UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
COORDENAÇÃO DO CURSO DE LICENCIATURA EM MATEMÁTICA

JEFFERSON PERUZZO

FATORAÇÃO E DIVISIBILIDADE EM ANÉIS COMUTATIVOS

TRABALHO DE CONCLUSÃO DE CURSO

TOLEDO
2017

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
COORDENAÇÃO DO CURSO DE LICENCIATURA EM MATEMÁTICA

JEFFERSON PERUZZO

FATORAÇÃO E DIVISIBILIDADE EM ANÉIS COMUTATIVOS

Trabalho de Conclusão de Curso apresentado ao curso de Licenciatura em Matemática da Universidade Tecnológica Federal do Paraná, Câmpus Toledo, como requisito parcial à obtenção do título de Licenciado em Matemática.

Orientadora: Larissa Hagedorn Vieira

TOLEDO
2017

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
COORDENAÇÃO DO CURSO DE LICENCIATURA EM MATEMÁTICA

TERMO DE APROVAÇÃO

O Trabalho de Conclusão de Curso intitulado "Fatoração e Divisibilidade em Anéis Comutativos" foi considerado **APROVADO** de acordo com a ata nº __ de __/__/____

Fizeram parte da banca examinadora os professores:

Professora Orientadora Larissa Hagedorn Vieira

Professor Adriano Gomes de Santana

Professor Robson Willians Vinciguerra

TOLEDO
2017

RESUMO

O presente trabalho constitui um estudo sobre fatoração e divisibilidade em anéis comutativos. São apresentadas diversas definições e teoremas relativos a anéis e ideais, bem como resultados acerca de divisibilidade e fatoração em anéis comutativos. Dentre essas definições, se apresentam os domínios de fatoração única e alguns resultados atrelados aos mesmos, mostrando que os números inteiros são um caso particular dessas estruturas. Por fim, são levantados elementos relativos à fatoração em anéis de polinômios de uma variável.

Palavras-chave: Anéis comutativos. Fatoração. Domínios de fatoração única.

ABSTRACT

This paper is a short study about factorization and divisibility in commutative rings. Many definitions related to rings, ideals and their relation to factorization are given in the text. Among them, the concept of unique factorization domains is introduced, as well as some results related to them, and the fact that the integers are a particular case of this algebraic structure. Also, some general results about factorization in the ring of polynomials in one indeterminate over a ring R are presented.

Key-words: Commutative rings. Factorization. Unique factorization domains.

LISTA DE SÍMBOLOS

$\mathbb{Z}$	Conjunto dos números inteiros
$\mathbb{N}$	Conjunto dos números naturais
$\mathbb{N}^*$	Conjunto dos números naturais sem o 0
(a)	Ideal gerado pelo elemento a
$a\|b$	a divide b
a^{-1}	Inverso do elemento a
$\mathbb{Z}_m$	Anel das classes de equivalência módulo m
$\overline{a}$	Classe de equivalência de a
$R[x]$	Anel de polinômios em uma variável sobre R

SUMÁRIO

1 INTRODUÇÃO

Este trabalho visa apresentar um breve estudo sobre fatoração e divisibilidade em anéis comutativos, de modo a estender para anéis comutativos arbitrários alguns conceitos e resultados presentes e válidos no anel $\mathbb{Z}$ dos números inteiros.

Os conceitos de fatoração e divisibilidade têm importância em diversas áreas, tanto da Matemática, quanto fora dela. Por exemplo: os algoritmos de criptografia RSA e de curvas elípticas. Enquanto o conceito de divisibilidade se faz presente na aritmética modular, que por sua vez possui uma vasta gama de aplicações tais como: o relógio de ponteiro e o Cadastro de Pessoas Físicas (CPF).

No primeiro capítulo se apresenta uma série de definições e resultados que são necessários para a compreensão do tema estudado. Das quais destacamos a definição de anéis, ideais principais, primos e maximais e suas estruturas particulares.

O segundo capítulo trata de definições e resultados relativos à divisibilidade e fatoração em anéis comutativos. Dentre as definições, destacam-se as de elementos primos e irredutíveis, domínios de fatoração única, domínios Euclidianos, máximo divisor comum e uma série de teoremas e propriedades afins.

Por fim, apresentam-se resultados gerais acerca de fatoração em anéis de polinômios de uma variável sobre anéis comutativos. Entre esses resultados, serão demonstrados o algoritmo da divisão de polinômios e a divisibilidade de um polinômio $f(x)$ por um monômio $x - c$, sendo c uma raiz de f.

A fim de tornar a compreensão do trabalho mais acessível, serão apresentados vários exemplos e demonstrações relativos ao tema proposto.

O referencial teórico principal utilizado ao longo do texto é baseado em [4] e [3]. Sendo o tema abordado bastante amplo, ressaltamos que o trabalho não visa esgotá-lo.

2 PRELIMINARES

O presente capítulo trata das definições e teoremas necessários (a título de pré-requisito) para a compreensão geral do problema pesquisado.

Definição 2.1. *Um conjunto não vazio G munido de uma operação binária $\cdot : G \times G \to G$ é denominado um* grupo abeliano *se:*

i) $\forall a, b, c \in G, a\,(bc) = (ab)\,c$;

ii) $\exists e \in G$ *tal que* $ea = ae = a$ *(elemento neutro);*

iii) $\forall a \in G$ *existe* $a^{-1} \in G$ *tal que* $aa^{-1} = a^{-1}a = e$*, ou seja, todos os elementos são inversíveis;*

iv) $\forall a, b \in G, ab = ba$.

Uma observação pertinente é que, quando o grupo G é aditivo, denotamos $e = 0_G$.

Um conceito indispensável para o estudo do tema pesquisado é o de anel. Conforme definido em [4], temos que:

Definição 2.2. *Um* anel *é um conjunto não vazio R dotado de duas operações binárias (geralmente denotadas por adição $(+)$ e multiplicação$(\cdot)$) tal que:*

i) (R,+) é um grupo abeliano;

ii) $\forall a, b, c \in R$, $(ab)c = a(bc)$ *(associatividade da multiplicação);*

iii) $a, b, c \in R$, $a(b + c) = ab + ac$ *e* $(a + b)c = ac + bc$ *(distributividade à esquerda e à direita da multiplicação sobre a adição).*

Se ainda:

iv) $a, b \in R$, $ab = ba$*, se diz que o anel é* comutativo.

Se existe um elemento $1_R \in R$ *tal que*

v) $1_R a = a1_R = a$*, se diz que R é um* anel com identidade.

O conjunto $\{c \in R | cr = rc, \forall r \in R\}$ é chamado de centro do anel R, e denotado por $C(R)$. Se um anel R é comutativo, então todos os seus elementos pertencem ao centro.

Vejamos alguns casos particulares de anéis.

Definição 2.3. *Um anel D com identidade $1_D \neq 0$ em que todos os elementos não nulos são inversíveis é chamado de* anel de divisão. *Um* corpo *é um anel de divisão comutativo.*

Definição 2.4. *Um anel comutativo $(R, +, \cdot)$ com identidade $1_R \neq 0$ é chamado* domínio *ou* domínio de integridade *se satisfaz a seguinte condição:*

$$\forall x, y \in R \backslash \{0\}, \quad xy \neq 0.$$

Uma consequência importante da Definição 2.4 é a lei do cancelamento. Num domínio de integridade R, se $x, y, z \in R$, com $z \neq 0$ e $xz = yz$, segue que $x = y$. A lei do cancelamento será utilizada algumas vezes ao longo deste trabalho. Dessa forma, convém apresentar uma demonstração da validade desta lei. Seja R um domínio de integridade e $x, y, z \in R$ tal que $z \neq 0$ e $xz = yz$. Temos que $xz = yz \Rightarrow xz - yz = 0_R \Rightarrow (x-y)z = 0_R$. Como R é um domínio de integridade, $z = 0_R$ ou $x - y = 0_R$. Por hipótese, $z \neq 0_R$. Portanto, $x - y = 0_R$, de onde se conclui que $x = y$.

Exemplo 2.4.1. *O anel $\mathbb{Z}$ dos números inteiros é um domínio de integridade. O conjunto E dos inteiros pares é um anel comutativo sem identidade.*

Exemplo 2.4.2. *Para qualquer $n \in \mathbb{N}$, o conjunto $\mathbb{Z}_n$ das classes de equivalência módulo n é um anel. Se $p \in \mathbb{Z}$ é primo, então $\mathbb{Z}_p$ é um corpo.*

Um outro conceito relevante para o assunto pesquisado é o de ideal. De acordo com [2], o próprio conceito de ideal surgiu em termos históricos, a partir das tentativas de matemáticos em resolver problemas de fatoração única.

Definição 2.5. *Seja R um anel e S um conjunto não vazio de R que é fechado em relação às operações de R. Se S é um anel com as operações de R, S é chamado de* subanel *de R. Um subanel I de um anel R é um* ideal à esquerda *se*

$$r \in R \text{ e } x \in I \Rightarrow rx \in I;$$

I é um ideal à direita *se*

$$r \in R \text{ e } x \in I \Rightarrow xr \in I;$$

I é um ideal *se for ideal à direita e à esquerda simultaneamente.*

Um ideal I (à esquerda) de R tal que $I \neq \{0\}$ e $I \neq R$ é dito um ideal próprio. Se R é um anel com identidade 1_R e I é um ideal, então $I = R$ se, e somente se, $1_R \in I$. Consequentemente, um ideal não nulo I de R é próprio apenas se I não possui elementos

inversíveis. Supondo que $u \in R$ é inversível e $u \in I$, ter-se-ia que $1_R = u^{-1}u \in I$. Em particular, qualquer anel de divisão D não tem ideais próprios, pois todos os elementos não nulos de D são inversíveis.

Exemplo 2.5.1. *No anel R das matrizes $n \times n$ sobre um anel de divisão D, seja I_k o conjunto de todas as matrizes que têm entradas não nulas apenas na coluna k. Verifica-se que I_k é um ideal à esquerda, mas não é um ideal à direita. Se J_k é o conjunto de todas as matrizes com entradas não nulas apenas na linha k, verifica-se que J_k é um ideal à direita, mas não é um ideal à esquerda.*

Exemplo 2.5.2. *Para qualquer $n \in \mathbb{Z}$, verifica-se que $n\mathbb{Z}$ é um ideal de $\mathbb{Z}$, pois para qualquer $p \in \mathbb{Z}, x = nk \in n\mathbb{Z}$ ocorre que $px = pnk = n(pk) \in n\mathbb{Z}$ e $xp = n(kp) \in n\mathbb{Z}$.*

Exemplo 2.5.3. *Em qualquer anel R, verifica-se que R e $\{0\}$ são ideais de R, conhecidos conhecidos como ideais triviais.*

Um resultado prático para verificar se um determinado subconjunto de um anel é um ideal é apresentado no seguinte teorema:

Teorema 2.6. *Um subconjunto não vazio I de um anel R é um ideal à esquerda (resp. à direita) se, e somente se, para quaisquer $a, b \in I$ e $r \in R$:*

i) $a, b \in I \Rightarrow a - b \in I$; *e*

ii) $a \in I, r \in R \Rightarrow ra \in I$ *(resp.* $ar \in I$*).*

Demonstração. ($\Rightarrow$) Sendo I um ideal, segue que I é um subanel. Ainda, se $a, b \in I$, então $-b \in I$, pois $(I, +)$ é um grupo. Logo, $a + (-b) = a - b \in I$. Além disso, se $a \in I, r \in R$, é trivial que $ar \in I$, pois I é um ideal.
($\Leftarrow$) Inicialmente, observe que $(I, +)$ é um grupo abeliano, pois se verifica que:

i) a associatividade de $(+)$ é herdada de R;

ii) como $a \in I$, então $a - a = 0 \in I$. Logo, existe elemento neutro;

iii) seja $a \in I$. Como $0 \in I, 0 - a = -a \in I$, logo todos os elementos têm inversos aditivos;

iv) comutatividade de $(+)$ é herdada de R.

Ainda, a associatividade de $(\cdot)$ e distributividade também são herdadas de R. Assim, I é um subanel.

Por fim, como $a \in I, r \in R$ implica $ra \in I$, o subanel I é um ideal. □

Teorema 2.7. *Seja R um anel com identidade e $\mathcal{A} = \{A_i | i \in I\}$ uma cadeia de ideais em R. Então, $A = \bigcup_{i \in I} A_i$ é um ideal em R.*

Demonstração. Sejam $a, b \in A$ então $a \in A_i$ e $b \in A_j$ para algum $i, j \in I$. Mas como $\mathcal{A}$ é uma cadeia, tem-se que $A_i \subset A_j$ ou $A_j \subset A_i$. Sem perda de generalidade, suponha que $A_j \subset A_i$. Dessa forma, $a, b \in A_i$. Como A_i é um ideal, segue que $a - b, ra \in A_i$, $\forall r \in R$ (Teorema 2.6). Visto que $A_i \subset A$, $a - b, ra \in A$. Assim, A é um ideal. □

Existem ideais com características específicas que são relevantes para o tema estudado. Isso motiva a seguinte definição:

Definição 2.8. *Seja X um subconjunto de um anel R. Seja $\{A_i | i \in I\}$ a família de todos os ideais (à esquerda) de R que contêm X. Então, $\bigcap_{i \in I} A_i$ é chamado de* ideal (à esquerda) gerado por X, *e denotado (X).*

Um ideal (x) gerado por um único elemento é chamado de ideal principal. Um anel de ideais principais é um anel em que todos os ideais são principais. Se um anel de ideais principais também é um domínio de integridade, será chamado de domínio de ideais principais ou apenas domínio principal.

Exemplo 2.8.1. *$\mathbb{Z}$ é um domínio principal.*

Exemplo 2.8.2. *$\mathbb{Z}[x]$, o anel de polinômios em uma variável sobre $\mathbb{Z}$ não é um domínio principal.*[1]

Exemplo 2.8.3. (Adaptado de [2, p. 258]) *O conjunto $I = \{x \in \mathbb{Z} | 9$ divide $21x\}$ é um ideal principal em $\mathbb{Z}$, gerado pelo elemento 3. De fato, se $x, y \in I$, então $9|21x$ e $9|21y$ e, portanto, 9 é divisor de $21x - 21y = 21(x - y)$, igualdade que mostra que $(x - y) \in I$. Se $x \in I$, então $9|21x$ e daí segue que $9|21(ax)$, qualquer que seja $a \in \mathbb{Z}$, ou seja, $ax \in I$. Pelo Teorema 2.6, conclui-se que I é um ideal. Sendo um ideal em $\mathbb{Z}$, então I é gerado pelo menor de seus elementos estritamente positivos. Uma verificação direta mostra que esse elemento é o número 3. Portanto, $I = (3)$. Ou seja, I é um ideal principal em $\mathbb{Z}$.*

O teorema a seguir é importante para o tema pesquisado.

Teorema 2.9. *Seja R um anel, $a \in R$ e $X \subset R$.*

i) O ideal principal (a) consiste de todos os elementos da forma $ra + as + na + \sum_{i=1}^{m} r_i a s_i$, com $r, s, r_i, s_i \in R, m \in \mathbb{N}^*, n \in \mathbb{Z}$.

[1] Anéis de polinômio serão considerados com mais detalhes no Capítulo 4.

ii) Se R tem identidade, então $(a) = \left\{ \sum_{i=1}^{n} r_i a s_i | r_i, s_i \in R, n \in \mathbb{N} \right\}$.

iii) Se a está no centro de R, então $(a) = \{ra + na | r \in R, n \in \mathbb{Z}\}$.

iv) $Ra = \{ra | r \in R\}$ *(resp.* $aR = \{ar | r \in R\}$*) é um ideal à esquerda (resp. à direita) em R (que pode não conter a). Além disso, se R tem identidade $a \in Ra$ e $a \in aR$.*

v) Se R tem identidade e a está no centro de R, então $Ra = (a) = aR$.

vi) Se R tem identidade e X está no centro de R, então (X) consiste em todas as somas finitas $r_1 a_1 + \ldots + r_n a_n$ $(n \in \mathbb{N}^*, r_i \in R, a_i \in X)$.

Demonstração. i) Sejam $r' \in R$ e $a' \in I$, onde I é o conjunto de todos os elementos da referida forma. Então,

$$\begin{aligned} r'a' &= r'\left(ra + as + na + \sum_{i=1}^{m} r_i a s_i\right) \\ &= r'ra + r'as + r'na + r'\sum_{i=1}^{m} r_i a s_i \\ &= r'ra + r'na + r'as + r'\sum_{i=1}^{m} r_i a s_i \\ &= (r'r + r'n)a + \sum_{i=1}^{m+1} r'_i a s_i \ , \end{aligned}$$

onde $r'_i = r'r_i, r_{m+1} = r'$ e $s_{m+1} = s$.

Nota-se que $(r'r + r'n)a + \sum_{i=1}^{m+1} r'_i a s_i \in I$ pelo fato de que $r'r + nr' \in R$. Conclui-se que I é um ideal à esquerda pois, dado $r' \in R, a' \in I$, segue que $r'a' \in I$. Analogamente, I é um ideal à direita. Ainda, se $r = s = r_i = s_i = 0, n = 1$, então $a \in I$.

Seja, agora, I' qualquer ideal que contém a. Segue que $ra \in I'$ e $r_i a \in I'$, pois I' é um ideal (à esquerda) por hipótese.

Ainda, $as, r_i a s_i \in I'$, pois I' também é um ideal à direita.

Por fim, $na = \underbrace{a + a + \ldots + a}_{n-\text{vezes}} \in I'$, pois I' é um subanel de R (fechado para a adição). Daí segue que $ra + as + na + \sum_{i=1}^{m} r_i a s_i \in I'$ e $I \subseteq I'$. Isso significa que I é um subconjunto de qualquer ideal que contém a, ou seja, I está contido na interseção de todos os I'. Logo, $I = (a)$.

ii) Se R tem identidade 1_R, é possível indexar os elementos ra, as e na como elementos da forma $r_i a s_i$, a fim de que possam ser descritos por meio do somatório. Isso se

dá reescrevendo os elementos em questão da seguinte maneira: $ra = ra1_R = r_{m+1}as_{m+1}$, $as = 1_Ras = r_{m+2}as_{m+2}$ e $na = n(1_Ra) = (n1_R)a1_R = r_{m+3}as_{m+3}$. Assim, qualquer elemento de (a) é da forma $ra + as + na + \sum_{i=1}^{m} r_i as_i = \sum_{i=1}^{m+3} r_i as_i$.

iii) Se a está no centro de R, qualquer elemento de (a) é da forma

$$\begin{aligned} ra + as + na + \sum_{i=1}^{m} r_i as_i &= ra + sa + na + \sum_{i=1}^{m} r_i s_i a \\ &= \left(r + s + \sum_{i=1}^{m} r_i s_i \right) a + na \\ &= r'a + na \ , \end{aligned}$$

onde $r' = r + s + \sum_{i=1}^{m} r_i s_i$.

iv) Sejam $p, s, q \in R$. Temos que $pa - sa = (p - s)a = r'a \in Ra, r' \in R$ e $qsa = (qs)a = r''a \in Ra, r'' \in R$. Portanto, Ra é ideal à esquerda pelo Teorema 2.6. De modo análogo, mostramos que aR é um ideal à direita.

Se $1_R \in R$ é a identidade, basta escrever $a = a1_R \in aR$. Analogamente, temos $1_Ra \in Ra$.

v) Pelo item iii), temos

$$\begin{aligned} (a) &= \{ra + na | r \in R, n \in \mathbb{Z}\} \\ &= \{ra + (n1_R)a | r \in R, n \in \mathbb{Z}\} \\ &= \{(r + n1_R)a | r \in R, n \in \mathbb{Z}\} \\ &= \{r'a | r' \in R\} \\ &= Ra. \end{aligned}$$

Como a está no centro de R, $r'a = ar' \forall r' \in R$ e, assim, $(a) = Ra = aR$.

vi) Seja R um anel com identidade e X um subconjunto contido no centro de R. Seja I um ideal que contém X e $a_i \in X$. Como I é um ideal que contém a_i, então I deve conter (a_i) (o "menor" ideal contendo a_i). Como, por (v), $(a_i) = Ra_i$, segue que I deve conter $Ra_i = \{ra_i | r \in R\}$.

Sendo I um ideal, o elemento $r_1a_1 + r_2a_2 + \cdots + r_na_n$ pertence a I. Considere $I' = \{r_1a_1 + \cdots + r_na_n | r_i \in R, a_i \in X\}$. Consequentemente, $I' \subseteq I$. Para algum $r \in R$ e $r_1a_1 + \cdots + r_na_n \in I'$, o elemento $r\,(r_1a_1 + \cdots + r_na_n) = (rr_1)a_1 + \cdots + (rr_n)a_n \in I'$, implicando que I' é um ideal à esquerda. Como a_i está no centro de R, I' também é um ideal à direita.

Temos, assim, que I' é um ideal de R que está contido em qualquer ideal que

contém X. Isto é, I' está contido na intercessão de todos os ideais que contêm X. Assim, conclui-se que $I' = (X)$. □

Dado um anel R, é possível definir operações com conjuntos. Sejam $A_1, \ldots, A_n$ subconjuntos não vazios de um anel R. A adição de $A_1, \cdots, A_n$ é definida da seguinte maneira: $A_1 + A_2 + \cdots + A_n = \{a_1 + a_2 + \cdots + a_n | a_i \in A, i = 1, 2, \ldots, n\}$. Se A e B são conjuntos não vazios de um anel R, o produto AB é denotado pelo conjunto de todas as somas finitas $\{a_1b_1 + \cdots + a_nb_n \mid n \in \mathbb{N}^*, a_i \in A, b_i \in B\}$. Se os conjuntos A_i são ideais de R, o seguinte teorema garante que a soma de ideais é um ideal.

Teorema 2.10. *Sejam $A_1, A_2, \ldots, A_n$ ideais (à esquerda) de um anel R. Então, a adição $A_1 + A_2 + \cdots + A_n$ é um ideal (à esquerda) de R.*

Demonstração. Sejam $x, y \in A_1 + A_2 + \cdots + A_n$. Temos que $x = a_1 + a_2 + \cdots + a_n$ e $y = a'_1 + a'_2 + \cdots + a'_n$. Segue que

$$\begin{aligned} x - y &= (a_1 + a_2 + \cdots + a_n) - (a'_1 + a'_2 + \cdots + a'_n) \\ &= a_1 + a_2 + \cdots + a_n - a'_1 - a'_2 - \cdots - a'_n. \end{aligned}$$

Como R é um grupo abeliano, é possível associar os elementos da seguinte forma: $(x - y) = (a_1 - a'_1) + (a_2 - a'_2) + \cdots + (a_n - a'_n)$. Visto que cada A_i é um ideal, segue que $(a_i - a'_i) \in A_i$, para cada i. Assim, $x - y \in A_1 + A_2 + \cdots + A_n$.

Seja $r \in R$. Temos que $rx = r(a_1 + a_2 + \cdots + a_n) = ra_1 + ra_2 + \cdots + ra_n$. Como cada A_i é um ideal, $ra_i \in A_i$ para cada i. Assim, $rx \in A_1 + A_2 + \cdots + A_n$.

Conclui-se, pelo Teorema 2.6, que $A_1 + A_2 + \cdots + A_n$ é um ideal de R.

□

Se A e B são ideais de um anel R, então o produto de conjuntos AB tal qual definido anteriormente também é um ideal de R. A demonstração é análoga à do Teorema 2.10.

Dois tipos de ideais que merecem destaque para o desenvolvimento do trabalho serão caracterizados a seguir, a saber, são os ideais primos e maximais.

Definição 2.11. *Um ideal P de um anel R é* primo *se $P \neq R$ e, para quaisquer ideais $A, B \subset R$,*

$$AB \subset P \quad \Rightarrow \quad A \subset P \text{ ou } B \subset P.$$

Teorema 2.12. *Se P é um ideal de um anel R tal que $P \neq R$ e para todo $a, b \in R$*

$$ab \in P \Rightarrow a \in P \text{ ou } b \in P,$$

então P é primo. Por outro lado, se P é primo e R é comutativo, a recíproca é verdadeira.

Demonstração. Sejam A e B ideais tais que $AB \subset P$ mas $A \not\subset P$. Então existe $a \in A - P$. Para todo $b \in B$, $ab \in AB \subset P$. Mas por hipótese, $ab \in P$ implica $a \in P$ ou $b \in P$. Como $a \notin P$, segue que $b \in P$. Logo, $B \subset P$, isto é, P é primo.

Como P é um ideal e $ab \in P$, segue que $(ab) \subset P$. Agora, se presumimos que R é comutativo, $(a)(b) \subset (ab) \subset P$.

Essa contingência se dá pelo seguinte motivo:

$$\begin{aligned}
(a)(b) &= \{r_1 a s_1 b + \cdots + r_n a s_n b \mid n \in \mathbb{N}^*, r_i, s_i \in R\} \\
&= \{r_1 s_1 ab + \cdots + r_n s_n ab \mid n \in \mathbb{N}^*, r_i, s_i \in R\} \\
&= \{q_1 ab + \cdots + q_n ab \mid n \in \mathbb{N}^*, q_i = r_i s_i \in R\} \\
&= \{(q_1 + \cdots + q_n)ab \mid n \in \mathbb{N}^*, q_i = r_i s_i \in R\} \\
&= \{qab \mid q = q_1 + \cdots q_n \in R, n \in \mathbb{N}^*\} \subset (ab)
\end{aligned}$$

Como P é primo, $(a) \subset P$ ou $(b) \subset P$, concluindo-se que $a \in P$ ou $b \in P$. □

Exemplo 2.12.1. *O ideal $2\mathbb{Z} = \{x \in \mathbb{Z} | x = 2k, k \in \mathbb{Z}\}$ é primo em $\mathbb{Z}$, pois se $ab \in 2\mathbb{Z}$, temos que $2|ab$ e, como 2 é primo, $2|a$ ou $2|b$. Assim, $a \in 2\mathbb{Z}$ ou $b \in 2\mathbb{Z}$.*

Definição 2.13. *Um ideal M em um anel R é* maximal *se $M \neq R$ e para qualquer ideal N tal que $M \subset N \subset R$ se tem que ou $N = M$ ou $N = R$.*

Exemplo 2.13.1. *Considere o anel $\mathbb{Z}$. O ideal (3) dos múltiplos de 3 é maximal em $\mathbb{Z}$. No entanto, o ideal (4) não é maximal, pois $(4) \subsetneq (2) \subsetneq \mathbb{Z}$.*

Teorema 2.14. *Seja R um anel comutativo com identidade. Todo ideal maximal M de R é primo.*

Demonstração. Suponha que M não seja primo, isto é, existem elementos $a, b \in R$ tais que $ab \in M$ mas $a \notin M$ e $b \notin M$. Como a soma de ideais é um ideal (Teorema 2.10), temos que $(a) + M$ e $(b) + M$ são ideais em R.

Como $a \notin M$, temos que $M \subsetneq (a) + M$ e, como $b \notin M$, $M \subsetneq (b) + M$.

Da hipótese de que M é maximal, é necessário que $R = (a) + M = (b) + M$. Ainda, como $1 \in R$, existem $r \in R$, $m \in M$ tais que $1 = ar + m$ e $s \in R$, $n \in M$ tais que $1 = bs + n$. Temos:

$$\begin{aligned}
1 = 1 \cdot 1 &= (ar + m)(bs + n) \\
&= abrs + arn + mbs + mn
\end{aligned}$$

Nota-se que $abrs + arn + mbs + mn \in M$, pois $ab, n, m \in M$.

Daí, $1 \in M$. Mas já foi exposto que, para qualquer ideal M, $1 \in M \Leftrightarrow M = R$, contradizendo a hipótese de que M é maximal. Por isso, se $ab \in M$, deve-se ter $a \in M$ ou $b \in M$, implicando M ser primo. Logo, todo ideal maximal é primo. □

Observa-se, entretanto, que a recíproca do Teorema 2.14 não é verdadeira. Como contraexemplo, observamos que o ideal $\{0\} \times \mathbb{Z}$ é primo em $\mathbb{Z} \times \mathbb{Z}$, mas não é maximal.

Teorema 2.15. *Num anel não nulo R com identidade, ideais maximais sempre existem. Ainda, todo ideal em R (exceto o próprio R) está contido num ideal maximal.*

A fim de demonstrar esse teorema, é necessário ter em mente o Lema de Zorn, enunciado a seguir.

Lema 2.16 (Lema de Zorn)**.** *Se A é um conjunto não vazio parcialmente ordenado tal que toda cadeia em A tem um limitante superior em A, então A contém um elemento máximo.*

A demonstração do Lema 2.16 não será realizada por se desviar um pouco do escopo do trabalho. No entanto, a mesma pode ser encontrada em [4, p. 10]. Não obstante, algumas considerações se fazem pertinentes para a compreensão adequada do resultado. Um conjunto parcialmente ordenado é um conjunto não vazio A com uma relação $\leq$ em $A \times A$, que é reflexiva, transitiva e antissimétrica. O conjunto parcialmente ordenado pode ser denotado por $(A, \leq)$.

Dois elementos $a, b \in A$ são comparáveis se $a \leq b$ ou $b \leq a$. No entanto, num conjunto parcialmente ordenado, não é necessário que dois elementos quaisquer sejam comparáveis.

Uma ordem parcial de um conjunto A na qual quaisquer dois elementos são comparáveis recebe o nome de ordem linear (ou total), e o conjunto é dito linearmente ordenado.

Um elemento $a \in A$ é um elemento máximo em A se para qualquer $c \in A$ que é comparável com a, ocorre que $c \leq a$. Note que não é necessário termos $c \leq a$ para todo $c \in A$, apenas para os c que são comparáveis com a.

Seja $B \subset A$ um subconjunto não vazio. Um limitante superior de B é um elemento $d \in A$ tal que $b \leq d$ para todo $b \in B$. Um subconjunto não vazio $B \subset A$ que é linearmente ordenado é chamado de cadeia em A. Informações mais detalhadas acerca da ordenação em conjuntos, que porventura se fujam dos objetivos do trabalho, podem ser encontradas em [4]

Demonstração do Teorema 2.15. Observe que 0_R é um ideal próprio, pois $R \neq 0_R$ por hipótese. Se 0_R for o único ideal próprio de R, garante-se que ele é maximal. Seja A um ideal próprio de R e $\mathcal{S}$ o conjunto de todos os ideais B tal que $A \subset B \neq R$, isto é, o conjunto de todos os ideais próprios de R que contêm A. Note que $\mathcal{S} \neq \emptyset$, pois

$A \subset \mathcal{S}$. É possível estabelecer uma relação de ordem parcial em $\mathcal{S}$ por meio da inclusão de conjuntos, com a relação de ordem definida por $B_1 \leq B_2 \iff B_1 \subset B_2$. A fim de aplicar o Lema 2.16 é necessário mostrar que toda cadeia $\mathcal{C} = \{C_i | i \in I\}$ de ideais em $\mathcal{S}$ tem um limitante superior em $\mathcal{S}$.

Seja $C = \bigcup_{i \in I} C_i$. Pelo Teorema 2.7, C é um ideal.

Ainda, $A \subset C_i \ \forall i \in I$, pois por definição, cada C_i é um ideal próprio de R em $\mathcal{S}$ que contém A. Assim, $A \subset \bigcup_{i \in I} C_i = C$. Como cada $C_i \in \mathcal{S}$, $C_i \neq R$. Segue que $1_R \notin C_i$ e, por conseguinte, $1_R \notin \bigcup_{i \in I} C_i = C$. Assim, $C \neq R$, implicando que $C \in \mathcal{S}$.

Como a ordenação de $\mathcal{S}$ é dada pela inclusão de conjuntos, tem-se que C limita superiormente a cadeia $\mathcal{C}$, pois para todo $i \in I$, $C_i \subset \bigcup_{i \in I} C_i = C$. Visto que $C \in \mathcal{S}$, $\mathcal{S}$ tem um limitante superior e, portanto, um elemento máximo (Lema 2.16).

Tendo em vista que os elementos de $\mathcal{S}$ são ideais próprios de R, o elemento máximo de $\mathcal{S}$ é um ideal que contém todos os outros ideais próprios de R. Portanto, tal elemento é um ideal maximal.

□

As definições e teoremas apresentados até o momento possibilitam a compreensão da fatoração e divisibilidade em anéis comutativos, tema a ser tratado no capítulo seguinte.

3 FATORAÇÃO E DIVISIBILIDADE

Tomando como base o referencial teórico apresentado anteriormente, é possível construir as seguintes definições a respeito dos conceitos de divisibilidade e fatoração em anéis comutativos.

Definição 3.1. *Um elemento a não nulo de um anel comutativo R* divide *um elemento $b \in R$ (notação: $a|b$) se existir $x \in R$ tal que $ax = b$. Os elementos $a, b \in R$ são ditos* associados *se $a|b$ e $b|a$.*

Praticamente todas as definições acerca de divisibilidade em anéis comutativos podem ser formuladas em termos de ideais principais, como ilustrado no seguinte teorema:

Teorema 3.2. *Sejam a, b e u elementos de um anel comutativo R com identidade.*

i) $a|b$ *se, e somente se,* $(b) \subset (a)$.

ii) *a e b são associados se, e somente se,* $(a) = (b)$.

iii) *u é inversível se, e somente se,* $u|r$ *para todo* $r \in R$.

iv) *u é inversível se, e somente se,* $(u) = R$.

v) *A relação "a é associado a b" é uma relação de equivalência em R.*

vi) *Se $a = br$ com $r \in R$ inversível, então a e b são associados. Se R é um domínio de integridade, a recíproca é verdadeira.*

Demonstração. i) ($\Rightarrow$) Como $a|b$, existe $x \in R$ tal que $ax = b$. Como R é comutativo, $xa = b$. Seja $m \in (b)$. Tem-se que $m = rb$ para algum $r \in R$. Como $a|b$, $m = rax = rxa$. Como $r, x \in R$, $\quad rx \in R$. Logo, $m = (rx)a \in (a)$. Assim, $(b) \subset (a)$.
($\Leftarrow$) Note que $b = b \cdot 1_R \in (b)$. Como $(b) \subset (a)$ por hipótese, $b \in (a)$, isto é, $b = ar$, para algum $r \in R$. Portanto, $a|b$.

ii) ($\Rightarrow$) Será mostrado que $(a) \subset (b)$ e $(b) \subset (a)$. De fato, como $a|b$, temos que $(b) \subset (a)$ pelo item (i); como $b|a$, $(a) \subset (b)$ pelo mesmo item. Logo, $(a) = (b)$.
($\Leftarrow$) Como $(a) = (b)$, temos que $(a) \subset (b)$ e $(b) \subset (a)$. Pelo item (i), segue que $b|a$ e $a|b$, isto é, a e b são associados.

iii) ($\Rightarrow$) Seja $u \in R$ um elemento inversível. Dado $r \in R$, temos $r = 1_R r = uu^{-1}r$. Como $u^{-1}r \in R$, basta tomar $x = u^{-1}r$. Segue que $r = ux$, isto é, $u|r$.

($\Leftarrow$) Como $u|r, \forall r \in R$, em particular, $u|1_R$. Assim, existe $x \in R$ tal que $ux = 1_R$. Como R é comutativo, $ux = 1_R = xu$. Portanto, u é inversível.

iv)($\Rightarrow$) É necessário lembrar que, pelo Teorema 2.9, $(u) = \{ru | r \in R\} = \{ur | r \in R\}$. Tem-se que $(u) \subset R$ pelo fato de (u) ser um ideal. Será mostrado que $R \subset (u)$. Seja $r \in R$. Como u é inversível, existe $u^{-1} \in R$ tal que $uu^{-1} = 1_R = u^{-1}u$. Segue que $r = r1_R = ru^{-1}u = r'u \in (u)$, pois $ru^{-1} \in R$. Assim, $R \subset (u)$ e, consequentemente, $R = (u)$.
($\Leftarrow$) Como $(u) = R$ e $1_R \in R$, então $1_R \in (u)$. Logo, existe $k \in R$ tal que $uk = ku = 1_R$, ou seja, u é inversível.

v) É necessário mostrar que a relação "a e b são associados" é reflexiva, simétrica e transitiva. De fato, sejam $a, b, c \in R$:

- Verifica-se que $a|a$, pois $a = a1_R$ e $1_R \in R$. Portanto, $a|a$, isto é, a é associado a a e a relação é reflexiva.

- Supondo que $a|b$ e $b|a$. Então b é associado a a, pois $b|a$ e $a|b$. Desse modo, observa-se que a relação é simétrica.

- Dados $a, b, c \in R$ tais que a e b são associados e b e c são associados. Será mostrado que a e c são associados. Como $a|b$ e $b|c$, segue que

$$ax = b \text{ e } bx' = c \Rightarrow axx' = c \Rightarrow ax'' = c.$$

  Como $x'' = xx' \in R$, temos que $a|c$. Como $b|a$ e $c|b$, temos:

$$by = a \text{ e } cy' = b \Rightarrow cy'y = a \Rightarrow cy'' = a,$$

  onde $y'y = y'' \in R$. Logo, $c|a$. Conclui-se que a e c são associados e a relação é transitiva.

Consequentemente, a relação em questão é uma relação de equivalência.

vi) Como $a = br$, $b|a$. Pelo fato de r ser inversível, existe $r^{-1} \in R$ e, assim, $ar^{-1} = b$, isto é, $a|b$. Portanto, a e b são associados.
A recíproca pode ser escrita da seguinte maneira: se a e b são associados, então $a = br$, com r inversível. Suponha que R é um domínio de integridade e que $a|b$ e $b|a$. Logo, $br = a$ e $am = b$, para $r, m \in R$. Logo, $(am)r = a$. Pela lei do cancelamento, segue que $mr = 1_R$, isto é, r é inversível. □

Exemplo 3.2.1. *Considere o anel* $\mathbb{Z}$. *Tem-se que* $(4) \subset (2)$ *e* $2|4$ (i). *Ainda em* $\mathbb{Z}$, *percebe-se que* $(-1) = \{(-1)n \mid n \in \mathbb{Z}\} = \mathbb{Z}$ *e verifica-se que* -1 *é inversível em* $\mathbb{Z}$ (iv).

A noção de elementos irredutíveis e primos é fundamental para o tema pesquisado, pois os domínios de fatoração única a serem estudados posteriormente são definidos em termos desses elementos.

Definição 3.3. *Seja R um anel comutativo com identidade. Um elemento $c \in R$ é dito* irredutível *se:*

i) c é não nulo e não inversível;

ii) para quaisquer $a, b \in R$, $c = ab \Rightarrow$ a ou b é inversível.

Um elemento $p \in R$ é dito primo *se:*

i) p é não nulo e não inversível;

ii) para quaisquer $a, b \in R$, $p|ab \Rightarrow p|a$ ou $p|b$.

Exemplo 3.3.1. *Se $p \in \mathbb{Z}$ é primo, então $-p$ e p são elementos irredutíveis e primos no mesmo sentido da Definição 3.3. Agora, no anel $\mathbb{Z}_6$ dos restos da divisão por 6, tem-se que $\overline{2}$ é primo. Contudo, $\overline{2} \in \mathbb{Z}_6$ não é irredutível, visto que $\overline{2} = \overline{2} \cdot \overline{4}$, mas nem $\overline{2}$ nem $\overline{4}$ são inversíveis em $\mathbb{Z}_6$.*

Elementos primos (resp. irredutíveis) possuem uma relação muito próxima com ideais principais primos (resp. maximais) num anel R, como ilustra o teorema a seguir.

Teorema 3.4. *Sejam p e c elementos não nulos de um domínio de integridade R.*

i) p é primo se, e somente se, (p) é um ideal primo não nulo.

ii) c é irredutível se, e somente se, (c) é maximal no conjunto S de todos os ideais próprios de R.

iii) Todo o elemento primo de R é irredutível.

iv) Se R é um domínio principal, então p é irredutível se, e somente se, p é primo.

v) Todo associado de um elemento irredutível (resp. primo) de R é irredutível (resp. primo).

vi) Os únicos divisores de um elemento irredutível de R são seus associados e os elementos inversíveis de R.

Demonstração. i) ($\Rightarrow$) Como p é primo, $p \neq 0$ e, assim, $(p) \neq 0$. Ainda, como p não é inversível, pelo Teorema 3.2(iv), segue que $(p) \neq R$. Sejam $a, b \in R$ tais que $ab \in (p)$. Segue que ab é da forma rp, com $r \in R$, isto é, $ab = rp$, o que implica que $p|ab$. Como p é primo, $p|a$ ou $p|b$. Se $p|a$ existe $x \in R$ tal que $a = px$, isto é, $a \in (p)$; se $p|b$, existe $y \in R$ tal que $b = py$, isto é, $b \in (p)$. Logo, (p) é primo.
($\Leftarrow$) Se (p) é um ideal primo e $p|ab$, então existe $r \in R$ tal que $ab = rp$. Logo, $ab \in (ab)$ e segue que $a \in (p)$ ou $b \in (p)$. Se $a \in (p)$, $p|a$; se $b \in (p), p|b$. Logo, p é primo.

ii) ($\Rightarrow$) Como c não é inversível, $(c) \neq R$. Suponha que (c) não é maximal em S, isto é, existe um ideal $(a) \neq R$ tal que $(c) \subsetneq (a)$. Como $c \in (c)$ (pois R é comutativo e tem identidade), segue que $c \in (a)$. Assim, $c = ar$, para algum $r \in R$.
Dado que c é irredutível, a ou r são inversíveis. Se a for inversível, $(a) = R$, o que não ocorre. Se r é inversível e como $c = ar$, então c e a são associados (Teorema 3.2 (vi)), isto é, $c|a$ e $a|c$. Como $c|a$, $(a) \subset (c)$ (Teorema 3.2(i)). Como, por hipótese $(c) \subsetneq (a)$, segue que $(a) = (c)$, que é uma contradição. Logo, (c) é maximal em S.
($\Leftarrow$) Será mostrado que, se (c) é maximal em S, então c é irredutível. De fato, como (c) é maximal em S por hipótese, $(c) \neq R$ e $(c) \neq \{0\}$. Logo, c não é inversível (Teorema 3.2(iv)) e $c \neq 0$. Se $c = ab$ para algum $a, b \in R$, temos que $a|c$ e, assim, $(c) \subset (a)$ (Teorema 3.2(i)). Como (c) é maximal em S por hipótese, segue que $(c) = (a)$ ou $(a) = R$.

Se $(a) = R$, a é inversível (Teorema 3.2(iv)); se $(c) = (a)$, a e c são associados, isto é, $a|c$ e $c|a$. Como $c|a, a = cd$ para algum $d \in R$. Assim,

$$a = cd = abd \Rightarrow 1_R = bd,$$

pois a lei do cancelamento é válida num domínio de integridade. Tendo em vista que $1_R = bd$, segue que b é inversível. Assim, dado que $c \neq 0$ não é inversível e $c = ab$ implica que a ou b são inversíveis, conclui-se que c é irredutível.

iii) Seja $p \in R$ primo, e $a, b \in R$ tais que $p = ab$. Note que $p|ab$, pois $p = p1_R = ab$. Como p é primo, $p|a$ ou $p|b$. Se $p|a$, $a = pr$, para algum $r \in R$. Segue que $a = pr = abr$ e, consequentemente, $1_R = br$. Portanto, b é inversível e conclui-se que p é irredutível. Se $p|b$, de modo análogo mostra-se que a é inversível.

iv) ($\Leftarrow$) Seja R um domínio principal e $p \in R$ primo. Como consequência imediata do item anterior, p é irredutível.
($\Rightarrow$) Seja $p \in R$ irredutível. Segue que (p) é maximal no conjunto S de todos os ideais próprios de R (pelo item (ii)). Como p é irredutível, segue que (p) é maximal (item (ii)). Ainda, tem-se que (p) é primo pelo Teorema 2.14. Conclui-se, pelo item (i), que p é primo.

v) Vamos mostrar que, se $c \in R$ é irredutível e $d \in R$ é associado a c, então d é irredutível. De fato, $c = du$, com u inversível (Teorema 3.2, recíproca do item (vi), pois R é

um domínio de integridade). Inicialmente, note que $d \neq 0$, pois se $d = 0$, $c = du = 0u = 0$, contradizendo o fato de que c é irredutível. Se $d = ab$, com $a, b \in R$, então $c = du = abu$. Segue que a é inversível ou bu o é. Se a é inversível, segue que $d = ab$ é irredutível; se bu é inversível, segue que b também o é, pois $b^{-1} = b^{-1}u^{-1}u = (ub)^{-1} = (bu)^{-1}u$. Agora, $b\,[(bu)^{-1}u] = bu(bu)^{-1} = 1_R$. Logo, $d = ab$ é irredutível.

vi) Seja $r \in R$ irredutível e $u \in R$ inversível. Pelo Teorema 3.2 (iii), temos que $u|r$. Seja $p \in R$ tal que p e r são associados, isto é, $p|r$ e $r|p$, segue que p é divisor de r. Suponha que existe $q \in R$ tal que $q|r$ e q não é inversível. Segue que $r = qm$, para algum $m \in R$. Como r é irredutível, m é inversível. Logo, r e q são associados (Teorema 3.2(vi)). Conclui-se, dessa forma, que os únicos divisores de um elemento $r \in R$ são seus associados e os elementos inversíveis de R.

□

A partir da demonstração apresentada é possível perceber que várias partes do Teorema 3.4 são válidas para anéis comutativos arbitrários.

As definições expostas até o momento num anel comutativo arbitrário são as análogas dos conceitos de divisibilidade e números primos no anel $\mathbb{Z}$. Na verdade, tratam-se das mesmas definições, visto que $\mathbb{Z}$ é um caso particular de anel comutativo.

Como cada elemento em $\mathbb{Z}$ pode ser escrito de forma única como um produto finito de elementos irredutíveis, tem-se que $\mathbb{Z}$ é um exemplo de domínio de fatoração única (também dito domínio fatorial ou DFU).

Definição 3.5. *Um domínio de integridade R é um* domínio de fatoração única *se:*

i) todo elemento não nulo e não inversível a em R pode ser escrito como $a = c_1c_2 \ldots c_n$, com $c_1, \ldots, c_n$ irredutíveis;

ii) se $a = c_1c_2 \ldots c_n$ e $a = d_1d_2 \ldots d_m$ (c_i, d_j irredutíveis), então $n = m$ e para alguma permutação σ de $\{1, 2, \ldots, n\}$, c_i e $d_{\sigma(i)}$ são associados para todo i.

Algumas observações se fazem pertinentes. Inicialmente, note-se que é necessário que um domínio de fatoração única seja um domínio de integridade. Se esse não fosse o caso, não seria possível garantir que o produto de dois elementos não nulos fosse também não nulo; em segundo lugar, observa-se que num domínio de fatoração única, elementos irredutíveis são também primos. Portanto, elementos primos e irredutíveis são os mesmos nessa estrutura. Já se há mostrado que em um domínio de integridade (em particular, num domínio de fatoração única), elementos primos são irredutíveis. O seguinte teorema mostra a recíproca.

Teorema 3.6. *Em um domínio fatorial R, elementos irredutíveis são primos.*

Demonstração. Seja R um DFU e $p \in R$ com p irredutível. Sejam $a, b \in R$ tais que $p|ab$, isto é, $ab = pc$, com $c \in R$. Pela condição (i) da Definição 3.5, a, b e c podem ser fatorados em elementos irredutíveis. Sejam $a = a_1 \cdots a_n$, $b = b_1 \cdots b_m$ e $c = c_1 \cdots c_k$, com a_i, b_i e c_i irredutíveis a fatoração dos elementos a, b e c. Segue que $ab = a_1 \cdots a_n b_1 \cdots b_m$ e $pc = pc_1 \cdots c_k$. Como $ab = pc$, segue que $a_1 \cdots a_n b_1 \cdots b_m = p(c_1 \cdots c_k)$. Tendo em vista que R é um domínio fatorial, pela condição (ii) da Definição 3.5, observa-se que $n + m = k + 1$ e p é associado a algum dos fatores a_i de a ou a algum dos fatores b_i de b. Portanto, $p|a$ ou $p|b$. Conclui-se, assim, que p é primo. □

Por fim, ressalta-se que a Definição 3.5(ii) não é trivial, pois existem domínios de integridade nos quais todos os elementos podem ser fatorados como um produto finito de irredutíveis, mas em que essa fatoração não é única. Um domínio de integridade com essa propriedade é ilustrado no exemplo a seguir.

Exemplo 3.6.1. Adaptado de [4]. Considere $R = \{a + b\sqrt{10} | a, b \in \mathbb{Z}\} = \mathbb{Z}[\sqrt{10}]$ um subanel do corpo $\mathbb{R}$ e uma função $N : R \to \mathbb{Z}$ definida por $a + b\sqrt{10} \mapsto (a + b\sqrt{10})(a - b\sqrt{10}) = a^2 - 10b^2$. A função N, chamada norma, é tal que $N(uv) = N(u)N(v)$, $\forall u, v \in R$ e $N(u) = 0$ se, e somente se, $u = 0$.

De fato, sejam $u = a + b\sqrt{10}$ e $v = c + d\sqrt{10}$. Verifica-se

$$\begin{aligned} N(uv) = &\quad N(ac + ad\sqrt{10} + bc\sqrt{10} + 10bd) \\ = &\quad N((ac + 10bd) + (ad + bc)\sqrt{10}) \\ = &\quad (ac)^2 + 20acbd + 100(bd)^2 - 10((ad)^2 + 2adbc + (bc)^2) \\ = &\quad (ac)^2 - 10(ad)^2 - 10(bc)^2 + 100(bd)^2, \end{aligned}$$

enquanto que

$$\begin{aligned} N(u)N(v) &= (a^2 - 10b^2)(c^2 - 10d^2) \\ &= (ac)^2 - 10(ad)^2 - 10(bc)^2 + 100(bd)^2. \end{aligned}$$

Portanto, $N(uv) = N(u)N(v)$. A partir disso, é possível inferir outro resultado referente à função norma: se $u|v$, então $N(u)|N(v)$. De fato, se $u|v$, existe $k \in \mathbb{Z}[\sqrt{10}]$ tal que $v = uk$. Pelo que foi demonstrado anteriormente, $N(v) = N(uk) = N(u)N(k)$, ou seja, $N(u)|N(v)$.

Agora, se $u = 0 = 0 + 0\sqrt{10}$, $N(u) = 0^2 - 10 \cdot 0^2 = 0$. Reciprocamente, se $N(u) = 0$, seque que

$$\begin{aligned} a^2 - 10b^2 &= 0 \\ a^2 &= 10b^2 \\ a &= \pm b\sqrt{10}. \end{aligned}$$

Como $a, b \in \mathbb{Z}$, a única solução é $a = b = 0$, ou seja, $u = 0$.

Observa-se ainda que $u \in R$ é inversível se, e somente se, $N(u) = \pm 1$. Suponha que $u = a + b\sqrt{10}$ é inversível, isto é, existe $u^{-1} = c + d\sqrt{10} \in R$ tal que $uu^{-1} = 1$. Temos que $N(u)N(u^{-1}) = N(uu^{-1}) = N(1) = 1$. Como $N(u), N(u^{-1}) \in \mathbb{Z}$, a única solução para a $N(u)N(u^{-1}) = 1$ é $N(u) = N(u^{-1}) = 1$ ou $N(u) = N(u^{-1}) = -1$. Portanto, $N(u) = \pm 1$.

Reciprocamente, se $N(u) = \pm 1$, segue que $a^2 - 10b^2 = \pm 1$, o que implica que $(a + b\sqrt{10})(a - b\sqrt{10}) = \pm 1$. Como $a + b\sqrt{10} \in R$, segue que $\pm(a - b\sqrt{10})$ é o inverso de u.

Considere os elementos $2, 3, 4 + \sqrt{10}$ e $4 - \sqrt{10}$. Note que, pelo provado acima, os elementos elencados não são inversíveis pois $N(2) = 4, N(3) = 9, N(4 \pm \sqrt{10}) = 6$. Contudo, os elementos são irredutíveis, como se demonstra a seguir:

- 2 é irredutível. Suponha, por absurdo, que 2 não seja irredutível. Como 2 é não nulo e não inversível (pois $N(2) \neq \pm 1$), resta supor que existem $u, v \in R$ tais que $2 = uv$, com u, v não inversíveis. Segue que

$$4 = N(2) = N(uv) = N(u)N(v).$$

  Como $N(u) \neq \pm 1$ e $N(v) \neq \pm 1$, segue que $N(u) = N(v) = \pm 2$.

  Mostrar-se-á que tais elementos não existem em $\mathbb{Z}[\sqrt{10}]$. De fato, se $u = a + b\sqrt{10}$, verifica-se que $N(u) = a^2 - 10b^2 = \pm 2$. Reduzindo a módulo 5, observa-se que $a^2 - 10b^2 \equiv 2 \pmod 5$. Como $10 \equiv 0 \pmod 5$, segue que $a^2 \equiv 2 \pmod 5$.

  Após testar cada elemento de $\mathbb{Z}_5$, verifica-se que não existe $a \in \mathbb{Z}_5$ tal que $a^2 \equiv 2 \pmod 5$. Portanto, não existe $u \in R$ tal que $N(u) = \pm 2$.

  Assim, 2 não é irredutível em $\mathbb{Z}[\sqrt{10}]$.

- 3 é irredutível. Suponha, por absurdo, que 3 não seja irredutível. Como 3 é não nulo e $N(3) \neq \pm 1$, devem existir $u, v \in \mathbb{Z}[\sqrt{10}]$ não inversíveis tais que $3 = uv$. Teríamos, então,

$$N(3) = N(uv) = N(u)N(v) = 9.$$

  Visto que $N(u), N(v) \neq \pm 1$, resta que $N(u) = N(v) = \pm 3$. Supondo que existe $u = a + b\sqrt{10} \in \mathbb{Z}[10]$ tal que $N(u) = 3$, teríamos que $a^2 - 10b^2 = 3$. Reduzindo a módulo 5, temos que $a^2 \equiv 3 \pmod 5$. Pela verificação dos elementos de $\mathbb{Z}_5$, percebe-se que tal a não existe. Logo, não existe $u \in \mathbb{Z}[\sqrt{10}]$ tal que $N(u) = 3$. Assim, 3 é irredutível em $\mathbb{Z}[\sqrt{10}]$.

- $4 \pm \sqrt{10}$ é irredutível. De fato, suponha que $4 \pm \sqrt{10}$ não seja irredutível. Como $4 \pm \sqrt{10} \neq 0$ e $N(4 \pm \sqrt{10}) = 6$, devem existir $u, v \in \mathbb{Z}[\sqrt{10}]$, não inversíveis, tais que $uv = 4 \pm \sqrt{10}$.

  No entanto,

  $$N(4 \pm \sqrt{10}) = N(u)N(v) = 6.$$

  Como $N(u), N(v) \neq \pm 1$, pelo fato de que os elementos não são inversíveis, resta que $N(u), N(v) = \pm 2$ ou $N(u), N(v) = \pm 3$. Pelo mostrado anteriormente, tais elementos não podem existir. Logo, $4 \pm \sqrt{10}$ é irredutível em $\mathbb{Z}[\sqrt{10}]$.

Agora, considere o elemento $6 = 6 + 0\sqrt{10} \in R$. Note que $6 = 2 \cdot 3$, com 2 e 3 irredutíveis em $\mathbb{Z}[\sqrt{10}]$ e $6 = (4 + \sqrt{10})(4 - \sqrt{10})$, com $4 + \sqrt{10}$ e $4 - \sqrt{10}$ irredutíveis em R. Dessa forma, observa-se que em R a fatoração do elemento 6 em um produto de elementos irredutíveis existe, mas não é única. Isso justifica a necessidade do segundo item da Definição 3.5.

Tendo em vista a relação entre elementos irredutíveis e ideais primos e o exemplo do anel $\mathbb{Z}$, parece plausível que todo domínio de ideais principais é um DFU.

Teorema 3.7. *Todo o domínio de ideais principais R é um domínio de fatoração única.*

Isso de fato se verifica e o teorema será demonstrado apropriadamente. No entanto, cabe ressaltar que a recíproca não é verdadeira, pois existem anéis (a saber, o anel de polinômios $\mathbb{Z}[x]$) que são domínios de fatoração única sem ser domínios principais.

A fim de demonstrar o Teorema 3.7 é necessário se ter em mente, além do que já foi apresentado, os resultados a seguir:

Lema 3.8. *Se R é um anel de ideais principais e $(a_1) \subset (a_2) \subset \ldots$ é uma cadeia de ideais em R, então existe um inteiro positivo n tal que $(a_j) = (a_n)$ $\forall j \geq n$.*

Demonstração. Seja $A = \bigcup_{i \geq 1}(a_i)$. Pelo Teorema 2.7, A é um ideal de R. Visto que todos os ideais de R são principais, A é principal. Digamos que $A = (a)$. Como $a \in A = \bigcup_{i \geq 1}(a_i)$, segue que $a \in (a_n)$ para algum n. Assim, pela Definição 2.8, $(a) \subset (a_n)$.

Assim, para todo $j \geq n$, $(a) \subset (a_n) \subset (a_j) \subset A = (a)$. Conclui-se que $(a_n) = (a_j)$, para todo $j \geq n$. □

Teorema 3.9 (Teorema da Recursão)**.** *Se S é um conjunto, $a \in S$ e para qualquer $n \in \mathbb{N}, f_n : S \to S$ é uma função, então existe uma única função $\phi : \mathbb{N} \to S$ tal que $\phi(0) = a$ e $\phi(n + 1) = f_n(\phi(n))$, para todo $n \in \mathbb{N}$.*

A demonstração do Teorema 3.9 não será apresentada por se distanciar do objetivo do trabalho. No entanto, a mesma pode ser encontrada em [4, p. 10].

Ainda, é necessário ter em mente o Axioma da Escolha, dentre suas várias formulações, a mais adequada aos objetivos de seu uso no trabalho é: seja C uma coleção de conjuntos não vazios. É possível escolher um elemento de cada conjunto de C.

Demonstração do Teorema 3.7. Seja R um domínio principal. Seja S o conjunto de todos os elementos não nulos e não inversíveis de R que não podem ser fatorados como um produto finito de elementos irredutíveis. Primeiramente, será demonstrado que S é vazio e, portanto, todo elemento não nulo e não inversível de R tem ao menos uma fatoração como um produto finito de elementos irredutíveis. Em seguida, demonstrar-se-á que essa fatoração é única.

Suponha que S não é vazio e que $a \in S$. Segue que $(a) \neq R$ pelo Teorema 3.2(iv). Ainda, observa-se que (a) está contido num ideal maximal (c) pelo Teorema 2.15. Como (c) é maximal em R, em particular (c) é maximal no conjunto dos ideais próprios de R. Assim, o elemento c é irredutível em R, pelo Teorema 3.4(ii).

Como $(a) \subset (c)$, temos que $c|a$ (Teorema 3.2(i)). Visto que $S \neq \emptyset$ por hipótese, é possível escolher, para cada $a \in S$, um divisor irredutível c_a de a, com $c_a \in (c)$ (Axioma da Escolha).

Como R é um domínio de integridade, c_a determina um único elemento não nulo $x_a \in R$ tal que $c_a x_a = a$. Note que x_a é de fato único. Se $y_a \in R$ fosse outro elemento com a propriedade que $c_a y_a = a$, ter-se-ia $c_a y_a = c_a x_a$ implica que $y_a = x_a$, pela lei do cancelamento em domínios de integridade.

Afirma-se que $x_a \in S$, ou seja, x_a não é nulo, não é inversível e não pode ser fatorado como um produto finito de irredutíveis. Já dispomos que $x_a \neq 0$. Então, inicialmente, será mostrado que x_a não é inversível. Supondo, por absurdo que x_a fosse inversível, teríamos que $a = c_a x_a$ implica que a é associado a c_a (Teorema 3.2(vi)). Como c_a é irredutível, a também o seria (Teorema 3.4(v)), o que implica que $a = a$ pode ser fatorado como um produto de irredutíveis, contrariando a hipótese de que $a \in S$ (isto é, a não pode ser fatorado). Portanto, conclui-se que x_a não é inversível.

Agora, sabendo que x_a não é inversível suponhamos, por absurdo, que $x_a \notin S$. Isso implica que x_a pode ser fatorado como um produto finito de irredutíveis. Seja tal fatoração $x_a = c_1 \cdots c_n$, com c_i irredutíveis. Segue que $a = c_a x_a = c_a c_1 \cdots c_n$, com c_a, c_i irredutíveis, contrariando a hipótese de que $a \in S$. Portanto, x_a não pode ser fatorado como um produto de elementos irredutíveis.

Como x_a não é inversível, é não nulo e não pode ser fatorado num produto de irredutíveis, conclui-se que $x_a \in S$.

Além disso, afirma-se que $(a) \subsetneq (x_a)$. Como $a = c_a x_a$, temos que $x_a | a$, implicando que $(a) \subset (x_a)$, pelo Teorema 3.2(i). Mas se $(a) = (x_a)$, ter-se-ia que $(x_a) \subset (a)$, implicando que $a | x_a$ e que $x_a = ay$ para algum $y \in R$. Assim, $a = c_a x_a = c_a y a$, implicando $1 = c_a y$. Mas isso contradiz o fato de que c_a é irredutível (portanto não inversível). Assim, $(a) \subsetneq (x_a)$.

Pelo exposto até agora é possível considerar que a função $f : S \to S$ dada por $f(a) = x_a$ é bem definida. Utilizando o Teorema da Recursão e tomando $f = f_n$ para todo n, existe uma função $\varphi : \mathbb{N} \to S$ tal que $\varphi(0) = a$ e $\varphi(n+1) = f(\varphi(n)) = x_{\varphi(n)}$, para $n \geq 0$.

Aplicando a função φ recursivamente:

$$\varphi(0) = a,$$

$$\varphi(1) = \varphi(0+1) = f(\varphi(0)) = f(a) = x_a, \text{ denotado por } a_1;$$

$$\varphi(2) = \varphi(1+1) = f(\varphi(1)) = f(a_1) = x_{a_1}, \text{ denotado por } a_2;$$

$$\varphi(3) = \varphi(2+1) = f(\varphi(2)) = f(a_2) = x_{a_2}, \text{ denotado por } a_3;$$

$$\vdots$$

Assim se obtém uma sequência de elementos de $S : a, a_1, a_2, \ldots$ tais que:

$$a = c_a x_a \Rightarrow (a) \subsetneq (x_a) \text{ e } x_a \in S;$$

$$\text{denotando } x_a = a_1, \text{ temos } a_1 = c_{a_1} x_{a_1} \Rightarrow (a_1) \subsetneq (x_{a_1}) \text{ e } x_{a_1} \in S;$$

$$\text{denotando } x_{a1} = a_2, \text{ temos } a_2 = c_{a_2} x_{a_2} \Rightarrow (a_2) \subsetneq (x_{a_2}) \text{ e } x_{a_2} \in S;$$

$$\vdots$$

Denotando $x_{a_n} = a_{n+1}$, obtemos a cadeia de ideais $(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \ldots$. Mas isso contradiz o Lema 3.8, pois qualquer que seja $n \in \mathbb{N}$, $(a_j) \neq (a_n)$. Portanto, conclui-se que S é vazio, isto é, todos os elementos não nulos e não inversíveis de R podem ser fatorados como um produto de elementos irredutíveis. Resta mostrar que essa fatoração é de fato única. Para tal, suponha que $a = c_1 \cdots c_n = d_1 \cdots d_m$, com c_i, d_i irredutíveis. Já foi mostrado que c_i, d_i também são primos, pois R é um domínio principal.

Usando a associatividade de R, temos que $c_1(c_2 \cdots c_n) = d_1 \cdots d_m$ implica que $c_1 | d_i$ para algum d_i. Sem perda de generalidade, pode-se afirmar que $c_1 | d_1$ (pela comutatividade de R). Segue que $d_1 = c_1 u_1$, com u_1 inversível.

Assim, escrevemos

$$c_1c_2\cdots c_n = c_1u_1d_2\cdots d_m,$$

e, pela lei do cancelamento em domínios de integridade,

$$c_2\cdots c_n = u_1d_2\cdots d_m.$$

Suponha que para $1 \leq i \leq k < n, d_i = u_ic_i$, com u_i inversível. Temos que

$$\begin{aligned}
c_1\cdots c_kc_{k+1}\cdots c_n &= (u_1c_1\cdots u_kc_k)\, d_{k+1}\cdots d_m \\
c_1\cdots c_kc_{k+1}\cdots c_n &= (c_1\cdots c_k)\,(u_1\cdots u_k)\, d_{k+1}\cdots d_m \\
c_{k+1}\cdots c_n &= (u_1\cdots u_k)\, d_{k+1}\cdots d_m \\
c_{k+1}\cdots c_nu_1^{-1}\cdots u_k^{-1} &= d_{k+1}\cdots d_m \\
c_{k+1}\left(c_{k+2}\cdots c_nu_1^{-1}\cdots u_k^{-1}\right) &= d_{k+1}\cdots d_m.
\end{aligned}$$

Segue que $c_{k+1}|d_{k+1}\cdots d_m$, ou seja, c_{k+1} divide d_j para algum $k+1 \leq j \leq m$. Portanto, $c_i|d_i\ \forall i$ e, assim, $d_i = c_iu_i$. Então

$$\begin{aligned}
c_1c_2\cdots c_n &= c_1u_1\cdots c_nu_nd_{n+1}\cdots d_m \\
c_1c_2\cdots c_n &= (c_1\cdots c_n)\,(u_1\cdots u_n)\, d_{n+1}\cdots d_m.
\end{aligned}$$

Logo,

$$1_R = (u_1\cdots u_n)\, d_{n+1}\cdots d_m \tag{3.1}$$

Mas perceba que isso implica que os d_i são inversíveis, contrariando a hipótese de que são irredutíveis. Como consequência, $m = n$. Pelas considerações anteriores, cada c_i é associado a algum d_i. Portanto, a fatoração é única num domínio principal.

Será demonstrada agora a afirmação em (3.1). Seja R é um domínio principal e sejam $p_1, p_2 \in R$ tais que p_1p_2 é inversível. Vamos mostrar que p_1 e p_2 são inversíveis. Como p_1p_2 é inversível, existe $z \in R$ tal que $(p_1p_2)z = 1_R \Rightarrow p_1(p_2z) = 1$, logo p_1 é inversível.

Ainda, $(p_1p_2)z = p_1(p_2z) = (p_1z)p_2 \Rightarrow p_2$ é inversível.

Suponha que $p_1\cdots p_n$ é inversível. Se $p_1\cdots p_np_{n+1}$ for inversível, então existe $x \in R$ tal que $(p_1\cdots p_np_{n+1})x = 1$, o que equivale a $(p_1\cdots p_nx)p_{n+1} = 1$ de onde se conclui que p_{n+1} é inversível.

Observamos que a comutatividade e a existência da identidade são necessários para garantir a igualdade em (3.1). □

Exemplo 3.9.1. *Já foi visto que $\mathbb{Z}$ é um domínio principal. Temos também que $\mathbb{Z}$ é um*

domínio fatorial. O elemento 15*, por exemplo, pode ser fatorado em produto de elementos irredutíveis como* $15 = 3 \cdot 5 = (-3)(-5) = (-5)(-3) = 5 \cdot 3$*, onde* 3 *e* -3*,* 5 *e* -5 *são associados respectivamente.*

Alguns domínios de integridade têm características particulares que não são compartilhadas pelos demais.

Definição 3.10. *Seja* $\mathbb{N}$ *o conjunto dos inteiros não negativos e* R *um anel comutativo.* R *é um* anel Euclidiano *se existe uma função* $\varphi : R\backslash\{0\} \mapsto \mathbb{N}$ *tal que*

i) se $a, b \in R$ *e* $b \neq 0$*, então* $\varphi(a) \leq \varphi(ab)$*;*

ii) se $a, b \in R$ *e* $b \neq 0$*, então existem* $q, r \in R$ *tal que* $a = qb + r$*, com* $r = 0$*, ou* $r \neq 0$ *e* $\varphi(r) < \varphi(b)$*.*

Um anel Euclidiano que é um domínio de integridade é dito um domínio Euclidiano.

A Definição 3.10 é uma generalização do algoritmo de Euclides dos números inteiros. A função Euclidiana φ nos permite "medir" se um elemento do conjunto é menor que outro.

Algumas observações se fazem pertinentes. Inicialmente, a função Euclidiana não é necessariamente única num domínio Euclidiano, como será apresentado nos exemplos que se seguem. Ainda, os elementos $q, r \in R$ também não são necessariamente únicos. Por fim, é possível observar que qualquer conjunto bem ordenado, como $\mathbb{Z}$, por exemplo, pode ser usado no lugar de $\mathbb{N}$ para definir a função Euclidiana.

Exemplo 3.10.1. *Como exemplos de domínios Euclidianos elencam-se* $\mathbb{Z}$ *com a função* $\varphi(x) = |x|$*;* $\mathbb{Z}$ *com a função* $\varphi(x) = x^2$*,* $\mathbb{F}$ *sendo um corpo qualquer com a função* $\varphi(x) = 1, \forall x \in \mathbb{F}$*.*

Com relação aos anéis Euclidianos, é possível demonstrar que são anéis principais. Como consequência, os domínios Euclidianos são domínios de fatoração única.

Teorema 3.11. *Seja* R *um anel Euclidiano. Então* R *é um anel principal com identidade. Consequentemente, todo domínio Euclidiano é um domínio de fatoração única.*

Demonstração. Seja I um ideal não nulo de R. Queremos mostrar que I é principal. É possível escolher $a \in I$ de forma que $\varphi(a)$ é o menor inteiro no conjunto dos inteiros não negativos $\{\varphi(x) | x \neq 0, x \in I\}$. Tal a existe pelo fato de que $\varphi(x) \in \mathbb{N}$, que é bem ordenado, isto é, qualquer subconjunto de $\mathbb{N}$ possui um elemento mínimo.

Seja $b \in I$. Como R é Euclidiano, então $b = qa + r$, com $r = 0$ ou $r \neq 0$ e $\varphi(r) < \varphi(a)$. Como $a \in I$, segue que $aq \in I \Rightarrow -aq \in I \Rightarrow r = b - aq \in I$, por I ser um ideal e $b \in I$.

Como $\varphi(r) < \varphi(a)$ contradiz a escolha de a, segue que $r = 0$ e, portanto, $b = qa$, implicando que $b \in Ra$. Consequentemente, $I \subset Ra \subset (a) \subset I$ (pelo Teorema 2.9). Assim, $I = Ra = (a)$. Dado que I é um ideal arbitrário, todos os ideais de R são gerados por um único elemento. Conclui-se que R é um anel principal.

Agora, como R é ele mesmo um ideal, $R = Ra$ para algum $a \in R$. Então $a = ae = ea$ para algum $e \in R$. Se $b \in R = Ra$, então $b = xa$ para algum $x \in R$. Assim, $be = (xa)e = x(ae) = xa = b$. Ou seja, e é a identidade multiplicativa de R.

Um domínio Euclidiano é, em particular, um anel Euclidiano; um domínio principal é, em particular um anel principal. Assim, é possível concluir, por conta do Teorema 3.7, que os domínios Euclidianos são domínios de fatoração única. □

Observa-se, todavia, que a recíproca do Teorema 3.11 não é verdadeira. Existem domínios principais (consequentemente, fatoriais) que não são Euclidianos.

Exemplo 3.11.1. *O domínio* $D = \left\{ z_1 \frac{1}{2} + z_2 \frac{\sqrt{-19}}{2}, z_1, z_2 \in \mathbb{Z}, \text{ de mesma paridade} \right\}$ *não é Euclidiano. Uma demonstração da validade desse exemplo pode ser encontrada em [1].*

Feitas as considerações acerca de fatoração e divisibilidade em anéis, é possível definir o máximo divisor comum (mdc) num anel, bem como algumas propriedades e resultados referentes aos mesmos.

Definição 3.12. *Seja X um subconjunto não vazio de um anel comutativo R. Um elemento $d \in R$ é dito* maior divisor comum de X *se:*

i) $d|a$, $\forall a \in X$;

ii) $c|a$, $\forall a \in X \Rightarrow c|d$.

Algumas observações se fazem pertinentes neste momento. Inicialmente, frisamos que o mdc de um conjunto nem sempre existe. Tomando como exemplo $E = 2\mathbb{Z}$ o anel dos inteiros pares, observamos que 2 não tem divisores, pois $1 \notin E$, enquanto que 2 e 4 não têm um maior divisor comum.

Ainda, mesmo quando um mdc de $a_1, a_2, \ldots, a_n$ existe, o mesmo não é necessariamente único.

Exemplo 3.12.1. *Considere o anel* $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}, i = \sqrt{-1}\}$ *(inteiros de Gauss). Os elementos* $2, -2, 2i$ *e* $-2i$ *são máximos divisores comuns de* 2 *e* 4*, nos termos da Definição 3.12.*

Apesar disso, em um anel comutativo dois mdc's quaisquer são associados. De fato, sejam d_1 e d_2 mdc's de $a_1, a_2, \ldots, a_n$. Por definição, $d_1|a_i$, $\forall i$ e $d_2|a_i$, $\forall i$. Ainda, pela Definição 3.12(ii), temos que $d_1|d_2$ e $d_2|d_1$. Portanto, d_1 e d_2 são associados. Isso é bem ilustrado no exemplo anterior.

Em relação aos elementos associados ao mdc de um conjunto, tem-se o seguinte resultado:

Teorema 3.13. *Qualquer elemento associado ao mdc de um subconjunto não vazio X contido em um anel R é, ele próprio, um mdc de X.*

Demonstração. Considere que $d \in R$ é um mdc de X e d' é associado a d. Para todo $a_i \in X$, constata-se que $d|a_i$, isto é, $a_i = dm_i$, para algum $m_i \in R$. Mas como $d'|d$, $d = d'k$, para algum $k \in R$. Segue que $a_i = d'km_i$, ou seja, $d'|a_i$, $\forall i$.

A condição (ii) da Definição 3.12 é sempre satisfeita. Basta notar que d' associado a d implica que $d'|d$. Logo um elemento associado a um mdc de X é, ele próprio, um mdc de X. □

Por fim, se R é um anel com identidade e $a_1, a_2, \ldots, a_n$ tem 1_R como seu mdc, então os elementos $a_1, a_2, \ldots, a_n$ são ditos primos relativos.

Teorema 3.14. *Sejam $a_1, a_2, \ldots, a_n$ elementos de um anel comutativo R com identidade.*

i) O elemento $d \in R$ é um máximo divisor comum de $\{a_1, a_2, \ldots, a_n\}$ tal que $d = a_1r_1 + \cdots + a_nr_n$ para algum $r_i \in R$ se, e somente se, $(d) = (a_1) + (a_2) + \cdots + (a_n)$.

ii) Se R é um anel principal, então existe um máximo divisor comum de $a_1, a_2, \ldots, a_n$, e cada mdc é da forma $a_1r_1 + \cdots + a_nr_n$ onde $r_i \in R$.

iii) Se R é um domínio de fatoração única, então existe um máximo divisor comum de $a_1, a_2, \ldots, a_n$.

Antes de demonstrar o Teorema 3.14, convém observar que fora das hipóteses do item (i) não se implica que d pode ser expresso como uma combinação linear de $\{a_1, a_2, \ldots, a_n\}$.

A fim de justificar o exemplo a seguir, convém demonstrar a seguinte proposição acerca de normas.

Proposição 3.14.1. *Seja R um anel e $N : R \mapsto \mathbb{Z}$ uma função norma que preserva a multiplicação. Se $u|a$ e $u|b$, então $N(u)|\operatorname{mdc}\{N(a), N(b)\}$.*

Demonstração. Já foi mostrado que se $x|y$, então $N(x)|N(y)$. Segue que $N(u)|N(a)$ e $N(u)|N(b)$. Isso significa que $N(u)$ é um divisor comum de $\{N(a), N(b)\}$. Há dois casos a serem considerados:

i) Se $N(u)$ é o maior divisor comum de $\{N(a), N(b)\}$, então $N(u)|\operatorname{mdc}\{N(a), N(b)\}$ (trivial);

ii) se $N(u)$ não é o mdc de $\{N(a), N(b)\}$, segue que $N(u)|\operatorname{mdc}\{N(a), N(b)\}$ pela Definição 3.12(ii).

Assim $N(u)|\operatorname{mdc}\{N(a), N(b)\}$. □

Com essas considerações, apresentar-se-á um exemplo de que o mdc de dois elementos não pode ser escrito como combinação linear desses elementos.

Exemplo 3.14.1. *Considere o anel* $\mathbb{Z}[\sqrt{10}]$ *estudado anteriormente, com a mesma função norma. Observa-se que* $\operatorname{mdc}\{2, 4+\sqrt{10}\} = 1$. *Isso se dá pelos seguintes fatos:* $1|2$ *e* $1|4+\sqrt{10}$ *(trivial). Ainda, supondo que existe* $u \in \mathbb{Z}[\sqrt{10}]$ *tal que* $u|2$ *e* $u|4+\sqrt{10}$ *temos que* $N(u)|\operatorname{mdc}\{N(2), N(4+\sqrt{10})\} = \operatorname{mdc}\{4, 6\} = 2$, *isto é,* $N(u)|2$. *Os únicos divisores inteiros de* 2 *são* ± 1 *e* ± 2. *Já foi visto que não existe* $u \in \mathbb{Z}[\sqrt{10}]$ *tal que* $N(u) = \pm 2$. *Portanto,* $N(u) = \pm 1$, *implicando que* u *é inversível e* $u|1$.

Será mostrado agora que 1 *não pode ser escrito como combinação linear de* 2 *e* $4+\sqrt{10}$. *De fato, supondo que existam* $x, y \in \mathbb{Z}[\sqrt{10}]$ *tais que seja possível denotar* $1 = 2x + y(4+\sqrt{10}) = 2x + 4y + y\sqrt{10}$, *obtém-se o seguinte sistema:*

$$\begin{cases} 2x + 4y = 1 \\ y\sqrt{10} = 0 \end{cases}$$

cuja solução é $y = 0$, $x = \frac{1}{2} \notin \mathbb{Z}[\sqrt{10}]$. *Isto significa que o sistema não tem solução em* $\mathbb{Z}[\sqrt{10}]$ *e que* $1 = \operatorname{mdc}\{2, 4+\sqrt{10}\}$ *não é uma combinação linear de* 2 *e* $4+\sqrt{10}$.

Demonstração do Teorema 3.14. i) ($\Rightarrow$) Suponha que $d = r_1a_1 + r_2a_2 + \cdots + r_na_n$ é um mdc de $a_1, a_2, \ldots, a_n$. Pela Definição 3.12, $d|a_1, \ldots, d|a_n$. Segue, pelo Teorema 3.2(i), que $(a_1) \subset (d), \ldots, (a_n) \subset (d)$. Como (d) é um ideal – e a soma de ideais é um ideal – temos que $(a_1) + (a_2) + \cdots + (a_n) \subset (d)$.

Para a outra contingência, note que $d = r_1a_1 + \cdots + r_na_n \in (a_1) + \cdots + (a_n)$ e, pelo Teorema 2.10, $(a_1) + \cdots + (a_n)$ é um ideal de R. Logo $(d) \subset (a_1) + (a_2) + \cdots + (a_n)$ e, portanto, $(d) = (a_1) + (a_2) + \cdots + (a_n)$.

($\Leftarrow$) Assume-se agora que $(d) = (a_1)+(a_2)+\cdots+(a_n)$. Como R tem identidade e $a_1, a_2, \ldots, a_n$ estão no centro de R (pois R é comutativo), temos, pelo Teorema 2.9(v) que $(a_i) = a_iR = Ra_i$, $\forall a_i$.

Ainda, $d \in (d) = (a_1) + (a_2) + \cdots + (a_n)$ pelo Teorema 2.9(iv), pois R tem identidade. Segue que $d = r_1a_1 + r_2a_2 + \cdots + r_na_n$ para algum $r_i \in R$.

Agora, $(d) = (a_1)+(a_2)+\cdots+(a_n)$ implica que cada $(a_i) \subset (d)$ e, pelo Teorema 3.2(i), $d|a_i$, $\forall i$. Então d é um divisor de cada a_i.

Suponha, agora, que $c \in R$ também seja um divisor de cada a_i. Pelo Teorema 3.2(i), $(a_i) \subset (c)$ para cada a_i. Mas como (c) é um ideal, temos que $(d) = (a_1) + (a_2) + \cdots + (a_n) \subset (c)$ e, pelo Teorema 3.2(i), segue que $c|d$.

Assim, pela Definição 3.12, d é um máximo divisor comum de $\{a_1, \cdots, a_n\}$.

(ii) Seja R um anel principal e $a_1, a_2, \ldots, a_n \in R$. Pelo Teorema 2.10, $(a_1) + (a_2) + \cdots + (a_n)$ é um ideal de R. Como R é principal, todos os ideais são gerados por um único elemento. Então $(a_1) + (a_2) + \cdots + (a_n) = (d)$ para algum $d \in R$. Pelo item (i), se sucede que d é um máximo divisor comum de $\{a_1, a_2, \ldots, a_n\}$ e é da forma $d = r_1a_1 + r_2a_2 + \cdots + r_na_n$.

Considere que d' é um outro mdc de $\{a_1, a_2, \cdots, a_n\}$. Foi mostrado anteriormente que d e d' são associados, o que implica que $d|d'$. Ou seja, existe $r \in R$ tal que $d' = dr$. Como $d = r_1a_1 + r_2a_2 + \ldots + r_na_n$, a distributividade de R justifica que

$$\begin{aligned} d' &= r(r_1a_1 + r_2a_2 + \cdots + r_na_n) \\ &= rr_1a_1 + rr_2a_2 + \cdots + rr_na_n \\ &= r'_1a_1 + r'_2a_2 + \cdots + r'_na_n, \end{aligned}$$

onde $r'_i = rr_i \in R$. Dessa forma, qualquer mdc de $\{a_1, a_2, \ldots, a_n\}$ é da forma $d = r_1a_1 + r_2a_2 + \cdots + r_na_n$.

iii) Suponha que R é um domínio de fatoração única. Se algum dos a_i for inversível, temos que mdc$\{a_i, \ldots, a_n\}$ é 1. Se nenhum deles for inversível e não nulo, então para cada $a_i \in R$, temos $a_i = c_1^{m_{i1}}c_2^{m_{i2}}\cdots c_t^{m_{it}}$ com c_k irredutíveis e distintos e cada $m_{ij} \geq 0$ (o que possibilita a utilização de expoentes nulos quando necessário), sendo possível $d = 1$ caso não existam fatores comuns entre os a_i.

Caso existam fatores comuns, segue que o elemento $d = c_1^{k_1}c_2^{k_2}\cdots c_t^{k_t}$, com $k_j = \min\{m_{1j}, m_{2j}, \ldots, m_{nj}\}$ é um divisor de cada $a_1, a_2, \ldots, a_n$. Vamos supor que existe um $c \in R$ que também seja um divisor de cada a_i. Como R é um domínio fatorial, $c = d_1d_2\cdots d_l$, com d_i irredutíveis. Como $c = d_1d_2\cdots d_l$ divide $a_i = c_1^{m_{i1}}c_2^{m_{i2}}\cdots c_t^{m_{it}}$, então cada d_j divide a_i. Mas como cada c_i é irredutível (não inversível, por definição), o fato de que $d_j|a_i$ implica que d_j é associado a c_i, para algum c_i.

Então, $c = c_1^{n_1}c_2^{n_2}\cdots c_t^{n_t}$ para algum $n_i \geq 0$. Se cada $n_i \leq k_i$, então $c|d$. Suponha, agora, que $n_i* > k_i*$ para algum $i*$. Então existe um $a_i = c_1^{m_{i1}}c_2^{m_{i2}}\cdots c_{i*}^{k_{i*}}\cdots c_t^{m_{it}}$ e c não divide este a_i, o que é uma contradição.

Conclui-se, assim, que $n_i \leq k_i$ e $c|d$. Isto é, d é um máximo divisor comum de $a_1, a_2, \ldots, a_n$.

□

Teorema 3.15. *Se R é um domínio de fatoração única, $a, b \in R$ são primos relativos e $a|bc$, então $a|c$.*

Demonstração. Inicialmente, há de se considerar que se $\text{mdc}(a, b) = 1$ e $a = a_1^{k_1} \cdots a_n^{k_n}$, $b = b_1^{c_1} \cdots b_m^{c_m}$, então a_i e b_j são primos relativos. De fato, se a_i e b_j não fossem primos relativos, para algum i, j existiria $d \in R$ tal que $d|a_i$ e $d|b_j$ e $d = \text{mdc}(a_i, b_j)$. Logo, $dk_i = a_i$ e $dk_j = b_j$, ou seja, $a = a_1^{k_1} \cdots dk_i \cdots a_n^{k_n}$, $b = b_1^{c_1} \cdots dk_j \cdots b_m^{c_m}$, implicando que $d|a$ e $d|b$, contradizendo a hipótese de que a, b são primos relativos.

Supondo, agora, que exista $c \in R$, com $c = c_1 \cdots c_l$ tal que $a \nmid c$. Pelo anterior, $a_i \nmid c_k$ para todo i, k. Como $a \nmid b$ por hipótese, e a_i, b_j, c_k são irredutíveis, segue $a \nmid bc$, o que é um absurdo.

Logo, $a|c$. □

4 ANÉIS DE POLINÔMIOS

Muitos do resultados estudados até o momento podem ser ilustrados em um tipo de anel bem conhecido: o anel de polinômios numa variável.

Definição 4.1. *Seja R um anel. Um* polinômio numa variável sobre R *é uma sequência $(a_0, a_1, \ldots, a_n, \ldots)$, onde $a_i \in R$ para todo índice i, e $a_i \neq 0$ somente para um número finito de índices. Seja $R[x]$ o conjunto de todos os polinômios numa variável sobre R. $R[x]$ é um anel com as operações definidas por*

$$(a_0, a_1, \ldots) + (b_0, b_1, \ldots) = (a_0 + b_0, a_1 + b_1, \ldots)$$

e

$$(a_0, a_1, \ldots)(b_0, b_1, \ldots) = (c_0, c_1, \ldots)$$

onde $c_n = \sum_{i=0}^{n} a_{n-i} b_i$.

Algumas observações se fazem pertinentes. Se R é comutativo (respectivamente, tem identidade, é um domínio de integridade), $R[x]$ também o é. Considerando que R tem identidade, o elemento $(0, 1_R, 0, \ldots) \in R[x]$ será denotado por x. Assim, qualquer polinômio não nulo $f = (a_0, a_1, \ldots, a_{n-1}, a_n, 0, 0, \ldots)$ pode ser escrito de maneira única como $f = a_0 + a_1 x + \cdots + a_n x^n = \sum_{i=0}^{n} a_i x^i \in R[x] \setminus \{0\}$. Os termos $a_i \in R$ são chamados coeficientes, e a_0 é o termo constante.

Definição 4.2. *Seja R um anel e seja $f(x) = \sum_{i=0}^{n} a_i x^i \in R[x] \setminus \{0\}$, com $a_n \neq 0$. O inteiro n se chama* grau *de $f(x)$. O coeficiente a_n se chama* coeficiente líder *de $f(x)$. Quando o coeficiente líder for igual a 1, o polinômio é dito* mônico.

É conveniente definir o grau do polinômio nulo como sendo $-\infty$ e adotar as seguintes convenções acerca de grau $0 = -\infty$: $(-\infty) < n$ e $(-\infty) + n = -\infty = n + (-\infty)$ para qualquer inteiro n; $(-\infty) + (-\infty) = -\infty$. Dessa maneira, é possível fazer com que o algoritmo da divisão de polinômios seja similar ao algoritmo de Euclides na divisão de números inteiros.

Antes de apresentar o algoritmo da divisão de polinômios e sua demonstração, é conveniente demonstrar um resultado relativo ao grau do produto de polinômios.

Teorema 4.3. *Seja R um anel e $f, g \in R[x]$. Então,* $\operatorname{grau} fg \leq \operatorname{grau} f + \operatorname{grau} g$. *Em particular, se R é um domínio de integridade,* $\operatorname{grau} fg = \operatorname{grau} f + \operatorname{grau} g$.

Demonstração. Para o caso em que $g = f = 0$, o resultado é trivial. Supondo que $f, g \neq 0$, verifica-se que $f = \sum_{i=0}^{n} a_i x^i$ tem grau n e $g = \sum_{i=0}^{m} b_i x^i$ tem grau m. Segue que

$$fg = a_0 b_0 + \cdots + (a_{n-1} b_m + a_n b_{m-1}) x^{n+m-1} + a_n b_m x^{m+n}$$

tem grau não maior do que $m + n$.

Ou seja, $\operatorname{grau}(fg) \leq \operatorname{grau} f + \operatorname{grau} g$.

Se R for um domínio de integridade, se garante que $a_n b_m \neq 0$. Portanto, $\operatorname{grau}(fg) = \operatorname{grau} f + \operatorname{grau} g$. □

Teorema 4.4 (Algoritmo da divisão de polinômios)**.** *Seja R um anel com identidade e $f, g \in R[x]$ polinômios não nulos tais que o coeficiente líder de g é inversível em R. Então existem polinômios $q, r \in R[x]$ unicamente determinados tais que*

$$f = qg + r \ \textit{e} \ \operatorname{grau} r < \operatorname{grau} g.$$

Demonstração. (Existência) Se $\operatorname{grau} g > \operatorname{grau} f$, basta tomar $q = 0$ e $r = f$. Caso $\operatorname{grau} g \leq \operatorname{grau} f$, é possível escrever $f = a_n x^n + \cdots + a_0$ e $g = b_m x^m + \cdots + b_0$, com $a_n, b_m \neq 0, m \leq n$ e b_m inversível em R.
Procede-se por indução sobre $\operatorname{grau} f = n$. Para $n = 0$, temos que $m \leq 0$ implica em $m = 0$, pois m é não negativo. Assim, $f = a_0, g = b_0$ e b_0 possui inverso. Tomando $q = b_0^{-1} a_0$ e $r = 0$, temos que $\operatorname{grau} r < \operatorname{grau} g$ e

$$qg + r = b_0^{-1} a_0 b_0 = a_0 = f.$$

Como hipótese indutiva, suponha a existência de polinômios q e r satisfazendo a condição do teorema para polinômios de graus menores do que $n = \operatorname{grau} f$. Considere o polinômio $(a_n b_m^{-1} x^{n-m})\, g$. Temos:

$$(a_n b_m^{-1} x^{n-m})\,(b_m x^m + b_{m-1} x^{m-1} + \cdots + b_0) = \\ = a_n x^n + a_n b_m^{-1} b_{m-1} x^{n-1} + \cdots + a_n b_m^{-1} b_0 x^{n-m}.$$

É fácil ver que $(a_n b_m^{-1} x^{n-m})\, g$ tem coeficiente líder a_n e grau n. Segue que

$$f - \left(a_n b_m^{-1} x^{n-m}\right) g = a_n x^n + a_{n-1} x^{n-1} \cdots + a_0 - a_n x^n - a_{n-1} b_m^{-1} b_{m-1} x^{n-1} - \cdots - a_n b_m^{-1} b_0 x^{n-m}$$

$$= \left(a_{n-1} - a_{n-1} b_m^{-1} b_{m-1}\right) x^{n-1} + \cdots + \left(a_{n-m} - a_n b_m^{-1} b_0\right) x^{n-m} + \cdots + a_0,$$

é um polinômio de grau menor que n.
Pela hipótese indutiva, existem polinômios q' e r tais que

$$f - \left(a_n b_m^{-1} x^{n-m}\right) g = q'g + r \text{ e } \operatorname{grau} r < \operatorname{grau} g,$$

$$f = \left(a_n b_m^{-1} x^{n-m}\right) g + q'g + r$$

$$f = \left[\left(a_n b_m^{-1} x^{n-m}\right) + q'\right] g + r.$$

Tomando-se $q = (a_n b_m^{-1} x^{n-m}) + q'$, temos $f = qg + r$.

(Unicidade) Suponha que os polinômios $r_1, q_1, r_2, q_2 \in R[x]$ sejam tais que $f = q_1 g + r_1 = q_2 g + r_2$ e $\operatorname{grau} r_1 < \operatorname{grau} g$ (ou $r_1 = 0$) e $\operatorname{grau} r_2 < \operatorname{grau} g$ (ou $r_2 = 0$). Então $q_1 g + r_1 = q_2 g + r_2$ implica que $(q_1 - q_2)g = r_2 - r_1$.

Considerando que o coeficiente líder b_m de g é inversível, segue que

$$\operatorname{grau}(q_1 - q_2) + \operatorname{grau} g = \operatorname{grau}\left[(q_1 - q_2)g\right] = \operatorname{grau}(r_2 - r_1).$$

Como $\operatorname{grau}(r_2 - r_1) \leq \max(\operatorname{grau} r_2, \operatorname{grau} r_1) < \operatorname{grau} g$, a igualdade acima é verdadeira apenas se $\operatorname{grau}(q_1, q_2) = -\infty = \operatorname{grau}(r_2 - r_1)$. Consequentemente, $q_1 - q_2 = 0$ e $r_2 - r_1 = 0$, comprovando a unicidade requerida.

□

A partir do Teorema 4.4 é possível extrair alguns corolários acerca da divisibilidade e de fatoração em anéis de polinômios.

Corolário 4.4.1 (Teorema do Resto)**.** *Seja R um anel com identidade e*

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

Para qualquer $c \in R$ existe um único $q(x) \in R[x]$ tal que $f(x) = q(x)(x - c) + f(c)$.

Demonstração. Se $f = 0$, verifica-se que $f(c) = 0, \forall c \in R$. Assim, basta tomar $q(x) = 0$. Temos $q(x)(x - c) + f(c) = 0(x - c) + 0 = 0 = f$.
Supondo que $f \neq 0$. Pelo Teorema 4.4, existem polinômios $q, r \in R[x]$ unicamente determinados tais que $f(x) = q(x)(x - c) + r(x)$ e $\operatorname{grau} r(x) < \operatorname{grau}(x - c) = 1$. Segue que $r(x) = r$ é um polinômio constante (possivelmente 0).

Se $q(x) = \sum_{j=0}^{n-1} b_j x^j$, segue que

$$\begin{aligned}
f(x) &= q(x)(x-c) + r \\
f(x) &= b_{n-1}x^n - cb_{n-1}x^{n-1} + b_{n-2}x^{n-1} - \cdots - cb_1 x + b_0 x - b_0 c + r \\
f(x) &= b_{n-1}x^n + (-cb_{n-1} + b_{n-2})\, x^{n-1} + \cdots + (-cb_1 + b_0)\, x - b_0 c + r \\
f(x) &= -b_0 c + \sum_{k=1}^{n-1} (-cb_k + b_{k-1})\, x^k + b_{n-1}x^n + r.
\end{aligned}$$

Daí, tomando $x = c$ e substituindo em $f(x)$ e agrupando os termos semelhantes nos somatórios, obtém-se:

$$\begin{aligned}
f(c) &= -b_0 c + \sum_{k=1}^{n-1} (-cb_k + b_{k-1})\, c^k + b_{n-1}c^n + r \\
&= -b_0 c + \sum_{k=1}^{n-1} -c^{k+1}b_k + \sum_{k=1}^{n-1} c^k b_{k-1} + b_{n-1}c^n + r \\
&= \sum_{k=0}^{n-1} -c^{k+1}b_k + \sum_{k=1}^{n} c^k b_{k-1} + r \\
&= -cb_0 - \cdots - c^n b_{n-1} + cb_0 + \cdots + c^n b_{n-1} + r \\
&= 0 + r = r.
\end{aligned}$$

Assim, conclui-se que para todo $c \in R$ existe um único $q \in R[x]$ tal que $f(x) = q(x)(x-c) + f(c)$. □

Outra consequência do Teorema 4.4 relaciona anéis de polinômio de uma variável sobre um corpo e domínios fatoriais.

Corolário 4.4.2. *Se $\mathbb{F}$ é um corpo, então o anel de polinômios $\mathbb{F}[x]$ é um domínio Euclidiano. Consequentemente, $\mathbb{F}[x]$ é um domínio principal e um domínio de fatoração única. Os elementos irredutíveis de $\mathbb{F}[x]$ são os polinômios constantes não nulos.*

Demonstração. Assume-se como conhecido que $\mathbb{F}[x]$ é um corpo. Consequentemente, $\mathbb{F}[x]$ é um domínio de integridade.

Considere a função $\varphi : \mathbb{F}[x]\setminus\{0\} \to \mathbb{N}\cup\{0\}$ definida por $\varphi(f) = \operatorname{grau} f$. Dado que todo elemento de $\mathbb{F}$ é inversível, temos que $\operatorname{grau} fg = \operatorname{grau} f + \operatorname{grau} g \geq \operatorname{grau} f$. Pelo Teorema 4.4 existem polinômios $q, r \in \mathbb{F}[x]$ tais que $f = qg + r$, com $\operatorname{grau} r < \operatorname{grau} g$. Logo $(\mathbb{F}[x], \varphi)$ satisfaz a Definição 3.10.

Pelo Teorema 3.11, $\mathbb{F}[x]$ é um domínio principal e, consequentemente, um domínio de fatoração única.

Para a segunda parte, considere que se f é inversível em $\mathbb{F}[x]$, então existe $g \in \mathbb{F}[x]$ tal que $fg = 1$. Segue que $0 = \operatorname{grau} 1 = \operatorname{grau} fg = \operatorname{grau} f + \operatorname{grau} g$.

Como $\operatorname{grau} f$ e $\operatorname{grau} g$ são não negativos, $\operatorname{grau} f + \operatorname{grau} g = 0$ implica que $\operatorname{grau} f = \operatorname{grau} g = 0$. Assim, f é um polinômio constante e não nulo (pelo fato de ser inversível). Reciprocamente, se f é um polinômio constante e não nulo de $\mathbb{F}[x]$, segue que $f \in \mathbb{F}$. Como $\mathbb{F}$ é um corpo, existe $f^{-1} \in \mathbb{F} \subset \mathbb{F}[x]$ também é um polinômio constante não nulo.
Assim, é possível concluir que os elementos inversíveis de $\mathbb{F}[x]$ são polinômios constantes não nulos. □

A seguir será demonstrado que os fatores mônicos de grau 1 de um polinômio $f \in R[x]$ podem ser relacionados com as raízes de f em R.

Definição 4.5. *Seja R um subanel de um anel comutativo S, $c \in S$ e $f = \sum_{i=0}^{m} a_i x^i \in R[x]$ tal que $f(c) = 0$. Então, c é uma* raiz *ou* zero *de f (ou ainda, uma* solução *da equação polinomial $f(x) = 0$).*

Teorema 4.6. *Seja R um anel comutativo com identidade e $f \in R[x]$. Então $c \in R$ é uma raiz de f se, e somente se, $x - c$ divide f.*

Demonstração. ($\Rightarrow$) Supondo agora que $c \in R$ é uma raiz de $f(x)$. Temos que $f(c) = 0$. Pelo Corolário 4.4.1, $f(x) = q(x)(x - c) + f(c)$. Como $f(c) = 0$, temos que $f(x) = q(x)(x - c)$, ou seja, $(x - c)|f(x)$.
($\Leftarrow$) Pelo Corolário 4.4.1, tem-se que $f(x) = q(x)(x - c) + f(c)$, $\forall c \in R$. Agora, se $(x - c)|f$, então existe $h(x) \in R[x]$ tal que $h(x)(x - c) = f(x)$. Segue que $h(x)(x - c) = q(x)(x - c) + f(c)$, implicando em $[h(x) - q(x)](x - c) = f(c)$. Substituindo c, temos $f(c) = [h(c) - q(c)](c - c) = 0$.
Portanto, se $(x - c)|f(x)$, segue que $f(c) = 0$ e c é uma raiz. □

Exemplo 4.6.1. *Considere o polinômio $f(x) = x^2 + 2x + 1$ sobre $\mathbb{Z}$. Verifica-se, pela aplicação do Teorema 4.6, que -1 é uma* solução *para esse polinômio, pois $x-(-1) = x+1$ e $(x^2 + 2x + 1) = (x + 1)(x + 1)$, isto é, $x + 1 \mid x^2 + 2x + 1$.*

5 CONSIDERAÇÕES FINAIS

Como mencionado, o objetivo do trabalho foi estender noções de divisibilidade e fatoração em $\mathbb{Z}$ para estruturas algébricas mais gerais, por meio de definições precisas e de resultados deduzidos a partir dessas definições e dos pré-requisitos apresentados.

Foi possível concluir que algumas condições são necessárias para que os conceitos de divisibilidade e fatoração única estejam bem definidos. Inicialmente, é necessário que os anéis em questão sejam comutativos - para a divisibilidade - e domínios de integridade - para a fatoração. Ainda, inferir que há uma relação muito forte entre a divisibilidade de elementos e os ideais gerados por esses elementos.

A fatoração única (a menos de multiplicação por elementos inversíveis) não é uma propriedade exclusiva do conjunto $\mathbb{Z}$, pois qualquer domínio principal possui fatoração única, sabendo-se que nem todos os domínios fatoriais são domínios principais.

A divisão e a fatoração são bem definidas em anéis de polinômios de uma variável sobre anéis comutativos, o que é muito em diversas áreas da Matemática, como a Álgebra e o Cálculo, pois permite a resolução de certos problemas envolvendo limites.

Dessa forma, é possível perceber que a divisibilidade e a fatoração em anéis comutativos constitui uma área de estudo substancial, não apenas dentro da Álgebra, mas também na Matemática em geral.

Dada a natureza do trabalho e a extensão do tema pesquisado, não se tinha a intenção de esgotar o assunto. Mas foi possível levantar os primeiros elementos para que a pesquisa possa ser retomada posteriormente.

REFERÊNCIAS

[1] CAMPOLI, O. A. A principal ideal domain that is not a euclidean domain. **The American Mathematical Monthly**, Mathematical Association of America, v. 95, n 9, p.868-871. 1988. Disponível em <http://www.jstor.org/stable/2322908> .

[2] DOMINGUES, H.; IEZZI, G. **Álgebra Moderna**, 4° ed. São Paulo: Atual, 2003.

[3] GARCIA, A.; LEQUAIN, Y. **Elementos de Álgebra**, 6° ed., Rio de Janeiro: IMPA, 2015.

[4] HUNGERFORD, T. W. **Algebra**. 8° ed. New York. Springer-Verlag, 1974.

[5] LANG, S. **Algebra**, 3° ed., New York: Springer-Verlag, 2002.