Um estudo sobre a divisibilidade nos domínios $\mathbb{Z}$ e $\mathbb{K}[X]$

Maria Paula Almeida Cavalcante Dias
Orientada pelo Prof. Me. Lucas Casanova Silva
e pela Profa. Ma. Gabriela Cotrim de Moraes

IFSP
São Paulo

2015

Um estudo sobre a divisibilidade nos domínios $\mathbb{Z}$ e $\mathbb{K}[X]$

Monografia apresentada ao Instituto Federal de Educação, Ciência e Tecnologia, em cumprimento ao requisito exigido para a obtenção do grau acadêmico Licenciado em Matemática.

Maria Paula Almeida Cavalcante Dias
Orientada pelo Prof. Me. Lucas Casanova Silva
e pela Profa. Ma. Gabriela Cotrim de Moraes

IFSP
São Paulo

2015

Dados Internacionais de Catalogação na Publicação (CIP)

Dias, Maria Paula Almeida Cavalcante

Um estudo sobre a divisibilidade nos domínios $\mathbb{Z}$ e $\mathbb{K}[X]$/ Maria Paula Almeida Cavalcante Dias - São Paulo: IFSP, 2015.

49f.

Trabalho de Conclusão do Curso Superior de Licenciatura em Matemática - Instituto Federal de Educação, Ciência e Tecnologia de São Paulo

Orientador(es): Lucas Casanova Silva, Gabriela Cotrim de Moraes

1. Anéis de Polinômios. 2. Domínio euclidiano. 3. Domínio fatorial. I. Um estudo sobre a divisibilidade nos domínios $\mathbb{Z}$ e $\mathbb{K}[X]$.

Maria Paula Almeida Cavalcante Dias

UM ESTUDO SOBRE A DIVISIBILIDADE NOS DOMÍNIOS $\mathbb{Z}$ E $\mathbb{K}[X]$

Monografia apresentada ao Instituto Federal de Educação, Ciência e Tecnologia, em cumprimento ao requisito exigido para a obtenção do grau acadêmico Licenciado em Matemática.

APROVADA EM: ____/____/_____ CONCEITO: _____

Profa. Ma. Vânia Batista Flose Jardim
Instituto Federal de Educação, Ciência e Tecnologia
Membro da Banca

Profa. Ma. Gabriela Cotrim de Moraes
Instituto Federal de Educação, Ciência e Tecnologia
Coorientadora - Membro da banca

Prof. Me. Lucas Casanova Silva
Instituto Federal de Educação, Ciência e Tecnologia
Orientador

Aluna: Maria Paula Almeda Cavalcante Dias

À minha família.

AGRADECIMENTOS

Aos meus pais, pelo amor, incentivo e dedicação durante toda a vida.

Às minhas irmãs, pelo carinho.

Ao Felipe, pelo companherismo.

Ao corpo docente do IFSP - Câmpus São Paulo por todo o conhecimento adquirido durante o curso.

Ao professor Lucas Casanova Silva pela orientação e confiança.

À professora Gabriela Cotrim de Moraes pela orientação e colaboração.

Aos colegas, pelo apoio durante o curso.

O livro do mundo está escrito
em linguagem matemática.
Galileu Galilei

RESUMO

O objetivo deste trabalho é apresentar um breve pesquisa sobre anéis de polinômios e sobre a divisibilidade em domínios de integridade. Vamos nos restringir ao estudo dos domínios $\mathbb{Z}$ e $\mathbb{K}[X]$, em que $\mathbb{K}$ é um corpo. Estudaremos, de maneira sucinta, a divisão em $\mathbb{Z}$, anéis de polinômios e, por fim, domínios euclidianos e domínios fatoriais, onde veremos a relação existente entre a divisão em $\mathbb{Z}$ e a divisão em $\mathbb{K}[X]$.

Palavras-chave: Anéis de Polinômios, Domínio euclidiano, Domínio fatorial.

ABSTRACT

The aim of this work is to present a summarized study of polynomials rings and the divisibility of integral domain. The monograph was restricted of domains $\mathbb{Z}$ and $\mathbb{K}[X]$, when $\mathbb{K}$ is a field. There is a brief study of the division in $\mathbb{Z}$, polynomials rings and finally, euclidean domains and factorial domains, where there is an analysis of the relationship between the division in $\mathbb{Z}$ and division in $\mathbb{K}[X]$.

Keywords: Polynomials rings, Euclidean domain, Factorial domain.

Sumário

CAPÍTULO

1

INTRODUÇÃO

Em meados do século XVI, Simon Steve (1548 – 1620) introduziu a ideia de um novo objeto matemático para formulação de problemas, o polinômio (ou multinômio), e estudou as operações deste objeto (MILIES, 2004, p. 6).

Posteriormente, como Domingues (2003, p. 282) aponta em um breve histórico que faz no início dos capítulos de sua obra, François Viète (1540 – 1603) e René Descartes (1596 – 1650) contribuíram para o desenvolvimento dos polinômios, com a representação de constantes e variáveis por letras. Domingues (2003, p. 211) ainda conta que, a partir do século XIX, a organização lógica e a axiomatização da matemática receberam tratamento especial, que o trabalho de George Peacock (1791 – 1858) introduziu a ideia de *álgebra simbólica* (EVES, 2011, p. 546) e que, mais tarde, William R. Hamilton (1805 – 1865), David Hilbert (1862 – 1943), dentre outros matemáticos, colaboraram para a organização da Álgebra, definindo inúmeras estruturas algébricas, dentres elas, o *anel* que, apenas em 1914 foi definido como estrutura matemática de maneira puramente algébrica, por Adolf A. H. Fraenkel (1891 – 1965).

A Álgebra estuda as estruturas matemáticas e a forma com que elas se relacionam. O estudo dessa área da matemática por alunos da licenciatura é, então, de extrema importância quando se pensa no desenvolvimento do raciocínio lógico dos alunos da educação básica, como aponta Tinoco (2009).

O desejo de estudar conteúdos complementares aos que foram abordados durante a

disciplina de *Álgebra* do curso de Licenciatura em Matemática do IFSP- Câmpus São Paulo, e o interesse por esta área impulsionaram o desenvolvimento deste trabalho. O fato de os polinômios terem grande presença na matemática, inclusive nos conteúdos trabalhados na educação básica também foram determinantes na escolha do tema.

O objetivo deste trabalho é apresentar um estudo sobre os anéis de polinômios e um breve comparativo com a *Teoria dos Números Inteiros*. Assim, o trabalho foi dividido em três capítulos, além desta introdução, da fundamentação teórica e das considerações finais. Inicialmente, apontaremos alguns tópicos preliminares importantes para o entendimento das partes seguintes do trabalho. Na sequência, será apresentado um pequeno estudo sobre os anéis de polinômios. E, finalmente, traremos uma breve formalização de teoremas da *Teoria dos Números Inteiros* e de polinômios sobre corpos, são eles: *O algoritmo euclidiano, A fatoração única* e o Teorema da *Existência do mdc*.

Neste trabalho, o estudo desses dois conceitos, de anel e de polinômio, e ainda a teoria dos números inteiros, se apoiará, principalmente, nas obras de Hygino H. Domingues, Gelson Iezzi e de César Polcino Milies, além de outras fontes que podem ser encontradas nas referências.

CAPÍTULO

2

CONCEITOS PRELIMINARES

Neste capítulo, apresentaremos alguns conceitos que são essenciais para o entendimento dos capítulos seguintes. Aqui, trabalharemos com três teoremas sobre os números inteiros e com anéis e corpos, estruturas que serão utilizadas para constuir os anéis dos polinômios.

2.1 Números inteiros

Nesta seção, apresentaremos três tópicos da teoria dos números que, no último capítulo, serão generalizados para domínios de integridade.

Antes de iniciarmos, enunciaremos o segundo princípio de indução, pois, tal princípio, será utilizado em algumas demonstrações.

Segundo princípio de indução: Dado $a \in \mathbb{Z}$, suponhamos que a cada inteiro $n \geq a$ esteja associada uma afirmação $P(n)$. Então $P(n)$ é verdadeira para todo $n \geq a$ se:

(i) $P(a)$ for verdadeira;

(ii) Dado $r > a$, $r \in \mathbb{Z}$, se $P(k)$ é verdadeira para todo k, com $a \leq k < r$, então $P(r)$ é verdadeira.

A demonstração do segundo príncipio de indução pode ser encontrada na referência 1.

Definição 2.1 (Divisão euclidiana)**.** Sejam a, b dois números inteiros. Dizemos que a *divide* b (ou que a é divisor de b, ou ainda que b é múltiplo de a) e escreveremos $a \mid b$, se existe $c \in \mathbb{Z}$ tal que $b = ac$.

Quando não existir $c \in \mathbb{Z}$ que satisfaça a equação $b = ac$, então diremos que a não divide b e denotamos por $a \nmid b$.

Propriedades da divisão em $\mathbb{Z}$: Sejam $a, b, c, d \in \mathbb{Z}$ e com os divisores diferentes de zero. Temos que:

(i) $a \mid a$
Demonstração: $a = 1 \cdot a$, então $a \mid a$.

(ii) Se $a \mid b$ e $b \mid c$ então $a \mid c$
Demonstração: Se $a \mid b$, então existe $t \in \mathbb{Z}$ tal que $b = ta$, e se $b \mid c$, então existe $r \in \mathbb{Z}$ tal que $c = rb$, logo $c = r(ta) = (rt)a$, portanto $a \mid c$.

(iii) Se $a \mid b$ e $c \mid d$ então $ac \mid bd$
Demonstração: Se $a \mid b$, então existe $t \in \mathbb{Z}$ tal que $b = ta$ e $c \mid d$ então existe $r \in \mathbb{Z}$ tal que $d = rc$. Assim, $bd = (ta)(rc) = (tr)(ac)$. Portanto $ac \mid bd$.

(iv) Se $a \mid b$ e $a \mid c$ então $a \mid (b + c)$
Demonstração: Se $a \mid b$, então existe $t \in \mathbb{Z}$ tal que $b = ta$, e $a \mid c$ então existe $r \in \mathbb{Z}$ tal que $c = ra$. Assim, $b + c = ta + ra = (t + r)a$. Portanto, $a \mid (b + c)$.

(v) Se $a \mid b$ então, para todo $m \in \mathbb{Z}$, temos que $a \mid mb$
Demonstração: Se $a \mid b$, então existe $t \in \mathbb{Z}$ tal que $b = ta$. Se $b = ta$ então $mb = m(ta) = (mt)a$ para todo m inteiro. Portanto $a \mid mb$.

(vi) Se $a \mid b$ e $a \mid c$ então, para todo $m, n \in \mathbb{Z}$, $a \mid (mb + nc)$
Demonstração: Se $a \mid b$, por (v), $a \mid mb$, o mesmo ocorre se $a \mid c$, então $a \mid nc$. Se $a \mid mb$ e $a \mid nc$ então, por (iv), $a \mid (mb + nc)$.

Na demonstração do teorema 2.1 utilizaremos o *princípio da boa ordem*. Abaixo, este princípio será enunciado.

Princípio da boa ordem: Todo conjunto não vazio de inteiros não negativos contém um elemento mínimo.

Teorema 2.1 (Algoritmo euclidiano)**.** *Sejam a, b dois números inteiros, com $b \neq 0$, então existem inteiros q, r únicos tais que $a = bq + r$ em que $0 \leq r <\mid b \mid$.*

Demonstração.

Existência

Para mostrarmos a existência dos inteiros q, r dividiremos a demonstração em alguns casos:

(i) Considerando $a \geq 0$ e $b > 0$. Vamos tomar o conjunto $S = \{a - bx \mid x \in \mathbb{Z}, \text{ com } a - bx \geq 0\}$. Quando $x = 0$ temos que $a - bx = a \geq 0$, então a é um um elemento de S, e portanto, $S \neq \varnothing$. Sabemos que existe $r \in S$ tal que $r = minS$, pelo *princípio da boa ordem*. Se r é elemento de S, então r pode ser escrito como $r = a - bq \geq 0$ para algum q inteiro, logo $a = bq + r$.

Por outro lado, se $r \geq b$, poderíamos tomar:

$$a - b(q + 1) = a - bq - b = r - b \geq 0$$

e isso significaria que $a - b(q + 1)$ é um elemento de S. Mas $r - b < r = minS$, pois $b > 0$, uma contradição. Portanto, concluímos que $r < b$. Assim, existem q, r que satisfazem o teorema.

(ii) Considerando $a < 0$ e $b > 0$. Pelo item anterior, podemos escrever:

$$\mid a \mid = bq' + r' \text{ tais que } 0 \leq r' < b$$

Se $r' = 0$ então $- \mid a \mid = a = b(-q') + 0$, portanto existem q', r' que satisfazem o teorema. Se $r' > 0$ temos que:

$$a = - \mid a \mid = b(-q') - r' = b(-q') + b - b - r = b(-q' - 1) + (b - r')$$

Sabemos que $0 < b - r' < b$. Então, podemos tomar $q = -q' - 1$ e $r = b - r'$. E assim, q e r satisfazem o teorema.

(iii) Considerando $b < 0$ e a é qualquer. Pelos itens anteriores, podemos obter:

$$a = \mid b \mid q' + r, \text{ em que } 0 \leq r < \mid b \mid$$

Se $b < 0$ então $\mid b \mid = -b$, logo

$$a = \mid b \mid q' + r = (-b)q' + r = b(-q') + r$$

Então, os inteiros $q = -q'$ e r satisfazem o teorema.

Unicidade

Para provarmos a unicidade de q, r vamos dividir a demonstração em dois casos:

(i) Se $b > 0$, suponha que existam dois pares (q_1, r_1) e (q_2, r_2) que satisfaçam a equação $a = bq + r$, em que $0 \leq r_1 < b$ e $0 \leq r_2 < b$. Então temos :

$$\begin{aligned} a = bq_1 + r_1 \text{ e } a = bq_2 + r_2, \\ \Rightarrow bq_1 + r_1 = bq_2 + r_2 \\ \Rightarrow bq_1 - bq_2 = r_2 - r_1 \\ \Rightarrow b(q_1 - q_2) = r_2 - r_1 \\ \Rightarrow b \mid (r_1 - r_2) \end{aligned}$$

Como $0 \leq r_1 < b$ e $0 \leq r_2 < b$ então $-b < -r_1 \leq 0$ logo $-b < r_2 - r_1 < b$ e portanto $\mid r_2 - r_1 \mid < b$. Assim, como $b \mid (r_2 - r_1)$ e $\mid r_2 - r_1 \mid < b$ concluímos que $r_2 - r_1 = 0$ então $r_2 = r_1$. E ainda $q_1 - q_2 = 0$ logo $q_1 = q_2$,já que $b \neq 0$ e $r_2 - r_1 = 0$.

(ii) Se $b < 0$, então $\mid b \mid > 0$ portanto, por (i), existem únicos inteiros q', r tais que $a = \mid b \mid q' + r$, em que $0 \leq r < \mid b \mid$. E por $\mid b \mid$ ser igual a $-b$ e $q = -q'$ ser único, obtemos que $a = (-b)q' + r = b(-q') + r$ então $a = bq + r$, com $0 \leq r < \mid b \mid$.

□

Exemplos

1) $3 \mid 6$, pois existe o inteiro 2 tal que $2 \cdot 3 = 6$.

2) Sejam os inteiros 23 e 5. Segundo o algoritmo euclidiano, $23 = 4 \cdot 5 + 3$, em que $0 \leq 3 < \mid 5 \mid$.

Definição 2.2 (Mdc entre números inteiros)**.** Chamamos de *máximo divisor comum*, e escrevemos *mdc*, o maior divisor comum de dois números inteiros, isto é, $mdc(a, b) = max\{d : d \mid a, d \mid b\}$.

Observação: Se d é o máximo divisor comum de a e b, então d também é o máximo divisor comum de a e $-b$, de $-a$ e b e de $-a$ e $-b$.

Teorema 2.2 (Existência do mdc)**.** *Quaisquer que sejam a, b inteiros, existe $d \in \mathbb{Z}$ tal que d é o máximo divisor comum de a e b.*

Demonstração. Considerando $a > 0$ e $b > 0$, vamos tomar o conjunto $L = \{ax + by \mid x, y \in \mathbb{Z}\}$. Se, por exemplo, fizermos $x = y = 1$ então $a + b$ pertence à L e, portanto, existem elementos positivos em L. Seja d o menor dos elementos positivos. Vamos mostrar que d é o máximo divisor comum de a e b.

(i) d é maior que zero.

(ii) Como d pertence à L, então podemos escrever $d = ax_0 + by_0$. Aplicando o algoritmo da divisão, temos que

$$a = dq + r, \text{ com } 0 \leq r < d$$

e daí

$$a = (ax_0 + by_0)q + r \text{ ou ainda, } r = a(1 - qx_0) + b(-y_0)q$$

Logo, $r \in L$. Como r é maior ou igual a zero e $d = ax_0 + by_0$, o menor elemento positivo de L, então $r = 0$,o que implica que $a = dq$ e, portanto, $d \mid a$. Analogamente podemos provar que $d \mid b$.

(iii) Se $d' \mid a$ e $d' \mid b$ então $a = x_1 d'$, para algum, $x_1 \in \mathbb{Z}$ e $b = y_1 d'$, para algum $y_1 \in \mathbb{Z}$. Como $d = ax_0 + by_0$, então $d = (x_1 d')x_0 + (y_1 d')y_0 = (x_1 x_0)d' + (y_1 y_0)d' = d'(x_1 x_0 + y_1 y_0) = d$. Portanto $d' \mid d$.

□

Exemplo: O conjunto dos divisores de 12 e 36 é $\{1, 2, 3, 4, 6, 12\}$. O elemento máximo deste conjunto é o 12. Portanto o $mdc(12, 36) = 12$.

Definição 2.3 (Número primo)**.** Um número p é *primo* se tem exatamente dois divisores positivos, 1 e $\mid p \mid$.

Isto significa que somente 1 e $\mid p \mid$ dividem p.

Teorema 2.3 (Teorema fundamental da aritmérica)**.** *Dado um número inteiro $a > 1$, existem r números inteiros, primos positivos $p_1 p_2 ... p_r$, de maneira que $a = p_1 p_2 ... p_r (r \geq 1)$. Além disso, se tivermos também $a = q_1 q_2 ... q_s$, em que os q_j são primos positivos, então $r = s$ e cada p_i é igual a um dos q_j.*

Em outras palavras, *todo número natural maior do que 1 ou é primo ou pode ser escrito de modo único (a menos da ordem dos fatores) como um produto de números primos.*

Demonstração.
Vamos mostrar a existência e a unicidade de $p_1 p_2 ... p_r$:

(i) Vamos utilizar o segundo princípio de indução. Se $a = 2$, então a afirmação é válida pois 2 é primo.

Suponhamos o teorema válido para todo b inteiro tal que $2 \leq b < a$. Sabemos que existe um número primo $p_1 > 0$ que divide a, então $a = p_1 a_1$. Se $a_1 = 1$ ou a_1 é

primo, então a é primo. Caso contrário, como $2 \leq a_1 < a$, a hipótese de indução nos garante que $a_1 = p_2...p_r (r-1 \geq 1)$, em que os p_i são estritamente positivos e primos, logo $a = p_1...p_r$.

(ii) Se $p_1...p_r = q_1...q_s$, então $p_1 \mid (q_1...q_s)$, portanto $p_1 \mid q_j (1 \leq j \leq s)$.

Suponhamos $j = 1$. Então $p_1 \mid q_1$ e daí $p_1 = q_1$ uma vez que q_1 é primo e $p_1 > 0$. Cancelando p_1 e q_1 na igualdade inicial e prosseguindo com o raciocínio desenvolvido até aqui, chega-se à unicidade da decomposição.

□

Exemplo: O elemento 28 de $\mathbb{Z}$ pode ser escrito como

$$28 = 2 \cdot 2 \cdot 7 = 7 \cdot 2 \cdot 2 = 2 \cdot 7 \cdot 2$$

em que 2 e 7 são inteiros primos positivos.

2.2 Anéis e Corpos

Definição 2.4 (Anel)**.** Um sistema matemático constituído de um conjunto $\mathbb{A}$ não vazio e duas operações sobre ele, uma adição e uma multiplicação definidas, respectivamente, por:

$$+ : (x, y) \mapsto x + y$$
$$\cdot : (x, y) \mapsto xy$$

é chamado *anel*, e representado por $(\mathbb{A}, +, \cdot)$, ou simplesmente $\mathbb{A}$, se essas operações atendem as seguintes condições, $\forall a, b, c \in \mathbb{A}$:

(i) A adição em $\mathbb{A}$ é associativa, isto é, $(a + b) + c = a + (b + c)$;

(ii) A adição em $\mathbb{A}$ é comutativa, ou seja, $a + b = b + a$;

(iii) Existe elemento neutro para a adição em A, portanto $\exists 0_{\mathbb{A}} \in \mathbb{A} \mid a + 0_{\mathbb{A}} = a, \forall a \in \mathbb{A}$;

(iv) Existem os simétricos aditivos em $\mathbb{A}$, logo $\forall a \in \mathbb{A}, \exists a' \in \mathbb{A} \mid a + a' = 0_{\mathbb{A}}$;

(v) A multiplicação em $\mathbb{A}$ é associativa, ou seja, $a(bc) = (ab)c$;

(vi) A multiplicação em $\mathbb{A}$ é distributiva (à direita e à esquerda) em relação à adição, então $a(b + c) = ab + ac$ e $(a + b)c = ac + bc$.

Observações:

1) O elemento $0_{\mathbb{A}}$ é chamado *zero* do anel $\mathbb{A}$.

2) Por vezes, ocultaremos o sinal de multiplicação "$\cdot$". Escreveremos ab quando quisermos dizer $a \cdot b$.

Exemplos:

(1) $(\mathbb{R}, +, \cdot)$ é um anel pois, a adicão usual em $\mathbb{R}$ é associativa, comutativa, possui elemento neutro e conta com os simétricos de seus elementos. Além disso, a multiplicação usual em $\mathbb{R}$ é associativa e é distributiva em relação à adição.

(2) $(\mathbb{Z}_m, +, \cdot) = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, ..., \overline{m-1}\}$ é um anel com as operações:

$$\overline{a} + \overline{b} = \overline{a+b} \text{ e}$$
$$\overline{a} \cdot \overline{b} = \overline{a \cdot b}, \forall \overline{a}, \overline{b} \in \mathbb{Z}_m$$

pois,

(i) $\overline{a} + (\overline{b} + \overline{c}) = \overline{a} + (\overline{b+c}) = \overline{a + (b+c)} = \overline{(a+b)+c}$, já que a adição em $\mathbb{Z}$ é associativa. Então, $\overline{(a+b)+c} = (\overline{a+b}) + \overline{c} = (\overline{a} + \overline{b}) + \overline{c}, \forall \overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_m$.

(ii) $\overline{a} + \overline{b} = \overline{a+b} = \overline{b+a}$ já que em $\mathbb{Z}$ vale a comutatividade da adição. Logo, $\overline{b+a} = \overline{b} + \overline{a}, \forall \overline{a}, \overline{b} \in \mathbb{Z}_m$.

(iii) $\exists\ \overline{0} \in \mathbb{Z}_m \mid \overline{0} + \overline{a} = \overline{a}, \forall \overline{a} \in \mathbb{Z}_m$. De fato, pois $\overline{0} + \overline{a} = \overline{0+a} = \overline{a}$, e isso ocorre porque 0 e a são elementos de $\mathbb{Z}$, e em $\mathbb{Z}$ o elemento 0 é neutro para a adição. Portanto $\overline{0}$ é o elemento neutro da adição em $\mathbb{Z}_m$.

(iv) $\exists\ \overline{a'} \in \mathbb{Z}_m \mid \overline{a} + \overline{a'} = \overline{0}, \forall \overline{a} \in \mathbb{Z}_m$. De fato, $\overline{a} + \overline{a'} = \overline{0} \Rightarrow \overline{a+a'} = \overline{0} \Rightarrow a + a' \equiv 0 (mod\ m)$, isso quer dizer que $m \mid (a + a') - 0 \Rightarrow a + a' = qm$ para algum $q \in \mathbb{Z}$. Logo, $a' = qm - a$, então $\overline{a'} = \overline{qm - a} \Rightarrow \overline{a'} = \overline{qm} + \overline{(-a)}$, mas $\overline{qm} = \overline{m}$, portanto, $\overline{a'} = \overline{m - a}$ é o simétrico aditivo de $\overline{a}, \forall \overline{a} \in \mathbb{Z}_m$.

(v) $\overline{a} \cdot (\overline{b} \cdot \overline{c}) = \overline{a} \cdot (\overline{b \cdot c}) = \overline{a \cdot (b \cdot c)} = \overline{(a \cdot b) \cdot c}$, já que a multiplicação em $\mathbb{Z}$ é comutativa. Então $\overline{(a \cdot b) \cdot c} = (\overline{a \cdot b}) \cdot \overline{c} = (\overline{a} \cdot \overline{b}) \cdot \overline{c}, \forall \overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_m$.

(vi) $\overline{a} \cdot (\overline{b} + \overline{c}) = \overline{a} \cdot \overline{(b+c)} = \overline{a \cdot (b+c)} = \overline{ab + ac} = \overline{ab} + \overline{ac} = \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c}$. Perceba que usamos a distributividade de $\mathbb{Z}$ para mostrarmos a distributividade da multiplicação em relação à adição de $\mathbb{Z}_m$.

Definição 2.5 (Subtração em um anel)**.** Sejam a e b dois elementos de um anel $\mathbb{A}$. A *subtração* entre esses dois elementos é dada por:

$$a - b = a + (-b), \forall a, b \in \mathbb{A}$$

em que o elemento $-b$ é o simétrico aditivo de b.

Note que um conjunto A qualquer com a operação de *subtração* e uma multiplicação **não** é um anel, pois, por exemplo, a subtração não é comutativa:

$$7 - 4 = 3 \text{ e } 4 - 7 = -3 \text{ e } 3 \neq -3$$

Definição 2.6 (Potência em um anel)**.** Seja a um elemento de um anel $\mathbb{A}$ e $n \in \mathbb{N}^*$, define-se:

$$a^1 = a \text{ e } a^n = a^{n-1} \cdot a, \forall n > 1$$

A definição acima será bastante utilizada ao trabalharmos com anéis de polinômios.

Propriedades de um anel: Seja o anel $(\mathbb{A}, +, \cdot)$. As seguintes afirmações são verdadeiras:

a) em relação à adição:

(i) o elemento neutro é único;
Demonstração: Suponha que existam dois elementos neutros e_1 e e_2. Se e_1 é neutro, então $e_1 + e_2 = e_2$ e se e_2 é neutro, então $e_1 + e_2 = e_1$. Portanto $e_1 = e_2$.

(ii) o simétrico aditivo de cada elemento é único;
Demonstração: Suponha que existam dois simétricos aditivos x' e x'' para o elemento x. Então $x' = 0 + x' = (x'' + x) + x' = x'' + (x + x') = x'' + 0 = x''$.

(iii) dados $a_1, a_2, a_3, ..., a_n \in \mathbb{A} (n \geq 2)$, $-(a_1 + a_2 + a_3 + ... + a_n) = (-a_1) + (-a_2) + (-a_3) + ... + (-a_n)$;
Demonstração: $(a_1 + a_2 + a_3... + a_n) + ((-a_1) + (-a_2) + (-a_3)... + (-a_n)) = (a_1 + (-a_1)) + (a_2 + (-a_2)) + (a_3 + (-a_3)) + ... + (a_n + (-a_n)) = 0 + 0 + 0 + ... + 0 = 0$. Portanto $(-a_1) + (-a_2) + (-a_3) + ... + (-a_n)$ é o simétrico aditivo de $(a_1 + a_2 + a_3 + ... + a_n)$. Observe que na primeira passagem utilizamos a associatividade e a comutatividade do anel $\mathbb{A}$.

(iv) $(-(-a)) = a$, $\forall a \in \mathbb{A}$;
Demonstração: $-a$ é o simétrico aditivo de a, então $a + (-a) = 0$, portanto a é o simétrico aditivo de $-a$, logo $a = (-(-a))$.

(v) $a \in \mathbb{A}$ é *elemento regular* para a adição em $\mathbb{A}$ (ou vale a lei do cancelamento para a adição em $\mathbb{A}$): $a + x = a + y \Rightarrow x = y$;
Demonstração: Se $a + x = a + y$, temos que $(-a) + (a + x) = -a + (a + y)$. Assim $((-a) + a) + x = ((-a) + a) + y$ então $0 + x = 0 + y$ portanto $x = y$.

b) relação à multiplicação:

(i) $a0 = 0a = 0, \forall a \in \mathbb{A}$;
Justificação: $0 + a0 = a0 = a(0 + 0) = a0 + a0$ então $0 + a0 = a0 + a0$ portanto $0 = a0$ (por (v)).
A justificação é análoga para $0a = 0$.

(ii) $a(-b) = (-a)b = -(ab), \forall a, b \in \mathbb{A}$;
Justificação: $ab + (-(ab)) = 0 = a0 = a(b + (-b)) = ab + a(-b)$ então $ab + (-(ab)) = ab + a(-b)$ portanto $-(ab) = a(-b)$ (por (v)).
A justificação é análoga para $-(ab) = (-a)b$.

(iii) $ab = (-a)(-b), \forall a, b \in \mathbb{A}$;
Justificação: $(-a)(-b) = (-(-a)b)$ e $(-(-a)b) = -(-(ab))$ (por (ii)). Além disso, o simétrico aditivo de $-(ab)$ é o próprio ab. Portanto, $(-a)(-b) = ab$.

(iv) $a(b - c) = ab - ac, \forall a, b, c \in \mathbb{A}$;
Justificação: $a(b-c) = a(b+(-c)) = ab+a(-c) = ab+(-(ac)) = ab-ac$. Note que a conclusão foi dada pela definição 2.5.

(v) $a^m \cdot a^n = a^{m+n}, \forall a \in \mathbb{A}$ e $\forall m, n \in \mathbb{N}^*$;
Justificação (por indução sobre n): Para $n = 1$ é válido pois $a^m a^1 = a^m a = a^{m+1}$ pela definição 2.6. Agora, suponha $a^m a^r = a^{m+r}$, então $a^m a^{r+1} = a^m(a^r a^1) = (a^m a^r)a^1 = a^{m+r}a = a^{(m+r)+1} = a^{m+(r+1)}$.

(vi) $(a^m)^n = a^{mn}, \forall a \in \mathbb{A}$ e $\forall m, n \in \mathbb{N}^*$.
Justificação (por indução sobre n): Para $n = 1$ é válido pois $(a^m)^1 = a^m$ por definição. Agora, suponha $(a^m)^r = a^{mr}$, então $(a^m)^{r+1} = (a^m)^r a^m = a^{mr}a^m = a^{mr+m} = a^{m(r+1)}$.

Definição 2.7 (Subanel)**.** Sejam $(\mathbb{A}, +, \cdot)$ um anel e L um subconjunto não vazio de $\mathbb{A}$. L é um *subanel* de $\mathbb{A}$ se $(L, +, \cdot)$ é um anel.

Proposição 2.1. Seja $\mathbb{A}$ um anel, $L \subset \mathbb{A}$ e $L \neq \varnothing$. L é um subanel de $\mathbb{A}$ se, e somente se $a - b, ab \in L$ sempre que $a, b \in L$.

Demonstração.
($\Rightarrow$)
Hipótese: L é um subanel de $\mathbb{A}$.
Tese: $a - b, ab \in L, \forall a, b \in L$.

Se L é um subanel de $\mathbb{A}$, então, pela definição 2.7, L é um anel e L é fechado para as operações de $\mathbb{A}$, ou seja, a soma $a + b$ está em L e a multiplicação ab também está em L, para todo elemento a, b de L.

Seja b um elemento de L então o seu simétrico aditivo, $-b$, também está em L, pois L é um anel. Sendo assim, se a e $-b$ pertencem a L, podemos tomar $a + (-b) = a - b$, e como sabemos que em L a adição é fechada, logo $a - b$ pertence a L.

Logo, $a - b, ab \in L$.

($\Leftarrow$)
Hipótese: $a - b, ab \in L, \forall a, b \in L$.

Tese: $\mathbb{L}$ é um subanel de $\mathbb{A}$.

Por hipótese, podemos concluir que L é fechado para a multiplicação, pois se a, b são elementos de L então a multiplicação ab também está em L. Sabemos que a adição em L é associativa e comutativa e a multiplicação em L é associativa e distributiva em relação à adição, já que os elementos de L são elementos de A, pois $L \subset \mathbb{A}$, então, essas propriedades são herdadas do anel $\mathbb{A}$. Então, basta mostrar que $0_{\mathbb{A}} \in L$ e que os simétricos dos elementos de L também estão em L.

Temos que $a, b \in L \Rightarrow a - b \in L$, por hipótese. Se $a = b$, então $a - a = a + (-a) = 0_{\mathbb{A}} \in L$. Sabendo que $0_{\mathbb{A}} \in L$ e $a - b \in L, \forall a, b \in L$, se tomarmos $a = 0_{\mathbb{A}}$, então $-b \in L$, já que $0_{\mathbb{A}}$ é o elemento neutro da adição.

Se $-b \in L$, então $a - (-b) = a + b \in L$. Então a adição é fechada em L. Concluímos, então que L é um anel.

Logo, L é um subanel de $\mathbb{A}$. □

Exemplos:

1) $(\mathbb{R}, +, \cdot)$ é um anel. Vamos mostrar que $L = \{a + b\sqrt{2} \ | a, b \in \mathbb{Z}\}$ é um subanel de $(\mathbb{R}, +, \cdot)$.

   Usando a proposição 2.1 temos que se $a - b \in L$ e $ab \in L, \forall a, b \in L$, então L é um subanel de $(\mathbb{R}, +, \cdot)$, então vamos tomar $(a + b\sqrt{2}), (c + d\sqrt{2}) \in L$.

   (i) $(a + b\sqrt{2}) - (c + d\sqrt{2}) = a + b\sqrt{2} - c - d\sqrt{2} = [(a - c) + (b - d)\sqrt{2}] \in L$, pois $a, b, c, d \in \mathbb{R}$. Então L é fechado para a *subtração*.

   (ii) $(a + b\sqrt{2}) \cdot (c + d\sqrt{2}) = ac + ad\sqrt{2} + bc\sqrt{2} + 2bd = [(ac + 2bd) + (ad + bc)\sqrt{2}] \in L$, pois $a, b, c, d \in \mathbb{R}$. Logo, L é fechado para a operação de multiplicação.

   Portanto, $(L, +, \cdot)$ é um subanel de $(\mathbb{R}, +, \cdot)$.

2) Vamos mostrar que o conjunto $L = \left\{ \begin{pmatrix} 0 & a \\ b & c \end{pmatrix} | a, b, c \in \mathbb{R} \right\}$ não é um subanel de $(M_2(\mathbb{R}), +, \cdot)$.

   Vamos tomar $\begin{pmatrix} 0 & a \\ b & c \end{pmatrix}, \begin{pmatrix} 0 & e \\ f & g \end{pmatrix} \in L$.

   L é fechado para a *subtração*,

$$\begin{pmatrix} 0 & a \\ b & c \end{pmatrix} - \begin{pmatrix} 0 & e \\ f & g \end{pmatrix} = \begin{pmatrix} 0 & a - e \\ b - f & c - g \end{pmatrix} \in L$$

   Mas L não é fechado para a multiplicação,

$$\begin{pmatrix} 0 & a \\ b & c \end{pmatrix} \cdot \begin{pmatrix} 0 & e \\ f & g \end{pmatrix} = \begin{pmatrix} af & ag \\ cf & be + cg \end{pmatrix}$$

somente pertence a L quando $a = 0$ ou $f = 0$. Portanto, L não é um subanel de $(M_2(\mathbb{R}), +, \cdot)$.

Definição 2.8 (Homomorfismo de anéis)**.** Sejam $(\mathbb{A}, +, \cdot)$ e $(\mathbb{B}, \oplus, \odot)$ dois anéis quaisquer. A função $f : \mathbb{A} \to \mathbb{B}$ é um *homomorfismo* se:

(i) $f(x + y) = f(x) \oplus f(y)$, $\forall x, y \in \mathbb{A}$;

(ii) $f(x \cdot y) = f(x) \odot f(y)$, $\forall x, y \in \mathbb{A}$.

Definição 2.9 (Isomorfismo de anéis)**.** Sejam $(\mathbb{A}, +, \cdot)$ e $(\mathbb{B}, \oplus, \odot)$ dois anéis quaisquer. A função $f : \mathbb{A} \to \mathbb{B}$ é um *isomorfismo* se f é um homomorfismo e f é bijetora.

Se a função $f : \mathbb{A} \to \mathbb{B}$ é um isomorfismo de $\mathbb{A}$ em $\mathbb{B}$ dizemos que $\mathbb{A}$ e $\mathbb{B}$ são *isomorfos*.

Exemplo: Sejam os anéis $\mathbb{A}$, com as operações usuais de adição e multiplicação, e $\mathbb{A} \times \{0\}$ com as operações de adição e multiplicação definidas a seguir:

$$(x, 0) + (y, 0) = (x + y, 0)$$
$$(x, 0) \cdot (y, 0) = (xy, 0), \forall (x, 0), (y, 0) \in \mathbb{A} \times \{0\}$$

Vamos mostrar que a função $f : \mathbb{A} \to \mathbb{A} \times \{0\}$, definida por $f(x) = (x, 0)$, é um isomorfismo de $\mathbb{A}$ em $\mathbb{A} \times \{0\}$.

(i) f é injetora, pois dados $x, y \in \mathbb{A}$ tais que $f(x) = f(y)$ temos que $(x, 0) = (y, 0)$ portanto $x = y$;

(ii) f é sobrejetora, pois $\forall (y, 0) \in \mathbb{A} \times \{0\}, \exists y \in \mathbb{A} \mid f(y) = (y, 0)$;

Portanto, f é bijetora.

(iii) $f(x + y) = (x + y, 0) = (x, 0) + (y, 0) = f(x) + f(y), \forall x, y \in \mathbb{A}$;

(iv) $f(xy) = (xy, 0) = (x, 0) \cdot (y, 0) = f(x)f(y), \forall x, y \in \mathbb{A}$.

Assim, f é um isomorfismo de $\mathbb{A}$ em $\mathbb{A} \times \{0\}$.

Definição 2.10 (Anel comutativo)**.** Seja $\mathbb{A}$ um anel. Se a multiplicação em $\mathbb{A}$ é comutativa, ou seja, se $\forall a, b \in \mathbb{A}, ab = ba$ então $\mathbb{A}$ é um anel comutativo.

Definição 2.11 (Anel com unidade)**.** Seja $\mathbb{A}$ um anel. Se $\mathbb{A}$ conta com o elemento neutro da multiplicação, isto é, se existir $1_{\mathbb{A}} \in \mathbb{A}, 1_{\mathbb{A}} \neq 0_{\mathbb{A}}$ tal que $1_{\mathbb{A}} \cdot a = a \cdot 1_{\mathbb{A}} = a, \forall a \in \mathbb{A}$, então $\mathbb{A}$ é um anel com unidade.

Se $\mathbb{A}$ atender as definições 2.10 e 2.11, então $\mathbb{A}$ é um anel comutativo com unidade.

Exemplo: Vamos mostrar que $(\mathbb{Q}, \oplus, \odot)$ é um anel comutativo com unidade, com adição e multiplicação abaixo definidas:

$$x \oplus y = x + y - 3$$
$$x \odot y = x + y - \tfrac{xy}{3}$$

Antes de mostrar que a multiplicação é comutativa e tem elemento neutro, vamos mostrar que $(\mathbb{Q}, \oplus, \odot)$ é um anel.

(i) A adição em $(\mathbb{Q}, \oplus, \odot)$ é associativa pois, $x \oplus (y \oplus z) = x \oplus (y + z - 3) = x + (y + z - 3) - 3 = (x + y - 3) + z - 3 = (x + y - 3) \oplus z = (x \oplus y) \oplus z$, já que x, y e z são elementos de $\mathbb{Q}$.

(ii) A adição é comutativa em $(\mathbb{Q}, \oplus, \odot)$ pois, $x \oplus y = x + y - 3 = y + x - 3 = y \oplus x$, já que x e y são elementos de $\mathbb{Q}$.

(iii) A adição possui elemento neutro: $\exists\ e \in (\mathbb{Q}, \oplus, \odot) \mid x \oplus e = x$. De fato, para que $x \oplus e$ seja igual a x, então $x + e - 3 = x$, portanto $e = 3$ é o elemento neutro da adição.

(iv) Existem os simétricos aditivos: $\exists\ x' \in (\mathbb{Q}, \oplus, \odot) \mid x \oplus x' = 3$. De fato, para que $x \oplus x'$ seja igual 3 então $x + x' - 3 = 3$, portanto $x' = 6 - x$ é o simétrico aditivo de x.

(v) A multiplicação é associativa em $(\mathbb{Q}, \oplus, \odot)$ pois, $x \odot (y \odot z) = x \odot (y + z - \frac{yz}{3}) = x + (y + z - \frac{yz}{3}) - \frac{x(y+z-\frac{yz}{3})}{3} = x + y + z - \frac{yz}{3} - \frac{xy}{3} - \frac{xz}{3} + \frac{xyz}{9}$ e $(x \odot y) \odot z = (x + y - \frac{xy}{3}) \odot z = (x + y - \frac{xy}{3}) + z - \frac{(x+y-\frac{xy}{3})z}{3} = x + y + z - \frac{yz}{3} - \frac{xy}{3} - \frac{xz}{3} + \frac{xyz}{9}$, já que x, y e z são elementos de $\mathbb{Q}$. Portanto $x \odot (y \odot z) = (x \odot y) \odot z$.

(vi) A multiplicação é distributiva pois, $x \odot (y \oplus z) = x \odot (y + z - 3) = x + (y + z - 3) - \frac{x(y+z-3)}{3} = 2x + y + z - 3 - \frac{xy}{3} - \frac{xz}{3}$ e $(x \odot y) \oplus (x \odot z) = (x + y - \frac{xy}{3}) \oplus (x + z - \frac{xz}{3}) = (x + y - \frac{xy}{3}) + (x + z - \frac{xz}{3}) - 3 = 2x + y + z - 3 - \frac{xy}{3} - \frac{xz}{3}$, já que x, y e z são elementos de $\mathbb{Q}$. Portanto $x \odot (y \oplus z) = (x \odot y) \oplus (x \odot z)$.

A demonstração é análoga para a distributividade à direita.

Agora vamos mostrar a comutatividade da multiplicação.

Em $\mathbb{Q}$, sabemos que a adição e a multiplicação são comutativas então,

$$x \odot y = x + y + \frac{xy}{3} = y + x + \frac{yx}{3} = y \odot x$$

Portanto, $(\mathbb{Q}, \oplus, \odot)$ é um anel comutativo.

Para que exista o elemento neutro da operação $\odot$, deve ocorrer:

$$x \odot e = x + e + \frac{xe}{3} = x$$

Isso acontece se, e somente se $e = 0$.

Dessa forma, $e = 0$ é o elemento neutro da operação $\odot$.

Portanto, $(\mathbb{Q}, \oplus, \odot)$ é um anel comutativo com unidade.

Definição 2.12 (Domínio de integridade)**.** Seja $\mathbb{A}$ um anel comutativo com unidade. $\mathbb{A}$ será um *anel de integridade* ou um *domínio de integridade* se $\mathbb{A}$ não possuir *divisores de zero*, ou seja,

$$ab = 0 \Leftrightarrow a = 0 \text{ ou } b = 0, \forall a, b \in \mathbb{A}$$

Exemplo: O anel $\mathbb{Z}_9$ com suas operações usuais possui divisores de zero:

$$\overline{3} \cdot \overline{3} = \overline{9} = \overline{0}, \text{ mas } \overline{3} \neq \overline{0}$$

Proposição 2.2. Um anel $\mathbb{A}$ comutativo com unidade é um domínio de integridade se, e somente se vale a lei do cancelamento para a multiplicação, ou seja,

$$ab = ac \Leftrightarrow b = c, \forall a, b, c \in \mathbb{A}, \text{ com } a \neq 0$$

Observação: Neste caso, a será um *elemento regular* em relação à multiplicação em $\mathbb{A}$.

Demonstração.
$(\Rightarrow)$
Hipótese: $\mathbb{A}$ é domínio de integridade.
Tese: Em $\mathbb{A}$, vale a lei do cancelamento.

Supondo $ab = ac$, somando o simétrico multiplicativo de ac de ambos os lados da equação, podemos obter $ab - ac = 0$ e daí, como a, b e c são elementos de um anel, vale a distributividade em $\mathbb{A}$, logo temos que $a(b - c) = 0$ então $b - c = 0$ já que $a \neq 0$ e $\mathbb{A}$ é um domínio de integridade, por hipótese. Logo $b = c$.

$(\Leftarrow)$
Hipótese: Em $\mathbb{A}$, vale a lei do cancelamento.
Tese: $\mathbb{A}$ é um domínio de integridade.

Queremos mostrar que se $ab = 0$ se, e somente se $a = 0$ ou $b = 0$ para todo a, b de $\mathbb{A}$.

(i) Se $a = 0$ então $a \cdot b = 0 \cdot b = (x - x) \cdot b$, para qualquer x de $\mathbb{A}$. Já que $\mathbb{A}$ é anel, então vale a distributividade, logo, teremos que $(x - x) \cdot b = xb - xb = 0$ já que um elemento adicionado com o seu simétrico aditivo é sempre igual a zero. Portanto, concluímos que se $a = 0$ então $a \cdot b = 0$. A demonstração é análoga se $b = 0$.

(ii) Temos que $a \cdot b = 0$. Vamos supor $a \neq 0$, então pelo item anterior $a \cdot 0 = 0$. Então, podemos escrever que $a \cdot b = 0 = a \cdot 0$, e como temos, por hipótese, que em $\mathbb{A}$ vale a lei do cancelamento, obtemos que $b = 0$.

□

Exemplos:

1) O anel $\mathbb{Z}$ com as operações usuais de adição e multiplicação, ou seja, $(\mathbb{Z}, +, \cdot)$, é um domínio de integridade, pois quando a multiplicação de dois elementos for igual a zero, então, necessariamente, um dos dois elementos é igual zero ou os dois o são, isto é,

$$\forall a, b \in \mathbb{Z}, ab = 0 \Leftrightarrow a = 0 \text{ ou } b = 0$$

2) Observe que os conjuntos numéricos $\mathbb{Q}$ e $\mathbb{R}$ com as operações usuais de adição e multiplicação também são denominados domínios de integridade.

3) O conjunto $\mathbb{C}$ com adição:

$$\text{se } z = a + bi, w = c + di, \text{ então}$$
$$z + w = (a + bi) + (c + di) = (a + c) + (b + d)i, \forall z, w \in \mathbb{C}$$

e com multiplicação:

$$z \cdot w = (a + bi) \cdot (c + di) = (ac - bd) + (ad + bc)i, \forall z, w \in \mathbb{C}$$

também é um domínio de integridade.

Definição 2.13 (Elementos associados)**.** Sejam dois elementos a, b de um domínio de integridade $\mathbb{D}$, a e b são *associados* quando ocorre $a \mid b$ e $b \mid a$, ou seja, existem dois elementos c, d de $\mathbb{D}$ tais que $b = ac$ e $a = bd$.

Definição 2.14 (Corpo)**.** Seja $\mathbb{K}$ um anel comutativo com unidade. Se o conjunto dos elementos de $\mathbb{K}$ que possuem simétrico multiplicativo, ou inverso, for igual a $\mathbb{K}^* = \mathbb{K} - \{0\}$, então $\mathbb{K}$ é um *corpo*.

Isto é, todo elemento x de $\mathbb{K}$ tem simétrico multiplicativo x', exceto o elemento zero (elemento neutro da adição), ou seja,

$$x \cdot x' = 1, \forall x \in \mathbb{K}^*$$

Isso quer dizer que, em um corpo $\mathbb{K}$, a adição e a multiplicação são associativas e comutativas, que a adição e a multiplicação possuem elemento neutro, que todos os elementos de $\mathbb{K}$ possuem simétricos aditivos e que todos os elementos de $\mathbb{K}^*$ possuem simétricos multiplicativos.

Observe que todo corpo é um domínio de integridade, ou seja, se tomarmos $xy = 0$ temos que concluir que ou $x = 0$ ou $y = 0$. De fato, sejam dois elementos x, y de um domínio de integridade $\mathbb{A}$, sabemos que se y pertence a um corpo, $y \neq 0$, então existe y' tal que $yy' = 1$. Assim, podemos escrever $x = xyy'$. Mas $xy = 0$ então $x = 0y' = 0$. Dessa forma, concluímos que se $y \neq 0$, então necessariamente, $x = 0$.

Note que a recíproca "todo domínio de integridade é um corpo"não é verdadeira, pois $\mathbb{Z}$ é um domínio de integridade, mas o conjunto $U(\mathbb{Z})$ dos elementos inversíveis de $\mathbb{Z}$ é apenas $\{-1, 1\}$, então $\mathbb{Z}$ não é um corpo.

Exemplos:

1) Os conjuntos numéricos $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ com as suas operações usuais são corpos, pois $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ são anéis comutativos com unidade e todos os seus elementos, exceto o zero, têm simétrico multiplicativo.

2) Em $(\mathbb{R}, +, \cdot)$ os elementos 2 e 4 são associados, isto quer dizer que $2 \mid 4$ $(2 \cdot 2 = 4)$ e $4 \mid 2$ $(4 \cdot \frac{1}{2} = 2)$.

   Observe que o elemento $\frac{1}{2}$ é simétrico multiplicativo de 2, e vice-versa. Isso quer dizer que os elementos c, d citados na definição 2.13, serão sempre os simétricos multiplicativos. Dessa forma, podemos concluir que, se D for um corpo, então todos os seus elementos podem ser associados, exceto o zero.

3) Em $\mathbb{R}[X]$, o anel dos polinômios com coeficientes e variável em $\mathbb{R}$, os polinômios $f = 1 + X$ e $g = 2 + 2X$ são associados, pois $f \mid g$ e $g \mid f$, ou seja, $1 + X = \frac{1}{2}(2 + 2X)$ e $2 + 2X = 2(1 + X)$.

Nos próximos capítulos, estudaremos este tipo de anel e algumas propriedades.

CAPÍTULO

3

POLINÔMIOS

Apresentaremos a seguir um breve estudo sobre os *polinômios*. O objetivo deste capítulo é construir o anel dos polinômios e estudar algumas de suas características.

3.1 Sequências numéricas

Definição 3.1 (Sequência de elementos de $\mathbb{A}$)**.** Seja uma aplicação $f : \mathbb{N} \to \mathbb{A}$, em que $\mathbb{N} = \{0, 1, 2, ...\}$ e $\mathbb{A}$ um anel, tal que $f(i) = a_i$. Chamamos de *sequência de elementos de* $\mathbb{A}$ a representação $f = (a_0, a_1, ..., a_i, ...)$. A sequência f também pode ser denotada por (a_i).

Definição 3.2 (Igualdade de sequências)**.** Duas sequências $f = (a_i)$ e $g = (b_i)$ de um anel $\mathbb{A}$ são iguais se, e somente se $a_i = b_i, \forall i \in \mathbb{N}$, já que f e g são aplicações de $\mathbb{N}$ em $\mathbb{A}$.

Definição 3.3 (Adição de sequências)**.** Sejam $f = (a_i)$ e $g = (b_i)$ duas sequências de um anel $\mathbb{A}$. A adição $f + g$ é definida por:

$$f + g = (a_i + b_i) = (a_1 + b_1, a_2 + b_2, ...), \forall i \in \mathbb{N}$$

Exemplo: Sejam $f = (a_i)$, em que $a_i = 2i, \forall i \in \mathbb{N}$ e $g = (b_i)$, em que $b_i = i + 1, \forall i \in \mathbb{N}$ duas sequências de elementos de $\mathbb{R}$. Vamos escrever $h = (c_i)$, em que $c_i = a_i + b_i$.

$c_i = a_i + b_i \Rightarrow c_i = 2i + (i+1) = 3i + 1, \forall i \in \mathbb{N}$. Assim, $f + g = (1, 4, 7, ...)$.

Definição 3.4 (Multiplicação de sequências)**.** Sejam $f = (a_i)$ e $g = (b_i)$ duas sequências de um anel $\mathbb{A}$. A multiplicação $f \cdot g = h = (c_k)$ é definida por:
$c_0 = a_0 b_0$
$c_1 = a_0 b_1 + a_1 b_0$
$c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0$
$c_3 = a_0 b_3 + a_1 b_2 + a_2 b_1 + a_3 b_0$
e assim sucessivamente. Logo:

$$c_k = \sum_{i=0}^{k} a_i b_{k-i} \text{ para cada } k \in \mathbb{N}$$

Exemplo: Vamos encontrar os cinco primeiros temos do produto $h = c_k$ das sequências $f = (a_i)$ tal que $a_i = i$ e $g = (b_j)$ em que $b_j = 2j$ sobre $\mathbb{R}$.

Vamos calcular h da seguinte maneira: $h = c_k = \sum_{i=0}^{k} i \cdot 2(k-i)$.

Se $f = (0, 1, 2, 3, 4, 5, ...)$ e $g = (0, 2, 4, 6, 8, 10, ...)$ então $c_0 = 0 \cdot 0 = 0, c_1 = 0 \cdot 2 + 1 \cdot 0 = 0, c_2 = 0 \cdot 4 + 1 \cdot 2 + 2 \cdot 0 = 2, c_3 = 0 \cdot 6 + 1 \cdot 4 + 2 \cdot 2 + 3 \cdot 0 = 8, c_4 = 0 \cdot 8 + 1 \cdot 6 + 2 \cdot 4 + 3 \cdot 2 + 4 \cdot 0 = 20$, portanto,a sequência $h = f \cdot g = (0, 0, 2, 8, 20, ...)$.

3.2 Polinômios ou sequências quase nulas

Definição 3.5 (Sequência quase nula)**.** Uma sequência $(a_0, a_1, a_2, ...)$ sobre um anel $\mathbb{A}$ (ou seja, com $a_0, a_1, a_2, ... \in \mathbb{A}$), é uma *sequência quase nula*, se existir um índice $r \in \mathbb{N}$ tal que $a_m = 0, \forall m > r, m \in \mathbb{N}$.

Definição 3.6 (Polinômio)**.** Um *polinômio* sobre $\mathbb{A}$ é uma sequência quase nula de elementos de $\mathbb{A}$.

O polinômio $(0_{\mathbb{A}}, 0_{\mathbb{A}}, ..., 0_{\mathbb{A}}, ...)$ sobre $\mathbb{A}$ é chamado *polinômio nulo* ou *polinômio identicamente nulo*. Observe que a sequência nula ou polinômio nulo é uma sequência quase nula.

A partir da definição acima, podemos observar que uma sequência sobre um anel $\mathbb{A}$ será um polinômio sobre $\mathbb{A}$ quando tiver um número finito de termos não nulos.

Exemplos:

1) Seja o anel $\mathbb{R}$. A sequência $f = (137, -1, 18, 0, 0, 0, ...)$ é um polinômio sobre $\mathbb{R}$, pois $137, -1, 18 \in \mathbb{R}$ e além disso, a partir do 4° termo da sequência, todos os termos são iguais a zero.

2) Considere o anel $\mathbb{Z}$ x $\mathbb{Z}$. A sequência $g = ((1,1),(1,1),(1,1),...,(1,1),(1,1),...)$ não é um polinômio sobre $\mathbb{Z}$ x $\mathbb{Z}$, pois não existe um índice $r \in \mathbb{N}$ tal que $a_m = (0,0), \forall m > r, m \in \mathbb{N}$, apesar de $(1,1) \in \mathbb{Z}$ x $\mathbb{Z}$.

3) Seja o anel $M_2(\mathbb{Q})$. A sequência $g = \left(\begin{pmatrix} 2 & -3 \\ 1/2 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, ...\right)$ é um polinômio sobre $M_2(\mathbb{Q})$, pois $\begin{pmatrix} 2 & -3 \\ 1/2 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \in M_2(\mathbb{Q})$ e a partir do terceiro termo da sequência os elementos são todos nulos.

3.3 Anel de polinômios

Nesta seção, construiremos o anel dos polinômios sobre $\mathbb{A}$ e, a partir de agora, indicaremos por $\mathbb{A}[X]$ o conjunto dos polinômios sobre o anel $\mathbb{A}$.

Proposição 3.1. Se $\mathbb{A}$ é um anel então $\mathbb{A}[X]$ também é um anel.

Demonstração.
Sejam $f = (a_i), g = (b_i)$ e $h = (c_i)$, com $f, g, h \in \mathbb{A}[X]$. Como vimos na seção 3.1, a adição e a multiplicação são fechadas em $\mathbb{A}[X]$, isto é, a adição e a multiplicação são fechadas para sequências (quase nulas), além disso,

(i) a adição é associativa: $f + (g + h) = (f + g) + h, \forall f, g, h \in \mathbb{A}[X]$.

Se tomarmos $f + (g + h) = (d_i)$ e $(f + g) + h = (e_i)$, teremos que $d_i = a_i + (b_i + c_i) = (a_i + b_i) + c_i = e_i$ para todo i natural. Esta última igualdade é válida pois, temos, por hipótese, que $\mathbb{A}$ é um anel, então, seus elementos satisfazem a propriedade associativa.

(ii) a adição é comutativa: $f + g = g + f, \forall f, g \in \mathbb{A}[X]$.

Da mesma maneira do item anterior, se tomarmos $f + g = (d_i)$ e $g + f = (e_i)$ teremos que $d_i = a_i + b_i = b_i + a_i = e_i$ para todo i natural. Esta igualdade é válida pois $\mathbb{A}$ é um anel, então os seus elementos satisfazem a propriedade comutativa.

(iii) a adição possui elemento neutro: $\exists e \in \mathbb{A}[X] \mid f + e = f, \forall f \in \mathbb{A}[X]$.

Se tomarmos $f = (a_i)$ e $e = (z_i)$ então a igualdade $f + e = (a_i) + (z_i) = (a_i)$, então $z_i = 0$ para todo i natural. Se $z_i = 0$ para todo i natural, então $(z_i) = (0, 0, 0, ...)$. Portanto o *polinômio nulo* $(z_i) = 0'$ é o elemento neutro da adição em $\mathbb{A}[X]$.

(iv) todos os elementos possuem simétricos aditivos: $\forall f \in \mathbb{A}[X], \exists f' \in \mathbb{A}[X] \mid f + f' = 0'$.

Da mesma maneira do item anterior, toma-se $f = (a_i)$ e $f' = (b_i)$, assim, a soma de f e f' deve ser o polinômio nulo, logo $a_i + b_i = 0$ então $a_i = -b_i$ para todo i natural. Como a_i, b_i são elementos de um anel, então $f' = (-a_0, -a_1, -a_2, ..., -a_i, ...) = -f$ e, portanto, $-f$ é o polinômio simétrico aditivo de f em $\mathbb{A}[X]$.

(v) a multiplicação é associativa: $f(gh) = (fg)h, \forall f, g, h \in \mathbb{A}[X]$.

Se $f = (a_i), g = (b_j), h = (c_k), gh = (d_l), f(gh) = (e_m), fg = (x_n)$ e $(fg)h = y_m$, temos que:

$$e_m = \sum_{i+l=m} a_i d_l = \sum_{i+l=m} a_i(\sum_{j+k=l} b_j c_k) = \sum_{i+j+k=m} a_i(b_j c_k) = \sum_{i+j+k=m} (a_i b_j)c_k = \sum_{n+k=m} (\sum_{i+j=n} a_i b_j)c_k = \sum_{n+k=m} x_n c_k = y_m, \text{ para todo } m \text{ natural.}$$

(vi) a multiplicação é distributiva em relação à adição:$f(g + h) = fg + fh$ e $(f + g)h = fh + gh, \forall f, g, h \in \mathbb{A}[X]$.

Se $f = (a_i), g = (b_j), h = (c_j), f(g + h) = (d_k), fg = (e_k)$ e $fh = (e'_k)$, temos que:

$$d_k = \sum_{i+j=k} a_i(b_j + c_j) = \sum_{i+j=k} a_i b_j + \sum_{i+j=k} a_i c_i = e_k + e'_k \text{ para todo } k \text{ natural.}$$

Concluímos que $f(g + h) = fg + fh$. A demonstração é análoga para a distributividade à direita.

Fica provado que o conjunto dos polinômios sobre um anel $\mathbb{A}$, $\mathbb{A}[X]$, com as operações de adição e multiplicação de $\mathbb{A}$, também é um anel. □

Observação: Denotaremos o polinômio identicamente nulo por 0.

Proposição 3.2. Se $\mathbb{A}$ é um anel comutativo, então $\mathbb{A}[X]$ também é um anel comutativo.

Demonstração.
Queremos mostrar que $f \cdot g = g \cdot f, \forall f, g \in \mathbb{A}[X]$. Se tomarmos $f = (a_i), g = (b_j), fg = (c_k)$ e $gf = (d_k)$, então $c_k = \sum_{i+j=k} a_i b_j = \sum_{i+j=k} b_j a_i = d_k$ para todo k natural. □

Proposição 3.3. Se $\mathbb{A}$ é um anel com unidade, então $\mathbb{A}[X]$ também é um anel com unidade.

Demonstração.
Queremos mostrar que existe um elemento u em $\mathbb{A}[X]$ tal que $f \cdot u = f, \forall f \in \mathbb{A}[X]$. Se tomarmos $f = (a_0, a_1, ..., a_i, 0, ...)$ e $u = (1, 0, 0, ..., 0, ...,)$, vamos obter $(c_k) = ((a_0 b_0), (a_0 b_1 + a_1 b_0), (a_0 b_2 + a_1 b_1 + a_2 b_0), ..., (a_0 b_k + a_1 b_{k-1} + ... + a_i b_0)) = (a_0, a_1, a_2, ...a_i) = f$ já que todos os b_j, com $j > 0$, são iguais a zero. Portanto $f \cdot u = f$, assim u é a unidade de $\mathbb{A}[X]$.

A demonstração é análoga para mostrar que $u \cdot f = f$. □

Proposição 3.4. Se $\mathbb{A}$ é um domínio de integridade então $\mathbb{A}[X]$ também é um domínio de integridade.

Demonstração.
Sejam $f = (a_0, a_1, ..., a_m, 0, ...)$ e $g = (b_0, b_1, ..., b_n, 0, ...)$ dois polinômios não nulos de $\mathbb{A}[X]$ tais que $a_m \neq 0$, $b_n \neq 0$, $a_{m+i} = 0$ e $b_{n+i} = 0$ para todo i natural. Sendo $fg = (c_k)$, vamos calcular c_{m+n}. Assim, temos que

$$c_{m+n} = a_0 b_{m+n} + a_1 b_{m+n-1} + ... + a_m b_n + ... + a_{m+n} b_0 = a_m b_n$$

pois todos os elementos a_{m+i} e b_{n+i}, para todo i natural, são iguais a zero. Por hipótese, temos que a_m e b_n são diferentes de zero, então $a_m b_n \neq 0$ já que a_m e b_n são elementos de um domínio de integridade $\mathbb{A}$. Portanto, se $a_m b_n \neq 0$ então $fg \neq 0$.

A demonstração é análoga para provar que $gf = 0$. □

Proposição 3.5. Se $\mathbb{A}$ é um anel, então $\mathbb{L} = \{(a, 0, 0, 0, ...) \mid a \in \mathbb{A}\}$ é um subanel de $\mathbb{A}[X]$.

Demonstração.
Vamos mostrar que L é um subanel de $\mathbb{A}$ usando as condições da proposição 2.1.

(i) $\mathbb{L} \neq \varnothing$, pois $(0, 0, 0, ...) = 0_{\mathbb{A}} \in \mathbb{L}$.

(ii) Se $f = (a, 0, 0, ...)$ e $g = (b, 0, 0, ...)$, então $f - g = (a - b, 0, 0, 0, ...) \in \mathbb{L}$, já que $a - b \in \mathbb{A}$.

(iii) Se $f = (a, 0, 0, ...)$ e $g = (b, 0, 0, ...)$, então $f \cdot g = (ab, 0, 0, 0, ...) \in \mathbb{L}$, já que $ab \in \mathbb{A}$.

□

Proposição 3.6. Se $\mathbb{A}$ é um anel, $\mathbb{A}$ é isomorfo ao subanel $\mathbb{L} = \{(a, 0, 0, ...) \mid a \in \mathbb{A}\}$ de $\mathbb{A}[X]$.

Demonstração.
Seja a função $\varphi : \mathbb{A} \to \mathbb{L}$ definida por $\varphi(x) = (x, 0, 0, ...)$.

Vamos mostrar que φ é um isomorfismo:

(i) $\varphi(a + b) = (a + b, 0, 0, ...) = (a, 0, 0, ...) + (b, 0, 0, ...) = \varphi(a) + \varphi(b), \forall a, b \in \mathbb{A}$.

(ii) $\varphi(ab) = (ab, 0, 0, ...) = (a, 0, 0, ...) \cdot (b, 0, 0, ...) = \varphi(a) \cdot \varphi(b), \forall a, b \in \mathbb{A}$.

(iii) Sejam $a, b \in \mathbb{A}$ tal que $\varphi(a) = \varphi(b)$, então $(a, 0, 0, ...) = (b, 0, 0, ...)$, portanto $a = b$. Logo φ é injetora.

(iv) Seja $f = (x, 0, 0, ...) \in \mathbb{L}$, então $\exists x \in \mathbb{A} \mid \varphi(x) = f = (x, 0, 0, ...)$. Portanto φ é sobrejetora.

Assim, temos que $\mathbb{A}$ e $\mathbb{L}$ são isomorfos, e que a função φ identifica a cada $a \in \mathbb{A}$ o polinômio $(a, 0, 0, ...) \in \mathbb{L}$ que é chamado *polinômio constante.* □

Definição 3.7 (Grau de um polinômio)**.** Seja $f = (a_i)$ um polinômio não nulo. O número natural n de maneira que $a_n \neq 0$ e $a_i = 0, \forall i > n$ é chamado *grau* de f e é denotado por ∂f.

Assim, o termo a_n é chamado *coeficiente dominante* de f. Caso o termo a_n seja 1, então f é um *polinômio mônico.*

Exemplos:

1) O polinômio g em $\mathbb{Q}[X]$, $g = (-1, \frac{1}{2}, 0, 0, 5, 0, 0, ...)$ tem grau 4.

2) O polinômio h em $(M_2(\mathbb{Z}))[X]$, $h = \left(\begin{pmatrix} 1 & 2 \\ 0 & 7 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, ... \right)$ tem grau 0.

Observação: Note que o grau do polinômio nulo não existe e o grau de um polinômio constante é igual a 0.

As proposições a seguir garantem algumas condições sobre o grau de um polinômio que é resultado de uma adição ou de uma multiplicação de outros dois polinômios.

Em relação à adicão de polinômios:

Proposição 3.7. Sejam $f = (a_i)$ e $g = (b_j)$ dois polinômios de $\mathbb{A}[X]$, então:

(i) ou $f + g = 0$ ou $\partial(f + g) \leq max\{\partial f, \partial g\}$;

(ii) $\partial(f + g) = max\{\partial f, \partial g\}$, se $\partial f \neq \partial g$.

Demonstração.
Vamos demonstrar os itens (i) e (ii).

(i) Se $f+g = (c_i)$ e $n = max\{\partial f, \partial g\}$, obtemos: $c_i = a_i+b_i = 0$ para todo $i > n$ natural. Sendo assim, ou $f + g = 0$, e portanto, o grau de $f + g$ não existe, ou $\partial(f + g) \leq n$, se $f + g \neq 0$.

(ii) Se $\partial f \neq \partial g$, vamos admitir que $n = \partial f > \partial g$. Dessa forma, temos que:

$c_n = a_n + b_n = a_n + 0 = a_n \neq 0$, já que $\partial f = n$ e todos os c_i serão iguais a 0, para todo $i > n$. Portanto $\partial(f + g) = n$.

□

Exemplos:

1) Sejam dois polinômios $f = (2, -5, 8, 0, 0, ..., 0, ...)$ e $g = (-2, 5, -8, 0, 0, ..., 0, ...)$ de $\mathbb{Z}[X]$. Temos que $f + g = 0$. Portanto $\partial(f + g)$ não existe.

   Note que $g = -f$.

2) Sejam $f = (4, 7, -1, 0, 0, ..., 0, ...)$ e $g = (2, 1, 0, 0, ..., 0, ...)$ dois polinômios de $\mathbb{R}$, então $f + g = (6, 8, -1, 0, 0, ..., 0, ...)$. Portanto $\partial(f + g) = 2 = max\{\partial f = 2, \partial g = 1\}$.

3) Sejam $f = (\overline{1}, \overline{3}, \overline{3}, \overline{0}, ..., \overline{0}, ...)$ e $g = (\overline{2}, \overline{1}, \overline{1}, \overline{0}, ..., \overline{0}, ...)$ dois polinômios de $\mathbb{Z}_4$. A soma $f + g = (\overline{3}, \overline{0}, \overline{0}, \overline{0}, ..., \overline{0}, ...)$ tem grau igual a $0 < max\{\partial f = 2, \partial g = 2\}$.

Em relação à multiplicação de polinômios:

Proposição 3.8. Se $f = (a_i)$ e $g = (b_i)$ dois polinômios não nulos de $\mathbb{A}[X]$, então:

(i) ou $f \cdot g = 0$ ou $\partial(f \cdot g) \leq \partial f + \partial g$;

(ii) $\partial(f \cdot g) = \partial f + \partial g$ quando o coeficiente dominante de f ou de g é um elemento regular para a multiplicação em A.

Demonstração.
Vamos demonstrar os itens (i) e (ii).

(i) Se $\partial f = m$, $\partial g = n$ e $fg = (c_k)$, temos que o elemento $c_{m+n+p} = a_0 b_{m+n+p} + a_1 b_{m+n+p-1} + ... + a_m b_{n+p} + ... + a_{m+n+p} b_0$. Mas $\partial g = n$ então $b_j = 0$, para todo $j > n$. O mesmo ocorre com f, pois $\partial f = m$ então $a_i = 0$, para todo $i > m$. Logo $c_{m+n+p} = 0$ para qualquer p natural. Sendo assim, concluímos que ou $fg = 0$ (e daí o grau de fg não existe), ou $\partial(fg) \leq m + n$.

(ii) Se $\partial f = m$ e $\partial g = n$, temos que o elemento $c_{m+n} = a_0 b_{m+n} + a_1 b_{m+n-1} + ... + a_m b_n + ... + a_{m+n} b_0 = a_m b_n$, pois, como no item anterior, sabemos que $a_i = 0$ para todo $i > m$ e $b_j = 0$ para todo $j > n$, além disso, por hipótese, temos que a_m e b_n são elementos regulares em $\mathbb{A}$, portanto $a_m b_n \neq 0$. E daí, $c_{m+n} \neq 0$. Logo, segue que $\partial(fg) = m + n$.

□

Observação: Para domínios de integridade, a igualdade $\partial(fg) = \partial f + \partial g$ sempre é válida.
Exemplos:

1) Sejam dois polinômios $f = (4, 3, 0, 0, ..., 0, ...)$ e $g = (1, 2, 5, 0, 0, ..., 0, ...)$ de $\mathbb{R}[X]$. Então $f \cdot g = (4, 11, 26, 15, 0, 0, ..., 0, ...)$. Portanto, $\partial(fg) = 3 = 1 + 2 = \partial f + \partial g$.

2) Em $\mathbb{Z}_6$ o polinômio $fg = (\overline{2}, \overline{5}, \overline{5}, \overline{0}, \overline{0}, ..., \overline{0}, ...)$, em que $f = (\overline{2}, \overline{1}, \overline{3}, \overline{0}, \overline{0}, ...\overline{0}, ...)$ e $g = (\overline{1}, \overline{2}, \overline{0}, \overline{0}, ...\overline{0}, ...)$, tem grau $\partial(fg) = 2 < 2 + 1 = \partial f + \partial g$, pois $\mathbb{Z}_6$ não é domínio de integridade.

Observação (Notação polinomial): Até aqui, o objeto polinômio foi definido como uma sequência quase nula. Utilizamos esta notação pois, a notação usual de polinômio, de certa forma, esconde o seu significado. Se definirmos

$$1 = (1, 0, 0, ...) \text{ e } X = (0, 1, 0, 0, ...)$$

então

$$X^2 = X \cdot X = (0, 0, 1, 0, 0, ...)$$
$$X^3 = X^2 \cdot X = (0, 0, 0, 1, 0, 0, ...)$$

e assim sucessivamente. Dessa forma X^n é um polinômio em que o termo $a_n = 1$ e todos os outros, anteriores e posteriores a ele, são iguais a zero.

Se tomarmos o polinômio $f = (a_0, a_1, a_2, 0, 0, ...)$, f pode ser escrito como

$$f = (a_0, 0, 0, ...) + (0, a_1, 0, 0, ...) + (0, 0, a_2, 0, 0, ...) =$$
$$(a_0, 0, 0, ...) \cdot (1, 0, 0, ...) + (0, a_1, 0, 0, ...)(0, 1, 0, 0, ...) + (0, 0, a_2, 0, 0, ...)$$
$$(0, 0, 1, 0, 0, ...) = a_0 + a_1X + a_2X^2 + a_3 \cdot 0 + a_4 \cdot 0 + ... = a_0 + a_1X + a_2X^2$$

Podemos perceber que esta representação facilita a manipulação dos elementos de $A[X]$. Não entraremos em detalhes mas, a notação de sequência que atribuímos inicialmente aos polinômios deixa explícito que $\mathbb{A}[X]$ é um espaço vetorial. Portanto, o polinômio $f = (a_0, 0, 0, ...) \cdot (1, 0, 0, ...) + (0, a_1, 0, 0, ...)(0, 1, 0, 0, ...) + (0, 0, a_2, 0, 0, ...)(0, 0, 1, 0, 0, ...)$ que exemplificamos anteriormente está escrito em termos da base canônica do espaço vetorial dos polinômios:

$$1 = (1, 0, 0, ...), X = (0, 1, 0, 0, ...), X^2 = (0, 0, 1, 0, 0, ...), X^3 = (0, 0, 0, 1, 0, 0, ...), ...$$

A partir de agora, como existe umarelação biunívoca entre estas duas notações, utilizaremos a notação usual de polinômios.

Polinômios inversíveis

Quando dizemos que um elemento é "inversível"estamos nos referindo à existência de seu simétrico multiplicativo, ou seja, de seu inverso. Quando isso ocorre, para um elemento x de um anel, existe x^{-1} tal que $xx^{-1} = 1$ em que o elemento 1 é a unidade do anel.

Aqui, o objetivo é mostrar que, quando $\mathbb{A}$ é um domínio de integridade, o conjunto $U(\mathbb{A}[X])$ dos elementos inversíveis de $\mathbb{A}[X]$ é, exatamente, o conjunto $U(\mathbb{A})$ dos elemtentos inversíveis de $\mathbb{A}$, ou seja, os polinômios constantes. Isto quer dizer que $U(\mathbb{A}[X]) = U(\mathbb{A})$.

Como vimos na proposição 3.6, usando a notação usual de polinômios, um elemento $(a, 0, 0, ...)$ do subanel $\mathbb{L}$ de $\mathbb{A}[X]$ é igual ao elemento a que pertence ao anel $\mathbb{A}$. Portanto, podemos dizer que o anel $\mathbb{A}$ é um subanel de $\mathbb{A}[X]$, isto quer dizer que os elementos de $\mathbb{A}$ estão em $\mathbb{A}[X]$, então os elementos inversíveis de $\mathbb{A}$ também estão em $\mathbb{A}[X]$, ou seja, $U(\mathbb{A}) \subset U(\mathbb{A}[X])$. Portanto, para mostrarmos a igualdade $U(\mathbb{A}[X]) = U(\mathbb{A})$, basta mostrar que $U(\mathbb{A}[X]) \subset U(\mathbb{A})$.

Considere dois polinômios f e g de $\mathbb{A}[X]$ tais que $fg = 1$. Ao olharmos para o grau dos polinômios desta igualdade, vamos obter que $\partial(fg) = \partial(1)$. Como $\partial(1) = 0$, pois o polinômio 1 é constante, e $\partial(fg) = \partial f + \partial g$, portanto, $\partial f + \partial g = 0$. Logo $\partial f = -\partial g$. Esta equação somente é válida se $\partial f = 0$ e $\partial g = 0$, isto é, f, g serem polinômios constantes, ou seja, "$f, g \in \mathbb{A}$". Como $fg = 1$, temos que f e g são inversíveis, então $f, g \in U(\mathbb{A})$. Assim, fica provado que se A é um domínio de integridade, então o conjunto dos elementos inversíveis de $\mathbb{A}[X]$ é o próprio $\mathbb{A}$.

Observação: Note que f, g são polinômios não nulos, pois como $\mathbb{A}$ é um domínio de integridade, então $fg = 1$ implica que $f \neq 0$ e $g \neq 0$. Logo existe ∂f e ∂g. O exemplo a seguir mostra o que queremos dizer com esta observação.

Exemplo: Em $\mathbb{Z}_4[X]$, o polinômio $f = \overline{1} + \overline{2}X$ é inversível pois

$$ff = (\overline{1} + \overline{2}X)(\overline{1} + \overline{2}X) = \overline{1} + \overline{0}X + \overline{0}X^2 = \overline{1} \Rightarrow \partial(ff) = 0.$$

Veja que $\mathbb{Z}_4$ não é um domínio de integridade.

Observação (Anel de polinômios sobre um corpo): Já que todo corpo é um anel de integridade, então todas os resultados obtidos para anéis de polinômios sobre anéis de integridade, trabalhados nas seções anteriores, são válidos para anéis de polinômios sobre corpos.

3.4 Divisão em $\mathbb{A}[X]$

Definição 3.8 (Divisão de polinômios)**.** Sejam $\mathbb{A}$ um anel comutativo com unidade e f e g dois polinômios sobre $\mathbb{A}$. Se existir um polinômio $h \in \mathbb{A}[X]$ de modo que $g = f \cdot h$ então dizemos que f *divide* g ou que g é *divisível* por f e denotamos por $f \mid g$.

Caso contrário, f não divide g, e denotaremos por $f \nmid g$.

Exemplo: Sejam $f = 1 + X$ e $g = 1 - X^2$ dois polinômios de $\mathbb{Z}[X]$. Como $1 - X^2 = (1 + X)(1 - X)$ e o polinômio $1 - X$ está em $\mathbb{Z}[X]$, então $f \mid g$.

Propriedades da divisão em $\mathbb{A}[X]$

Seja $\mathbb{A}[X]$ um anel comutativo com unidade. Listaremos quatro propriedades importantes da divisão neste anel que usaremos mais adiante.

(i) $f \mid f, \forall f \in \mathbb{A}[X]$, pois como $\mathbb{A}[X]$ é um anel com unidade, existe $h = 1 \in \mathbb{A}[X]$ tal que $f = f \cdot h$.

(ii) Se $f \mid g$ e $g \mid h$, então $f \mid h$. Isso ocorre porque se $f \mid g \Rightarrow \exists f' \in \mathbb{A}[X]$ tal que $g = f \cdot f'$ e se $g \mid h \Rightarrow \exists g' \in \mathbb{A}[X]$ tal que $h = g \cdot g'$ então $h = g \cdot g' = (f \cdot f') \cdot g' = f \cdot (f' \cdot g')$ já que a multiplicação em $\mathbb{A}[X]$ é associativa. E daí, se tomarmos $f' \cdot g' = h'$, teremos $h = f \cdot h'$. Logo $f \mid h$.

(iii) Sempre que $f \mid g$ também ocorre que f divide todo múltiplo de g, ou seja, $f \mid hg, \forall h, g, f \in \mathbb{A}[X]$. Isso pode ser explicado pelo item anterior. Temos que $f \mid g$. Se tomarmos um polinômio h então $g \mid gh$. Assim, pelo item (ii) $f \mid gh$.

(iv) Se $f \mid g_1$ e $f \mid g_2$ então $f \mid (g_1h_1 + g_2h_2), \forall f, g_1, g_2, h_1, h_2 \in \mathbb{A}[X]$, pois se $f \mid g_1 \Rightarrow g_1 = f \cdot q_1$ para algum $q_1 \in \mathbb{A}[X]$, e o mesmo ocorre se $f \mid g_2 \Rightarrow g_2 = f \cdot q_2$, para algum $q_2 \in \mathbb{A}[X]$. Assim, podemos obter (1) $g_1 \cdot h_1 = (f \cdot q_1) \cdot h_1$ e (2) $g_2 \cdot h_2 = (f \cdot q_2) \cdot h_2$ e se somarmos (1) com (2), aplicando a propiedade associativa da multiplicação, teremos $f(q_1 \cdot h_1) + f \cdot (q_2 \cdot h_2) = f \cdot (q_1 \cdot h_1 + q_2 \cdot h_2)$ daí concluímos que $g_1h_1 + g_2h_2 = f \cdot (q_1 \cdot h_1 + q_2 \cdot h_2)$ e portanto $f \mid (g_1 \cdot h_1 + g_2 \cdot h_2)$.

3.4.1 Algoritmo euclidiano

Teorema 3.1 (Algoritmo euclidiano)**.** *Dados dois polinômios $f = a_0 + a_1X + ... + a_nX^n$ e $g = b_0 + b_1X + ... + b_mX^m$ de um anel comutativo com unidade $\mathbb{A}[X]$. Vamos supor $g \neq 0$ e o coeficiente dominante de g, ou seja, o coeficiente que multiplica a indeterminada X com maior expoente, inversível. Nessas condições, existem $q, r \in \mathbb{A}[X]$ de modo que $f = gq + r$ tais que ou $r = 0$ ou $\partial r < \partial g$.*

Demonstração.
O teorema diz que dados dois polinômios f e g, satisfazendo as condições acima, a equação $f = gq + r$ implica que ou $g \mid f$, o que acarreta em $r = 0$, ou o grau de r ser menor que o grau de g.

Temos as seguintes possibilidades:

(i) f ser o polinômio nulo, ou seja, $f = 0$, e para que isso aconteça, $gq + r$ deve ser 0, então r e q são iguais a zero, pois caso $q \neq 0$, então $q = \frac{-r}{g}$, e como g não divide r, chegaríamos que $q = -r$, o que é absurdo.

(ii) $\partial f < \partial g$. Quando isso ocorre, tomamos $q = 0$ e $r = f$ e daí $f = g \cdot 0 + f$, e por hipótese $\partial r < \partial g$.

(iii) $\partial f \geq \partial g$. Neste caso, vamos proceder por indução.
Se $\partial f = 0$, então $\partial g = 0$. Daí $f = a_0$ e $g = b_0$. Entao basta tomar $r = 0$ e $q = b_0^{-1}a_0$ e portanto $a_0 = b_0(b_0^{-1}a_0) + 0$.

Agora vamos supor que $\partial f = n$ e que o teorema seja válido para todo polinômio g de grau menor ou igual a n. Consideremos o polinômio $f_1 = f - a_n b_m^{-1} X^{n-m} g$.

Se $f_1 = 0$ ou $\partial f_1 < \partial g$, então $r = f_1$ e $q = a_n b_m^{-1} X^{n-m}$. Caso contrário, tem-se $\partial f_1 \leq n-1$ e $\partial f_1 \geq \partial g$. Pela hipótese de indução, existem $q_1, r_1 \in \mathbb{A}[X]$ de maneira que:

$$f_1 = gq_1 + r_1, \text{ em que } r_1 = 0 \text{ ou } \partial r_1 < \partial g.$$

Então

$$f - a_n b_m^{-1} X^{n-m} g = gq_1 + r_1$$

o que acarreta que

$$f = g(q_1 + a_n b_m^{-1} X^{n-m}) + r_1, \text{ em que } r_1 = 0 \text{ ou } \partial r_1 < \partial g.$$

□

Corolário 3.1. Seja $\mathbb{A}$ um corpo. Dados $f, g \in \mathbb{A}[X]$ com $g \neq 0$, existe um único par (q, r) de polinômios de $\mathbb{A}[X]$ de maneira que $f = gq + r$ e $\partial r < \partial g$ quando $r \neq 0$.

Demonstração.
A existência já foi mostrada anteriormente. Basta provarmos a unicidade.

Suponha que $f = gq + r$, em que $\partial r < \partial g$, com $r \neq 0$ e $f = gq_1 + r_1$, em que $\partial r_1 < \partial g$, com $r_1 \neq 0$. Então, temos que:

$$\begin{aligned} f = gq + r \text{ e } f = gq_1 + r_1 \\ \Rightarrow gq + r = gq_1 + r_1 \\ \Rightarrow gq - gq_1 = r_1 - r \\ g(q - q_1) = r_1 - r \end{aligned}$$

Se $r_1 - r$ for igual a zero, então $q - q_1 = 0$, já que $\mathbb{A}$ é um domínio de integridade.

Suponhamos $r_1 \neq r$. Logo $\partial(g(q-q_1)) \overset{*}{=} \partial g + \partial(q-q_1) = \partial(r_1-r)$. Então $\partial(r_1-r) \geq \partial g$. Mas é impossível isto ocorrer, já que $\partial(r_1 - r) \leq max\{\partial r_1, \partial r\} < \partial g$. Portanto, $r = r_1$ e por consequência $q = q_1$. □

$*$ $\mathbb{A}$ é um corpo, então todo elemento $a \in \mathbb{A}^*$ é regular para a multiplicação. Assim, podemos considerar $\partial(g(q - q_1)) = \partial g + \partial(q - q_1)$.

Definição 3.9 (Polinômios irredutíveis)**.** Seja $\mathbb{K}$ um corpo. Um polinômio $p \in \mathbb{K}[X]$ é *irredutível* em $\mathbb{K}[X]$ se:

(i) p não é um polinômio constante;

(ii) $f \mid p$, então ou f é um polinômio constante não nulo ou existe um $c \in \mathbb{K}^*$ tal que $f = cp$.

Quando um polinômio p não é irredutível, então ele é composto, isto é, pode ser escrito como uma multiplicação de polinômios não constantes. Note que todo polinômio de grau 1 sobre um corpo $\mathbb{K}$ é irredutível, pois $p = ax + b$ com $a, b \in \mathbb{K}$ e $a \neq 0$, é não constante e, além disso, se $g \mid f$, então existe $h \in \mathbb{K}[X]$ tal que $f = gh$. Daí, $\partial f = \partial(gh)$, e portanto, $1 = \partial g + \partial h$. Assim, ou $\partial g = 0$ ou $\partial h = 0$. Se $\partial g = 0$ então $g = c \in \mathbb{K}^*$. Se $\partial h = 0$, então $h = d \in \mathbb{K}^*$ e $g = \frac{1}{k}f$. Concluímos que, ou g é um elemento de $\mathbb{K}^*$ ou g é um polinômio múltiplo de f.

Definição 3.10 (mdc entre polinômios)**.** Sejam $\mathbb{K}$ um corpo e $f, g \in \mathbb{K}[X]$. Define-se $d \in \mathbb{K}[X]$ como um *máximo divisor comum* (mdc) de f e g se

(i) $d \mid f$ e $d \mid g$;

(ii) $\forall d' \in \mathbb{K}[X]$, se $d' \mid f$ e $d' \mid g \Rightarrow d' \mid d$.

Exemplo: Em $R[X]$, dados os polinômios $f = 2+2X$ e $g = 1-X^2$, o polinômio $d = 1+X$ é um máximo divisor de f e g, de fato:

(i) $d = 1 + X \mid 2 + 2X = f$, pois $f = 2 \cdot (1 + X) = 2d$, e $d = 1 + X \mid 1 - X^2 = g$, pois, $g = (1 - X)(1 + X) = (1 - X)d$;

(ii) Se $d_1 \mid f$ então existe $q \in R[X]$ tal que $f = d_1 q$. Como $\partial f = 1$ então $\partial d_1 = 0$ ou $\partial d_1 = 1$. Se $\partial d_1 = 0$, então d_1 é um polinômio constante (e diferente do polinômio nulo), e se tomarmos a igualdade $d = d_1(\frac{1}{d_1} + \frac{1}{d_1}X)$ então $d_1 \mid d$.

Mas se $\partial d_1 = 1$ então temos que $d_1 = a + bX$ e, assim, q é um polinômio constante c, em que $a, b, c \in \mathbb{R}^*$. Mas se $f = d_1 q$ então $f = (a + bX)c = ac + bcX = 2 + 2X$,

portanto, segue que $ac = bc = 2$ e $a = b$. Reescrevendo d_1 temos que $d_1 = a + aX = a(1 + X)$ então $d = \frac{1}{a}[a(1 + X)] = \frac{1}{a}d_1$. Logo, fica provado que $d_1 \mid d$.

Definição 3.11 (Ideal)**.** Um subconjunto I, $I \neq \emptyset$, de um anel comutativo $\mathbb{A}$ é um *ideal* em $\mathbb{A}$ se, e somente se:

(i) Se $x, y \in I$, temos que $x - y \in I$;

(ii) Se $a \in \mathbb{A}$ e $x \in I$, temos que $ax \in I$

Os conjuntos $\mathbb{A}$ e $\{0\}$ são ideias triviais de $\mathbb{A}$.

Exemplo: O subconjunto $5\mathbb{Z} = \{5q \mid q \in \mathbb{Z}\}$ do anel comutativo $\mathbb{Z}$ é um ideal em $\mathbb{Z}$, pois:

1) O conjunto $5\mathbb{Z}$ é não vazio pois o elemento 0 pertence à $5\mathbb{Z}$, já que $0 = 5 \cdot 0$;

2) $5q_1 - 5q_2 = 5(q_1 - q_2) \in 5\mathbb{Z}$;

3) $a(5q) = 5(aq) \in 5\mathbb{Z}$, já que $\mathbb{Z}$ é um anel comutativo.

Definição 3.12 (Ideal principal)**.** O ideal $I =< a_1, a_2, ..., a_n >= \{x_1a_1 + x_2a_2 + ... + x_na_n \mid x_1, x_2, ..., x_n \in \mathbb{A}\}$ de $\mathbb{A}$ é chamado *ideal gerado* por $a_1, a_2, ..., a_n$.

Se um ideal I é gerado por um único elemento de $a \in \mathbb{A}$, então I é um *ideal principal* gerado por a, e I é denotado por $< a >$.

Teorema 3.2. *Se $\mathbb{K}$ é um corpo então todo ideal em $\mathbb{K}[X]$ é principal.*

A demonstração do teorema acima pode ser encontrada na referência 4.

Teorema 3.3 (Existência do mdc)**.** *Seja $\mathbb{K}$ um corpo. Então dados f, g dois polinômios de $\mathbb{K}[X]$, existem h_1, h_2 de tal forma que o polinômio $d = fh_1 + gh_2$ é um máximo divisor comum de f e g.*

Demonstração.
Considere o ideal $I = < f, g > = \{fm_1 + gm_2 \mid m_1, m_2 \in \mathbb{K}[X]\}$. Todo ideal em $\mathbb{K}[X]$ é principal. Logo existe d em I de maneira que $I =< d >$. Agora, vamos mostrar que d é máximo divisor comum de f e g.

(i) f é elemento de $I =< d >$, pois $f = f \cdot 1 + g \cdot 0$. Então, existe $q_1 \in \mathbb{K}[X]$ tal que $f = dq_1$ e, portanto, $d \mid f$. Analogamente, podemos chegar que $d \mid g$.

(ii) d é elemento de I, logo existem $h_1, h_2 \in \mathbb{K}[X]$ tais que $d = fh_1 + gh_2$. Se $d' \in \mathbb{K}[X]$ divide f e divide g, então $f = d'x_1$ e $g = d'x_2$ e, portanto, $d = (d'x_1)h_1 + (d'x_2)h_2$ e assim, $d = d'(x_1h_1 + x_2h_2)$ então $d' \mid d$.

□

Observação: Para que d seja único basta adicionar à proposição que d deve ser mônico.

Proposição 3.9. Seja $\mathbb{K}[X]$ um corpo. Se $f, g \in \mathbb{K}[X]$ e se $d \in \mathbb{K}[X]$ é um máximo divisor comum de f, g, então $d' \in \mathbb{K}[X]$ será também um máximo divisor comum de f, g se, e somente se existe $k \in \mathbb{K}^*$ tal que $d' = kd$.

Demonstração.
($\Rightarrow$) Se d' é máximo divisor comum de f e g então $d' \mid f$ e $d' \mid g$ e, portanto, $d' \mid d$, já que d é máximo divisor comum de f e g. Da mesma maneira chegamos que $d \mid d'$. Assim:

$$d' \mid d \text{ então } d = q_1 d' \text{ para algum } q_1 \in \mathbb{K}[X]$$
$$d \mid d' \text{ então } d' = q_2 d \text{ para algum } q_2 \in \mathbb{K}[X]$$

portanto $d = d(q_1 q_2)$. O caso $d = 0$ ocorre quando $f = g = 0$ e então $d' = 0$. Mas se $d \neq 0$ então $q_1 q_2 = 1$ e, portanto, $q_1, q_2 \in \mathbb{K}^*$. Se fizermos $q_2 = k \in \mathbb{K}^*$, teremos $d' = kd$.

Isso mostra que se um polinômio mônico $d \in \mathbb{K}[X]$ é máximo divisor comum de f e g então $d' = kd, \forall k \in K^*$ também é máximo divisor comum de f e g.

($\Leftarrow$) Por hipótese, temos que $d' = kd$. Se

(i) $d \mid f$ então $f = dq$. E daí $f = kd(\frac{1}{k}q) = d'(\frac{1}{k}q)$ e, portanto, $d' \mid f$. Analogamente, pode-se provar que $d' \mid g$.

(ii) um elemento $d_1 \in K[X]$ é tal que $d_1 \mid f$ e $d_1 \mid g$ então $d_1 \mid d$ e, portanto, $d_1 \mid kd$ logo $d_1 \mid d'$.

Portanto d' é um outro máximo divisor comum. □

A proposição acima nos diz que o mdc entre dois polinômios sobre um corpo não é único.

Teorema 3.4 (Teorema da fatoração única)**.** *Seja $\mathbb{K}$ um corpo e f um polinômio não constante de $\mathbb{K}[X]$. Então existem polinômios irredutíveis $p_1, p_2, ..., p_r \in \mathbb{K}[X]$ $(r \geq 1)$ tais que $f = p_1 p_2 ... p_r$. Além disso, se $f = q_1 q_2 ... q_s$, onde $q_1, q_2, ..., q_s \in \mathbb{K}[X]$ $(s \geq 1)$ também são irredutíveis sobre $\mathbb{K}[X]$, então $r = s$ e cada polinômio p_i é igual ao produto de um polinômio q_j por um elemento conveniente de $\mathbb{K}^*$. Portanto, a fatoração é única, a menos da ordem dos polinômios irredutíveis e de multiplicação por constantes não nulas.*

Demonstração.
Vamos mostrar a existência e a unicidade de $p_1 p_2 ... p_r$.

(i) Vamos mostrar a existência de $p_1p_2...p_r$:

Quando f é irredutível, então existe $p_1 = f$ tal que $f = p_1$.

Agora vamos proceder por indução. Se $\partial f = 1$ então f é irredutível, como mostramos em Polinômios inversíveis.

Suponha $\partial f = n > 1$, f um polinômio composto, e que o teorema seja válido, em relação à existência, para todo polinômio de grau r, com $1 \leq r < n$.

Se f é composto então existem $g, h \in \mathbb{K}[X]$, com f, g não constantes, tais que $f = gh$ e $0 < \partial g < \partial f$ e $0 < \partial h < \partial f$. Pela hipótese de indução temos que:

$$g = p_1p_2...p_t \text{ e } h = p_{t+1}p_{t+2}...p_r \text{ em que os } p_i \text{ são irredutíveis, } t \geq 1 \text{ e } r - t \geq 1$$

Logo, mostramos que existem $p_1p_2...p_r$ tais que $f = p_1p_2...p_r$.

(ii) Vamos mostrar a unicidade de $p_1p_2...p_r$:

Suponha $f = p_1p_2...p_r = q_1q_2...q_s$ e $r \leq s$. Como $p_1 \mid (q_1q_2...q_s)$ e p_1 é irredutível, então p_1 divide algum dos q_i. Vamos supor que $p_1 \mid q_1$ então, como $\mathbb{K}$ é um corpo, temos que $p_1 = c_1q_1$ e, portanto,

$$f = (c_1q_1)p_2...p_r = q_1q_2...q_s.$$

Como em $K[X]$ vale a lei do cancelamento,

$$(c_1p_2)p_3...p_r = q_2...q_s$$

Repetindo o raciocínio acima, chegaremos que:

$$c_1c_2...c_r = k = q_1...q_w \text{ para algum } w \in \mathbb{N}, \text{ com } w < s.$$

e, isso implica que,

$$\partial k = \partial(q_1...q_w)$$

mas $\partial k = 0$, então $\partial(q_1...q_w)$ deve ser igual a zero. Porém, uma multiplicação de polinômios tem grau igual a zero somente quando estes polinômios são constantes. Portanto o polinômio $q_1...q_w$ é constante. Dessa forma, chegaremos que $r = s$ e provamos a unicidade da decomposição de f.

□

Exemplo: O polinômio $f = 2 - 2X^2$ pode ser decomposto como $f = (1 - X)(2 + 2X)$ e também como $f = (1 - X)(1 + X) \cdot 2$. Observe que $(1 - X)(2 + 2X) = (1 - X)(1 + X) \cdot 2$ pois $2+2X = 2(1+X)$ em que $1+X$ é fator de f, e o elemento 2 é o elemento conveniente de $\mathbb{K}[X]$ que multiplicamos por $1 + X$.

CAPÍTULO

4

DIVISIBILIDADE EM DOMÍNIOS DE INTEGRIDADE

Vimos no capítulo 2 que um domínio de integridade é um anel comutativo com unidade e sem divisores de zero. Neste capítulo faremos um breve estudo sobre a divisibilidade em domínios de integridade. Nosso raciocínio de divisão será restrito aos domínios $\mathbb{Z}$ e $\mathbb{K}[X]$, em que $\mathbb{K}$ é um corpo.

4.1 Domínio euclidiano

O escopo desta seção é generalizar o *Algoritmo euclidiano* para domínios de integridade. Para tanto, abaixo segue a definição de domínio euclidiano.

Definição 4.1 (Domínio Euclidiano)**.** Um *domínio euclidiano* $(\mathbb{D}, +, \cdot, \phi)$ é um domínio de integridade $(\mathbb{D}, +, \cdot)$ com uma função $\phi : \mathbb{D}^* \to \mathbb{N}$ que satisfaz as seguintes condições:

(i) $\forall a, b \in \mathbb{D}, b \neq 0$ existem $t, r \in \mathbb{D}$ tais que $a = bt + r$, em que $\phi(r) < \phi(b)$ ou $r = 0$.

(ii) $\forall a, b \in \mathbb{D}^*, \phi(a) \leq \phi(ab)$

Observe que a definição acima não garante a unicidade de t e r.

Pela definição 4.1, se um domínio de integridade $\mathbb{D}$ é um domínio euclidiano, então, em $\mathbb{D}$, vale a o algoritmo euclidiano.

Para que um domínio de integridade seja um domínio euclidiano deve existir ao menos uma função $\phi : \mathbb{D}^* \to \mathbb{N}$ que satisfaz as condições (i) e (ii). Para mostrar que os domínios de integridade $\mathbb{Z}$ e $\mathbb{K}[X]$, quando $\mathbb{K}$ é um corpo, são domínios euclidianos utilizaremos a função *módulo* e a função *grau*, para números inteiros e polinômios, respectivamente.

$\mathbb{Z}$ é um domínio euclidiano

Demonstração.
Como já foi visto no capítulo 2, $\mathbb{Z}$ com as operações usuais de adição e multiplicação é um domínio de integridade.

Então temos que encontrar uma função que satisfaça os itens (i) e (ii) da definição 4.1.

Vamos tomar a função *módulo*:

$$\phi : \mathbb{Z}^* \to \mathbb{N}, \text{ definida por } \phi(x) =\mid x \mid$$

(i) $\forall a, b \in \mathbb{Z}$, com $b \neq 0$, existem $t, r \in \mathbb{Z}$ tais que $a = bt + r$ em que $\phi(r) < \phi(b)$ ou $r = 0$, pois o teorema 2.1 nos garante isso.

(ii) $\forall a, b \in \mathbb{Z}^*$, temos que $\mid a \mid \leq \mid ab \mid$. Fazendo $\phi(a) =\mid a \mid$ e $\phi(ab) =\mid ab \mid =\mid a \mid \cdot \mid b \mid$, concluímos que $\phi(a) \leq \phi(a \cdot b)$.

□

$\mathbb{K}[X]$, quando $\mathbb{K}$ é corpo, é um domínio euclidiano

Demonstração.
Sabemos que todo corpo é um domínio de integridade, portanto, $\mathbb{K}[X]$ também é um domínio de integridade, como vimos na proposição 3.4.

Agora, devemos tomar uma função que satisfaça os itens (i) e (ii) da definição x, que como dissemos, é a função *grau*:

$$\phi : (\mathbb{K}[X])^* \to \mathbb{N}, \text{ definida por } \phi(f) = \partial f$$

(i) $\forall f, g \in (\mathbb{K}[X])^*, g \neq 0$, existem $t, r \in \mathbb{K}[X]$ tais que $f = gt + r$, em que $\phi(r) < \phi(g)$ ou $r = 0$, pois o teorema 3.1 nos garante isso.

(ii) $\forall f, g \in (\mathbb{K}[X])^*, \phi(f) \leq \phi(fg)$, pois se $\phi(f) = \partial f$, $\phi(fg) = \partial(fg) = \partial f + \partial g$, temos que $\partial f \leq \partial f + \partial g$.

□

Podemos concluir que a divisão euclidiana em $\mathbb{Z}$ e em $\mathbb{K}[X]$ funcionam de maneira semelhante.

Observação: Quando $\mathbb{K}$ não é um corpo, nem sempre existem dois elementos de $\mathbb{K}$ que satisfazem as condições (i) e (ii) acima com a função grau. Por exemplo, em $\mathbb{Z}[X]$, não existe um elemento $c \in \mathbb{Z}[X]$ tal que $x^2 = c \cdot 2x$. Logo $\mathbb{Z}[X]$ não é um domínio euclidiano. Perceba que se os polinômios da igualdade anterior fossem polinômios sobre $\mathbb{R}$, o polinômio c seria $\frac{1}{2}x$.

4.2 Domínio fatorial

O objetivo desta seção é generalizar a *fatoração única*.

Definição 4.2 (Domínio fatorial)**.** Um domínio de intergidade $\mathbb{D}$ é um *domínio fatorial* ou *Domínio de fatoração única* se

(i) todo elemento $d \neq 0$ de $\mathbb{D}$ que não admite inverso multiplicativo, pode ser escrito da seguinte maneira: $d = p_1 p_2 ... p_n$, em que $n \geq 1$ e os p_i são irredutíveis, para todo i natural;

(ii) Se $a = p_1 p_2 ... p_r$ e $a = q_1 q_2 ... q_s$ são duas fatorações de $a \in \mathbb{D}$ em elementos irredutíveis de $\mathbb{D}$, então $r = s$ e cada p_i é associado a um q_j.

$\mathbb{Z}$ é um domínio fatorial

Demonstração.
Sabemos que $\mathbb{Z}$ é um domínio de integridade. Vamos mostrar que $\mathbb{Z}$ é um domínio fatorial:

(i) Todo elemento a de $\mathbb{Z}$ tal que $a \neq 0$, $a \neq 1$ e $a \neq -1$, pode ser escrito como um produto de elementos irredutíveis de $\mathbb{Z}$: $a = p_1 p_2 ... p_n$.

(ii) Se $a = p_1 p_2 ... p_r$ e $a = q_1 q_2 ... q_s$ são duas decomposições de a, então $r = s$, isto é, a decomposição é a mesma, a menos da ordem dos elementos, $p_1 p_2 ... p_r = q_1 q_2 ... q_s$.

Os itens (i) e (ii) são verdadeiros, pois o teorema 2.3 nos garante isso. □

$\mathbb{K}[X]$, quando K é corpo, é um domínio fatorial

Demonstração.
Sabemos que $\mathbb{K}[X]$ é um domínio de integridade. Vamos mostrar que $\mathbb{K}[X]$ é um domínio fatorial:

(i) todo elemento $f \neq 0$ de $\mathbb{K}[X]$ que não admite inverso, ou seja, todo polinômio não constante, pode ser escrito como produto de polinômios irredutíveis: $f = d_1 d_2 ... d_n$.

(ii) Se $f = d_1 d_2 ... d_r$ e $f = q_1 q_2 ... q_s$ são duas decomposições de $f \in \mathbb{K}[X]$ em elementos irredutíveis de $\mathbb{K}[X]$, então a decomposição é a mesma, a menos da ordem dos elementos e de multiplicações por elementos de K^*, $d_1 d_2 ... d_r = q_1 q_2 ... q_s$.

Os itens (i) e (ii) são verdadeiros, pois o teorema 3.4 nos garante isso. □

Observação: Perceba que, se $\mathbb{K}$ não é corpo, então $\mathbb{K}[X]$ não é um domínio fatorial. Pois quando $\mathbb{K}$ não é um corpo, existe algum elemento $p \neq 0$ de $\mathbb{K}$ tal que p não admite inverso multiplicativo mas p não pode ser escrito como um produto de polinômios não constantes de $\mathbb{K}[X]$. Por exemplo, o anel dos polinômios sobre $\mathbb{Z}$, $\mathbb{Z}[X]$, não é um domínio fatorial, pois o elemento 3, por exemplo, é diferente de zero e apesar de não admitir inverso em $\mathbb{Z}$, não pode ser escrito como produto de polinômios irredutíveis (e portanto, não constantes) de $\mathbb{Z}[X]$.

Teorema 4.1 (Existência do mdc)**.** *Seja $\mathbb{D}$ um domínio fatorial. Dados dois elementos a, b do domínio $\mathbb{D}$, existe máximo divisor comum desses elementos em $\mathbb{D}$.*

Demonstração.
Se $a = 0$, então b é um máximo divisor de a e b. Pois $b = 1 \cdot b$ e $0 = 0 \cdot b$ então $b \mid b$ e $b \mid 0$.

Agora, se a admite inverso multiplicativo em $\mathbb{D}$ então a é máximo divisor comum de a e b, isto é $a \mid a$ e $a \mid b$ pois $b = (b \cdot \frac{1}{a}) \cdot a$.

Mas se $a, b \notin U(\mathbb{D})$ vamos decompor a e b:

$$a = up_1^{r_1} p_2^{r_2} ... p_n^{r_n} \text{ e } b = vp_1^{s_1} p_2^{s_2} ... p_n^{s_n}, \text{ em que } u, v \in U(\mathbb{D})$$

Vamos mostrar que o elemento $d = p_1^{k_1} p_2^{k_2} ... p_n^{k_n}$, em que $k_i = min\{r_i, s_i\}$, com $i = 1, 2, ..., n$, é um máximo divisor comum de a e b.

Podemos perceber que $d \mid a$ e $d \mid b$. Agora suponha que $d' \in \mathbb{D}$ é tal que $d' \mid a$ e $d' \mid b$. Então $d' = wp_1^{t_1} p_2^{t_2} ... p_n^{t_n}$ com $w \in U(\mathbb{D})$, e $t_i \leq r_i$ e $t_i \leq s_i$. Portanto $t_i \leq min\{r_i, s_i\}$, em que $i = 1, 2, ..., n$. Então $d' \mid d$. □

CAPÍTULO

5

CONSIDERAÇÕES FINAIS

Observou-se, então, que a estrutura dos polinômios muito se assemelha à dos números inteiros, isso se deve ao fato de que, a estrutura do anel de polinômios sobre um corpo e a estrutura dos números inteiros são domínios euclidianos e domínios de fatoração única. Como vimos, existe a divisão euclidiana em $K[X]$, quando K é corpo, assim como ocorre com os inteiros, em consequência, existe mdc, com suas peculiaridades, é claro, e além disso, o Teorema Fundamental da Aritmética pode ser interpetrado para polinômios.

REFERÊNCIAS

1. DOMINGUES, Hygino Hugueros.; IEZZI, Gelson. *Álgebra moderna*. 2. ed. São Paulo: Atual, 1982.

2. DOMINGUES, Hygino Hugueros.; IEZZI, Gelson. *Álgebra moderna*. 4. ed refor. São Paulo: Atual, 2003.

3. EVES, Howard. *Introdução à história da matemática*. Tradução de Hygino H. Domingues. 5. ed. Campinas, Editora da UNICAMP, 2011.

4. FRALEIGH, Jonh B.; *A First Course in Abstract Algebra*. 7. ed. Kingston: Pearson, 2003.

5. GONÇALVES, Adilson. *Introdução à álgebra*. Rio de Janeiro: IMPA, 2003.

6. MILIES, Francisco César Polcino.; COELHO, Sônia Pitta. *Números: uma introdução à matemática*. 3. ed. São Paulo: Universidade de São Paulo, 2001.

7. MILIES, Francisco César Polcino. Breve história da álgebra abstrata. In: BIENAL DA SOCIEDADE BRASILEIRA DE MATEMÁTICA, 2., 2004, Salvador. *Anais...* Salvador: Universidade Federal da Bahia, 2004. p. 6-7.

8. SOUSA, Márcio Monte Alegre. *Divisibilidade em domínio de integridade*. 2013. 26 f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional - Profmat) - Departamento de Matemática, Universidade Federal de Sergipe, Sergipe.

9. TINOCO, Lúcia A.(Coord.). Álgebra: pensar? Calcular? Comunicar?. In: CONGRESSO IBERO-AMERICANO DE EDUCAÇÃO MATEMÁTICA, 6., 2009, Puerto Montt, Chile. *Anais...* Puerto Montt, Chile: Universidade de Los Lagos, 2009.