UNIVERSIDADE ESTADUAL DA PARAÍBA
CAMPUS I
CENTRO DE CIÊNCIAS E TECNOLOGIA
DEPARTAMENTO DE MATEMÁTICA
CURSO DE LICENCIATURA PLENA EM MATEMÁTICA

LUANA DE SOUSA COELHO DA SILVA

O CRITÉRIO DE EISENSTEIN PARA IRREDUTIBILIDADE EM $\mathbb{Q}[x]$

CAMPINA GRANDE – PB
2020

LUANA DE SOUSA COELHO DA SILVA

O CRITÉRIO DE EISENSTEIN PARA IRREDUTIBILIDADE EM $\mathbb{Q}[x]$

Trabalho de Conclusão de Curso apresentado ao Departamento de Matemática do Centro de Ciências e Tecnologia da Universidade Estadual da Paraíba como requisito parcial à obtenção do título de Licenciada em Matemática.

Área de concentração: Álgebra

Orientador: Prof. Dr. Israel Buriti Galvão

CAMPINA GRANDE – PB
2020

S586c Silva, Luana de Sousa Coelho da.
O Critério de Eisenstein para irredutibilidade em Q[x] [manuscrito] / Luana de Sousa Coelho da Silva. - 2020.
54 p.
Digitado.
Trabalho de Conclusão de Curso (Graduação em Matemática) - Universidade Estadual da Paraíba, Centro de Ciências e Tecnologia , 2021.
"Orientação : Prof. Dr. Israel Buriti Galvão , Departamento de Matemática - CCT."
1. Critério de Eisenstein. 2. Anéis de polinômios. 3. Polinômios irredutíveis. 4. Irredutibilidade. I. Título
21. ed. CDD 515.55

Elaborada por Giulianne M. Pereira - CRB - 15/714 BC/UEPB

LUANA DE SOUSA COELHO DA SILVA

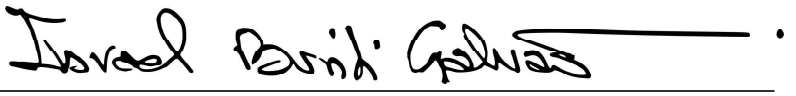
O CRITÉRIO DE EISENSTEIN PARA IRREDUTIBILIDADE EM $\mathbb{Q}[x]$

Trabalho de Conclusão de Curso apresentado ao Departamento de Matemática do Centro de Ciências e Tecnologia da Universidade Estadual da Paraíba como requisito parcial à obtenção do título de Licenciada em Matemática.

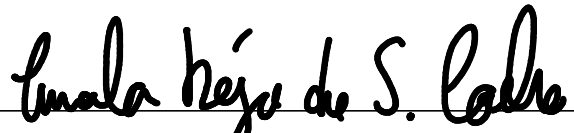
Área de concentração: Álgebra

Aprovado em: 14/12/2020

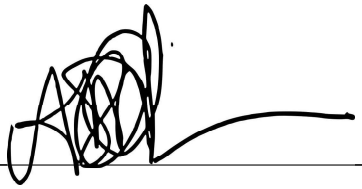
BANCA EXAMINADORA



Prof. Dr. Israel Buriti Galvão (Orientador)
Universidade Estadual da Paraíba (UEPB)



Profa. Dra. Emanuela Régia de Sousa Coelho
Universidade Estadual da Paraíba (UEPB)



Prof. Dr. Arlandson Matheus Silva Oliveira
Universidade Estadual da Paraíba (UEPB)

À minha família pela compreensão e apoio, DEDICO.

AGRADECIMENTOS

Agradeço:

A Deus por Ele ser a razão de tudo.

Aos meus pais, Domingas e Odon, por todo carinho e incentivo.

Às minhas irmãs Ana e Luciana pela amizade e confiança.

A Israel Galvão pela sugestão do tema e pela preciosa condução deste trabaho.

À professora Emanuela Coelho e ao professor Arlandson Matheus pelo aceite ao convite para participação na banca, pelo tempo e esforço, de cada um, dedicados à leitura do trabalho e por suas consequentes contribuições ao seu aperfeiçoamento.

A Higor e a Luanna pela amizade e pelos momentos que vivemos nesta universidade.

Às pessoas maravilhosas que conheci ao longo destes anos nesta instituição.

A todos os professores da UEPB dos quais tive a oportunidade de ser aluna por todo conhecimento compartilhado.

Àqueles que não foram mencionados aqui, mas que tiveram sua parcela de contribuição.

A cada um de vocês, muito obrigada!

"[...] os encantos dessa ciência sublime [a Matemática] em toda sua beleza se revelam apenas àqueles que têm coragem de irem a fundo nela [...]" (Carl Friedrich Gauss em carta a Sophie Germain, 30 de abril de 1807)

RESUMO

Este trabalho tem por objetivos principais apresentar e demonstrar o Critério de Eisenstein para irredutibilidade no anel de polinômios sobre $\mathbb{Q}$. Para tanto, inicialmente, é feito um estudo da Teoria dos Anéis de modo a definir conceitos básicos necessários ao desenvolvimento do trabalho. Como resultado, constatou-se que esse critério é muito útil para identificar se um polinômio inteiro é irredutível sobre $\mathbb{Q}$.

Palavras-chave: Critério de Eisenstein. Anéis de polinômios. Polinômios irredutíveis. Irredutibilidade.

ABSTRACT

This work has as its main objectives to present and prove Eisenstein's Criterion for irreducibility in the polynomial ring over $\mathbb{Q}$. Thus, at first, a study of the Ring Theory is made in order to define basic concepts necessary for the development of this work. As a result, it was found that this criterion is very useful to identify whether an integer polynomial is irreducible over $\mathbb{Q}$.

Keywords: Eisenstein's Criterion. Polynomial rings. Irreducible polynomials. Irreducibility.

SUMÁRIO

Página

1 INTRODUÇÃO

Um polinômio sobre um anel A na indeterminada x é uma expressão formal do tipo:

$$f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n,$$

em que $a_i \in A$ e $n \in \mathbb{N}$.[1] Os elementos a_i tais que $0 \leq i \leq n$ são chamados de coeficientes do polinômio.

Essa expressão é chamada de notação usual de representação dos polinômios e costuma ser vista na Educação Básica. No entanto, tal notação não deixa clara a distinção entre um polinômio e uma função polinomial.

A melhor maneira de definir polinômios é por meio de sequências quase nulas como é a que é feita no capítulo 3 deste trabalho. Dessa forma, além de ser possível diferenciar polinômios e função polinomial, pode-se entender o que é a "indeterminada" em tal contexto. Entretanto, após esses esclarecimentos, recomenda-se a passagem da notação por meio de sequências para a notação usual devido à simplicidade de se trabalhar com esta última.

A terna formada pelo conjunto dos números inteiros e pelas operações usuais de adição e multiplicação possui propriedades que permitem classificá-la como um anel. Este é uma estrutura algébrica mais geral formada por um conjunto não vazio e por duas operações binárias internas que possuem certas propriedades. O conjunto dos polinômios sobre um anel em uma indeterminada munido das duas operações que se definem sobre ele possui essa estrutura e, por isso, é chamado de anel de polinômios.

Quando os coeficientes de um polinômio estão contidos em $\mathbb{Z}$, o polinômio é chamado de inteiro e o anel formado por todos esses polinômios é representado por $\mathbb{Z}[x]$. Do mesmo modo, quando os coeficientes de um polinômio são elementos do conjunto dos números racionais ($\mathbb{Q}$), o anel desses polinômios é indicado por $\mathbb{Q}[x]$.

Em relação aos polinômios irredutíveis, pode-se dizer que eles possuem propriedades semelhantes àquelas que os números primos possuem no conjunto dos números inteiros. Assim, dada a importância que os números primos têm em criptografia, é possível ver também a importância dos polinômios irredutíveis em Teoria de Códigos Corretores de Erros.

Sabe-se que os números primos só admitem fatorações triviais, ou seja, toda vez que um primo é escrito como um produto $a \cdot b$ com $a, b \in \mathbb{Z}$, conclui-se que $a \in \{-1, 1\}$ ou $b \in \{-1, 1\}$. O conjunto $\{-1, 1\}$ contém todos os elementos invertíveis de $\mathbb{Z}$. Semelhantemente, um polinômio $f(x)$ é dito irredutível sobre um anel A quando se $f(x) = g(x)h(x)$ — com $g(x), h(x) \in A[x]$ —, então $g(x)$ é invertível ou $h(x)$ é invertível.

Para um número inteiro muito grande, não é fácil determinar se ele é primo ou não.

[1] Neste trabalho, o zero é considerado um número natural.

Da mesma forma, não é fácil determinar se um polinômio é irredutível ou não sobre um anel. Todavia, há critérios que auxiliam essa tarefa. Um desses é o chamado Critério de Eisenstein.[2]

Este critério possui algumas versões mais gerais, por exemplo, a exposta por Domingues e Iezzi (2003, p. 343). Porém, este trabalho está concentrado em apresentar a versão para determinar se um polinômio inteiro é irredutível em $\mathbb{Q}[x]$. Assim, pode-se enunciá-lo da seguinte forma:

> Seja $0 \neq f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n \in \mathbb{Z}[x]$. Se existe um número primo p tal que $p \nmid a_n$, $p \mid a_i$ para cada $i \in \{0, 1, \ldots, n-1\}$ e $p^2 \nmid a_0$, então $f(x)$ é irredutível em $\mathbb{Q}[x]$.

Com o uso desse critério é possível demonstrar que o polinômio ciclotômico de índice primo é irredutível sobre o conjunto dos números racionais. Essa classe de polinômio é muito importante em Teoria dos Números e dentro da Álgebra Abstrata. Inclusive, costuma-se apresentar a demonstração da irredutibilidade desses polinômios de índice primo como um corolário do Critério de Eisenstein.

Segue uma descrição dos conteúdos dos próximos capítulos. No capítulo 2, é feito um estudo da Teoria dos Anéis de modo a apresentar as definições e resultados básicos. No capítulo 3, são definidos os polinômios em uma indeterminada, bem como o conceito de anéis de polinômios e de irredutibilidade. Ainda no capítulo 3, é apresentado o Critério de Eisenstein e feita sua demonstração. Por fim, no capítulo 4, são apresentadas algumas aplicações do critério em questão, como também são definidos os polinômios ciclotômicos e feita a demonstração de irredutibilidade sobre $\mathbb{Q}$ para os de índice primo.

[2] Apesar de o critério receber esse nome, ele foi descoberto inicialmente e de forma independente por Theodor Schönemann (1812-1868). Para mais informações, recomenda-se a leitura do **Apêndice B**.

2 DEFINIÇÕES BÁSICAS

Neste capítulo, são apresentadas as definições, propriedades e resultados basilares para a devida compreensão do presente texto. Ademais, quando necessário, para melhorar o entendimento, são apresentados exemplos ou aplicações. Para elaborá-lo, foram usadas as referências Boeing (2013), Domingues e Iezzi (2003), Gonçalves (2017), Herstein (1975) e Lee (2018).

2.1 Anel

O anel é a primeira estrutura algébrica a ser definida. Por estrutura algébrica, entende-se um conjunto munido de uma ou mais operações que possuem certas propriedades. Se C é um conjunto não vazio, então uma operação binária interna em (ou sobre) C é uma função $* : C \times C \longrightarrow C$. Essa função "$*$" associa a cada par $(x, y) \in C$ um elemento $*(x, y)$, que é chamado de **composto** de x e y pela operação "$*$". Costuma-se indicar esse composto da seguinte forma $x * y$.

Definição 2.1. Um conjunto A não vazio munido de duas operações binárias internas, "+" e "$\cdot$", é chamado **anel** se para quaisquer $a, b, c \in A$ valem:

(i) $(a + b) + c = a + (b + c)$ (associatividade da adição);

(ii) $a + b = b + a$ (comutatividade da adição);

(iii) $\exists\, 0 \in A$ tal que $a + 0 = 0 + a = a$ (existência do elemento neutro para a adição);

(iv) $\exists\ -a$ tal que $a + (-a) = (-a) + a = 0$ (existência de simétricos aditivos);

(v) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (associatividade da multiplicação);

(vi) $a \cdot (b + c) = a \cdot b + a \cdot c$ e $(b + c) \cdot a = b \cdot a + c \cdot a$ (distributividade da multiplicação em relação à adição).

As operações "+" e "$\cdot$" são chamadas de **adição** e **multiplicação**, respectivamente. Os compostos $a + b$ e $a \cdot b$ são chamados de **soma** e **produto**, nessa ordem. Por conveniência, quando possível, denota-se o produto $a \cdot b$ apenas por ab.

Notação. Quando não houver ambiguidade quanto às operações envolvidas, por simplicidade, denota-se o anel $(A, +, \cdot)$ apenas por A.

Observação 2.1. O simétrico aditivo (ou inverso aditivo) de um elemento a de um anel A é único. De fato, admita, por contradição, que $b, c \in A$ são simétricos de a e que $b \neq c$. Dessa forma, se 0 é o elemento neutro, tem-se $b = b + 0$. Como c é simétrico de a, então $a + c = 0$ e, pode-se escrever $b = b + (a + c)$. Pela propriedade associativa da adição, obtém-

-se $b = (b + a) + c$. Sendo b simétrico de a, conclui-se que $b + a = 0$ e, assim, $b = c$, que é um absurdo. Pela unicidade do simétrico aditivo, pode-se considerar a operação "–": $A \times A \longrightarrow A$, que associa o par $(x, y) \in A \times A$ ao elemento $x + (-y)$. Tal operação é chamada de **subtração** e ao composto $x + (-y)$ dá-se o nome de **diferença** entre x e y. É comum indicar $x + (-y)$ apenas por $x - y$.

Vê-se que, em um anel, a adição é sempre comutativa e também possui elemento neutro. Quando a multiplicação possui propriedades adicionais, o anel recebe algumas denominações. Veja-as a seguir:

Definição 2.2. Um anel A será chamado:

(i) **anel comutativo** se para quaisquer $a, b \in A$, tem-se $a \cdot b = b \cdot a$ (comutatividade da multiplicação).

(ii) **anel com unidade**, ou **anel unitário**, se $\exists\, 1 \in A$ tal que $a \cdot 1 = 1 \cdot a = a,\ \forall\, a \in A$ (existência da unidade).

Observação 2.2. Há autores que incluem a existência da unidade na definição de anel.[1]

Observação 2.3 (Unicidade da unidade). Se A é um anel com unidade, então existe um único elemento $1 \in A$ tal que $1 \cdot a = a \cdot 1 = a$ para qualquer $a \in A$. Suponha, por absurdo, que exista um elemento $1' \neq 1$ que satisfaça $1' \cdot a = a \cdot 1' = a$ para todo $a \in A$. Dessa forma, desde que $1'$ é uma unidade, então $1 = 1 \cdot 1'$. Porém, como 1 também é uma unidade, decorre que $1 \cdot 1' = 1'$, de outra maneira, $1 = 1'$, o que é um absurdo. Isto posto, a unidade de um anel, quando existe, é única.

Além disso, de maneira similar à demonstração feita na *Observação 2.3*, prova-se que o elemento neutro da adição é único.

Seguem alguns exemplos clássicos da estrutura algébrica aqui definida.

Exemplo 2.1. O conjunto dos números inteiros munido da adição e da multiplicação usuais é um anel comutativo com unidade, podendo ser representado da seguinte forma $(\mathbb{Z}, +, \cdot)$. O zero é o elemento neutro da adição e o número 1 é a unidade.

Exemplo 2.2. $(M_2(\mathbb{Z}), +, \cdot)$ (conjunto das matrizes de ordem 2 com entradas pertencentes ao conjunto dos inteiros) é um anel não comutativo com unidade, pois:

$$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 3 & 2 \end{pmatrix}$$

e

[1] Nicolas Bourbaki (pseudônimo de um grupo de matemáticos, em sua maioria franceses, que escreveu vários livros objetivando fundamentar a matemática na Teoria dos Conjuntos) é um exemplo. Rotman (2006) é outro exemplo.

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 3 \\ 1 & 2 \end{pmatrix}.$$

Note que $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ é a unidade, pois sendo $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z})$, têm-se:

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

e

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Exemplo 2.3 (Anel dos inteiros de Gauss)**.** Um **inteiro de Gauss** é um elemento da forma $a + b \cdot i$ em que $a, b \in \mathbb{Z}$ e $i = \sqrt{-1}$. Seja $\mathbb{Z}[i]$ o conjunto formado por todos esses elementos. Note que $\mathbb{Z}[i] \subset \mathbb{C}$. O conjunto $\mathbb{Z}[i]$ munido da adição e multiplicação dos números complexos forma um anel.

Exemplo 2.4 (Conjunto dos inteiros módulo n)**.** O conjunto $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \ldots, \overline{n-1}\}$, $n \geq 1$, munido da adição e da multiplicação de classes de equivalência módulo n é um anel.[2]

A seguir são apresentadas algumas propriedades básicas dos anéis acompanhadas de suas respectivas demonstrações.

2.1.1 Propriedades básicas

Sejam $(A, +, \cdot)$ um anel cujo elemento neutro é 0 e a, b e $c \in A$. Valem as seguintes propriedades:

(i) Se $a + b = a + c$, então $b = c$.

Essa propriedade é chamada de **lei do cancelamento para a adição**. Somando o elemento $-a$ aos dois lados da igualdade da hipótese, tem-se, por associatividade, $(-a + a) + b = (-a + a) + c$, ou seja, $0 + b = 0 + c$. Logo, $b = c$.

(ii) $a \cdot 0 = 0 \cdot a = 0$.

Note que $a \cdot 0 = a \cdot (0 + 0)$. Pela propriedade distributiva, tem-se $a \cdot 0 = a \cdot 0 + a \cdot 0$. Somando $-(a \cdot 0)$ a ambos os membros, decorre que $0 = a \cdot 0$. Demonstra-se, de forma análoga, que $0 \cdot a = 0$.

[2]Recomenda-se a referência Beachy e Blair (2019, p. 38) para informações sobre esse conjunto.

(iii) $a(-b) = (-a)b = -(ab)$.

Somando $a(-b)$ e ab e usando a propriedade distributiva, obtém-se a igualdade $a(-b)+ab = a(-b+b)$, isto é, $a(-b)+ab = a\cdot 0$. Pelo item (ii), segue que $a(-b)+ab = 0$. Por consequência, $a(-b) = -(ab)$. Da mesma forma, mostra-se que $(-a)b = -(ab)$.

(iv) $(-a)(-b) = ab$.

Trocando b por $-b$ em $(-a)b = -(ab)$, tem-se $(-a)(-b) = -[a(-b)]$, isto é, $(-a)(-b) = -(-ab)$. Portanto, $(-a)(-b) = ab$.

(v) $a(b-c) = ab-ac$ e $(b-c)a = ba-ca$. Escrevendo $a(b-c)$ como $a[b+(-c)]$, obtém-se, por distributividade, $a[b+(-c)] = a\cdot b + a\cdot(-c)$. Usando o item (iii), vem que $a[b+(-c)] = ab+(-ac)$, de outra maneira, $a[b+(-c)] = ab-ac$. Assim, $a(b-c) = ab-ac$. De modo similar, prova-se que $(b-c)a = ba-ca$.

Caso A seja um anel unitário, então:

(vi) $(-1)a = -a$.

Somando a e $(-1)a$, consegue-se, pela propriedade distributiva, a igualdade $a + (-1)a = [1+(-1)]a$, ou seja, $a+(-1)a = 0\cdot a$. Pelo item (ii), verifica-se $a+(-1)a = 0$. Dessarte, $(-1)a = -a$.

(vii) $(-1)(-1) = 1$.

Tomando $a = 1$ e $b = -1$ em $(-a)b = -(ab)$, segue que $(-1)(-1) = -[1\cdot(-1)]$. Pelo item (iii), sucede que $(-1)(-1) = -(-1)$. Logo, $(-1)(-1) = 1$.

(vii) Se $1 = 0$, então $A = \{0\}$.

Se $1 = 0$, então $a = a\cdot 1 = a\cdot 0 = 0$, isto é, $A = \{0\}$.

2.1.2 Subanéis

Um subanel é um tipo especial de subconjunto de um anel. Segue sua definição.

Definição 2.3. Seja A um anel e S um subconjunto não vazio de A. Diz-se que S é um **subanel** de A se S ainda tem a estrutura de anel com as operações de A.

Notação. A notação $S \leq A$ é usada para indicar que S é um subanel de A.

Proposição 2.1. *Sejam $(A,+,\cdot)$ um anel e S um subconjunto não vazio de A. Então S é um subanel de A se, e somente se, para quaisquer $a, b \in S$:*

(i) $a - b \in S$;

(ii) $a\cdot b \in S$.

Demonstração.
($\Rightarrow$) Se S é um subanel de A, então para quaisquer $a, b \in S$, tem-se $-b \in S$ e $a + (-b) = a - b \in S$, pois "+" é uma operação em S. Além disso, $a \cdot b \in S$, pois "$\cdot$" também é uma operação em S.
($\Leftarrow$) Suponha que as duas condições são satisfeitas e que $S \subset A$. Tome $a, b \in S$ com $a = b$. Pela condição (i), segue que $a - b = a - a = 0 \in S$. Se $x \in S$, então $-x = 0 - x \in S$, pela condição (i). Agora considerando $x, y \in S$, segue que $x + y = x - (-y) \in S$, ou seja, o conjunto S é fechado[3] para a adição. Ademais, pela condição (ii), tem-se $x \cdot y \in S$ para quaisquer $x, y \in S$. Por fim, como as propriedades comutativa, associativa e distributiva são hereditárias, conclui-se que S é um subanel de A. □

São apresentados, a seguir, dois exemplos de subanéis demonstrados com o uso desta proposição.

Exemplo 2.5. Sejam A um anel e $a \in A$. O conjunto $B = \{x \in A : ax = 0\}$ é um subanel de A. De fato, $B \neq \varnothing$, pois $a \cdot 0 = 0$, ou seja, $0 \in B$. Ademais, sendo $x, y \in B$, tem-se, por distributividade, $a(x - y) = ax - ay$, isto é, $a(x - y) = 0 - 0 = 0$. Portanto, $x - y \in B$. Outrossim, por associatividade, segue que $a(xy) = (ax)y$, ou seja, $a(xy) = 0 \cdot y = 0$. Logo, $x \cdot y \in B$.

Exemplo 2.6. Seja A um anel. O conjunto $C = \{x \in A : ax = xa, \forall a \in A\}$, denominado **centro do anel** A, é um subanel de A. Com efeito, $C \neq \varnothing$, porque $a \cdot 0 = 0 \cdot a = 0$, isto é, $0 \in C$. Além disso, sendo $x, y \in C$, tem-se, pela propriedade distributiva, $a(x-y) = ax-ay$, ou seja, $a(x - y) = xa - ya$. Dessa maneira, $a(x - y) = (x - y)a$. Logo, $x - y \in C$. Além do mais, pela propriedade associativa, $a(xy) = (ax)y$, em outros termos, $a(xy) = (xa)y$. Ainda por associatividade decorre que $a(xy) = x(ay)$. Como $y \in C$, tem-se $a(xy) = x(ya)$. Por fim, novamente por associatividade, $a(xy) = (xy)a$. Portanto, $x \cdot y \in C$.

Observação 2.4. Seja S um subanel de um anel A com unidade. Podem ocorrer três situações:

- S **não ser unitário**. Como exemplo, pode-se citar o conjunto $2\mathbb{Z}$, que é um subanel de $\mathbb{Z}$ e não tem unidade. Em geral, para $n \in \mathbb{Z}$, tem-se que $n\mathbb{Z}$ é um subanel de $\mathbb{Z}$. De fato, se $a, b \in n\mathbb{Z}$ então existem $p, q \in \mathbb{Z}$ tais que $a = np$ e $b = nq$. Dessa forma, $a - b = n(p - q) \in n\mathbb{Z}$ e $a \cdot b = n(npq) \in n\mathbb{Z}$.

- S **ser unitário** e sua unidade ser a **mesma** do anel A. O conjunto dos inteiros é um subanel do conjunto dos racionais e suas unidades são as mesmas, o número 1.

- S **ser unitário** e sua unidade ser **diferente** da do anel A. Considere o anel $\mathbb{Z}_{12}$, cuja unidade é $\overline{1}$, e o subanel $\{\overline{0}, \overline{4}, \overline{8}\}$, que tem como unidade o elemento $\overline{4}$.

[3] Se $*$ é uma operação em um conjunto C, diz-se que esse conjunto é fechado para essa operação quando se quer enfatizar que, para cada $x, y \in C$, o composto $x * y$ pertence a C.

2.2 Domínio de integridade

Ao se deparar com uma equação do tipo $(x-3)(x+3)=0$, no conjunto dos números reais, conclui-se que $x-3=0$ ou $x+3=0$, ou seja, $x=3$ ou $x=-3$. Isso ocorre porque o conjunto dos números reais é um anel que não tem divisores de zero. Veja a seguir o que isso quer dizer.

Definição 2.4 (Divisores de zero)**.** Sejam a e b elementos não nulos de um anel comutativo A. Se $a \cdot b = 0$, os elementos a e b serão chamados de **divisores de zero**.

Nos exemplos que seguem, têm-se dois anéis que possuem elementos dessa natureza.

Exemplo 2.7. Considere o anel $\mathbb{Z}_6$. Têm-se $\overline{2} \neq \overline{0}$ e $\overline{3} \neq \overline{0}$ e $\overline{2} \cdot \overline{3} = \overline{0}$. Logo, $\overline{2}$ e $\overline{3}$ são divisores de zero nesse anel.

Exemplo 2.8. Seja o anel $M_2(\mathbb{Z})$. Considere os elementos $A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ e $B = \begin{pmatrix} 0 & 0 \\ 4 & 5 \end{pmatrix}$. Tem-se $A \cdot B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 4 & 5 \end{pmatrix} = \begin{pmatrix} 1\cdot 0 + 0 \cdot 4 & 1 \cdot 0 + 0 \cdot 5 \\ 0 \cdot 0 + 0 \cdot 4 & 0 \cdot 0 + 0 \cdot 5 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. Ou seja, A e B são diferentes da matriz nula e o produto entre elas é igual à matriz nula. Logo, A e B são divisores de zero.

Isso posto, pode-se definir um tipo especial de anel.

Definição 2.5 (Domínio de integridade)**.** Diz-se que um anel comutativo com unidade $A \neq \{0\}$ é um **domínio de integridade** se não possui divisores de zero, isto é, para quaisquer $a, b \in A$ com $ab = 0$ ocorre que $a = 0$ ou $b = 0$.

Observação 2.5. Um domínio de integridade também pode ser chamado de **anel de integridade** ou, simplesmente, **domínio**.

Veja mais dois exemplos.

Exemplo 2.9. O conjunto dos números inteiros é um domínio de integridade.

Exemplo 2.10. O conjunto dos inteiros de Gauss é um domínio de integridade. Como visto no **Exemplo 2.3**, esse conjunto é $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z} \text{ e } i = \sqrt{-1}\}$. Tome dois elementos não nulos $z_1, z_2 \in \mathbb{Z}[i]$. Como $\mathbb{Z}[i] \in \mathbb{C}$, pode-se escrever esses elementos usando coordenadas polares da seguinte forma $z_1 = r_1 e^{i\theta_1}$ e $z_2 = r_2 e^{i\theta_2}$, sendo r_1 e r_2 números reais maiores do que zero. Além disso, θ_1 e θ_2 são os argumentos, em radianos, de z_1 e de z_2 de forma que $0 \leq \theta_1, \theta_2 < 2\pi$. Dessa forma, tem-se $z_1 z_2 = r_1 r_2 e^{i(\theta_1+\theta_2)}$. Uma vez que r_1 e r_2 são reais maiores do que zero e que $e^{i(\theta_1+\theta_2)} \neq 0$, conclui-se que $z_1 z_2 \neq 0$.

Proposição 2.2 (Lei do cancelamento para a multiplicação)**.** *Seja A um domínio de integridade. Se $a, b, c \in A$ e $a \neq 0$, então*

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

Demonstração. Se $ab = ac$, então

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

Mas A é um domínio de integridade e $a \neq 0$, logo $b - c = 0$, ou seja, $b = c$. □

Observe que se vale a lei do cancelamento para a multiplicação em um anel $A \neq \varnothing$, então A é um domínio de integridade. Para isso, considere que $a, b \in A$ e $ab = 0$. Deve-se ter $a = 0$ ou $b = 0$. De fato, se $a \neq 0$, então $ab = a \cdot 0$ e aplicando a lei do cancelamento segue que $b = 0$. Se $b \neq 0$, obtém-se $a = 0$.

2.3 Corpos

Comparando os anéis $\mathbb{Q}$ e $\mathbb{Z}$, pode-se notar que todo elemento não nulo de $\mathbb{Q}$ possui um elemento que é simétrico em relação à multiplicação. Em $\mathbb{Z}$, se for considerado o elemento 2, é possível ver que não existe $z \in \mathbb{Z}$ tal que $2 \cdot z = 1$. Só há dois elementos não nulos em $\mathbb{Z}$ que possuem simétricos, a saber, -1 e 1. Essa diferença permite distinguir mais um caso especial de anéis: **corpo**. Previamente, é necessário definir formalmente o que é "ser simétrico em relação à multiplicação".

Definição 2.6 (Elementos invertíveis)**.** Seja A um anel com unidade. Um elemento $a \in A$ será chamado **invertível** se existir $b \in A$ tal que $a \cdot b = b \cdot a = 1$. O elemento b é chamado de inverso multiplicativo ou simétrico multiplicativo.

Notação. Para indicar o simétrico multiplicativo de a é usada a notação a^{-1}.

O conjunto dos elementos invertíveis de um anel A é indicado, neste trabalho, por $\mathcal{U}(A)$. Desse modo, pode-se escrever $\mathcal{U}(\mathbb{Z}) = \{-1, 1\}$.

Definição 2.7 (Corpo)**.** Um **corpo** é um anel comutativo com unidade em que cada elemento não nulo possui um simétrico multiplicativo.

Exemplo 2.11. Os números racionais, reais e complexos são exemplos de corpos.

Exemplo 2.12. O conjunto $\mathbb{Q}\left[\sqrt{2}\right] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ é um exemplo de corpo. Sua unidade é o elemento $1 + 0\sqrt{2} = 1$. Considerando um elemento $a + b\sqrt{2} \neq 0$ arbitrário nesse conjunto, seu inverso é $\dfrac{1}{a + b\sqrt{2}}$. Multiplicando esse último elemento por $\dfrac{a - b\sqrt{2}}{a - b\sqrt{2}}$, tem-se:

$$\frac{1}{a + b\sqrt{2}} \cdot \left(\frac{a - b\sqrt{2}}{a - b\sqrt{2}}\right) = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} + \left(\frac{-b}{a^2 - 2b^2}\right)\sqrt{2}.$$

Note que tanto $\dfrac{a}{a^2 - 2b^2}$ quanto $\dfrac{-b}{a^2 - 2b^2}$ pertencem ao conjunto dos números racionais.

Segue uma proposição que relaciona domínios e corpos.

Proposição 2.3. *Todo corpo é um domínio de integridade.*

Demonstração. Seja K um corpo e $x, y \in K$. Considere $x \neq 0$ e $x \cdot y = 0$. Então, multiplicando x^{-1} à esquerda, em ambos os membros da igualdade, tem-se $x^{-1}(xy) = x^{-1} \cdot 0$. Por associatividade, segue que $(x^{-1}x)y = 0$, isto é, $1 \cdot y = 0$. Logo, $y = 0$. Dessa forma, o conjunto K não tem divisores de zero. Consequentemente, K é um domínio de integridade. □

Para a demonstração do **Lema 2.1** a ser exposto, cabe a definição de elemento nilpotente, apresentada a seguir.

Definição 2.8 (Elementos nilpotentes)**.** Seja A um anel. Um elemento $a \in A$ é chamado **nilpotente** se existe um inteiro positivo n tal que $a^n = 0$.

Exemplo 2.13. É imediato que 0 é nilpotente, pois existe um inteiro positivo n tal que $0^n = 0$.

Exemplo 2.14. O elemento $\overline{3}$ é nilpotente em $\mathbb{Z}_9$, pois $\overline{3}^2 = \overline{0}$.

Exemplo 2.15. A matriz $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ é nilpotente no anel $(M_2(\mathbb{Z}), +, \cdot)$, porque:

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Como já visto, todo corpo é um domínio de integridade, mas nem todo domínio de integridade é um corpo. No entanto, todo domínio de integridade **finito** é um corpo. O **Lema 2.1** é apresentado em seguida com o propósito de fornecer uma demonstração para esse fato.

Lema 2.1. *O zero é o único elemento nilpotente em um domínio de integridade.*

Demonstração. Seja A um domínio de integridade e considere $x \in A$ um elemento nilpotente. Dessa forma, existe $n \in \mathbb{N} - \{0\}$ tal que $x^n = 0$. Assuma que n é o menor inteiro positivo com tal propriedade, o qual existe devido ao Princípio da Boa Ordem[4]. Se $n = 1$, então $x = 0$. Se $n > 1$, então $n - 1 \in \mathbb{N} - \{0\}$. Daí, tem-se $x^n = x \cdot x^{n-1} = 0$. Como A é um domínio de integridade, então $x = 0$ ou $x^{n-1} = 0$. Uma vez que n é o menor inteiro positivo tal que $x^n = 0$, não se pode ter $x^{n-1} = 0$. Por conseguinte, $x = 0$, ou seja, o zero é o único elemento nilpotente em um domínio de integridade. □

Proposição 2.4. *Todo domínio de integridade* ***finito*** *é um corpo.*

[4]Como sugestão para informações sobre esse princípio, veja a referência Evaristo e Perdigão (2020, p. 84).

Demonstração. Seja A um domínio de integridade finito. Considere $a \in A$ e $a \neq 0$. Se $a = 1$, então $a^{-1} = 1$. Admita então que $a \neq 1$. Será mostrado que a é invertível. Os elementos $a, a^2, a^3, a^4, \ldots$ não podem ser todos distintos, caso contrário, o conjunto A seria infinito. Dessa forma, existem $i, j \in \mathbb{N}$ tais que $a^i = a^j$, com $i < j$ (sem perda de generalidade). Então:

$$a^i = a^j \implies a^i - a^j = 0 \implies a^i(1 - a^{j-i}) = 0.$$

Como $a \neq 0$ e pelo **Lema 2.1**, conclui-se que $a^i \neq 0$. Além disso, como A é um domínio de integridade, esse conjunto não possui divisores de zero. Consequentemente, tem-se $(1 - a^{j-i}) = 0$. Daí, $1 = a^{j-i} = a \cdot a^{j-i-1}$. Desse modo, vê-se que a possui inverso multiplicativo e, portanto, o conjunto A é um corpo. □

2.4 Ideais

Em 1637, o matemático Pierre de Fermat (1601-1665) afirmou que não existem inteiros positivos x, y, z e n tais que $x^n + y^n = z^n$ para $n > 2$. Essa afirmação, conhecida como o Último Teorema de Fermat, chamou a atenção de muitos matemáticos. Um deles foi Gabriel Lamé (1795-1870), que apresentou uma "demonstração" supondo que os inteiros ciclotômicos admitiam fatoração única. A busca pela unicidade da fatoração levou Ernst Eduard Kummer (1810-1893) a desenvolver o conceito de números ideais e com esse conceito ele provou o Último Teorema de Fermat para o caso dos chamados primos regulares.

Outro matemático que se envolveu nessa busca foi Richard Dedekind (1831-1916), que, por sua vez, generalizou a ideia de número ideal para o que se entende hoje como ideal de um anel. Para mais informações sobre isso, considere ver Boeing (2013).

Definição 2.9 (Ideal)**.** Sejam A um anel e I um subconjunto não vazio de A. Diz-se que I é um **ideal** de A se:

(i) $a - b \in I$ para quaisquer $a, b \in I$;

(ii) $ai \in I$ e $ia \in I$ para todo $a \in A$ e para todo $i \in I$ (propriedade da absorção).

Existem noções de ideal à esquerda e ideal à direita. Se o conjunto A satisfizer a condição (i) e, para todo $a \in A$ e todo $i \in I$, ter-se $ai \in I$, então ele será chamado de **ideal à esquerda**. Caso o conjunto A satisfizer a condição (i) e, para todo $a \in A$ e todo $i \in I$, ocorrer $ia \in I$, ele será denominado **ideal à direita**.

Quando o anel A é comutativo, os conceitos de ideal à esquerda e ideal à direita não têm distinção.

Exemplo 2.16. Seja A um anel. Os conjuntos $\{0\}$ e A são ideais de A, chamados de **ideais triviais**.

A título de curiosidade, note que se A é um anel unitário e I é um ideal de A contendo a unidade de A, então $A = I$. Como prova, considere $a \in A$ e seja 1 sua unidade. Pela propriedade da absorção, tem-se $a \cdot 1 = a \in I$. Assim $A \subset I$, mas, por definição, $I \subset A$. Portanto, $A = I$.

Os dois exemplos subsequentes mostram ideais que não contêm a unidade do anel do qual são subconjuntos. Assim, não coincidem com o anel.

Exemplo 2.17. O conjunto dos inteiros pares é um ideal do anel dos inteiros, pois a diferença de dois números pares é um número par e o produto de um número par por qualquer inteiro é par.

Exemplo 2.18. Considere o anel $(M_2(\mathbb{R}), +, \cdot)$ e o conjunto $B = \left\{ \begin{pmatrix} x & 0 \\ y & 0 \end{pmatrix} : x, y \in \mathbb{R} \right\}$. Veja que $B \subset M_2(\mathbb{R})$. Sejam as matrizes $X, Y \in B$. É fácil ver que $X - Y \in B$. Agora, assuma $X = \begin{pmatrix} w & 0 \\ z & 0 \end{pmatrix}$ e $C = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, com $C \in M_2(\mathbb{R})$. Tem-se:

$$CX = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} w & 0 \\ z & 0 \end{pmatrix} = \begin{pmatrix} aw + bz & 0 \\ cw + dz & 0 \end{pmatrix},$$

mas

$$XC = \begin{pmatrix} w & 0 \\ z & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} wa & wb \\ za & zb \end{pmatrix}.$$

Note que $CX \in B$, mas, em geral, tem-se $XC \notin B$. Logo, o conjunto C é um ideal à esquerda, mas não o é à direita.

Proposição 2.5. *Todo ideal I de um anel A é subanel de A.*[5]

Demonstração. Será utilizada a **Proposição 2.1** para esta demonstração. Por definição de ideal, se $a \in A$ e $r \in I$, então $ar \in A$. Considere $a = 0$, então $0 \cdot r = 0 \in I$, ou seja, $0 \in I$, por conseguinte, $I \neq \varnothing$. Além disso, segue imediatamente da definição de ideal que para quaisquer $a, b \in I$, tem-se $a - b \in I$. Ainda, se $a, b \in I$, então $a \in A$, pois $I \subseteq A$. Sendo I um ideal, decorre que $ab \in I$. Logo, todo ideal de um anel A é um subanel de A. □

Lema 2.2. *Seja I um ideal de um anel A. Se I contém algum elemento invertível de A, então $I = A$.*

Demonstração. Seja $u \in I$ um elemento invertível de A. Então existe $u^{-1} \in A$ tal que $u \cdot u^{-1} = 1$. Como I é um ideal, segue que $u \cdot u^{-1} \in I$, isto é, $1 \in I$. Assim, como consequência, qualquer que seja o elemento $a \in A$, tem-se $a = 1 \cdot a \in I$. Portanto, $I = A$. □

Definição 2.10 (Ideal próprio)**.** Um ideal I de um anel A é um **ideal próprio** de A se I é um subconjunto próprio de A, isto é, $I \neq A$.

[5] Se a existência da unidade for incluída na definição de anel, então nem todo ideal é um subanel.

Proposição 2.6. *Seja K um corpo. O conjunto $\{0\}$ é o único ideal próprio de K.*

Demonstração. A demonstração será feita por contradição. Seja $I \neq \{0\}$ um ideal próprio de K. Considere $r \in I - \{0\}$. Como K é um corpo, todos os seus elementos não nulos são invertíveis. Assim, r é invertível e, pelo **Lema 2.2**, tem-se $I = K$, que é um absurdo. Logo, um corpo não possui ideais próprios além de $\{0\}$. □

Definição 2.11. Sejam A um anel comutativo com unidade e $a \in A$. O seguinte conjunto é um ideal de A, chamado de **ideal principal gerado por a**:

$$\langle a \rangle = \{ra : r \in A\}.$$

O conjunto $\langle a \rangle$ é de fato um ideal de A. Com efeito, sejam $x, y \in \langle a \rangle$. Então, $x = r_1 a$ e $y = r_2 a$ para determinados $r_1, r_2 \in A$. Tem-se $x - y = r_1 a - r_2 a = (r_1 - r_2)a \in \langle a \rangle$. Agora suponha que $z \in \langle a \rangle$ e $r \in A$. Tem-se $z = r_3 a$ para algum $r_3 \in A$. Note que $rz = r(r_3 a) = (rr_3)a \in \langle a \rangle$. Além disso, como A é um anel comutativo segue que $rz \in \langle a \rangle$.

Exemplo 2.19. O ideal $\langle \overline{2} \rangle = \{\overline{0}, \overline{2}, \overline{4}\}$ em $\mathbb{Z}_6$ é um ideal principal.

Exemplo 2.20. Se $n \in \mathbb{N} - \{0\}$, então o conjunto $n\mathbb{Z} = \{0, \pm n, \pm 2n, \ldots\}$ é um ideal principal de $\mathbb{Z}$.

Definição 2.12 (Ideal primo)**.** Um ideal próprio I de um anel comutativo A é chamado de **ideal primo** de A se:

$$a, b \in A \text{ e } ab \in I \implies a \in I \text{ ou } b \in I.$$

Exemplo 2.21. O ideal $I = \{0\}$ é um ideal primo de $\mathbb{Z}$, pois se $ab \in I$ e $a, b \in \mathbb{Z}$, então $a = 0$ ou $b = 0$.

Proposição 2.7. *O ideal $p\mathbb{Z}$ é um ideal primo do anel $\mathbb{Z}$ se, e somente se, p for um número primo.*

Demonstração.
($\Rightarrow$) A demonstração será feita por redução ao absurdo. Suponha que $p\mathbb{Z}$ é um ideal primo de $\mathbb{Z}$ e que p é composto, isto é, existem $a, b \in \mathbb{Z}$ tais que $p = ab$ e $1 < a, b < p$. Desse modo, tem-se $ab \in p\mathbb{Z}$, mas $a \notin p\mathbb{Z}$ e $b \notin p\mathbb{Z}$, ou seja, $p\mathbb{Z}$ não é um ideal primo, que é uma contradição. Logo, p é um número primo.
($\Leftarrow$) Reciprocamente, assumindo que p seja um número primo, tome $a, b \in \mathbb{Z}$ de modo que $ab \in p\mathbb{Z}$. Então, $ab = pk$ para algum $k \in \mathbb{Z}$, ou seja, $p \mid ab$. Como p é primo segue que $p \mid a$ ou $p \mid b$ (veja **Proposição A.4**). Dessa maneira, existem $k_1, k_2 \in \mathbb{Z}$ tais que $a = pk_1$ ou $b = pk_2$. Assim, $a \in p\mathbb{Z}$ ou $b \in p\mathbb{Z}$. Portanto, $p\mathbb{Z}$ é um ideal primo de $\mathbb{Z}$. □

Definição 2.13 (Ideal maximal)**.** Um ideal próprio M de um anel comutativo A é chamado **ideal maximal** de A se para qualquer ideal I de A e $M \subseteq I \subseteq A$, então $I = M$ ou $I = A$.

Exemplo 2.22. O ideal $\{0\}$ é maximal em qualquer corpo. Como visto na **Proposição 2.6**, um corpo só possui ideais triviais.

A **Proposição 2.8**, a seguir, é importante para o entendimento do próximo exemplo de ideal maximal a ser apresentado.

Proposição 2.8. *Um subconjunto não vazio I de $n\mathbb{Z}$ é um ideal de $n\mathbb{Z}$ se, e somente se, $I = m(n\mathbb{Z})$ para algum $m \in \mathbb{N}$.*

Demonstração.
($\Rightarrow$) Suponha que I é um ideal de $n\mathbb{Z}$. Então, se $I = \{0\}$ e considerando $m = 0$, tem-se $I = m(n\mathbb{Z}) = 0 \cdot (n\mathbb{Z})$. Agora, assuma que $I \neq \{0\}$. Desse modo, existe $a \in I$ com $a \neq 0$. Como I é um ideal, então I é um subanel e, dessa forma, $-a \in I$. Então, o conjunto I possui algum inteiro positivo. Pelo Princípio da Boa Ordem, o conjunto de todos os inteiros positivos de I possui um menor elemento. Seja t esse elemento. Como $t \in I \subset n\mathbb{Z}$, então existe um inteiro positivo m tal que $t = mn$. Note que $m(n\mathbb{Z}) \subset I$, pois $mn \in I$ e I é um ideal. Por outro lado, tome um elemento $u \in I$ e divida-o pelo elemento t. Dessa forma, pelo Algoritmo da Divisão de números inteiros, existem $q, r \in \mathbb{Z}$ tais que $u = tq + r$ com $0 \leq r < t$. Como u e tq estão em I, tem-se $u - tq = r \in I$. Sendo t o menor inteiro positivo em I e $0 \leq r < t$, então $r = 0$. Logo, $u = tq + 0 = tq = (mn)q = m(nq) \in m(n\mathbb{Z})$. Assim, $I \subset m(n\mathbb{Z})$. Portanto, constatada a dupla inclusão, tem-se $I = m(n\mathbb{Z})$.
($\Leftarrow$) Considere $I = m(n\mathbb{Z})$ para algum $m \in \mathbb{N}$. Dados $a, b \in I$, existem $x_1, x_2 \in \mathbb{Z}$ tais que $a = mnx_1$ e $b = mnx_2$. Segue que $a - b = mnx_1 - mnx_2 = mn(x_1 - x_2) \in I$. Agora, tomando arbitrariamente $nx_3 \in n\mathbb{Z}$, tem-se $nx_3 \cdot a = nx_3 \cdot (mnx_1) = mn(nx_3x_1) \in I$. Da mesma forma, $a \cdot nx_3 = (mnx_1) \cdot nx_3 = mn(nx_3x_1) \in I$. Portanto $I = m(n\mathbb{Z})$ é um ideal de $n\mathbb{Z}$. □

Exemplo 2.23. O ideal $4\mathbb{Z}$ é maximal no anel $2\mathbb{Z}$, pois considerando I um ideal de $2\mathbb{Z}$ tal que $4\mathbb{Z} \subseteq I \subseteq 2\mathbb{Z}$, tem-se, pela **Proposição 2.8**, que $I = 2m\mathbb{Z}$ para algum $m \in \mathbb{N}$. Como $4\mathbb{Z} \subseteq 2m\mathbb{Z}$, então $2m \mid 4$ (veja **Proposição A.1**). Como os divisores positivos de 4 são 1, 2 e 4, tem-se $m = 1$ ou $m = 2$. Dessa forma, $I = 2\mathbb{Z}$ ou $I = 4\mathbb{Z}$.

2.5 Anel quociente

Quando se tem um conjunto e uma relação de equivalência, é possível particionar tal conjunto em subconjuntos de forma que os elementos destes últimos sejam equivalentes.

Nesta seção, é considerado um anel A e a seguinte relação nessa estrutura.

Definição 2.14. Sejam A um anel e I um ideal de A. Dois elementos $a, b \in A$ são ditos **congruentes módulo** I, se $a - b \in I$.

Notação. Será usada a notação $a \equiv b \pmod{I}$ para indicar que a é congruente a b módulo I.

Observação 2.6. Uma relação é dita de equivalência quando ela é **reflexiva**, **simétrica** e **transitiva**.

Proposição 2.9. *A relação $a \equiv b \pmod{I}$ é uma relação de equivalência.*

Demonstração. De fato, a relação $a \equiv b \pmod{I}$ possui essas três propriedades.
Reflexiva: Se $a \in A$, então $a - a = 0 \in I$. Logo, $a \equiv a \pmod{I}$.
Simétrica: Sejam $a, b \in A$. Se $a \equiv b \pmod{I}$, então $a - b \in I$. Dessa forma, como I um ideal, segue que $-(a-b) \in I$, isto é, $-a + b = b - a \in I$. Portanto, $b \equiv a \pmod{I}$.
Transitiva: Sejam $a, b, c \in A$. Se $a \equiv b \pmod{I}$ e $b \equiv c \pmod{I}$, então $a - b \in I$ e $b - c \in I$. Como I é um ideal, então $(a-b) + (b-c) \in I$. Desse modo, $a - c \in I$.
Assim, a relação $a \equiv b \pmod{I}$ é de equivalência. □

Definição 2.15. Seja I um ideal de um anel A. O conjunto de todos os elementos de A que são congruentes a $a \in A$ módulo I é chamado de **classe de equivalência de a módulo I**.

Notação. A classe de equivalência de a módulo I será denotada por $\overline{a}$.

Observação 2.7. Note que, para todo $a \in A$, tem-se $\overline{a} \neq \varnothing$, porque $a \equiv a \pmod{I}$. Logo, $a \in \overline{a}$.

Proposição 2.10. *Se I é um ideal de um anel A e $a \in A$, então $\overline{a} = a + I = \{a + i : i \in I\}$.*

Demonstração. Se $x \in \overline{a}$, então $x \equiv a \pmod{I}$, ou seja, $x - a \in I$. Dessa maneira, $x = a + y$ para algum $y \in I$, isto é, $x \in a + I$. Logo, $\overline{a} \subset a + I$. Além disso, se $x \in a + I$, então existe algum $y \in I$ tal que $x = a + y$, em outros termos, $x - a = y$. Desse modo, $y \in I$, ou seja, $x - a \in I$, o que quer dizer que $x \equiv a \pmod{I}$, de onde conclui-se que $x \in \overline{a}$. Por conseguinte, $a + I \subset \overline{a}$. Portanto, $\overline{a} = a + I$. □

Observação 2.8. Sejam $x, y \in A$. Tem-se $x + I = y + I$ se, e somente se, $x - y \in I$.

O conjunto de todas as classes de equivalência geradas no anel A pelo ideal I será indicado por A/I.

Definição 2.16 (Anel quociente)**.** Seja I um ideal de um anel A. O conjunto A/I munido das seguintes operações, para quaisquer $a, b \in A$,

$$(a + I) + (b + I) = a + b + I \quad \text{e} \quad (a + I) \cdot (b + I) = a \cdot b + I$$

é chamado de **anel quociente** de A pelo ideal I.

Essas operações estão bem definidas, isto é, as operações independem do representante da classe. De fato, sejam $a_1, a_2, b_1, b_2 \in A$ tais que $(a_1 + I) = (a_2 + I)$ e $(b_1 + I) = (b_2 + I)$. Por conseguinte, $a_1 - a_2 \in I$ e $b_1 - b_2 \in I$. Como um ideal é um subanel (fechado para a adição), segue que $(a_1 - a_2) + (b_1 - b_2) \in I$, ou seja, $(a_1 + b_1) - (a_2 + b_2) \in I$, que equivale a $(a_1 + b_1) + I = (a_2 + b_2) + I$. Logo, a adição está bem definida.

Em relação à multiplicação, veja que $a_1b_1 - a_2b_2 = a_1b_1 - a_1b_2 + a_1b_2 - a_2b_2$, isto é, $a_1b_1 - a_2b_2 = a_1(b_1 - b_2) + (a_1 - a_2)b_2$. Por hipótese, têm-se $a_1 - a_2 \in I$ e $b_1 - b_2 \in I$. Uma vez que I é um ideal, decorre que $a_1(b_1 - b_2) \in I$ e $(a_1 - a_2)b_2 \in I$. Como I é fechado para a adição, conclui-se que $a_1(b_1 - b_2) + (a_1 - a_2)b_2 \in I$, isto é, $a_1b_1 - a_2b_2 \in I$, que é equivalente a escrever $a_1b_1 + I = a_2b_2 + I$. Assim, a multiplicação também está bem definida.

Pode-se verificar facilmente que o conjunto A/I munido das duas operações anteriores é um anel. Dessa forma, constata-se que $0 + I$ é o elemento neutro para a adição.

Exemplo 2.24. Como o conjunto $4\mathbb{Z}$ é um ideal de $\mathbb{Z}$, tem-se que $\mathbb{Z}/4\mathbb{Z}$ é um anel quociente. Perceba que $\mathbb{Z}/4\mathbb{Z} = \{0 + 4\mathbb{Z}, 1 + 4\mathbb{Z}, 2 + 4\mathbb{Z}, 3 + 4\mathbb{Z}\}$. Veja as tábuas de operação nesse anel:

- Tábua da adição:

$+$	$0+4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$
$0+4\mathbb{Z}$	$0+4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$
$1+4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$	$0+4\mathbb{Z}$
$2+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$	$0+4\mathbb{Z}$	$1+4\mathbb{Z}$
$3+4\mathbb{Z}$	$3+4\mathbb{Z}$	$0+4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$

- Tábua da multiplicação:

$\cdot$	$0+4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$
$0+4\mathbb{Z}$	$0+4\mathbb{Z}$	$0+4\mathbb{Z}$	$0+4\mathbb{Z}$	$0+4\mathbb{Z}$
$1+4\mathbb{Z}$	$0+4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$
$2+4\mathbb{Z}$	$0+4\mathbb{Z}$	$2+4\mathbb{Z}$	$0+4\mathbb{Z}$	$2+4\mathbb{Z}$
$3+4\mathbb{Z}$	$0+4\mathbb{Z}$	$3+4\mathbb{Z}$	$2+4\mathbb{Z}$	$1+4\mathbb{Z}$

O exemplo a seguir foi extraído de Lee (2018, p. 153).

Exemplo 2.25. Considere o anel $A = M_2(\mathbb{Z})$ e o ideal $I = M_2(2\mathbb{Z})$. O anel quociente A/I é igual ao conjunto $B = \left\{ \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} + I : b_{ij} \in \{0, 1\} \right\}$. A demonstração será feita por dupla inclusão:

($A/I \subseteq B$) Tome $\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} + I \in A/I$. Note que, para cada $a_{ij} \in \mathbb{Z}$, tem-se:

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} + I = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} + I$$

em que $b_{ij} = 0$ se a_{ij} é par e $b_{ij} = 1$ se a_{ij} é ímpar. Isso ocorre porque, nessas condições, $a_{ij} - b_{ij}$ é sempre par, ou seja,

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} - \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} = \begin{bmatrix} a_{11} - b_{11} & a_{12} - b_{12} \\ a_{21} - b_{21} & a_{22} - b_{22} \end{bmatrix} \in I.$$

$(A/I \supseteq B)$ É fácil ver que todos os elementos do conjunto B são também elementos do conjunto A/I.

Desse modo, os elementos do anel quociente A/I são do tipo $\begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} + I$ com $b_{ij} \in \{0, 1\}$. Como existem $2^4 = 16$ arranjos com repetição 4 a 4 dos elementos 0 e 1, então o conjunto A/I tem 16 elementos.

Considere os elementos $\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} + I$ e $\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} + I$. Veja como se opera esses dois elementos:

$$\left(\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} + I\right) + \left(\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} + I\right) = \begin{bmatrix} 1 & 2 \\ 1 & 2 \end{bmatrix} + I = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} + I$$

e

$$\left(\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} + I\right) \cdot \left(\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} + I\right) = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} + I.$$

2.6 Homomorfismo de anéis

O conceito de homomorfismo está ligado à ideia de preservar a estrutura das operações de dois conjuntos. De acordo com Herstein (1975, p. 54), "Se há uma ideia central que é comum a todos os aspectos da álgebra moderna, é a noção de homomorfismo."

Definição 2.17. Sejam $(A, +, \cdot)$ e $(B, +, \cdot)$ dois anéis. Uma função $\phi : A \longrightarrow B$ é um **homomorfismo** entre os anéis A e B se para quaisquer $a, b \in A$ valem:

(i) $\phi(a + b) = \phi(a) + \phi(b)$;

(ii) $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$.

Note que as operações dos anéis A e B estão sendo indicadas pelos mesmos símbolos.

Observação 2.9. Se a função ϕ for bijetiva, o homomorfismo será denominado **isomorfismo** e os anéis A e B serão chamados de **isomorfos**. Será usada a notação $A \simeq B$ para indicar que A é isomorfo a B. Além disso, um **automorfismo** de A é um isomorfismo de A em A.

Exemplo 2.26. Sejam A e B anéis quaisquer. A função $\phi : A \longrightarrow B$ definida por $\phi(x) = 0$, $x \in A$, é um homomorfismo. De fato, $\phi(a+b) = 0 = 0+0 = \phi(a)+\phi(b)$ e $\phi(a \cdot b) = 0 = 0 \cdot 0 = \phi(a) \cdot \phi(b)$ para quaisquer $a, b \in A$.

Exemplo 2.27. A função $\phi : \mathbb{Z} \longrightarrow \mathbb{Z}_n$, $n > 1$, tal que $\phi(x) = \overline{x}$, $x \in \mathbb{Z}$, é um homomorfismo. Com efeito, $\phi(a+b) = \overline{a+b} = \overline{a} + \overline{b} = \phi(a) + \phi(b)$ e $\phi(a \cdot b) = \overline{a \cdot b} = \overline{a} \cdot \overline{b} = \phi(a) \cdot \phi(b)$ para quaisquer $a, b \in \mathbb{Z}$.

Definição 2.18 (Núcleo de um homomorfismo)**.** Seja $\phi : A \longrightarrow B$ um homomorfismo de anéis. O **núcleo** desse homomorfismo é seguinte conjunto:

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

Exemplo 2.28. O núcleo do homomorfismo do **Exemplo 2.26** é $N(\phi) = A$, pois $\phi(x) = 0$ para todo $x \in A$.

Exemplo 2.29. A função $\phi : \mathbb{C} \longrightarrow \mathbb{C}$ definida por $\phi(a+bi) = a - bi$ é um homomorfismo e seu núcleo é o conjunto $N(\phi) = \{0\}$. Realmente, se $\phi(a+bi) = 0$, então $a - bi = 0$ e, consequentemente, $a = b = 0$.

Definição 2.19. Seja $\phi : A \longrightarrow B$ um homomorfismo entre anéis. A **imagem** de ϕ é o seguinte conjunto:

$$Im(\phi) = \{b \in B : b = \phi(a) \text{ para algum } a \in A\}.$$

Na proposição que segue, são apresentadas algumas propriedades importantes do homomorfismo entre anéis.

Proposição 2.11. *Se $\phi : A \longrightarrow B$ um homomorfismo de anéis, então:*

(i) $\phi(0_A) = 0_B$*;*

(ii) $\phi(-a) = -\phi(a)$, $\forall\, a \in A$*;*

(iii) $\phi(a-b) = \phi(a) - \phi(b)$ *para quaisquer* $a, b \in A$*;*

(iv) $N(\phi)$ *é um ideal de* A*;*

(v) ϕ *é injetiva se, e somente se,* $N(\phi) = \{0_A\}$*;*

(vi) $Im(\phi)$ *é um subanel de* B*.*

Demonstração. (i) Tem-se $\phi(0_A) = \phi(0_A + 0_A)$. Como ϕ é um homomorfismo, então $\phi(0_A) = \phi(0_A) + \phi(0_A)$. Subtraindo $\phi(0_A)$ de ambos os membros, segue que $0_B = \phi(0_A)$.

(ii) Sendo $a \in A$, tem-se $\phi(0_A) = \phi[a + (-a)]$. Como ϕ é um homomorfismo, então $\phi(0_A) = \phi(a) + \phi(-a)$. Pelo item (i), decorre que $0_B = \phi(a) + \phi(-a)$, isto é, $\phi(-a) = -\phi(a)$.

(iii) Recordando que $a - b = a + (-b)$ e, usando o item (ii), tem-se:

$$\phi(a - b) = \phi[a + (-b)] = \phi(a) + \phi(-b) = \phi(a) - \phi(b), \forall a, b \in A.$$

(iv) Como $\phi(0_A) = 0_B$, segue que $N(\phi) \neq \varnothing$. Agora, deve-se provar que para quaisquer $x, y \in N(\phi)$ e $a \in A$, tem-se $x - y, ax$ e $xa \in N(\phi)$. Como $x, y \in N(\phi)$, então $\phi(x) = \phi(y) = 0_B$. Daí, $\phi(x - y) = \phi(x) - \phi(y) = 0_B - 0_B = 0_B$. Logo, $x - y \in N(\phi)$. Outrossim, $\phi(xa) = \phi(a) \cdot \phi(x) = \phi(a) \cdot 0_B = 0_B$. Por conseguinte, $xa \in N(\phi)$. Similarmente, tem-se $ax \in N(\phi)$. Portanto, $N(\phi)$ é um ideal de A.

(v) ($\Rightarrow$) Suponha que ϕ é injetiva. No item (i), foi provado que $\phi(0_A) = 0_B$, ou seja, $0_A \in N(\phi)$. Dessa forma, $\{0_A\} \subset N(\phi)$. Por outro lado, se $x \in N(\phi)$, então $\phi(x) = 0_B = \phi(0_A)$. Como ϕ é injetiva, tem-se $x = 0_A$. Assim, $N(\phi) \subset \{0_A\}$. Consequentemente, $N(\phi) = \{0_A\}$.

($\Leftarrow$) Admita que $N(\phi) = \{0_A\}$. Sejam $x, y \in A$ tais que $\phi(x) = \phi(y)$. Como provado no item (iii), tem-se $\phi(x - y) = \phi(x) - \phi(y)$. Daí, $\phi(x - y) = 0_B$, ou seja, $x - y \in N(\phi) = \{0_A\}$. Desse modo, $a - b = 0_A$, isto é, $a = b$. Logo, ϕ é injetiva.

(vi) Como $0_B = \phi(0_A) \in Im(\phi)$, então $Im(\phi) \neq \varnothing$. Além do mais, se $\phi(a), \phi(b) \in Im(\phi)$, então $\phi(a) - \phi(b) = \phi(a - b)$. Daí, $\phi(a) - \phi(b) \in Im(\phi)$. Tem-se ainda $\phi(a) \cdot \phi(b) = \phi(a \cdot b)$, ou seja, $\phi(a) \cdot \phi(b) \in Im(\phi)$. Logo, $Im(\phi)$ é subanel de B. □

Teorema 2.1 (Teorema fundamental do homomorfismo entre anéis)**.** *Se $\phi : A \longrightarrow B$ é um homomorfismo, então $\psi : A/N(\phi)$ e $Im(\phi)$ são isomorfos.*

Demonstração. Considere a seguinte função:

$$\begin{aligned} \psi : A/N(\phi) &\longrightarrow Im(\phi) \\ a + N(\phi) &\longmapsto \phi(a) \end{aligned}$$

Tal função está bem definida. De fato, se $a + N(\phi) = a' + N(\phi)$, então $a - a' \in N(\phi)$. Dessa forma, $\psi(a + N(\phi)) = \phi(a) + 0$. Como $a - a' \in N(\phi)$, segue que $\psi(a + N(\phi)) = \phi(a) + \phi(a - a')$. Agora, pela definição de homomorfismo, tem-se $\psi(a + N(\phi)) = \phi(a + a' - a) = \phi(a')$, ou seja, $\psi(a + N(\phi)) = \psi(a' + N(\phi))$. A função como definida é um homomorfismo.

De fato,

$$\begin{aligned}\psi[(a+N(\phi))+(b+N(\phi))] &= \psi\left((a+b)+N(\phi)\right)\\ &= \phi(a+b)\\ &= \phi(a)+\phi(b)\\ &= \psi(a+N(\phi))+\psi(b+N(\phi)).\end{aligned}$$

Além disso,

$$\begin{aligned}\psi[(a+N(\phi))\cdot(b+N(\phi))] &= \psi\left((a\cdot b)+N(\phi)\right)\\ &= \phi(a\cdot b)\\ &= \phi(a)\cdot\phi(b)\\ &= \psi(a+N(\phi))\cdot\psi(b+N(\phi)).\end{aligned}$$

Agora, para a bijetividade da função, veja:

Injetividade: Suponha que $a+N(\phi)\in N(\psi)$. Então $\psi(a+N(\phi))=\phi(a)=0$. Assim, $a\in N(\phi)$, o que significa que $a+N(\phi)=0+N(\phi)$. Logo, $N(\psi)=\{0+N(\phi)\}$. Pelo item item (v) da **Proposição 2.11**, a função ψ é injetiva.

Sobrejetividade: Sabe-se que a imagem de ψ está contida na imagem ϕ. Falta mostrar que $Im(\phi)\subset Im(\psi)$. Considere $\phi(a)\in Im(\phi)$. Nesse caso, $a\in A$, portanto, $a+N(\phi)\in A/N(\phi)$ e $\psi(a+N(\phi))=\phi(a)$. Portanto, $Im(\phi)\subset Im(\psi)$ e a função ψ é sobrejetiva.

Desse modo, está provada a bijetividade da função ψ. Como essa função é um homomorfismo bijetivo entre os anéis $A/N(\phi)$ e $Im(\phi)$, então segue que esses anéis são isomorfos. □

No próximo capítulo, é definido o tipo de anel que mais importa para este trabalho, qual seja, anel de polinômios.

3 IRREDUTIBILIDADE EM ANÉIS DE POLINÔMIOS

Neste capítulo, são introduzidos o conceito de polinômio em uma indeterminada por meio de sequências, o de anel de polinômio e o de irredutibilidade. Além disso, nesta parte do trabalho, é apresentado e demonstrado o Critério de Eisenstein sobre $\mathbb{Q}$. A construção deste capítulo baseou-se nas referências Biazzi (2014), Domingues e Iezzi (2003), Lee (2018), Rotman (2006) e Saracino (2008).

3.1 Polinômios em uma indeterminada

Com a intenção de proporcionar uma melhor compreensão em relação ao conceito de "indeterminada" e também diferenciar função polinomial e polinômio, a definição deste será abordada por meio de sequências como é feito, por exemplo, em Rotman (2006). Para tanto, antes será definido o conceito de **sequência** em uma anel A.

Definição 3.1. Seja A um anel comutativo com unidade.[1] Uma **sequência** em A é uma função tal que $\sigma : \mathbb{N} \longrightarrow A$.

Será denotada por a_i a imagem de $i \in \mathbb{N}$ pela função σ. Dessa forma, pode-se escrever:

$$\sigma = (a_0, a_1, a_2, \ldots, a_i, \ldots),$$

em que os elementos $a_i \in A$ são chamados de **coeficientes** da sequência. Ademais, duas sequências σ e τ em A são iguais se, e somente se, $\sigma(i) = \tau(i)$ para todo $i \geq 0$. Agora, pode-se definir o que é um polinômio.

Definição 3.2. Uma sequência $\sigma = (a_0, a_1, a_2, \ldots, a_i, \ldots)$ em um anel comutativo com unidade A é chamada **polinômio** se existe algum inteiro $n \geq 0$ tal que $a_i = 0$ para todo $i > n$, ou seja, $\sigma = (a_0, a_1, a_2, \ldots, a_n, 0, 0, 0 \ldots)$.

Além disso, o polinômio $\sigma = (0, 0, 0, \ldots)$ é chamado **polinômio identicamente nulo**. Se $\sigma \neq 0$, então existe algum número natural n de forma que $a_n \neq 0$ e $a_i = 0$ para todo $i > n$. Desse modo, o coeficiente a_n é chamado **coeficiente líder**, ou **coeficiente dominante**, de σ. Quando o coeficiente líder é igual a 1, o polinômio é chamado **polinômio mônico**. Adicionalmente, quando os coeficientes do polinômio pertencem ao conjunto dos números inteiros, ele é chamado de **polinômio inteiro**. O número natural n, por sua vez, é chamado **grau** de σ e será denotado por $\partial(\sigma)$. O grau do polinômio identicamente nulo não é definido, pois todos seus coeficientes são iguais a zero. Há também o **polinômio constante** que pode referir-se ao polinômio identicamente nulo ou a um polinômio de grau zero.

[1] A exigência de o anel ser comutativo e com unidade foi apenas por conveniência.

Suponha que $\sigma = (a_0, a_1, a_2, \ldots, a_n, 0, 0, \ldots)$ e $\tau = (b_0, b_1, b_2, \ldots, b_m, 0, 0, \ldots)$ são dois polinômios com coeficientes em um anel A. A **adição** entre σ e τ é definida da seguinte forma:

$$\sigma + \tau = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots, a_i + b_i, \ldots),$$

e a **multiplicação** é definida como segue:

$$\sigma \cdot \tau = (c_0, c_1, c_2, \ldots, c_k, \ldots),$$

em que $c_k = \sum_{i+j=k} a_i \cdot b_j = \sum_{i=0}^{k} a_i \cdot b_{k-i}$.

Pelo **Lema 3.1** é possível ver que a soma e o produto de dois polinômios são também polinômios.

Lema 3.1. *Sejam A um anel comutativo com unidade e σ e τ dois polinômios não identicamente nulos com coeficientes em A.*

(i) Se $\sigma + \tau \neq 0$, então $\partial(\sigma + \tau) \leq \max(\partial(\sigma), \partial(\tau))$.

(ii) Se $\sigma \cdot \tau \neq 0$, então $\partial(\sigma \cdot \tau) \leq \partial(\sigma) + \partial(\tau)$.

(iii) Se A é um domínio de integridade, então $\sigma \cdot \tau \neq 0$ e $\partial(\sigma \cdot \tau) = \partial(\sigma) + \partial(\tau)$.

Demonstração. (i) Sejam $\sigma = (a_0, a_1, \ldots)$ e $\tau = (b_0, b_1, \ldots)$ polinômios de graus m e n, respectivamente. Sem perda de generalidade, suponha que $m > n$. Então o coeficiente líder de $\sigma + \tau$ será a_m e, desse modo, $\partial(\sigma + \tau) = m = \max(\partial(\sigma), \partial(\tau))$. Se $m = n$, então o coeficiente líder $\sigma + \tau$ será $a_m + b_m$ e, assim, $\partial(\sigma + \tau) = m$, caso $a_m + b_m \neq 0$, ou $\partial(\sigma + \tau) < m$, caso $a_m + b_m = 0$. Logo, $\partial(\sigma + \tau) \leq \max(\partial(\sigma), \partial(\tau))$.

(ii) Suponha que $\sigma = (a_0, a_1, \ldots)$ tenha grau m e $\tau = (b_0, b_1, \ldots)$ tenha grau n. Sejam $\sigma \cdot \tau = (c_0, c_1, \ldots)$ e $\partial(\sigma \cdot \tau) = k$. Assim, tem-se $c_k \neq 0$ e deve-se mostrar que $c_l = 0$ para todo $l > m + n \geq k$. Pela definição tem-se $c_l = \sum_{i+j=l} a_i \cdot b_j$. Suponha que $l > m + n$ e $i \leq m$, então $j = l - i \geq l - m > n$. Desse modo, $b_j = 0$. Agora, suponha que $i > m$ e, ainda, que $l > m + n$, então $a_i = 0$, pois $\partial(\sigma) = m$. Note que, em qualquer dos dois casos, tem-se $a_i \cdot b_j = 0$, ou seja, $c_l = 0$. Portanto, $\partial(\sigma \cdot \tau) \leq \partial(\sigma) + \partial(\tau)$.

(iii) Suponha que A é um domínio e sejam $\sigma = (a_0, a_1, \ldots)$ e $\tau = (b_0, b_1, \ldots)$ polinômios de graus m e n, respectivamente, com coeficientes em A. Além disso, seja $\sigma \cdot \tau = (c_0, c_1, \ldots)$. Tem-se $a_i = 0$, para todo $i > m$, e $b_j = 0$, para todo $j > n$. Perceba que o coeficiente de índice $m + n$ é dado por:

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

Analise os dois casos a seguir. Se $i < m$, então $m - i > 0$ e, por conseguinte, $j = m + n - i = (m - i) + n > n$. Assim, neste caso, tem-se $b_j = 0$. Agora, se $i > m$,

então $a_i = 0$, pois $\partial(\sigma) = m$. Dessa forma, cada termo do desenvolvimento do coeficiente de índice $m+n$, com exceção de $a_m b_n$, é igual a 0. Consequentemente, $c_{m+n} = a_m b_n$. Sendo $a_m \neq 0$ e $b_n \neq 0$ elementos de um domínio, segue que $c_{m+n} = a_m b_n \neq 0$ e $\sigma \cdot \tau \neq 0$. Ademais, note que para cada $k > m+n$, o desenvolvimento de c_k contém termos da forma $a_i b_{k-i}$. Como $k = i + (k-i) > m+n$, então $i > m$ ou $k - i > n$. Desse modo, o produto $a_i b_{k-i} = 0$ para todo $k > m+n$ e, como resultado, $\partial(\sigma \cdot \tau) = k = m+n = \partial(\sigma) + \partial(\tau)$. □

Sendo assim, percebe-se que tanto os coeficientes não nulos da soma quanto os do produto de dois polinômios são finitos, isto é, a soma e o produto de dois polinômios são polinômios.

Veja a demonstração em Biazzi (2014, p. 19-22) de que a adição e a multiplicação de polinômios em um anel comutativo com unidade são associativas, comutativas, possuem elemento neutro e que, além disso, existem elementos simétricos para a adição, e a multiplicação é distributiva em relação a esta. Dessa forma, o polinômio identicamente nulo é o elemento neutro para a operação de adição e o polinômio $(1, 0, 0, 0, \ldots)$ é o neutro da multiplicação. O simétrico do polinômio $\sigma = (a_0, a_1, a_2, \ldots, a_m, 0, \ldots)$, por sua vez, é o polinômio $-\sigma = (-a_0, -a_1, -a_2, \ldots, -a_m, 0, \ldots)$.

Agora, é introduzida a notação usual de polinômios como apresentada em Lee (2018). Cabe destacar que essa mudança de notação é possível devido à existência de um isomorfismo natural entre as duas formas. Para tal alteração de notação, o polinômio $(0, 1, 0, 0, \ldots)$ será identificado por x e denominado **indeterminada**. Além disso, o polinômio constante $(a_0, 0, 0, \ldots)$ será representado apenas por a_0. Pela multiplicação de polinômios como foi definida, tem-se:

$$x \cdot a_0 = (0, 1, 0, 0, \ldots) \cdot (a_0, 0, 0, \ldots) = (0, a_0, 0, 0, \ldots).$$

Analogamente,

$$a_0 \cdot x = (a_0, 0, 0, \ldots) \cdot (0, 1, 0, 0, \ldots) = (0, a_0, 0, 0, \ldots).$$

Assim, o neutro da multiplicação será indicado por $(1, 0, 0, 0, \ldots) = 1$.

Têm-se também:

$$x \cdot x = x^2 = (0, 1, 0, 0, \ldots) \cdot (0, 1, 0, 0, \ldots) = (0, 0, 1, 0, \ldots)$$

e

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

Por essas observações, pode-se conjecturar que, no polinômio x^n, com $n \geq 1$, o coeficiente de índice n é igual a 1 e os demais são todos nulos. Veja a seguir que isso de fato

ocorre.

Lema 3.2. *Se $n \geq 1$, então o polinômio x^n possui o coeficiente de índice n igual a 1 e os demais são todos iguais a zero.*

Demonstração. A demonstração será feita por indução sobre n. Para o passo base ($n = 1$), já foi visto que $x^1 = x = (0, 1, 0, 0, \ldots)$. Como hipótese de indução, admita que para algum $k \in \mathbb{N}$ o polinômio x^k possua o coeficiente de índice k igual a 1 e os demais iguais a zero. Agora, tem-se que provar que o polinômio x^{k+1} possui o coeficiente de índice $k+1$ igual a 1 e todos os outros iguais a zero. De fato, tem-se $x^{k+1} = x^k \cdot x$. Sejam $x^{k+1} = (c_0, c_1, \ldots)$, $x^k = (a_0, a_1, \ldots)$ e $x = (b_0, b_1, \ldots)$, sendo x a indeterminada. Pela multiplicação de polinômios, tem-se $c_l = \sum_{i+j=l} a_i \cdot b_j = \sum_{i=0}^{k} a_i \cdot b_{l-i}$. Note que o coeficiente de índice $k+1$ é dado por:

$$c_{k+1} = a_0 b_{k+1} + \ldots + a_1 b_k + \ldots + a_k b_1 + a_{k+1} b_0.$$

Quando $j = 1$, tem-se $b_j = 1$ e para $j \neq 1$, tem-se $b_j = 0$. Além disso, tem-se $a_i = 1$ para $i = k$ e $a_i = 0$ para $i \neq k$. Assim, conclui-se que $c_{k+1} = a_k b_1 = 1$. Se $l > k+1$, então $l = i + (l - i) > k + 1$. Desse modo, $i > k$ ou $l - i = j > 1$. Como consequência, o produto $a_i b_{l-i}$ é igual a zero. Com raciocínio análogo, nota-se que quando $l < k+1$, tem-se $l = i + (l - i) < k + 1$, ou seja, $i < k$ ou $l - i < 1$. Assim, o produto $a_i b_{l-i}$ também é igual a zero quando $l < k + 1$. Com isso, tem-se que todos os coeficientes com índice diferente de $k + 1$ são iguais a zero, e o de índice igual a k é 1. Logo, a afirmação é válida para todo $n \geq 1$. □

Com uso desse lema é possível recuperar a notação usual. Além disso, atente-se para o fato de que $(r, 0, 0, \ldots) \cdot (a_0, a_1, a_2, \ldots) = (ra_0, ra_1, ra_2, \ldots)$. E, como já mencionado, o polinômio $(r, 0, 0, \ldots)$ será representado apenas por r. Dessa forma,

$$(r, 0, 0, \ldots) \cdot (a_0, a_1, a_2, \ldots) = (ra_0, ra_1, ra_2, \ldots) = r(a_0, a_1, a_2, \ldots).$$

Com esses esclarecimentos e o uso do **Lema 3.2**, será demonstrada a proposição que segue.

Proposição 3.1. *Se $\sigma = (a_0, a_1, a_2, \ldots, a_n, 0, 0, \ldots)$ é um polinômio, então $\sigma = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$.*

Demonstração.

$$\begin{aligned}
\sigma &= (a_0, a_1, a_2, \ldots, a_n, 0, 0, \ldots) \\
&= (a_0, 0, 0, \ldots) + (0, a_1, 0, \ldots) + (0, 0, a_2, \ldots) + \ldots + (0, 0, 0, \ldots, a_n) \\
&= a_0(1, 0, 0, \ldots) + a_1(0, 1, 0, \ldots) + a_2(0, 0, 1, \ldots) + \ldots + a_n(0, 0, 0, \ldots, 1) \\
&= a_0 \cdot 1 + a_1 x + a_2 x^2 + \ldots + a_n x^n \\
&= a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n
\end{aligned}$$

□

O polinômio σ na forma $a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$ é chamado de polinômio de grau n na indeterminada x.

3.1.1 Anel de polinômios

Agora, considere o conjunto de todos os polinômios na indeterminada x com coeficientes em um anel A. Da forma como foram definidas tanto a adição quanto a multiplicação de polinômios, tal conjunto munido dessas duas operações adquire a estrutura de um anel, por isso será denominado de **anel de polinômios** sobre A na indeterminada x e será denotado por $A[x]$.

Usando a notação usual é comum escrever o polinômio σ como $p(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$.

Alguns chamam a indeterminada de **variável**. Porém, este não é o termo mais adequado, pois, como definido, x é sempre igual a $(0, 1, 0, 0, \ldots)$ e, portanto, não varia. Todavia, no contexto das funções polinomiais, a indeterminada pode assumir o papel de variável.

Definição 3.3. Sejam A um anel comutativo unitário e $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n \in A[x]$. A função $\tilde{f} : A \longrightarrow A$ definida por $\tilde{f}(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + \ldots + a_n\alpha^n$ é chamada **função polinomial** associada a $f(x)$.

Sem exigir muito rigor, pode-se escrever apenas $f(\alpha)$ no lugar de $\tilde{f}(\alpha)$. É interessante notar que polinômios distintos podem estar associados a funções polinomiais idênticas. Para ver isso, considere o anel $\mathbb{Z}_3[x]$, ou seja, o conjunto dos polinômios na indeterminada x e com coeficientes em $\mathbb{Z}_3$. Tome os polinômios $f(x) = \overline{1}x^3 + \overline{2}x$ e $g(x) = \overline{1}x^5 + \overline{2}x$, que são distintos, pois os coeficientes correspondente são diferentes. Considerando-os agora como leis de funções de $\mathbb{Z}_3$ em $\mathbb{Z}_3$, tem-se $f(x) = g(x)$; pois $f(\overline{0}) = g(\overline{0}) = \overline{0}$, $f(\overline{1}) = g(\overline{1}) = \overline{0}$ e $f(\overline{2}) = g(\overline{2}) = \overline{0}$. Logo, as funções $f(x)$ e $g(x)$ são iguais para todo $x \in \mathbb{Z}_3$.

A proposição a seguir mostra um resultado interessante.

Proposição 3.2. *Se A é domínio de integridade, então $A[x]$ também é.*

Demonstração. Como visto no item (iii) do **Lema 3.1**, se A é um domínio de integridade e $\sigma, \tau \in A[x]$ são dois polinômios não identicamente nulos, então $\sigma \cdot \tau \neq 0$. Assim, $A[x]$ é um domínio de integridade quando A também é. □

Na subseção que segue, pode-se entender que se $A[x]$ é um anel de polinômios, então A é subanel de $A[x]$. Além disso, pela **Proposição 3.3** é possível notar que $A[x]$ não tem a estrutura de corpo.

3.1.2 Imersão de A em $A[x]$

Sejam A um anel comutativo unitário e a seguinte função $\psi : A \longrightarrow A[x]$ que associa a cada $\alpha \in A$ o polinômio $f_\alpha(x) = \alpha$. A função como foi definida é um homomorfismo injetivo entre os anéis A e $A[x]$. De fato, $\psi(\alpha + \beta) = f_{\alpha+\beta}(x) = \alpha + \beta$. No entanto, $(f_\alpha + f_\beta)(x) = f_\alpha(x) + f_\beta(x) = \alpha + \beta$. Desse modo, $\psi(\alpha + \beta) = f_\alpha(x) + f_\beta(x) = \psi(\alpha) + \psi(\beta)$. De maneira similar, tem-se $\psi(\alpha \cdot \beta) = \psi(\alpha) \cdot \psi(\beta)$. Logo, a função ψ é um homomorfismo. Para a injetividade, tome $\alpha, \beta \in A$ com $\alpha \neq \beta$ e note que $f_\alpha(1_A) = \alpha$ e $f_\beta(1_A) = \beta$. Portanto, $\psi(\alpha) \neq \psi(\beta)$. Assim, está provado que $\psi : A \longrightarrow A[x]$ é um homomorfismo injetivo. Como $A/N(\psi) = A$, então pelo **Teorema 2.1**, tem-se $A \simeq Im(\psi)$, ou seja, são isomorfos. Nesse sentido, pode-se considerar $A \subset A[x]$ e A um subanel de $A[x]$.

Se A é um domínio de integridade, o conjunto dos elementos invertíveis de $A[x]$ coincide com os de A, ou seja, $\mathcal{U}(A) = \mathcal{U}(A[x])$. Assim, nem todos os elementos não nulos de $A[x]$ possuem simétrico multiplicativo e, consequentemente, $A[x]$ não é corpo. Veja a demonstração desse resultado na proposição a seguir.

Proposição 3.3. *Se A é um domínio de integridade, então $\mathcal{U}(A) = \mathcal{U}(A[x])$.*

Demonstração. Suponha que $f(x) \in A[x]$ é invertível. Dessa forma, existe $g \in A[x]$ tal que $f(x)g(x) = 1$. Como $\partial(f(x)) + \partial(g(x)) = \partial(f(x) \cdot g(x)) = 0$, então $\partial(f(x)) = \partial(g(x)) = 0$. Logo, os polinômios f e g são constantes. Pela imersão comentada anteriormente, segue que esses polinômios constantes são os elementos invertíveis do domínio A. Portanto, o conjunto dos elementos invertíveis de $A[x]$ é igual ao dos de A. □

3.2 Irredutibilidade

Levando em consideração o anel dos números inteiros, pode-se perceber que o número 3, por exemplo, só pode ser escrito em forma de produto como $3 = 1 \cdot 3$ ou $3 = (-1) \cdot (-3)$. Perceba que, nas duas formas, um dos fatores é um elemento invertível em $\mathbb{Z}$. Isso significa que o número 3 é irredutível nesse anel. Além disso, 3 é um número primo. No conjunto dos inteiros, ser primo e ser irredutível são características coincidentes. No entanto, nem sempre isso ocorre em todo anel. Por exemplo, no anel $\mathbb{Z}[\sqrt{-5}]$, o elemento 3 é irredutível, porém não é primo, veja Domingues e Iezzi (2003, p. 326).

Definição 3.4. Seja D um domínio de integridade. Um elemento $p \in D$, com $p \neq 0$ e $p \notin \mathcal{U}(D)$, é chamado **irredutível** se para quaisquer $a, b \in D$ e $p = ab$, então a é invertível ou b é invertível.

Um elemento não irredutível é chamado de redutível. Quando $D = A[x]$ é um anel de polinômios e $f(x) \in A[x]$ é um elemento irredutível, diz-se que $f(x)$ é irredutível em $A[x]$ ou sobre A.

Exemplo 3.1. Qualquer primo p é irredutível em $\mathbb{Z}$, porque se $p = ab$ com $a, b \in \mathbb{Z}$, então $a \in \{-1, 1\}$ ou $b \in \{-1, 1\}$.

Exemplo 3.2. O polinômio $3x^3 + 9x^2 + 12$ é irredutível em $\mathbb{Q}[x]$, mas redutível em $\mathbb{Z}[x]$. Observe que $3x^3 + 9x^2 + 12 = 3(x^3 + 3x^2 + 4)$ e 3 é um elemento invertível de $\mathbb{Q}[x]$, mas não de $\mathbb{Z}[x]$.

Observação 3.1. Como visto na **Proposição 3.3**, os únicos elementos invertíveis de um anel de polinômios sobre um domínio são os elementos invertíveis deste. Dessa forma, suponha que K é um corpo. Um polinômio $f(x) \in K[x]$ não nulo e não invertível é chamado de **irredutível** em $K[x]$, ou sobre K, se $p(x) = g(x)h(x)$, então $g(x)$ é constante ou $h(x)$ é constante.

Exemplo 3.3. O polinômio $x^2 - 5$ é redutível em $\mathbb{R}[x]$, pois $x^2 - 5 = \left(x - \sqrt{5}\right)\left(x + \sqrt{5}\right)$ e os polinômios $\left(x - \sqrt{5}\right)$ e $\left(x + \sqrt{5}\right)$ são ambos não constantes.

Exemplo 3.4. O polinômio $x^2 + 1$ é irredutível sobre $\mathbb{R}$, mas é redutível sobre $\mathbb{C}$. Note que $x^2 + 1 = (x - i)(x + i)$. Além disso, $x - i$ e $x + i$ são não constantes.

3.3 Critério de Eisenstein

Existem critérios variados para determinar a irredutibilidade em anéis de polinômios. No entanto, o escopo deste trabalho é apresentar as potencialidades apenas do Critério de Eisenstein. Esse critério é atribuído ao matemático alemão Ferdinand Gotthold Max Eisenstein (1823-1852), discípulo de Gauss.

Todavia, para culminar na demonstração desse critério é preciso do **Lema de Gauss**, das definições de **conteúdo de um polinômio** e de **polinômio primitivo** em $\mathbb{Z}[x]$.

Definição 3.5 (Conteúdo de um polinômio)**.** Seja $0 \neq f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n \in \mathbb{Z}[x]$. O **conteúdo** de $f(x)$, que será denotado por $\mathcal{C}(f)$, é o máximo divisor comum (mdc)[2] dos seus coeficientes, ou seja, $\mathcal{C}(f) = \text{mdc}(a_o, a_1, a_2, \ldots, a_n)$.

Exemplo 3.5. Seja o polinômio $f(x) = 2x^3 + 12x^2 + 6x + 4$. Seu conteúdo é igual ao $\text{mdc}(2, 12, 6, 4)$, isto é, $\mathcal{C}(f) = 2$.

[2]Veja a **Definição A.2** no **Apêndice A**.

Definição 3.6. Um polinômio inteiro $f(x)$ é chamado **primitivo** quando o seu contéudo é igual a 1, ou seja, quando $\mathcal{C}(f) = 1$.

Exemplo 3.6. O polinômio $g(x) = 5x^2 + 8x + 3$ é primitivo, pois $\mathcal{C}(g) = \text{mdc}(5, 8, 3) = 1$.

Perceba que se $f(x)$ é um polinômio de $\mathbb{Z}[x]$, então $f(x) = \mathcal{C}(f) \cdot \tilde{f}(x)$ sendo $\tilde{f}(x)$ um polinômio primitivo. Por exemplo, o polinômio $f(x) = 2x^3 + 12x^2 + 6x + 4$ pode ser escrito como $f(x) = 2(x^3 + 6x^2 + 3x + 2)$.

Agora, pode-se enunciar o seguinte lema.

Lema 3.3 (Lema de Gauss)**.** *O produto de dois polinômios primitivos é primitivo.*

Demonstração. Sejam $g(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ e $h(x) = b_0 + b_1x + \ldots + b_kx^k$ dois polinômios primitivos em $\mathbb{Z}[x]$. Além disso, considere $f(x) = g(x) \cdot h(x) = c_0 + c_1x + c_2x^2 + \ldots + c_mx^m$. É suficiente mostrar que existe algum coeficiente de $f(x)$ que não é divisível por algum primo p. Para tanto, seja a_r o coeficiente de $g(x)$ de maior índice que não é divisível por p, uma vez que $g(x)$ é primitivo tal coeficiente existe. Do mesmo modo, seja b_l o coeficiente de maior índice de $h(x)$ que também não é divisível por p. Sabe-se que o coeficiente de índice $r + l$ é dado por $c_{r+l} = a_0b_{r+l} + \ldots + a_{r-1}b_{l+1} + a_rb_l + a_{r+1}b_{l-1} + \ldots + a_{r+l}b_0$. Como p não divide a_r e b_l, então $p \nmid a_rb_l$, caso contrário p não seria primo. Note que para cada a_ib_j se $i > r$, então $r - i < 0$ e, por conseguinte, $j = r + l - i = (r - i) + l < l$. De maneira análoga, se $j > l$, então $i < r$. Dessa forma, p não divide a_rb_l, mas divide todos os termos restantes do desenvolvimento de c_{r+l}. Portanto, $p \nmid c_{r+l}$ e, por conseguinte, $f(x) = g(x)h(x)$ é primitivo. □

Observação 3.2. Se $0 \neq a \in \mathbb{Z}$ e $f(x) \in \mathbb{Z}[x]$, então $\mathcal{C}(a \cdot f) = |a| \cdot \mathcal{C}(f)$. Seja $f(x) = b_0 + b_1x + \ldots + b_nx^n$. Dessa forma, tem-se $f(x) = ab_0 + ab_1x + \ldots + ab_nx^n$. Para mostrar que $\text{mdc}(ab_0, ab_1, \ldots, ab_n) = |a| \cdot \text{mdc}(b_0, b_1, \ldots, b_n)$, basta usar a propriedade distributiva do mdc, a qual pode ser vista na **Proposição A.5**, no **Apêndice A**.

Ademais, para quaisquer $f(x), g(x) \in \mathbb{Z}[x]$, tem-se $\mathcal{C}(f \cdot g) = \mathcal{C}(f) \cdot \mathcal{C}(g)$. De fato, se d_1 e d_2 são os conteúdos dos polinômios $f(x)$ e $g(x)$, nessa ordem, então os polinômios $\dfrac{1}{d_1}f(x)$ e $\dfrac{1}{d_2}g(x)$ são primitivos. Desse modo, pelo Lema de Gauss, o produto $\dfrac{1}{d_1d_2}f(x)g(x)$ é também primitivo. Assim, tem-se:

$$\begin{aligned}
\mathcal{C}(f \cdot g) &= \mathcal{C}\left[d_1d_2\left(\frac{1}{d_1d_2}f(x)g(x)\right)\right] \\
&= |d_1d_2| \cdot \mathcal{C}\left(\frac{1}{d_1d_2}f(x)g(x)\right) \\
&= d_1d_2 \cdot 1 \\
&= d_1d_2 \\
&= \mathcal{C}(f) \cdot \mathcal{C}(g).
\end{aligned}$$

Uma importante consequência do **Lema 3.3** é o seguinte resultado.

Lema 3.4. *Seja $f(x) \in \mathbb{Z}[x]$. Se $f(x)$ é redutível em $\mathbb{Q}[x]$, então $f(x)$ é redutível em $\mathbb{Z}[x]$.*

Demonstração. Suponha que $g(x), h(x) \in \mathbb{Q}[x]$ são dois polinômios não constantes tais que $f(x) = g(x) \cdot h(x)$. Sejam $c, d \in \mathbb{Z}$ e $g_1(x), h_1(x) \in \mathbb{Z}[x]$. Pode-se escrever $g(x) = (1/c)g_1(x)$ e $h(x) = (1/d)h_1(x)$, ou seja, tomou-se um denominador comum aos coeficientes de cada um dos polinômios. Ademais, pode-se escrever também $g_1(x) = \mathcal{C}(g_1)g_2(x)$ e $h_1(x) = \mathcal{C}(h_1)h_2(x)$ sendo $g_2(x), h_2(x) \in \mathbb{Z}(x)$ polinômios primitivos. Dessa forma,

$$f(x) = \frac{\mathcal{C}(g_1)\mathcal{C}(h_1)}{cd} \cdot g_2(x)h_2(x). \tag{3.1}$$

Note que os graus dos polinômios g_2 e h_2 são respectivamente iguais aos de g e h. Além disso, pela igualdade (3.1), tem-se:

$$cd \cdot f(x) = \mathcal{C}(g_1)\mathcal{C}(h_1) \cdot g_2(x)h_2(x). \tag{3.2}$$

Tomando o conteúdo de ambos os membros da igualdade (3.2), obtém-se:

$$|cd| \cdot \mathcal{C}(f) = \mathcal{C}(g_1)\mathcal{C}(h_1) \cdot \mathcal{C}(g_2 \cdot h_2). \tag{3.3}$$

Pelo Lema de Gauss, tem-se $\mathcal{C}(g_2 \cdot h_2) = 1$ e, assim, a igualdade (3.3) fica:

$$\mathcal{C}(f) = \frac{\mathcal{C}(g_1)\mathcal{C}(h_1)}{|cd|}.$$

Como $\mathcal{C}(f) \in \mathbb{Z}$, então $\dfrac{\mathcal{C}(g_1)\mathcal{C}(h_1)}{|cd|} \in \mathbb{Z}$. Logo, observando a igualdade (3.1), percebe-se que $f(x)$ pode ser escrito como o produto de dois polinômios não constantes em $\mathbb{Z}[x]$. □

Teorema 3.1 (Critério de Eisenstein)**.** *Seja $0 \neq f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n \in \mathbb{Z}[x]$. Se existe um número primo p tal que:*

(i) $p \nmid a_n$,

(ii) $p \mid a_i$ *para cada* $i \in \{0, 1, \ldots, n-1\}$ *e*

(iii) $p^2 \nmid a_0$,

então $f(x)$ é irredutível em $\mathbb{Q}[x]$.

Demonstração. A prova será feita por redução ao absurdo. Se um polinômio $f(x) \in \mathbb{Z}[x]$ é redutível em $\mathbb{Q}[x]$, então ele é redutível em $\mathbb{Z}[x]$. Sendo assim, admita, por contradição, que existam $g(x), h(x) \in \mathbb{Z}[x]$ tais que $f(x) = g(x)h(x)$ e $1 \leq \partial(g(x)), \partial(h(x)) < n$ e que, também, são satisfeitas as condições do Critério de Eisenstein para um primo p. Sejam

$g(x) = b_0 + b_1x + \ldots + b_mx^m$ e $h(x) = c_0 + c_1x + \ldots + c_kx^k$. Tem-se $a_0 = b_0c_0$. Uma vez que $p \mid a_0$ e $p^2 \nmid a_0$, decorre que p divide somente um dos dois coeficientes b_0 ou c_0. Caso estes coeficientes fossem ambos divisíveis por p, então seria possível escrever $b_0 = pk_1$ e $c_0 = pk_2$ $(k_1, k_2 \in \mathbb{Z})$ e, dessa forma, $p^2 \mid b_0c_0$, que seria uma contradição. Assim, sem perda de generalidade, admita que $p \mid b_0$ e $p \nmid c_0$. Note que o coeficiente líder do polinômio f é dado por $a_n = b_m \cdot c_k$. Como $p \nmid a_n$, então, em particular, $p \nmid b_m$. Suponha que b_i, com $1 \leq i \leq m$, é o primeiro coeficiente de $g(x)$, da esquerda para a direita, de modo que $p \nmid b_i$ (uma vez que $1 \leq i \leq m$ e $p \nmid b_m$, o conjunto desses coeficientes é não vazio e, assim, pelo PBO, possui um menor elemento). Sabe-se que $a_i = b_0c_i + b_1c_{i-1} + \ldots + b_ic_0$. Dessa forma, $p \mid b_0, b_1, \ldots b_{i-1}$ e $p \nmid c_0$. Consequentemente, $p \nmid b_ic_0$, ou seja, $p \nmid a_i$, o que é um absurdo, pois $1 \leq i \leq m < n$ e, por hipótese, $p \mid a_i$ para cada $0 \leq i \leq n-1$. Desse modo, sempre que o grau do polinômio $g(x)$ for menor do que o do polinômio $f(x)$, vai existir um coeficiente a_i com $i \in \{0, 1, \ldots, n-1\}$ de forma que $p \nmid a_i$. □

Observação 3.3. Note que, se fosse feita a escolha $p \nmid b_0$ e $p \mid c_0$, a análise seria em relação ao polinômio $h(x)$.

No próximo capítulo, são apresentadas algumas aplicações desse critério.

4 APLICAÇÕES DO CRITÉRIO DE EISENSTEIN

Neste capítulo, apresentam-se algumas aplicações do critério estudado. Outrossim, é definido o polinômio ciclotômico e demonstrado que, quando este tem índice primo, ele é irredutível em $\mathbb{Q}[x]$.

4.1 Exemplos elementares

Seguem dois exemplos de aplicação direta do Critério de Eisenstein.

Exemplo 4.1. O polinômio $3x^3 + 4x^2 + 6x + 18$ é irredutível em $\mathbb{Q}[x]$. De fato, o número 2 é primo e $2 \nmid 3$, $2 \mid 4$, $2 \mid 6$ e $2 \mid 18$. Além disso, $2^2 \nmid 18$.

Exemplo 4.2. O polinômio $x^4 - 3x + 6$ é irredutível em $\mathbb{Q}[x]$ pelo Critério de Eisenstein. De início, é conveniente notar que $x^4 - 3x + 6 = x^4 + 0x^3 + 0x^2 + x + 6$. Agora, observe que, escolhendo o primo 3, tem-se $3 \nmid 1$, $3 \mid 0$, $3 \mid -3$, $3 \mid 6$ e, por fim, $3^2 \nmid 6$.

4.2 Irracionalidade de $\sqrt{2}$

Atribui-se ao matemático grego Hipaso de Metaponto a descoberta da irracionalidade da raiz quadrada de 2. Esse número pode ser visto como a medida da hipotenusa de um triângulo retângulo isósceles de catetos unitários. Como Hipaso pertencia à Escola Pitagórica e esta acreditava que todo segmento é comensurável, alguns dizem que ele foi assassinado pelos pitagóricos por ter divulgado a descoberta. A demonstração da irracionalidade de $\sqrt{2}$ envolve redução ao absurdo e pode ser vista em Iezzi e Murakami (1977, p. 46).

Segue uma outra forma de demonstrar a irracionalidade de $\sqrt{2}$, mas usando o Critério de Eisenstein.

Aplicação 4.1. O número $\sqrt{2}$ é irracional. Se x é a raiz quadrada principal de 2, então $x^2 = 2$. Assim, considere o polinômio $x^2 - 2 = x^2 - 0x - 2$. Escolhendo o primo 2, note que $2 \nmid 1$, $2 \mid 0$, $2 \mid -2$ e $2^2 = 4 \nmid 2$. Assim, pelo Critério de Eisenstein esse polinômio é irredutível sobre $\mathbb{Q}$. Porém, pelas regras de produtos notáveis, tem-se $x^2 - 2 = (x - \sqrt{2})(x - \sqrt{2})$. Como $x^2 - 2$ é irredutível em $\mathbb{Q}[x]$, segue que $\sqrt{2} \notin \mathbb{Q}$. ◀

Observação 4.1. De forma geral, se p é um número primo, então $\sqrt{p}$ é um número irracional. Seja x a raiz quadrada principal de p, então $x^2 = p$. Desse modo, pode-se considerar o polinômio $x^2 - p = x^2 + 0x - p$ e proceder de forma análoga à feita na **Aplicação 4.1**.

Este critério é uma condição suficiente para um polinômio ser irredutível em $\mathbb{Q}[x]$. Assim, caso um polinômio não o satisfaça, não quer dizer que ele não seja irredutível nesse anel. No entanto, em certos casos após aplicar uma translação $x + a$ é possível decidir se o polinômio é irredutível ou não. Veja, na proposição a seguir, porque isso é possível.

Proposição 4.1. *Se A é um domínio de integridade e $a \in A$, então a função $\varphi : A[x] \longrightarrow A[x]$ definida por $\varphi(f(x)) = f(x+a)$ é um automorfismo.*

Demonstração. Sejam $f(x), g(x) \in A[x]$ e $h(x) = f(x) + g(x)$. Tem-se $\varphi(f(x) + g(x)) = \varphi(h(x)) = h(x+a)$, ou seja, $\varphi(f(x) + g(x)) = f(x+a) + g(x+a) = \varphi(f(x)) + \varphi(g(x))$. Agora, se $p(x) = f(x) \cdot g(x)$, então $\varphi(f(x) \cdot g(x)) = \varphi(p(x)) = p(x+a)$. Dessa forma, $\varphi(f(x) \cdot g(x)) = f(x+a) \cdot g(x+a) = \varphi(f(x)) \cdot \varphi(g(x))$. Portanto, a função φ é um homomorfismo. Para a injetividade, será usado o item (v) da **Proposição 2.11**. Assim, seja $f(x) \in N(\varphi)$, isto é, $\varphi(f(x)) = 0$. Por conseguinte, tem-se $f(x+a) = 0$ e, portanto, $f(x) = 0$. Para a sobrejetividade, tome $f(x) \in A[x]$. Então existe $f(x-a) \in A[x]$ tal que $\varphi(f(x-a)) = f(x-a+a) = f(x)$. Logo, a função φ é um isomorfismo de $A[x]$ em $A[x]$ e, por conseguinte, um automorfismo. □

Assim, o polinômio $f(x)$ é irredutível sobre A se, e somente se, o polinômio $f(x+a)$ também é.

Aplicação 4.2. O polinômio $f(x) = x^2 + x + 1$ é irredutível sobre $\mathbb{Q}$. De fato, pela proposição anterior, considerando o polinômio $f(x+1)$, tem-se:

$$\begin{aligned} f(x+1) &= (x+1)^2 + (x+1) + 1 \\ &= x^2 + 2x + 1 + (x+1) + 1 \\ &= x^2 + 3x + 3 \end{aligned}$$

Agora, tomando o primo 3, decorre que $3 \nmid 1$, $3 \mid 3$ e $3^2 \nmid 3$. Logo, o polinômio $f(x+1)$ é irredutível sobre $\mathbb{Q}$ e, consequentemente, $f(x)$ também é. ◀

4.3 Polinômios ciclotômicos

Uma aplicação clássica do Critério de Eisenstein é a demonstração da irredutibilidade do p-ésimo polinômio ciclotômico em que p é primo. Gauss já tinha provado essa irredutibilidade em sua obra "Disquisitiones Arithmeticae" (1801), porém ele o fez de uma forma não tão simples.

Os polinômios ciclotômicos[1] são importantes, pois estão relacionados às raízes da unidade e aos corpos ciclotômicos. Tanto essas raízes quanto esses corpos surgem de maneira natural na Teoria dos Números, bem como na resolução de equações como a do Último Teorema de Fermat. Além disso, esse tipo de polinômios tem aplicação na demonstração do Teorema de Wedderburn, o qual diz que "todo anel de divisão finito é um corpo". Um anel de divisão é um anel com unidade em que todos os elementos não nulos possuem simétrico multiplicativo.

[1] A palavra "ciclotômico" é de origem grega e significa "divisão de ciclo". Esse termo se justifica devido ao fato de as raízes enésimas da unidade dividirem o ciclo unitário do plano complexo em n arcos de mesmo comprimento.

Para falar de polinômios ciclotômicos, são necessárias algumas definições e resultados, que são apresentadas a seguir.

Definição 4.1 (Raízes enésimas da unidade)**.** Seja n um número inteiro positivo. Uma raiz enésima da unidade é um número complexo ζ tal que $\zeta^n = 1$.

Veja em Rotman (2006, p. 27) que cada raiz enésima da unidade é dada por

$$e^{2i\pi k/n} = \cos(2\pi k/n) + i\,\mathrm{sen}\,(2\pi k/n),$$

sendo k um número inteiro no conjunto $\{1, \ldots, n\}$. Percebe-se facilmente que cada raiz primitiva é uma raiz do polinômio $x^n - 1$. Assim, pelo Teorema Fundamental da Álgebra, pode-se escrever:

$$x^n - 1 = \prod_{\zeta^n=1} (x - \zeta).$$

Diz-se que um número complexo ζ é uma **raiz enésima primitiva da unidade** quando $\zeta^n = 1$ e n é o menor número inteiro positivo para o qual isso ocorre.

Observação 4.2. Seja ζ uma raiz d-ésima primitiva da unidade. Se, para um inteiro positivo n, tem-se $\zeta^n = 1$, então $d \mid n$. Com efeito, pelo algoritmo da divisão de números inteiros,[2] existem únicos inteiros q e r tais que $n = qd + r$ como $0 \leq r < d$. Entretanto,

$$1 = \zeta^n = \zeta^{qd+r} = \zeta^{qd}\zeta^r = (\zeta^q)^d\,\zeta^r = 1\zeta^r = \zeta^r.$$

Se $r \neq 0$, então seria um absurdo, uma vez que d é o menor número inteiro para o qual $\zeta^d = 1$. Assim, deve-se ter $r = 0$, ou seja, $n = qd$. Portanto, $d \mid n$.

Diante disso, segue a definição de polinômio ciclotômico.

Definição 4.2 (Polinômio ciclotômico)**.** Se d é um número inteiro positivo, então o **d--ésimo polinômio ciclotômico** é igual a

$$\Phi_d(x) = \prod(x - \zeta),$$

em que ζ é uma raiz d-ésima primitiva da unidade.

Assim, se $1 \leq d \leq 6$, então $\Phi_1(x) = x - 1$, $\Phi_2(x) = x + 1$, $\Phi_3(x) = x^2 + x + 1$, $\Phi_4(x) = x^2 + 1$, $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$ e $\Phi_6(x) = x^2 - x + 1$.

Antes de ser apresentada a próxima proposição, relembre que se n é um inteiro positivo, então:

$$x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + \ldots + x^2 + x + 1) \tag{4.1}$$

[2] Veja Domingues e Iezzi (2003, p. 34) para informações sobre esse algoritmo.

Isso pode ser comprovado resolvendo a multiplicação à direita, ou seja:

$$\begin{aligned}(x-1)(x^{n-1}+x^{n-2}+\ldots+x^2+x+1) &= x(x^{n-1}+x^{n-2}+\ldots+x^2+x+1)\\ &\quad -1(x^{n-1}+x^{n-2}+\ldots+x^2+x+1)\\ &= x^n+x^{n-1}+x^{n-2}+\ldots+x^3+x^2+x\\ &\quad -x^{n-1}-x^{n-2}+\ldots-x^2-x-1\\ &= x^n-1\end{aligned}$$

Observe que, quando $n = 6$, tem-se $x^6 - 1 = (x^3)^2 - 1^2 = (x^3 - 1)(x^3 + 1)$, ou seja, $x^6-1 = (x-1)(x^2+x+1)(x+1)(x^2-x+1)$. Organizando os fatores de forma conveniente, pode-se escrever $x^6 - 1 = (x - 1)(x + 1)(x^2 + x + 1)(x^2 - x + 1)$. Perceba que

$$x^6 - 1 = \Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x).$$

Além disso, note que, para cada $\Phi_d(x)$ presente na fatoração do polinômio $x^6 - 1$, tem-se $d \mid 6$. Veja agora a proposição que segue.

Proposição 4.2. *Para cada inteiro $n \geq 1$, tem-se:*

$$x^n - 1 = \prod_{d|n} \Phi_d(x),$$

em que d é algum divisor positivo de n.

Demonstração. A demonstração é feita tomando, para cada divisor d de n, os termos da fatoração de $x^n - 1 = \prod_{\zeta^n=1} (x-\zeta)$ nos quais ζ é uma raiz d-ésima primitiva da unidade, isto é:

$$x^n - 1 = \prod_{1\leq k\leq n} \left(x - e^{2ik\pi/n}\right) = \prod_{d|n} \prod_{\substack{1\leq k\leq n\\(k,n)=d}} \left(x - e^{2ik\pi/n}\right) = \prod_{d|n} \Phi_{\frac{n}{d}}(x) = \prod_{d|n} \Phi_d(x).$$

Nesta demonstração, (k, n) representa o máximo divisor comum entre k e n. Sejam os conjuntos $A_n = \{1, 2, \ldots, n\}$ e $B_d = \{k \in A_n : (k, n) = d\}$. Pode-se mostrar que a família de subconjuntos $\{B_d : d \mid n\}$ é uma partição de A_n. Isso explica a passagem do produtório simples para o duplo. A passagem de $\Phi_{\frac{n}{d}}(x)$ para $\Phi_d(x)$ se justifica, porque há uma bijeção no conjunto $D(n) = \{d \mid n : d > 0\}$ nele mesmo tal que $n \longmapsto \dfrac{n}{d}$. □

Se d é igual a um número primo p, então seus únicos divisores positivos são 1 e p. Dessa maneira, $x^p - 1 = \Phi_1(x)\Phi_p(x)$, ou seja, $x^p - 1 = (x - 1)\Phi_p(x)$. Pela igualdade 4.1, segue que $\Phi_p(x) = x^{p-1} + x^{p-2} + \ldots + x^2 + x + 1$.

A seguir é demonstrado que todo p-ésimo polinômio ciclotômico, em que p é primo, é irredutível sobre $\mathbb{Q}$.

Aplicação 4.3. O polinômio

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1$$

é irredutível em $\mathbb{Q}[x]$ para qualquer primo p.

Como não é possível aplicar o Critério de Eisenstein diretamente, considere o polinômio $\Phi_p(x+1)$. Dessa forma, obtém-se $\Phi_p(x+1) = \dfrac{(x+1)^p - 1}{(x+1) - 1}$.

Pelo Teorema Binomial (A.2), tem-se que o termo $(x+1)^p$ é igual a:

$$(x+1)^p = \binom{p}{0}x^p + \binom{p}{1}x^{p-1} + \binom{p}{2}x^{p-2} + \binom{p}{3}x^{p-3} + \ldots + \binom{p}{p-1}x^1 + \binom{p}{p}x^0,$$

em que $\binom{p}{k} = \dfrac{p!}{(p-k)!k!}$. Assim, pelas propriedades[3] $\binom{p}{1} = \binom{p}{p-1} = p$ e $\binom{p}{0} = \binom{p}{p} = 1$, tem-se:

$$\begin{aligned}\Phi_p(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} &= \frac{\binom{p}{0}x^p + \binom{p}{1}x^{p-1} + \binom{p}{2}x^{p-2} + \binom{p}{3}x^{p-3} + \ldots + \binom{p}{p-1}x^1 + \binom{p}{p}x^0 - 1}{x} \\ &= \frac{x^p + \binom{p}{1}x^{p-1} + \binom{p}{2}x^{p-2} + \binom{p}{3}x^{p-3} + \ldots + px}{x} \\ &= x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + \binom{p}{3}x^{p-4} + \ldots + p\end{aligned}$$

Pela **Proposição A.6**, o número primo p divide $\binom{p}{k}$ para $1 \leq k \leq p-1$. Além disso, $p \nmid 1$ e $p^2 \nmid p$. Logo, pelo Critério de Eisenstein esse polinômio é irredutível sobre $\mathbb{Q}$. ◀

4.4 Outras aplicações

Para finalizar este capítulo, seguem as duas últimas aplicações.

Aplicação 4.4. Seja p um número primo. O polinômio $x^p + px + p - 1$ é irredutível sobre $\mathbb{Q}$ se, e somente se, $p \geq 3$.

Para que o Critério de Eisenstein, possa ser aplicado, considere o seguinte o polinômio:

$$f(x+1) = (x+1)^p + p(x+1) + p - 1.$$

Já se sabe que $(x+1)^p$ é igual a:

$$(x+1)^p = \binom{p}{0}x^p + \binom{p}{1}x^{p-1} + \binom{p}{2}x^{p-2} + \binom{p}{3}x^{p-3} + \ldots + \binom{p}{p-1}x^1 + \binom{p}{p}x^0.$$

Desse modo,

[3] Veja a *Observação A.4* no **Apêndice A**.

$$(x+1)^p = x^p + px^{p-1} + \binom{p}{2}x^{p-2} + \binom{p}{3}x^{p-3} + \ldots + px + 1.$$

Assim,

$$\begin{aligned} f(x+1) &= x^p + px^{p-1} + \binom{p}{2}x^{p-2} + \binom{p}{3}x^{p-3} + \ldots + px + 1 + p(x+1) + p - 1 \\ &= x^p + px^{p-1} + \binom{p}{2}x^{p-2} + \binom{p}{3}x^{p-3} + \ldots + px + 1 + px + p + p - 1 \\ &= x^p + px^{p-1} + \binom{p}{2}x^{p-2} + \binom{p}{3}x^{p-3} + \ldots + 2px + 2p. \end{aligned}$$

Como dito anteriormente $p \mid \binom{p}{k}$ para cada $1 \leq k \leq p-1$. Além disso, observe que se $p = 2$, tem-se $p^2 = 2^2 = 2p$, isto é, $p^2 \mid 2p$. Então, pelo Critério de Eisenstein o polinômio dado é irredutível sobre $\mathbb{Q}$ só quando $p \geq 3$. ◀

Aplicação 4.5. O polinômio $f(x) = x^{101} + 101x^{100} + 102$ é irredutível em $\mathbb{Q}[x]$.

Considere o polinômio $f(x-1)$. Desenvolvendo-o, tem-se:

$$\begin{aligned} f(x-1) &= (x-1)^{101} + 101(x-1)^{100} + 102 \\ &= x^{101} - 101x^{100} + \binom{101}{2}x^{99} + \ldots - 101x - 1 + 101x^{100} - 101 \cdot 100x^{99} + \ldots + \\ &\quad + 101 \cdot 100x + x + 101 \cdot 1 + 102 \end{aligned}$$

Note que o coeficiente constante desse polinômio é $-1 + 101 + 102 = 202$. Considerando o primo 101, tem-se que esse número não divide o coeficiente líder e divide cada coeficiente não líder. Além disso, $101^2 \nmid 202$. Portanto, o polinômio dado é irredutível sobre $\mathbb{Q}$. ◀

5 CONSIDERAÇÕES FINAIS

Como visto, o Critério de Eisenstein possui várias aplicações em Álgebra Abstrata. Sua importância no estudo da prova de irredutibilidade dos polinômios ciclotômicos de índice primo pode ser percebida pela simplicidade dessa demonstração, a qual Gauss tinha obtido de uma maneira mais trabalhosa.

Cabe destacar que este trabalho trata-se apenas de um estudo inicial desse assunto e pode ser futuramente ampliado no sentido de avaliar solubilidade e, assim, irredutibilidade de polinômios com coeficientes em estruturas algébricas mais sofisticadas, como as álgebras.

REFERÊNCIAS

ALENCAR FILHO, Edgard de. **Teoria elementar dos Números**. São Paulo: Nobel, 1981.

BEACHY, John A.; BLAIR, William D. **Abstract Algebra**. 4. ed. Long Grove: Waveland Press, 2019.

BIAZZI, Ricardo Neves. **Polinômios irredutíveis**: critérios e aplicações. 2014. Dissertação (Mestrado Profissional em Matemática em Rede Nacional) - Instituto de Geociências e Ciências Exatas, Universidade Estadual Paulista, Rio Claro, 2014.

BOEING, Francielle Kuerten. **Fatoração Única em Corpos Ciclotômicos e o Último Teorema de Fermat**. 2013. Trabalho de Conclusão de Curso (Licenciatura em Matemática) - Centro de Ciências Tecnológicas, Universidade do Estado de Santa Catarina, Joinville, 2013.

COX, David A. Why Eisenstein proved the Eisenstein criterion and why Schönemann discovered it first. **The American Mathematical Monthly**, v. 118, n. 1, p. 3-21, 2011.

DOMINGUES, Hygino H.; IEZZI, Gelson. **Álgebra moderna**. 4. ed. reform. São Paulo: Atual, 2003.

EVARISTO, Jaime; PERDIGÃO, Eduardo. **Introdução à Álgebra Abstrata**. 3. ed. Maceió: Edufal, 2020.

GONÇALVES, Adilson. **Introdução à Álgebra**. 6. ed. Rio de Janeiro: IMPA, 2017.

HAZZAN, Samuel. **Fundamentos de matemática elementar**: combinatória, probabilidade. v. 5. 3. ed. São Paulo: Atual, 1977.

HERSTEIN, Israel Nathan. **Topics in Algebra**. 2. ed. New York: Wiley, 1975.

IEZZI, Gelson; MURAKAMI, Carlos. **Fundamentos de Matemática elementar**: conjuntos, funções. v.1 . 3. ed. São Paulo: Atual, 1977.

KLEINER, Israel. **A History of Abstract Algebra.** [S.l.]. Birkhäuser, 2007.

LEE, Gregory T. **Abstract Algebra: An Introductory Course**. [S.l.]. Springer, 2018.

ROTMAN, Joseph J. **A First Course in Abstract Algebra**. [S.l.]. Pearson Prentice Hall, 2006.

SANTOS, José Plínio de Oliveira Santos. **Introdução à Teoria dos Números**. Rio de Janeiro: IMPA, 1998.

SARACINO, Dan. **Abstract Algebra**: A First Course. 2. ed. Long Grove: Waveland Press, 2008.

SCHMITZ, M. The life of Gotthold Ferdinand Eisenstein. **Research Letters in the Information and Mathematical Sciences**, 2004, v. 6, p. 1-13.

APÊNDICE A – TEORIA DOS NÚMEROS

Neste apêndice, são apresentadas algumas definições e resultados importantes de Teoria dos Números que foram usados ao longo deste trabalho. A composição deste apêndice foi feita com base nas referências Alencar Filho (1981), Beachy e Blair (2019), Hazzan (1977), Rotman (2006) e Santos (1998).

A.1 Divisibilidade

A seguir é apresentada a definição de divisibilidade no anel dos números inteiros.

Definição A.1. Sejam a e b dois números inteiros. Diz-se que a **divide** b se existe um inteiro c tal que $b = a \cdot c$.

Quando a divide b, diz-se também que b é **múltiplo** de a ou que a é um **divisor**, ou **fator**, de b. Ainda, pode-se dizer que b é **divisível** por a. A notação para indicar que a divide b é $a \mid b$. Caso contrário, escreve-se $a \nmid b$.

Exemplo A.1. O número 5 divide o número 20, pois $20 = 5 \cdot 4$ e $4 \in \mathbb{Z}$. Assim, o número 20 é um múltiplo de 5.

Exemplo A.2. O número 0 divide o próprio número 0, porque $0 = 0 \cdot 0$ e $0 \in \mathbb{Z}$. Cabe destacar que o único múltiplo de 0 é o próprio 0, uma vez que, para qualquer c inteiro, tem-se $c \cdot 0 = 0$. Além disso, com essa mesma justificativa pode-se notar que 0 é múltiplo de qualquer número inteiro.

Pode-se denotar o conjunto de todos os múltiplos de um inteiro a da seguinte forma $a\mathbb{Z} = \{b \in \mathbb{Z} : b = a \cdot c \text{ para algum } c \in \mathbb{Z}\}$. Dessa maneira, o conjunto formado por todos os múltiplos de 5 pode ser representado por $5\mathbb{Z} = \{\ldots, -20, -15, -10, -5, 0, 5, 10, 15, 20, \ldots\}$.

Se um inteiro b é múltiplo de um inteiro a, então todo múltiplo de b é também múltiplo de a. Veja a proposição a seguir.

Proposição A.1. *Se a e b são dois números inteiros, então $a \mid b$ se, e somente se, $b\mathbb{Z} \subseteq a\mathbb{Z}$.*

Demonstração.
($\Rightarrow$) Se $a \mid b$, então existe $c \in \mathbb{Z}$ tal que $b = a \cdot c$. Agora, tome $x \in b\mathbb{Z}$. Assim, existe um certo $k \in \mathbb{Z}$ de modo que $x = b \cdot k$. Por substituição, decorre que $x = (a \cdot c) \cdot k$. Usando a propriedade associativa da multiplicação, tem-se $x = a \cdot (c \cdot k)$, ou seja, $x \in a\mathbb{Z}$. Portanto, $b\mathbb{Z} \subseteq a\mathbb{Z}$.
($\Leftarrow$) Reciprocamente, se $b\mathbb{Z} \subseteq a\mathbb{Z}$, então $b \in a\mathbb{Z}$. Consequentemente existe $q \in \mathbb{Z}$ tal que $b = aq$, isto é, $a \mid b$.

□

A proposição a seguir apresenta propriedades importantes da divisibilidade de números inteiros.

Proposição A.2. *Se $a, b, c \in \mathbb{Z}$, então valem as seguintes propriedades:*

(i) $a \mid a$.

(ii) Se $a \mid b$, *então* $a \mid bc$.

(iii) Se $a \mid b$, *então* $ca \mid bc$.

(iv) Se $ca \mid cb$ *e* $c \neq 0$, *então* $a \mid b$.

(v) $1 \mid a$.

(vi) Se $a \mid b$ *e* $b \neq 0$, *então* $|a| \leq |b|$.

(vii) Se $a \mid b$ *e* $b \mid a$, *então* $|a| = |b|$.

(viii) Se $a \mid b$ *e* $a \neq 0$, *então* $\dfrac{b}{a} \mid b$.

Proposição A.3. *Sejam $a, b, c, m, n \in \mathbb{Z}$. Se $c \mid a$ e $c \mid b$, então $c \mid (am + an)$.*

Demonstração. Por definição, se $c \mid a$ e $c \mid b$, então existem $k_1, k_2 \in \mathbb{Z}$ tais que $a = ck_1$ e $b = ck_2$. Multiplicando a igualdade $a = ck_1$ por m e, a $b = ck_2$ por n, obtêm-se $ma = mck_1$ e $nb = nck_2$. Agora, adicionando essas duas ultimas igualdades, tem-se $ma+nb = mck_1+nck_2$, ou seja, $ma + nb = (mk_1 + nk_2)c$. Portanto, $c \mid (ma + nb)$. □

A seguir será apresentada a definição de um divisor muito importante.

Definição A.2. Sejam $a, b \in \mathbb{Z}$, ambos não nulos ao mesmo tempo. Um inteiro d é chamado **máximo divisor comum** de a e b se $d \mid a$ e $d \mid b$. Além disso, qualquer divisor comum de a e de b é também divisor de d.

Para denotar o **máximo divisor comum** de a e b será usada a notação $\text{mdc}(a, b)$. Costuma-se também representar esse divisor por (a, b).

O resultado a seguir é um teorema muito importante em Teoria dos Números envolvendo o máximo divisor comum de dois números inteiros.

Teorema A.1 (Identidade de Bézout)**.** *Se $a, b \in \mathbb{Z}$ (a ou b diferente de zero) e $d = \text{mdc}(a, b)$, existem $x, y \in \mathbb{Z}$ tais que*

$$d = ax + by.$$

Demonstração. Veja Santos (1998, p. 5). □

Corolário A.1. *Se* $\text{mdc}(a,b) = 1$ *e* $a \mid bc$*, então* $a \mid c$*.*

Demonstração. Suponha que $\text{mdc}(a,b) = 1$ e e $a \mid bc$. Pela Identidade de Bézout, existem $x, y \in \mathbb{Z}$ de forma que $1 = ax+by$. Multiplicando essa igualdade por c, obtém-se $c = cax+cby$. Como $a \mid cax$ e $a \mid cby$ (que segue da hipótese e do item (ii) da **Proposição A.2**), conclui-se, pela **Proposição A.3**, que $a \mid (cax + cby)$, ou seja, $a \mid c$. □

A seguir é apresentada a definição de número primo.

Definição A.3. Um número inteiro $p > 1$ é chamado primo se, e somente se, o conjunto dos seus divisores positivos é $\{1, p\}$.

Quando um número inteiro maior do que 1 não é **primo**, ele é chamado **composto**.

Observação A.1. Sejam p um número primo e a um número inteiro. Então, $\text{mdc}(a,p) = 1$ se, e somente se, $p \nmid a$. De fato, como p é primo seus únicos divisores positivos são 1 e p. Sabe-se que 1 divide qualquer número. Se $p \mid a$, então o único divisor comum é 1.

Proposição A.4. *Se* p *é primo e* $p \mid ab$*, então* $p \mid a$ *ou* $p \mid b$*.*

Demonstração. Suponha que p é primo e que $p \mid ab$. Se $p \mid a$, não há o que provar. Se $p \nmid a$, então, pela observação anterior, $\text{mdc}(a,p) = 1$ e, pelo **Corolário A.1**, decorre que $p \mid b$. □

Observação A.2. Essa propriedade pode ser generalizada da seguinte forma. Se p é um número primo e $p \mid a_1 a_2 \dots a_n$, então $p \mid a_i$ para algum $i \in \{1, 2, \dots, n\}$. De fato, escrevendo o $a_1 a_2 \dots a_n$ como $a_1(a_2 \dots a_n)$, tem-se, pela **Proposição A.4**, $p \mid a_1$ ou $p \mid a_2 \dots a_n$. Se $p \mid a_1$, está provado. Se $p \nmid a_1$, então $p \mid a_2 \dots a_n$. Dessa forma, escreve-se $a_2 \dots a_n = a_2(a_3 \dots a_n)$ e repete-se a análise feita. Repetindo-se esse processo n vezes tem-se o resultado.

Proposição A.5 (Propriedade distributiva do mdc)**.** *Se* $a, b, t \in \mathbb{Z}$ *e* $t \neq 0$*, então*

$$\text{mdc}(ta, tb) = |t| \,\text{mdc}(a,b).$$

Demonstração. Sejam $c = \text{mdc}(ta, tb)$ e $d = \text{mdc}(a,b)$. Assim, por definição de mdc, $d \mid a$ e $d \mid b$. Pelo item (iii) da **Proposição A.2**, têm-se $td \mid ta$ e $td \mid tb$. Como c é o mdc de ta e de tb, então, por definição, $td \mid c$. Consequentemente, existe $x \in \mathbb{Z}$ tal que $c = tdx$. Desse modo, $tdx \mid ta$ e $tdx \mid tb$, isto é, $dx \mid a$ e $dx \mid b$. Como $d = \text{mdc}(a,b)$, segue que $dx \mid d$, ou seja, $x \mid 1$. Logo, $x \in \{1, -1\}$. Assim, $c = |td|$. Como d é um máximo divisor comum, então $d > 0$ e, por conseguinte, $c = |t|d$. Portanto, $\text{mdc}(ta, tb) = |t| \,\text{mdc}(a,b)$. □

Observação A.3. Essa propriedade pode ser generalizada para n números inteiros, ou seja:

$$\text{mdc}(ta_1, ta_2, \dots, ta_n) = |t| \,\text{mdc}(a_1, a_2, \dots, a_n).$$

A.2 Números binomiais

Antes de definir número binomial, é preciso saber o que é um fatorial.

Definição A.4. Seja n um número inteiro não negativo. O **fatorial** de n, denotado por $n!$, é o número inteiro tal que:

$$n! = \begin{cases} 1 \text{ se } n = 0 \text{ ou } n = 1 \\ n \cdot (n-1) \cdot (n-2) \ldots 3 \cdot 2 \cdot 1 \text{ se } n \geq 2 \end{cases}$$

O fatorial de n também pode ser chamado n fatorial.

Exemplo A.3. $5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120$.

De forma geral, tem-se $n! = n(n-1)!$.

A seguir, apresenta-se a definição de número binomial.

Definição A.5. Sejam n e k dois números inteiros tais que $0 \leq k \leq n$. Chama-se **número binomial** de numerador n e classe k o número inteiro $\binom{n}{k}$ de forma que

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

Exemplo A.4. $\binom{10}{8} = \dfrac{10!}{8!(10-8)!} = \dfrac{10 \cdot 9 \cdot 8!}{8! \cdot 2!} = \dfrac{10 \cdot 9}{2} = 45.$

Toda expressão do tipo $(x+y)^n$ em que $x, y \in \mathbb{R}$ e $n \in \mathbb{N}$ é chamada de **binômio de Newton**.

Observação A.4. Os seguintes casos particulares seguem da definição:

(i) $\binom{n}{0} = \dfrac{n!}{0!(n-0)!} = \dfrac{n!}{1 \cdot n!} = \dfrac{n!}{n!} = 1.$

(ii) $\binom{n}{1} = \dfrac{n!}{1!(n-1)!} = \dfrac{n(n-1)!}{1 \cdot n!} = \dfrac{n(n-1)!}{(n-1)!} = n.$

(iii) $\binom{n}{n} = \dfrac{n!}{n!(n-n)!} = \dfrac{n!}{n! \cdot 0!} = \dfrac{n!}{n! \cdot 1} = \dfrac{n!}{n!} = 1.$

Teorema A.2 (Teorema Binomial)**.** *Se $x, y \in \mathbb{R}$ e $n \in \mathbb{N}$, então:*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k.$$

Demonstração. Veja Hazzan (1977, p. 50). □

Proposição A.6. *Se p é um número primo, então $p \mid \binom{p}{k}$ para $0 < k < p$.*

Demonstração. Sabe-se que:

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p(p-1)\dots(p-k+1)}{k!}.$$

Dessa forma, tem-se $k!\binom{p}{k} = p(p-1)\dots(p-k+1)$, isto é, $p \mid k!\binom{p}{k}$. Se $p \mid k!$, então, pela *Observação A.2*, p divide algum fator de $k!$. Uma vez que $0 < k < p$, então cada fator de $k!$ é estritamente menor do que p. Assim, p não divide nenhum desses fatores e, consequentemente, $p \nmid k!$. Portanto, pela **Proposição A.4**, tem-se $p \mid \binom{p}{k}$ para cada $0 < k < p$. □

APÊNDICE B – NOTA HISTÓRICA

Conforme Kleiner (2007), a palavra "álgebra" até o início do século XIX significava resolver equações polinomiais. Os polinômios não eram tratados como entes separados destas. Na aritmética do matemático grego Diofanto de Alexandria (250 a.C.), por exemplo, eles podem ser interpretados como "lados" das equações. O primeiro passo no desenvolvimento da escrita dos polinômios foi dado por esse matemático, considerado por muitos como "o pai da Álgebra". Ele criou uma notação para valores desconhecidos de um problema, representando-os pela letra grega ς, a qual é a última letra da palavra grega "ἀριθμός" (número). Além disso, ele também introduziu outras notações, a saber, Δ^{Υ} para o quadrado da quantidade desconhecida, K^{Υ} para o cubo da quantidade desconhecida, $\Delta^{\Upsilon}\Delta$ para a quarta potência, e assim por diante. Essa notação permitia a escrita apenas de polinômios de grau no máximo igual a 6. Usando a escrita de Diofanto, o polinômio $x^3 - 3x^2 + 2x + 4$ era representado por $K^{\Upsilon}\alpha\varsigma\beta\mathring{M}\delta \pitchfork \Delta^{\Upsilon}\gamma$, sendo $\alpha = 1$, $\beta = 2$, $\gamma = 3$ e $\delta = 4$ e o símbolo $\pitchfork$ usado para o sinal negativo; não havia equivalente para o atual "+" e, por isso, os termos positivos eram indicados juntos. Além disso, nessa notação o símbolo $\mathring{M}$ era usado para indicar o termo constante e vinha sempre acompanhado de um coeficiente.

Outros matemáticos que tiveram contribuição nessa trajetória foram Al-Khwarizmi e Al-Karaji (953-1029). Este último não só estendeu a notação de Diofanto para escrever polinômios de graus maiores, como também forneceu regras para as operações com estes.

Foi o matemático francês François Viète (1540-1603) que introduziu a notação moderna e as regras de manipulação algébrica. Considerado por vários historiadores como o fundador da Álgebra Moderna, ele representava as variáveis por vogais e as constantes por consoantes maiúsculas. Ademais, ele utilizava palavras para representar potências. Em continuação ao trabalho de Viète, René Descartes (1596-1650) introduziu a utilização das letras x, y e z para indicar variáveis e das letras a, b e c para indicar constantes. Descartes também introduziu a notação para potências tal qual a usada atualmente.

De acordo com Domingues e Iezzi (2003, p. 282), o conceito de polinômio irredutível só começou a ser abordado na primeira metade do século XIX. Foi com o estudo dos polinômios ciclotômicos, na obra "Disquisitiones Arithmeticae" (1801) do matemático alemão Carl Friedrich Gauss (1777-1855), que iniciou-se essa abordagem. Gauss desenvolveu esse estudo motivado pela inscrição de polígonos regulares em um círculo usando régua e compasso, que era um problema de muito interesse para os gregos antigos.

O Critério de Eisenstein também já foi conhecido como Critério de Schönemann-Eisenstein, uma vez que o matemático alemão Theodor Schönemann (1812-1868), descobriu esse teorema de forma independente antes de Eisenstein. Ambos os matemáticos publicaram suas versões no Jornal de Crelle, fundado pelo matemático alemão August

Leopold Crelle (1780-1855).

Consoante Cox (2011), a prevalência do nome "Critério de Eisenstein" deve-se à influência do livro "Moderne Algebra", publicado pela primeira vez em 1930 e de autoria de Bartel Leendert van der Waerden (1903-1996). Esse autor colocava apenas o nome de Eisenstein no critério, mas havia uma menção a Schönemann na primeira edição do livro, a qual foi removida na segunda edição (1937).

Ferdinand Gotthold Max Eisenstein nasceu no dia 16 de abril de 1823 na capital da Alemanha, Berlim. O nome de seu pai era Johan Konstantin Eisenstein (1791-1875) e o de sua mãe, Helene Pollack (1799-1876). Eisenstein era o mais velho dos seis filhos do casal e foi o único destes que sobreviveu à meningite infantil. Devido a essa doença e outras, ele foi hipocondríaco durante toda sua vida. De acordo com Schmitz (2004), Eisenstein quase não tinha amigos quando ele era criança e, além disso, sempre teve dificuldades em sua situação financeira. Apesar de tudo, ele sempre teve o apoio de Gauss e também a sua admiração. Além do interesse pela matemática, tinha inclinação para a música. Ele morreu em 11 de outubro de 1852 vítima de tuberculose.

Theodor Schönemann, cujo sobrenome também pode ser escrito como Schoenemann, nasceu em 4 de abril de 1812. Além de ele ter descoberto o Critério de Eisenstein antes de Eisenstein, também descobriu o Lema de Hensel e a Lei de Reciprocidade de Scholz antes dos matemáticos dos quais essas descobertas levam o nome.

Apesar de o Critério de Eisenstein ser chamado assim, Schönemann merece reconhecimento por seu trabalho e descoberta.