)$ para algum $i \in \{1,\dots,n\}$.*

Demonstração. Segue do teorema 1.73 e do Princípio de Indução Matemática. □

Teorema 1.75. *Se F é um corpo então todo polinômio não constante $f(X) \in F[X]$ pode ser fatorado em $F[X]$ em um produto de polinômios irredutíveis de maneira única a menos da ordem no referido produto e por constantes não-nulas em F.*

Demonstração. Seja $f(X)$ um polinômio não-constante. Se $f(X)$ não é irredutível, então $f(X) = g(X)h(X)$, com o grau de $g(X)$ e o grau de $h(X)$ ambos menores que o grau de $f(X)$. Se $g(X)$ e $h(X)$ são ambos irredutíveis, o resultado está provado.
Caso contrário, pelo menos um desses se fatora em polinômios de grau menor. Continuando esse processo, chegamos a uma fatoração

$$f(X) = p_1(X)p_2(X)\dots p_r(X),$$

em que cada $p_i(X)$ é irredutível para $i = 1, 2, \dots, r$.
Resta-nos mostrar a unicidade a menos de ordem de produto e constantes não nulas em F . Suponha que

$$p_1(X)p_2(X)\dots p_r(X) = f(X) = q_1(X)q_2(X)\dots q_s(X)$$

sejam duas fatorações de $f(X)$ em polinômios irredutíveis.
Pelo corolário 1.74 $p_1(X)$ divide algum $q_j(X)$, sem perda de generalidade podemos

supor que $p_1(X)$ divide $q_1(X)$.
Se $q_1(X)$ é irredutível, então

$$q_1(X) = u_1 p_1(X),$$

com $u_1 \in F - \{0\}$ e, portanto, $u_1 \in U(F[X])$.
Assim substituindo $q_1(X)$ por $u_1 p_1(X)$ obtemos

$$p_1(X)p_2(X)\dots p_r(X) = u_1 p_1(X)q_2(X)\dots q_s(X) \Rightarrow p_2(X)\dots p_r(X) = u_1 q_2(X)\dots q_s(X).$$

Por um argumento semelhante, se, digamos $q_2(X) = u_2 p_2(X)$, então

$$p_3(X)\dots p_r(X) = u_1 u_2 q_3(X)\dots q_s(X).$$

Continuando esse processo obtemos:

$$1 = u_1 u_2 \dots u_r q_{r+1}(X)\dots q_s(X). \tag{1.17}$$

Mas (1.17) só faz sentido se $1 = u_1 u_2 \dots u_r$.
Assim, os fatores irredutíveis $p_i(X)$ e $q_j(X)$ são os mesmos, exceto possivelmente por ordem de fatores e elementos em $U(F[X])$. □

2 Domínio de fatoração única

Vimos no Capítulo 1 a definição de domínio de integridade bem como alguns resultados, a seguir tratamos de um domínio de integridade com características mais peculiares, a saber: apresentamos definições e resultados sobre domínio de fatoração única, mais especificamente, mostraremos que todo domínio de ideais principais (PID) é um domínio de fatoração única (UFD). Além disso, mostraremos que se D é um domínio de fatoração única então o anel de polinômios $D[X]$ também é um domínio de fatoração única.

Definição 2.1. *Sejam R um anel comutativo com unidade e $a, b \in R$, quaisquer. Se existe $c \in R$ tal que $b = ac$, então a divide b (ou a é um fator de b), denotado por $a \mid b$. Caso contrário, dizemos que a não divide b: $a \nmid b$.*

Definição 2.2. *Um elemento u de um anel R comutativo com unidade é uma unidade de R se u divide 1, isto é, se u tem um inverso multiplicativo em R, ou ainda, $u \in U(R)$. Dizemos que dois elementos a e b são associados em R se $a = bu$, em que $u \in U(R)$.*

Observação 2.3. Em particular, se a e b são associados temos que $a \mid b$ e $b \mid a$.

Exemplo 2.4. Sabemos que as únicas unidades em $\mathbb{Z}$ são 1 e -1. Assim, os únicos associados de a em $\mathbb{Z}$ são a e $-a$.

Definição 2.5. *Seja D um domínio de integridade, qualquer.*
Dizemos que $p \in D$ é irredutível quando em qualquer fatoração $p = ab$ em D, temos a ou b em $U(D)$.

Definição 2.6. *Um domínio de integridade D é um domínio de fatoração única(UFD) se as seguintes condições forem satisfeitas:*

1. *Todo elemento de D que é diferente do elemento nulo e não é uma unidade pode ser fatorado em um produto de um número finito de elementos irredutíveis em D.*

2. *Se $p_1 \dots p_r$ e $q_1 \dots q_s$ são duas fatorações do mesmo elemento de D e são elementos irredutíveis, então $r = s$ e os $q_j's$ podem ser reenumerados de modo que p_i e q_i sejam associados.*

Exemplo 2.7.
Sejam $D = \mathbb{Z}$ e $a = -15 \in \mathbb{Z}$.
Consideremos as fatorações em elementos irredutíveis em $\mathbb{Z}$:

- $-15 = p_1 \cdot p_2 = -3 \cdot 5$

- $-15 = q_1 \cdot q_2 = -5 \cdot 3$

Podemos reenumerar por $q_2 = -5$ e $q_1 = 3$. Daí,

- $p_1 = -3$ é associado a $q_1 = 3$, pois $-3 = -1 \cdot 3$, $-1 \in U(\mathbb{Z})$;
- $q_2 = -5$ é associado a $p_2 = 5$, pois $5 = (-1) \cdot (-5)$, $-1 \in U(\mathbb{Z})$.

O objetivo agora é mostrar que todo PID é um UFD. Para tanto precisamos dos seguintes resultados.

Definição 2.8. *Se $\{A_i : i \in I\}$ é uma coleção de conjuntos então a união $\bigcup_{i \in I} A_i$ dos conjuntos A_i é o conjunto de todos x tais que $x \in A_i$ para pelo menos um $i \in I$.*

Lema 2.9. *Se R é um anel comutativo e $N_1 \subseteq N_2 \subseteq ...$ é uma cadeia ascendente de ideais N_i em R, então $N = \bigcup_i N_i$ é um ideal de R.*

Demonstração. Sejam $a, b \in N$, quaisquer. Assim, existem ideais N_i e N_j na cadeia, com $a \in N_i$ e $b \in N_j$. Agora, $N_i \subseteq N_j$ ou $N_j \subseteq N_i$, vamos supor que $N_i \subseteq N_j$, então ambos a e b pertencem a N_j. Isso implica que $a \pm b$, $ab \in N_j \subseteq N$, ou seja, $a \pm b$, $ab \in N$. Tomando $a = 0$, vemos que $b \in N$ implica $-b \in N$, e $0 \in N$ desde $0 \in N_i, \forall i$. Assim, N é um subanel de R. Para $a \in N$ e $d \in R$, temos $a \in N_i$, para algum N_i. Dessa forma, como N_i é um ideal: $da \in N_i \subseteq N$. Logo, $da \in N$. Portanto, N é um ideal de R. □

Lema 2.10. *Seja D é um PID. Se $N_1 \subseteq N_2 \subseteq \ldots$ é uma cadeia ascendente de ideais N_i, então existe um número inteiro positivo r tal que $N_r = N_s$ para todo $s \geq r$.*

Esta propriedade é conhecida como condição da cadeia ascendente (ACC).

Demonstração. Pelo lema 2.9 , sabemos que $N = \bigcup_i N_i$ é um ideal de D e como um ideal em D, que é um PID, $N = \langle c \rangle$ para algum $c \in D$. Uma vez que $N = \bigcup_i N_i$ segue que $c \in N_r$, para algum $r \in \mathbb{Z}^+$, assim $s \geq r$, temos:

$$\langle c \rangle \subseteq N_r \subseteq N_s \subseteq N = \langle c \rangle.$$

De fato $N_r = N_s$ para $s \geq r$. □

Observação 2.11. Para quaisquer elementos a e b de um domínio de integridade D, tem-se:

- $\langle a \rangle \subseteq \langle b \rangle$ se, e somente se, $b \mid a$;
- $\langle a \rangle = \langle b \rangle$ se, e somente se, a e b são associados em D.

De fato: para a primeira propriedade, note que $\langle a\rangle \subseteq \langle b\rangle$ se, e somente se, $a \in \langle b\rangle$, que é válido se, e somente se, $a = bd$ para algum $d \in D$, ou seja, se, e somente se, $b \mid a$.
Usando esta primeira propriedade, vemos que $\langle a\rangle = \langle b\rangle$ se, e somente se $a = bc$ e $b = ad$ para determinados $c, d \in D$.
Disso segue que $a = adc$ e consequentemente, como D é domínio de integridade , segue da proposição 1.12, que $1 = dc$.
Assim, d e $c \in U(D)$, e a e b são associados.

Agora podemos provar a condição 1 da definição 2.6 para que um PID seja um UFD.

Teorema 2.12. *Seja D um PID, qualquer. Todo elemento que não é o elemento neutro e não é uma unidade em D é um produto de elementos irredutíveis em D.*

Demonstração. Seja $a \in D$, qualquer, tal que $a \neq 0$ e $a \notin U(D)$.
Primeiro mostramos que a tem pelo menos um fator irredutível.
Se a é um irredutível, não há o que ser feito.
Se a não é irredutível, então $a = a_1b_1$, onde a_1 e $b_1 \notin U(D)$.
Agora, $\langle a\rangle \subset \langle a_1\rangle$, pois $a = a_1b_1$. Se $\langle a\rangle = \langle a_1\rangle$, então a e a_1 seriam elementos associados e $b_1 \in U(D)$, o que é absurdo pela construção de b_1.
Continuando este procedimento então, começando agora com a_1, chegamos a uma cadeia de ideais estritamente ascendente:

$$\langle a\rangle \subset \langle a_1\rangle \subset \langle a_2\rangle \subset \dots.$$

Pela ACC no lema 2.10 essa cadeia termina em algum $\langle a_r\rangle$ e a_r necessariamente é irredutível. Portanto, a tem um fator irredutível a_r, já que $\langle a\rangle \subset \langle a_r\rangle$, com a_r irredutível.
Com o que acabamos de provar, para um elemento a que não é nem 0 nem uma unidade em D, ou a é irredutível ou $a = p_1c_1$ com p_1 irredutível e $c_1 \notin U(D)$.
Por um argumento análogo podemos concluir que $\langle a\rangle \subset \langle c_1\rangle$. Se c_1 não é irredutível, então $c_1 = p_2c_2$ para um irredutível p_2 com $c_2 \notin U(D)$.
Continuando, construímos uma cadeia de ideais estritamente ascendente:

$$\langle a\rangle \subset \langle c_1\rangle \subset \langle c_2\rangle \subset \dots.$$

Esta cadeia necessariamente termina em algum $c_r = q_r$ que é um irredutível.
Consequentemente $a = p_1p_2 \dots p_rq_r$ pelo lema 2.10. □

Lema 2.13. *Um ideal $\langle p\rangle$ em um PID é maximal se, e somente se, p é um elemento irredutível.*

Demonstração. ($\Rightarrow$) Sejam D um PID e $\langle p\rangle$ um ideal maximal de D.
Suponha que $p = ab$ em D, logo $\langle p\rangle \subseteq \langle a\rangle$.
Se $\langle a\rangle = \langle p\rangle$, então a e p seriam associados e consequentemente b deve ser uma unidade de D.
Se $\langle a\rangle \neq \langle p\rangle$, então necessariamente $\langle a\rangle = \langle 1\rangle = D$, já que $\langle p\rangle$ é ideal maximal.
Mas então a e 1 são elementos associados, assim $a \in U(D)$.
Portanto mostramos que se $p = ab$ então a ou b deve ser uma unidade. Portanto, p é um irredutível de D.

($\Leftarrow$) Suponha que p seja um elemento irredutível em D.
Para mostrar que $\langle p\rangle$ é ideal maximal, suponha que $I = \langle a\rangle$ seja ideal de D tal que

$$\langle p\rangle \subsetneqq \langle a\rangle \subseteq D. \tag{2.1}$$

Mostremos que $\langle a\rangle = \langle p\rangle$. De fato, como $\langle p\rangle \subset \langle a\rangle$ temos $p = ab$. Mas p é irredutível logo $a \in U(D)$ ou $b \in U(D)$.
Se $a \in U(D)$ então $\langle a\rangle = \langle 1\rangle = D$.
Se $a \notin U(D)$ então $b \in U(D)$, ou seja, existe $u \in D$ tal que $bu = 1$.
Assim, $pu = abu = a$ e segue $\langle a\rangle \subseteq \langle p\rangle$. Consequentemente $\langle a\rangle = \langle p\rangle$ o que é absurdo por (2.1).
Logo, necessariamente $a \in U(D)$ e $\langle a\rangle = D$, provando que $\langle p\rangle$ é ideal maximal.
□

Lema 2.14. *Em um PID, se um elemento p é irredutível e tal que $p \mid ab$, então $p \mid a$ ou $p \mid b$.*

Demonstração. Seja D um PID qualquer e suponha que para um elemento irredutível p em D temos $p \mid ab$. Logo, $(ab) \in \langle p\rangle$. Como todo ideal maximal em D é um ideal primo pelo teorema 1.37, $(ab) \in \langle p\rangle$ implica que $a \in \langle p\rangle$ ou $b \in \langle p\rangle$, resultando $p \mid a$ ou $p \mid b$. □

Corolário 2.15. *Se p é um elemento irredutível em um PID e p divide o produto $a_1a_2\ldots a_n$, para $a_i \in D$, então $p \mid a_i$ para pelo menos um índice $i \in \{1,\ldots,n\}$.*

Demonstração. A prova deste corolário segue pelo Princípio de Indução Finita e do lema 2.14 □

Definição 2.16. *Um elemento não nulo p de um domínio de integridade D é primo se, para quaisquer a, $b \in D$ tal que, $p \mid ab$ então $p \mid a$ ou $p \mid b$.*

Teorema 2.17. *Todo PID é um UFD.*

Demonstração. O Teorema 2.12 afirma que se D é um PID, então cada $a \in D$, onde a não é o elemento neutro e não é uma unidade de D, tem uma fatoração, digamos, $a = p_1p_2\ldots p_r$, com cada p_i elemento irredutível em D.
Resta-nos mostrar a unicidade a menos de um arranjo nos índices.
Para tanto, suponha que

$$a = q_1q_2\ldots q_s$$

seja outra fatoração em elementos irredutíveis.
Assim, temos que $p_1 \mid (q_1q_2\ldots q_s)$ o que implica $p_1 \mid q_j$ para algum j, pelo corolário 2.15.
Alterando a ordem dos $q_j's$ se necessário, podemos assumir que $j = 1$ logo $p_1 \mid q_1$.
Dessa forma $q_1 = p_1u_1$, e como p_1 é um irredutível segue que u_1 é uma unidade, ou seja, p_1 e q_1 são associados.
Temos então,

$$p_1p_2\ldots p_r = p_1u_1q_2\ldots q_s.$$

Como D é domínio de integridade segue pela proposição 1.12 temos que

$$p_2\ldots p_r = u_1q_2\ldots q_s.$$

Continuando esse processo, começando agora com p_2, obtemos:

$$1 = u_1 u_2 \dots u_r q_{r+1} \dots q_s.$$

Como o q_j é irredutível, necessariamente $r = s$. □

Corolário 2.18. *Se F é corpo então $F[X]$ é um UFD.*

Demonstração. Se F é um corpo sabemos pelo teorema 1.71 que $F[X]$ é PID. E pelo teorema 2.17 todo PID é UFD, portanto F corpo implica $F[X]$ UFD. □

Corolário 2.19. *O domínio de integridade $\mathbb{Z}$ é um UFD.*

Demonstração. Como $\mathbb{Z}$ é PID, segue pelo teorema 2.17 que é UFD. □

Observação 2.20. Veremos mais adiante no exemplo 2.34 que nem todo UFD é um PID, ou seja, a afirmação recíproca do teorema 2.17 é falsa.

A partir de agora estamos interessados em demonstrar que se F é um UFD então o anel de polinômios $F[X]$ também é um UFD. Para tanto precisamos da seguinte definição.

Definição 2.21. *Sejam D um UFD e $a_1, a_2, ..., a_n$ elementos não nulos de D. Um elemento d de D é um máximo divisor comum (mdc) de todos os a_i se $d \mid a_i$ para $i = 1, ..., n$ e qualquer outro $d' \in D$ que divida a_i também divide d.*

Observação 2.22. Chamamos d "um"máximo divisor comum em vez de "o"máximo divisor comum porque máximos divisores comuns são definidos a menos de unidades. De fato, suponha que d e d' sejam dois máximos divisores comuns de $a_i, \dots, a_n$.
Logo, $d \mid d'$ e $d' \mid d$ pela definição.
Assim $d = q'd'$ e $d' = qd$ para determinados $q, q' \in D$. Logo

$$1d = q'qd \Rightarrow q'q = 1 \Rightarrow qq' \in U(D).$$

Exemplo 2.23. Vamos encontrar um máximo divisor comum entre 420, -168 e 252 no UFD $\mathbb{Z}$.

Fatorando, obtemos

$$420 = 2^2.3.5.7, -168 = 2^3.(-3).7 \text{ e } 252 = 2^2.3^2.7.$$

Escolhemos um desses três números, digamos 420, e procuramos a maior potência de cada um de seus fatores irredutíveis (a menos de associados) que divide todos os números, $420, -168$ e 252 em nosso caso. Tomamos como mdc o produto dessas potências, mais altas, de irredutíveis. Para nosso exemplo, essas potências de fatores irredutíveis de 420 são $2^2, 3^1, 5^0$ e 7^1, de modo que tomamos como máximo divisor comum $d = \text{mdc}$ $(420, -168, 252) = 4.3.1.7 = 84$. Veja também que mdc $(420, -168, 252) = -84$ isso porque 1 e -1 são as únicas unidades.

Definição 2.24. *Seja D um UFD. Um polinômio não constante $f(X) = a_0 + a_1X + \dots + a_nX^n$ em $D[X]$ é primitivo se 1 é um máximo divisor comum dos a_i para $i \in 0, 1, ..., n$, isto é, mdc $(a_0, a_1, \dots, a_n) = 1$.*

Exemplo 2.25. Em $\mathbb{Z}[X]$, $4X^2 + 3X + 2$ é primitivo pois mdc $(4, 3, 2) = 1$, mas $4X^2 + 6X + 2$ não, já que mdc $(4, 6, 2) = 2 \notin U(\mathbb{Z})$.

Observe que todo polinômio irredutível não-constante em $D[X]$ é necessariamente um polinômio primitivo.

Lema 2.26. *Se D é um UFD, então para cada polinômio não constante $f(X) \in D[X]$ temos $f(X) = (c)g(X)$, onde $c \in D$, $g(X) \in D[X]$ é primitivo. O elemento c é único a menos de um fator unidade em D e é chamado conteúdo de $f(X)$. Também $g(X)$ é único a menos de um fator unidade em D.*

Demonstração. Seja $f(X) \in D[X]$ dado, onde $f(X)$ é um polinômio não-constante com os coeficientes $a_0, a_1, \ldots, a_n$. Seja $c =$ mdc $(a_0, a_1, \ldots, a_n)$. Então para cada $i \in 1, \ldots, n$ temos $a_i = cq_i$ para algum $q_i \in D$.
Pela lei distributiva, temos: $f(X) = a_0 + a_1X + \ldots + a_nX^n = cq_0 + cq_1X + \ldots + cq_nX^n = (c)g(X)$, onde nenhum irredutível em D divide todos os coeficientes $q_0, q_1, ..., q_n$ de $g(X)$, ou seja, mdc $(q_0, q_1, \ldots, q_n) = 1$. Assim, $g(X)$ é um polinômio primitivo.
Provemos a unicidade de c : se $f(X) = (d)h(X)$ para $d \in D$, $h(X) \in D[X]$, com $h(X)$ primitivo, então cada fator irredutível de c deve dividir d e vice-versa.
Considerando $(c)g(X) = (d)h(X)$ e cancelando os fatores irredutíveis de c em d, obtemos $(u)g(X) = (v)h(X)$ com $u \in U(D)$. Mas então v deve ser uma unidade de D ou poderíamos cancelar fatores irredutíveis de v em u. Portanto, u e $v \in U(D)$, logo, c é único a menos de um fator unidade. Além disso, a partir de $f(X) = (c)g(X)$, vemos que o polinômio primitivo $g(X)$ também é único a menos de um fator unidade. □

Exemplo 2.27. Em $Z[X], 4X^2 + 6X - 8 = (2)(2X^2 + 3X - 4)$, onde $2X^3 + 3X - 4$ é primitivo.

Lema 2.28. *(Lema de Gauss) Se D é um UFD, então um produto de dois polinômios primitivos em $D[X]$ é ainda primitivo.*

Demonstração. Considere $f(X) = a_0 + a_1X + ... + a_nX^n$ e $g(X) = b_0 + b_1X + ... + b_mX^m$ primitivos em $D[X]$, e seja $h(X) = f(X)g(X)$.
Seja p um irredutível em D. Então p não divide todos a_i e p não divide todos b_j, pois $f(X)$ e $g(X)$ são primitivos, logo, mdc $(a_0, \ldots, a_n) = 1 =$ mdc $(b_0, \ldots, b_m)$.
Seja a_r o primeiro coeficiente de $f(x)$ não divisível por p; isto é, $p \mid a_i$ para $i < r$, mas $p \nmid a_r$. Da mesma forma, considere $p \mid b_j$, para $j < s$, mas $p \nmid b_s$.
O coeficiente de X^{r+s} em $h(X) = f(X)g(X)$ é

$$c_{r+s} = (a_0b_{r+s} + \ldots + a_{r-1}b_{s+1}) + a_rb_s + (a_{r+1}b_{s-1} + \ldots + a_{r+s}b_0).$$

Agora como $p \mid a_i$, para $i < r$, segue que $p \mid (a_0b_{r+s} + \ldots + a_{r-1}b_{s+1})$ e também como $p \mid b_j$, para $j < s$, temos $p \mid (a_{r+1}b_{s-1} + \ldots + a_{r+s}b_0)$.
Mas p não divide a_r ou b_s, logo p não divide a_rb_s e, consequentemente, p não divide c_{r+s}.
Isto mostra que dado um irredutível $p \in D$, existe algum coeficiente de $f(X)g(X) = h(X)$ não divisível por p. Portanto $h(X)$ é primitivo. □

Corolário 2.29. *Se D é um UFD, então um produto finito de polinômios primitivos em $D[X]$ é ainda primitivo.*

Demonstração. Este corolário segue do lema 2.28 e pelo Princípio de Indução Finita. □

Lema 2.30. *Sejam D um UFD e F um corpo de frações de D. Se $f(X)$ é um polinômio irredutível e não constante, em $D[X]$, então $f(X)$ é também polinômio irredutível em $F[X]$. Além disso, se $f(X)$ é primitivo em $D[X]$ e irredutível em $F[X]$, então $f(X)$ é irredutível em $D[X]$.*

Demonstração. Suponha que um polinômio não constante $f(X) \in D[X]$ se fatora em polinômios de menor grau em $F[X]$, isto é, $f(X) = r(X)s(X)$ para $r(X), s(X) \in F[X]$ e $\partial r < \partial f$ e $\partial s < \partial f$. Assim, como F é o corpo das frações de D, cada coeficiente em $r(X)$ e $s(X)$ é da forma $\frac{a}{b}$ para determinados $a \in D$ e $b \in D^*$.

Digamos que $r(X) = \frac{a_n}{b_n}X^n + \frac{a_{n-1}}{b_{n-1}}X^{n-1} + \ldots + \frac{a_1}{b_1}X + \frac{a_0}{b_0}$

e

$$s(X) = \frac{p_l}{q_l}X^l + \frac{p_{l-1}}{q_{l-1}}X^{l-1} + \ldots + \frac{p_1}{q_1}X + \frac{p_0}{q_0},$$

logo,

$$r(X) = \frac{1}{b_n b_{n-1} \ldots b_1 b_0}\left(a_n(b_{n-1}\ldots b_1 b_0)X^n + a_{n-1}(b_n b_{n-2}\ldots b_1 b_0)\,X^{n-1} + \ldots\right.$$

$$\left. + a_1(b_n \ldots b_2 b_0)X + a_0(b_1 \ldots b_2 b_1)\right) \Rightarrow b_n b_{n-1}\ldots b_1 b_0\; r(X) = a_n(b_{n-1}\ldots b_1 b_0)X^n +$$

$$a_{n-1}(b_n b_{n-2}\ldots b_1 b_0)X^{n-1} + \ldots + a_1(b_n \ldots b_2 b_0)X + a_0(b_1 \ldots b_2 b_1) := r_1(X).$$

Do mesmo modo:

$$q_l(q_{l-1}\ldots q_1 q_0)s(X) = p_l(q_{l-1}\ldots q_1 q_0)X^l + p_{l-1}(q_n q_{l-2}\ldots q_1 q_0)X^{l-1} + \ldots$$

$$+ p_1(q_1 \ldots q_2 q_0)X + p_0(q_l \ldots q_2 q_1) := s_1(X).$$

Assim,

$$f(X) = r(X)s(X) \Rightarrow (b_n \ldots b_1 b_0)(q_l \ldots q_1 q_0)s(X) = r_1(X)s_1(X) \Rightarrow df(X) = r_1(X)s_1(X)$$

em que $r_1(X)$ e $s_1(X)$ pertencem a $D[X]$ e $d \in D$ e $d = b_n \ldots b_1 b_0 q_l \ldots q_1 q_0 \in D$, mais ainda $\partial r_1 = \partial r$ e $\partial s_1 = \partial s$, respectivamente.

Pelo lema 2.26, $f(X) = (c)g(X), r_1(X) = (c_1)r_2(X)$, e $s_1(X) = (c_2)s_2(X)$ para polinômios primitivos $g(X), r_2(X)$ e $s_2(X)$ em $D[X]$, e $c, c_1, c_2 \in D$. Logo, $(dc)g(X) = (c_1c_2)r_2(X)s_2(X)$, e pelo lema 2.28, $r_2(X)s_2(X)$ é primitivo. Pela parte da unicidade do lema 2.26 segue que $c_1c_2 = dcu$, para $u \in U(D)$. Ou seja, com isso $(dc)g(X) = (dcu)r_2(X)s_2(X)$, assim $f(X) = (c)g(X) = (cu)r_2(X)s_2(X)$. Mostramos que se $f(x)$ fatora não trivialmente em $F[X]$, então $f(X)$ fatora não trivialmente em polinômios de mesmos graus em $D[X]$. Portanto, se $f(X) \in D[X]$ é irredutível em $D[X]$, necessariamente é irredutível em $F[X]$. Um polinômio não constante $f(X) \in D[X]$ que é primitivo em $D[X]$ e irredutível em $F[X]$ é também irredutível em $D[X]$, já que $D[X] \subseteq F[X]$. □

Corolário 2.31. *Se D é um UFD e F é um corpo das frações de D, então um polinômio não constante $f(X) \in D[X]$, se fatora em um produto de dois polinômios $r(X)$ e $s(X)$ tais que $\partial r < \partial f$ e $\partial s < \partial f$ em $F[X]$ se, e somente se, $f(X)$ tem uma fatoração em polinômios de mesmos graus em $r(X)$ e $s(X)$ em $D[X]$.*

Demonstração. ($\Rightarrow$) Segue da demonstração do lema 2.30.

($\Leftarrow$) Vale já que $D[X] \subseteq F[X]$.

□

Estamos agora preparados para provar nosso principal teorema.

Teorema 2.32. *Se D é um UFD, então $D[X]$ é um UFD.*

Demonstração. Seja $f(X) \in D[X]$, em que $f(X)$ é um polinômio não nulo e $f(X) \notin U(D[X])$. Se $f(X)$ é de grau 0, já obtemos a decomposição em elementos irredutíveis, já que D é um UFD.

Suponha que $\partial f(X) > 0$ e seja $f(X) = g_1(X)g_2(X)\dots g_r(X)$ uma fatoração de $f(X)$ em $D[X]$ em que r é o maior número possível de fatores de graus positivos, ($\partial g_i > 0, \forall\, i \in \{1, \dots, r\}$). Agora cada fator e cada $g_i(X)$ como $g_i(X) = c_i h_i(X)$ onde c_i é o conteúdo de $g_i(X)$ e $h_i(X)$ é um polinômio primitivo cuja existência é garantida pelo lema 2.26. Cada um dos $h_i(X)$ é irredutível, porque se ele pudesse ser fatorado, nenhum dos fatores poderia pertencer a D, logo todos teriam grau positivo e implicaria numa fatoração correspondente de $g_i(X)$, contradizendo a escolha de r, já que teríamos uma fatoração de $f(X)$ com mais de r fatores de grau positivo. Assim, temos

$$f(X) = c_1 h_1(X) c_2 h_2(X) \dots c_r h_r(X)$$

onde $h_i(X)$ são irredutíveis em $D[X]$.

Se fatoramos agora cada c_i em irredutíveis em D, obtemos uma fatorização de $f(X)$ em um produto de irredutíveis em $D[X]$.

Sobre a unicidade, veja que se a fatoração de $f(X) \in D[X]$, onde $f(X)$ tem grau 0, é única, uma vez que D é um UFD. Se $f(X)$ tem grau maior que 0, podemos ver qualquer fatoração de $f(X)$ em irredutíveis em $D[X]$, como uma fatoração em $F[X]$ em unidades (isto é, os fatores em D) e polinômios irredutíveis em $F[X]$ pelo lema 2.30. Pelo teorema 1.75, esses polinômios são únicos, exceto por possíveis fatores constantes em F. Mas visto como um irredutível em $D[X]$, cada polinômio de grau maior que zero que aparece na fatoração de $f(X)$ em $D[X]$ é primitivo. Pela unicidade do lema 2.26, isso mostra que esses polinômios são únicos em $D[X]$ a menos de fatores unidades, isto é, associados. O produto dos irredutíveis em D na fatoração de $f(X)$ é o conteúdo de $f(X)$, que é novamente único a menos de unidade pelo lema 2.26. Portanto, todos os irredutíveis em $D[X]$ que aparecem na fatoração são únicos a menos de ordem e elementos associados. □

Corolário 2.33. *Se F é um corpo e $X_1, \dots, X_n$ são variáveis indeterminadas, então $F[X_1, \dots, X_n]$ é um UFD.*

Demonstração. Pelo corolário 2.18, $F[X_1]$ é um UFD. Pelo teorema 2.32, $(F[X_1])[X_2] = F[X_1, X_2]$ também é UFD. Continuando esse processo, vemos pelo Princípio de Indução Finita que a $F[X_1, \dots X_n]$ é um UFD. □

Exemplo 2.34. Se F é um corpo e X e Y são variáveis indeterminadas então $F[X,Y]$ é UFD pelo corolário 2.33. Considere N o conjunto de todos os polinômios em X e Y pertencentes a $F[X,Y]$ tendo termo constante nulo, ou seja, $N = \langle X, Y \rangle$.

Veja que N é um ideal de $F[X,Y]$ porém não é ideal principal já que não há mais como eliminar nenhum gerador. Portanto, $F[X,Y]$ não é um PID.

3 Domínio euclidiano

No que segue estamos interessados em tratar de domínios de integridade em que é possível estabelecer um algoritmo da divisão, a saber, domínios euclidianos. Para tanto a seguinte definição é crucial. Tais domínios euclidianos são exemplos interessantes de PID e de UFD como veremos no teorema 3.4 e no corolário 3.5.

Definição 3.1. *Uma norma euclidiana em um domínio de integridade D é uma função v que aplica os elementos não nulos de D em $\mathbb{Z}_+$ de forma que as seguintes condições sejam satisfeitas:*

1. *Para quaisquer $a, b \in D$ com $b \neq 0$, existem q e r em D tais que $a = bq + r$, com $r = 0$ ou $v(r) < v(b)$.*

2. *Para quaisquer $a, b \in D$, com $a \neq 0$ e $b \neq 0$, $v(a) \leqslant v(ab)$.*

Ao par (D, v) denominamos domínio euclidiano, ou seja, um domínio de integridade é um domínio euclidiano se existir uma norma euclidiana v em D. Além disso o algoritmo dado na condição 1 é chamado algoritmo euclidiano.

Exemplo 3.2. O domínio de integridade $\mathbb{Z}$ é um domínio euclidiano, pois a função v definida por $v(n) =\mid n \mid$ para $n \neq 0$ em $\mathbb{Z}$ é uma norma euclidiana em $\mathbb{Z}$. Veja que a condição 1 é garantida pelo algoritmo de divisão para $\mathbb{Z}$. Enquanto que a condição 2 segue da propriedade $\mid a \mid \leqslant \mid a \mid\mid b \mid = \mid ab \mid$ e $\mid a \mid \geqslant 1$, $a \neq 0$ em $\mathbb{Z}$.

Exemplo 3.3. Se F é um corpo, então $F[X]$ é um domínio Euclidiano, para a função v definida por $v\,(f(X)) = \partial f$ para $f(X) \in F[X]$, e $f(X) \neq 0$, é uma norma euclidiana. A Condição 1 é válida pelo teorema 1.66 e a Condição 2, segue já que o grau do produto da soma de dois polinômios é a soma de seus graus.

Teorema 3.4. *Todo domínio euclidiano é um PID.*

Demonstração. Seja D um domínio euclidiano com uma norma euclidiana v, e considere N ideal em D qualquer. Queremos mostrar que $\exists\, b \in D$ tal que $N = \langle b \rangle$, ou seja, N é um ideal principal.
Se $N = \{0\}$, então $N = \langle 0 \rangle$ e N é principal.
Suponha que $N \neq \{0\}$, logo existe $b \neq 0$ em N.
Escolha b tal que $v(b)$ é mínimo entre todos $v(n)$ para $n \in N$ o que é garantido pelo Princípio do Menor Inteiro aplicado ao conjunto $\{v(n) : n \in N\} \subset \mathbb{Z}_+$.
Considere $a \in N$, qualquer, então pela Condição 1 da definição 3.1 existem q e r em D tais que $a = bq + r$, com $r = 0$ ou $v(r) < v(b)$.
Agora $r = a - bq$ e $a, b \in N$, de modo que $r \in N$ já que N é um ideal.

Assim, $v(r) < v(b)$ é impossível pela escolha de b, logo necessariamente $r = 0$ e então $a = bq \in \langle b \rangle$.
Portanto, $N = \langle b \rangle$. □

Corolário 3.5. *Todo domínio euclidiano é um UFD.*

Demonstração. Pelo teorema 3.4, um domínio euclidiano é um PID e pelo teorema 2.17, um PID é um UFD. □

Vamos agora investigar algumas propriedades dos domínios euclidianos relacionados a sua estrutura multiplicativa. Veremos que podemos usar a condição 2 de uma norma euclidiana para caracterizar os elementos de $U(D)$.

Teorema 3.6. *Para um domínio euclidiano D com uma norma euclidiana v, $v(1)$ é o valor mínimo entre todos os valores $v(a)$ para $a \neq 0$ e $a \in D$.*
Ainda, $u \in U(D)$ se, e somente se, $v(u) = v(1)$.

Demonstração. ($\Rightarrow$) Pela condição 2 segue que para $a \neq 0$: $v(1) \leqslant v(1a) = v(a)$.
Por outro lado, se u é uma unidade em D, então, $v(u) \leqslant v(uu^{-1}) = v(1)$.
Assim, $v(u) = v(1)$ para $u \in U(D)$.

($\Leftarrow$) Suponha que $u \in D$, $u \neq 0$, seja tal que $v(u) = v(1)$.
Então, pela condição 1, existem q e r em D, tais que $1 = uq + r$, com, $r = 0$ ou $v(r) < v(u)$.
Mas como $v(u) = v(1)$ é mínimo entre todos os $v(d)$ para $d \in D$, $d \neq 0$, $v(r) < v(u)$ não ocorre.
Daí $r = 0$ e consequentemente $1 = uq$, ou seja, $u \in U(D)$.

□

Exemplo 3.7. Para $\mathbb{Z}$ com $v(n) = |n|$, o mínimo de $v(n) \in \mathbb{Z}_+$ com $n \in \mathbb{Z}$, $n \neq 0$, é 1. Sabemos que e 1 e -1 são os únicos elementos de $\mathbb{Z}$ com $v(n) = 1$ e ainda $U(\mathbb{Z}) = \{-1, 1\}$, ou seja, -1 e 1 são exatamente as unidades de $\mathbb{Z}$, comprovando assim a afirmação do teorema 3.6.

Exemplo 3.8. Para $F[X]$ com $v(f(X)) = \partial f(X)$, para $f(X) \neq 0$, o valor mínimo de $v(f(X))$ para todos os não nulos $f(X) \in F[X]$ é 0. Os polinômios não nulos de grau 0 são exatamente os elementos não nulos de F, e essas são precisamente as unidades de $F[X]$, ou seja, $U(F[X]) = F^*$.

Vejamos agora uma generalização do algoritmo de divisão dado no teorema 1.66.

Teorema 3.9. *(Algoritmo Euclidiano) Seja D um domínio Euclidiano com uma norma Euclidiana v, e sejam a e b elementos não-nulos de D. Considere r_1 como na Condição 1 da definição 3.1 para uma norma Euclidiana, isto é, $a = bq_1 + r_1$ em que $r_1 = 0$ ou $v(r_1) < v(b)$. Se $r_1 \neq 0$, seja r_2 tal que $b = r_1q_2 + r_2$, onde $r_2 = 0$ ou $v(r_2) < v(r_1)$. Mais geralmente, de modo indutivo, seja r_{i+1}, tal que $r_{i-1} = r_iq_{i+1} + r_{i+1}$, em que $r_{i+1} = 0$ ou $v(r_{i+1}) < v(r_i)$. Nestas condições, $r_1, r_2, \ldots$ necessariamente termina com algum $r_s = 0$. Se $r_1 = 0$, então b é um máximo divisor comum de a e b. Se $r_1 \neq 0$ e r_s é o primeiro $r_i = 0$, então um máximo divisor comum de a e b será r_{s-1}. Além disso, se d é um máximo divisor comum de a e b, então existem λ e μ em D tais que $d = \lambda a + \mu b$.*

Demonstração. Como $v(r_i) < v(r_{i-1})$ e $v(r_i)$ é um inteiro não negativo, segue-se que, após um número finito de passos, devemos obter $r_s = 0$, para algum s.

Se $r_1 = 0$, então $a = bq_1$ e b é um máximo divisor comum de a e b. Suponha $r_1 \neq 0$. Então, se $d \mid a$ e $d \mid b$, temos $d \mid (a - bq_1)$, consequentemente $d \mid r_1$. No entanto, se $d_1 \mid r_1$ e $d_1 \mid b$, então $d_1 \mid (bq_1 + r_1)$, assim $d_1 \mid a$. Portanto, o conjunto de divisores comuns de a e b é o mesmo conjunto que o conjunto de divisores comuns de b e r_1. Por um argumento análogo, se $r_2 \neq 0$, o conjunto de divisores comuns de b e r_1 é o mesmo conjunto que o conjunto de divisores comuns de r_1 e r_2. Continuando este processo, vemos finalmente que o conjunto de divisores comuns de a e b é o mesmo conjunto que o conjunto de divisores comuns de r_{s-2} e r_{s-1}, em que r_s é o primeiro r_i igual a 0. Dessa forma, um maximo divisor comum de r_{s-2} e r_{s-1} também é um máximo divisor comum de a e b. Mas a equação

$$r_{s-2} = q_s r_{s-1} + r_s = q_s r_{s-1}$$

mostra que um máximo divisor comum de r_{s-2} e r_{s-1} é r_{s-2}. Resta mostrar que podemos expressar um máximo divisor comum d de a e b como $d = \lambda a + \mu b$. No que fizemos acima, se $d = b$, então $d = 0a + 1b$ e terminamos. Se $d = r_{s-1}$, então, podemos expressar cada r_i na forma $\lambda_i r_{i-1} + \mu_i r_{i-2}$ para determinados $\lambda_i, \mu_i \in D$. Para ilustrar usando o primeiro passo, a partir da equação $r_{s-3} = q_{s-1} r_{s-2} + r_{s-1}$ obtemos

$$d = r_{s-1} = r_{s-3} - q_{s-1} r_{s-2}. \tag{3.1}$$

Agora, expressamos r_{s-2} em termos de r_{s-3} e r_{s-4} e substituímos em (3.1) para escrever d em termos de r_{s-3} e r_{s-4}. Eventualmente, teremos

$$d = \lambda_3 r_2 + \mu_3 r_1 = \lambda_3(b - r_1 q_2) + \mu_3 r_1 = \lambda_3 b + (\mu_3 - \lambda_3 q_2) r_1 = \lambda_3 b + (\mu 3 - \lambda_3 q_2)(a - bq_1)$$

o que pode ser escrito na forma $d = \lambda a + \mu b$. Se d' é qualquer outro máximo divisor comum de a e b, então $d' = ud$, para alguma unidade u, então $d' = (\lambda u)a + (\mu u)b$. □

Exemplo 3.10. : Ilustraremos o algoritmo euclidiano para a norma Euclidiana $|\ |$ em $\mathbb{Z}$, calculando um máximo divisor comum de 22.471 e 3.266. Para tanto, basta aplicar o algoritmo de divisão do teorema 3.9 repetidamente, o último resto que aparece não nulo é o mdc. Usando a notação do teorema 3.9, temos:

	$a = 22.471$
	$b = 3.266$
$22.471 = (3.266)6 + 2.875$	$r_1 = 2.875$
$3.266 = (2.875)1 + 391$	$r_2 = 391$
$2.875 = (391)7 + 138$	$r_3 = 138$
$391 = (138)2 + 115$	$r_4 = 115$
$138 = (115)1 + 23$	$r_5 = 23$
$115 = (23)5 + 0$	$r_6 = 0$

Assim, r_5 é um máximo divisor comum de 22.471 e 3.266. Com esse procedimento encontramos um máximo divisor comum sem fazer uma fatoração. Isso é importante, pois, por vezes, é muito difícil encontrar uma fatoração de um inteiro em primos.

Exemplo 3.11. Observe que a condição 1 do algoritmo de divisão na definição de uma norma Euclidiana não diz nada sobre r ser "positivo". Ao calcular um mdc em $\mathbb{Z}$ pelo algorítmo euclidiano para $|\ |$, como no exemplo 3.10, certamente é de nosso interesse

tornar o $|r_1|$ o menor possível em cada divisão. Assim, repetindo o exemplo 3.10, seria mais eficiente escrever:

$$\begin{array}{cc} & a = 22.471 \\ & b = 3.266 \\ 22.471 = (3.266)7 - 391 & r_1 = -391 \\ 3.266 = (391)8 + 138 & r_2 = 138 \\ 391 = (138)3 - 23 & r_3 = -23 \\ 138 = (23)6 + 0 & r_4 = 0 \end{array}$$

Podemos mudar o sinal do r_i de negativo para positivo quando desejamos, uma vez que os divisores da r_1 e $-r_1$ são os mesmos.

4 Inteiros gaussianos e Normas multiplicativas

Finalizamos esta dissertação com um exemplo não usual de domínio euclidiano (e portanto um exemplo não canônico tanto de PID quanto de UFD), cuja natureza é diferente de $\mathbb{Z}$ e $F[X]$. Para tanto iniciamos com a abordagem sobre inteiros gaussianos.

4.1 Inteiros gaussianos

Definição 4.1. *Um inteiro gaussiano (ou inteiro de Gauss) é um número complexo $a+bi$, em que $a, b \in \mathbb{Z}$.*
Para um inteiro gaussiano $\alpha = a+bi$, a norma $N(\alpha)$ de α é a^2+b^2.

Denotamos por $\mathbb{Z}[i]$ o conjunto de todos os inteiros de Gauss. O lema a seguir apresenta algumas propriedades básicas da função norma $N : \mathbb{Z}[i] \to \mathbb{Z}_+$ que são necessárias para a demonstração do teorema 4.4. Observe que $\mathbb{Z} \subset \mathbb{Z}[i] \subset \mathbb{C}$.

Lema 4.2. *As seguintes propriedades da função norma N são válidas para quaisquer $\alpha, \beta \in \mathbb{Z}[i]$:*

1. $N(\alpha) \geqslant 0$;
2. $N(\alpha) = 0$ *se, e somente se,* $\alpha = 0$;
3. $N(\alpha\beta) = N(\alpha)N(\beta)$.

Demonstração. Considerando $\alpha = a_1 + a_2 i$ e $\beta = b_1 + b_2 i$, temos:

1. $N(\alpha) := a^2 + b^2 \geq 0$. Portanto, $N(\alpha) \geqslant 0$.
2. $(\Rightarrow)$ $0 = N(\alpha) = a^2 + b^2 \Rightarrow a^2 + b^2 = 0$, com $a, b \in \mathbb{Z} \Rightarrow a = 0 = b \Rightarrow \alpha = 0$.
   $(\Leftarrow)$ Se $\alpha = 0$ então $a = 0 = b$, logo: $N(\alpha) = a^2 + b^2 = 0^2 + 0^2 = 0$
3. $N(\alpha\beta) = N((a_1 + a_2 i) \cdot (b_1 + b_2 i)) = N((a_1 b_1 - a_2 b_2) + i(a_1 b_2 + b_1 a_2)) =$
   $= (a_1 b_1 - a_2 b_2)^2 + (a_1 b_2 + b_1 a_2)^2 =$
   $= [(a_1 b_1)^2 - 2(a_1 b_1)(a_2 b_2) + (a_2 b_2)^2] + [(a_1 b_2)^2 + 2(a_1 b_2)(b_1 a_2) + (b_1 a_2)^2] =$
   $= (a_1 b_1)^2 + (a_2 b_2)^2 + (a_1 b_2)^2 + (b_1 a_2)^2 = a_1^2 b_1^2 + a_1^2 b_2^2 + a_2^2 b_1^2 + a_2^2 b_2^2 =$
   $= (a_1^2 + a_2^2) \cdot (b_1^2 + b_2^2) = N(\alpha)N(\beta)$.

□

Lema 4.3. $(\mathbb{Z}[i], +, .)$, *com as operações* $(+)$ *e* $(\cdot)$ *induzidas de* $\mathbb{C}$ *é um domínio de integridade.*

Demonstração. : Veja que $\mathbb{Z}[i]$ é um anel comutativo com unidade, pelo exemplo 1.8. Mostremos que $\mathbb{Z}[i]$ não tem divisores de zero: se $\alpha, \beta \in \mathbb{Z}[i]$ são tais que $\alpha\beta = 0$ então, pelo lema 4.2, $N(\alpha)N(\beta) = N(\alpha\beta) = N(0) = 0$, logo $N(\alpha)N(\beta) = 0$.

Assim, $\alpha\beta = 0$ implica que $N(\alpha) = 0$ ou $N(\beta) = 0$. Ainda pelo lema 4.2, isso implica que $\alpha = 0$ ou $\beta = 0$. Assim, $\mathbb{Z}[i]$ não tem divisores de 0.
Portanto $\mathbb{Z}[i]$ é um domínio de integridade. □

Teorema 4.4. *A função* v *dada por* $v(\alpha) = N(\alpha)$, *para* $\alpha \neq 0 \in \mathbb{Z}[i]$, *é uma norma euclidiana em* $\mathbb{Z}[i]$, *ou seja,* $(\mathbb{Z}[i], v)$ *é um domínio euclidiano.*

Demonstração. Verifiquemos a condição 2 da definição 3.1: para $\beta = b_1 + b_2 i \neq 0$, em $\mathbb{Z}[i]$, temos $N(\beta) = N(b_1 + b_2 i) = b_1^2 + b_2^2 \geq 1$, pois b_1 ou b_2 é não nulo.

Logo, $N(\beta) \geq 1$, para qualquer $\beta \neq 0$ em $\mathbb{Z}[i]$.

Desta forma, para $\alpha \neq 0$ e $\beta \neq 0$ em $\mathbb{Z}[i]$, temos $N(\alpha\beta) = N(\alpha)N(\beta) \geqslant N(\alpha)1 = N(\alpha)$. Ou seja, $N(\alpha) \leqslant N(\alpha\beta)$.

Provemos a condição 1, a saber, o algoritmo de divisão para N.

Sejam $\alpha, \beta \in \mathbb{Z}[i]$ quaisquer, com $\alpha = a_1 + a_2 i$ e $\beta = b_1 + b_2 i$, onde $\beta \neq 0$.

Devemos encontrar σ e ρ em $\mathbb{Z}[i]$ de tal forma que $\alpha = \beta\sigma + \rho$, em que $\rho = 0$ ou $N(\rho) < N(\beta) = {b_1}^2 + {b_2}^2$.

Em $\mathbb{C}$, considere $\dfrac{\alpha}{\beta} = r + si$ para $r, s \in \mathbb{Q}$.

Afirmação: Dados r, $s \in \mathbb{Q}$ existem q_1, $q_2 \in \mathbb{Z}$ tais que:

$$|r - q_1| \leqslant \frac{1}{2} \text{ e } |s - q_2| \leqslant \frac{1}{2}. \tag{4.1}$$

Com efeito, dado $r \in \mathbb{Q}$, podemos afirmar que $r \in [a, b]$, com a, $b \in \mathbb{Z}$ e

$$b - a = 1. \tag{4.2}$$

Suponha que $|r - q_1| > \dfrac{1}{2}$ para todo $q_1 \in \mathbb{Z}$.

Dessa forma teríamos $b - a = (b - r) + (r - a) > \dfrac{1}{2} + \dfrac{1}{2} = 1$, o que contradiz (4.2).

Portanto, a afirmação é verdadeira.

Analogamente, existe $q_2 \in \mathbb{Z}$ tal que $|s - q_2| \leqslant \dfrac{1}{2}$.

Tomemos $\sigma = q_1 + q_2 i$ e $\rho = \alpha - \beta\sigma$.

Se $\rho = 0$ está provado, caso contrário por (4.1) e pela construção de σ, temos:

$$N\left(\frac{\alpha}{\beta} - \sigma\right) = N((r + si) - (q_1 + q_2 i)) = N((r - q_1) + (s - q_2)i) =$$

$$(r - q_1)^2 + (s - q_2)^2 = |\, r - q_1 \,|^2 + |\, s - q_2 \,|^2 \leqslant \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2}.$$

Assim,

$$N(\rho) = N(\alpha - \beta\sigma) = N\left(\beta\left(\frac{\alpha}{\beta} - \sigma\right)\right) = N(\beta)N\left(\frac{\alpha}{\beta} - \sigma\right) \leqslant N(\beta)\frac{1}{2}, \tag{4.3}$$

Por (4.1), segue que

$$N(\rho) \leq \frac{N(\beta)}{2} < N(\beta) \Rightarrow N(\rho) < N(\beta).$$

Portanto, $N(\rho) < N(\beta)$. □

Exemplo 4.5. Podemos aplicar todos os resultados do capítulo 3 sobre domínios euclidianos ao $(\mathbb{Z}[i], v)$.
Em particular, como $N(1) = 1$, as unidades do $\mathbb{Z}[i]$ são exatamente os elementos $\alpha = a_1 + a_2 i$ em que $N(\alpha) = a_1^2 + a_2^2 = 1$.
Veja que como a_1 e a_2 são números inteiros, segue então que as únicas possibilidades para que $a_1^2 + a_2^2 = 1$ são: $a_1 = \pm 1$ com $a_2 = 0$, ou $a_1 = 0$ com $a_2 = \pm 1$.
Assim, as unidades de $\mathbb{Z}[i]$ são:

$$u_1 = 1,\ u_2 = -1,\ u_3 = i \text{ e } u_4 = -i, \text{ ou seja, } U(\mathbb{Z}[i]) = \{-1, 1, -i, i\}.$$

Também é possível usar o algorítmo euclidiano para calcular o m.d.c. de dois elementos diferentes de zero em $\mathbb{Z}[i]$.

Note ainda, que 5 é um irredutível em $\mathbb{Z}$, porém 5 não é mais um irredutível em $\mathbb{Z}[i]$, pois $5 = (1 + 2i)(1 - 2i)$ e nem $(1 + 2i)$ nem $(1 - 2i)$ pertencem a $U(\mathbb{Z}[i])$.

4.2 Normas multiplicativas

Na seção 4.1 tratamos da norma para $\mathbb{Z}[i]$. Nesta presente seção abordaremos norma de modo mais geral, a saber, norma multiplicativa para um domínio de integridade D, qualquer.

Definição 4.6. *Seja D um domínio de integridade, qualquer. Uma norma multiplicativa N em D é uma função que aplica cada elemento de D em um número inteiro em $\mathbb{Z}$, de tal forma que as seguintes condições são satisfeitas:*

1. *$N(\alpha) = 0$ se, e somente se, $\alpha = 0$;*
2. *$N(\alpha\beta) = N(\alpha)N(\beta)$, para quaisquer $\alpha, \beta \in D$.*

Teorema 4.7. *Se D é um domínio de integridade com uma norma multiplicativa N, então $N(1) = 1$ e $|N(u)| = 1$ para cada elemento $u \in U(D)$.*
Se, além disso, todo α tal que $|N(\alpha)| = 1$ é um elemento de $U(D)$, então todo elemento ρ em D, com $|N(\rho)| = p$, com $p \in \mathbb{Z}$ número primo, é um irredutível de D.

Demonstração. Seja D um domínio de integridade com uma norma multiplicativa N.
Então: $N(1) = N((1)(1)) = N(1)N(1)$ mostra que $N(1) = 1$.
Além disso, se o u é uma unidade em D, então

$$1 = N(1) = N(uu^{-1}) = N(u)N(u^{-1}).$$

Como $N(u)$ é um inteiro, isso implica que $|N(u)| = 1$.
Agora suponha que as unidades de D sejam exatamente os elementos de D com norma igual a ± 1 e seja $\rho \in D$ tal que $|N(\rho)| = p$, onde p é um primo em $\mathbb{Z}$.
Então, se $\rho = \alpha\beta$, temos: $p = |N(\rho)| = |N(\alpha)N(\beta)|$, então $|N(\alpha)| = 1$ ou $|N(\beta)| = 1$.
Por suposição, isso significa que α ou β é uma unidade de D. Assim ρ é um irredutível de D. □

Exemplo 4.8. Para $\mathbb{Z}[i]$, a função N definida por $N(a+bi) = a^2+b^2$ fornece uma norma multiplicativa no sentido da nossa definição.
Vimos que a função v dada por $v(\alpha) = N(\alpha)$ para $\alpha \in \mathbb{Z}[i]$, com α diferente de zero, é uma norma euclidiana em $\mathbb{Z}[i]$, portanto as unidades são precisamente os elementos α de $\mathbb{Z}[i]$ com $N(\alpha) = N(1) = 1$.
Assim, a segunda parte do teorema 4.7 se aplica a $\mathbb{Z}[i]$.
Vimos no exemplo 4.5 que 5 não é irredutível em $\mathbb{Z}[i]$, pois $5 = (1-2i)(1+2i)$.
Como $N(1+2i) = N(1-2i) = 1^2+2^2 = 5$ e 5 é um primo em $\mathbb{Z}$, vemos pelo teorema 4.7 que $1+2i$ e $1-2i$ são ambos irredutíveis em $\mathbb{Z}[i]$.
Ou seja, o teorema 4.7 é uma ferramenta útil para tratar de irredutibilidade em um domínio de integridade.

Como uma aplicação de norma mutiplicativa, daremos agora um exemplo de um domínio de integridade que não é um UFD.

Exemplo 4.9. Veja que pelo exemplo 1.8 item 2 temos que $\mathbb{Z}[\sqrt{-5}]$ é um anel comutativo com unidade. Para ser domínio de integridade basta mostrar que $\mathbb{Z}[\sqrt{-5}]$ não tem divisores de zero. Para tanto definimos a função N, por:

$$\begin{array}{rccc} N: & \mathbb{Z}[\sqrt{-5}] & \to & \mathbb{Z}_+ \\ & a+b\sqrt{-5} & \mapsto & N(a+b\sqrt{-5}) := a^2+5b^2 \end{array}$$

Veja que $\mathbb{Z}[\sqrt{-5}]$ não tem divisores de zero.
Suponha que α, $\beta \in \mathbb{Z}[\sqrt{-5}]$ são tais que:

$$\begin{gathered} \alpha\beta = 0 \Rightarrow N(\alpha\beta) = N(0) = 0 \Rightarrow \\ N(\alpha)N(\beta) = N(\alpha\beta) = 0 \Rightarrow \\ N(\alpha)N(\beta) = 0 \Rightarrow N(\alpha) = 0 \text{ ou } N(\beta) = 0 \Rightarrow \\ \alpha = 0 \text{ ou } \beta = 0. \end{gathered}$$

Veja que N é uma norma multiplicativa em $\mathbb{Z}[\sqrt{-5}]$, pois:

1. $N(\alpha) = 0$ se, e somente se, $\alpha = a+b\sqrt{-5} = 0$, ou seja,

$$0 = N(\alpha) = N(a+b\sqrt{5}i) \Leftrightarrow a^2+5b^2 = 0 \Leftrightarrow a = 0 = b \Leftrightarrow \alpha = 0.$$

   Ou seja, $N(\alpha) = 0 \Leftrightarrow \alpha = 0$.

2. $N(\alpha\beta) = N(\alpha)N(\beta)$.
   Considerando $\alpha = a_1 + a_2\sqrt{5}i$ e $\beta = b_1 + b_2\sqrt{5}i$.
   Desta forma $N(\alpha\beta) = N((a_1+a_2\sqrt{5}i)(b_1+b_2\sqrt{5}i)) =$

$$N((a_1b_1-5a_2b_2)+(a_1b_2+a_2b_1)\sqrt{5}i) = (a_1b_1-5a_2b_2)^2+5(a_1b_2+a_2b_1)^2 =$$

$$a_1^2b_1^2 - 10a_1b_1a_2b_2 + 25a_2^2b_2^2 + 5a_1^2b_2^2 + 10a_1b_2a_2b_1 + 5a_2^2b_1^2 =$$

$$a_1^2b_1^2 + 5a_1^2b_2^2 + 5a_2^2b_1^2 + 25a_2^2b_2^2 = N(a_1+a_2\sqrt{5}i)N(b_1+b_2\sqrt{5}i) = N(\alpha)N(\beta).$$

Dessa maneira, pelo teorema 4.7 temos que os elementos α de $\mathbb{Z}[\sqrt{-5}]$ candidatos a unidades em $\mathbb{Z}[\sqrt{-5}]$ são aqueles que $N(\alpha) = 1$. Agora, se $\alpha \in \mathbb{Z}[\sqrt{-5}]$ e $N(\alpha) = 1$ temos $a^2 + 5b^2 = 1$ e isso só é possível se $b = 0$ e $a = \pm 1$.
Portanto, $U(\mathbb{Z}[\sqrt{-5}]) = \{-1, 1\}$, já que os candidatos $-1, 1$ são de fato irredutíveis em $\mathbb{Z}[\sqrt{-5}]$. Ou seja, $\alpha \in U(\mathbb{Z}[\sqrt{-5}]) \Leftrightarrow \mid N(\alpha) \mid = 1$.

Mostremos agora que $\mathbb{Z}[\sqrt{-5}]$ não é um UFD. Com efeito, veja que:

$$21 = 3 \cdot 7$$

e

$$21 = (1 + 2\sqrt{-5}) \cdot (1 - 2\sqrt{-5}).$$

Ocorre que $3, 7, (1+2\sqrt{-5})$ e $(1-2\sqrt{-5})$ são irredutíveis em $\mathbb{Z}[\sqrt{-5}]$, pelo teorema 4.7, e portanto 21 admite duas fatorações distintas e consequentemente $\mathbb{Z}[\sqrt{-5}]$ não é UFD.

Resta-no mostrar a irredutibilidade dos elementos $3, 7, 1 + 2\sqrt{-5}$ e $1 - 2\sqrt{-5}$ em $\mathbb{Z}[\sqrt{-5}]$; faremos isto via o teorema 4.7.

- 3 e 7 são irredutíveis em $\mathbb{Z}[\sqrt{-5}]$, pois: suponha que $3 = \alpha\beta \Rightarrow N(3) = N(\alpha\beta) \Rightarrow N(\alpha)N(\beta) = 9$.
  Então $9 = N(3) = N(\alpha)N(\beta)$ mostra que devemos ter $N(\alpha) = 1, 3$ ou 9. Se $N(\alpha) = 1$, então α é uma unidade.
  Se $\alpha = a + b\sqrt{-5}$, então $N(\alpha) = a^2 + 5b^2$, e para escolha alguma de inteiros a e b é possível $N(\alpha) = 3$.
  Se $N(\alpha) = 9$, então $N(\beta) = 1$, então β é uma unidade.
  Assim, de $3 = \alpha\beta$, podemos concluir que α ou β é uma unidade.
  Portanto, 3 é irredutível em $\mathbb{Z}[\sqrt{-5}]$.
  Um argumento similar mostra que 7 é também irredutível em $\mathbb{Z}[\sqrt{-5}]$.

- $1 + 2\sqrt{-5}$ e $1 - 2\sqrt{-5}$ são irredutíveis em $\mathbb{Z}[\sqrt{-5}]$, de fato: Se $1 + 2\sqrt{-5} = \gamma\delta$, temos $21 = N(1 + 2\sqrt{-5}) = N(\gamma)N(\delta)$.
  Assim $N(\gamma) = 1, 3, 7$, ou 21.
  Vimos que não há nenhum elemento de $\mathbb{Z}[\sqrt{-5}]$ da norma 3 ou 7.
  Isso é $N(\gamma) = 1$, e γ é uma unidade, ou $N(\gamma) = 21$, portanto $N(\delta) = 1$, e δ é uma unidade.
  Portanto, $1 + 2\sqrt{-5}$ é um irredutível em $\mathbb{Z}[\sqrt{-5}]$.
  Analogamente, $1 - 2\sqrt{-5}$ também é um irredutível em $\mathbb{Z}[\sqrt{-5}]$.

Referências

[1] Domingues, H.; Iezzi, G. Álgebra Moderna, 4.ed. São Paulo: Atual. (2003).

[2] Fraleigh, J. B.; *A first course in Abstract Algebra*, 7.ed. New York: Person Education. (2003).