UNIVERSIDADE ESTADUAL DA PARAÍBA

CENTRO DE CIÊNCIAS E TECNOLOGIA

DEPARTAMENTO DE MATEMÁTICA

CURSO DE LICENCIATURA EM MATEMÁTICA

Anéis de Polinômios sobre Anéis Comutativos

WALLACE FERREIRA GOMES

CAMPINA GRANDE - PB

Abril de 2016

WALLACE FERREIRA GOMES

Anéis de Polinômios sobre Anéis Comutativos

Trabalho de Conclusão de Curso apresentado ao curso de Licenciatura em Matemática do Departamento de Matemática e Estatística do Centro de Ciências e Tecnologia da Universidade Estadual da Paraíba em cumprimento às exigências legais para obtenção do título de licenciado em Matemática.

Orientador: Dr. Vandenberg Lopes Vieira

CAMPINA GRANDE-PB

Abril de 2016

WALLACE FERREIRA GOMES

Anéis de Polinômios sobre Anéis Comutativos

Trabalho de Conclusão de Curso apresentado ao curso de Licenciatura em Matemática do Departamento de Matemática e Estatística do Centro de Ciências e Tecnologia da Universidade Estadual da Paraíba em cumprimento às exigências legais para obtenção do título de licenciado em Matemática.

Aprovado em: 19 / Abril /2016

COMISSÃO EXAMINADORA

Prof. Dr. Vandenberg Lopes Vieira
Dpto. Matemática - CCT/UEPB
ORIENTADOR

Prof. Ms. José Ginaldo de Souza Farias
Dpto. Matemática - CCT/UEPB
EXAMINADOR

Prof. Ms. Walber Santiago Colaço

G633a Gomes, Wallace Ferreira
Anéis de polinômios sobre anéis comutativos [manuscrito] / Wallace Ferreira Gomes. - 2016.
64 p.

Digitado.
Trabalho de Conclusão de Curso (Graduação em Matemática) - Universidade Estadual da Paraíba, Centro de Ciências e Tecnologia, 2016.
"Orientação: Prof. Drº Vandenberg Lopes Vieira, Departamento de Matemática".

1.Anéis de Polinômios. 2.Anéis Comutativos. 3. Teoria dos Anéis. 4. Domínios Euclidianos. I. Título.

21. ed. CDD 516.2

Dedicatória

Dedico este trabalho a minha esposa, Sr^{a} Rosilda da Silva, e aos meus filhos Asafe Miguel e João Gabriel. Aos meus familiares e amigos; enfim, a todos que sempre me incentivaram e, acima de tudo, me compreenderam.

Agradecimentos

Ao meu Senhor Jesus, por sempre estar ao meu lado e ter me dado todas as condições para que eu pudesse chegar ao singelo lugar onde estou, mas que foi o qual desejei.

Declaro ainda minha gratidão aos professores do Departamento de Matemática que tão diretamente influenciaram nessa conquista, ou ainda, não só influenciaram, mas que foram os principais responsáveis para que eu tivesse força para chegar até aqui. Em especial aos maiores incentivadores e responsáveis pelo crescimento no ramo da Álgebra Abstrata: Ernesto Trajano, Daniel Cordeiro, Fernando Luiz, José Ginaldo, Maria Isabella. Em particular, agradeço ao meu orientador, o Dr. Vandenberg Lopes Vieira, por ter sido tão decisivo no direcionamento da minha vida acadêmica e à quem devo boa parte dos frutos que casualmente eu venha a colher.

Ainda no âmbito acadêmico, eu não poderia passar sem dizer o meu "Muito obrigado"aos colegas de sala remanescentes da turma 2011.2, por me acompanharem até este ponto deste caminhada.

Aos meus pais Edilma Ferreira e Fábio Gomes, por não ter me deixado faltar nada na vida que realmente eu necessita-se, e por terem se dedicado a minha educação e formação da minha personalidade. Agradeço também aos meus familiares que sempre me incentivaram e me apoiaram, colocaram-se a disposição para ajudar de qualquer maneira, em especial a minha Avó , Maria do Carmo (que Deus a tenha ao seu lado) e as Minhas Tias, Eridan e Edna, por serem uma segunda mãe nesta terra, pois não negaram o seu auxilio em qualquer oportunidade. Bem como a minha irmã, Renally, por sempre me incentivar nos estudos acadêmicos .

Ainda, a minha esposa, Sr^{a} Rosilda da Silva, por ter sido minha fiel companheira, escalada por Jesus para jogar essa partida até o fim da vida, sendo compreensiva e amável, estando sempre ao meu lado nas batalhas que passei aqui nesta instituição. E mais, por ter sido uma das minhas motivações para o termino do curso e por pretender não parar os meus estudos na área da Álgebra Abstrata.

Por fim, mas não menos importante, eu deixo os agradecimentos aos meus grandes, velhos e maravilhosos amigos. Foram eles quem mais me seguraram e, principalmente, suportaram as minhas lamentações, e ouviram minhas dificuldades, sem jamais deixar de incentivar e mostrar extrema confiança no meu potencial (até mais do que deviam, diga-se de passagem).

Obrigado a Luciano Soares, Francielly Gomes, Naelson Silva e ao meu companheiro João Eudes. E para não esquecer, agradeço a todos os meus queridos mangás, HQs, Séries, Filmes e Novelas por estarem sempre ao meu lado nestes últimos anos.

E sim para não esquecer e ser subjugado, agradeço a minha irmã Vitoria Rennika Ferreira Gomes, por ser a pessoa que é.

Epígrafe

"Para conseguir grandes coisas, é necessário não apenas planejar, mas também acreditar; não apenas agir, mas também sonhar."

(Nagato Pain)

Resumo

Neste trabalho, abordarmos os Anéis de Polinômios sobre Anéis Comutativos, em que os mesmo são resultados importantes para estudos mais aprofundados na Álgebra Comutativa e na Teoria Algébrica dos Números. Como este trabalho se trata de um trabalho de conclusão de curso em nível de graduação, procuramos utilizar o caminho mais pratico para o leitor desenvolver o intersere em estudos mais avançados nas áreas já supracitadas. Após um resumo preliminar da teoria básica dos anéis, introduzimos conceitos de Anéis de polinômios e demonstramos os principais teoremas relacionados a domínios fatoriais e euclidianos. Enunciamos e Demonstramos o Teorema de Gauss que conclui que se um anel $\mathcal{R}$ é Domínio de Fatoração Única então o Anel de Polinômio $\mathcal{R}[X]$ também é um Domínio de Fatoração Única.

Palavras chave: Domínios, Corpos, Anéis Fatoriais, Anéis Euclidianos, Anéis Principais, Equações Diofantinas.

Abstract

In this work, we discuss the Polynomials rings over commutative rings, in which the same are important results for further study in Commutative Algebra and Algebraic Number Theory. As this work is not a completion of course work at the undergraduate level, we try to use the most practical way for the reader develop intersere in more advanced studies in the areas already mentioned above. After a preliminary summary of the basic theory of rings, we introduced polynomials rings concepts and demonstrate the main theorems related domains Factorial and Euclidean. Enunciated and demonstrate the Gauss theorem that concludes that a ring $\mathcal{R}$ is Factorization Domain Only then the polynomial ring $\mathcal{R}[X]$ is also a Unique Factorization Domain .

Key words: *Domains, Fields, Factorial Rings, Euclidean Rings, Principal Rings, Diophantine Equations.*

Sumário

Introdução

A Teoria dos Anéis é um ramo da Álgebra Abstrata que se dedica ao estudo de anel, domínio e corpo. O termo anel[1] foi utilizado primeiramente por Hilbert[2] no final do século XIX. Já o conceito de anéis foi finalmente introduzido por Dedekind[3]. A Teoria dos Anéis foi desenvolvida a partir do estudo de anéis de polinômio em n variáveis e dos números inteiros. No decorrer deste trabalho destacaremos importantes definições e resultados referentes à essa teoria, tais como: Se tivermos um corpo $\mathcal{K}$ e $\mathcal{P}$ como sendo seu corpo primo, se a característica de $\mathcal{K}$ for prima, temos que $\mathcal{P}$ é isomorfo a $\mathbb{Z}_p$; e se a característica de $\mathcal{K}$ for zero, teremos que $\mathcal{P}$ é isomorfo a $\mathbb{Q}$.

Dentre os conceitos estudados em álgebra, o conceito de domínio de fatoração única tem importância ímpar, uma vez que sendo um anel comutativo em que todo elemento não-nulo e diferente da unidade se escreve como produto de irredutives. Tais elementos apresentam propriedades similares às propriedades que são estudadas nos números inteiros em um curso de Teoria dos Números. De fato, temos que em geral, é possível provar que todo Domínio Euclidiano é um domínio de fatoração única. Daremos uma demonstração de que se um anel é um Domínio de Fatoração Única, então o anel de polinômios de n-variáveis construído sobre esse anel é também um domínio de fatoração única. Assumiremos também familiaridade com conceitos e definições básicas da Teoria dos Números, como os conceitos de congruencial modulo m, e relações de equivalência; e da Teoria dos Grupos, os conceitos de homomorfismo, núcleo de um homomorfismo e teorema de lagrange.

[1] O termo original usado por Hilbert foi zahlring.

[2] David Hilbert (1862-1943) foi um notável matemático alemão. Dentre suas contribuições merece ser destacado os *Espaços de Hilbert* e 23 problemas que o mesmo deixou, conhecidos como os *Problemas de Hilbert*.

[3] Julius Wilhelm Richard Dedekind (1831-1916) foi um matemático alemão.

Objetivos

Neste trabalho temos como objetivo principal mostrar e provar alguns resultados relevantes sobre a Teoria Básica dos Anéis, destacar algumas relações com resultados vistos primeiramente em um curso básico de Teoria dos Números, e posteriormente finalizarmos com o Teorema de Gauss, que refere-se à uma consequência de que, se tivermos um anel E fatorial (Domínio de Fatoração Única), então o anel de polinômios $E[X]$ também é fatorial.

Os objetivos específicos são:

- Demonstrar algumas resultados que são válidos no domínio dos inteiros, e expandi-los para um domínio qualquer.
- Apresentar e provar o teorema que afirma que se E é um domínio fatorial(DFU), então o anel de polinômios $E[X]$ também é fatorial.
- Despertar o interesse do leitor para os estudos da Álgebra Comutativa ou da Teoria Algébrica dos Números.

Justificativa

Ao estudarmos os conceitos das estruturas algébricas básicas, como o grupo e o anel, podemos perceber que determinados resultados são validos somente para estruturas comutativas. Este fato em conjunto com a possibilidade de tratarmos de estruturas com duas operações, torna o estudo de anéis mais interessantes do que o de grupos. Em álgebra, temos uma área que trabalha essencialmente com o estudo de anéis comutativos, a Álgebra Comutativa, e é com foco para estudos posteriores nesta área que decidimos construir, esse trabalho.

Para os leitores que querem seguir os estudos em Álgebra Abstrata, especialmente em estudos avançados da Teoria dos Números, especialmente na Teoria Algébrica dos Números[4], irá encontrar neste trabalho os principais tópicos relacionados à Teoria Algébrica, com exceção dos relacionados ao conceito de modulo que poderá ser encontrado em [5].

[4]Temos que a Teoria Algébrica dos Números é um ramo da Teoria dos Números Clássica na qual os conceitos presentes inicialmente são expandidos para os números algébrico e tem fortes raízes na Teoria dos Anéis.

Capítulo 1

Conceitos Preliminares

Neste capítulo, apresentaremos os resultados básicos da Teoria dos Anéis que serão usados nos capítulos seguintes. Admitiremos já conhecidos os conceitos e resultados básicos sobre conjuntos, relações de equivalência, funções, operações e grupos. Explanaremos conceitos de anéis e subanéis, domínios e corpos, homomorfismo de anéis, corpo de frações de um domínio, ideais e anéis quocientes. Por fim, vamos destacar de forma especial os ideais primos e maximais que serão de importância ímpar na explanação dos domínios fatoriais (DFU), no Capítulo 3.

1.1 Anéis

Definição 1.1. *Um conjunto não vazio $\mathcal{R}$ munido de duas operações, uma adição e uma multiplicação, indicadas por "+" e "$\cdot$", respectivamente, é dito um* ***anel*** *quando as seguintes propriedades são satisfeitas:*

(1) A operação de adição define uma estrutura de grupo abeliano sobre $\mathcal{R}$;

(2) A multiplicação é associativa, isto é,

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c, \ \forall \ a, \ b, \ c \in \mathcal{R}.$$

(3) A multiplicação é distributiva tanto pela direita, quanto pela esquerda em relação à adição, isto é,

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad e \quad (a + b) \cdot c = a \cdot c + b \cdot c, \ \forall \ a, \ b, \ c \in \mathcal{R}.$$

Sendo assim, se $\mathcal{R}$ é um anel, o mesmo será indicado por $(\mathcal{R}, +, \cdot)$. No entando, quando não houver dúvida quanto às operações consideradas sobre $\mathcal{R}$, vamos indicar simplesmente por $\mathcal{R}$. Além disso, ao invés de expressarmos a operação entre elementos por $a \cdot b$, vamos usar ab para simplificar a notação.

Definição 1.2. *Um anel $\mathcal{R}$ é dito* ***comutativo*** *quando a operação de multiplicação é comutativa, ou seja,*

$$a \cdot b = b \cdot a \quad , \forall \quad a, b \in \mathcal{R}.$$

Definição 1.3. *Diz-se que um anel $\mathcal{R}$ tem unidade, ou simplesmente, que é um* ***anel com unidade****, quando existe o elemento neutro da operação multiplicação, ou seja,*

$$\exists\ 1 \in \mathcal{R},\ \textit{tal que, } a1 = 1a = a,\ \forall\ a \in \mathcal{R}.$$

Exemplo 1.1. *Munidos da operação adição e multiplicação usuais, temos que $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, são exemplos triviais de anéis comutativos com unidade.*

Exemplo 1.2. *O conjunto das matrizes 2 por 2 com entradas reais denotado por $M_2(\mathbb{R})$ é um anel não comutativo com unidade, dada por:*

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

Exemplo 1.3. *Notemos que o conjunto $2\mathbb{Z}$ dos números inteiros pares é fechado em relação a adição e multiplicação usual, e que de fácil modo podemos verificar que $2\mathbb{Z}$ é um anel comutativo. No entanto, $2\mathbb{Z}$ não tem unidade.*

Sugerimos ao leitor verificar a construção do conjunto dos inteiros módulo n[1], denotado por $\mathbb{Z}_n$, em [1] e [11]. Considerando as seguintes operações em $\mathbb{Z}_n$:

$$\begin{array}{rccc} + : & \mathbb{Z}_n \times \mathbb{Z}_n & \to & \mathbb{Z}_n \\ & (\overline{a}, \overline{b}) & \mapsto & \overline{a} + \overline{b} = \overline{a+b} \end{array} \quad \text{e} \quad \begin{array}{rccc} \cdot : & \mathbb{Z}_n \times \mathbb{Z}_n & \to & \mathbb{Z}_n \\ & (\overline{a}, \overline{b}) & \mapsto & \overline{a} \cdot \overline{b} = \overline{a \cdot b} \end{array}.$$

Temos que, $(\mathbb{Z}_n, +, \cdot)$ é um anel comutativo com unidade.

Exemplo 1.4. *Seja d um inteiro que não é quadrado perfeito, então o conjunto*

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d}\ :\ a,\ b \in \mathbb{Z}\}$$

[1]Também é conhecido como o conjunto das classes de congruência módulo n ou como o conjunto das classes residuais módulo n.

com as operações

$$x + y = (a_1 + a_2) + (b_1 + b_2)\sqrt{d}$$

e

$$x \cdot y = (a_1a_2 + b_1b_2d) + (a_1b_2 + a_2b_1)\sqrt{d}$$

onde $x = a_1 + b_1\sqrt{d}$ *e* $y = a_2 + b_2\sqrt{d} \ \in \mathbb{Z}[\sqrt{d}]$*, é um anel comutativo com unidade, também chamado de anel quadrático. Em particular, ressaltamos que se* $d = -1$ *, o anel é dito* ***anel de inteiros de Gauss***[2] *(ou ainda* ***inteiros gaussianos****), e tem a seguinte configuração:*

$$\mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[i] = \{a + bi \ : \ a, \ b \ \in \mathbb{Z}\}.$$

Por fim, vamos considerar um conjunto muito peculiar, chamado de conjunto dos quatérnios, que trata de uma forma generalizada do conjunto dos números complexos. Tal conjunto foi descrito pela primeira vez pelo matemático irlandês Hamilton[3], onde de início teve papel fundamental no uso da mecânica, mas hoje tem aplicação em Geometria e da Teoria dos Números. Portanto, vamos definir e construir as operações adição e multiplicação neste conjunto. Consideremos,

$$\mathcal{Q} = \{a_0 + a_1i + a_2j + a_3k \ : \ a_t, \ t = 1, 2, 3, 4 \ \text{ e } \ i, \ j, \ k \text{ são unidades imaginárias.}\}.$$

Observe que, dados $q_1, \ q_2 \in \mathcal{Q}$, temos que

$$q_1 = q_2 \Leftrightarrow a_0 = b_0 \text{ e } a_1 = b_1 \text{ e } a_2 = b_2 \text{ e } a_3 = b_3.$$

Sobre $\mathcal{Q}$, definimos a adição da seguinte forma:

$$\begin{aligned} q_1 + q_2 &= (a_0 + a_1i + a_2j + a_3k) + (b_0 + b_1i + b_2j + b_3k) \\ &= (a_0 + b_0) + (a_1 + b_1)i + (a_2 + b_2)j + (a_3 + b_3)k. \end{aligned} \tag{1.1}$$

E a multiplicação é dada por:

$$\begin{aligned} q_1 \cdot q_2 \ &= \ (a_0 + a_1i + a_2j + a_3k) \cdot (b_0 + b_1i + b_2j + b_3k) \\ &= \ (a_0b_0 - a_1b_1 - a_2b_2 - a_3b_3) \ + \ (a_0b_1 + a_1b_0 + a_2b_3 - a_3b_2)i \\ &+ \ (a_0b_2 + a_2b_0 + a_3b_1 - a_1b_3)j \ + \ (a_0b_3 + a_3b_0 + a_1b_2 - a_2b_1)k. \end{aligned} \tag{1.2}$$

[2]Carl Friesrish Gauss, foi um matemático alemão que deu grandes contribuições à Matemática, principalmente na Teoria dos Números. Os inteiros de Gauss teve seu surgimento quando o mesmo pesquisava sobre reciprocidade cúbica.

[3]William Rowan Hamilton, um Fisico-matemático irlandês, teve alguns trabalhos fundamentados na Matemática, principalmente na área de Álgebra, tendo com destaque a descoberta do conjunto dos quartérnios, que na maioria dos livros é representado por $\mathbb{H}$. Sendo essa notação não universal.

No entanto, notemos que a seguinte relação, $i^2 = j^2 = k^2 = ijk = -1,\ ij = -ji = k,\ jk = -kj = i,\ ki = -ik = j$, foi utilizada na definição da multiplicação.

Exemplo 1.5. *O conjunto $\mathcal{Q}$ munido das operações de (1.1) e (1.2) é um anel não comutativo com unidade $1 = 1 + 0i + 0j + 0k \in \mathcal{Q}$.*

1.1.1 Propriedades Elementares de um Anel

Enunciaremos a seguir algumas propriedades relevantes e necessárias para a continuidade do nosso estudo.

Teorema 1.1. *Seja $\mathcal{R}$ um anel. Então, para quaisquer $a,\ b \in \mathcal{R}$, temos*

(1) $0 \cdot a = a \cdot 0 = 0$;

(2) $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$;

(3) $(-a) \cdot (-b) = a \cdot b$.

A demonstração do teorema anterior, não será apresentada.

Proposição 1.1. *Sejam $\mathcal{R}$ um anel e $a \in \mathcal{R}$. Então, para quaisquer $m, n \in \mathbb{N}$, tem-se*

(1) $a^n \cdot a^m = a^{(n+m)},\ \forall\ n,\ m \in \mathbb{N}$;

(2) $(a^n)^m = a^{nm},\ \forall\ n,\ m \in \mathbb{N}$.

Demonstração: Demonstraremos apenas a propriedade (2). Para isso, iremos utilizar indução sobre m. Para $m = 1$ temos

$$(a^n)^1 = a^{n \cdot 1} \Rightarrow a^n = a^n.$$

Agora suponhamos que para cada $m \in \mathbb{N}$,

$$(a^n)^m = a^{nm}.$$

Sendo assim,

$$a^{(a^n)^{m+1}} = a^{nm+n} = a^{nm} \cdot a^n = a^{n(m+1)}.$$

Portanto,

$$(a^n)^m = a^{nm},\ \forall\ n, m \in \mathbb{N}.$$

■

Lema 1.1 (Binômio de Newton)**.** *Sejam $\mathcal{R}$ um anel comutativo com unidade e $a,\ b \in \mathcal{R}$. Então,*

$$(a+b)^n = \sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) a^{n-k} \cdot b^k,\ \forall\ n\ \in \mathbb{N}.$$

Demonstração: Vamos utilizar indução sobre n, similarmente como na proposição anterior. Observe que, sendo

$$\mathcal{S} = \left\{ n \in \mathbb{N} : (a+b)^n = \sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) a^{n-k} \cdot b^k \right\}.$$

Para $n = 1$ temos que $1 \in \mathcal{S}$. Agora, suponhamos que a proposição seja válida para $n > 1$, isto é, $n \in \mathcal{S}$. Então

$$(a+b)^n = \sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) a^{n-k} \cdot b^k$$

Sendo assim, temos

$$\begin{aligned} a(a+b)^n &= a\left(\sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) a^{n-k} \cdot b^k \right) \\ &= a^{n+1} + \sum_{k=1}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) a^{n-k+1 \cdot b^k} \end{aligned}$$

e

$$\begin{aligned} (a+b)^n b &= \left(\sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) a^{n-k} \cdot b^k \right) b \\ &= a^{n+1} + \sum_{k=1}^{n} \left(\begin{array}{c} n \\ k-1 \end{array} \right) a^{n-k+1} \cdot b^k + b^{n+1} \end{aligned}$$

Como

$$\begin{aligned} (a+b)^{n+1} &= (a+b)^n (a+b) \\ &= (a+b)^n a + (a+b)^n b\ , \\ &= a(a+b)^n + (a+b)^n b \end{aligned}$$

temos que

$$\begin{aligned}(a+b)^{n+1} &= a^{n+1} + \sum_{k=1}^{n} \binom{n}{k} a^{n-k+1} \cdot b^k + \sum_{k=1}^{n} \binom{n}{k-1} a^{n-k+1} \cdot b^k + b^{n+1} \\ &= a^{n+1} + \sum_{k=1}^{n} \left[\binom{n}{k} + \binom{n}{k-1} \right] a^{n-k+1} b^k + b^{n+1} \\ &= a^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} a^{n-k+1} b^k + b^{n+1} \\ &= \sum_{k=0}^{n+1} \binom{n+1}{k} a^{n+1-k} b^k\end{aligned}$$

Logo, $n+1 \in \mathcal{S}$. Portanto, $\mathcal{S} = \mathbb{N}$. ■

1.1.2 Subanéis

O conceito de subanel de um anel $\mathcal{R}$ segue o mesmo principio do conceito de subgrupo de um grupo G, de modo que se torna conveniente ser estudado no nosso trabalho. Serão apresentados exemplos de subanéis e uma generalização da intersectação de subanéis que também é um subanel.

Definição 1.4. *Sejam $\mathcal{R}$ um anel e $\mathcal{S}$ um subconjunto não vazio de $\mathcal{R}$. Dizemos que $\mathcal{S}$ é um* ***subanel*** *de $\mathcal{R}$, se com as operações induzidas de $\mathcal{R}$, $\mathcal{S}$ também for um anel.*

Exemplo 1.6. *Se considerarmos um anel $\mathcal{R}$, temos que os subconjuntos, $\mathcal{S}_1 = \{0\}$ e $\mathcal{S}_2 = \mathcal{R}$ são subanéis de $\mathcal{R}$, chamados de* ***subanéis triviais****.*

Proposição 1.2. *Sejam $\mathcal{R}$ um anel e $\mathcal{S}$ um subconjunto não vazio de $\mathcal{R}$. Então $\mathcal{S}$ é um subanel se, e somente se, as seguintes propriedades são satisfeitas:*

(1) $\mathcal{S}$ é um subgrupo de $\mathcal{R}$,ou seja,

$$a - b \in \mathcal{S},\ \forall\ a,\ b \in \mathcal{S};$$

(2) $ab \in \mathcal{S},\ \forall\ a,\ b \in \mathcal{S}$.

Demonstração: A priori, note que se $\mathcal{S}$ é subanel, então as condições (1) e (2) são satisfeitas. Reciprocamente, sejam $a,\ b \in \mathcal{S}$. Como $0 \in \mathcal{S}$ então $0 - y = -y \in \mathcal{S}$. Assim $x - (-y) = x + y \in \mathcal{S}$. Analogamente, temos por (2) que $ab \in \mathcal{S}$. Logo, $\mathcal{S}$ está munido das operações do anel $\mathcal{R}$. ■

Exemplo 1.7. *Seja o anel dos inteiros $\mathbb{Z}$. O subconjunto*

$$\mathcal{S} = n\mathbb{Z} = \{nk \ : \ k \in \mathbb{Z}\},$$

é um subanel de $\mathbb{Z}$, onde $n \in \mathbb{Z}_+$. De fato, se $a, b \in \mathcal{S}$, então existem k_1, $k_2 \in \mathbb{Z}$ tais que $a = nk_1$ e $b = nk_2$. Logo,

$$a - b = nk_1 - nk_2 = n(k_1 - k_2) \in \mathcal{S},$$

pois $k_1 - k_2 \in \mathbb{Z}$. Por outro lado, temos

$$ab = (nk_1)(nk_2) = n(k_1k_2n) \in \mathcal{S},$$

pois $k_1k_2n \in \mathbb{Z}$. Portanto, $n\mathbb{Z}$ é um subanel de $\mathbb{Z}$.

Exemplo 1.8. *Sejam $\mathcal{R}$ um anel e $\mathcal{S}$ e $\mathcal{K}$ subanéis de $\mathcal{R}$. Então $\mathcal{S} \cap \mathcal{K}$ é um subanel de $\mathcal{R}$.*

Vamos omitir a solução do exemplo anterior, ressaltando que seu resultado pode ser generalizado da seguinte forma: se $\mathcal{S}_1, \mathcal{S}_2, \ldots, \mathcal{S}_n$ são subanéis de $\mathcal{R}$, então,

$$\bigcap_{i=1}^{n} \mathcal{S}_i,$$

é um subanel de $\mathcal{R}$. O mesmo não pode ser afirmado para

$$\bigcup_{i=1}^{n} \mathcal{S}_i,$$

pois, $\bigcup_{i=1}^{n} \mathcal{B}_i$ é um subanel de $\mathcal{A}$ se, e somente se,

$$\begin{aligned}
&\mathcal{B}_i \supset \mathcal{B}_1 \cup \mathcal{B}_2 \\
&\mathcal{B}_i \supset (\mathcal{B}_1 \cup \mathcal{B}_2) \cup \mathcal{B}_3 \\
&\quad \vdots \\
&\mathcal{B}_i \supset (\mathcal{B}_1 \cup \cdots \cup \mathcal{B}_{i-1} \cup \mathcal{B}_{i+1} \cup \cdots \cup \mathcal{B}_{n-1}) \cup \mathcal{B}_n,
\end{aligned}$$

para algum $i \in \{1, 2, \ldots, n\}$.

1.2 Domínios e Corpos

Nesta seção definindo domínio e corpo, e posteriormente apresentaremos resultados relacionados a ambas classes de anéis, pois esses anéis especiais serão de grande importância para o desenvolvimento do nosso estudo. A priori, definiremos o conceito de divisor de zero, onde esse fato é peça fundamental na definição de um domínio de integridade.

1.2.1 Domínios de Integridade

Definição 1.5. *Sejam $\mathcal{R}$ um anel e $a \in \mathcal{R}$ um elemento não nulo. Então a é dito um* ***divisor de zero*** *se existir $b \in \mathcal{R}$, $b \neq 0$ tal que,*

$$a \cdot b = 0 \quad ou \quad b \cdot a = 0.$$

Exemplo 1.9. *Para o anel $\mathcal{R} = M_2(\mathbb{R})$, temos*

$$\begin{pmatrix} 2\sqrt{5} & 0 \\ 7 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & x \end{pmatrix} = \begin{pmatrix} 2\sqrt{5}.0 + 0.0 & 2\sqrt{5}.0 + 0.x \\ 7.0 + 0.0 & 7.0 + 0.x \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

ou seja, os elementos utilizados na operação são divisores de zero.

Exemplo 1.10. *No anel $\mathcal{R} = \mathbb{Z}_6$, temos que $a = \bar{2}$ e $b = \bar{3}$ são divisores de zero em $\mathcal{R}$, pois*

$$\bar{2} \cdot \bar{3} = \overline{2 \cdot 3} = \bar{6} = \bar{0}.$$

Definição 1.6. *Seja $\mathcal{D}$ um anel comutativo com unidade. Então, $\mathcal{D}$ é dito um* ***domínio de integridade*** *(ou simplesmente um* ***domínio****), se $\mathcal{D}$ não tem divisores de zero.*

Exemplo 1.11. *Os anéis $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ e $(\mathbb{C}, +, \cdot)$ são todos exemplos clássicos de domínios.*

Exemplo 1.12. *Conforme vimos anteriormente, o anel $\mathcal{R} = \mathbb{Z}_6$ possui divisores de zero, e, portanto, não é um domínio.*

Teorema 1.2. *O anel $\mathcal{R} = \mathbb{Z}_n$ é um domínio se, e somente se, n é primo.*

Demonstração: Suponhamos inicialmente que n não seja primo e que $\mathbb{Z}_n$ seja um domínio. Então existem $a, b \in \mathbb{N}$, com $1 < a$, $b < n$, tais que $a \cdot b = n$. Dessa forma,

$$a \cdot b = n \Rightarrow \overline{a \cdot b} = \bar{n} \Rightarrow \bar{a} \cdot \bar{b} = \bar{n} = \bar{0},$$

ou seja, $\bar{a}$ e $\bar{b}$ são divisores de zero, o que contradiz o fato de $\mathbb{Z}_n$ ser domínio.

Agora, vamos supor que n é primo. Logo existem $\bar{a}$ e $\bar{b} \in \mathbb{Z}_n$, de modo

$$\bar{a} \cdot \bar{b} = \bar{0} \Rightarrow a \cdot b \equiv 0 \ (mod \ n) \Rightarrow n|a \cdot b \Rightarrow n|a \text{ ou } n|b,$$

pois n é primo.

Suponhamos que $n|a$, ou seja, $a = n \cdot k$, $k \in \mathbb{Z}$. Assim,

$$\bar{a} = \overline{n \cdot k} \Rightarrow \bar{a} = \bar{n} \cdot \bar{k} \Rightarrow \bar{a} = \bar{0} \cdot \bar{k} \Rightarrow \bar{a} = \bar{0},$$

que é um absurdo, $\mathbb{Z}_n$ é um domínio. ■

Exemplo 1.13. *O anel $\mathcal{R} = \mathbb{Z}_5$ é um domínio, pois $n = 5$ é primo.*

Proposição 1.3. *Um anel $\mathcal{D}$ é um domínio se, e somente se, todo elemento não nulo de $\mathcal{D}$ é regular com relação à multiplicação, ou seja, dados $a, b, c \in \mathcal{D}$,*

$$ab = ac \Rightarrow b = c.$$

Demonstração: Suponhamos que $\mathcal{D}$ seja um domínio e tomemos $a, b, c \in \mathcal{D}$, com $a \neq 0$. Logo,

$$ab = ac \Rightarrow ab - ac = 0 \Rightarrow a(b - c) = 0 \Rightarrow b = c.$$

Pois $\mathcal{D}$ é domínio, e $a \neq 0$. Assim a é regular.

Por outro lado, sejam $a, b, c \in \mathcal{D}$ tais que $ab = 0$. Devemos mostrar que $a = 0$ ou $b = 0$. Suponhamos que $a \neq 0$. Como $a \cdot 0 = 0$, e por hipótese a é regular, segue que

$$a \cdot b = 0 = a \cdot 0 \Rightarrow b = 0.$$

Assim, temos que $\mathcal{D}$ é um domínio. ■

Definição 1.7. *Sejam $\mathcal{R}$ um anel e $a \in \mathcal{R}$. Chamamos a de* ***elemento idempotente****, quando:*

$$a^2 = a.$$

É claro que 0 e 1 são sempre idempotentes. Os idempotentes 0 e 1 são chamados de **idempotentes triviais**.

Exemplo 1.14. *No anel $\mathbb{Z}_{15}$ todos os elementos idempotentes são $\overline{0}, \overline{1}, \overline{6}$ e $\overline{10}$, pois,*

$$\overline{6}^2 = \overline{36} = \overline{6} \quad e \quad \overline{10}^2 = \overline{100} = \overline{10}.$$

Proposição 1.4. *Seja $\mathcal{D}$ um domínio. Então os únicos elementos idempotentes são os elementos 0 e 1.*

Demonstração: Consideremos $a \in \mathcal{D}$ um elemento idempotente, então

$$a^2 = a \Rightarrow a^2 - a = 0 \Rightarrow a(a - 1) = 0 \Rightarrow a = 0 \text{ ou } a - 1 = 0 \Rightarrow a = 1,$$

pois $\mathcal{D}$ é domínio. Sendo assim, os únicos elementos idempotentes de um domínio são os elementos 0 e 1. ■

1.2.2 Corpos

Destacaremos aqui o conceito de **corpo**, que é um tipo bastante especial de anel e de importância essencial nos estudos posteriores sobre domínios principais e de fatoração única.

Observação 1. *Note que como $a \cdot 0 = 0$, para todo $a \in \mathcal{R}$, então $x = 0 \in \mathcal{R}$ não é invertível em $\mathcal{R}$, a menos que $\mathcal{R} = \{0\}$.*

Definição 1.8. *Seja $\mathcal{K}$ um anel comutativo com unidade, então $\mathcal{K}$ é dito um **corpo**, se todo elemento de $\mathcal{K}$ for invertível, ou seja, dado $a \in \mathcal{K}$, $a \neq 0$, existe $b \in \mathcal{K}$ tal que*

$$a \cdot b = 1.$$

Notemos que se considerarmos $\mathcal{K}^*$ como sendo o conjunto dos elementos não nulos de $\mathcal{K}$, de fácil modo verificamos que, o grupo multiplicativo sobre $\mathcal{K}$ é dado por

$$U_\bullet(\mathcal{K}) = \mathcal{K}^*,$$

visto que $U_\bullet(\mathcal{K})$ é o conjunto dos elementos invertíveis de $\mathcal{K}$ sob a multiplicação. Então, tendo isso em mãos, um corpo pode ser definido da seguinte forma:

Definição 1.9. *Um anel $\mathcal{K}$ comutativo com unidade, é um **corpo** se, e somente se, $\mathcal{K}^*$ é um grupo multiplicativo sob a multiplicação em $\mathcal{K}$, ou seja,*

$$U_\bullet(\mathcal{K}) = \mathcal{K}^*.$$

Exemplo 1.15. *Os anéis $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, e $(\mathbb{C}, +, \cdot)$ são todos exemplos clássicos de corpos. Notemos que $(\mathbb{Z}, +, \cdot)$ não é um corpo mesmo sendo um anel comutativo com unidade, pois $U_\bullet(\mathbb{Z}) = \{1, -1\} \neq \mathbb{Z}^*$.*

Exemplo 1.16. *O anel $(\mathbb{Z}[i], +, \cdot)$ não é um corpo, pois dado $a + bi \in \mathbb{Z}[i]$, temos*

$$\begin{aligned} (a+bi)^{-1} &= \frac{1}{a+bi} \\ &= \frac{1}{a+bi} \cdot \frac{a-bi}{a-bi} \\ &= \left(\frac{a}{a^2+b^2}\right) - \left(\frac{b}{a^2+b^2}\right) i \end{aligned} \quad .$$

Temos assim

$$\frac{a}{a^2+b^2} \notin \mathbb{Z} \quad e \quad \frac{b}{a^2+b^2} \notin \mathbb{Z}.$$

Teorema 1.3. *Todo corpo é um domínio.*

Demonstração: A priori, observemos que $\mathcal{K}$ é comutativo com unidade, então basta provarmos que $\mathcal{K}$ não possui divisores de zero. Para isso, sejam $a, b \in \mathcal{K}$, tais que $a \cdot b = 0$. Suponhamos que $a \neq 0$. Logo existe $a^{-1} \in \mathcal{K}$ para o qual $a \cdot a^{-1} = 1$. Sendo assim, temos

$$a \cdot b = 0 \Rightarrow a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 \Rightarrow a^{-1} \cdot 0 = 0,$$

ou ainda,

$$(a^{-1} \cdot a) \cdot b = 0 \Rightarrow 1 \cdot b = 0.$$

Portanto, $b = 0$. ■

Vale destacar que em anel a reciproca não é valida, no entanto, o teorema a seguir nos garanti que se o corpo for um domínio finito, então a reciproca é valida.

Teorema 1.4. *Todo domínio finito é um corpo.*

Demonstração: Consideremos $\mathcal{D}$ um domínio finito, por exemplo $\mathcal{D} = \{a_1, a_2, a_3, \ldots, a_n\}$. Queremos mostrar que, para cada $a \in \mathcal{D}$, com $a \neq 0$, existe $a^{-1} \in \mathcal{D}$ tal que $a \cdot a^{-1} = 1$. Consideremos a aplicação :

$$\begin{array}{rccc} f_a & : & \mathcal{D} & \longrightarrow & \mathcal{D} \\ & & a_i & \longmapsto & f_a(a_i) = aa_i \end{array}$$

Dados $a_i, a_j \in \mathcal{D}$,

$$f(a_i) = f(a_j) \Rightarrow aa_i - aa_j = 0 \Rightarrow a(a_i - a_j) = 0.$$

Como $a \neq 0$, e $\mathcal{D}$ é um domínio, temos $a_i = a_j$. Dessa forma, f_a é injetiva. Como $\mathcal{D}$ é finito, segue que f_a é sobrejetiva e, por isso, f_a é bijetiva. Isto significa que existe $a_i \in \mathcal{D}$ tal que $f_a(a_i) = 1$, ou ainda,

$$a \cdot a_i = 1.$$

Por conseguinte, se a é um elemento arbitrário não nulo de $\mathcal{D}$, mostramos que ele é invertível. Portanto, $\mathcal{D}$ é um corpo. ■

Para simplificação de notação quando conveniente, se $\mathcal{K}$ for um corpo e $a, b \in K$, com $b \neq 0$, então indicaremos $a \cdot b^{-1}$ por $\frac{a}{b}$, e chamaremos de quociente de a por b.

Definição 1.10. *Seja $\mathcal{R}$ um anel com unidade. Se existir algum $n \in \mathbb{N}$ tal que*

$$n \cdot a = 0 \ , \ \forall a \in \mathcal{R},$$

então ao menor deles chama-se ***característica de*** $\mathcal{R}$ *e diz-se que* $\mathcal{R}$ *tem característica positiva. Caso contrário, diremos que* $\mathcal{R}$ *tem característica zero. Denotaremos tal característica* $\mathcal{R}$ *por* $car(\mathcal{R})$.

Proposição 1.5. *Se* $\mathcal{K}$ *é um corpo finito, então* $car(\mathcal{K}) = p$, *sendo* p *um número primo.*

Demonstração: Sejam $\mathcal{K}$ um corpo finito e $car(\mathcal{K}) = p$. Suponhamos que p não é primo. Então, existem m e $n \in \mathbb{N}$, com $1 < m, n < p$, tal que

$$0 = p \cdot 1 = (m \cdot n)1 = m(n \cdot 1) = (m \cdot 1) \cdot (n \cdot 1).$$

O que é um absurdo, pois $\mathcal{K}$ é domínio. Logo, $car(\mathcal{K}) = p$, com p sendo um número primo. ■

Teorema 1.5. *Sejam* $\mathcal{K}$ *um corpo finito de característica* p *e* $q = p^r$, *para algum* $r \in \mathbb{N}$. *Então,* $(a + b)^q = a^q + b^q$.

Demonstração: Como o teorema binomial é valido sobre um corpo, então dados a, $b \in \mathcal{K}$, temos

$$(a + b)^p = a^p + \begin{pmatrix} p \\ 1 \end{pmatrix} a^{p-1} \cdot b + \ldots + \begin{pmatrix} p \\ p-1 \end{pmatrix} a \cdot b^{p-1} + b^p.$$

Como para cada $\begin{pmatrix} p \\ i \end{pmatrix}$, $0 < i < p$, que é um inteiro, e a mesma equivale a

$$\frac{p(p-1)\ldots(p-i+1)}{1 \cdot 2 \cdot \ldots \cdot i},$$

então, $1 \cdot 2 \cdot \ldots \cdot i$ divide $p(p-1)\ldots(p-i+1)$. Mas p é primo e $i < p$, logo em particular $1 \cdot 2 \cdot \ldots \cdot i$ divide $(p-1)\ldots(p-i+1)$. Assim, $\begin{pmatrix} p \\ i \end{pmatrix} \equiv 0 \ (mod \ p)$. E mais, temos que $car(\mathcal{K}) = p$, então

$$\begin{pmatrix} p \\ 1 \end{pmatrix} a^{p-1}b = \begin{pmatrix} p \\ 2 \end{pmatrix} a^{p-2}b^2 = \ldots = \begin{pmatrix} p \\ p-1 \end{pmatrix} ab^{p-1} = 0.$$

Desse modo,

$$(a + b)^p = a^p + b^p.$$

Por conseguinte, se $q = p^r$, então com uma simples indução sobre r, obtemos que $(a + b)^q = a^q + b^q$. ■

Definição 1.11. *Sejam $\mathcal{K}$ um corpo e $\mathcal{F}$ um subconjunto não vazio de $\mathcal{K}$. Diremos que $\mathcal{F}$ é um* ***subcorpo*** *de $\mathcal{K}$ quando, com as operações induzidas de $\mathcal{K}$, o mesmo também é um corpo, ou seja, $\mathcal{F}$ é um subcorpo se, e somente se, as seguintes condições são satisfeitas:*

(1) $a - b \in \mathcal{F}, \forall\ a,\ b \in \mathcal{F}$;

(2) $a \cdot b^{-1} \in \mathcal{F}, \forall\ a,\ b \in \mathcal{F}, b \neq 0$.

Exemplo 1.17. *Consideremos o corpo $\mathbb{R}$ e o subconjunto $\mathcal{F} = \{a + b\sqrt{2} : \ \ a, b \in \mathbb{Q}\}$ de $\mathbb{R}$. Então $\mathcal{F}$ é um subcorpo de $\mathbb{R}$. De fato, dados $a_1 + b_1\sqrt{2}$ $a_2 + b_2\sqrt{2} \in \mathcal{F}$, temos*

$$(a_1 + b_1\sqrt{2}) - (a_2 + b_2\sqrt{2}) = (a_1 - a_2) + (b_1 - b_2)\sqrt{2} \in \mathcal{F};$$

e ainda, para $\alpha = a_2 + b_2\sqrt{2} \neq 0$, temos

$$\begin{aligned} \beta = (a_2 + b_2\sqrt{2})^{-1} &= \frac{1}{a_2 + b_2\sqrt{2}} \\ &= \left(\frac{a_2}{a_2^2 - 2b_2^2}\right) + \left(\frac{-b_2}{a_2^2 - 2b_2^2}\right)\sqrt{2} \in \mathcal{F}. \end{aligned}$$

Assim, o produto $(a_1 + b_1\sqrt{2}) \cdot (a_2 + b_2\sqrt{2})^{-1}$ *tem que ser igual a 1.* Como $\alpha, \beta \in \mathbb{Q}$, *temos que $\lambda \in \mathcal{F}$. Portanto, $\mathcal{F}$ é um subcorpo de $\mathbb{R}$.*

Exemplo 1.18. *Sejam $\mathcal{K}$ um corpo finito de característica $p > 0$ e q uma potência inteira de p. Temos que $\mathcal{F} = \{a \in \mathcal{K} : a^q - a = 0\}$ é um subcorpo de $\mathcal{K}$. De fato, dados $a, b \in \mathcal{F}$, tem-se $a^q - a = 0$ e $b^q - b = 0$. Logo*

$$\begin{aligned} (a-b)^q - (a-b) &= a^q - b^q - a + b \\ &= (a^q - a) - (b^q - b) \\ &= 0 - 0 \\ &= 0 \end{aligned} \quad .$$

Assim, $a - b \in \mathcal{F}$. Agora, para $b \neq 0$, temos

$$(a \cdot b^{-1})^q - (a \cdot b^{-1}) = a^q \cdot b^{-q} - a^q \cdot b^{-q} = 0.$$

1.3 Homomorfismo de anéis

Nesta seção será apresentada a fundamentação do conceito de homomorfismo de anéis e alguns resultados relacionados a isomorfismo de anéis, que é um caso particular de homomorfismo de

anéis. Tais conceitos são importantes pois, se um anel é isomorfo a outro, as propriedades algébricas que um possui o outro também possui, ou seja, se um é corpo o outro também é, se um possui unidade o outro também possui unidade. Doravante poderemos classificar os anéis a menos de isomorfismo em classes disjuntas.

Definição 1.12. *Sejam $\mathcal{R}$ e $\mathcal{S}$ anéis. Uma aplicação $\varphi : \mathcal{R} \to \mathcal{S}$ é dita um* ***homomorfismos de $\mathcal{R}$ em $\mathcal{S}$*** *(ou simplesmente um homomorfismo de anéis), se*

$$\varphi(a+b) = \varphi(a) + \varphi(b) \quad e \quad \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b), \ \forall a, b \in \mathcal{R}.$$

Intuitivamente, vemos que um homomorfismo de $\mathcal{R}$ em $\mathcal{S}$ é uma aplicação que "preserva" as operações dos anéis. Notemos que $\varphi : \mathcal{R} \to \mathcal{S}$ é um homomorfismo de grupos abelianos aditivos $(\mathcal{R}, +)$ e $(\mathcal{S}, +)$. Quando tivermos um homomorfismo injetivo, chamaremos de **monomorfismo**, e se o homomorfismo for sobrejetivo, o mesmo é dito **epimorfismo**.

Exemplo 1.19. *Consideremos $\mathcal{R}$ um anel qualquer. A aplicação $id : \mathcal{R} \to \mathcal{R}$ dada por $id(a) = a$ para todo $a \in \mathcal{R}$, é um homomorfismo, chamado de homomorfismo identidade.*

Exemplo 1.20. *Seja $\varphi : \mathbb{Z} \to \mathbb{Z}_n$, tal que $\varphi(a) = \bar{a}$, para todo $a \in \mathbb{Z}$. Temos que φ é um epimorfismo, pois, dados $a, b \in \mathbb{Z}$, temos*

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

$$\varphi(a \cdot b) = \overline{a \cdot b} = \bar{a} \cdot \bar{b} = \varphi(a) \cdot \varphi(b),$$

então φ é um homomorfismo e, em particular um epimorfismo, como dito anteriormente.

Exemplo 1.21. *Seja a aplicação $\varphi : \mathbb{Z} \to 2\mathbb{Z}$, definida por $\varphi(x) = 2x$ para todo $x \in \mathbb{Z}$. Dados $a, b \in \mathbb{Z}$, é evidente que $\varphi(a+b) = \varphi(a) + \varphi(b)$, ou seja, φ é um homomorfismo entre os grupos $(\mathbb{Z}, +)$ e $(2\mathbb{Z}, +)$. No entanto,*

$$\varphi(a \cdot b) = 2ab \quad e \quad \varphi(a) \cdot \varphi(b) = 2a \cdot 2b = 4ab.$$

Notemos que a igualdade só é válida para $a = 0$ ou $b = 0$. Logo, φ não é um homomorfismo entre os anéis $\mathbb{Z}$ e $2\mathbb{Z}$.

Observação 2. *Notemos que todo homomorfismo de anéis é também um homomorfismo entre grupos, mas não é válida a recíproca.*

Proposição 1.6. *Sejam $\mathcal{R}_1$ e $\mathcal{R}_2$ anéis e $\varphi : \mathcal{R}_1 \to \mathcal{R}_2$ um homomorfismo,*

(1) $Im(\varphi)$ é um subanel de $\mathcal{R}_2$;

(2) Se φ é um epimorfismo, e existe $1 \in \mathcal{R}_1$, então $\varphi(1) = 1$;

(3) Se φ é um epimorfismo e $\mathcal{R}_1$ é comutativo, então $\mathcal{R}_2$ é comutativo.

Demonstração:
(1) É imediato que $Im(\varphi) \neq \varnothing$, pois $\varphi(0) = 0$. Se a' e b' são dois elementos quaisquer de $Im(\varphi)$, então existe a e b em $\mathcal{R}_1$ tais que $\varphi(a) = a'$ e $\varphi(b) = b'$. Assim,

$$a' - b' = \varphi(a) - \varphi(b) = \varphi(a - b),$$

$$a' \cdot b' = \varphi(a) \cdot \varphi(b) = \varphi(a \cdot b),$$

donde $a' - b',\ a' \cdot b' \in Im(\varphi)$. Logo, $Im(\varphi)$ é um subanel de $\mathcal{R}_2$.
(2) Se a' é um elemento qualquer de $\mathcal{R}_2$, então existe $a \in \mathcal{R}_1$ tal que $\varphi(a) = a'$. Assim,

$$a' \cdot \varphi(1) = \varphi(a) \cdot \varphi(1) = \varphi(a \cdot 1) = \varphi(a) = a'.$$

Logo, $\varphi(1)$ é o elemento unidade de $\mathcal{R}_2$, ou seja, $\varphi(1) = 1$.
(3) Para $a_1, b_1 \in \mathcal{R}_2$, mostremos que $\mathcal{R}_2$ é um anel comutativo. Como φ é um epimorfismo, existem $a, b \in \mathcal{R}_1$, de modo que $\varphi(a) = a_1$ e $\varphi(b) = b_1$. Observemos que, sendo $\mathcal{R}_1$ comutativo,

$$a_1 \cdot b_1 = \varphi(a) \cdot \varphi(b) = \varphi(a \cdot b) = \varphi(b \cdot a) = \varphi(b) \cdot \varphi(a) = b_1 \cdot a_1,$$

ou seja, obtemos que $\mathcal{R}_2$ também é comutativo. ■

Definição 1.13. *Sejam $\mathcal{R}$ e $\mathcal{S}$ anéis e $\varphi : \mathcal{R} \to \mathcal{S}$ um homomorfismo de anéis, então chamaremos de* ***núcleo de*** *φ, o conjunto $Ker(\varphi)$, dado por*

$$Ker(\varphi) = \{x \in \mathcal{R} : \varphi(x) = 0\}.$$

Exemplo 1.22. *A aplicação $\varphi : \mathbb{Z} \to \mathbb{Z}_n$, definida por $\varphi(a) = \bar{a}$, como já mostrada é homomorfismo de anéis. Já o seu núcleo é $Ker(\varphi) = n\mathbb{Z}$, pois, tomando $a \in \mathbb{Z}$, $a \in Ker(\varphi)$, temos*

$$a \in Ker(\varphi) \Leftrightarrow \bar{a} = \bar{0} \Leftrightarrow a \equiv 0 (mod\ n) \Leftrightarrow a = nk, \quad com \quad k \in \mathbb{Z}.$$

Exemplo 1.23. *Consideremos $\varphi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, dada por $\varphi(x, y) = y$, para qualquer $(x, y) \in \mathbb{Z} \times \mathbb{Z}$. Temos que φ é um homomorfismo. Visto que, tomados $x = (a, b), y = (c, d) \in \mathbb{Z} \times \mathbb{Z}$ temos,*

$$\varphi(x + y) = \varphi[(a, b) + (c, d)] = \varphi(a + c, b + d) = b + d = \varphi(a, b) + \varphi(c, d) = \varphi(x) + \varphi(y), .$$

De forma análoga, mostra-se $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$. *Concluímos assim que* φ *é um homomorfismo. Já* $Ker(\varphi)$ *é dado por*

$$(x, y) \in Ker(\varphi) \Leftrightarrow \varphi(x, y) = 0 \Leftrightarrow y = 0.$$

Portanto,

$$Ker(\varphi) = \{(x, 0) : x \in \mathbb{Z}\}.$$

Proposição 1.7. *Um homomorfismo de anéis* $\varphi : \mathcal{R} \to \mathcal{S}$ *é injetivo se, e somente se,* $Ker(\varphi) = \{0\}$.

Demonstração: Suponhamos que φ seja injetivo e tomemos $a \in Ker(\varphi)$. Sendo assim, $\varphi(a) = 0$. Como $\varphi(0) = 0$, temos que $\varphi(a) = \varphi(0)$. Logo, pela hipótese tem-se

$$\varphi(a) = \varphi(0) \Rightarrow a = 0.$$

Portanto, $Ker(\varphi) = \{0\}$. Reciprocamente dados $a, b \in \mathcal{R}$, temos,

$$\varphi(a) = \varphi(b) \Rightarrow \varphi(a) - \varphi(b) = 0 \Rightarrow \varphi(a - b) = 0.$$

Por conseguinte, sendo $Ker(\varphi) = \{0\}$, temos

$$a - b = 0 \Rightarrow a = b.$$

Logo, φ é injetivo. ■

Definição 1.14. *Dados os anéis* $\mathcal{R}$ *e* $\mathcal{S}$. *Um homomorfismo* $\varphi : \mathcal{R} \to \mathcal{S}$ *bijetivo é chamado* ***isomorfismo****. Particularmente, um isomorfismo* $\varphi : \mathcal{R} \to \mathcal{R}$ *é dito um* ***automorfismo*** *de* $\mathcal{R}$.

Proposição 1.8. *Se* $\varphi : \mathcal{R} \to \mathcal{S}$ *é um isomorfismo de anéis, então* $\varphi^{-1} : \mathcal{S} \to \mathcal{R}$ *também é um isomorfismo de anéis.*

Demonstração: Como sabemos que um isomorfismo se trata de uma aplicação bijetiva, particularmente um homomorfismo de grupos abelianos aditivos. De início, vamos mostrar que $\varphi^{-1} : \mathcal{S} \to \mathcal{R}$ é um homomorfismo entre $(S, +)$ e $(R, +)$. Para isso, dados $a_1, b_1 \in \mathcal{S}$, existem $a, b \in \mathcal{R}$, tais que,

$$\varphi(a) = a_1 \Leftrightarrow \varphi^{-1}(a_1) = a \quad \text{e} \quad \varphi(b) = b_1 \Leftrightarrow \varphi^{-1}(b_1) = b.$$

Donde,

$$\varphi^{-1}(a_1 + b_1) = \varphi^{-1}[(\varphi(a) + \varphi(b))] = \varphi^{-1}[\varphi(a + b)] = a + b = \varphi^{-1}(a_1) + \varphi^{-1}(b_1).$$

Agora, resta-nos mostrar que φ^{-1} "preserva" a multiplicação. Para isso, consideremos os mesmos elementos arbitrários, anteriores. Com isso,

$$\varphi^{-1}(a_1 \cdot b_1) = \varphi^{-1}(\varphi(a) \cdot \varphi(b)) = \varphi^{-1}(\varphi(a \cdot b)) = a \cdot b = \varphi^{-1}(a_1) \cdot \varphi^{-1}(b_1).$$

■

De mão do resultado anterior, se $\varphi : \mathcal{R} \to \mathcal{S}$ é um isomorfismo, diremos que $\mathcal{R}$ e $\mathcal{S}$ são **isomorfos** (ou ainda, que algebricamente são idênticos), e denotaremos tal fato por $\mathcal{R} \simeq \mathcal{S}$. E mais, tendo em vista isso, podemos dizer que a relação de isomorfia é uma relação de equivalência.

Exemplo 1.24. *Sejam $\mathcal{R}$ um anel e $Id : \mathcal{R} \to \mathcal{R}$ uma aplicação tal que $Id(a) = a$, $\forall a \in \mathcal{R}$. Então Id é um isomorfismo de anéis. De fato, além de ser bijetora Id, é também um homomorfismo, visto que*

$$Id(a + b) = a + b = Id(a) + Id(b) \quad e \quad Id(a \cdot b) = a \cdot b = Id(a) \cdot Id(b).$$

Exemplo 1.25. *A aplicação $\varphi : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[\sqrt{2}]$ definida por $\varphi(m + n\sqrt{2}) = m - n\sqrt{2}$ é um isomorfismo de anéis. De fato, tomados $a = m + n\sqrt{2}$ e $b = r + s\sqrt{2}$ pertencentes a $\mathbb{Z}[\sqrt{2}]$. Temos,*

$$\varphi(a+b) = \varphi[(m+n\sqrt{2})+(r+s\sqrt{2})] = \varphi[(m+r)+(n+s)\sqrt{2}] = (m+r)-(n+s)\sqrt{2} = \varphi(a)+\varphi(b)$$

$$e$$

$$\begin{aligned} \varphi(a \cdot b) &= \varphi[(m + n\sqrt{2}) \cdot (r + s\sqrt{2})] = \varphi[(mr + 2ns) + (ms + nr)\sqrt{2}] \\ &= (mr + 2ns) - (ms + nr)\sqrt{2} = \varphi(a) \cdot \varphi(b). \end{aligned}$$

Além disso, vamos verificar o $Ker(\varphi)$, que é dado por,

$$a \in Ker(\varphi) \Leftrightarrow \varphi(m + n\sqrt{2}) = 0 - 0\sqrt{2} \Leftrightarrow m = n = 0.$$

Logo, $Ker(\varphi) = \{0\}$. Devido a φ ser um homomorfismo e termos $Ker(\varphi) = \{0\}$, temos por consequência que φ é injetiva. Por outro lado, a aplicação é sobrejetiva, pois dado, $y = m + n\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ e tomarmos $x = m - n\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, tem-se

$$\varphi(x) = \varphi(m - n\sqrt{2}) = m + n\sqrt{2} = y.$$

Portanto, φ é um isomorfismo de anéis.

Corpo Primo

Definição 1.15. *Todo corpo que admite um único subcorpo é denotado* ***corpo primo****.Isto é, se $\mathcal{K}$ é um corpo, chamamos um subcorpo $\mathcal{P}$ de* ***corpo primo****, quando*

$$\mathcal{P} = \bigcap_{i \in \wedge} \mathcal{K}_i,$$

em que $\mathcal{K}_i$ é um subcorpo de $\mathcal{K}$.

Teorema 1.6. *Sejam $\mathcal{K}$ um corpo e $\mathcal{P}$ seu corpo primo, temos que*

(1) Se $car(\mathcal{K}) = p$, então $\mathcal{P} \simeq \mathbb{Z}_p$;

(2) Se $car(\mathcal{K}) = 0$, então $\mathcal{P} \simeq \mathbb{Q}$.

Demonstração:
(1) A priori, temos que $\mathcal{R} = \mathbb{Z} \cdot 1_{\mathcal{K}} = \{a \cdot 1_{\mathcal{K}} : a \in \mathbb{Z}\}$, é um subdomínio de $\mathcal{K}$, contido em todo subdomínio de $\mathcal{K}$. Visto que $\mathcal{R}$ não é vazio, pois $1_{\mathcal{K}} = 1 \cdot 1_{\mathcal{K}} \in \mathcal{R}$. Se tomarmos $a \cdot 1_{\mathcal{K}}, b \cdot 1_{\mathcal{K}} \in \mathcal{R}$, temos

$$a \cdot 1_{\mathcal{K}} - b \cdot 1_{\mathcal{K}} = a \cdot 1_{\mathcal{K}} + [-(b \cdot 1_{\mathcal{K}})] = a \cdot 1_{\mathcal{K}} + [(-b) \cdot 1_{\mathcal{K}}] = [a + (-b)] \cdot 1_{\mathcal{K}} = (a - b) \cdot 1_{\mathcal{K}},$$

e

$$(a \cdot 1_{\mathcal{K}})(b \cdot 1_{\mathcal{K}}) = (ab) \cdot 1_{\mathcal{K}}.$$

O que mostra que $\mathcal{R}$ é um subdomínio de $\mathcal{K}$. Agora, mostremos que $\varphi : \mathbb{Z}_p \to \mathcal{R}$, dada por $\varphi(\bar{a}) = a \cdot 1_{\mathcal{K}}$ está bem definida. Para isso, tomemos $\bar{a}, \bar{b} \in \mathbb{Z}_p$, então temos

$$\bar{a} = \bar{b} \Leftrightarrow a \equiv b (mod\ p) \Leftrightarrow p | a - b.$$

Logo, $a - b = pk$, para algum k inteiro. Decorre disso que,

$$(a - b) \cdot 1_{\mathcal{K}} = (pk) \cdot 1_{\mathcal{K}} = 0_{\mathcal{K}},$$

pois $car(\mathcal{K}) = p$. Assim,

$$a \cdot 1_{\mathcal{K}} = b \cdot 1_{\mathcal{K}} \Rightarrow \varphi(\bar{a}) = \varphi(\bar{b}),$$

o que nos mostra que φ é uma aplicação. Além disso, φ é um homomorfismo, visto que

$$\varphi(\bar{a} + \bar{b}) = \varphi(\overline{a + b}) = (a + b) \cdot 1_{\mathcal{K}} = a \cdot 1_{\mathcal{K}} + b \cdot 1_{\mathcal{K}} = \varphi(\bar{a}) + \varphi(\bar{b})$$

e

$$\varphi(\bar{a}\cdot\bar{b}) = \varphi(\overline{a\cdot b}) = a\cdot b\cdot 1_{\mathcal{K}} = a\cdot(b\cdot 1_{\mathcal{K}}) = (a\cdot 1_{\mathcal{K}})(b\cdot 1_{\mathcal{K}}) = \varphi(\bar{a})\cdot\varphi(\bar{b}).$$

Além disso,

$$\varphi(\bar{a}) = \varphi(\bar{b}) \Rightarrow a\cdot 1_{\mathcal{K}} = b\cdot 1_{\mathcal{K}} \Rightarrow (a-b)\cdot 1_{\mathcal{K}} = 0_{\mathcal{K}}.$$

Isso implica que $p|a-b$, ou ainda, $\bar{a} = \bar{b}$, de modo que φ é injetora. Por fim, se $a\cdot 1_{\mathcal{K}} \in \mathcal{R}$, então $\varphi(\bar{a}) = a\cdot 1_{\mathcal{K}}$, isto é, φ é sobrejetora. Com isso, concluímos que φ é um isomorfismo, ou seja, $\mathbb{Z}_p \simeq \mathcal{R}$, e consequentemente, $\mathcal{R}$ é um corpo. Como $\mathcal{R}$ está contido em todo subcorpo de $\mathcal{K}$, então $\mathcal{R}$ é o corpo primo de $\mathcal{K}$, de maneira que $\mathcal{P} \simeq \mathbb{Z}_p$.

(2) Seja a aplicação $\varphi : \mathbb{Q} \to \mathcal{K}$, definida por

$$\varphi\left(\frac{a}{b}\right) = \frac{a\cdot 1_{\mathcal{K}}}{b\cdot 1_{\mathcal{K}}}.$$

Sabendo que φ está bem definida. Temos que dados $\frac{a\cdot 1}{b\cdot 1}, \frac{c\cdot 1}{d\cdot 1} \in \mathcal{K}$, tem-se

$$\frac{a\cdot 1}{b\cdot 1} = \frac{c\cdot 1}{d\cdot 1} \Leftrightarrow (a\cdot 1)(d\cdot 1) = (c\cdot 1)(b\cdot 1) \Leftrightarrow (ad)\cdot 1 = (bc)\cdot 1 \Leftrightarrow (ad-bc)\cdot 1 = 0.$$

Mas sendo $car(\mathcal{K}) = 0$, e $\mathcal{K}$ sendo corpo, temos

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

Com isso, mostramos que φ é injetiva.

Além disso, temos que φ é um homomorfismo. De fato, tomados $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$, temos

$$\varphi\left(\frac{a}{b}+\frac{c}{d}\right) = \left(\frac{ad+bc}{bd}\right) = \frac{(ad+bc)\cdot 1}{(bd)\cdot 1} = \frac{(ad)\cdot 1 + (bc)\cdot 1}{(bd)\cdot 1} = \frac{(a\cdot 1)(d\cdot 1)+(b\cdot 1)(c\cdot 1)}{(b\cdot 1)(d\cdot 1)} =$$

$$= \frac{a\cdot 1}{b\cdot 1} + \frac{c\cdot 1}{d\cdot 1} = \varphi\left(\frac{a}{b}\right) + \varphi\left(\frac{c}{d}\right).$$

Já a preservação da multiplicação é feita de maneira análoga. Logo, φ é homomorfismo. Portanto,

$$\mathbb{Q} \simeq \varphi(\mathbb{Q}).$$

Logo podemos concluir que $\varphi(\mathbb{Q})$ é corpo primo, pois $\mathbb{Q}$ é corpo primo de $\mathbb{R}$. Consequentemente,

$$\mathcal{P} \simeq \mathbb{Q}.$$

■

1.4 Corpo de Frações em um Domínio

Sejam a e b dois elementos de um domínio $\mathcal{D}$. Diremos que a é múltiplo de b se, e somente se, existe c em $\mathcal{D}$ tal que $a = bc$. Notemos que, a ser múltiplo de b com $b \neq 0$, indica que c é único. O que queremos mostrar a seguir é a generalização da construção do corpo $\mathbb{Q}$, isto é, dado um domínio $\mathcal{D}$, construiremos um corpo $\mathcal{F}$ que contém $\mathcal{D}$ e cujos representantes são da forma $\frac{a}{b}$, com $a, b \in \mathcal{D}$ e $b \neq 0$.

Teorema 1.7. *Sejam $\mathcal{D}$ um domínio e*

$$\mathcal{S} = \mathcal{D} \times \mathcal{D}^* = \{a, b \in \mathcal{D} \quad e \quad b \neq 0\}$$

temos que a relação $\sim$ dada, para quaisquer $(a, b),\ (c, d) \in \mathcal{S}$, por

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

é de equivalência.

Demonstração: Vamos mostrar que $\sim$ é de equivalência. Para isso, sejam $(a, b),\ (c, d),\ (e, f) \in \mathcal{S}$. Note que, $(a, b) \sim (a, b)$, pois $ab = ba$, já que $\mathcal{D}$ é domínio, ou seja, $\sim$ é reflexiva.

Agora, se $(a, b) \sim (c, d)$, então $ad = bc$, ou ainda $da = cb$, ou seja, $cb = da$, de modo que $(c, d) \sim (a, b)$. Logo $\sim$ é simétrica.

Por fim, se $(a, b) \sim (c, d)$ e $(c, d) \sim (e, f)$, então

$$ad = bc \ \text{ e } \ cf = de.$$

Multiplicando por f e por b as igualdades acima, respectivamente, temos

$$adf = bcf \ \text{ e } \ bcf = bde.$$

Logo, $adf = bde$, e como $d \neq 0$, tem-se

$$af = be \Rightarrow (a, b) \sim (e, f).$$

Portanto, $\sim$ é transitiva.

Ou seja, concluímos que $\sim$ é de equivalência. ■

Note que, se (a, b) é um elemento qualquer de $\mathcal{S}$, indicaremos por $\overline{(a, b)}$ a classe de equivalência módulo $\sim$ determinada por (a, b). É comum representarmos a classe $\overline{(a, b)}$ por $\frac{a}{b}$, de modo que

$$\frac{a}{b} = \{(c, d) \in \mathcal{S} \ : \ (c, d) \sim (a, b)\}$$

.

Portanto, o conjunto quociente $\frac{\mathcal{S}}{\sim}$, que indicaremos por $\mathcal{F}$ é o conjunto,

$$\mathcal{F} = \left\{ \frac{a}{b} \ : \ a,\ b \in \mathcal{D} \ \text{ e } \ b \neq 0 \right\}.$$

Além disso, sabemos que

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

Proposição 1.9. *Seja $\mathcal{F}$ o conjunto*

$$\mathcal{F} = \left\{ \frac{a}{b} \ : \ a,\ b \in \mathcal{D} \ \ e \ \ b \neq 0 \right\}.$$

Então,

$$+: \begin{array}{ccc} \mathcal{F}\times\mathcal{F} & \to & \mathcal{F} \\ \left(\frac{a}{b},\frac{c}{d}\right) & \mapsto & \frac{ad+bc}{bd} \end{array} \quad e \quad \cdot: \begin{array}{ccc} \mathcal{F}\times\mathcal{F} & \to & \mathcal{F} \\ \left(\frac{a}{b},\frac{c}{d}\right) & \mapsto & \frac{ac}{bd} \end{array}$$

definem duas operações sobre $\mathcal{F}$.

Omitiremos a demonstração desta proposição, mas a mesma pode ser encontrada em [8], de modo bastante explicativa.

Definição 1.16. *Com as operações da proposição anterior, $(\mathcal{F},+,\cdot)$ é um corpo, chamado* ***corpo de frações do domínio*** *$\mathcal{D}$.*

1.5 Ideais

A seguir definiremos uma classe de anéis muito importante no nosso estudo, os ideais. Que por sua vez existe uma certa analogia entre o seu conceito e o conceito de subgrupo normal. Como veremos, com um ideal $\mathcal{I}$ de um anel $\mathcal{R}$, é possível construirmos o anel quociente $\mathcal{R}/\mathcal{I}$, cujas operações são definidas a partir das operações de $\mathcal{R}$. Devemos ressaltar que a definição de ideal foi introduzida em meados do seculo XIX, por Richard Dedekind, com a intenção de resolver questões que envolviam a Teoria dos Números. Destacamos que o conceito de ideal pode ser aplicado a todos os tipos de anéis, mas nos restringimos a usá-lo apenas nos anéis comutativos, por causa do foco do nosso trabalho.

Definição 1.17. *Seja $\mathcal{R}$ um anel e $\mathcal{I}$ um subconjunto não vazio de $\mathcal{R}$, então $\mathcal{I}$ é dito um* ***ideal*** *de $\mathcal{R}$ se as seguintes condições são satisfeitas:*

(1) $a - b \in \mathcal{I},\ a, b \in \mathcal{I}$;

(2) $ax \in \mathcal{I}$ *e* $xa \in \mathcal{I},\ \forall a \in \mathcal{I}$ *e* $\forall x \in \mathcal{R}$.

Notemos que o item *(2)* afirma que $\mathcal{I}$ absorve o produto de qualquer elemento de $\mathcal{I}$ por um elemento de $\mathcal{R}$. E mais, se a condição *(1)* for satisfeita e $ax \in \mathcal{I}$, para todo $a \in \mathcal{I}$ e $x \in \mathcal{R}$, o mesmo é dito um ideal à direita de $\mathcal{R}$ e se, o item *(1)* é satisfeito e $xa \in \mathcal{I}$, para todo $a \in \mathcal{I}$ e $x \in \mathcal{R}$ temos um ideal à esquerda de $\mathcal{R}$.

Exemplo 1.26. *Os conjuntos* $\{0\}$ *e* $\mathcal{R}$ *são ideais de* $\mathcal{R}$*, chamados de ideais triviais.*

Exemplo 1.27. *Seja* $\varphi : \mathcal{R} \to \mathcal{S}$ *um homomorfismo de anéis, então* $Ker(\varphi)$ *é um ideal de* $\mathcal{R}$*. De fato, dados* $a,\ b \in Ker(\varphi)$*, temos*

$$\varphi(a - b) = \varphi(a) - \varphi(b) = 0 - 0 = 0 \Rightarrow a - b \in Kar(\varphi).$$

Agora, para $x \in \mathcal{R}$*, temos*

$$\varphi(a \cdot x) = \varphi(a) \Rightarrow \cdot\varphi(x) = 0 \cdot \varphi(x) = 0 \Rightarrow a \cdot x \in Ker(\varphi).$$

Da mesma forma, tem-se $x \cdot a \in Ker(\varphi)$*. Portanto,* $Ker(\varphi)$ *é um ideal de* $\mathcal{R}$*.*

Proposição 1.10. *Sejam* $\mathcal{R}$ *um anel com unidade e* $\mathcal{I}$ *um ideal de* $\mathcal{R}$*. Se* $u \in \mathcal{R}$ *é invertível e* $u \in \mathcal{I}$*, então* $\mathcal{I} = \mathcal{R}$*.*

Demonstração: É claro que $\mathcal{I} \subset \mathcal{R}$, pois $\mathcal{I}$ é ideal de $\mathcal{R}$. Vamos mostrar que $\mathcal{R} \subset \mathcal{I}$. Para isso, tomemos um elemento arbitrário $a \in \mathcal{R}$, o qual podemos denotar por $a = a \cdot 1$. Se $u \in \mathcal{I}$, é invertível, então existe $u^{-1} \in \mathcal{R}$ de modo que $1 = u \cdot u^{-1}$. Por conseguinte, temos

$$a = a \cdot 1 = a(u \cdot u^{-1}) = (a \cdot u) \cdot u^{-1}.$$

Notemos que $\mathcal{I}$ é um ideal, sendo assim, $a = (a \cdot u) \cdot u^{-1} \in \mathcal{I}$, concluindo a demonstração. ■

Agora, vamos explanar um pouco da aritmética dos ideais, de modo similar ao que é visto em subanéis.

Proposição 1.11. *Sejam* $\mathcal{R}$ *um anel com unidade e* $\mathcal{I}$ *e* $\mathcal{J}$ *ideais de* $\mathcal{R}$*. Então* $\mathcal{I} \cap \mathcal{J}$ *também é um ideal de* $\mathcal{R}$*.*

Demonstração: Claramente, $\mathcal{I} \cap \mathcal{J} \neq \varnothing$, pois $0 \in \mathcal{I} \cap \mathcal{J}$. Sejam $x,\ y \in \mathcal{I} \cap \mathcal{J}$. Então $x,\ y \in \mathcal{I}$ e $x,\ y \in \mathcal{J}$. Logo, $x - y \in \mathcal{I}$ e $x - y \in \mathcal{J}$, sendo assim $x - y \in \mathcal{I} \cap \mathcal{J}$. Agora note que se $x \in \mathcal{I} \cap \mathcal{J}$ e $a \in \mathcal{R}$, tem-se

$$ax \in \mathcal{I} \cap \mathcal{J},$$

pois $\mathcal{I},\ \mathcal{J}$ são ideais de $\mathcal{R}$. Então $\mathcal{I} \cap \mathcal{J}$ também é um ideal de $\mathcal{R}$. ■

Observação 3. *Vale ressaltar que a proposição acima pode ser estendida para uma família qualquer de ideais de um anel $\mathcal{R}$, ou seja, sejam $\mathcal{R}$ um anel e $\{\mathcal{I}_i\}_{i\in\Omega}$ uma família de ideais de $\mathcal{R}$ onde Ω é um conjunto de índices quaisquer. Então,*

$$\bigcap_{i\in\Omega}\mathcal{I}_i$$

é também um ideal de $\mathcal{R}$.

Definição 1.18. *Sejam $\mathcal{R}$ um anel com unidade e $\mathcal{I}$ e $\mathcal{J}$ ideais de $\mathcal{R}$. Então define-se o* ***produto*** *e a* ***soma*** *de $\mathcal{I}$ e $\mathcal{J}$ como sendo*

$$\mathcal{I}\cdot\mathcal{J}=\left\{\sum_{i=1}^{n}x_iy_i : x_i\in\mathcal{I} \;\; e \;\; y_i\in\mathcal{J}\right\}.$$

e

$$\mathcal{I}+\mathcal{J}=\{x+x : x\in\mathcal{I} \;\; e \;\; y\in\mathcal{J}\}.$$

Ressaltando-se que o produto é constituído por todos os elementos da forma,

$$x_1y_1+x_2y_2+x_3y_3+\ldots+x_iy_i, \;\; \text{com} \;\; x_i\in\mathcal{I} \;\; \text{e} \;\; y_i\in\mathcal{J}.$$

Definição 1.19. *Sejam $\mathcal{R}$ um anel comutativo e $\{a_1,a_2,a_3,\ldots,a_n\}$ um subconjunto não vazio de $\mathcal{R}$, então o ideal*

$$\mathcal{I}=\{x_1a_1+x_2a_2+\ldots+x_na_n \;\; : \;\; x_i\in\mathcal{R}, \;\forall\; i=1,\ldots,n\}$$

é dito ***ideal gerado*** *por $a_1,a_2,\ldots,a_n$. Sendo denotado por*

$$\mathcal{I}=<a_1,a_2,\ldots,a_n>.$$

Nota-se que em particular se $a\in\mathcal{R}$, o ideal

$$\mathcal{I}=<a>=\{x\cdot a \;\; : \;\; x\in\mathcal{R}\}$$

chama-se ***ideal principal gerado*** *por a.*

Exemplo 1.28. *Sendo $\mathbb{Z}$ um ideal de $\mathbb{Q}$, temos que $\mathbb{Z}$ é um ideal principal, pois*

$$\mathbb{Z}=<1>.$$

Definição 1.20. *Seja $\mathcal{D}$ um domínio, se todo ideal de $\mathcal{D}$ for principal, então dizemos que $\mathcal{D}$ é um* ***domínio de ideais principais*** *(DIP).*

Exemplo 1.29. *$\mathbb{Z}$ é um domínio de ideais principais. De fato, pois sendo $\mathcal{I}$ um ideal de $\mathbb{Z}$. Se $\mathcal{I} = \{0\}$, então $\mathcal{I}$ é um ideal principal de $\mathbb{Z}$ gerado por 0. Suponhamos que $\mathcal{I} \neq \{0\}$. Então existe $a \in \mathcal{I}$ tal que $a \neq 0$. Mas como $\mathcal{I}$ é ideal, $-a \in \mathcal{I}$. Com isso, garantimos que existem em $\mathcal{I}$, elementos que são estritamente positivos. Portanto, o conjunto $\{x \in \mathcal{I} \ : \ x > 0\} \neq \varnothing$. Consideremos, então*

$$b = min\{x \in \mathcal{I} \ : \ x > 0\}.$$

Vamos mostrar que $\mathcal{I} =< b >$. Dado $x \in \mathcal{I}$, temos que existem $r, \ s \in \mathbb{Z}$ tais que

$$x = bs + r, \ com \ \ 0 \leq r < b.$$

Sendo assim,

$$r = x - bs \in \mathcal{I}.$$

Pois $x, \ bs \in \mathcal{I}$. Como b é o menor elemento de $\mathcal{I}$ dentre os que são estritamente positivos e $0 \leq r < b$, então necessariamente temos $r = 0$. Por conseguinte, $x = bs$, ou seja, $x \in < b >$, ou seja, $I \subset < b >$; como a inclusão $< b > \subset \mathcal{I}$ é imediata, pois $b \in \mathcal{I}(b = 1 \cdot b)$ podemos concluir que $\mathcal{I} =< b >$, o que mostra que $\mathbb{Z}$ é um DIP.

Observação 4. *Nem sempre se tem $a \in \mathcal{I}$, para um ideal principal $\mathcal{I} =< a >$ de um anel $\mathcal{R}$.*

Teorema 1.8. *Seja $\mathcal{K}$ um anel comutativo. $\mathcal{K}$ é um corpo se, e somente se, os únicos ideais de $\mathcal{K}$ são os triviais.*

Demonstração: A priori, suponhamos que $\mathcal{K}$ é um corpo e tomemos $\mathcal{I}$ como sendo um ideal de $\mathcal{K}$, tal que $\mathcal{I} \neq \{0\}$. Sendo assim, existe $a \in \mathcal{I}$, com $a \neq 0$. Como $\mathcal{K}$ é corpo e a é invertível, temos $\mathcal{I} = \mathcal{K}$.

Reciprocamente, note que sendo $a \in \mathcal{K}$, com $a \neq 0$. Tem-se, o ideal $\mathcal{I} =< a >$, tal que $\mathcal{I} \neq \{0\}$. Desse modo, temos por hipótese que $\mathcal{I} = \mathcal{K}$. Como $1 \in \mathcal{K}$, existe $x \in \mathcal{K}$ com

$$1 = ax.$$

Portanto, a é invertível, e como a é elemento arbitrário não nulo de $\mathcal{K}$, concluímos que $\mathcal{K}$ é um corpo. ■

Definição 1.21. *Sejam $\mathcal{R}$ um anel comutativo e $\mathcal{P}$ um ideal de $\mathcal{R}$, com $\mathcal{P} \neq \mathcal{R}$. Então, chamamos $\mathcal{P}$ de* ***ideal primo*** *quando para $a, \ b \in \mathcal{R}$,*

$$ab \in \mathcal{P} \Rightarrow a \in \mathcal{P} \ \ ou \ \ b \in \mathcal{P}.$$

Exemplo 1.30. *$\mathcal{I} = \{0\}$ é um ideal primo de $\mathbb{Z}$, pois, se $ab \in \mathcal{I}$ temos $ab = 0$ então $a = 0$ ou $b = 0$, já que $\mathbb{Z}$ é domínio, ou seja, $a \in \mathcal{I}$ ou $b \in \mathcal{I}$.*

Exemplo 1.31. *No anel $\mathbb{Z} \times \mathbb{Z}$ temos o ideal $\mathcal{I} = \{0\} \times \mathbb{Z}$ é um ideal primo. De fato, dados $(a, b),\ (c, d) \in \mathbb{Z}\times\mathbb{Z}$, tais que $(a, b)\cdot(c, d) = (ac, bd)\ \in \{0\}\times\mathbb{Z}$, temos $ac = 0$ e, por conseguinte, $a = 0$ ou $c = 0$, donde $(a, b) \in \{0\} \times \mathbb{Z}$ ou $(c, d) \in \{0\} \times \mathbb{Z}$.*

Definição 1.22. *Sejam $\mathcal{R}$ um anel comutativo e $\mathcal{M}$ um ideal de $\mathcal{R}$, com $\mathcal{M} \neq \mathcal{R}$. Chamamos $\mathcal{M}$ de **ideal maximal** se existir para todo ideal $\mathcal{N}$ de $\mathcal{R}$ tal que $\mathcal{M} \subsetneq \mathcal{N}$, tem-se $\mathcal{N} = \mathcal{R}$.*

Exemplo 1.32. *Se $\mathcal{K}$ é corpo, então $\mathcal{M} = \{0\}$ é maximal.*

Exemplo 1.33. *O ideal $2\mathbb{Z}$ de $\mathbb{Z}$ é maximal. De fato, se $\mathcal{I}$ é ideal de $\mathbb{Z}$ que contém $2\mathbb{Z}$ propriamente, então $\mathcal{I}$ possui um número ímpar $2t + 1$. Mas, como $2t \in \mathcal{I}$, pois $2t \in 2\mathbb{Z}$ e $\mathcal{I} \supset 2\mathbb{Z}$, então $(2t + 1) - (2t) = 1 \in \mathcal{I}$. Donde $\mathcal{I} = \mathbb{Z}$.*

1.6 Anéis Quociente

Nesta seção, tomamos como pressuposto que o leitor já é familiarizado com a Teoria dos Grupos, portanto não faremos a construção detalhada da relação de equivalência " $\equiv (mod\ \mathcal{I})$ ", definida sobre um ideal $\mathcal{I}$ de um anel $\mathcal{R}$, que é dada por

$$a \equiv b\ (mod\ \mathcal{I}) \Leftrightarrow a - b \in \mathcal{I},\ \forall\ a,\ b \in \mathcal{R},$$

pois é uma construção de maneira análoga a feita para os grupos quocientes. Se o leitor achar necessário relembrar tais conceitos com mais detalhes indicamos [8].

Definição 1.23. *Sejam $\mathcal{R}$ um anel comutativo e $\mathcal{I}$ um ideal de $\mathcal{R}$, com a operação*

$$+ :\ \frac{\mathcal{R}}{\mathcal{I}} \times \frac{\mathcal{R}}{\mathcal{I}} \ \rightarrow \ \frac{\mathcal{R}}{\mathcal{I}} \qquad\qquad \cdot :\ \frac{\mathcal{R}}{\mathcal{I}} \times \frac{\mathcal{R}}{\mathcal{I}} \ \rightarrow \ \frac{\mathcal{R}}{\mathcal{I}}$$

$$e$$

$$\left(\overline{a}, \overline{b}\right) \ \mapsto\ \overline{a} + \overline{b} = \overline{a + b} \qquad\qquad \left(\overline{a}, \overline{b}\right) \ \mapsto\ \overline{a} \cdot \overline{b} = \overline{a \cdot b}$$

*Temos que, $(\frac{\mathcal{R}}{\mathcal{I}}, +, \cdot)$ é um anel, dito **anel quociente** de $\mathcal{R}$ em $\mathcal{I}$.*

Teorema 1.9. *Sejam $\mathcal{R}$ um anel comutativo com unidade e $\mathcal{M}$ um ideal de $\mathcal{R}$. Então $\mathcal{M}$ é maximal se, e somente se, $\mathcal{R}/\mathcal{M}$ é um corpo.*

Demonstração: Notemos que basta provarmos que todo elemento $m+j \neq j$ é invertível. Para isso, suponhamos que $\mathcal{M}$ é maximal. Seja $\bar{a} \in \frac{\mathcal{R}}{\mathcal{M}}$, $\bar{a} \neq \bar{0}$ e $\mathcal{J} =< a >$ um ideal de $\mathcal{R}$. Assim,

$$\mathcal{M} + \mathcal{J} = \{m + j \ : \ m \in \mathcal{M} \ \text{ e } \ j \in \mathcal{J}\}$$

é um ideal de $\mathcal{R}$. Notemos que $\mathcal{M} + \mathcal{J} \supset \mathcal{M}$, pois

$$m_1 \in \mathcal{M} \Rightarrow m_1 = m_1 + 0 \in \mathcal{M} + \mathcal{J} \Rightarrow \mathcal{M} \subset \mathcal{M} + \mathcal{J}.$$

Mas, sendo $\bar{a} \neq \bar{0}$

$$a \notin \mathcal{M},$$

assim

$$\mathcal{M} + \mathcal{J} \nsubseteq \mathcal{M},$$

como $\mathcal{M}$ é maximal segue que

$$\mathcal{M} + \mathcal{J} = \mathcal{R}.$$

Dessa maneira, existem $x \in \mathcal{J}$ e $y \in \mathcal{M}$, tais que

$$x + y = 1 \in \mathcal{R}.$$

Observemos que

$$x \in \mathcal{J} \Rightarrow x = ab, \ b \in \mathcal{R}.$$

Assim,

$$ab + y = 1 \Rightarrow \overline{ab} + \overline{y} = \overline{1} \Rightarrow \overline{ab} = \overline{1} (pois \ \overline{y} = \overline{0}) \Rightarrow \overline{a}\overline{b} = \overline{1}.$$

Portanto, $\bar{a}$ é invertível, assim $\mathcal{R}/\mathcal{M}$ é corpo.

Reciprocamente, suponhamos que $\mathcal{R}/\mathcal{M}$ seja corpo e $\mathcal{J}$ um ideal de $\mathcal{R}$. Com $\mathcal{M} \nsubseteq \mathcal{J}$, então existe $a \in \mathcal{J}$ com $\bar{a} \neq \bar{0}$. Dessa forma, existe $b \in \mathcal{R}/\mathcal{M}$, tal que

$$\bar{a} \cdot \bar{b} = \bar{1} \Rightarrow \overline{ab} = \overline{1} \Rightarrow ab - 1 \in \mathcal{M},$$

ou seja, $ab - 1 = m$, para $m \in \mathcal{M}$, então

$$1 = ab - m \in \mathcal{J}.$$

Portanto, $\mathcal{J} = \mathcal{R}$, ou seja, $\mathcal{M}$ é ideal maximal de $\mathcal{R}$. ■

1.7 Teorema Fundamental dos Homomorfismos para Anéis

Nesta seção iremos enunciar e demonstrar o principal teorema que versa sobre homomorfismo de anéis. Este teorema é análogo ao encontrado na Teoria dos Grupos.

Teorema 1.10. *Seja $\varphi : \mathcal{R} \longrightarrow \mathcal{S}$ um homomorfismo de anéis, então*

$$\frac{\mathcal{R}}{\ker(\varphi)} \simeq \mathrm{Im}(\varphi).$$

Demonstração: Definamos a aplicação

$$\begin{aligned} \phi : \ \frac{\mathcal{R}}{\ker(\varphi)} &\to \quad \mathrm{Im}(\varphi) \\ \overline{x} &\mapsto \ \phi(\overline{x}) = \varphi(x). \end{aligned}$$

Dados $\overline{x_1}, \overline{x_2} \in \dfrac{\mathcal{R}}{\ker(\varphi)}$, tais que

$$\overline{x_1} = \overline{x_2} \Rightarrow x_1 = x_2 + a, \quad a \in \ker(\varphi),$$

então

$$\begin{aligned} \phi(\overline{x_1}) &= \varphi(x_1) \\ &= \varphi(x_2 + a) \\ &= \varphi(x_2) + \varphi(a) \\ &= \varphi(x_2) \\ &= \phi(\overline{x_2}), \end{aligned}$$

ou seja, ϕ estão bem definida. Dessa maneira,

$$\begin{aligned} \phi(\overline{x_1}) = \phi(\overline{x_2}) &\Rightarrow \varphi(x_1) = \varphi(x_2) \\ &\Rightarrow \varphi(x_1) - \varphi(x_2) = 0 \\ &\Rightarrow \varphi(x_1 - x_2) = 0 \\ &\Rightarrow x_1 - x_2 \in \ker(\varphi) \\ &\Rightarrow x_1 \equiv x_2 \ (\mathrm{mod}\, \ker(\varphi)) \\ &\Rightarrow \overline{x_1} = \overline{x_2}, \end{aligned}$$

ou seja, ϕ é injetiva. Dado $y \in \mathrm{Im}(\varphi)$, então

$$y = \varphi(x), \quad \text{para algum } x \in \mathcal{R},$$

assim, para $\overline{x} \in \dfrac{\mathcal{R}}{\ker(\varphi)}$ temos

$$\phi(\overline{x}) = \varphi(x) = y,$$

ou seja, ϕ é sobrejetiva. Por fim,

$$\begin{aligned}\phi(\overline{x_1} + \overline{x_2}) &= \phi(\overline{x_1 + x_2}) \\ &= \varphi(x_1 + x_2) \\ &= \varphi(x_1) + \varphi(x_2) \\ &= \phi(\overline{x_1}) + \phi(\overline{x_2})\end{aligned}$$

e

$$\begin{aligned}\phi(\overline{x_1} \cdot \overline{x_2}) &= \phi(\overline{x_1 \cdot x_2}) \\ &= \varphi(x_1 \cdot x_2) \\ &= \varphi(x_1) \cdot \varphi(x_2) \\ &= \phi(\overline{x_1}) \cdot \phi(\overline{x_2}),\end{aligned}$$

ou seja, ϕ é um homomorfismo. Portanto,

$$\frac{\mathcal{R}}{\ker(\varphi)} \simeq \mathrm{Im}(\varphi).$$

■

Exemplo 1.34. *Para $n \in \mathbb{N}$ temos que,*

$$\frac{\mathbb{Z}}{n\mathbb{Z}} \backsimeq \mathbb{Z}_p.$$

De fato, definimos a aplicação

$$\begin{array}{rccc}\varphi: & \mathbb{Z} & \to & \mathbb{Z}_p \\ & a & \mapsto & \varphi(a) = \overline{a}\end{array}$$

Dados $a,\ b \in \mathbb{Z}$, temos que $a = b$, temos $\varphi(a) = \varphi(b)$, ou seja, φ está bem definida. Assim,

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

e

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

ou seja, φ é um homomorfismo de anéis. Dado $y \in \mathbb{Z}_p$, então $y = \bar{x}$, assim basta tomar $x \in \mathbb{Z}$, então $\varphi(x) = \bar{x} = y$ o que mostra que φ é sobrejetiva, e ainda, $Ker(\varphi) = n\mathbb{Z}$. Portanto, pelo TFH, tem-se que

$$\frac{\mathbb{Z}}{n\mathbb{Z}} \backsimeq \mathbb{Z}_p.$$

Capítulo 2

Aritmética nos Domínios

Neste capítulo, vamos apresentar alguns resultados relevantes sobre domínios arbitrários, que se resume em certas generalizações de conceitos obtidos sobre o domínio $\mathbb{Z}$. Dentre esses, destacamos a existência de máximo divisor comum, bem como resultados relacionados à fatoração de um dado $a \in \mathcal{D} - \{0\}$, com $a \notin U_{\bullet}(\mathcal{D})$, como produto finito de irredutíveis de $\mathcal{D}$.

2.1 Relação de divisibilidade

Recordamos que um domínio $\mathcal{D}$ chama-se domínio principal quando cada ideal $\mathcal{I}$ em $\mathcal{D}$ é da forma $\mathcal{I} =< a >$, para algum $a \in \mathcal{D}$.

Definição 2.1. *Sejam $\mathcal{D}$ um domínio e $a,\ b \in \mathcal{D}$. Diremos que a é um divisor de b ou que a divide b(ou ainda que a é um fator de b) quando existe $c \in \mathcal{D}$ tal que*

$$b = ac.$$

Por conveniência, usaremos a mesma notação de divisibilidade em $\mathbb{Z}$, que é $a|b$, que indica que a é um divisor de b. Já a sua negação usaremos $a \nmid b$.

Teorema 2.1. *Sejam $\mathcal{D}$ um domínio e $a,\ b,\ c,\ d \in \mathcal{D}$. Então,*

(1) $a|b$ e $a|0$.

(2) Se $a|b$ e $b|c$, então $a|c$.

(3) Se $a|b$ e $a|c$, então $a|(xb + yc)$, para $\forall x,\ y \in \mathbb{R}$.

(4) Se $a|b$ e $c|d$, então $ac|bd$.

A demonstração do teorema anterior, será omitida levando em consideração que existe prova análoga em um curso básico de Teoria dos Números.

Definição 2.2. *Sejam a e b dois elementos arbitrários de um domínio $\mathcal{D}$ Diz-se que a é associado a b quando existe $u \in U_\bullet(\mathcal{D})$. tal que*

$$a = ub.$$

Usaremos a notação $a \sim b$ para indicar que a é associado a b. Além disso, notemos que a relação entre dois elementos associados é de equivalência sobre $\mathcal{D}$. E que a classe de equivalência determinada por um elemento a é o conjunto $\bar{a} = aU_\bullet(\mathcal{D})$. Além disso, vamos resaltar que no contexto do nosso trabalho $aU_\bullet(\mathcal{D})$ se refere a classe de equivalência dos elementos associados que é determinada pelo elemento a, e não a classe lateral determinada pelo elemento a, que é vista em um curso de Teoria dos Grupos.

Exemplo 2.1. *Para $\mathcal{K}$ sendo corpo, temos $U(K) = K$, portanto, o conjunto quociente pela relação de associatividade descrita acima é formado por 0 e $\mathcal{K}$, ou seja, se pegarmos dois elementos não nulos de $\mathcal{K}$, eles são associados.*

Exemplo 2.2. *Dois números inteiros a e b são associados se, e somente se, $a = b$ ou $a = -b$. De fato, seja o domínio $\mathbb{Z}$, sabemos que os únicos elementos invertíveis são ± 1. Sendo assim para $a,\ b \in \mathbb{Z}$ tais que $a|b$ e $b|a$. Então existem $c,\ d \in \mathbb{Z}$ tais que $b = ac$ e $a = bd$. Logo, $b = bdc$ o que implica $dc = 1$. Portanto, $c = d = \pm 1$. Assim, $a = b$ ou $a = -b$. De modo análogo temos a reciproca.*

Lembremos que se $a \in \mathcal{D}$ e $u \in U_\bullet(\mathcal{D})$. Temos $u|a$ e $(au)|a$, pois $a = u(u^{-1}a) = (au)u^{-1}$. Sendo assim, temos

$$U_\bullet(\mathcal{R}) \cup aU_\bullet(\mathcal{R}) \subset D(a)$$

para todo $a \in \mathcal{R}$ e $D(a) = \{x \in \mathcal{R} \ : \ x|a\}$.

Chamaremos os elementos do conjunto $U_\bullet(\mathcal{R}) \cup aU_\bullet(\mathcal{R})$ de **divisores impróprios de** a e se existir qualquer outro divisor de a de **divisor próprio de** a.Sendo assim um elemento b de $\mathcal{R}$ é um divisor próprio de a se, e somente se, $b|a$ e b não é invertível e nem é associado ao elemento a. Indicaremos por $P(a)$ o conjunto dos divisores próprios de a. Portanto,

$$D(a) = U_\bullet(\mathcal{R}) \cup aU_\bullet(\mathcal{R}) \cup P(a) \ \text{ e } \ (U_\bullet(\mathcal{R}) \cup aU_\bullet(\mathcal{R})) \cap P(a) = \varnothing.$$

Definição 2.3. *Sejam $\mathcal{R}$ um domínio e $a \in \mathcal{R}$. Então a é* ***invertível*** *se, e somente se, as condições abaixo são satisfeitas,*

(1) $a \notin U_\bullet(\mathcal{R}) \cup \{0\}$;

(2) $P(a) = \varnothing$. Isto é, os únicos divisores de a são os impróprios.

Definição 2.4. *Diremos que um elemento a de um domínio $\mathcal{R}$ é* ***redutível*** *se, e somente se, as condições abaixo são satisfeitas,*

(1) $a \in U_\bullet(\mathcal{R}) \cup \{0\}$;

(2) $P(a) \neq \varnothing$. Isto é, a admite ao menos um divisor proprio.

Exemplo 2.3. *No domínio dos inteiros $\mathbb{Z}$ temos que $U_\bullet(\mathbb{Z}) = \{-1, 1\}$. Portanto para todo inteiro não nulo a, temos*

$$U_\bullet(\mathbb{Z}) \cup aU_\bullet(\mathbb{Z}) = \{-1, 1, -a, a\}.$$

Notemos que se $p \in \mathbb{Z}$, com $p \neq 0$ e $p \neq \pm 1$, temos que p é irredutível se, e só se, os únicos divisores de p são ± 1 e $\pm p$; Sendo assim pela definição usual de um número primo, então p é irredutível se, e somente se, p é primo. De maneira análoga um inteiro a é redutível se, e somente se, a é composto.

Exemplo 2.4. *O elemento $2 \in \mathbb{Z}[i]$ não é primo e consequentemente não é irredutível. Sendo assim, $2 \notin U(\mathbb{Z}[i])$. Agora,*

$$2 = (1 + i) \cdot (1 - i),$$

Mas, se $2|(1 + i)$, digamos $(1 + i) = 2\alpha$, com $\alpha \in \mathbb{Z}[i]$, então

$$N(1 + i) = N(2) \cdot N(\alpha),$$

o que implica que $2 = 4 \cdot N(\alpha)$. Como $N(\alpha) \in \mathbb{N}$, então concluímos desta ultima igualdade que $4|2$ em $\mathbb{N}$, o que é um absurdo. Sendo assim $2|(1 - i)$. Portando, 2 não é primo em $\mathbb{Z}[i]$.

Definição 2.5. *Um domínio $\mathcal{D}$ é dito um* ***Domínio de Fatoração Única (ou DFU)*** *quando as seguintes condições são validas:*

(1) Todo elemento não nulo e não invertível $a \in \mathcal{D}$, pode ser escrito da forma

$$a = p_1, p_2, \ldots, p_r,$$

onde $p_i \in \mathcal{D}$ é irredutível, para cada $i = 1, 2, \cdots, r$.

(2) Quaisquer que sejam as famílias $(p_i)_{1\leq i\leq s}$ *e* $(q_i)_{1\leq j\leq t}$*, de elementos irredutíveis de* $\mathcal{D}$*, se*

$$p_1p_2\ldots p_s = q_1q_2\ldots q_t,$$

então $s = t$ *e existe uma permutação* σ *de* $[1, s]$ *tal que*

$$p_i \sim q_{\sigma(i)}$$

para $i = 1, 2, \ldots, s$*.*

Notemos que de acordo com a condição (2) da definição anterior, o fato que a decomposição de a cuja existência é assegurada meante (1), é única a menos da ordem dos fatores irredutíveis e a menos de elementos inversíveis.

Exemplo 2.5. *Conforme o Teorema Fundamental da Álgebra, o domínio dos inteiros* $\mathbb{Z}$ *é um DFU.*

Veremos mais adiante outros exemplos de Domínios de Fatoração Única como o anel de polinômios $K[X]$ com coeficientes num corpo K, os anéis euclidianos e os anéis de polinômios com coeficientes num DFU. Tais exemplos serão expostos no próximo capitulo.

2.2 Máximo Divisor Comum

Definição 2.6. *Sejam* $\mathcal{D}$ *um domínio e* $a,\ b \in \mathcal{D}$*. Chamamos um elemento* $d \in \mathcal{D}$ *de* ***máximo divisor comum (mdc)*** *de* a *e* b *quando as seguintes condições são satisfeitas:*

(1) $d|a$ *e* $d|b$*;*

(2) Para todo d' *em* $\mathcal{D}$*, se* $d'|a$ *e se* $d'|b$*, então* $d'|d$*.*

Conforme veremos mais adiante nem sempre existe um mdc de dois elementos quaisquer de um domínio arbitrário.

Definição 2.7. *Diremos que um domínio* $\mathcal{D}$ *é um anel com máximo divisor comum quando para dois elementos quaisquer de* $\mathcal{D}$ *admitem um mdc em* $\mathcal{D}$*.*

Exemplo 2.6. *O domínio dos inteiros* $\mathbb{Z}$ *é um anel com máximo divisor comum.*

A seguir enunciaremos e demostraremos para garantirmos que todo DFU possui mdc.

Lema 2.1. *Seja $\mathcal{D}$ um domínio de fatoração única, então $\mathcal{D}$ possui mdc.*

Demonstração: Para $a, b \in \mathcal{D}$, podemos supor evidentemente

$$a \in U_\bullet(\mathcal{D}) \cup \{0\} \quad \text{e} \quad b \in U_\bullet(\mathcal{D}) \cup \{0\},$$

portanto, pela definição (DFU) existem elementos irredutíveis $q_1, q_2, \ldots, q_s$ e $q'_1, q'_2, \ldots, q'_t$ tais que

$$a = q_1 q_2 \ldots q_s \quad \text{e} \quad b = q'_1 q'_2 \ldots q'_t.$$

Sendo assim, vamos considerar o conjunto

$$H = \{\overline{q_1},\ \overline{q_2},\ \ldots,\ \overline{q_s},\ \overline{q'_1}\ \overline{q'_2}\ \ldots,\ \overline{q'_t}\}$$

onde $\overline{q_i} = q_i U_\bullet(\mathcal{D})(i = 1, 2, \ldots, s)$ e $\overline{q_j} = q_j U_\bullet(\mathcal{D})(j = 1, 2, \ldots, t)$. Indicaremos por r o n úmero de elementos deste conjunto e suponhamos

$$H = \{\overline{p_1},\ \overline{p_2},\ \ldots,\ \overline{p_r}\}.$$

Cada elemento p_i é irredutível e se $i \neq j$ $(1 \leq i,\ j \leq r)$ então p_i não é associado a p_j; Além disso, cada elemento q_i $(1 \leq i \leq s)$ e q'_i $(1 \leq j \leq t)$ é associado a um e somente um fator irredutível qp_k $(1 \leq k \leq r)$. Portanto, os elementos a e b podem ser representados sob a forma

$$a = up_1^{\alpha_1} up_2^{\alpha_2} \ldots up_r^{\alpha_r} \quad \text{e} \quad b = vp_1^{\beta_1} vp_2^{\beta_2} \ldots vp_r^{\beta_r}.$$

Onde cada α_i ou β_i é um natural e u e v são elementos inversíveis de E. Alem do mais, $a|b$ se, e somente se, $\alpha_i \leq \beta_i$ para $i = 1, 2, \ldots r$. Consideremos $\delta_i = min\{\alpha_i,\ \beta_i\}$ $(i = 1, 2, \ldots, r)$ e consideremos o elemento

$$d = p_1^{\delta_1} p_2^{\delta_2} \ldots p_r^{\delta_r}.$$

Para afirmamos que d é um mdc de a e b temos que verificar se

(1) Temos $\delta_i \leq \alpha_i$ e $\delta_i \leq \beta_i$ para $i = 1, 2, \ldots, r$. Por conseguinte $d|a$ e $d|b$.

(2) Seja $d' \in E$ um divisor comum de a e b. Se $d' in U_\bullet(\mathcal{D})$ temos $d'|d$.

Sendo assim suponhamos que $d' \notin U_\bullet(\mathcal{D})$. Então pela definição (DFU), existem elementos irredutíveis $q''_1, q''_2, \ldots, q''_n$ em $\mathcal{D}$ tais que

$$d' = q''_1 q''_2 \ldots q''_n.$$

Como $d'|a$ e $d'|b$ resulta que cada fator q_i'' é associado a um, e somente um fator irredutível p_k $(1 \leq k \leq r)$, logo d' pode ser representado sob a forma

$$d' = wp_1^{r_1} wp_2^{r_2} \dots wp_r^{r_r},$$

onde w é invertível e cada r_k é um numero natural. E mais de $d'|a$ e $d'|b$ temos $r_k \leq \alpha_k$ e $r_k \leq \beta_k$. Logo, $r_k \leq min\{\alpha_k,\ \beta_k\} = \delta_k$, para $k = 1, 2, \dots r$. Por conseguinte $d'|d$. ■

Teorema 2.2. *Um domínio $\mathcal{D}$ é um domínio de fatoração única se, e somente se, $\mathcal{D}$ satisfaz as condições*

(1) Todo elemento não nulo e não invertível a, existem elementos irredutíveis $p_1, p_2, \dots, p_i$;

(2) Para dois elementos quaisquer de $\mathcal{D}$, admitem mdc em $\mathcal{D}$.

Demonstração: Sabemos que todo DFU possui um *mdc* de acordo com o lema anterior. Sendo assim, temos que satisfaz as condições (1) e (2). Reciprocamente, suponhamos que $\mathcal{D}$ satisfaz as condições (1) e (2) acima, sendo assim queremos mostrar que se $p \in \mathcal{D}$ e p é irredutível, então p é primo, resultando assim que $\mathcal{D}$ é um DFU. Seja p um elemento irredutível em $\mathcal{D}$ e suponhamos que $p|(ab)$ e $p \nmid a$, com a e b em $\mathcal{D}$. De tal fato temos que a e b são primos entre si, portanto o $p|b$. ■

Capítulo 3

Anéis Fatoriais

Este capítulo é o principal ponto do nosso trabalho. A priori, iremos abordar os anéis de polinômios que é uma seção de suma importância para uma generalização mais elegante sobre os anéis fatoriais que enunciamos no capitulo anterior. Em seguida iremos mostrar que todo domínio de Ideais Principais é um DFU e também mostraremos que todo Domínio Euclidiano é um DFU. Após isso iremos enunciar e demonstrar que se $\mathcal{R}$ é um anel fatorial (DFU), então o anel de polinômio $\mathcal{R}[X]$ é fatorial. Tal teorema é intitula em vários livros como Teorema de Gauss. Por fim iremos mostrar uma aplicação de DFU na resolução de equações diofantinas, tal seção poderá ser mais explanada em [2].

3.1 Anéis de Polinômios

Em alguns textos com uma linguagem em um nível mais elegante, nos deparamos com os autores utilizando o conceito de um elemento transcendente sobre um dado corpo, para definir os anéis de polinômios. Como nosso foco é fundamentar um caminho introdutório para a área da Álgebra Comutativa ou a Teoria dos Números Algébricos não iremos utilizar tais conceitos.

Definição 3.1. *Seja $\mathcal{R}$ um anel. Então um polinômio sobre $\mathcal{R}$ (ou com coeficientes em $\mathcal{R}$) é uma soma infinita da forma*

$$f(X) = \sum_{i=0}^{\infty} a_i X^i = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n + \cdots ,$$

onde $a_i \in \mathcal{R}$ e $a \neq 0$, para um número finito de índices i. Os elementos a_i são chamados de coeficientes de $f(X)$. O conjunto de todos os polinômios sobre $\mathcal{R}$ iremos indicar por $\mathcal{R}[X]$.

Exemplo 3.1. *Seja o polinômio*

$$n(X) = 0 + 0X + 0X^2 + \cdots \quad \in \mathcal{R}[X]$$

com $\mathcal{R}$ sendo anel é chamado ***polinômio identicamente nulo*** *ou simplesmente* ***polinômio nulo*** *sobre $\mathcal{R}$.*

O polinômio $n(X)$ acima será denotado por $\mathbf{0}$, ou seja,

$$n(X) = 0 = \sum_{i \geq 0} 0X^i.$$

Exemplo 3.2. *O polinômio*

$$f(X) = \overline{4} + \bar{0}X + \bar{0}X^2 + \cdots + 0X^n + \cdots$$

que podemos expressar por

$$f(X) = \overline{4}$$

com $f(X) \in \mathbb{Z}_5[X]$. É dito polinômio constante.

Definição 3.2. *Seja $\mathcal{R}$ um anel e*

$$a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \in \mathcal{R}[X].$$

Se $a_n \neq 0$, n é dito o grau de $f(X)$ e denotamos por $\partial f(X) = n$. Neste caso a_nX^n é chamado de ***termo líder*** *e a_n de* ***coeficiente líder****. No caso particular de $a_n = 1$, diremos que $f(X)$ é um* ***polinômio mônico*** *ou um* ***polinômio unitário*** *ou ainda um* ***polinômio normalizado****.*

Exemplo 3.3. *Seja $\mathcal{R} = \mathbb{Z}[X]$ o anel de polinômios com coeficientes inteiros, então para*

$$f(X) = 2 + X^2 + 3X^3 + 5X^6 \in \mathcal{R}$$

o coeficiente líder é 5.

A seguir iremos construir as operações de adição e multiplicação em $\mathcal{R}[X]$, de modo a torná-lo um anel sob tais operações. Para isso, sejam $\mathcal{R}$ um anel e $f(X),\ g(X) \in \mathcal{R}[X]$ de modo que

$$f(X) = a_0 + a_1X + \cdots + a_nX^n \ \text{ e } \ g(X) = b_0 + b_1X + \cdots + b_nX^n.$$

Então definimos as operações em $\mathcal{R}[X]$, como

$$f(X)+g(X)=\sum_{i=0}^{\max\{n,m\}}(a_i+b_i)X^i \tag{3.1}$$

para a soma e,

$$f(X)\cdot g(X)=\sum_{i=0}^{n+m}(\sum_{j=0}^{i}a_i+b_{i-j})X^i \tag{3.2}$$

para a multiplicação.

Exemplo 3.4. *Sejam $\mathbb{Z}[X]$ um anel e consideremos $f(x)$ e $g(X)\in\mathbb{Z}[X]$, tais que*

$$f(X)=2+X^2+3X^3 \quad e \quad g(X)=X+X^2.$$

Desse modo,

$$f(x)+g(X)=2+X+2X^2+3X^3$$

e também

$$f(X)\cdot g(X)=2X+2X^2+X^3+4X^4+3X^5.$$

Exemplo 3.5. *Consideremos os polinômios $f(X)$ e $g(X)$ em $\mathbb{Z}_8[X]$ dados por*

$$f(X)=\overline{3}+\overline{4}X \quad e \quad \overline{2}+\overline{4}X+\overline{2}X^2.$$

Note que os coeficientes de $f(X)$ são $a_0=\overline{3}$, $a_1=\overline{4}$ e $a_n=\overline{0}$ para todo $n\geq 2$. Já os de $g(x)$ são $b_0=\overline{2}$, $b_1=\overline{4}$, $b_2=\overline{2}$ e $b_m=\overline{0}$ para todo $m\geq 3$. Sendo assim, $c_k=\overline{0}$ para todo $k\geq 2$ e, temos

$$f(X)+g(X)=\overline{5}+2X^2.$$

Já a multiplicação temos que $d_k=\overline{0}$ para $k\geq 3$, que nos apresenta

$$f(X)\cdot g(X)=\overline{6}+\overline{4}X+\overline{6}X^2.$$

Teorema 3.1. *Seja $\mathcal{R}$ um anel. Então induzindo as operações (3.1) e (3.2) sobre $\mathcal{R}[X]$, temos que $(\mathcal{R}[X],+,\cdot)$ é um anel.*

Demonstração: A priori, note que $(\mathcal{R}[X],+,\cdot)$ é um grupo abeliano. Sendo assim basta mostrarmos a distributividade sobre a adição e a associatividade sobre a multiplicação. Para isso consideremos

$$f(X)=\sum_{i=0}^{\infty}a_iX^i, \quad g(X)=\sum_{j=0}^{\infty}b_jX^j \quad \text{e} \quad h(X)=\sum_{k=0}^{\infty}c_kX^k.$$

Então,

$$\begin{aligned} f(X)\cdot[g(X)+h(X)] &= \left(\sum_{i=0}^{\infty}a_iX^i\right)\cdot\left[\left(\sum_{j=0}^{\infty}b_jX^j\right)+\left(\sum_{k=0}^{\infty}c_kX^k\right)\right] \\ &= \left(\sum_{i=0}^{\infty}a_iX^i\right)\cdot\left(\sum_{j=0}^{\infty}b_jX^j\right)+\left(\sum_{i=0}^{\infty}a_iX^i\right)\cdot\left(\sum_{k=0}^{\infty}c_kX^k\right) \\ &= [f(X)\cdot g(X)]+[f(X)\cdot h(X)]\,. \end{aligned}$$

Agora, vamos mostrar a associatividade sobre a operação multiplicação, tal prova requer um pouco mais de atenção, no entanto a mesma não é de nível muito elevado. Assim para os mesmos polinômios $f(X),\ g(X)$ e $h(X)\in\ \mathcal{R}[X]$, temos

$$\begin{aligned} f(X)\cdot[g(X)\cdot h(X)] &= \left(\sum_{i=0}^{\infty}a_iX^i\right)\cdot\left[\left(\sum_{j=0}^{\infty}b_jX^j\right)\cdot\left(\sum_{k=0}^{\infty}c_kX^k\right)\right] \\ &= \left(\sum_{i=0}^{\infty}a_iX^i\right)\cdot\left[\sum_{n=0}^{\infty}\left(\sum_{j=0}^{n}b_jc_{n-j}\right)X^n\right] \\ &= \sum_{s=0}^{\infty}\left[\sum_{n=0}^{\infty}a_{s-n}\left(\sum_{j=0}^{n}b_jc_{n-j}\right)\right]X^s \\ &= \sum_{s=0}^{\infty}\left(\sum_{i+j+k=s}a_ib_jc_k\right)X^s \\ &= \sum_{s=0}^{\infty}\left[\sum_{m=0}^{\infty}\left(\sum_{i=0}^{m}a_ib_{m-i}\right)c_{s-m}\right]X^s \\ &= \left[\sum_{m=0}^{\infty}\left(\sum_{i=0}^{m}a_ic_{m-i}\right)X^m\right]\cdot\left(\sum_{k=0}^{\infty}c_kX^k\right) \\ &= \left[\left(\sum_{i=0}^{\infty}a_iX^i\right)\cdot\left(\sum_{j=0}^{\infty}b_jX^j\right)\right]\cdot\left(\sum_{k=0}^{\infty}c_kX^k\right) \\ &= [f(X)\cdot g(X)]\cdot h(X), \end{aligned}$$

Portanto, $(\mathcal{R}[X],+,\cdot)$ é um anel. ■

O teorema a seguir mostra que algumas propriedades do anel $\mathcal{R}$ são levadas para o anel $\mathcal{R}[X]$. A demonstração do teorema será omitida pois julgamos a mesma trivial para o seguinte momento do nosso trabalho.

Teorema 3.2. *Seja $\mathcal{R}$ um anel. Então,*

(1) Se $\mathcal{R}$ é comutativo, então $\mathcal{R}[X]$ é comutativo;

(2) Se $\mathcal{R}$ tem unidade, então $\mathcal{R}[X]$ tem unidade;

(3) Se $\mathcal{R}$ é domínio, então $\mathcal{R}[X]$ também é domínio.

Proposição 3.1. *Se $\mathcal{D}$ é um domínio e $f(X), g(X) \in \mathcal{D}[X] - \{0\}$, então*

$$\partial(f(X) \cdot g(X) = \partial f(X) + \partial g(X).$$

Demonstração: Consideremos

$$f(X) = a_0 + a_1X + \cdots + a_nX^n \text{ e } g(X) = b_0 + b_1X + \cdots + b_mX^m,$$

com $a_n \neq 0$ e $b_m \neq 0$, e que $\partial f(X) = n$ e $\partial g(X) = m$. Então,

$$f(X) \cdot g(X) = \sum_{i=0}^{n+m} \left(\sum_{j=0}^{i} a_j b_{i-j} \right) X^i.$$

Observemos que o coeficiente líder é a_nb_m. Como temos $\mathcal{D}$ sendo domínio e a_n, b_m não nulos, segue que $a_nb_m \neq 0$. Por isso,

$$\partial(f(X) \cdot g(X)) = n + m = \partial f(X) + \partial g(X).$$

■

Vale destacar na proposição anterior que bastaria que um dos polinômios não ser divisor de zero.

Corolário 3.1. *Sejam $\mathcal{K}$ um corpo e $f(X), g(X) \in \mathcal{K}[X] - \{0\}$, então*

$$\partial(f(X) \cdot g(X)) = \partial f(X) + \partial g(X).$$

3.2 Divisibilidade em $\mathcal{R}[X]$

A seguir vamos enunciar alguns resultados de divisibilidade em $\mathcal{R}[X]$, tais conceitos são similares aos apresentados no capitulo anterior, aqui vamos omitir as demonstrações pois são análogas as do capitulo 2.

Definição 3.3. *Sejam $\mathcal{R}$ um domínio e $f(X), g(X) \in \mathcal{R}[X]$. Então diremos que $g(X)$ divide $f(X)$ ou $f(X)$ é divisível por $g(X)$ quando existe $q(X) \in \mathcal{R}[X]$, tal que*

$$f(X) = g(X) \cdot q(X).$$

Exemplo 3.6. *Em $\mathbb{Z}[X]$ o polinômio $g(X) = 1 + 3X + X^3$ divide $f(X) = 3 + 10X + 3X^2 + 3X^3X^4$, pois*

$$f(X) = (3 + X)(1 + 3X + X^3).$$

Proposição 3.2. *Sejam $f(x), g(x), h(x) \in \mathcal{R}[X]$, então*

(1) $f(X) \mid f(X)$;

(2) Se $g(X) \mid h(X) \quad e \quad h(X) \mid f(X)$, *então* $g(X) \mid f(X)$;

(3) Se $g(X) \mid f(X)$, *então* $g(X) \mid f(X)h(X)$;

(4) Se $g(X) \mid f(X) \quad e \quad g(X) \mid h(X)$, *então* $g(X) \mid (f(X)k_1(X)+h(X)k_2(X)), \forall\, k_1(X), k_2(X) \in \mathcal{R}[X]$.

Teorema 3.3. *(Algoritmo da Divisão em $\mathcal{R}[X]$) Sejam $f(X), g(X) \in \mathcal{R}[X]$, com $g(X) \neq 0$ e com o coeficiente líder de $g(X)$ um elemento invertível em $\mathcal{R}$. Então, existem únicos $q(X), r(X) \in \mathcal{R}[X]$ tais que*

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

em que $r(X) = 0$ ou $\partial r(X) < \partial g(X)$.

A demonstração do Teorema anterior como foi dito no inicio desta seção também será omitida, no entanto a mesma se encontra com bastante detalhe em [8].

3.3 Fatoração Única em $\mathcal{R}[X]$

Nesta seção iniciaremos com alguns resultados que poderiam estar no capitulo anterior mais optamos inseri-los neste momento pois sera de suma importância para a demostração do teorema que afirma que todo domínio euclidiano é um domínio de fatoração única, que estará na próxima seção do nosso trabalho.

Teorema 3.4. *Se $\mathcal{D}$ é um DIP, então todo elemento $a \in \mathcal{D}$, não nulo e não invertível, possui um divisor irredutível.*

Teorema 3.5. *Todo DIP é um DFU.*

Demonstração: Seja $\mathcal{D}$ um DIP e tomemos $a \in \mathcal{D}$, com $a \neq 0$ e $a \notin U_\bullet(\mathcal{D})$.

(Existência da Fatoração) Se a é irredutível não há mais nada a provar. Caso contrario de acordo com o teorema anterior, existem um $p_1 \in \mathcal{D}$ que é irredutível e um $a_1 \in \mathcal{D}$ tais que

$$a = p_1 \cdot a_1.$$

Sendo a redutível, temos que $a_1 \notin U_\bullet(\mathcal{D})$. Se a_1 for irredutível, então segue-se a prova. Caso contrário, existem um irredutível p_2 e um elemento a_2 em $\mathcal{D}$ tais que

$$a_1 = p_2 \cdot a_2, \quad \text{com} \quad a_2 \notin U_\bullet(\mathcal{D}).$$

Logo,

$$< a > \subset < a_1 > \subset < a_2 >$$

Substituindo assim, o valor $a_1 = p_2 \cdot a_2$ em a temos

$$a = p_1 \cdot p_2 \cdot a_2.$$

Com efeito, existirá um $r > 1$ de modo que

$$< a > \subset < a_1 > \subset < a_2 > \subset \ \cdots \ \subset < a_{r-1} >,$$

com a_{r-1} sendo irredutível, ou seja, $< a_{r-1} >$ é um maximal. Logo,

$$< a_{r-1} >=< a_r >=< a_{r+1} >= \cdots$$

. Além disso, considerando $a_{r-1} = p_r$, temos

$$a = p_1 p_2 \cdots p_r.$$

Se por algum acaso isso não ocorresse, existiria uma cadeia ascendente de ideais em $\mathcal{D}$ que não seria estacionaria, o que contrairia o fato que se $\mathcal{D}$ é domínio de ideais principais, toda cadeia ascendente de ideais é estacionaria. Sendo assim provamos a existência da fatoração.

(Unicidade da Fatoração) Suponhamos agora que existam $q_1,\ q_2,\ \cdots\ q_s$ irredutíveis tais que $a = q_1,\ q_2,\ \cdots\ q_s$. Assim,

$$p_1,\ p_2,\ \cdots\ p_s = q_1,\ q_2,\ \cdots\ q_s,$$

Desse modo,

$$p_1 \mid q_1,\ q_2,\ \cdots\ q_s.$$

Mas como $\mathcal{D}$ é DIP e p_1 é irredutível então p_1 é primo. Assim temos, $p_1 \mid q_i$; para algum $i = 1,\ 2,\ \cdots\ s$. Sem perca de generalidade, podemos supor $p_1 \mid q_1$. Como q_1 é também irredutível, temos

$$q_1 = u_1 \cdot p_1 \quad \text{com} \quad u_1 \in U_\bullet(\mathcal{D}).$$

Portanto,

$$p_1 p_2 \cdots p_r = u_1 p_1 q_2 \cdots q_s,$$

ou seja,

$$p_2 \cdots p_r = u_1 q_2 \cdots q_s.$$

Analogamente através da ultima igualdade suponhamos que $p_2 \mid q_2$ e por isso,

$$q_2 = u_2 \cdot p_2 \quad \text{com} \quad u_2 \in U_\bullet(\mathcal{D}).$$

Assim,

$$p_3 \cdots q_r = u_1 u_2 q_3 \cdots q_s.$$

Seguindo o mesmo procedimento aplicado anteriormente, temos

$$1 = u_1 u_2 \cdots u_r \cdot q_{r+1} \cdots q_s$$

em que $u_1, u_2, \cdots, u_r \in U_\bullet(\mathcal{D})$. Desde que $q_{r+1}, \cdots, q_s$ são todos irredutíveis e assim não invertíveis devemos ter necessariamente $r = s$. Sendo p_i e q_i associados para cada $i + 1, 2, \cdots r$. Desse modo fica provada a unicidade (a menos de associados) da fatoração. ■

Vale ressaltar que nem sempre é valida a reciproca do teorema anterior.

Definição 3.4. *Sejam $\mathcal{R}$ um corpo e $p(X) \in \mathcal{R}[X]$. Então $p(X)$ é dito* ***irredutível em*** *$\mathcal{R}[X]$ ou* ***irredutível sobre*** *$\mathcal{R}$ se*

(1) $\partial p(X) \geq 1$*;*

(2) Se $p(X) = f(X)g(X)$*, com* $f(X), g(X) \in \mathcal{R}[X]$*, então*

$$f(X) \in \mathcal{R} \quad ou \quad g(X) \in \mathcal{R},$$

ou seja,

$$\partial f(X) = 0 \quad ou \quad \partial g(X) = 0.$$

Caso contrário, $p(X)$ é dito ***redutível em*** *$\mathcal{R}[X]$ ou* ***redutível sobre*** *$\mathcal{R}$.*

Definição 3.5. *Diremos que um polinômio não nulo*

$$f(X) = \sum_{i=0}^{n} a_i X^i \in \mathcal{R}[X]$$

é ***primitivo*** *se, e só se, seus coeficientes são relativamente primos, ou seja,*

$$mdc(a_0, a_1, a_2, \cdots, a_n) = 1.$$

Exemplo 3.7. *O polinômio* $p(X) = 3 + 2X + 5X^2 + 7X^3 \in \mathbb{Z}[X]$ *é primitivo. De fato,* $mdc(3, 2, 5, 7) = 1$.

Lema 3.1 (Gauss)**.** *O produto de dois polinômios primitivos é primitivo.*

Demonstração: A priori, sejam $f(X),\ g(X) \in \mathcal{R}[X]$ dois polinômios primitivos, tais que

$$f(X) = \sum_{i=0}^{n} a_i X^i \ \text{ e } \ g(X) = \sum_{j=0}^{m} b_j X^j$$

Agora, suponhamos que o polinômio

$$f(X) \cdot g(X) = \sum_{k=0}^{n+n} c_k X^k$$

onde

$$c_k = \sum_{i+j=k} a_i b_j$$

não é primitivo. Sendo assim, existe um elemento irredutível $p \in \mathcal{R}$ tal que $p \mid c_k$ para $k = 0, 1, \cdots, n+m$. Por outro lado, como $f(X)$ e $g(X)$ são primitivos, temos que p não divide todos os coeficientes de $f(X)$ e do mesmo modo para $g(X$. Logo, existem números naturais r e s, com $0 \leq r \leq n$ e $0 \leq s \leq m$, tais que $p \nmid a_r$, $p \nmid b_s$, $p \nmid a_i$ para $i < r$ e $p \mid b_j$ para $j < s$; Considerando-se o coeficiente líder c_{r+s} de $f(X) \cdot g(X)$, temos

$$c_{r+s} = (a_0 b_{r+s} + \cdots + a_{r-1} b_{s+1}) + a_r b_s + (a_{r+1} b_{s-1} + \cdots + a_{r+s} b_0),$$

De onde vem, $p \mid (a_r b_s)$, portanto, $p \mid a_r$ ou $p \mid b_s$ pois p é primo e $\mathcal{R}$ é fatorial, o que contradiz a definição dos elementos a_r e b_s. ∎

A seguir enunciaremos o Teorema mais importante do nosso trabalho. Antes disso enunciaremos sem demonstração um corolário que será fundamental na parte final da demonstração do teorema citado acima.

Lema 3.2. *Seja* $\mathcal{R}$ *um domínio de fatoração única. Se* $p(X) \in \mathcal{R}[X]$ *é um polinômio irredutível e* $p(X) \mid q_1(X) \cdots q_r(X)$*, para* $q_1(X) \cdots q_r(X) \in E[X]$*, então* $p(X)$ *divide algum* $q_i(X)$*, para* $i = 1, 2, \ldots, r$.

Teorema 3.6 (Teorema de Gauss)**.** *Se* $\mathcal{R}$ *um domínio de fatoração única, então* $\mathcal{R}[X]$ *também é um domínio de fatoração única.*

Demonstração: Tomemos $f(X) \in \mathcal{R}[X] - \{0\}$.Se $\partial f(X) = 0$, então termina a demonstração pois $f(X) \in \mathcal{R}$ e $\mathcal{R}$ é um DFU. Se não, supondo que $\partial f(X) \geq 1$ e que o resultado seja válido

para $\partial f(X) = r$, onde $0 \leq r < n-1$. Observemos que, se $f(X)$ for irredutível em $\mathcal{R}[X]$, o resultado segue de forma imediata. Caso contrário, tomemos

$$f(X) = f_1(X)f_2(X),$$

onde $f_1(X), f_2(X) \in \mathcal{R}[X]$, tais que $f_1(X) \notin \mathcal{R}$ e $f_2(X) \notin \mathcal{R}$, e ainda, $0 < \partial f_1(X), \partial f_2(X) < r$. Assim, o resultado segue indutivamente.

Agora, se $f(X)$ é irredutível, então o resultado segue de forma imediata. Caso contrário, suponhamos que o resultado seja válido para todos os polinômios que admitem uma decomposição como um produto de $n-1$ fatores irredutíveis. Assim, tomemos

$$f(X) = ap_1(X)p_2(X)\cdots p_n(X),$$

onde $p_i(X) \in \mathcal{R}[X]$ são polinômios mônicos e irredutíveis, para cada $i \in \{1, 2, \ldots, n\}$ e $a \in \mathcal{R}$. Suponhamos que exista outra decomposição de $f(X)$, dessa forma,

$$f(X) = bq_1(X)q_2(X)\cdots q_m(X),$$

onde $q_j(X) \in \mathcal{R}[X]$ são polinômios mônicos e irredutíveis, para cada $j \in \{1, 2, \ldots, m\}$ e $b \in E$. Notemos que o coeficiente líder de $f(X)$ é igual à a que também é igual à b, ou seja, $a = b$. Dessa maneira,

$$p_1(X)p_2(X)\cdots p_n(X) = q_1(X)q_2(X)\cdots q_m(X)$$

daí,

$$p_1(X)\left[p_2(X)\cdots p_n(X)\right] = q_1(X)q_2(X)\cdots q_m(X),$$

ou seja, $p_1(X)$ divide $q_1(X)q_2(X)\cdots q_m(X)$. Pelo lema 3.2 temos que, $p_1(X)$ divide algum $q_j(X)$, para $j = 1, 2, \ldots, m$. Sem perda de generalidade, suponhamos que

$$p_1(X) \mid q_1(X)$$

e como $p_1(X)$ e $q_1(X)$ são mônicos e irredutíveis, segue que

$$p_1(X) = q_1(X).$$

Assim,

$$p_2(X)p_3(X)\cdots p_n(X) = q_2(X)\cdots q_3(X)q_m(X).$$

Como $q_2(X)\cdots q_3(X)q_m(X)$ é um polinômio que se decompõe em um produto com $n-1$ fatores mônicos e irredutíveis, por indução temos que, $n = m$. ■

3.4 Domínios Euclidianos

Estudaremos nessa seção, certos domínios que admitem um algoritmo de divisão análogo ao que se pode ser visto no estudo dos números inteiros. No entanto é necessário o conceito de função euclidiana para defini-los.

Definição 3.6. *Seja $\mathcal{D}$ um domínio. Diremos que $\mathcal{D}$ é um* ***domínio euclidiano****(DE) quando existe uma função $\varphi : \mathcal{D}^* \to \mathbb{N}\{0\}$ satisfazendo as seguintes propriedades abaixo:*

(1) Se $a,\ b \in \mathcal{D}^*$ e $b \mid a$, então $\varphi(b) \leq \varphi(a)$.

(2) Dados $a,\ b \in \mathcal{D}$, com $b \neq 0$, existem $q,\ r \in \mathcal{D}$ tais que

$$a = bq + r, \quad com \ \ r = 0 \ \ ou \ \ \varphi(r) < \varphi(b).$$

A função φ acima será chamada de **função euclidiana** para $\mathcal{D}$, e mais, os elementos q e r são ditos **quociente** e **resto**, respectivamente, na divisão euclidiana de a por b.

Exemplo 3.8. *O domínio $\mathbb{Z}$ dos números inteiros é um anel euclidiano. De fato, pois existe a aplicação $\delta : Z^* \to \mathbb{N}$ definida por $\delta(n) = |n|$ que satisfaz o item (i) da definição anterior pois, $\delta(mn) = \delta(m)\delta(n)$ e $\delta(n) \geq 1$. Já o item (ii) é garantido pelo algoritmo de divisão dos inteiros.*

Teorema 3.7. *Todo domínio euclidiano é um domínio principal.*

Demonstração: Seja $\mathcal{D}$ um domínio euclidiano com função euclidiana φ. Agora consideremos $\mathcal{I}$ como sendo um ideal de $\mathcal{D}$, com $\mathcal{I} \neq \{0\}$. Sendo assim, existe $b \in \mathcal{I}$, $b \neq 0$. Pelo principio de boa ordenação podemos escolher $b \in \mathcal{I}$ de tal modo que

$$\varphi(b) = min\{\varphi(x) : \ x \in \mathcal{I} - \{0\}\}.$$

Queremos mostrar que $\mathcal{I} =< b >$. é evidente que $< b > \subset \mathcal{I}$; Agora, seja $a \in \mathcal{I}$. Como $\mathcal{D}$ é euclidiano, existem $q,\ r \in \mathcal{D}$, tais que

$$a = bq + r, \quad \text{com} \ \ r = 0 \ \ \text{ou} \ \ \varphi(r) < \varphi(b).$$

Desde que $a,\ b \in \mathcal{I}$. Portanto, pelo fato de origem de b, não pode ocorrer $\varphi(r) < \varphi(b)$. Por isso,$r = 0$ e, por conseguinte

$$a = b \cdot q \in < b >,$$

ou seja, $\mathcal{I} \subset < b >$. Logo, $\mathcal{I} =< b >$, o que conclui a demonstração. ■

Corolário 3.2. *Todo domínio euclidiano é um DFU.*

Demonstração: Seja $\mathcal{D}$ um domínio euclidiano. Sabemos pelo teorema anterior que todo DE é um DIP. E também sabemos que todo DIP é DFU. Logo, por transitividade $\mathcal{D}$ é DFU. ■

3.5 Consequências da Fatoração Única

Uma das diversas consequências da fatoração única é a resolução de equações diofantinas. Iremos resolver um exemplo envolvendo as equações diofantinas, levando em consideração a fatoração única do domínio que estaremos trabalhando.

Exemplo 3.9. *Para a equação*

$$y^2 + 1 = x^3. \tag{3.3}$$

Temos que não existem $x,\ y \in \mathbb{Z}$ *que satisfaçam a igualdade* (3.3).

Solução: A priori vamos deixar claro que estaremos trabalhando com o domínio $\mathcal{R} = \mathbb{Z}[i]$, que é um domínio euclidiano e por consequência um domínio de fatoração única, munido da aplicação norma dada por

$$\begin{aligned} N : \mathbb{Z}[i] &\rightarrow \mathbb{N} \cup \{0\} \\ a + bi &\mapsto a^2 + b^2 \end{aligned}$$

De inicio, vamos verificar se podemos escrever (3.3) como

$$y^2 + 1 = (y + i)(y - i) = x^3.$$

Então notemos que,

$$y^2 + 1 = (y + i)(y - i) = x_1^3 x_2^3, \ \text{ onde } \ x_1^3 = u_1(y + i) \ \text{ e } \ x_2^3 = u_2(y - i),$$

sendo u_1 e u_2 elementos unidade em E(esses elementos são os inversíveis de $\mathbb{Z}[i]$, isto é, ± 1 e $\pm i$).

Note que,

$$N(y + i) = N(y - i) = |y^2 + 1|,$$

ou seja, é um inteiro impar. Para que $(y + i)(y - i) = x_1^3 x_2^3$, seja satisfeito, devemos mostrar que não é possível encontrar um δ que divida o fator $(y+i)(y-i)$. Sendo assim, δ não dividirá $x_1^3 x_2^3$. Suponhamos que δ divida $(y+i)$ e $(y-i)$, então δ divide qualquer combinação linear de ambos os fatores, em particular à diferença, ou seja, $\delta \mid 2i$;

Assim,

$$N(q\delta) = N(q)N(\delta) = N(2i) = N(2)N(i) = N(2) = 4,$$

que implica que $N(\delta)$ é par. O que é um absurdo. Portanto $x_1^2 = u1(y+i)$ e $x_2^3 = u_2(y-i)$.

Sem perca de generalidade, vamos supor que, $x_1^2 = u1(y+i) = 1(a+bi)^3$. Assim,

$$y + i = a^3 + 3a^2bi + 3ab^2(-1) + (bi)^3 = a(a^2 - 3b^2) + ib(3a^2 - b^2),$$

organizando a equação anterior, obtemos

$$1 = b(3a^2 - b^2) \quad \text{e} \quad y = a(a^2 - 3b^2).$$

Por fim, observemos que a primeira equação não pode ser satisfeita para nenhum valor $a, b \in \mathbb{Z}$. Portanto, a equação diofantina $y^2 + 1 = (y+i)(y-i) = x^3$ não tem solução inteira.

3.6 Conclusão

Acreditamos que nossa intenção de estudar anéis de polinômios utilizando os domínio de fatoração única foi cumprida. Ao demonstrar o *teorema*(3.6) e resolver o *exemplo*(3.9) que é o principal teorema do nosso trabalho, e por conseguencia o principal e mais importante exemplo que dermos neste trabalho, obtivemos resultados centrais no estudo de anéis de polinômios com aplicações em Álgebra Comutativa, Teoria Álgebrica dos Números e Geometria Álgebrica. Acreditamos também que o presente material fornece a fundamentação elementar para os interessado em seguir os estudo mais rigorosos, sobre os anéis comutativos.

Referências Bibliográficas

[1] GONÇALVEZ, A. *Introdução à Álgebra*. 5 ed. Rio de Janeiro : IMPA, 2009.

[2] HERSTEIN, I. N. *Tópicos de Álgebra*. Tradução de Adalberto P. Bergamasco e L. H. Jacy Monteiro. São Paulo : Editora Polígono, 1970.

[3] HEFEZ, A; *Curso de Álgebra*, Vol. 1. Rio de Janeiro : IMPA, 2003.

[4] DOMINGUES, H. H.; IEZZI, Gelson. *Álgebra Moderna* : volume único. 4. ed. São Paulo : Atual, 2011.

[5] FRALEIGH, John B. *A first course in abstract algebra*. 7. ed. New York : Addison Wesley, 2002.

[6] GARCIA, A.; LEQUAIN, Y. *Elementos de Álgebra*. 5. ed. Rio de Janeiro : IMPA, 2010.

[7] MONTEIRO, L. H. J. *Elementos de Álgebra*. Rio de Janeiro : Livros Técnicos e Científicos Editora S. A., 1974.

[8] VIEIRA, V. L. *Álgebra Abstrata para Licenciatura* (2ª edição). Editora da Universidade Estadual da Paraíba (coedição: Editora Livraria da Física), Campina Grande/São Paulo, 2015.

[9] EVES, H. *Introdução à história da Matemática*. tradução de Hygino H. Domingues. Campinas, SP : Editora da Unicamp, 2004.

[10] GARBI, G. G. *O romance das equações algébricas*. 2. ed. São Paulo : Editora Livraria da Física, 2007.

[11] VIEIRA, V. L. *Um Curso Básico em Teoria dos Números*. Editora da Universidade Estadual da Paraíba (coedição: Editora Livraria da Física), Campina Grande/São Paulo, 2015.

[12] STEWART, I. *Algebraic number theory and fermat's last theorem.* 3. ed. New York : A K Peters, 2001.