**UNIVERSIDADE DO ESTADO DE SANTA CATARINA**
**CENTRO DE CIÊNCIAS TECNOLÓGICAS - CCT**
**MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL**

**VANESSA KLEIN SZABUNIA**

# **ARITMÉTICA E ÁLGEBRA NO ENSINO BÁSICO:** EXPLORANDO CORRELAÇÕES COM A TEORIA DE ANÉIS.

**JOINVILLE - SC**
**2023**

**VANESSA KLEIN SZABUNIA**

# ARITMÉTICA E ÁLGEBRA NO ENSINO BÁSICO: EXPLORANDO CORRELAÇÕES COM A TEORIA DE ANÉIS

Dissertação apresentada ao Curso de Pós-Graduação Mestrado Profissional em Matemática em Rede Nacional (PROFMAT) da Universidade do Estado de Santa Catarina (UDESC) no Centro de Ciências Tecnológicas (CCT) como requisito parcial para obtenção do grau de Mestre em Matemática.

Orientadora: Profa. Dra. Viviane Maria Beuter

**JOINVILLE, SC**
**2023**

**Ficha catalográfica elaborada pelo programa de geração automática da**

**Biblioteca Universitária Udesc,**

**com os dados fornecidos pelo(a) autor(a)**

Szabunia, Vanessa Klein
ARITMÉTICA E ÁLGEBRA NO ENSINO BÁSICO : EXPLORANDO CORRELAÇÕES COM A TEORIA DE ANÉIS. / Vanessa Klein Szabunia. -- 2023.
155 p.

Orientadora: Viviane Maria Beuter
Dissertação (mestrado) -- Universidade do Estado de Santa Catarina, Centro de Ciências Tecnológicas, Programa de Pós-Graduação Profissional em Matemática em Rede Nacional, Joinville, 2023.

1. Inteiros. 2. Polinômios. 3. Conexões. 4. Aritmética. 5. Álgebra. I. Beuter, Viviane Maria. II. Universidade do Estado de Santa Catarina, Centro de Ciências Tecnológicas, Programa de Pós-Graduação Profissional em Matemática em Rede Nacional. III. Título.

**VANESSA KLEIN SZABUNIA**

# ARITMÉTICA E ÁLGEBRA NO ENSINO BÁSICO: EXPLORANDO CORRELAÇÕES COM A TEORIA DE ANÉIS

Dissertação apresentada ao Curso de Pós-Graduação Mestrado Profissional em Matemática em Rede Nacional (PROFMAT) da Universidade do Estado de Santa Catarina (UDESC) no Centro de Ciências Tecnológicas (CCT) como requisito parcial para obtenção do grau de Mestre em Matemática.

**Banca Examinadora**

Orientador(a): Profa. Dra. Viviane Maria Beuter
Universidade do Estado de Santa Catarina - UDESC

Membro: Prof. Dra. Elisandra Bar de Figueiredo
Universidade do Estado de Santa Catarina - UDESC

Membro: Prof. Felipe Vieira
Universidade Federal de Santa Catarina - UFSC

Joinville, 29 de agosto de 2023.

# AGRADECIMENTOS

Agradeço, em primeiro lugar, a Deus pelo presente da vida.

Aos meus pais, Egbert José Klein e Vera Maria Martins Klein, agradeço pela educação e por me ensinarem, desde pequena, a acreditar e lutar pelos meus objetivos.

Ao meu marido e melhor amigo, Bruno Szabunia, sou grata por sempre me incentivar e por acreditar em mim. Aos meus filhos, Gustavo e Isabela, agradeço por compreenderem que, em determinados momentos, a mamãe precisava se dedicar aos estudos.

Também não posso deixar de agradecer aos meus colegas de trabalho e familiares pelo apoio, carinho e torcida durante todo o percurso do curso.

Agradeço aos professores do PROFMAT pelo conhecimento compartilhado, em especial à professora Elisandra Bar de Figueiredo e ao professor Felipe Vieira por fazerem parte dessa banca.

Não tenho palavras para expressar o quanto estou grata à professora Dra. Viviane Maria Beuter, que me orientou e prestou todo o suporte ao auxiliar no desenvolvimento desta dissertação.

Aos colegas do PROFMAT, Marciane, Marilete e, especialmente, ao Matheus, agradeço por compartilharem essa jornada comigo e por acreditarem que esse momento seria alcançado.

# RESUMO

Este trabalho busca apresentar conexões entre as áreas da Aritmética e Álgebra no contexto do Ensino Básico, a partir da aritmética dos números inteiros e da estrutura algébrica dos polinômios, dentro da Teoria de Anéis. Além de proporcionar ao professor um conhecimento sólido sobre o tema e contribuir com o desenvolvimento de práticas de ensino para a Educação Básica. Também foi desenvolvido um caderno pedagógico como produto educacional, acompanhado de sugestões de atividades práticas destinadas à aplicação em sala de aula. Tais atividades têm como objetivo utilizar os conhecimentos prévios dos alunos em Aritmética como ponto de partida para introduzir e explorar os conceitos da Álgebra.

**Palavras-chave:** Inteiros. Polinômios. Conexões. Aritmética. Álgebra.

# ABSTRACT

This work seeks to present connections between the areas of Arithmetic and Algebra in the context of Basic Education, starting from the arithmetic of integers and the algebraic structure of polynomials within the Theory of Rings. In addition to providing the teacher with a solid knowledge of the subject and contributing to the development of teaching practices for Basic Education. We have also developed an educational notebook as an educational product, accompanied by suggestions for practical activities intended for classroom application. These activities aim to use students' prior knowledge in Arithmetic as a starting point to introduce and explore Algebra concepts.

**Key-words:** Integers. Polynomials. Connections. Arithmetic. Algebra..

# LISTA DE FIGURAS

# SUMÁRIO

# 1 INTRODUÇÃO

Dentre as competências específicas da Matemática na Base Comum Curricular Nacional (BNCC), o Ensino Fundamental deve garantir ao aluno a compreensão das relações entre conceitos e procedimentos dos diferentes campos desta disciplina - Aritmética, Álgebra, Geometria, Estatística e Probabilidade, permitindo sentir segurança quanto à própria capacidade de construir e aplicar esses conhecimentos, desenvolvendo a autoestima e a perseverança na busca de soluções.

Além disso, a BNCC propõe cinco unidades temáticas, correlacionadas, que orientam a formulação de habilidades a serem desenvolvidas ao longo do Ensino Fundamental, são elas: Número, Álgebra, Geometria, Grandezas e Medidas, Probabilidade e Estatística. Com relação às unidades temáticas Número e Álgebra, a BNCC diz.

> [...] A unidade temática Número tem como finalidade desenvolver o pensamento numérico, que implica o conhecimento de maneiras de quantificar atributos de objetos e de julgar e interpretar argumentos baseados em quantidades. [...] No estudo desses **campos numéricos**, devem ser enfatizados registros, usos, significados e **operações**. (BRASIL, 2018, grifos nossos)

> [...] A unidade temática Álgebra tem como finalidade o desenvolvimento de um tipo especial de pensamento – pensamento algébrico – que é essencial para utilizar modelos matemáticos na compreensão, representação e análise de relações quantitativas de grandezas e, também, de situações e estruturas matemáticas, fazendo uso de **letras e outros símbolos**. [...] Em síntese, essa unidade temática deve enfatizar o desenvolvimento de uma linguagem, o **estabelecimento de generalizações**, a análise da interdependência de grandezas e a resolução de problemas por meio de **equações** ou inequações. (BRASIL, 2018, grifos nossos)

Entre os objetivos desse trabalho, queremos estudar algumas interações entre os seguintes campos: Aritmética e Álgebra, ou ainda, considerando as cinco unidades temáticas, correlacionar elementos das temáticas Número e Álgebra. Pretendemos destacar as conexões entre essas áreas, com enfoque na aritmética dos números inteiros e na estrutura algébrica dos polinômios. Dessa forma, buscaremos evidenciar como esses dois campos da Matemática se relacionam e se complementam, proporcionando uma compreensão mais abrangente desses conceitos. Além do mais, ao conectar essas áreas de forma significativa,

o ensino da matemática pode se tornar mais interessante e compreensível, estimulando o aprendizado dos estudantes.

É sabido que, com o objetivo de organizar e estruturar o amplo campo de estudo da matemática, essas áreas foram separadas no currículo escolar. Acredita-se que tal medida facilite aos educadores o planejamento de suas aulas com um currículo específico. Entretanto, é importante salientar que essa separação não implica que elas devam ser ensinadas de maneira isolada. Pelo contrário, a interligação entre a Aritmética e a Álgebra pode enriquecer o processo de aprendizado, permitindo aos alunos visualizarem como esses dois ramos da matemática se complementam e aplicam em diversos contextos.

> Estabelecer conexões é particularmente importante na aprendizagem da matemática porque quase todo novo conhecimento deve estar ligado aos conceitos que foram aprendidos antes. Ninguém se torna matematicamente capaz se aprender novos conceitos de maneira isolada. (CHAMBERS E TIMLIN, 2015, p.112).

## 1.1 Responsabilidade pedagógica

Inserir o pensamento algébrico se torna um desafio ao professor de matemática do Ensino Fundamental, uma vez que os alunos costumam apresentar grandes dificuldades, considerando-se, por vezes, incapazes de aprender este tipo de conteúdo e levando consigo, para o Ensino Médio, uma resistência no aprendizado de novos conceitos algébricos.

Para Cury e Ribeiro (2015), a Álgebra trabalhada desde os primeiros anos do Ensino Fundamental, pode ser considerada como um fio condutor do currículo escolar e o desenvolvimento do pensamento algébrico pode possibilitar abstrações e generalizações que estão na base dos processos de modelagem matemática da vida real.

> (...) desenvolvem uma gama de abordagens de resolução de problemas, algumas das quais serão mais vigorosas que outras em uma situação em particular. Se eles sabem algo sobre adição, quase espontaneamente desenvolverão uma abordagem de adição repetida para um problema de "multiplicação". Naturalmente desenvolverão uma abordagem por tentativa e refinamento para resolver "problemas algébricos". (SUTHERLAND, 2009, p.52).

Segundo Becker (2012) é necessário analisar quais conhecimentos cada aluno já possui sobre determinado assunto e quais são suas necessidades. Este exercício permite um olhar sobre a prática e as suspeitas que a sustentam articulando-a com a dinâmica do trabalho em sala de aula. Consequentemente, é essencial saber qual o nível de conheci-

mento que um aluno já possui, ou seja, começar com o conhecimento existente e dar uma contribuição maior em relação ao início.

Dentro deste cenário, é importante destacar que o professor assume o papel de mediador, encarregado de explorar o conhecimento prévio do aluno com o objetivo de aprofundar, organizar, ampliar e expandir sua base de saberes já existentes. Nesse sentido, a relevância de uma formação adequada para os professores torna-se fundamental, servindo como alicerce na edificação de instituições educacionais sólidas, contribuindo para a formação de cidadãos e profissionais mais habilidosos, éticos e humanizados.

> Os jovens estudantes universitários são confrontados com problemas que nada têm a ver com as coisas que estudaram na escola e, naturalmente, esquecem-nas rapidamente. Quando, depois de completarem o curso, se tornam professores, são confrontados com a necessidade de ensinar a matemática elementar na forma adequada ao grau de ensino, primário ou secundário, a que se dedicam, e, como não conseguem estabelecer praticamente nenhuma conexão entre esta tarefa e a matemática que aprenderam na universidade, facilmente aceitam o ensino tradicional, ficando seus estudos universitários como uma memória mais ou menos agradável que não tem influência na sua forma de ensinar. (KLEIN, 2009, p. 01).

O conhecimento sólido do professor proporciona, além de segurança para ministrar as aulas e transmitir confiança aos alunos, uma maior flexibilidade pedagógica para adaptar os conteúdos e métodos de ensino de acordo com as necessidades e características individuais dos estudantes. Com esse enfoque, surge a relevância da discussão sobre anéis e domínios euclidianos, ou seja, a comprovação de que é possível resgatar conhecimentos previamente adquiridos na Aritmética para ensinar a Álgebra.

Também temos como objetivo permitir ao professor um conhecimento sólido sobre o tema e contribuir com o desenvolvimento de práticas de ensino para a Educação Básica.

## 1.2 Desenvolvimento deste trabalho

Como já mencionamos, buscaremos relacionar as temática Número e Álgebra através da teoria de anéis, destacando as similaridades entre os Anéis dos Números Inteiros e os Anéis de Polinômios, que vão além de serem ambos anéis de integridade. A presença de um algoritmo da divisão em cada anel é o que os torna tão próximos.

Essa conexão também pode inspirar os professores a desenvolverem metodologias de ensino mais criativas e contextualizadas, tornando o aprendizado da Matemática mais envolvente e relevante para os alunos. Além disso, ao compreender as relações entre esses

dois ramos da Matemática, os alunos podem perceber que a matemática é uma ciência unificada, onde diferentes tópicos estão interligados e têm aplicações em diversas áreas do conhecimento.

Este trabalho está dividido da seguinte forma: no segundo capítulo, realizaremos uma breve abordagem histórica da Aritmética e da Álgebra e seu desenvolvimento ao longo do tempo.

No terceiro capítulo, iniciaremos a exploração da definição de um anel e como, a partir dos seis axiomas fundamentais, podemos deduzir novas propriedades. Abordaremos anéis de integridade e corpos, além de apresentar exemplos como conjuntos numéricos, anéis de polinômios, anéis de matrizes e outros. Vamos observar que, de forma semelhante ao anel dos inteiros, os anéis de polinômios com coeficientes pertencentes a um corpo numérico também se configuram como anéis de integridade. Entretanto, no terceiro capítulo, notaremos que suas estruturas algébricas são mais próximas, uma vez que ambos se enquadram como domínios euclidianos, ou seja, admitem a aplicação de um algoritmo de divisão. Com base nesse ponto, derivamos outras conclusões, como a fatoração de elementos primos ou irredutíveis. Nestes dois capítulos, exibiremos várias imagens de livros didáticos do Ensino Básico, com o propósito de aproximar os conceitos de anéis, que inicialmente podem parecer distantes em relação ao conteúdo abordado no ensino básico.

No quarto capítulo, o trabalho aborda elementos pertinentes ao ensino da matemática. Inicialmente, explora o processo de ensino e aprendizagem, seguido pelo planejamento pedagógico e pela contribuição da história da matemática como um guia educacional. Além disso, enfatiza a utilização das tecnologias como ferramentas de ensino e ressalta o desenvolvimento de competências essenciais no ensino da álgebra, alinhadas com as diretrizes da Base Nacional Comum Curricular

Na etapa conclusiva deste trabalho, encontram-se as considerações finais, nas quais os aspectos relacionados à nossa exploração da relação entre Aritmética e Álgebra, assim como a investigação histórica e as estratégias pedagógicas, são reunidos.

Em anexo, apresentamos o produto educacional desenvolvido, acompanhado de sugestões de atividades práticas destinadas à aplicação em sala de aula. Além disso, busca-se a elaboração de uma aula diferenciada, contendo atividades capazes de responder à pergunta que muitos educadores provavelmente já ouviram: “Por que colocar letras na matemática, se a disciplina não é Língua Portuguesa?”.

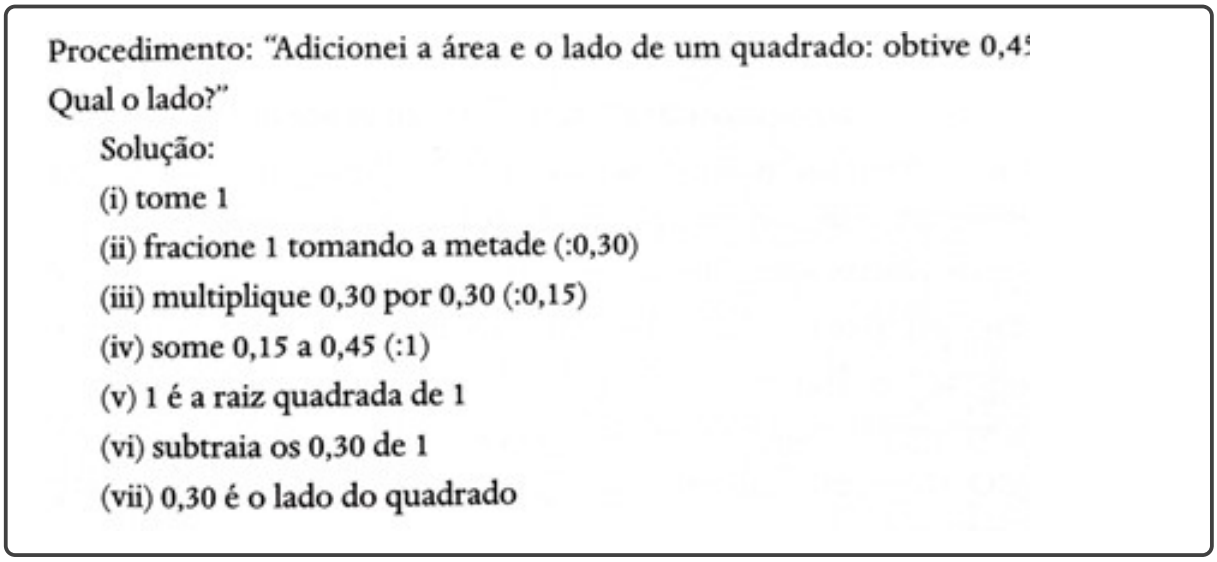
# 2 UM BREVE RELATO HISTÓRICO

## 2.1 Um pouco da Aritmética e da Álgebra na história da matemática

"Não existem muitas informações sobre a utilização de incógnitas pelo povo Babilônico, eles utilizavam a matemática discursiva renunciando a teoremas, raciocínio geométrico ou fórmulas." (CONTADOR, 2014, p.144)

De acordo com Roque (2013) cada etapa do procedimento era resolvida com o auxílio de um tablete. Data do período babilônico antigo (2000-1600 a.C) a maioria dos tabletes de argila mencionados na história da matemática. Na figura 1 temos um exemplo apresentado por Roque (2013) .

Figura 1 – Exemplo traduzido de problema Babilônico


Procedimento: "Adicionei a área e o lado de um quadrado: obtive 0,4
Qual o lado?"
Solução:
(i) tome 1
(ii) fracione 1 tomando a metade (:0,30)
(iii) multiplique 0,30 por 0,30 (:0,15)
(iv) some 0,15 a 0,45 (:1)
(v) 1 é a raiz quadrada de 1
(vi) subtraia os 0,30 de 1
(vii) 0,30 é o lado do quadrado

Fonte: ROQUE (2013, p.63)

> [...] a etapa (iii) exigia a consulta de um tablete de multiplicação ou de quadrado, e a etapa (v) evidente nesse caso particular, era resolvida pela consulta a um tablete de raízes quadradas (ROQUE, 2013, p. 64)

Atualmente é perceptível o uso de generalizações nos algoritmos usados na solução de problemas da mesma natureza que agora são resolvidos usando regras gerais, que podem ser especificadas para casos particulares. Para Roque (2013) a generalidade dos algoritmos babilônicos é distinta, pois eles constroem uma lista de exemplos típicos, interpolando-os,

em seguida, para resolver novos problemas. O exemplo apresentado na Figura 1, pode ser representado por uma equação

$$Ax^2 + Bx = C$$

e resolvido usando o procedimento babilônico descrito na figura 2:

Figura 2 – Caso geral para representar um problema Babilônico.

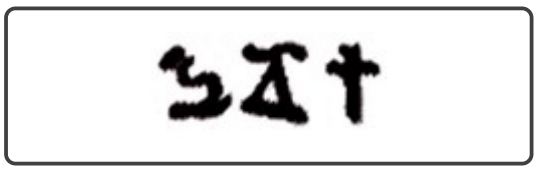
$$L = \left(\sqrt{\left(\frac{B}{2}\right)^2 + AC} - \frac{B}{2}\right) \times \frac{1}{A}$$

1) multiplique $A$ por $C$ (obtendo $AC$)
2) encontre metade de $B$ (obtendo $B/2$)
3) multiplique $B/2$ por $B/2$ (obtendo $(B/2)^2$)
4) adicione $AC$ a $(B/2)^2$ (obtendo $(B/2)^2 + AC$)
5) a raiz quadrada é $(\sqrt{(B/2)^2 + AC})$
6) subtraia $B/2$ da raiz acima
7) tome o recíproco de $A$ (obtendo $1/A$)
8) multiplique $1/A$ pelo resultado do passo (6) para obter o lado do quadrado
9) o lado do quadrado é $(\sqrt{(B/2)^2 + AC} - B/2) \times 1/A$

Fonte: ROQUE (2013, p.65)

Já a matemática egípcia é conhecida por vários avanços e muitos deles constam no *Papiro Rhind* (1650 a.C.). Note que é possível encontrar três incógnitas, conforme Figura 3, ou a palavra ”hau” que significa pilha.

Figura 3 – Incógnitas no papiro Rhind



Fonte: CONTADOR (2014, p.144)

O *Papiro Rhind* é um dos registros matemáticos mais antigos e bem preservados. Segundo Boyer (2012, p. 32), nesse documento, destaca-se que a operação aritmética fundamental no Egito era a adição, e as operações de multiplicação e divisão eram realizadas na época de Ahmes por meio de sucessivas “duplicações”.

> Vários dos problemas presentes nos Papiros de Rhind e de Moscou diziam respeito à repartição de víveres, animais e outros objetos. Esses problemas eram resolvidos de forma aritmética ou através de equações lineares da forma $x + ax = b$ ou $x + ax + bx = c$. Com exceção da fração 2/3, os egípcios trabalhavam com frações com numerador 1, o que trazia dificuldades para o manejo de tais equações. A solução encontrada foi resolvê-las por um método conhecido hoje como "método da falsa posição". (MOL, 2013, p.25))

Veja um exemplo do método da falsa posição na Figura 4.

Figura 4 – Método da falsa posição.

No método da falsa posição, um valor específico é atribuído à incógnita. A expressão do lado esquerdo é calculada para esse valor e o resultado encontrado é comparado com o resultado desejado. Em seguida, o resultado correto é encontrado por proporção. Como exemplo, o problema 24 do Papiro de Rhind propõe resolver a equação $x + (1/7)x = 19$. Inicialmente, é atribuído valor $x = 7$ e, para esse valor, encontramos $x + (1/7)x = 8$. Sabendo que $8(2 + 1/4 + 1/8) = 19$, a solução é obtida multiplicando 7 por $2+1/4+1/8$. Expressa em frações unitárias, a solução é $x = 16 + 1/2 + 1/8$.

Fonte: CONTADOR (2014, p.144)

Ao abordar questões cada vez mais frequentes no cotidiano dos Egípcios, desenvolvem-se tendências à abstração e, em certa medida, a ciência começa a estudar a si mesma. Foi assim que a Geometria Teórica se desenvolveu a partir da Álgebra e da medição no final da Aritmética.

Com base nos métodos de resolução de problemas desenvolvidos pelos povos Babilônico e Egípcio, garantir que esses povos utilizavam a Álgebra seria um desacordo com os usos e costumes de uma época, avançando para a cultura grega, também não podemos considerar que os *Elementos* de Euclides possuíam Álgebra. De acordo com Roque (2013, p.231), em ambos os casos, uma das mais fortes razões para não tirar conclusões apressadas é o fato de que neste período não era usado nenhum tipo de notação algébrica, que seria empregar o mesmo símbolo para representações diferentes.

> [...] considera-se que a primeira ocorrência da notação simbólica que caracteriza nossa Álgebra remota ao livro de Aritmética, escrito em grego por Diofanto. Acredita-se que esse autor tenha vivido no século III E.C., ainda que tal data é contestada. Além disso, embora se tenha notícia que Diofanto viveu em Alexandria, não se pode assegurar de que fosse grego, apesar de seu texto ser escrito nessa língua. O fato de sua obra parecer distinta da tradição grega levou até alguns historiadores, como H. Hankel, a conjecturar que ele fosse árabe. (ROQUE, 2013, p.231)

A contribuição mais conhecida de Diofanto é ter apresentado uma forma de figurar o valor desconhecido em um problema denotando-o como *arithmos*, que se origina de "aritmética." É possível perceber que a obra de Diofanto é completamente diferente de outras obras gregas da época assemelhando-se às obras "algébricas" dos babilônios, mas desvendando um grande avanço nesse campo em relação a elas.

No século III a.C, Euclides de Alexandria contribuiu com a Aritmética por meio de seu livro *Elementos*. De acordo com Boyer (2012, p. 89), essa obra não se limita apenas ao conhecimento geométrico, mas, pelo contrário, é um texto introdutório que abrange toda a matemática elementar, incluindo a Aritmética no sentido de "Teoria dos Números".

Iezzi, Dolce e Machado (2018, p.174) consideram a obra de Euclides, uma das mais importantes de toda a história da Matemática. Além de definir satisfatoriamente número primo, Euclides provou várias propriedades desses números, entre as quais que o conjunto dos números primos é infinito. Conforme Hefez (2016, p. 46), na obra *Elementos* de Euclides é observado que é sempre possível realizar a divisão de $a$ por $b$, com resto, desde que $b$ seja diferente de zero.

Segundo Boyer (2012), a solução de equações quadráticas com três termos parece ter sido um problema difícil para os egípcios. No entanto, Otto Neugebauer, em 1930, revelou que os babilônios já haviam eficientemente abordado essas equações em alguns dos mais antigos textos de problemas. No contexto do período babilônico antigo, aproximadamente 4.000 anos atrás, três tipos distintos de tais equações foram identificados.

Embora não haja registros egípcios que indiquem a resolução de equações cúbicas, entre os babilônios, diversos exemplos são encontrados. Equações cúbicas puras, como $x^3 = 0$, eram tratadas mediante a consulta direta a tabelas de cubos e raízes cúbicas. A técnica de interpolação linear era utilizada nessas tabelas para aproximar valores não constantes na referida tabela.

> [...] Por cerca de três milênios, até o início do século XIX, "Álgebra" significava resolver equações polinomiais, principalmente de grau quatro ou menos. Questões de notação para tais equações, a natureza de suas raízes e as leis que regem os vários sistemas de numeração aos quais as raízes pertenciam também eram motivo de preocupação nessa conexão. Todas essas questões ficaram conhecidas como Álgebra Clássica. (O termo "Álgebra" só foi utilizado primeiro no século IX dC.) Nas primeiras décadas do século XX, a Álgebra evoluiu para o estudo de sistemas axiomáticos. A abordagem axiomática logo passou a ser chamada de Álgebra Moderna ou Abstrata. A transição da Álgebra Clássica para a Moderna ocorreu no século XIX. (KLEINER, 2007, p.1, tradução nossa).

Chegando na era moderna, Boyer (2012) destaca que em 1801, Gauss incluiu o Teorema Fundamental da Aritmética em sua obra *Disquisitiones Arithmeticae*, sendo este um dos princípios fundamentais válidos no anel de integridade dos inteiros de Gauss. O teorema já era conhecido desde os tempos de Euclides e estabelece que todo número inteiro positivo pode ser representado de maneira única (exceto pela ordem dos fatores) como um produto de números primos.

> O teorema de Euclides sobre a existência de infinitos primos foi demonstrado por um matemático que, em 1855, sucederia a Gauss em Gottingen. Este foi Peter Gustav Lejeune Dirichlet (1805-1859), o homem que fez mais que qualquer outro para ampliar as *Disquisitiones*(BOYER, 2012, p. 345)

O "Último Teorema de Fermat" afirma que a equação $x^n + y^n = z^n$ não apresentava soluções inteiras não triviais quando $n$ era um inteiro maior que 2. Segundo Stewart (2002), Pierre de Fermat (1601-1665) rabiscou essa conjectura (sem provas, apesar do nome, não era um teorema) à margem de seu exemplar de *Aritmética* de Diofante por volta de 1650. Em 1874, o matemático francês Lamé anunciou uma "prova" desse teorema. No entanto, Lioville imediatamente aponta que ele assumia a unicidade da fatoração de uma maneira muito sutil. Os temores de Liouville foram confirmados quando mais tarde ele recebeu uma carta de Kummer que havia mostrado que a unicidade da fatoração falha em alguns casos, o primeiro sendo $n = 23$. Demorou quase 350 anos até que Andrew Wiles provasse que Fermat estava certo.

Em 1843, Ernest Eduard Kummer (1810-1893) introduziu na Aritmética o conceito de "número ideal". Ao generalizar o conceito de número inteiro, perde-se a propriedade de fatoração única. Para contornar essa questão, o matemático Dedekind adotou ideias de Kummer e introduziu o conceito de "ideal".

> O principal resultado do trabalho inovador de Dedekind em 1871 é que todo ideal diferente de zero no domínio de números inteiros de um corpo algébrico é um produto único de ideais primos. Antes que alguém pudesse enunciar este teorema, era preciso, é claro, definir os conceitos em sua declaração, ou seja, "o domínio dos inteiros de um corpo de número algébrico", "ideal" e "ideal primo". Dedekind levou cerca de vinte anos para formulá-los. (KLEINER, 1998, página 27).

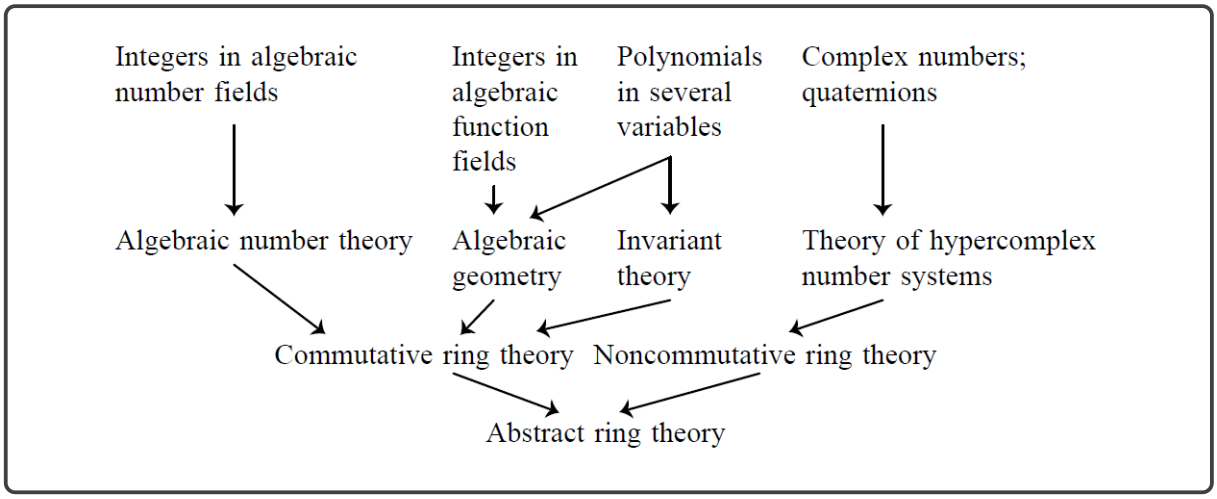
Verificou-se que no anel de integridade $R$ dos inteiros algébricos, todo ideal $I$ de $R$ pode ser representado de modo único (exceto quanto à ordem dos fatores) como um produto de ideais primos. Isto é, a unicidade de fatoração pode ser preservada através da teoria dos ideais, permitindo assim criar uma conexão entre a Álgebra, por meio da teoria de anéis e ideais, e a Aritmética, através da fatoração única dos números inteiros.

Ao longo da história, observa-se que, à medida que a Aritmética se desenvolve, ela própria torna-se limitada, tornando necessário o surgimento da Álgebra. A Álgebra entra em cena como uma extensão natural da Aritmética.

# 3 ANÉIS

De acordo com Kleiner (1998), a teoria dos anéis comutativos originou-se na Teoria dos Números Algébricos, na Geometria Algébrica e na Teoria dos invariantes. No centro do desenvolvimento desses assuntos estavam os anéis de números inteiros em corpos de números algébricos e corpos de funções algébricas, e os anéis de polinômios em duas ou mais variáveis. A Figura 5 é esboço esquemático do desenvolvimento da Teoria dos Anéis.

Figura 5 – Desenvolvimento da Teoria dos Anéis




Fonte: KLEINER (1998, p.19)

Dessa forma, observamos que exemplos vêm primeiro e as abstrações depois. Esta é, naturalmente, a ordem histórica.

Neste capítulo, abordaremos os conceitos iniciais da Teoria dos Anéis, apresentando suas definições formais, propriedades e proposições conforme são encontrados em livros de Álgebra do Ensino Superior. Além disso, para compreendermos melhor como esse tópico se relaciona com os conteúdos do Ensino Básico, faremos uso de trechos de livros didáticos ao longo do texto.

Na disciplina MA14 - Aritmética do PROFMAT, estudamos as propriedades das operações de adição e multiplicação dos números inteiros, com foco nas questões relacionadas à divisibilidade. Entre os tópicos estudados, destacam-se o algoritmo da divisão, o máximo divisor comum, os números primos e o Teorema Fundamental da Aritmética. Ao avançarmos para o estudo de polinômios, com coeficientes reais ou complexos, percebemos que conceitos semelhantes ou relacionados surgem novamente. Exploraremos a semelhança na estrutura algébrica entre o conjunto dos números inteiros e o conjunto

dos polinômios com coeficientes complexos ou reais. Veremos que, ambos, com as operações usuais de adição e multiplicação, são anéis de integridade, e é esse conceito que estudaremos a seguir.

## 3.1 Conceitos iniciais

Para enriquecer o desenvolvimento do texto sobre os anéis, além das principais referências em Domingues e Iezzi (2003), Janesch e Taneja (2011), e Gonçalves (2017), faremos conexões com livros didáticos do Ensino Básico, fornecendo imagens e abordagens dos conceitos em questão presentes nessas obras. Nesse sentido, priorizamos livros aprovados pelo Programa Nacional do Livro e do Material Didático (PNLD), entre os livros utilizados, destacam-se: Dante (2015), autor de "Teláris Matemática" e o livro de Iezzi, Dolce, Degenszajn e Périgo (2016), intitulado "Matemática, Ciência e Aplicações". Essa abordagem que integra os livros didáticos proporciona uma familiaridade com a Teoria dos Anéis em um contexto mais acessível, ampliando assim a compreensão do conteúdo de forma mais esclarecedora.

**Definição 3.1.1.** Seja $A$ um conjunto não vazio. Uma *operação binária* $*$ sobre $A$ é uma função de $A \times A$ em $A$, ou seja,

$$\begin{array}{rccc} * : & A \times A & \to & A \\ & (a, b) & \mapsto & a * b \end{array}$$

que associa cada elemento $(a, b) \in A \times A$ a um único elemento $a * b \in A$.

Por exemplo, a adição e multiplicação de números reais são operações binárias sobre o conjunto dos números reais.

**Definição 3.1.2.** Seja $A$ um conjunto não vazio no qual estão definidas duas operações, as quais chamaremos de adição e multiplicação em $A$ e denotaremos por $(+)$ e $(\cdot)$. Dizemos que $(A, +, \cdot)$ é um *anel* se as seguintes propriedades são satisfeitas:

(i) *Associatividade da adição:*

$$\forall\, a, b, c \in A,\ (a + b) + c = a + (b + c);$$

(ii) *Comutatividade da adição:*

$$\forall\, a, b \in A,\ a + b = b + a;$$

(iii) *Existência de elemento neutro da adição:*

$$\exists\, 0_A \in A, \text{ chamado de zero de } A, \text{ tal que } \forall\, a \in A,\ a + 0_A = a = 0_A + a;$$

(iv) *Existência de elemento simétrico para cada elemento:*

$$\forall\, a \in A, \exists\, b \in A, \text{chamado de simétrico de } a, \text{ tal que } a + b = b + a = 0_A;$$

(v) *Associatividade do multiplicação:*

$$\forall\, a, b, c \in A,\ (a \cdot b) \cdot c = a \cdot (b \cdot c);$$

(vi) *Distributividade da multiplicação em relação a adição:*

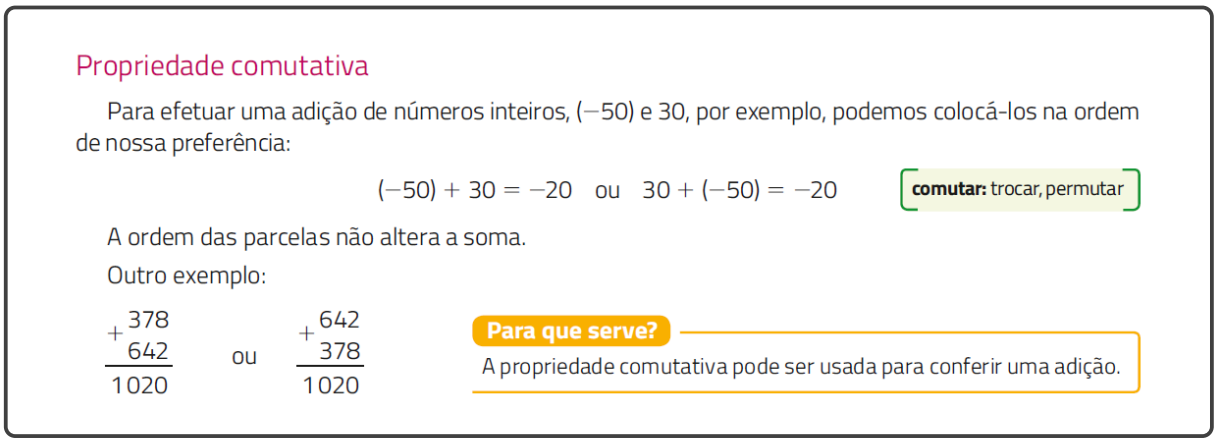
$$\forall\, a, b, c \in A,\ a \cdot (b + c) = a \cdot b + a \cdot c \text{ e } (a + b) \cdot c = a \cdot c + b \cdot c.$$

Quando não houver possibilidade de confusão sobre a operação considerada, podemos nos referir simplesmente ao anel $A$, sem mencionar a operação. Quando fazemos a multiplicação dos elementos $a$ e $b$ do anel $(A, +, \cdot)$, é comum omitir o símbolo $\cdot$ que indica a operação, ou seja, $a \cdot b = ab$.

Observamos que, em Hefez (2016, p. 03), livro texto da disciplina MA14 - Aritmética do PROFMAT, são apresentadas as seis propriedades acima, entre outras, em relação às operações de adição e multiplicação no conjunto dos números inteiros. Nessa bibliografia, a abordagem é essencialmente axiomática, ou seja, a partir de uma lista de propriedades básicas dessas duas operações no conjunto dos números inteiros, provam-se outras propriedades. Faremos o mesmo aqui, uma vez que nosso objetivo não é construir os números inteiros. Para os leitores interessados, a construção lógico-formal do conjunto dos números inteiros, assim como demonstrações das propriedades da adição e multiplicação, podem ser encontradas em Domingues (2017, p.189). A partir disso, temos que $(\mathbb{Z}, +, \cdot)$ é um anel.

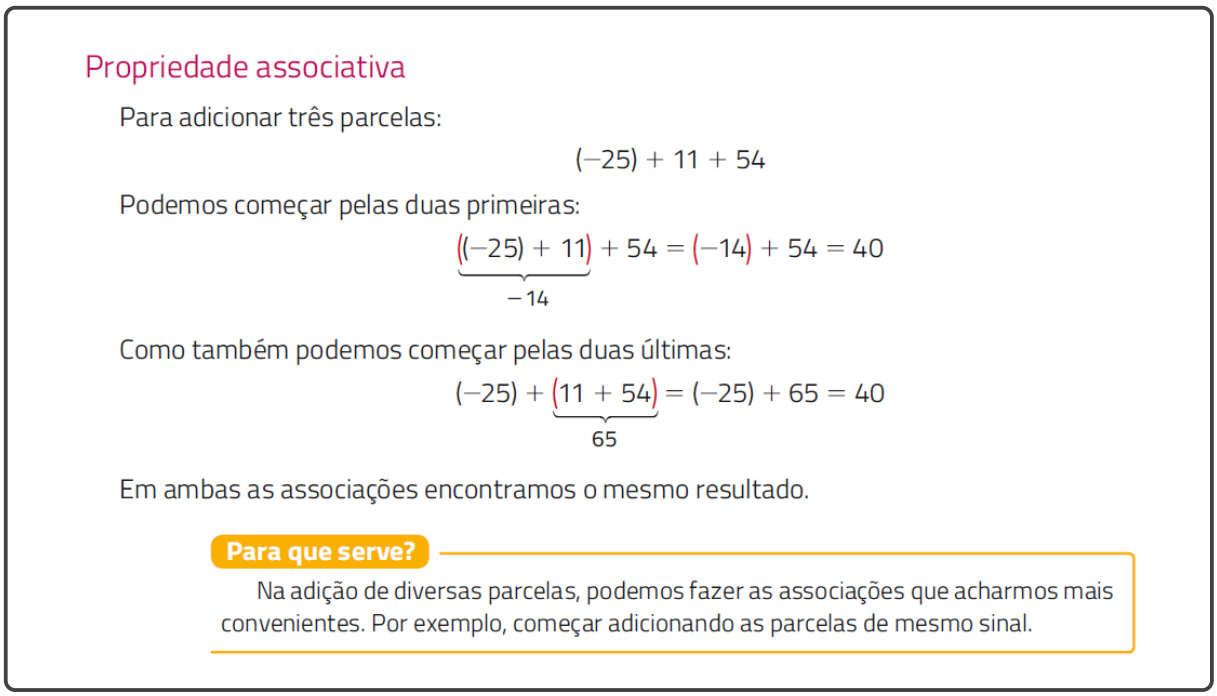
Autores de livros didáticos do Ensino Básico também expõem essas propriedades das operações em $\mathbb{Z}$ em seus livros. Veja os exemplos das propriedades da adição nas Figuras 6, 7 e 8:

Figura 6 – Comutatividade da adição.




Fonte: IEZZI; DOLCE; MACHADO (2018b, p.38)

Figura 7 – Associatividade da adição.



Propriedade associativa

Para adicionar três parcelas:

$$(-25) + 11 + 54$$

Podemos começar pelas duas primeiras:

$$\underbrace{(-25) + 11}_{-14} + 54 = (-14) + 54 = 40$$

Como também podemos começar pelas duas últimas:

$$(-25) + \underbrace{(11 + 54)}_{65} = (-25) + 65 = 40$$

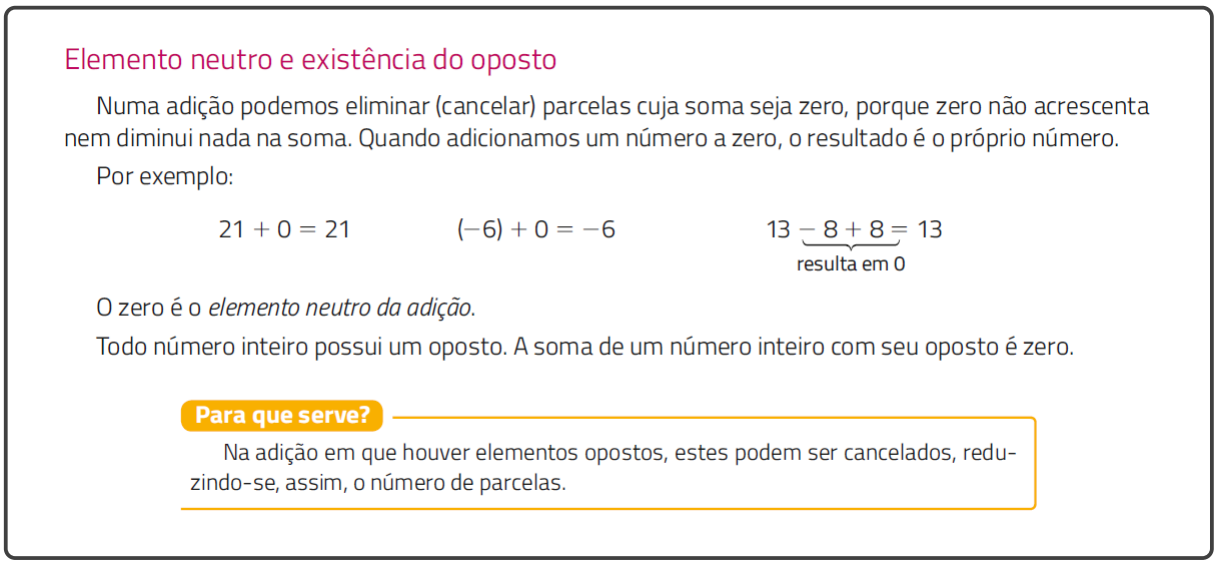
Em ambas as associações encontramos o mesmo resultado.

**Para que serve?**

Na adição de diversas parcelas, podemos fazer as associações que acharmos mais convenientes. Por exemplo, começar adicionando as parcelas de mesmo sinal.

Fonte: IEZZI; DOLCE; MACHADO (2018b, p.39)

Figura 8 – Elemento neutro e oposto.



Elemento neutro e existência do oposto

Numa adição podemos eliminar (cancelar) parcelas cuja soma seja zero, porque zero não acrescenta nem diminui nada na soma. Quando adicionamos um número a zero, o resultado é o próprio número.

Por exemplo:

$$21 + 0 = 21 \qquad (-6) + 0 = -6 \qquad 13 \underbrace{- 8 + 8}_{\text{resulta em 0}} = 13$$

O zero é o *elemento neutro da adição*.

Todo número inteiro possui um oposto. A soma de um número inteiro com seu oposto é zero.

**Para que serve?**

Na adição em que houver elementos opostos, estes podem ser cancelados, reduzindo-se, assim, o número de parcelas.

Fonte: IEZZI; DOLCE; MACHADO (2018b, p.39)

Além das propriedades da adição, a associatividade da multiplicação também é abordada, bem como a distributividade da multiplicação em relação a adição. Veja exemplos nas Figuras 9 e 10:

Figura 9 – Associatividade do produto.

**Associativa**

Em uma multiplicação de três ou mais números inteiros, os fatores podem ser associados de modos diferentes sem alterar o produto.

Essa é a **propriedade associativa da multiplicação**.
**Exemplo:**
Para calcular $(+3) \cdot (-6) \cdot (-2)$, podemos associar os fatores de dois modos:

$$\underbrace{(+3) \cdot (-6)} \cdot (-2) = \qquad (+3) \cdot \underbrace{(-6) \cdot (-2)} =$$
$$= (-18) \cdot (-2) = \qquad = (+3) \cdot (+12) =$$
$$= +36 \qquad = +36$$

- Na operação à esquerda, primeiro multiplicamos $(+3)$ e $(-6)$ e, depois, multiplicamos o resultado obtido $(-18)$ por $(-2)$, obtendo o produto $+36$.
- Na operação à direita, primeiro multiplicamos $(-6)$ por $(-2)$ e, depois, multiplicamos o resultado obtido $(+12)$ por $(+3)$, obtendo o produto $+36$.

Fonte: DANTE (2018, p.32)

Figura 10 – Distributividade do produto.

**Distributiva da multiplicação em relação à adição algébrica**

Ao multiplicar um número inteiro por uma adicão algébrica, obtemos o mesmo resultado que ao adicionar os produtos de cada parcela dessa adição por esse número.

Essa é a **propriedade distributiva da multiplicação em relação à adição algébrica**.
**Exemplo:**
Veja dois modos de calcular $(+3) \cdot [(-5) + (-2)]$.

- Primeiro multiplicamos o fator $(+3)$ por cada uma das parcelas da adição algébrica, $(-5)$ e $(-2)$, e, depois, adicionamos os resultados obtidos, $(-15)$ e $(-6)$, obtendo o resultado $-21$.

$$(+3) \cdot [(-5) + (-2)] =$$
$$= \underbrace{(+3) \cdot (-5)} + \underbrace{(+3) \cdot (-2)} =$$
$$= \quad -15 \quad + \quad (-6) \quad = -21$$

- No outro modo, primeiro adicionamos as parcelas e depois multiplicamos o resultado obtido $(-7)$ por $(+3)$, obtendo o mesmo resultado, $-21$.

$$(+3) \cdot \underbrace{[(-5) + (-2)]} =$$
$$= (+3) \cdot \quad (-7) \quad = -21$$

Fonte: DANTE (2018, p.32)

Sabemos que a tripla $(\mathbb{Z}, +, \cdot)$ satisfaz mais propriedades, como a comutatividade e existência do elemento neutro da multiplicação. Essas propriedades e demais, discutiremos ao longo desse capítulo.

Usando nosso conhecimento prévio sobre os conjuntos numéricos, temos:

**Exemplo 3.1.3.** Os conjuntos numéricos

$$(\mathbb{Z}, +, \cdot),\ (\mathbb{Q}, +, \cdot),\ (\mathbb{R}, +, \cdot) \text{ e } (\mathbb{C}, +, \cdot)$$

são exemplos clássicos de anéis com as operações usuais de adição e multiplicação.

Observamos que o conjunto dos números naturais $\mathbb{N} \cup \{0\}$, com as operações usuais de adição e multiplicação, não é um anel, pois o axioma (iv) da Definição 3.1.2 não é satisfeito.

A seguir iremos demonstrar alguns resultados fundamentais relacionados ao elemento zero e ao simétrico de um elemento decorrentes dos axiomas de anéis.

**Proposição 3.1.4.** *Sejam $(A, +, \cdot)$ um anel.*

*(a) O zero é único;*

*(b) O simétrico é único.*

*Demonstração.*

(a) Suponhamos que $0_A$ e $u$ satisfazem o item (iii) da Definição 3.1.2. Assim,

- $u = u + 0_A$, pois $0_A$ é neutro na adição e
- $u + 0_A = 0_A$, pois $u$ é neutro na adição.

Das duas igualdades acima podemos concluir que $u = 0_A$, ou seja, o elemento neutro da adição é único.

(b) Seja $a \in A$. Suponhamos que $b$ e $c$ são simétricos de $a$, ou seja, $a + b = b + a = 0_A$ e $a + c = c + a = 0_A$. Assim,

$$b = b + 0_A = b + (a + c) = (b + a) + c = 0_A + c = c.$$

Logo $c = b$ e, portanto, o simétrico de $a$ é único. □

Quando não houver confusão, denotaremos por 0 o elemento neutro da adição (também chamado de *zero*) do anel $(A, +, \cdot)$. Seja $a \in A$. Uma vez que o simétrico de $a$ é único, denotamos por $-a$ o simétrico de $a$.

A operação de adição $+$ em $A$, associa a cada par de elementos de $A$ um único elemento de $A$. Portanto, para quaisquer $a, b, c \in A$, se $b = c$, os pares $(a, b)$ e $(a, c)$ são idênticos em $A \times A$, o que implica que $a + b = a + c$. Isso significa que, se $b = c$, então

$a + b = a + c$ para qualquer $a \in A$. Da mesma forma, se $b = c$, então $b + a = c + a$. Além disso, considerando que a multiplicação $\cdot$ em $A$ também é uma operação em $A$, temos que se $b = c$, então $ab = ac$ e $ba = ca$. Isso prova a seguinte proposição:

**Proposição 3.1.5.** *Seja $(A, +, \cdot)$ um anel. Para quaisquer $a, b, c \in A$ temos que:*

*(a)* $b = c \;\Rightarrow\; a + b = a + c \;\; e \;\; b + a = c + a.$

*(b)* $b = c \;\Rightarrow\; ab = ac \;\; e \;\; ba = ca.$

Na próxima proposição, demonstraremos a validade da lei do cancelamento da adição em um anel. No entanto, devemos ter cuidado com a lei do cancelamento do produto nesse contexto, pois a sua validade depende de uma propriedade adicional do anel. Abordaremos essa questão em detalhes nas etapas seguintes da nossa análise.

**Proposição 3.1.6.** *Sejam $(A, +, \cdot)$ um anel. Para quaisquer $a, b, c \in A$:*

*(a)* $a + b = a + c \;\Rightarrow\; b = c$ *(lei do cancelamento da soma).*

*(b)* $a \cdot 0 = 0 = 0 \cdot a.$

*Demonstração.*

(a) Por hipótese $a + b = a + c$. Somando $-a$ em ambos os lados, obtemos

$$\begin{aligned}(-a) + (a + b) = (-a) + (a + c) \;&\Rightarrow\; (-(a) + a) + b = (-(a) + a) + c \\ &\Rightarrow\; 0 + b = 0 + c \;\Rightarrow\; b = c.\end{aligned}$$

Logo, se $b + a = c + a$, então $b = c$.

(b) Pelos axiomas (iii) e (vi) da Definição 3.1.2 temos que

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

Assim, $a \cdot 0 + 0 = a \cdot 0 = a \cdot 0 + a \cdot 0$. Pela lei do cancelamento da soma,

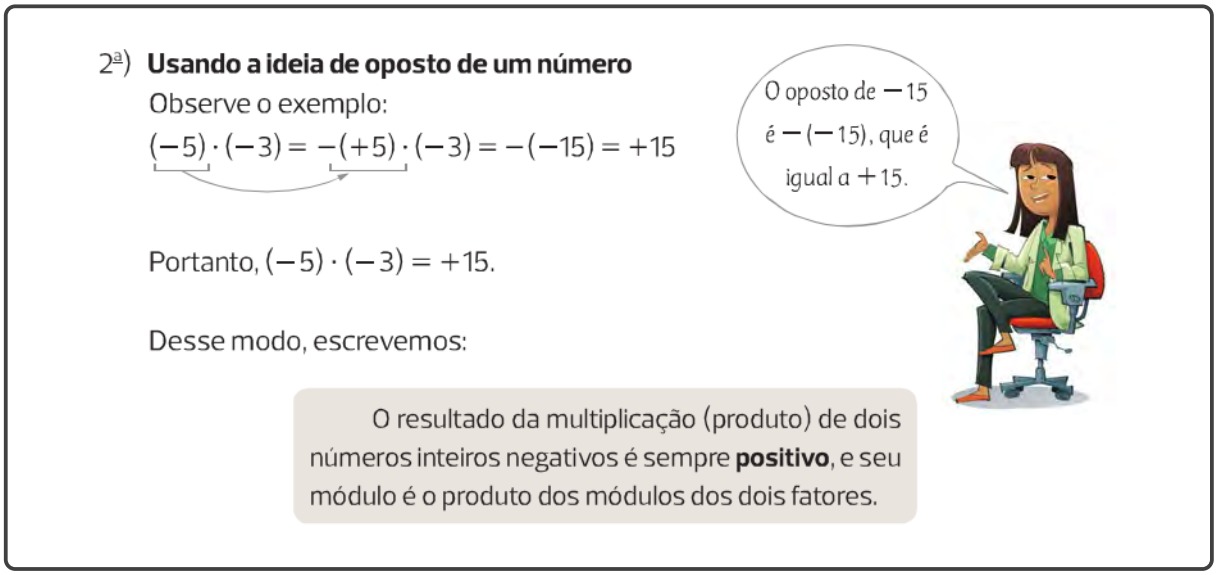
$$0 = a \cdot 0.$$

Analogamente, mostra-se que $a \cdot 0 = 0$. □

Ainda há outras propriedades de um anel que precisamos explorar. As propriedades que já vimos, assim como as próximas, são satisfeitas pelos números inteiros. Portanto, ao invés de considerar os números inteiros como um anel específico, podemos pensar em um anel como uma generalização dos números inteiros. Por exemplo, as regras de sinais

também são aplicáveis em um anel. Como podemos perceber na Figura 11 e na Proposição 3.1.7.

Figura 11 – Regras de sinais.




Fonte: DANTE (2015a, p.36)

**Proposição 3.1.7.** *Sejam* $(A, +, \cdot)$ *um anel e* $a, b, c \in A$*. Então,*

*(a)* $-(-a) = a$*;*

*(b)* $a(-b) = (-a)b = -(ab)$*;*

*(c)* $(-a)(-b) = ab$*.*

*Demonstração.*

(a) Sabemos que $-a$ é o simétrico de $a$, dessa forma, valem as igualdades:

$$a + (-a) = 0 = (-a) + a.$$

No entanto, essas mesmas igualdades mostram que $a$ é simétrico de $(-a)$. Pelo item (b) da Proposição 3.1.4, o simétrico é único, portanto, $a = -(-a)$. (Lembre que o símbolo $-$ indica o simétrico.)

(b) Temos que

$$(-a)b + ab = (-a + a)b = 0 \cdot b = 0.$$

Isso mostra que $(-a)b$ é simétrico de $ab$. Pela unicidade do simétrico, $(-a)b = -(ab)$. A igualdade $(-ab) = a(-b)$ é análoga.

(c) Pelos itens anteriores obtemos

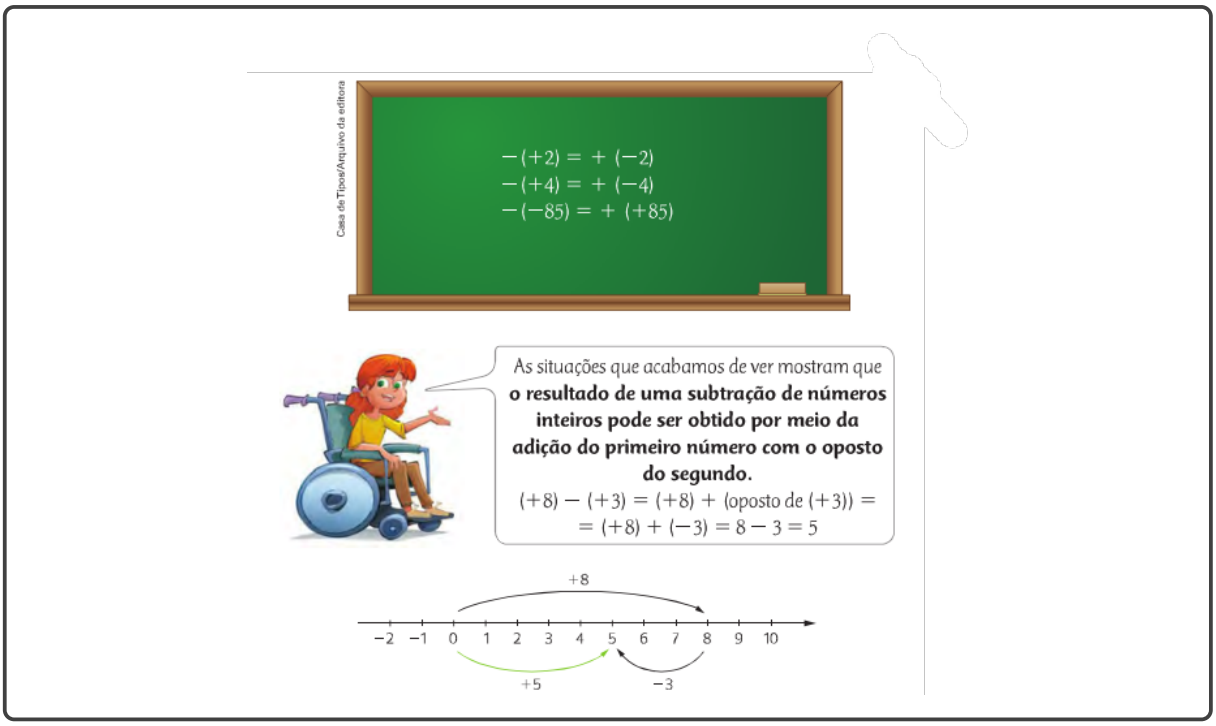
$$(-a)(-b) = -(a(-b)) = -(-(ab)) = ab. \qquad \square$$

A subtração entre dois elementos de um anel $A$ é definida a partir do axioma (iv) da Definição 3.1.2, como segue:

**Definição 3.1.8.** Sejam $(A, +, \cdot)$ um anel e $a, b \in A$. Denomina-se *subtração* entre $a$ e $b$ e indica-se por $a - b$ o elemento $a + (-b)$. Portanto,

$$a - b = a + (-b).$$

Figura 12 – Subtração de números inteiros




Fonte: DANTE (2015a, p.31)

**Proposição 3.1.9.** *Seja $(A, +, \cdot)$ um anel. Para quaisquer $a, b, c \in A$ temos:*

*(a)* $a(b - c) = ab - ac$ *e* $(a - b)c = ac - bc$;

*(b)* $-(a + b) = -a - b$.

*Demonstração.*

(a) Pela Definição 3.1.8, $a(b - c) = a(b + (-c))$. Utilizando o axioma (vi) da Definição 3.1.2, a Proposição 3.1.6 e a Definição 3.1.8 novamente, obtemos

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

De forma análoga podemos concluir que:

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

(b) Pelos quatro axiomas da adição da Definição 3.1.2 e pela a Definição 3.1.8 temos:

$$(a+b) + (-a-b) = (a+b) + (-a) + (-b) = a + (-a) + b + (-b) = 0 + 0 = 0.$$

Da mesma maneira, $(-a-b) + (a+b) = 0$. Isso mostra que $-a-b$ é o simétrico de $a+b$ e, pela unicidade do simétrico, concluímos que $-a-b = -(a+b)$. □

A seguir, apresentaremos mais exemplos de anéis.

Seja $i$ o número complexo tal que $i^2 = -1$. Os números complexos da forma $a+bi$, onde $a, b \in \mathbb{Z}$, são chamados de *inteiros de Gauss* e o conjunto desses números denotamos por $\mathbb{Z}[i]$. De acordo com Stewart e Tall (2016), entre os anos de 1808 e 1825, Gauss, investigava questões relacionadas à reciprocidade cúbica e à reciprocidade biquadrática, quando percebeu que essa investigação se tornava mais simples trabalhando sobre $\mathbb{Z}[i]$, o anel dos inteiros gaussianos, do que em $\mathbb{Z}$, o conjunto dos números inteiros.

**Exemplo 3.1.10.** Verificaremos que $(\mathbb{Z}[i], +, \cdot)$ é um anel, em que as operações de adição $(+)$ e multiplicação $(\cdot)$ são definidas, respectivamente, por

$$(a+bi) + (c+di) = (a+c) + (b+d)i$$

e

$$(a+bi) \cdot (c+di) = ac - bd + (ad+bc)i.$$

Para provar os seis axiomas da Definição 3.1.2, consideramos $\alpha = a+bi$, $\beta = c+di$ e $\gamma = e+fi \in \mathbb{Z}[i]$.

(i) Associatividade da adição:

$$\begin{aligned}\alpha + (\beta + \gamma) &= (a+bi) + [(c+di) + (e+fi)] = a + bi + [(c+e) + (d+f)i] \\ &= [a + (c+e)] + [b + (d+f)]i = [(a+c) + e] + [(b+d) + f]i \\ &= [(a+c) + (b+d)i] + [e+fi] = [(a+bi) + (c+di)] + (e+fi) \\ &= (\alpha + \beta) + \gamma.\end{aligned}$$

Observamos que ao longo das igualdades imediatamente acima, foram utilizadas a definição de adição em $\mathbb{Z}[i]$ e a associatividade da adição dos números inteiros.

(ii) Comutatividade da adição:

$$\begin{aligned}\alpha + \beta &= (a+bi) + (c+di) = (a+c) + (b+d)i = (c+a) + (d+b)i \\ &= (c+di) + (a+bi) = \beta + \alpha.\end{aligned}$$

Algumas destas igualdades seguem da comutatividade da adição em $(\mathbb{Z}, +, \cdot)$ e, novamente, da adição definida para os elementos de $\mathbb{Z}[i]$.

(iii) Elemento neutro da adição: É fácil ver que o número $0 = 0 + 0i \in \mathbb{Z}[i]$ é o zero.

(iv) Elemento simétrico: Dado $\alpha = a + bi \in \mathbb{Z}[i]$, temos que $\omega = -a - bi \in \mathbb{Z}[i]$. Satisfaz

$$\alpha + \omega = a + bi + (-a - bi) = (a - a) + (b - b)i = 0 + 0i = 0$$

e, analogamente, $\omega + \alpha = 0$. Logo, $\omega = -\alpha$, ou seja, $-a - bi$ é o simétrico de $a + bi$.

(v) Associatividade da multiplicação:

$$\begin{aligned}\alpha(\beta\gamma) &= (a + bi)[(c + di)(e + fi)] = (a + bi)[(ce - df) + (cf + de)i] \\ &= a(ce - df) - b(cf + de) + [a(cf + de) + b(ce - df)]i \\ &= ace - adf - bcf - bde + [acf + ade + bce - bdf]i.\end{aligned}$$

Por outro lado,

$$\begin{aligned}(\alpha\beta)\gamma &= [(a + bi)(c + di)](e + fi) = [(ac - bd) + (ad + bc)i](e + fi) \\ &= (ac - bd)e - (ad + bc)f + [(ac - bd)f + (ad + bc)e]i \\ &= ace - bde - adf - bcf + [acf - bdf + ade + bce]i\end{aligned}$$

Pela comutatividade e associatividade da multiplicação dos números inteiros, percebemos que $\alpha(\beta\gamma) = (\alpha\beta)\gamma$.

(vi) Distributividade da multiplicação em relação a adição:

$$\begin{aligned}\alpha(\beta + \gamma) &= (a + bi)[(c + di) + (e + fi)] = (a + bi)[(c + e) + (d + f)i] \\ &= a(c + e) - b(d + f) + [a(d + f) + b(c + e)]i \\ &= ac + ae - bd - bf + [ad + af + bc + be]i \\ &= (ac - bd) + (ae - bf) + [(ad + bc) + (af + be)]i \\ &= [(ac - bd) + (ad + bc)i] + [(ae - bf) + (af + be)i] \\ &= (a + bi)(c + di) + (a + bi)(e + fi) = \alpha\beta + \alpha\gamma.\end{aligned}$$

Além da utilização das definições de adição e multiplicação em $\mathbb{Z}[i]$, também utilizamos a associatividade e a comutatividade da adição e a distributividade dos inteiros. Similarmente, prova-se $(\alpha + \beta)\gamma = \alpha\gamma + \beta\gamma$.

Lembramos que o conjunto dos números complexos $\mathbb{C}$ é formado por todo os elementos da forma $a + bi$, em que $a, b \in \mathbb{R}$. Com isso, observamos que a demonstração de que $(\mathbb{C}, +, \cdot)$ é um anel é similar ao Exemplo 3.1.10; apenas é necessário trocar os números inteiros pelo números reais.

**Exemplo 3.1.11.** Sejam $p$ um número natural primo e $\mathbb{Z}[\sqrt{p}] = \{a + b\sqrt{p} \mid a, b \in \mathbb{Z}\}$. Definimos $+$ e $\cdot$ em $\mathbb{Z}[\sqrt{p}]$ como segue:

$$(a + b\sqrt{p}) + (c + d\sqrt{p}) = (a + c) + (b + d)\sqrt{p} \tag{3.1}$$

e

$$(a + b\sqrt{p}) \cdot (c + d\sqrt{p}) = ac + pbd + (ad + bc)\sqrt{p}. \tag{3.2}$$

Com essas operações, $(\mathbb{Z}[\sqrt{p}], +, \cdot)$ é um anel. A prova dessa afirmação é semelhante ao Exemplo 3.1.10.

Temos que o conjunto $\mathbb{Q}[\sqrt{p}] = \{a + b\sqrt{p} \mid a, b \in \mathbb{Q}\}$, em que a adição e multiplicação de seus elementos seguem, respectivamente, a mesma regras de 3.1 e 3.2, também é um anel.

### 3.1.1 Anéis de Integridades e Corpos

A seguir, apresentamos definições que conferem ao anel $A$ denominações especiais. A estrutura algébrica dos conjuntos numéricos do Exemplo 3.1.3 é mais "rica", pois também satisfaz as três seguintes propriedades:

**Definição 3.1.12.** Dizemos que o anel $(A, +, \cdot)$ é *comutativo* quando:

(vii) $\forall\, a, b \in A,\ a \cdot b = b \cdot a$. Ou seja, a multiplicação é comutativa em $A$.

**Definição 3.1.13.** Dizemos que o anel $(A, +, \cdot)$ é um anel *com unidade* quando:

(viii) $\exists\, 1 \in A, \forall\, a \in A$ tal que $a \cdot 1 = a = 1 \cdot a$. Isto é, em $A$ existe elemento neutro da multiplicação.

**Definição 3.1.14.** Dizemos que o anel $(A, +, \cdot)$ é *um anel sem divisores de zero* quando:

(ix) Para quaisquer $a, b \in A$, se $a \cdot b = 0$, então $a = 0$ ou $b = 0$.

Com esses itens adicionais, (vii), (viii) e (ix), os anéis do Exemplo 3.1.3 são considerados anéis de integridade, como vemos na definição abaixo:

**Definição 3.1.15.** Se $(A, +, \cdot)$ é um anel comutativo, com unidade e sem divisores de zero, então $A$ recebe o nome de *Anel de Integridade* ou *Domínio de Integridade*.

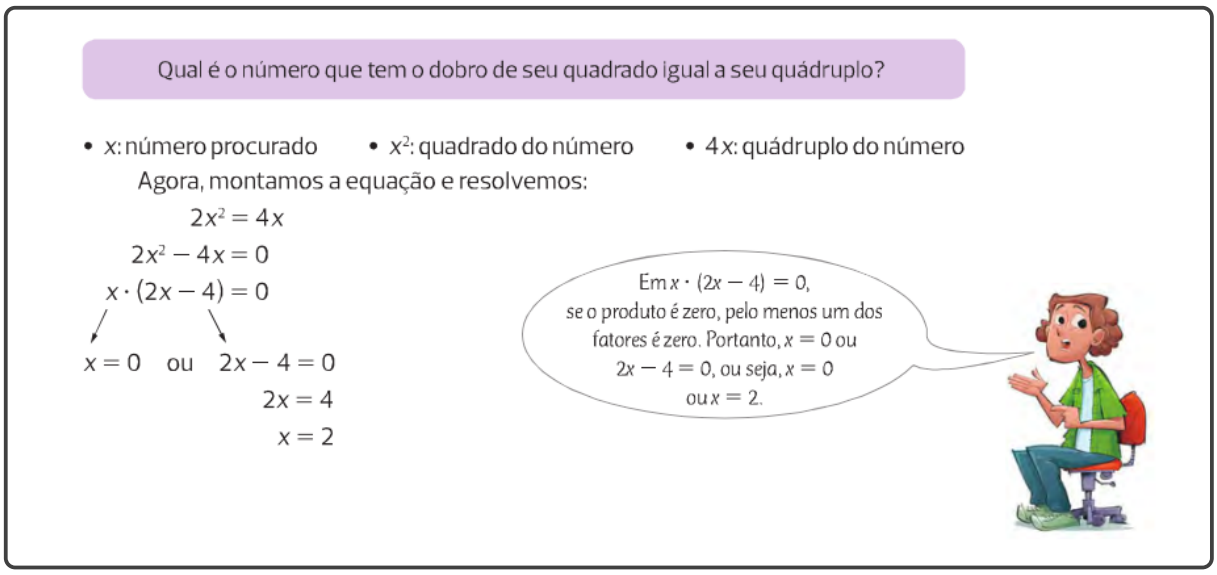
**Exemplo 3.1.16.** Os conjuntos numéricos

$$(\mathbb{Z}, +, \cdot),\ (\mathbb{Q}, +, \cdot),\ (\mathbb{R}, +, \cdot) \text{ e } (\mathbb{C}, +, \cdot)$$

são anéis de integridade com as operações usuais de soma e produto.

A propriedade sem divisores de zero é útil para resolver equações, como vemos na Figura 13.

Figura 13 – Sem divisores de zero.




Fonte: DANTE (2015b, p.53)

Sabemos que nos conjuntos numéricos vale a lei do cancelamento do produto. Isto é, se $a, b, c \in \mathbb{Z}$, $c \neq 0$ e $ac = bc$, então $a = b$. Em um anel, a lei do cancelamento do produto é equivalente a propriedade sem divisores de zero, como mostra a seguinte proposição.

**Proposição 3.1.17.** *Sejam $(A, +, \cdot)$ um anel e $a, b, c \in A$ com $c \neq 0$. As seguintes propriedades são equivalentes:*

*(i) se $a \cdot b = 0$, então $a = 0$ ou $b = 0$.*

*(ii) se $ac = bc$ ou $ca = cb$, então $a = b$.*

*Demonstração.* $(i) \Rightarrow (ii)$ Temos que

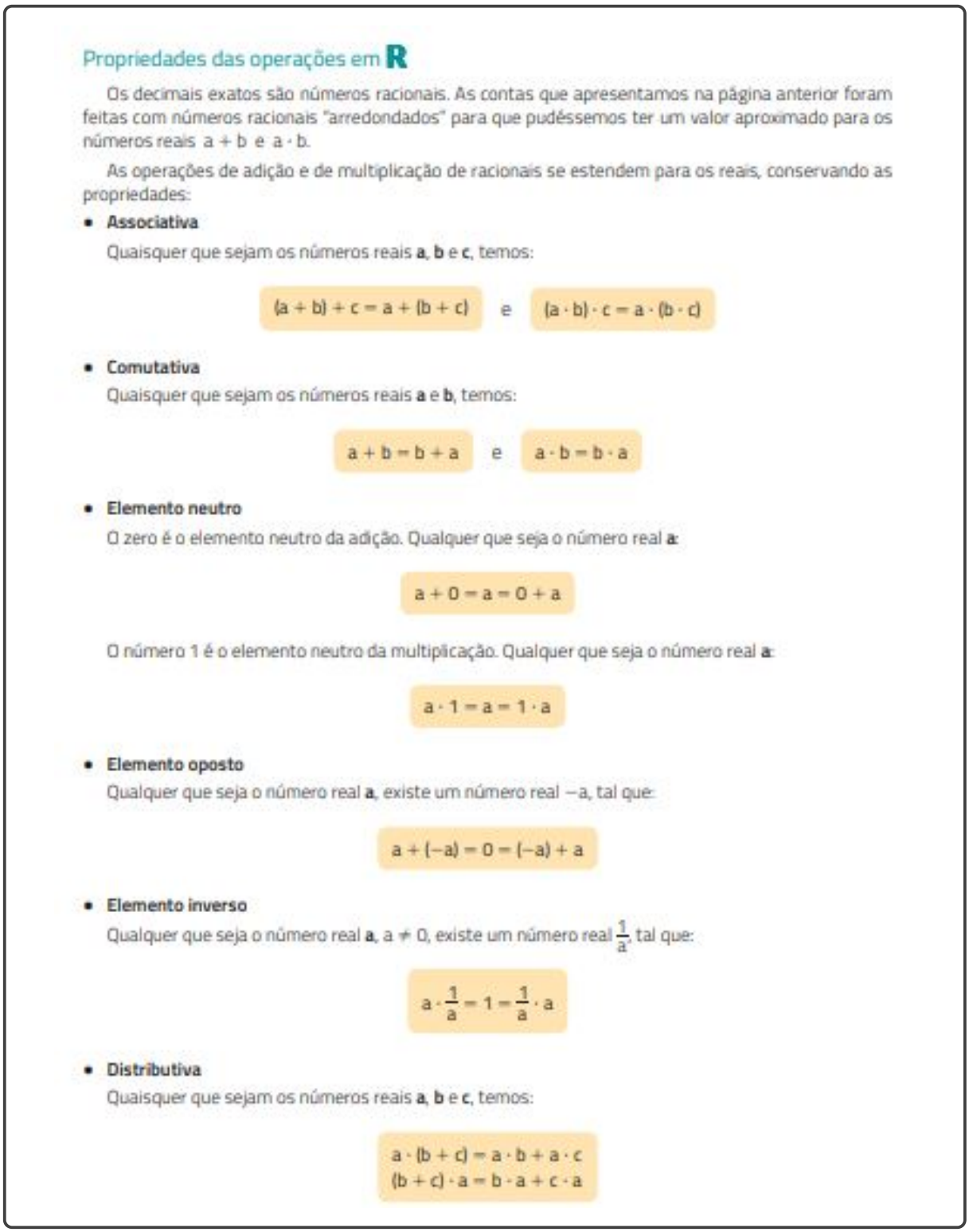
$$ac = bc \Rightarrow ac - bc = 0 \Rightarrow ac + (-b)c = 0 \Rightarrow (a - b)c = 0.$$

Por hipótese, $A$ não possui divisores de zero e como $c \neq 0$ temos que $b - a = 0$, ou seja, $b = a$. A outra verificação é análoga.

$(ii) \Rightarrow (i)$ Sejam $a, b \in A$, tais que $ab = 0$. Se $a = 0$, nada a fazer. Suponhamos que $a \neq 0$. Da Proposição 3.1.6 (b) segue que $ab = 0 = a \cdot 0$. Logo, pela hipótese, $b = 0$. □

Até o momento, os quatro conjuntos numéricos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ possuem a mesma estrutura algébrica. No entanto, veremos que os números inteiros se diferenciam dos demais.

Figura 14 – O conjunto dos números reais é um corpo.



## Propriedades das operações em $\mathbb{R}$

Os decimais exatos são números racionais. As contas que apresentamos na página anterior foram feitas com números racionais "arredondados" para que pudéssemos ter um valor aproximado para os números reais $a + b$ e $a \cdot b$.

As operações de adição e de multiplicação de racionais se estendem para os reais, conservando as propriedades:

- **Associativa**

  Quaisquer que sejam os números reais **a**, **b** e **c**, temos:

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

- **Comutativa**

  Quaisquer que sejam os números reais **a** e **b**, temos:

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

- **Elemento neutro**

  O zero é o elemento neutro da adição. Qualquer que seja o número real **a**:

  $$a + 0 = a = 0 + a$$

  O número 1 é o elemento neutro da multiplicação. Qualquer que seja o número real **a**:

  $$a \cdot 1 = a = 1 \cdot a$$

- **Elemento oposto**

  Qualquer que seja o número real **a**, existe um número real $-a$, tal que:

  $$a + (-a) = 0 = (-a) + a$$

- **Elemento inverso**

  Qualquer que seja o número real **a**, $a \neq 0$, existe um número real $\frac{1}{a}$, tal que:

  $$a \cdot \frac{1}{a} = 1 = \frac{1}{a} \cdot a$$

- **Distributiva**

  Quaisquer que sejam os números reais **a**, **b** e **c**, temos:

  $$a \cdot (b + c) = a \cdot b + a \cdot c$$
  $$(b + c) \cdot a = b \cdot a + c \cdot a$$

Fonte: IEZZI; DOLCE; MACHADO (2018c, p.37)

Na Figura 14, qual propriedade da multiplicação não é satisfeita em $\mathbb{Z}$?

**Definição 3.1.18.** Um *corpo* $\mathbb{K}$ é um anel comutativo com unidade 1 que satisfaz:

(x) $\forall a \in \mathbb{K} - \{0\}$, $\exists\, b \in \mathbb{K}$ tal que $a \cdot b = 1 = b \cdot a$.

**Definição 3.1.19.** Seja $A$ um anel com unidade. Dizemos que $a \in A$ é um *elemento inversível* quando existe $b \in A$ tal que $ab = 1_A = ba$. Denotamos o conjunto dos elementos inversíveis de $A$ por $A^\times$, isto é,

$$A^\times = \{a \in A \mid \exists\, b \in A \text{ tal que } ab = ba = 1\}.$$

**Exemplo 3.1.20.** Os conjuntos numéricos $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ e $(\mathbb{C}, +, \cdot)$ são corpos com as operações usuais de soma e produto.

**Exemplo 3.1.21.** O anel $(\mathbb{Z}, +, \cdot)$ **não** é um corpo, pois o elemento $2 \neq 0$ não é inversível em $\mathbb{Z}$, ou seja, não existe um número inteiro $x \in \mathbb{Z}$ tal que $2x = 1$. Os únicos elementos inversíveis em $\mathbb{Z}$ são 1 e $-1$, sendo que seus inversos são eles próprios.

Para o próximo exemplo lembramos que o módulo de um número complexo $\alpha = a + bi$ é usualmente denotado por $|\alpha|$ e que $|\alpha| = \sqrt{a^2 + b^2}$.

**Exemplo 3.1.22.** No anel dos inteiros de Gauss $\mathbb{Z}[i]$, um elemento $a + bi$ é inversível se, e somente se, $a^2 + b^2 = 1$. Neste caso, o inverso de $a + bi$ é $a - bi$.

De fato, é fácil ver que 1 é a unidade de $\mathbb{Z}[i]$. Se $a^2+b^2 = 1$, então $(a+bi)(a-bi) = a^2+b^2 = 1$, ou seja, $a-bi$ é o inverso se $a+bi$. Reciprocamente, suponhamos que $\alpha = a+bi$ é inversível. Então, existe $\beta = c + di$ tal que $\alpha\beta = 1$. Assim,

$$\begin{aligned} \alpha\beta = 1 \Rightarrow |\alpha\beta| = |1| \Rightarrow |\alpha\beta|^2 \Rightarrow |\alpha|^2|\beta|^2 = 1 \\ \Rightarrow (a^2 + b^2)(c^2 + d^2) = 1. \end{aligned}$$

Como $a, b, c, d$ são números inteiros, temos que $a^2 + b^2$ e $c^2 + d^2$ são números inteiros não negativos. Consequentemente, a única solução da equação $(a^2 + b^2)(c^2 + d^2) = 1$ é $a^2 + b^2 = c^2 + d^2 = 1$.

Podemos concluir que $(\mathbb{Z}[i])^\times = \{1, -1, i, -i\}$.

**Exemplo 3.1.23.** Seja $p$ um número natural primo. Então qualquer elemento $a + b\sqrt{p} \in (\mathbb{Q}[\sqrt{p}])^*$ é inversível e seu inverso é

$$\frac{a}{a^2 - pb^2} - \frac{b}{a^2 - pb^2}\sqrt{p}.$$

Com efeito, temos que 1 é a unidade de $\mathbb{Q}[\sqrt{p}]$.

Observamos que se $a + b\sqrt{p} \neq 0$ se, e somente se, $a = b = 0$. Obviamente, se $a = b = 0$ temos que $a + b\sqrt{p} = 0$. Agora, suponhamos que $a + b\sqrt{p} = 0$. Se $b \neq 0$, teríamos que $\sqrt{p} = \frac{-a}{b}$, o que não pode ocorrer, pois $\frac{-a}{b}$ é racional e $\sqrt{p}$ é irracional. Logo,

$b = 0$. Consequentemente, $0 = a + b\sqrt{p} = a + 0\sqrt{p} = a$, mostrando que $a = b = 0$. Com isso, se $a + b\sqrt{p} \neq 0$, então $a - b\sqrt{p} \neq 0$.

Como $a + b\sqrt{p}$ e $a - b\sqrt{p}$ são números reais não nulos, segue que

$$0 \neq (a + b\sqrt{p})(a - b\sqrt{p}) = a^2 - pb^2.$$

Também temos que $\dfrac{a}{a^2 - b^2p},\ \dfrac{b}{a^2 - b^2p} \in \mathbb{Q}$ e, que

$$\begin{aligned}(a + b\sqrt{p})\left(\frac{a}{a^2 - pb^2} - \frac{b}{a^2 - pb^2}\sqrt{p}\right) &= a\frac{a}{a^2 - pb^2} - pb\frac{b}{a^2 - pb^2} + \left[-a\frac{b}{a^2 - pb^2} + b\frac{a}{a^2 - pb^2}\right]\sqrt{p} \\ &= 1 + 0i = 1,\end{aligned}$$

como desejado.

**Proposição 3.1.24.** *Seja $(A, +, \cdot)$ um anel com unidade 1. Então:*

*(a) A unidade é única.*

*(b) Se $a \in A - \{0\}$ possui inverso em A, então o inverso de a é único.*

*Demonstração.*

(a) Suponhamos a existência de outro $u \in A$ que também seja uma unidade no anel, ou seja, $u \cdot a = a = a \cdot u$, para quaisquer $a \in A$. Assim, $u \cdot 1 = 1$. Como 1 também é uma unidade no anel, temos que $u \cdot 1 = u$. A partir dessas duas últimas igualdades, concluímos que $u = 1$. Portanto, a unidade no anel é única.

(b) Suponhamos que $b$ e $c$ são inversos. Então $ab = 1 = ba$ e $ac = 1 = ca$. Dessa forma,

$$c = 1 \cdot c = (b.a)c = b(ac) = b \cdot 1 = b.$$

Portanto, $c = b$ e o inverso é único. □

Seja $a \in A$ inversível. Uma vez que o inverso de $a$ é único, o denotamos por $a^{-1}$.

**Proposição 3.1.25.** *Se $(\mathbb{K}, +, \cdot)$ é um corpo, então $(\mathbb{K}, +, \cdot)$ é um anel de integridade.*

*Demonstração.* Como $\mathbb{K}$ é um corpo, temos que $\mathbb{K}$ é um anel com unidade, comutativo e que satisfaz o axioma $(x)$. Para mostrar que $\mathbb{K}$ é domínio, falta verificarmos que $\mathbb{K}$ é sem divisores de zero.

Suponhamos que $a, b \in \mathbb{K}$ tal que $ab = 0$. Se $a = 0$, então a demonstração está concluída. Agora, suponhamos que $a \neq 0$. Usando o axioma $(x)$, sabemos que existe $a^{-1} \in \mathbb{K}$ tal que $aa^{-1} = 1$. Utilizando os axiomas $(vi)$, $(viii)$ e $(x)$, temos:

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

Portanto, quando $ab = 0$, temos que $a = 0$ ou $b = 0$. Isso demonstra que $\mathbb{K}$ é um domínio. □

A recíproca da última proposição não é verdadeira. Temos que $(\mathbb{Z}, +, \cdot)$ é um anel de integridade, mas não é um corpo.

**Exemplo 3.1.26.** Realizando algumas cálculos adicionais no Exemplo 3.1.10, é fácil ver que $(\mathbb{Z}[i], +, \cdot)$ é um anel de integridade. Através do Exemplo 3.1.23, vemos que $(\mathbb{Q}[\sqrt{p}], +, \cdot)$ é um corpo.

**Exemplo 3.1.27.** Podemos construir novos anéis a partir de anéis conhecidos e uma forma de fazer isso é o que chamamos de produto direto. O produto direto é uma construção algébrica que combina dois ou mais anéis do seguinte modo:

Seja $A_1, A_2, \ldots, A_n$ uma coleção finita de anéis. O *produto direto* desses anéis é o conjunto cartesiano

$$A = A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in A_i,\ 1 \leq i \leq n\},$$

com as operações de adição e multiplicação definidas, respectivamente, por

$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$$

e

$$(a_1, a_2, \ldots, a_n) \cdot (b_1, b_2, \ldots, b_n) = (a_1 \cdot b_1, a_2 \cdot b_2, \ldots, a_n \cdot b_n),$$

para todo $a_i, b_i \in A_i$ e $1 \leq i \leq n$.

É fácil verificar que o produto direto $A$ é um anel. O zero de $A$ é o elemento $(0_1, 0_2, \ldots, 0_n)$, sendo $0_i$ o zero de $A_i$, para cada $i$. Além disso,

(a) Se todo $A_i$ têm unidade $1_i$, então $A$ tem unidade. Mais precisamente, denotando por $1_i$ a unidade $A_i$ para cada $i$, temos que a $n$-upla $(1_1, 1_2, \cdots, 1_n)$ é a unidade de $A$.

(b) Se $A_i$ são comutativos, então $A$ é comutativo.

No entanto, o produto direto $A$ tem divisores de zero se existe algum $A_i \neq \{0\}$. Por exemplo, em $A = \mathbb{Z} \times \mathbb{Z}$, os pares ordenados $(1, 0)$ e $(0, 2)$ são divisores de zero, uma vez que $(1, 0)(0, 2) = (0, 0)$ e nenhum deles é o zero do anel $\mathbb{Z} \times \mathbb{Z}$.

A seguir, apresentaremos outros exemplos de anéis, como os anéis de matrizes, os anéis de polinômios e o produto direto. Ao explorarmos esses exemplos, observaremos diferenças em suas estruturas algébricas.

## 3.2 Anéis de Matrizes

Seja $(A, +, \cdot)$ uma anel. Denotamos por $M_n(A)$ o conjunto das matrizes quadradas de ordem $n$ com entradas em $A$, ou seja,

$$M_n(A) = \left\{ \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \mid a_{ij} \in A \right\}.$$

De maneira abreviada, podemos escrever uma matriz quadrada $X = \begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & \vdots & & \vdots \\ x_{n1} & x_{n2} & \cdots & x_{nn} \end{pmatrix}$ por $X = (x_{ij})$, onde fica subentendido que $1 \leq i, j \leq n$.

**Definição 3.2.1.** Duas matrizes $X = (x_{ij})$ e $Y = (y_{ij})$ em $M_n(A)$ são *iguais* se possuem entradas correspondentes iguais, ou seja, $x_{ij} = y_{ij}$ para quaisquer $i, j$.

A Figura 15 mostra um exemplo de igualdade de matrizes e colabora com compreensão da Definição 3.2.1.

Figura 15 – Igualdade de Matrizes

Determine $x$ e $y$ para que sejam iguais as matrizes $\begin{pmatrix} 3x+2y & 2 \\ 2 & 3x-3y \end{pmatrix}$ e $\begin{pmatrix} 7 & 2 \\ 2 & -3 \end{pmatrix}$.

**Resolução:**

As duas matrizes têm a mesma ordem (2).

Para que as matrizes sejam iguais devemos ter ainda:

$$\begin{cases} 3x+2y=7 \\ 3x-3y=-3 \end{cases}$$

Resolvendo esse sistema de equações do 1º grau, temos:

$$\begin{array}{r} 3x+2y=7 \\ -3x+3y=3 \\ \hline 5y=10 \Rightarrow y=2 \end{array}$$

$3x + 2y = 7 \Rightarrow 3x + 2(2) = 7 \Rightarrow 3x + 4 = 7 \Rightarrow 3x = 3 \Rightarrow x = 1$

Portanto, $x = 1$ e $y = 2$.

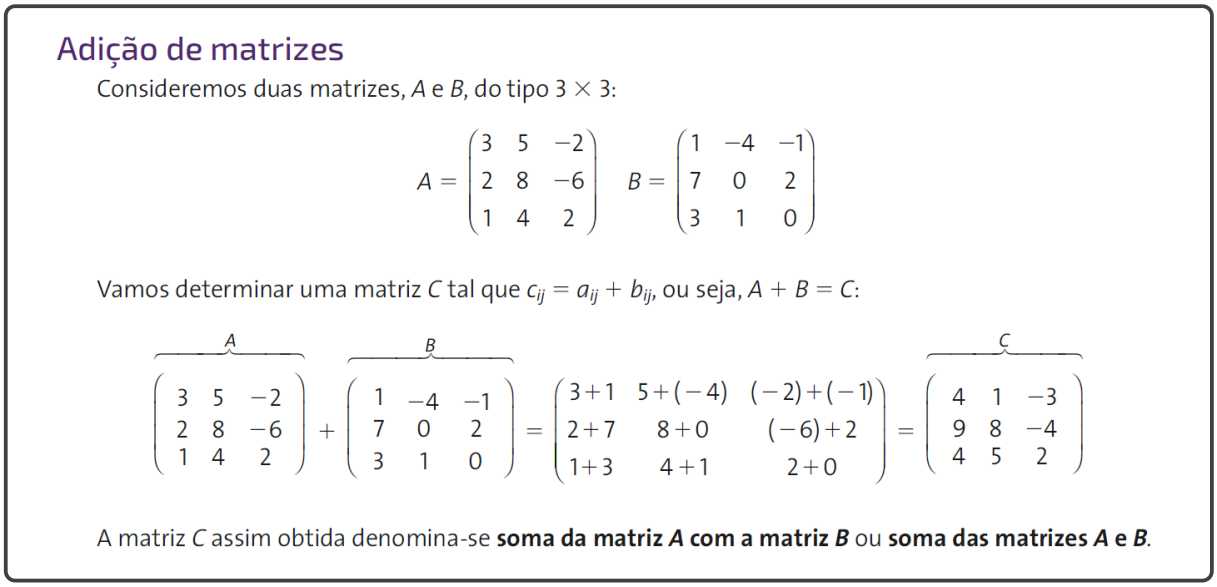
Fonte: DANTE (2016a, p.68)

**Definição 3.2.2.** Dadas $X = (x_{ij})$ e $Y = (y_{ij})$ em $M_n(A)$, definimos a adição e multiplicação de $X$ e $Y$ do seguinte modo:

- $X + Y = (x_{ij}) + (y_{ij}) = (x_{ij} + y_{ij})$;
- $X \cdot Y = (z_{ij})$, em que $z_{ij} = \sum_{k=1}^{n} x_{ik} y_{kj}$.

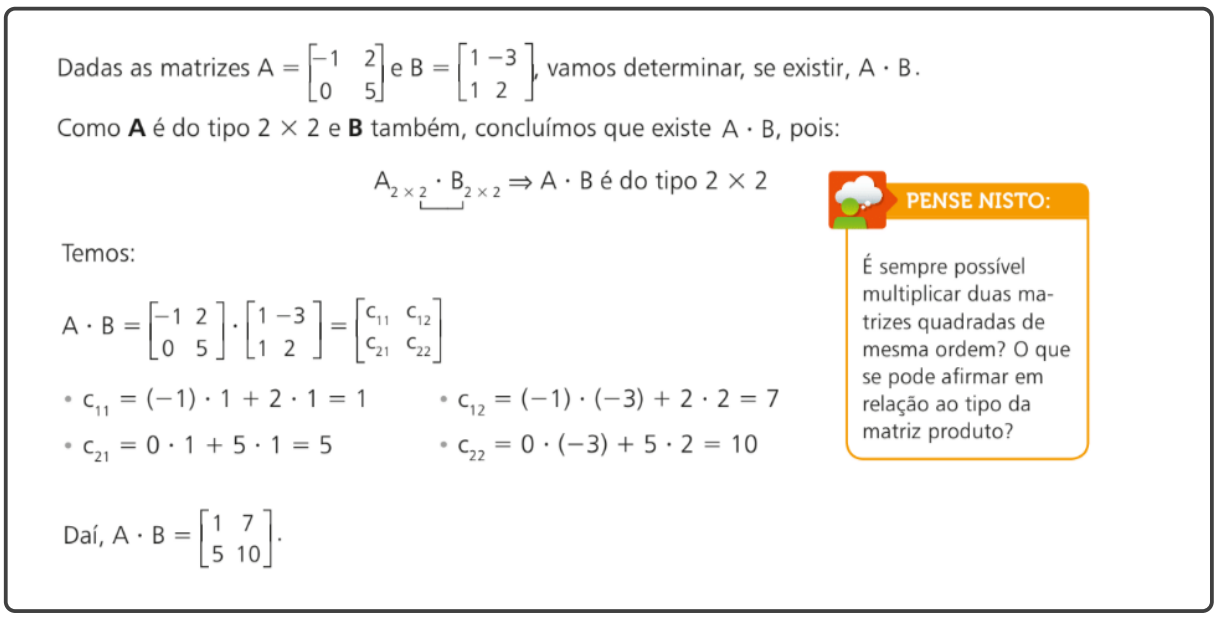
Observamos que a adição e multiplicação definidas acima são as usuais, como as matrizes com entradas reais que são estudadas no Ensino Médio. Veja as Figuras 16 e 17:

Figura 16 – Adição de Matrizes




Fonte: DANTE (2016a, p. 70)

Figura 17 – Multiplicação de Matrizes




Fonte: IEZZI; DOLCE; DEGENSZAJN; PERIGO; ALMEIDA (2016a, p.83)

Veremos a seguir, que com essas duas operações, o conjunto de todas as matrizes quadradas de ordem fixada e com entradas de um anel, também é um anel.

**Proposição 3.2.3.** *Seja $(A, +, \cdot)$ um anel e $n \geq 1$ um número natural. Então, $(M_n(A), +, \cdot)$ é um anel. E se $(A, +, \cdot)$ tem unidade, então $(M_n(A), +, \cdot)$ também tem.*

*Demonstração.* Para verificar os seis axiomas de anéis, consideramos $X = (x_{ij})$, $Y = (y_{ij})$ e $Z = (z_{ij})$ matrizes de $M_n(A)$.

(i) Associatividade da adição:

$$\begin{aligned} X + (Y + Z) = (x_{ij}) + (y_{ij} + z_{ij}) = (x_{ij} + (y_{ij} + z_{ij})) &\overset{(1)}{=} ((x_{ij} + y_{ij}) + z_{ij}) \\ &= (x_{ij} + y_{ij}) + (z_{ij}) = (X + Y) + Z. \end{aligned}$$

Na igualdade (1), utilizamos a associatividade da adição de $A$. Concluímos que $(X + Y) + Z = X + (Y + Z)$.

(ii) Comutatividade da adição:

$$X + Y = (x_{ij}) + (y_{ij}) = (x_{ij} + y_{ij}) \overset{(2)}{=} (y_{ij} + x_{ij}) = (y_{ij}) + (x_{ij}) = Y + X.$$

Em (2), utilizamos a propriedade comutativa da adição de $A$. Provamos que $X+Y = Y + X$.

(iii) Elemento neutro da adição:

Seja $0 = (0_{ij})$ a matriz nula de $M_n(A)$, ou seja, a matriz de ordem $n$ em que todas entradas são $0_A$. Então,

$$X + 0 = (x_{ij}) + (0_{ij}) = (x_{ij} + 0_{ij}) = (x_{ij}) = X.$$

Logo, $X + 0 = X$ e, analogamente, $0 + X = X$. Portanto, a matriz nula é o elemento neutro da adição em $M_n(A)$.

(iv) Elementos simétricos:

Denotamos por $-X$ a matriz $(-x_{ij})$, em que $-x_{ij}$ é o simétrico de $x_{ij}$ no anel $A$. Assim,

$$X + (-X) = (x_{ij}) + (-x_{ij}) = (x_{ij} - x_{ij}) = (0_{ij}) = 0.$$

Similarmente, $(-X) + X = 0$. Portanto, a matriz $-X = (-x_{ij})$ é o elemento simétrico da matriz $X = (x_{ij})$.

(v) Associatividade da multiplicação:

Queremos provar $(x_{ij})[(y_{ij})(z_{ij})] = [(x_{ij})(y_{ij})](z_{ij})$. Então, escrevendo,

$$(y_{ij})(z_{ij}) = (c_{ij}), \text{ em que } c_{ij} = \sum_{t=1}^{n} y_{it}z_{it},$$

$$(x_{ij})(c_{ij}) = (d_{ij}), \text{ em que } d_{ij} = \sum_{k=1}^{n} x_{ik}c_{kj},$$

$$(x_{ij})(y_{ij}) = (u_{ij}), \text{ em que } u_{ij} = \sum_{k=1}^{n} x_{ik}y_{kj} \text{ e}$$

$$(u_{ij})(z_{ij}) = (v_{ij}), \text{ em que } v_{ij} = \sum_{t=1}^{n} u_{it}z_{ij},$$

devemos provar que $d_{ij} = v_{ij}$. De fato,

$$\begin{aligned} d_{ij} &= \sum_{k=1}^{n} x_{ik}c_{kj} = \sum_{k=1}^{n} x_{ik}\sum_{t=1}^{n} y_{kt}z_{ij} = \sum_{k=1}^{n}\sum_{t=1}^{n} x_{ik}(y_{kt}z_{tj}) \\ &= \sum_{k=1}^{n}\sum_{t=1}^{n}(x_{ik}y_{kt})z_{tj} = \sum_{t=1}^{n}\sum_{k=1}^{n}(x_{ik}y_{kt})z_{tj} = \sum_{t=1}^{n} u_{it}z_{tj} = v_{ij}, \end{aligned}$$

como desejado. Observamos que ao longo dos cálculos desenvolvidos acima, usamos algumas propriedades do anel $A$, como a associatividade da multiplicação e distributividade.

(vi) Distributividade da multiplicação em relação a adição:

Faremos apenas pela esquerda $X(Y+Z) = XY + XZ$, a da direita é análoga.

$$\begin{aligned} X(Y+Z) &= (x_{ij})[(y_{ij}) + (z_{ij})] = (x_{ij})(y_{ij} + z_{ij}) = \sum_{k=1}^{n} x_{ik}(y_{kj} + z_{kj}) \\ &= \sum_{k=1}^{n}(x_{ik}y_{kj} + x_{ik}z_{kj}) = \sum_{k=1}^{n} x_{ik}y_{kj} + \sum_{k=1}^{n} x_{ik}z_{kj} = (x_{ij})(y_{ij}) + (x_{ij})(z_{ij}) \\ &= XY + XZ, \end{aligned}$$

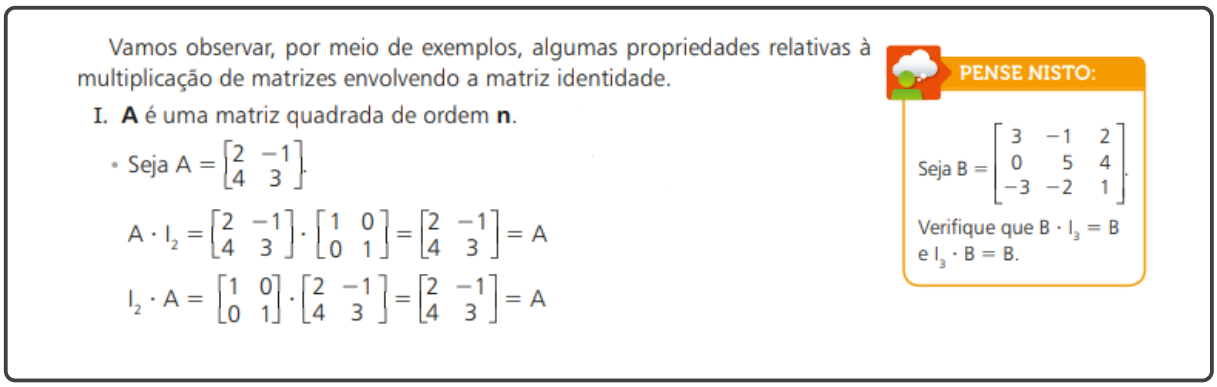
como desejado. Observamos que a distributividade, associatividade e comutatividade da adição do anel $A$ foram necessárias para provar algumas igualdades acima.

Para finalizar, se $(A, +, \cdot)$ tem unidade, então $(M_n(A), +, \cdot)$ tem unidade, em que a unidade é a matriz identidade: Veja a Figura 18

$$I_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}.$$

□

Figura 18 – Matriz Identidade



Vamos observar, por meio de exemplos, algumas propriedades relativas à multiplicação de matrizes envolvendo a matriz identidade.

I. **A** é uma matriz quadrada de ordem **n**.

- Seja $A = \begin{bmatrix} 2 & -1 \\ 4 & 3 \end{bmatrix}$.

$$A \cdot I_2 = \begin{bmatrix} 2 & -1 \\ 4 & 3 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 2 & -1 \\ 4 & 3 \end{bmatrix} = A$$

$$I_2 \cdot A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 2 & -1 \\ 4 & 3 \end{bmatrix} = \begin{bmatrix} 2 & -1 \\ 4 & 3 \end{bmatrix} = A$$

PENSE NISTO:

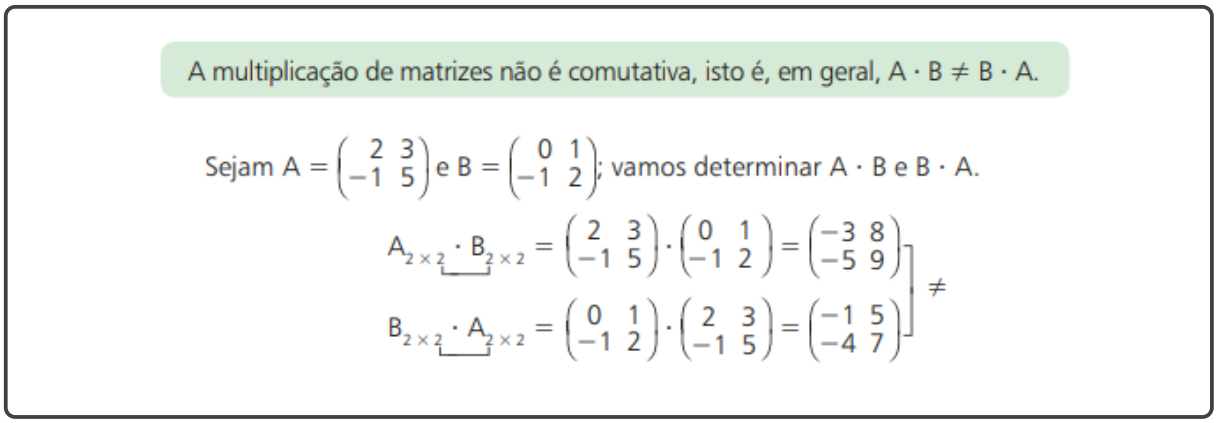
Seja $B = \begin{bmatrix} 3 & -1 & 2 \\ 0 & 5 & 4 \\ -3 & -2 & 1 \end{bmatrix}$.

Verifique que $B \cdot I_3 = B$ e $I_3 \cdot B = B$.

Fonte: IEZZI; DOLCE; DEGENSZAJN; PERIGO; ALMEIDA ( 2016, p.85)

Porém, para $n \geq 2$ e $A$ não trivial, temos que $(M_n(A), +, \cdot)$ não é comutativo e possui divisores de zero. Como podemos ver nas Figuras 19 e 20.

Figura 19 – Matrizes não comutativas.



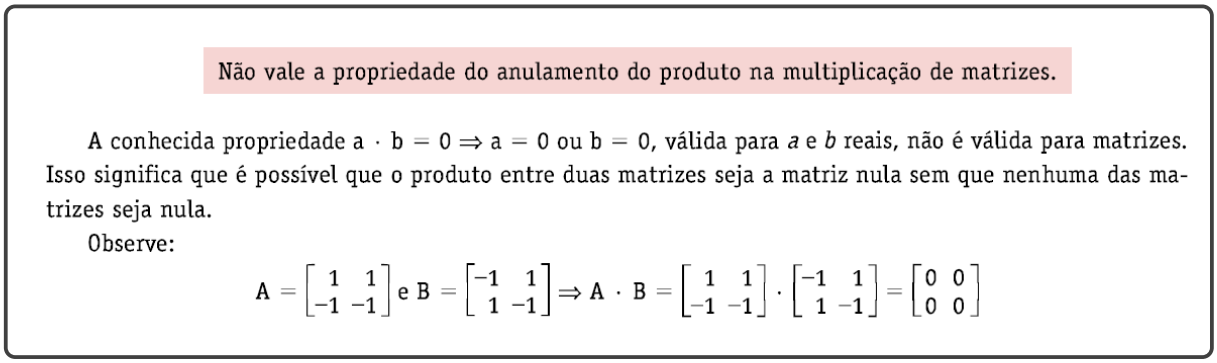
A multiplicação de matrizes não é comutativa, isto é, em geral, $A \cdot B \neq B \cdot A$.

Sejam $A = \begin{pmatrix} 2 & 3 \\ -1 & 5 \end{pmatrix}$ e $B = \begin{pmatrix} 0 & 1 \\ -1 & 2 \end{pmatrix}$; vamos determinar $A \cdot B$ e $B \cdot A$.

$$\left.\begin{aligned} A_{2\times 2} \cdot B_{2\times 2} &= \begin{pmatrix} 2 & 3 \\ -1 & 5 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ -1 & 2 \end{pmatrix} = \begin{pmatrix} -3 & 8 \\ -5 & 9 \end{pmatrix} \\ B_{2\times 2} \cdot A_{2\times 2} &= \begin{pmatrix} 0 & 1 \\ -1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 2 & 3 \\ -1 & 5 \end{pmatrix} = \begin{pmatrix} -1 & 5 \\ -4 & 7 \end{pmatrix} \end{aligned}\right] \neq$$

Fonte: IEZZI; DOLCE; DEGENSZAJN; PERIGO; ALMEIDA (2016, p.87)

Figura 20 – Matrizes divisores de zero.



Não vale a propriedade do anulamento do produto na multiplicação de matrizes.

A conhecida propriedade $a \cdot b = 0 \Rightarrow a = 0$ ou $b = 0$, válida para $a$ e $b$ reais, não é válida para matrizes. Isso significa que é possível que o produto entre duas matrizes seja a matriz nula sem que nenhuma das matrizes seja nula.

Observe:

$$A = \begin{bmatrix} 1 & 1 \\ -1 & -1 \end{bmatrix} \text{ e } B = \begin{bmatrix} -1 & 1 \\ 1 & -1 \end{bmatrix} \Rightarrow A \cdot B = \begin{bmatrix} 1 & 1 \\ -1 & -1 \end{bmatrix} \cdot \begin{bmatrix} -1 & 1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Fonte: IEZZI; DOLCE; DEGENSZAJN; PERIGO; ALMEIDA (2016, p.168)

## 3.3 Anéis de Polinômios

Na disciplina M14 - Aritmética do PROFMAT, exploramos as propriedades dos números inteiros, juntamente com as duas operações de adição e multiplicação, enfatizando questões relacionadas à divisibilidade. Entre os tópicos estudados, destacam-se o algoritmo da divisão, o máximo divisor comum, os números primos e o Teorema Fundamental da Aritmética.

Ao estudarmos os polinômios, com suas operações básicas: adição, subtração, multiplicação e divisão, notamos que os mesmos tópicos ou conceitos semelhantes aos da aritmética dos inteiros reaparecem ou surgem. Nesta seção, veremos que os anéis de polinômios com coeficientes em um anel de integridade ou corpo também são anéis de integridade. Além disso, no próximo capítulo, veremos que a estrutura algébrica muito parecida se deve ao fato de que em ambos os conjuntos existe um algoritmo da divisão.

**Definição 3.3.1.** Seja $(A, +, \cdot)$ um anel de integridade. Um *polinômio* sobre $A$, na variável (ou indeterminada) $x$, é uma expressão da forma:

$$a_0 + a_1x + a_2x^2 + \cdots + a_kx^k + \cdots$$

em que $a_0$, $a_1, a_2 \ldots$, $a_k$, $\ldots \in A$, para todo $i \in \mathbb{N} \cup \{0\}$ e existe $n \in \mathbb{N} \cup \{0\}$ tal que $a_j = 0$ para todo $j > n$.

Por exemplo, podemos tomar o anel $(A, +, \cdot)$ como sendo um dos conjuntos numéricos $(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot)$ ou $(\mathbb{C}, +, \cdot)$.

**Exemplo 3.3.2.** O polinômio $p(x) = 2 + 0x + 1x^2 + 3x^3 + 0x^4 + 0x^5 + \cdots$ sobre o anel $(\mathbb{Z}, +, \cdot)$ pode ser escrito de várias maneiras. Em particular,

$$p(x) = 2 + 0x + 1x^2 + 3x^3 \quad \text{ou} \quad p(x) = 2 + 0x + 1x^2 + 3x^3 + 0x^4.$$

**Definição 3.3.3.** Se $p(x) = a_0 + a_1x + \cdots + a_nx^n + a_{n-1}x^{n-1} + \cdots$ é tal que $a_n \neq 0$ e $a_j = 0$, para todo $j > n$, dizemos que $n$ é o *grau* do polinômio $p(x)$. Nesse caso, podemos indicar $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ e o grau de $p(x)$ por $\partial p(x) = n$.

Seja $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ um polinômio sobre $A$ na variável $x$, com $a_n \neq 0$. Dizemos que

- $a_0, a_1, a_2, \cdots$ são *coeficientes* de $p(x)$;
- $a_0$ é o *termo independente* de $p(x)$;
- $a_n$ é o *coeficiente dominante* $p(x)$.

Nas Figuras 21 e 22, veja exemplos de polinômios com coeficientes complexos apresentados num livro didático do Ensino Médio.

Figura 21 – Polinômios

Todas essas expressões são chamadas **expressões polinomiais** ou **polinômios**.

Chamamos expressão polinomial ou polinômio na variável complexa $x$ toda expressão da forma:

$$a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_2x^2 + a_1x + a_0$$

em que:

- $a_n, a_{n-1}, a_{n-2}, \ldots, a_2, a_1, a_0$ são números complexos denominados coeficientes;
- $n$ é um número inteiro positivo ou nulo;
- o maior expoente de $x$, com coeficiente não nulo, é o grau da expressão.

Veja, por exemplo, as expressões polinomiais:

a) $4x + 6$: expressão polinomial do 1º grau (grau 1).

b) $x^2 + 3x$: expressão polinomial do 2º grau (grau 2).

c) $x^3$: expressão polinomial do 3º grau (grau 3).

d) $6x^2 + (1 - i)x + 5$: expressão polinomial do 2º grau (grau 2).

Pela definição, **não** são expressões polinomiais:

- $x^{-2} + 3x^{-1} + 1$, pois o expoente da variável $x$ não pode ser negativo.
- $x^3 + \frac{1}{x^2} + \frac{1}{x}$, pois a variável $x$ não pode aparecer em denominador.

Fonte: DANTE (2016b, p.202)

Seja $A$ um anel. Para cada $a \in A^*$, o polinômio $p(x) = a + 0_x + 0x^2 + \cdots$ é chamado *polinômio constante* $a$ e é indicado por $p(x) = a$. Em particular, quando $a = 0$, temos o polinômio $p(x) = 0$, que é conhecido como *polinômio nulo*. Veja Figura 22.

Figura 22 – Polinômio Nulo

Um polinômio P(x) é chamado **polinômio nulo** ou **polinômio identicamente nulo** quando todos os seus coeficientes são iguais a zero. Indicamos por $P(x) \equiv 0$.

De maneira geral:

$P(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ é um polinômio nulo se, e somente se, $a_n = a_{n-1} = \ldots = a_1 = a_0 = 0$.

Como todos os coeficientes do polinômio nulo são iguais a zero, não definimos grau do polinômio nulo.

Fonte: BONJORNO; GIOVANNI; SOUSA (2016, p. 200)

Denotamos por $A[x]$ o conjunto de todos os polinômios sobre $A$ em uma indeterminada $x$, ou seja,

$$A[x] = \{a_0 + a_1x + \cdots + a_nx^n \mid n \in \mathbb{N} \cup \{0\}, a_i \in A \; \forall i \in \{1, 2, \cdots, n\}\}$$

**Observação 3.3.4.** Seja $A$ um anel. Para cada $a \in A$, podemos identificar esse elemento com o polinômio constante $p(x) = a$. Através desta identificação, $A \subseteq A[x]$, mais precisamente, existe uma cópia de $A$ contida em $A[x]$.

**Definição 3.3.5.** Os polinômios $p(x) = a_0 + a_1x + a_2x^2 + \cdots \in A[x]$ e $q(x) = b_0 + b_1x + b_2x^2 + \cdots \in A[x]$ são *iguais* quando $a_i = b_i, \forall i \in \mathbb{N} \cup \{0\}$. A seguir, apresenta-se um exemplo de igualdade de polinômios, conforme ilustrado na figura 23.

Figura 23 – Igualdade de Polinômios.

Determine $\alpha$ e $\beta$ de modo que
$p(x) = \alpha(x - 1) + \beta(x + 4)$ e $g(x) = 5x + 10$ sejam iguais.

**Resolução:**

$p(x) = \alpha(x - 1) + \beta(x + 4) = \alpha x - 1\alpha + \beta x + 4\beta =$
$= (\alpha + \beta)x + (-\alpha + 4\beta)$

Se $p(x) = g(x) \Rightarrow (\alpha + \beta)x + (-\alpha + 4\beta) = 5x + 10$

Assim, $\begin{cases} \alpha + \beta = 5 \\ -\alpha + 4\beta = 10 \end{cases} \Rightarrow 5\beta = 15 \Rightarrow \beta = 3$

$\alpha + 3 = 5 \Rightarrow \alpha = 2$

Logo, $\alpha = 2$ e $\beta = 3$.

Fonte: DANTE (2016b, p.205)

**Definição 3.3.6.** Sejam $p(x) = a_0+a_1x+\cdots+a_kx^k+\cdots$ e $q(x) = b_0+b_1x+\cdots+b_kx^k+\cdots$ dois elementos de $A[x]$. Definimos a adição e multiplicação, respectivamente, por

$$(p + q)(x) = p(x) + q(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_k + b_k)x^k + \cdots \in A[x]$$

e

$$(pq)(x) = p(x)q(x) = c_0 + c_1x + \cdots + c_kx^k + \cdots \in A[x]$$

onde $c_k = \sum_{i+j=k} a_ib_j$.

Nas Figuras 24, 25 e 26 são apresentados alguns exemplos das operações de adição e multiplicação de polinômios:

Figura 24 – Adição de Polinômios.

***Exemplo***

Para calcular a soma dos polinômios $P(x) \equiv 12x^4 + 6x^2 + 2x + 7$ e $Q(x) \equiv 4x^3 + 9x^2 - x - 8$, que devem ser entendidos como $P(x) \equiv 12x^4 + \mathbf{0x^3} + 6x^2 + 2x + 7$ e $Q(x) \equiv \mathbf{0x^4} + 4x^3 + 9x^2 - x - 8$, adicionamos os coeficientes dos termos de $P(x)$ com os coeficientes dos termos de $Q(x)$ que têm, respectivamente, o mesmo expoente na variável, isto é:

$$P(x) + Q(x) \equiv (12 + \mathbf{0})x^4 + (\mathbf{0} + 4)x^3 + (6 + 9)x^2 + (2 - 1)x + 7 - 8 \Rightarrow$$
$$\Rightarrow P(x) + Q(x) \equiv 12x^4 + 4x^3 + 15x^2 + x - 1$$

Fonte: BONJORNO; GIOVANNI; SOUSA (2016, p.283)

Figura 25 – Multiplicação de Mônicos.

O produto dos monômios $ax^r$ e $bx^s$, de variável $x$ e coeficientes $a$ e $b$, é o monômio $abx^{r+s}$.

***Exemplo***

$3x^4 \cdot 2x^5 = (3 \cdot 2)x^{4+5} = 6x^9$

Fonte: BONJORNO; GIOVANNI; SOUSA (2016, p.285)

Figura 26 – Multiplicação de Polinômios.

Sendo $P$ e $Q$ polinômios quaisquer, definimos o **produto** de $P$ por $Q$ como a soma dos produtos de cada monômio de $P$ por todos os monômios de $Q$.

A operação que associa $P(x)$ e $Q(x)$ ao produto desses polinômios é chamada de **multiplicação**.

***Exemplo***

Sendo $H(x) \equiv 5x^3 + 2x$ e $G(x) \equiv 2x^2 + 4x - 1$, temos:

$$H(x) \cdot G(x) \equiv (5x^3 + 2x)(2x^2 + 4x - 1) \equiv 10x^5 + 20x^4 - 5x^3 + 4x^3 + 8x^2 - 2x \Rightarrow$$

$$\Rightarrow H(x) \cdot G(x) \equiv 10x^5 + 20x^4 - x^3 + 8x^2 - 2x$$

Fonte: BONJORNO; GIOVANNI; SOUSA (2016, p.285)

Seja $A$ um anel. O teorema a seguir mostra que, com as operações definidas acima, $A[x]$ é um anel, e que a comutatividade, a existência de unidade e a inexistência de divisores de zero, são passadas de $A$ para $A[x]$.

**Teorema 3.3.7.** *Seja $(A, +, \cdot)$ é um anel. Com as operações de adição e multiplicação acima definidas temos que:*

*(a) $A[x]$ é um anel.*

*(b) Se $A$ é comutativo, então $A[x]$ é comutativo.*

*(c) Se $A$ tem unidade $1$, então $A[x]$ tem unidade.*

*(d) Se $A$ é um anel de integridade, então $A[x]$ é um anel de integridade.*

*Demonstração.*

(a) Para analisar os 6 axiomas de anel, tomamos

$$p(x) = a_0 + a_1x + a_2x^2 + \cdots \in A[x],$$
$$q(x) = b_0 + b_1x + b_2x^2 + \cdots \in A[x] \text{ e}$$
$$r(x) = c_0 + c_1x + c_2x^2 + \cdots \in A[x].$$

Percebam que os coeficientes dos polinômios são elementos de $A$, e, portanto, valem os axiomas de anel para os coeficientes.

(i) Associatividade da adição:

$$\begin{aligned} &p(x) + (q(x) + r(x)) \\ &\quad = (a_0 + a_1x + a_2x^2 + \cdots) + ((b_0 + c_0) + (b_1 + c_1)x + (b_2 + c_2)x^2 + \cdots) \\ &\quad = (a_0 + (b_0 + c_0)) + (a_1 + (b_1 + c_1))x + (a_2 + (b_2 + c_2))x^2 + \cdots \\ &\quad = ((a_0 + b_0) + c_0) + ((a_1 + b_1) + c_1)x + ((a_2 + b_2) + c_2)x^2 + \cdots \\ &\quad = ((a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \cdots) + (c_0 + c_1x + c_2x^2 + \cdots) \\ &\quad = (p(x) + q(x)) + r(x), \ \forall x \in A. \end{aligned}$$

Portanto, $p + (q + r) = (p + q) + r$ para quaisquer polinômios $p, q, r$ em $A[x]$.

(ii) Comutatividade da adição:

$$\begin{aligned} p(x) + q(x) &= (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \cdots \\ &= (b_0 + a_0) + (b_1 + a_1)x + (b_2 + a_2)x^2 + \cdots \\ &= q(x) + p(x), \ \forall x \in A. \end{aligned}$$

Logo, para quaisquer $p, q \in A[x]$ tem-se $p + q = q + p$.

(iii) Elemento neutro: Seja $p_0(x) = 0$ para todo $x \in A$. Temos que

$$\begin{aligned} p(x) + p_0(x) &= (a_0 + 0) + (a_1 + 0)x + (a_2 + 0)x^2 + \cdots \\ &= a_0 + a_1x + a_2x^2 + \cdots \\ &= p(x),\ \forall x \in A. \end{aligned}$$

Analogamente, $p_0(x) + p(x) = p(x),\ \forall x \in A$. Logo, o polinômio nulo $p_0$ é o zero de $A[x]$.

(iv) Existência de simétrico: Para cada $p(x) = a_0 + a_1x + a_2x^2 + \cdots \in A[x]$, tome o polinômio $-p(x) = -a_0 + (-a_1)x + (-a_2)x^2 + \cdots \in A[x]$. Como

$$p(x) + (-p(x)) = (a_0 - a_0) + (a_1 - a_1)x + (a_2 - a_2)x^2 + \cdots = 0 = p_0(x)$$

e, similarmente, $-p(x) + p(x) = p_0)(x)$. Logo, $-p$, definido acima, é o simétrico de $p$.)

(v) Associatividade da multiplicação:

Mostraremos que $p(x)(q(x)r(x)) = (p(x)q(x))r(x)$. Escrevendo

$$\begin{aligned} &q(x)r(x) = d_0 + d_1x + d_2x^2 + \cdots,\ d_i = \sum_{j+t=i} b_jc_t, \\ &p(x)(q(x)r(x)) = e_0 + e_1x + e_2x^2 + \cdots,\ e_i = \sum_{j+t=i} a_jd_t, \\ &p(x)q(x) = l_0 + l_1x + l_2x^2 + \cdots,\ l_i = \sum_{j+t=i} a_jb_t \text{ e} \\ &(p(x)q(x))r(x) = m_0 + m_1x + m_2x^2 + \cdots,\ m_i = \sum_{j+t=i} l_jc_t, \end{aligned}$$

devemos provar que $e_i = m_i$, $\forall i \in \mathbb{N} \cup \{0\}$. Para cada $i \in \mathbb{N} \cup \{0\}$,

$$\begin{aligned} e_i &= \sum_{j+t=i} a_jd_t = \sum_{j+t=i} a_j \left( \sum_{\alpha+\beta=t} b_\alpha c_\beta \right) = \sum_{j+\alpha+\beta=i} a_j \left(b_\alpha c_\beta\right) = \sum_{j+\alpha+\beta=i} \left(a_jb_\alpha\right) c_\beta \\ &= \sum_{n+\beta=i} \left( \sum_{j+\alpha=n} a_jb_\alpha \right) c_\beta = \sum_{n+\beta=i} l_nc_\beta = m_i. \end{aligned}$$

(vi) Distributividade:

Analisamos apenas a distributividade à esquerda, a outra é análoga. Queremos mostrar que $p(x)(q(x) + r(x)) = p(x)q(x) + p(x)r(x)$.

Escrevendo

$$\begin{aligned} &p(x)(q(x) + r(x)) = u_0 + u_1x + u_2x^2 + \cdots + \in, u_i = \sum_{j+t=i} a_j(b_t + c_t), \\ &p(x)q(x) = l_0 + l_1x + l_2x^2 + \cdots + \in, l_i = \sum_{j+t=i} a_jb_t \text{ e} \\ &p(x)r(x) = v_0 + v_1x + v_2x^2 + \cdots + \in, v_i = \sum_{j+t=i} a_jc_t, \end{aligned}$$

devemos mostrar que $u_i = l_i + v_i, \forall i \in \mathbb{N} \cup \{0\}$. Para $i \in \mathbb{N} \cup \{0\}$,

$$u_i = \sum_{j+t=i} a_j(b_t + c_t) = \sum_{j+t=i} (a_j b_t + a_j c_t) = \sum_{j+t=i} a_j b_t + \sum_{j+t=i} a_j c_t = l_i + v_i.$$

Como $A[x]$ satisfaz os 6 axiomas de anel, temos que $A[x]$ é um anel. □

(b) Dado dois polinômios $p(x) = a_0 + a_1x + \cdots + a_nx^n + \cdots$ e $q(x) = b_0 + b_1x + \cdots + b_nx^n$, sendo eles, dois elementos de $A[x]$, temos:

$$p(x)q(x) = l_0 + l_1x + \ldots + l_nx^n, \quad l_i = \sum_{j+t=i} a_j b_t$$

e

$$q(x)p(x) = w_0 + w_1x + \ldots + w_nx^n, \quad w_i = \sum_{j+t=i} b_j a_t,$$

Utilizando a hipótese de que o anel $A$ é comutativo, assim, para cada $i \in \mathbb{N} \cup \{0\}$,

$$l_i = \sum_{j+t=i} a_j b_t = \sum_{j+t=i} b_t a_j = w_i.$$

Portanto, $p(x)q(x) = q(x)p(x)$ para quaisquer polinômios de $A[x]$.

(c) Sejam 1 a unidade de $A$ o $g(x) = 1$ o polinômio constante igual a 1. Escrevendo $g(x) = b_0 + b_1x + b_2x^2 + \ldots + b_nx^n$, temos que $b_0 = 1$ e $b_t = 0$ para todo $t \geq 1$ e, para qualquer $p(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n \in A[x]$,

$$p(x)g(x) = c_0 + c_1x + c_2x^2 + \ldots + c_nx^n,$$

onde $c_i = \sum_{j+t=i} a_j b_t$, para todo $i \in \mathbb{N} \cup \{0\}$. A única possibilidade das parcelas do somatório $\sum_{j+t=i} a_j b_t$ serem não nulas é quando $t = 0$. Dessa forma, temos que:

$$c_i = \sum_{j+t=i} a_j b_t = \sum_{j+0=i} a_j b_0 = \sum_{j=i} a_j = a_i,$$

e consequentemente $p(x)g(x) = p(x)$. De forma análoga, podemos demonstrar que $g(x)p(x) = p(x)$. Portanto, concluímos que $g(x) = 1$ é a unidade do anel $A[x]$.

(d) Pelos itens anteriores e considerando que $A$ é um anel de integridade, concluímos que $A[x]$ é um anel comutativo e com unidade. Entretanto, ainda precisamos demonstrar que $A[x]$ é sem divisores de zero. Para isso, realizaremos uma prova por contradição. Suponhamos que existem polinômios $p(x)$ e $q(x) \in A[x]$, $p(x) \neq 0$, $q(x) \neq 0$, tais que $p(x)q(x) = 0$. Escrevemos

$$p(x) = a_0 + a_1x + a_2x^2 + \ldots \text{ e } q(x) = b_0 + b_1x + b_2x^2 + \ldots,$$

em que $\partial(p) = m$ e $\partial(q) = n$. Segue que $a_m \neq 0$ e $b_n \neq 0$, e como $A$ é um anel de integridade, temos que $a_m b_n \neq 0$. Por outro lado,

$$0 = p(x)q(x) = c_0 + c_1 x + c_2 x^2 + \cdots, \text{ em que } c_i = \sum_{j+t=i} a_j b_t.$$

Assim, $c_i = 0$ para todo $i$ e, em particular, $c_{n+m} = 0$. No entanto,

$$\begin{aligned} 0 = c_{n+m} &= \sum_{j+t=m+n} a_j b_t \\ &= a_0 b_{n+m} + a_1 b_{n+m-1} + \cdots + a_{m-1} b_{n+1} + a_m b_n + a_{m+1} b_{n-1} + \cdots + a_{n+m} b_0 \\ &= a_m b_n, \end{aligned}$$

pois $b_j = 0$, para $j > n$ e $a_j = 0$ para $j > m$. Isto contradiz o fato que $a_m b_n \neq 0$. Logo, $A[x]$ não possui divisores de zero.

Podemos nos questionar, se $\mathbb{K}$ é um corpo, então $\mathbb{K}[x]$ é um corpo? A resposta é não. De fato, o polinômio $q(x) = x$ não é inversível. Caso contrário, existiria um polinômio $p$, suponhamos de grau $n$, tal que $pq = 1$ é o polinômio constante. Provaremos no próximo capítulo, Proposição 4.1.4 (c), que $\partial(pq) = \partial(p) + \partial(q)$ e assim, teríamos que $0 = n + 1$, o que é um absurdo.

Apresentamos alguns exemplos de anéis e percebemos que nem todos têm a mesma estrutura algébrica. O anel dos inteiros $(\mathbb{Z}, +, \cdot)$ é um anel de integridade, assim como o anel dos inteiros de Gauss $(\mathbb{Z}[i], +, \cdot)$ e o anel dos polinômios com coeficiente num corpo $(\mathbb{K}[x], +, \cdot)$. Já os conjuntos numéricos $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ e o subconjunto dos números reais $(\mathbb{Q}[\sqrt{p}], +, \cdot)$ são corpos. Vimos também que o anel de matrizes pode ter unidade, mas é com divisores de zero e não comutativo. E um produto direto entre anéis pode ser anel comutativo e com unidade, mas possuem divisores de zero. Conceitos de divisibilidade não são abordados num contexto envolvendo matrizes, uma vez que um anel de matrizes não é um anel de integridade (possuem divisores de zero).

Gauss estendeu a ideia de número inteiro quando definiu o conjunto $\mathbb{Z}[i]$, pois descobriu que muito da antiga Teoria de Euclides sobre fatoração de inteiros poderia ser transportada para $\mathbb{Z}[i]$, com consequências importantes para a Teoria dos Números. Ele desenvolveu uma teoria de fatoração em primos para esses números complexos e demonstrou que essa decomposição em primos é única, assim como acontece com o conjunto dos números inteiros. No próximo capítulo, discutiremos o algoritmo da divisão e a fatoração em primos, com enfoque nos anéis dos inteiros e nos anéis dos polinômios, com o objetivo de investigar as similaridades desses anéis e de associar a Aritmética e a Álgebra do Ensino Básico.

Apesar dos anéis de inteiros $(\mathbb{Z}[i], +, \cdot)$ terem sido importantes para o desenvolvimento dessa teoria, não apresentaremos os resultados sobre este anel. Ao leitor interessado, indicamos o último capítulo do livro "Fundamentos de Aritmética" de Domingues (2017).

# 4 Domínios Euclidianos

Existem várias classes de anéis com "estrutura mais algébrica" do que anéis genéricos. Os considerados neste capítulo são anéis com algoritmo de divisão (Domínios Euclidianos), anéis nos quais todo ideal é principal (Domínios Principais) e anéis nos quais os elementos possuem fatoração em primos (Domínios de Fatoração Única). Os exemplos principais de tais anéis são o anel $\mathbb{Z}$ de números inteiros e anéis de polinômios $\mathbb{K}[x]$ com coeficientes em algum corpo $\mathbb{K}$. Com base nessas semelhanças, buscamos estabelecer conexões mais profundas entre a Aritmética e a Álgebra do Ensino Básico.

Em todo esse capítulo consideramos $(A, +, \cdot)$ um anel de integridade (domínio) e anéis de polinômios sobre um corpo $\mathbb{K}$. Para a elaboração desse capítulo, as principais referências utilizadas são Domingues e Iezzi (2003), Gonçalves (2017) e Dummit e Foote (2004).

## 4.1 Domínios Euclidianos

Apresentamos a definição de um tipo especial de anel de integridade. A inspiração é o algoritmo da divisão, que existe tanto em $\mathbb{Z}$ como em $\mathbb{R}[x]$ ou $\mathbb{C}[x]$.

**Definição 4.1.1.** Sejam $(A, +, \cdot)$ um anel de integridade e $d$ uma aplicação de $A - \{0\}$ em $\mathbb{N} \cup \{0\}$ que cumpre as seguintes condições:

(i) Se $a, b \in A - \{0\}$, então $d(ab) \geq d(a)$;

(ii) Se $a, b \in A$ e $b \neq 0$, então existem únicos $q, r \in A$ (o *quociente* e o *resto*, respectivamente) tais que $a = bq + r$, em que $r = 0$ ou $d(r) < d(b)$.

Neste caso, dizemos que $(A, +, \cdot)$ é um *Domínio Euclidiano*.

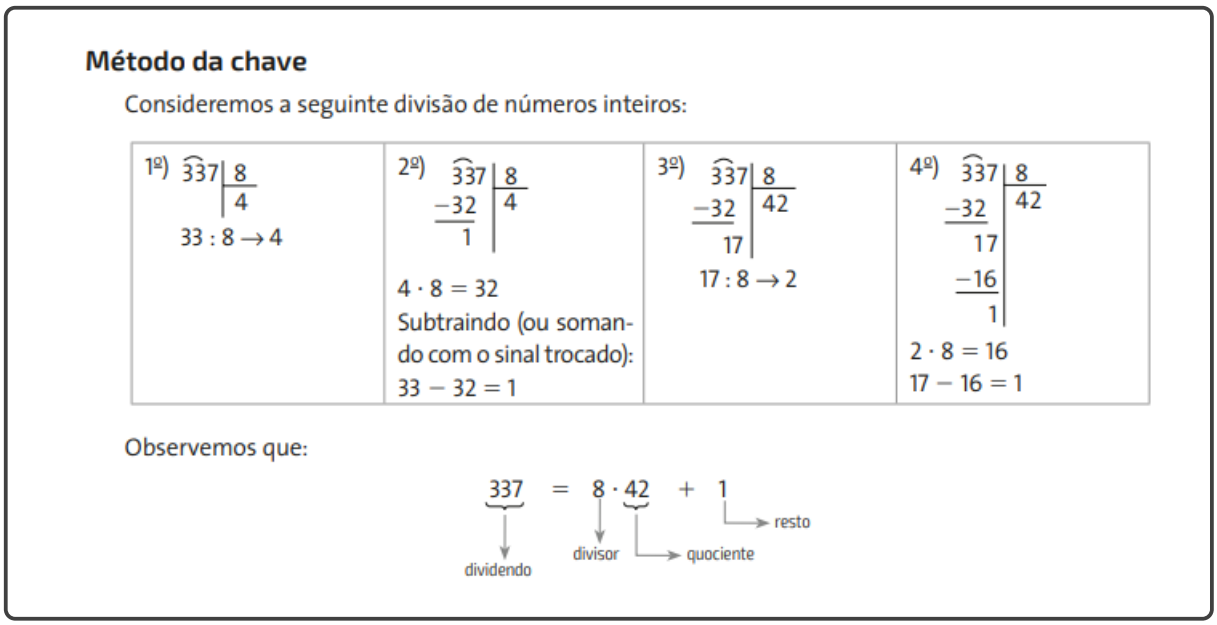
**Exemplo 4.1.2.** Corpos são exemplos triviais de Domínios Euclidianos em que qualquer aplicação $d : \mathbb{K} - \{0\} \to \mathbb{N} \cup \{0\}$ cumpre as condições. Por exemplo, defina $d(a) = 0$ para todo $a \in \mathbb{K}$. Daí, para qualquer $a, b$ com $b \neq 0$ temos

$$a = qb + 0, \text{ onde } q = ab^{-1} \text{ e } r = 0.$$

No anel dos números inteiros temos que a aplicação $d : \mathbb{Z} - \{0\} \to \mathbb{N}$ definida por $d(a) = |a|$ satisfaz a Definição 4.1.1. Facilmente vemos que a função módulo satisfaz a condição (i) e o item (ii) é demonstrado no Teorema 4.1.3.

Através da Figura 27, percebemos como a Divisão Euclidiana dos números é apresentada no Ensino Fundamental.

Figura 27 – Divisão Euclidiana nos Inteiros




Fonte: DANTE (2016b, p. 207)

**Teorema 4.1.3.** *Algoritmo da Divisão Euclidiana: Para quaisquer $a, b \in \mathbb{Z}$, com $b \neq 0$, existe um único par de números inteiros $q$ e $r$ tais que*

$$a = bq + r, \ \ com\ 0 \leq r < |b|.$$

*Demonstração.* Consideramos o conjunto

$$S = \{a - by \in \mathbb{N} \cup \{0\} \mid y \in \mathbb{Z}\}.$$

Pela propriedade Arquimediana, existe $n \in \mathbb{Z}$ de forma que $n(-b) > -a$, assim $a - nb > 0$ e percebemos que $S$ não é vazio. Pelo Princípio da Boa Ordenação (Veja Hefez (2016, p.10)), o conjunto $S$ admite um elemento mínimo, o qual denotamos por $r$. Assim, $r \geq 0$ e suponhamos que $r = a - bq$, para algum $q \in \mathbb{Z}$. Vamos provar que $r = |r| < |b|$ por contradição.

Suponhamos que $r \geq |b|$. Então, existe $s \in \mathbb{N} \cup \{0\}$ tal que $r = |b| + s$ e, consequentemente, $0 \leq s < r$. Entretanto, $s < r$ entra em contradição com a condição de minimalidade de $r$ em $S$, uma vez que

$$s = r - |b| = (a - bq) - |b| = a - bq \pm b = a - b(q \pm 1) \in S.$$

Portanto, existem $q, r \in \mathbb{Z}$ tais que $a = bq + r$ e $0 \leq r < |b|$.

Agora vamos provar a unicidade do quociente e resto. Para tanto, vamos supor que $a = bq + r = bq' + r'$, onde $q, q', r, r' \in \mathbb{Z}$ e $0 \leq r, r < |b|$. Dessa forma, temos que

$$-|b| < -r \leq r' - r \leq r' < |b|.$$

Portanto, $|r' - r| < |b|$. No entanto, $b(q - q') = r' - r$, o que resulta em

$$|b||q - q'| = |r' - r| < |b|,$$

o que só ocorre se $q - q' = 0$. Consequentemente, $q = q$'e $r = r'$. □

Sabemos que existe um algoritmo similar para a divisão de polinômios e, de fato, se trata da mesma ideia. Se $\mathbb{K}$ é um corpo, então o anel dos polinômios $\mathbb{K}[x]$ é um Domínio Euclidiano em que a aplicação da Definição 4.1.1 é a função "grau".

Observamos que o grau $\partial$ pode ser interpretado como uma aplicação do conjunto de todos os polinômios não nulos no conjunto $\mathbb{N} \cup \{0\}$. Assim,

$$\begin{aligned} \partial : \quad \mathbb{K}[x] - \{0\} &\to \mathbb{N} \cup \{0\} \\ p(x) &\mapsto \partial(p(x)) \end{aligned}$$

Antes de provar o algoritmo da divisão para os polinômios, precisamos de alguns resultados preliminares sobre o grau.

**Proposição 4.1.4.** *Sejam $\mathbb{K}$ um corpo e $p(x), q(x) \in \mathbb{K}[x]$ polinômios não nulos.*

*(a) Se $p(x) + q(x) \neq 0$, então $\partial(p(x) + q(x)) \leq \max\{\partial(p(x)), \partial(q(x))\}$.*

*(b) Se $\partial(p(x)) \neq \partial(q(x))$, então $p(x)+q(x) \neq 0$ e $\partial(p(x)+q(x)) = \max\{\partial(p(x)), \partial(q(x))\}$.*

*(c) Temos que $p(x)q(x) \neq 0$ e $\partial(p(x)q(x)) = \partial(p(x)) + \partial(q(x))$.*

*Demonstração.* Para todos os itens, vamos considerar $p(x) = a_0 + a_1x + \cdots + a_nx^n$, $q(x) = b_0 + b_1x + \cdots + b_mx^m$ com $\partial(p(x)) = n$ e $\partial(q(x)) = m$ e, assim, $a_n \neq 0 \neq b_m$.

(a) Sem perda de generalidade, assumimos que $n \geq m$. Temos que

$$0 \neq p(x) + q(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_m + b_m)x^m + \cdots + (a_n + b_n)x^n,$$

onde acrescentamos coeficientes $b_j = 0$ para j > m, se for necessário. Se $a_n + b_n \neq 0$, então $\partial(p(x) + q(x)) = n$, senão, $\partial(p(x) + q(x)) < n$.

Portanto, $\partial(p(x) + q(x)) \leq n = \max\{n, m\} = \max\{\partial(p(x)), \partial(q(x))\}$.

(b) Por hipótese, $\partial(p(x)) \neq \partial(q(x))$, então $n \neq m$. Vamos assumir que $n > m$. Então,

$$p(x) + q(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_m + b_m)x^m + a_{m+1}x^{m+1} + \cdots + a_nx^n.$$

Uma vez que $a_n \neq 0$, temos que $p(x) + q(x) \neq 0$ e, também

$$\partial(p(x) + q(x)) = n = \max\{n, m\} = \max\{\partial(p(x)), \partial(q(x))\}.$$

(c) Escrevendo $p(x)q(x) = c_0 + c_1x + c_2x^2 + \cdots$ temos que $c_k = \sum_{i+j=k} a_ib_j$. Quando $k > n+m$, cada uma das parcelas de somatório $c_k = \sum_{i+j=k} a_ib_j$ envolve $a_i$ com $i > n$ ou $b_j$ com $j > m$, portanto todas as parcelas são nulas, ou seja, $c_k = 0$ para todo $k > n+m$. Além disso, observamos que

$$c_{n+m} = a_0b_{n+m} + a_1b_{n+m-1} + \cdots + a_{n-1}b_{m+1} + a_nb_m + a_{m+1}b_{m-1} + \cdots + a_{n+m}b_0 = a_nb_m,$$

pois $a_i = 0$ para $i > n$ e $b_j = 0$ para $j > m$. Como $\mathbb{K}$ é corpo e $a_n \neq 0 \neq b_m$, temos que $c_{n+m} = a_nb_m \neq 0$. Portanto, $p(x)q(x) \neq 0$ e

$$\partial(p(x)q(x)) = n + m = \partial(p(x)) + \partial(q(x)).$$ □

Pelo item (4.1) da Proposição 4.1.4 temos que $\partial(p(x)q(x)) = \partial(p(x)) + \partial(q(x))$ o que mostra que $\partial(p(x)q(x)) \geq \partial(p(x))$ satisfazendo o item (i) da Definição 4.1.1. Após a Figura 28, provaremos a existência e unicidade do quociente e resto na divisão de dois polinômios.

Figura 28 – Divisão de Polinômios

| Sequência de passos | Exemplo |
|---|---|
| **1º)** Escreva os polinômios (dividendo e divisor) em ordem decrescente de seus expoentes e complete-os, quando necessário, com termos de coeficiente zero. | dividendo: $2x^3 + 4x^2 + 3x - 6$ \| divisor: $x^2 - x$ |
| **2º)** Divida o termo de maior grau do dividendo pelo de maior grau do divisor (o resultado será um termo do quociente). | $2x^3 + 4x^2 + 3x - 6$ \| $x^2 - x$ / $2x$ |
| **3º)** Multiplique o termo obtido no 2º passo pelo divisor e subtraia esse produto do dividendo. | $2x^3 + 4x^2 + 3x - 6$ \| $x^2 - x$ / $2x$ / $-2x^3 + 2x^2$ / $6x^2 + 3x - 6$ |
| **4º)** Se o grau da diferença for menor do que o grau do divisor, a diferença será o resto da divisão, e a divisão terminará aqui. Caso contrário, repita o 2º passo, considerando a diferença como um novo dividendo, até que o grau da diferença seja menor do que o grau do divisor ou até que a diferença seja igual a zero (polinômio nulo). | $2x^3 + 4x^2 + 3x - 6$ \| $x^2 - x$ / $2x + 6$ (quociente) / $-2x^3 + 2x^2$ / $6x^2 + 3x - 6$ / $-6x^2 + 6x$ / $9x - 6$ (resto) |

Portanto, no exemplo dado, $A(x) = 2x^3 + 4x^2 + 3x - 6$, $B(x) = x^2 - x$, $Q(x) = 2x + 6$ e $R(x) = 9x - 6$. Além disso, $2x^3 + 4x^2 + 3x - 6 = (x^2 - x) \cdot (2x + 6) + (9x - 6)$ e o grau do resto é 1, menor do que o grau do divisor, que é 2.

Fonte: BONJORNO; GIOVANNI; SOUSA (2016, p.205)

**Teorema 4.1.5.** *Seja $\mathbb{K}$ um corpo. Dados dois polinômios $f, g \in \mathbb{K}[x]$, com $g \neq 0$, existem polinômios $q$ e $r$ tais que $f = gq + r$, em que $r = 0$ ou $\partial(r) < \partial(g)$. Ademais, é único o par de polinômios $(q, r)$ que cumpre as condições da proposição.*

*Demonstração.* Vamos analisar em casos.

- $f = 0$ é o polinômio nulo: Neste caso basta tomar $q = r = 0$, pois $0 = g \cdot 0 + 0$.
- $f$ não é o polinômio nulo e $\partial(f) < \partial(g)$: Para essa situação, tomamos $q = 0$ como o polinômio nulo e $r = f$ em virtude de $f = g \cdot 0 + f$ e, por hipótese, $\partial(f) < \partial(g)$.
- $f$ não é o polinômio nulo e $\partial(f) \geq \partial(g)$: Sejam $f(x) = a_0 + a_1x + \cdots + a_nx^n$ e $g(x) = b_0 + b_1x + \cdots + b_mx^m$, com $\partial(g) = m$.

  Vamos demonstrar usando o Princípio de Indução Completa (Veja Morgado e Carvalho (2014, p.29).) sobre $\partial(f) = n$.

  Se $\partial(f) = 0$, então $\partial(g) = 0$. Nessa situação, $f$ e $g$ são polinômios constantes não nulos: $f(x) = a_0$ e $g(x) = b_0$, sendo $b_0$ inversível, por suposição. A divisão é bem definida em $\mathbb{K}$, sendo possível e exata: o quociente é $q(x) = b_0^{-1}a_0$ e o resto $r(x) = 0$. Com efeito, $a_0 = b_0(b_0^{-1}a_0) + 0$, ou seja, $f = gq + r$.

  Suponhamos que o teorema seja verdadeiro para todo polinômio de grau menor do que $n$.

  Consideramos o polinômio $f_1$ definido da seguinte forma:

$$f_1(x) = f(x) - a_nb_m^{-1}x^{n-m}g(x). \tag{4.1}$$

  Se $f_1 = 0$ ou $\partial(f_1) < \partial(g)$, então $q = a_nb_m^{-1}x^{n-m}$ e $r = f_1$. (Para chegar nesse resultado, basta isolar $f$ no primeiro membro.)

  Caso contrário, temos $\partial(f_1) \geq \partial(g)$ e $\partial(f_1) < n$, pois o coeficiente dominante de $f$ é igual ao do polinômio expresso por $a_nb_m^{-1}x^{n-m}g(x)$. Devido a hipótese de indução, existem polinômios $q_1$ e $r_1$ tais que:

$$f_1(x) = g(x)q_1(x) + r_1(x), \tag{4.2}$$

  com $r_1 = 0$ ou $\partial(r_1) < \partial(g)$.

  De (4.1) e (4.2) segue que

$$f(x) - a_nb_m^{-1}x^{n-m}g(x) = g(x)q_1(x) + r_1(x)$$

  e, assim,

$$f(x) = a_nb_m^{-1}x^{n-m}g(x) + g(x)q_1(x) + r_1(x)$$

  ou

$$f(x) = [a_nb_m^{-1}x^{n-m} + q_1(x)]g(x) + r_1(x).$$

  em que $r_1 = 0$ ou $\partial(r1) < \partial(g)$. Isso demonstra a existência do resto e do quociente na divisão de $f$ por $g$.

Falta provar a unicidade do quociente e do resto. Consideramos que é possível expressar $f = gq + r = gq_1 + r_1$, onde $\partial(r) < \partial(g)$, se $r \neq 0$, e $\partial(r_1) < \partial(g)$, se $r_1 \neq 0$. A partir dessas igualdades, podemos escrever

$$g(q - q_1) = r_1 - r.$$

Suponhamos que $r_1 - r \neq 0$ e, consequentemente, $q - q_1 \neq 0$. Desse modo podemos falar do grau de $r_1 - r$ e do $q - q_1$. Temos que $\partial(r_1 - r) = \partial(g(q - q_1)) = \partial(g) + \partial(q - q_1)$, o que implica que, $\partial(r_1 - r) \geq \partial(g)$. Por outro lado, $\partial(r_1 - r) \leq \max\{\partial(r_1), \partial(r)\} < \partial(g)$, o que resulta em uma contradição. Logo, $r_1 - r = 0$ e como $\mathbb{K}[x]$ é um anel de integridade e $g \neq 0$, segue que $q_1 - q = 0$. Portanto, $r_1 = r$ e $q_1 = q$. □

## 4.2 Domínios Principais

Nesta seção, exploraremos os Domínios Principais, uma classe especial de anéis com propriedades fundamentais e interessantes. Para isso, abordaremos o conceito de ideais em um anel de integridade, incluindo ideais gerados, que são tópicos não abordados no Ensino Básico. Por outro lado, em um Domínio Principal, veremos que o máximo divisor comum entre dois elementos sempre existe. Além disso, Domínios Principais são uma classe importante de anéis que possuem propriedades fundamentais de fatoração única e se assemelham aos inteiros em muitos aspectos, conforme discutiremos na Seção 4.3.

**Definição 4.2.1.** Sejam $(A, +, \cdot)$ um anel de integridade e $I$ um subconjunto não vazio de $A$. Dizemos que $I$ é um *ideal* de $A$ se satisfizer as seguintes propriedades:

(i) se $x, y, \in I$, então $x - y \in I$ e,

(ii) se $a \in A, x \in I$, então $ax \in I$.

**Exemplo 4.2.2.** Se $n$ é um número inteiro qualquer, então o conjunto de todos os múltiplos inteiros de $n$ é um ideal de $\mathbb{Z}$. De fato, seja $n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\}$ o conjunto dos múltiplos de $n$. Então,

- $0 = n \cdot 0 \in n\mathbb{Z}$ e $n\mathbb{Z} \neq \varnothing$;
- Se $x = ns$, $y = nt \in n\mathbb{Z}$, então $x - y = ns - nt = n(s - t) \in n\mathbb{Z}$;
- Se $a \in \mathbb{Z}$ e $x = nt \ \in n\mathbb{Z}$, então $kx = k(nt) = n(kt) \in n\mathbb{Z}$.

No Exemplo 4.2.2, se $n = 0$ temos que $n\mathbb{Z} = 0\mathbb{Z} = \{0\}$ é um ideal de $\mathbb{Z}$. Se $n = 5$, então $n\mathbb{Z} = 5\mathbb{Z}$ também é um ideal de $\mathbb{Z}$.

**Exemplo 4.2.3.** O subconjunto $I$ de todos os polinômios de $\mathbb{C}[x]$ com valor numérico 0 em $x = 0$, isto é, $I = \{p(x) \in \mathbb{C}[x] \mid p(0) = 0\}$, é um ideal de $\mathbb{C}[x]$. De fato,

- $I$ não é um conjunto vazio, pois o polinômio $p(x) = x$ pertence a $I$;
- Se $p, q \in I$, então $(p+q)(0) = p(0) + q(0) = 0$, o que mostra que $p + q \in I$;
- Se $p \in I$ e $a \in \mathbb{C}[x]$, então $(ap)(0) = a(0)p(0) = a(0) \cdot 0 = 0$, logo $ap \in I$.

**Definição 4.2.4.** Sejam $(A, +, \cdot)$ um anel de integridade e $B$ um subconjunto não vazio de $A$. Dizemos que $B$ é um *subanel* de $A$ se satisfizer as seguintes propriedades:

(i) se $x, y, \in B$, então $x + y \in B$ e $xy \in B$;

(ii) $(B, +, \cdot)$ é também é um anel.

A definição de subanel abrange um subconjunto não vazio de um anel que, por sua vez, é também um anel. Um exemplo clássico é o conjunto dos números inteiros $\mathbb{Z}$, que se configura como um subconjunto não vazio do anel dos números racionais $\mathbb{Q}$ e, que também é um anel contido em $\mathbb{Q}$, o que o classifica como um subanel de $\mathbb{Q}$.

Prova-se que qualquer ideal de um anel é, também, um subanel desse anel, ou seja, todo ideal é um anel. No entanto, nem todo subanel de um anel é um ideal desse anel, por exemplo, $\mathbb{Z}$ não é um ideal de $\mathbb{Q}$ uma vez que $3 \in \mathbb{Z}$ e $\frac{1}{2} \in \mathbb{Q}$, mas $\frac{1}{2} \cdot 3 \notin \mathbb{Z}$. Para uma compreensão mais aprofundada, veja Janesh e Taneja (2008).

**Proposição 4.2.5.** *Sejam $(A, +, \cdot)$ um anel de integridade e $x_1, x_2, \cdots, x_n \in A$. Então, o conjunto*

$$x_1A + \cdots + x_nA = \{x_1a_1 + \cdots + x_na_n \ \in A \mid a_i \in A, \ \forall i = 1, \cdots, n\}$$

*é um ideal de $A$.*

*Demonstração.*

- Como $0 = x_1 \cdot 0 + \cdots + x_n \cdot 0 \in x_1A + \cdots + x_nA$, segue que $x_1A + \cdots + x_nA \neq \varnothing$.
- Se $b = x_1b_1 + \cdots + x_nb_n, \ c = x_1c_1 + \cdots + x_nc_n \in x_1A + \cdots + x_nA$, então

  $$b - c = x_1(b_1 - c_1) + x_2(b_2 - c_2) + \cdots + x_n(b_n - c_n) \in x_1A + \cdots + x_nA,$$

  pois cada um dos $b_i - c_i$ pertencem à $A$.
- Se $a \in A$ e $b = x_1b_1 + \cdots + x_nb_n \in x_1A + \cdots + x_nA$, então

  $$ab = x_1(ab_1) + \cdots + x_n(ab_n) \in x_1A + \cdots + x_nA,$$

  pois cada um dos $ab_i$ pertencem à $A$.

Portanto, $Ax_1 + \cdots + Ax_n$ é um ideal de $A$. □

**Definição 4.2.6.** Sejam $(A, +, \cdot)$ um anel de integridade e $x_1, x_2, \cdots, x_n \in A$. O ideal $Ax_1 + \cdots + Ax_n$ é chamado *ideal de $A$ gerado por $x_1, x_2, \ldots, x_n$*.

**Exemplo 4.2.7.** Em $\mathbb{Z}$, temos que o ideal gerado por 4 e 6 é o conjunto

$$4\mathbb{Z} + 6\mathbb{Z} = \{4x + 6y \mid x, y \in \mathbb{Z}\}.$$

Temos que $4\mathbb{Z}+6\mathbb{Z} = 2\mathbb{Z}$. De fato, para quaisquer $x, y \in \mathbb{Z}$ temos que $4x+6y = 2(2x+3y) \in 2\mathbb{Z}$, logo, $4\mathbb{Z} + 6\mathbb{Z} \subseteq 2\mathbb{Z}$. Por outro lado, temos que $2 = \text{mdc}(4, 6)$ e, pela Identidade de Bezout, existem $x, y \in \mathbb{Z}$ tais que $2 = 4x + 6y$, assim, $2k = 4(xk) + 6(yk) \in 4\mathbb{Z} + 6\mathbb{Z}$ e $2\mathbb{Z} \subseteq 4\mathbb{Z} + 6\mathbb{Z}$.

**Definição 4.2.8.** Sejam $(A, +, \cdot)$ um anel de integridade e $x \in A$. O ideal $Ax$ é chamado de *ideal principal de $A$ gerado por $x$*.

Observamos que se $(A, +, \cdot)$ é um anel de integridade e $u \in A$ é inversível, então $uA = A$. Com efeito, por definição de ideal gerado temos que $uA \subseteq A$. Para qualquer $a \in A$ temos

$$a = 1a = (uu^{-1})a = u(u^{-1}a) \in uA,$$

logo, $A \subseteq uA$.

**Exemplo 4.2.9.** Seja $\mathbb{K}$ um corpo e $I$ um ideal de $\mathbb{K}$. Se $I$ é um ideal não nulo $I \neq \{0\}$, então existe $x \in I$ com $x \neq 0$. Como todo elemento diferente de zero num corpo é inversível, temos que $u\mathbb{K} = \mathbb{K}$. E como $u\mathbb{K} \subseteq I$ segue que $I = \mathbb{K}$. Logo, os únicos ideais de $\mathbb{K}$ são $\{0\}$ ou $\mathbb{K}$. Além disso, esses ideais são principais, gerados por 0 e 1, respectivamente.

**Definição 4.2.10.** Um anel de integridade $(A, +, \cdot)$ é dito *Domínio Principal* quando todos os seus ideais são principais. Ou seja, se $I$ é um ideal em um Domínio Principal, então existe $x \in A$ tal que $I = Ax$.

**Exemplo 4.2.11.** Pelo Exemplo 4.2.9 temos que todo corpo é um Domínio Principal.

**Proposição 4.2.12.** *Todo Domínio Euclidiano é um Domínio Principal.*

*Demonstração.* Seja $(A, +, \cdot)$ um Domínio Euclidiano e seja $I$ um ideal de $A$. Se $I = \{0\}$, então $I = 0 \cdot A$ é um ideal principal. Suponhamos que $I \neq \{0\}$. Seja $d : A - \{0\} \to \mathbb{N} \cup \{0\}$ a aplicação da Definição 4.1.1. Como o conjunto

$$S = \{d(a) \in \mathbb{N} \mid a \in I \text{ e } a \neq 0\}$$

não é vazio, logo, pelo Princípio da Boa Ordenação, $S$ tem um elemento mínimo. Denotamo-no por $d(b)$, com $b \in I$, esse elemento. Pela Definição 4.2.1, $bA = \{ba \mid a \in A\} \subseteq I$. Seja $x$ um elemento qualquer de $I$. Pela hipótese, existem elementos $q$ e $r$ em $A$ tais que

$$x = qb + r, \text{ em que } d(r) < d(b) \text{ se } r \neq 0.$$

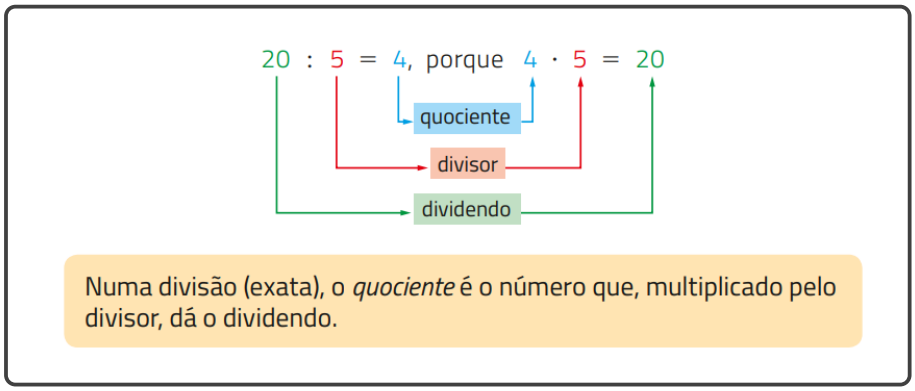
Uma vez que $x, b \in I$, segue que $r = x - qb \in I$. Pela minimalidade de $d(b)$ em $S$, a alternativa $r \neq 0$ não pode ocorrer, caso contrário $0 \leq d(r) < d(b)$. Portanto, $x - bq = 0$ e, consequentemente, $x = bq \in bA$, provando que $I \subseteq bA$. Das inclusões $bA \subseteq I$ e $I \subseteq bA$ concluímos que $I = bA$ é um ideal principal. □

**Exemplo 4.2.13.** Segue da proposição anterior e do Teorema 4.1.3 que $\mathbb{Z}$ é um Domínio Principal. Portanto, todo ideal de $\mathbb{Z}$ é da forma $n\mathbb{Z}$ para algum $n$ inteiro.

**Exemplo 4.2.14.** Pela proposição imediatamente acima e pelo Teorema 4.1.5, o anel $\mathbb{K}[x]$ é um Domínio Principal. Podemos ver que o ideal do Exemplo 4.2.3 é gerado pelo polinômio $p(x) = x$.

Vamos estender para um anel de integridade qualquer $(A, +, \cdot)$ a relação definida por "$x$ divide $y$", que já foi estudada no anel $\mathbb{Z}$ dos inteiros na disciplina M14 - Aritmética do PROFMAT, assim como no Ensino Básico. Na figura 29, podemos observar a divisão dos inteiros nos anos finais do Ensino Fundamental.

Figura 29 – Divisão nos Inteiros




Fonte: IEZZI; DOLCE; MACHADO (2018b, p.60)

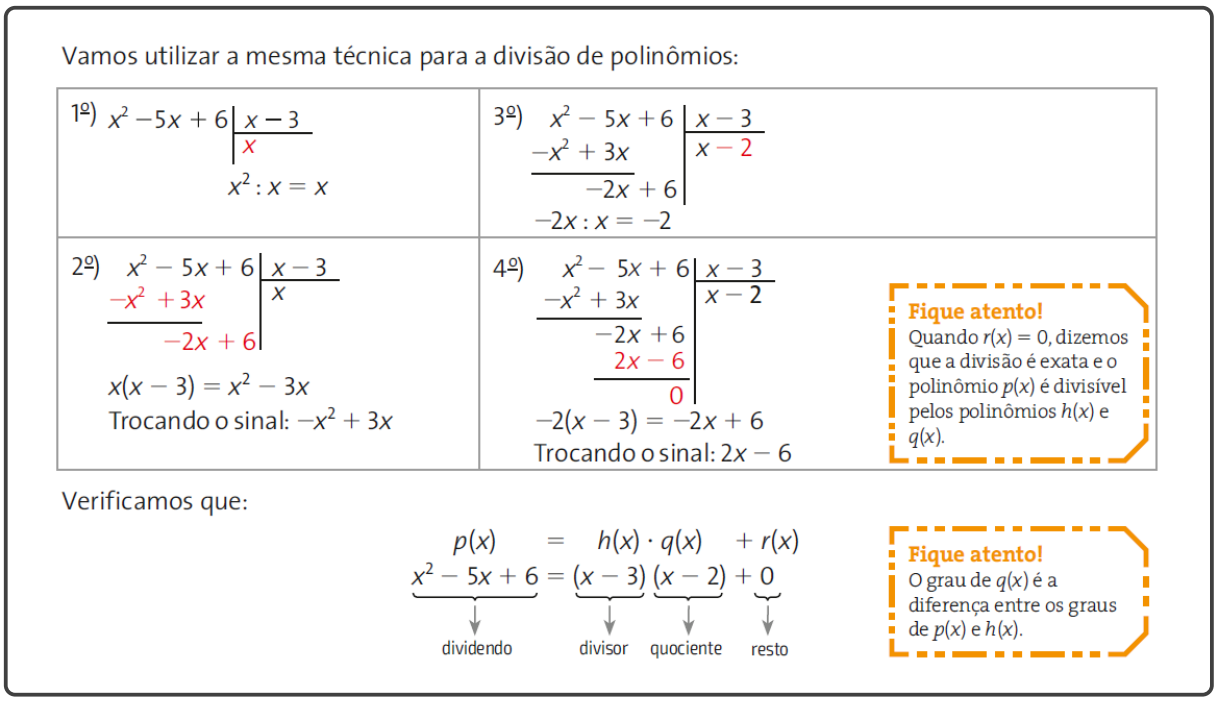
**Definição 4.2.15.** Sejam $(A, +, \cdot)$ um anel de integridade e $a, b \in A$ com $b \neq 0$. Dizemos que $a$ é um múltiplo de $b$ se existe um elemento $c \in A$ tal que $a = bc$. Neste caso, dizemos que $b$ *divide* $a$ ou é um *divisor* de $a$. Denotamos essa relação por $b \mid a$.

Por exemplo, em $\mathbb{Z}$, 6 divide 24, pois $24 = 6 \cdot 4$. Em $\mathbb{R}[x]$, o polinômio $p(x) = x - 1$ divide $q(x) = x^3 - 1$ uma vez que $x^3 - 1 = (x - 1)(x^2 + x + 1)$.

**Observação 4.2.16.** Observamos que, dados $a, b \in A$ com $b \neq 0$, temos que $b$ divide $a$ se, e somente se, na divisão euclidiana de $a$ por $b$ o resto é 0.

A Figura 30 ilustra como a divisão de polinômios é ensinada no nível básico de ensino, servindo como um exemplo representativo.

Figura 30 – Divisão de polinômios




Fonte: DANTE (2016b, p. 208)

A partir da Definição 4.2.15 podemos definir também o conceito de máximo divisor comum em um anel de integridade $(A, +, \cdot)$.

**Definição 4.2.17.** Seja $(A, +, \cdot)$ um anel de integridade. Dizemos que um elemento $d \in A$ é máximo *máximo divisor comum* dos elementos $a, b \in A$ se:

(i) $d \mid a$ e $d \mid b$;

(ii) todo divisor de $a$ e $b$ é também divisor de $d$ (ou seja, se $c \in A$ em que $c \mid a$ e $c \mid b$, então $c \mid d$).

**Exemplo 4.2.18.** De acordo com a definição acima, temos que 2 é um máximo divisor comum de 4 e 6. De fato, 2 divide 4 e 6, satisfazendo (i). Os divisores comuns de 4 e 6 são: $-2, -1, 1, 1$ e todos esses números dividem 2, satisfazendo o item (ii).

**Exemplo 4.2.19.** O polinômio $p(x) = 2x+2$ é um máximo divisor comum dos polinômios $m(x) = x^2 - 1$ e $n(x) = 2x^2 + 4x + 2$ em $\mathbb{R}[x]$:

- Temos $m(x) = x^2 - 1 = (x - 1)(x + 1) = \frac{1}{2}(x - 1)(2x + 2) = \frac{1}{2}(x - 1)p(x)$ e $n(x) = 2x^2 + 4x + 2 = 2(x + 1)(x + 1) = 2(x + 1)p(x)$, o que mostra que $p \mid m, n$.

- Temos que os divisores comuns de $m$ e $n$ são da forma $c(x) = u$ ou $c(x) = u(x+1)$ em que $u \in \mathbb{R}^*$. Notamos que todos esses polinômios dividem o polinômio $p$, resultando nos quocientes da forma $q(x) = \frac{2}{u}(x+1)$ ou $q(x) = \dfrac{2}{u}$, respectivamente.

**Definição 4.2.20.** Sejam $a$ e $b$ elementos de A. Dizemos que $a$ é *associado* a $b$ se $a \mid b$ e $b \mid a$. Essa relação em $A$ será indicada por $a \sim b$.

**Exemplo 4.2.21.** Por exemplo, em $\mathbb{Z}$, os números 2 e $-2$ são associados, pois $2 \mid -2$ e $-2 \mid 2$. Em $\mathbb{C}[x]$, consideramos os polinômios $p(x) = 3x^2 - 15x + 18$ e $q(x) = 2x^2 - 10x + 12$. Verificaremos que esses polinômios são associados. Podemos observar que $p(x) = \frac{2}{3}q(x)$, o que significa que $q(x)$ divide $p(x)$, sendo o quociente o polinômio constante $r(x) = \frac{2}{3}$. Da mesma forma, temos que $q(x) = \frac{3}{2}p(x)$, ou sejam $p(x)$ também divide $q(x)$ cujo quociente é $s(x) = \frac{3}{2}$.

**Proposição 4.2.22.** *Seja $d$ um máximo divisor comum de $a, b \in A$. Temos que $d'$ é um máximo divisor comum $a, b$ se, e somente se, $d \sim d'$.*

*Demonstração.* Suponha que $d$ e $d'$ sejam dois máximos divisores comuns de $a$ e $b$. Pelo item (i) da Definição 4.2.17, temos que $d$ e $d'$ são divisores de $a$ e $b$ e, portanto, pelo item $(ii)$ da Definição 4.2.17, segue que $d \mid d'$ e $d' \mid d$, isto é, $d \sim d'$.

Reciprocamente, suponha que $d$ seja um máximo divisor comum de $a$ e $b$ e que $d \mid d'$ e $d' \mid d$. Como $d \mid a, b$ e $d' \mid d$, pela transitividade da divisão, $d' \mid a, b$, mostrando que $d'$ satisfaz a condição (i) da Definição 4.2.17. Pelo item (ii) da Definição 4.2.17, se $c \in A$ é um divisor comum de $a$ e $b$, então $c \mid d$ e como $d \mid d'$, pela transitividade da divisão, $c \mid d'$. Logo, $d'$ também satisfaz a condição (ii) da Definição 4.2.17 e, portanto, $d'$ é uma máximo divisor comum $a$ e $b$. □

Como exemplo, podemos considerar o conjunto dos números inteiros $\mathbb{Z}$. Temos que 2 e -2 são máximos divisores comuns de 4 e 6. De fato, ao aplicarmos a Definição 4.2.17, verificamos que ambos satisfazem as duas condições considerando $a = 4$ e $b = 6$. Observamos que essa definição é uma generalização da definição vista na disciplina de Aritmética (HEFEZ, 2016, p. 74). A definição de máximo divisor comum em $\mathbb{Z}$ apresentada nesta bibliografia e em outros livros de Aritmética do Ensino Superior possui um item adicional em comparação à Definição 4.2.17, que exige que o máximo divisor comum seja maior ou igual a 0, garantindo assim a unicidade do máximo divisor comum em $\mathbb{Z}$. No entanto, neste contexto, não há tal unicidade, apenas a constatação de que os máximos divisores comuns são associados.

A seguinte proposição mostra que em um domínio principal $A$, quaisquer dois elementos possuem um máximo divisor comum.

**Proposição 4.2.23.** *Seja $(A, +, \cdot)$ um Domínio Principal. Dados dois elementos $a, b \in A$, existe um elemento $d$ que é máximo divisor comum de $a, b$.*

*Demonstração.* Seja $A$ um Domínio Principal e consideramos $a, b \in A$. Seja $aA + bA = \{ax + by \mid x, y \in A\}$ o ideal gerado por $a$ e $b$. Por hipótese, $aA + bA$ é um ideal principal e, assim, existe um elemento $d \in A$ tal que $aA + bA = dA$. Vamos mostrar que $d$ é um máximo divisor comum de $a, b$.

(i) Temos que $a = a \cdot 1 + b \cdot 0 \in aA + bA = dA$. Logo, existem $x \in A$ tal que $a = dx$, ou seja, $d \mid a$. Analogamente, $d \mid b$.

(ii) Seja $c$ um divisor comum de $a$ e $b$. Então, existem $x, y \in A$ tais que $a = cx$ e $b = cy$. Por outro lado, $d = d \cdot 1 \in dA = aA + bA$ e, assim, existem $n, m \in A$ tais que $d = an + bm$. Substituindo $a = cx$ e $b = cy$ em $d = an + bm$ obtemos $d = c(xn + ym)$, o que mostra que $c \mid d$. □

## 4.3 Domínio Fatorial

No caso dos inteiros $\mathbb{Z}$, existe um método adicional para determinar o máximo divisor comum de dois elementos $a$ e $b$, conhecido da aritmética elementar. Esse método utiliza a noção de fatoração em primos para $a$ e $b$, a partir da qual o máximo divisor comum pode ser facilmente determinado. Essa abordagem semelhante também é aplicada para determinar o máximo divisor comum entre polinômios, onde fatoramos os polinômios em produtos de polinômios irredutíveis. Esse conceito pode ser estendido para uma classe mais ampla de anéis, chamada Domínios de Fatoração Única, que serão definidos em breve. Para tal objetivo, precisamos de alguns conceitos preliminares.

**Definição 4.3.1.** Seja $(A, +, \cdot)$ um anel de integridade. Um elemento $p \in A$ se diz *primo* se:

(i) $p \neq 0$;

(ii) $p$ não é inversível;

(iii) quaisquer que sejam $a, b \in A$, se $p \mid ab$, então $p \mid a$ ou $p \mid b$.

De acordo com Hefez (2016), um número inteiro primo é definido da mesma forma que no Ensino Básico: Dizemos que $p \in \mathbb{Z}$ é primo se possui apenas dois divisores naturais, que são 1 e ele próprio. A Proposição 7.1 em Hefez (2016, p. 122), afirma que a definição usual de um número inteiro primo é equivalente à Definição 4.3.1. Essa proposição estabelece a correspondência entre ambas as definições em $\mathbb{Z}$.

Na realidade, no Ensino Básico, o conceito de número primo e demais tópicos associados, normalmente, são desenvolvidos no conjunto dos números naturais, como vemos na Figura 31.

Figura 31 – Números naturais primos e compostos

Um número natural e maior que 1 é *primo* quando só é divisível por 1 e por ele mesmo.

Um número natural e maior que 1 é *composto* quando é divisível por mais de dois números naturais.

Fonte: IEZZI; DOLCE; DEGENSZAJN; PERIGO; ALMEIDA (2016a, p. 147)

No Ensino Básico, após a noção de número primo, vem o conceito de número composto, como ilustrado na Figura 31. Mais adiante, definiremos o conceito de número composto em um Anel de Integridade de um modo um pouco diferente.

Os números primos ocupam uma posição de importância na resolução de inúmeros problemas relacionados a números naturais, e um dos principais motivos é que qualquer número natural pode ser decomposto como produto de números primos. Veja Figura 32.

Figura 32 – Fatoração em primos

**Decomposição em fatores primos**

Todo número natural composto pode ser decomposto em um produto de dois ou mais fatores diferentes de 1.

Veja, por exemplo, 36 decomposto em um produto de dois fatores diferentes de 1:

$$\overbrace{2 \times 18}^{36} \quad \text{ou} \quad \overbrace{4 \times 9}^{36} \quad \text{ou} \quad \overbrace{6 \times 6}^{36}$$

Vamos prosseguir, decompondo os fatores que são números compostos também em um produto de dois fatores, até que fiquem somente fatores primos:

$$\overbrace{2 \times \overbrace{2 \times 9}^{18}}^{36} = \overbrace{2 \times \overbrace{2 \times \overbrace{3 \times 3}^{9}}^{18}}^{36} = \underbrace{2}_{2^2} \times \underbrace{2}_{2^2} \times \underbrace{3 \times 3}_{3^2} = 2^2 \times 3^2$$

ou

$$\overbrace{\overbrace{4}^{2 \times 2} \times \overbrace{9}^{3 \times 3}}^{36} = \underbrace{2 \times 2}_{2^2} \times \underbrace{3 \times 3}_{3^2} = 2^2 \times 3^2$$

ou

$$\overbrace{\overbrace{6}^{2 \times 3} \times \overbrace{6}^{2 \times 3}}^{36} = 2 \times 3 \times 2 \times 3 = 2^2 \times 3^2$$

Quando um número está decomposto em um produto em que todos os fatores são números primos, dizemos que esse número está **decomposto em fatores primos**.

Portanto, o produto $2^2 \times 3^2$ é a decomposição em fatores primos do número 36.

Fonte: BIANCHINI (2015, p. 107)

Devido à sua relevância para a Aritmética, essa decomposição para os números inteiros é conhecida como o Teorema Fundamental da Aritmética:

**Teorema 4.3.2.** (Teorema Fundamental da Aritmética) *Para todo número inteiro* $n \neq 0, -1, 1$ *existem números primos* $p_1 < p_2 < \cdots < p_s$ $(s \geq 1)$ *tais que*

$$n = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$$

*com* $a_i > 0$ *para todo* $i \in \{1, 2, \ldots, s\}$ *Essa decomposição em fatores primos é única e é chamada de* decomposição canônica.

A demonstração desse teorema pode ser encontrada no livro "Aritmética" de Hefez (2016, p.123). Neste capítulo, mais adiante, iremos demonstrar a validade desse teorema utilizando a teoria desenvolvida aqui. Para isso, vamos generalizar essa noção de fatoração para um anel de integridade, onde tal fatoração será feita em fatores irredutíveis em vez de fatores primos.

**Definição 4.3.3.** Seja $(A, +, \cdot)$ um anel de integridade. Um elemento $p \in A$ se diz *irredutível* se:

(i) $p \neq 0$;

(ii) $p$ não é inversível;

(iii) quaisquer que sejam $a, b \in A$, se $p = ab$, então $a$ é inversível ou $b$ é inversível.

Em relação aos elementos de um anel de integridade, aqueles que não são nulos, inversíveis e nem irredutíveis são denominados *compostos*. Em outras palavras, um elemento é considerado composto se for possível fatorá-lo em dois ou mais elementos não inversíveis.

Para verificar se um polinômio em $\mathbb{K}[x]$ é irredutível ($\mathbb{K}$ corpo), primeiro precisamos discutir quais polinômios são inversíveis. Os polinômios inversíveis em $\mathbb{K}[x]$ são exclusivamente os polinômios constantes. É fácil ver que qualquer polinômio constante é inversível, pois para qualquer $a \in \mathbb{K}^*$ temos que o polinômio $p(x) = a^{-1}$ é o inverso de $q(x) = a$. Por outro lado, se $q$ é um polinômio inversível, então existe um polinômio $p$ tal que $pq = 1$. Logo, $\partial(p) + \partial(q) = 0$ e isso só é possível se $\partial(p) = \partial(q) = 0$. Portanto, $q$ é um polinômio constante.

**Exemplo 4.3.4.** Seja $\mathbb{K}$ um corpo.

(a) Se $p \in \mathbb{K}[x]$ é um polinômio constante, então $p$ é inversível e, portanto, não é irredutível nem composto em $\mathbb{K}[x]$ .

(b) Se $\partial(p) = 1$, então $p$ é irredutível em $K$. De fato, se $p = fg$, então o grau de $p$ é igual a soma do grau de $f$ e $g$. Isso só é possível se o grau de $f$ é 1 e o grau de $g$ é 0, ou vice-versa, então $f$ ou $g$ é um polinômio constante e, portanto, inversível.

**Exemplo 4.3.5.** Em $\mathbb{K}[x]$, o polinômio $p(x) = x$ é primo. De fato, $p$ não é nulo e nem inversível. Se $p \mid fg$, então o termo independente de $fg$ é 0, e isso só é possível se $f$ ou $g$ possui termo independente igual a 0, logo, $p$ dividirá tal polinômio.

Será que todo elemento primo em um anel de integridade é irredutível e vice-versa? A seguinte proposição mostra que uma das direções é válida em qualquer anel de integridade.

**Proposição 4.3.6.** *Todo elemento primo de um anel de integridade $(A, +, \cdot)$ é também irredutível.*

*Demonstração.* Considerando $a, b \in A$ tais que $p = ab$, podemos afirmar que $p \mid ab$ uma vez que $p \mid p$. Assim, pela definição de elemento primo, verificamos que $p \mid a$ ou $p \mid b$. No caso em que $p \mid a$, existe um elemento $c \in A$ tal que $a = pc$. Substituindo $a = pc$ na igualdade $p = ab$, obtemos $p = pcb$. Como $p \neq 0$ e num anel de integridade vale a lei do cancelamento, isso nos leva a $1 = cb$ e, consequentemente, percebemos que $b$ é um elemento inversível em $A$. Analogamente, se $p \mid b$, teríamos que $a$ é um elemento inversível em $A$. Em ambos, temos que $p$ é irredutível □

Não é verdade em geral que um elemento irredutível seja necessariamente primo. Um dos contraexemplos é no anel de inteiros quadrático $\mathbb{Z}[\sqrt{-5}] = \{a+b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$. Prova-se que o elemento $3 \in \mathbb{Z}[\sqrt{-5}]$ é irredutível, mas 3 não é primo. Para mais detalhes veja Dummit e Foote (2004, Capítulo 8). No entanto, a recíproca da Proposição 4.3.6 é verdadeira num Domínio Principal, como mostra a proposição a seguir.

**Proposição 4.3.7.** *Em um Domínio Principal todo elemento irredutível é primo.*

*Demonstração.* Seja $p$ um elemento irredutível de um Domínio Principal $(A, +, \cdot)$. Então $p \neq 0$ e não é inversível. Supondo que $p \mid ab$, é necessário mostrar que $p \mid a$ ou $p \mid b$.

Tomamos $I = aA + pA$ como ideal de $A$ gerado pelos elementos $a$ e $p$. Uma vez que $A$ é um Domínio Principal, segue que $I = dA$ para algum $d \in I$. Podemos ver que $p = a \cdot 0 + p \cdot 1 \in I = dA$. Portanto, existe $c \in A$ tal que $p = dc$. Devido à irredutibilidade de $p$, um dos fatores, $d$ ou $c$, é inversível.

Se $d$ é inversível, então $dA = A$. Isso resulta que o ideal $I$ contém todos os elementos de $A$, o que nos permite escrever $A = aA + pA$. Agora, usaremos essa igualdade para mostrar que $p$ divide $b$.

Temos que $1 \in A$ e, assim, existem $x$, $y \in A$ tais que $1 = ax + py$. Multiplicando $b$ ambos os lados da igualdade $1 = ax + py$ obtemos,

$$b = b(ax + py) = abx + pby.$$

Como $p$ está dividindo as duas parcelas do lado direito da igualdade $b = (ab)x + pby$, concluímos que $p$ divide $b$.

Agora vamos considerar o outro caso, em que $c$ é um elemento inversível. Logo, existe um elemento $c^{-1} \in A$ tal que $cc^{-1} = 1$. Vimos que $p = dc$. Multiplicando ambos os lados dessa igualdade por $c^{-1}$ obtemos, $pc^{-1} = dcc^{-1} = d$.

Temos que $a = a \cdot 1 + p \cdot 0 \in aA + pA = I = dA$. Logo, $a = dq$ para algum $q \in A$. Substituindo $d = pc^{-1}$ na equação $a = dq$, obtemos $a = qpc^{-1} = pc^{-1}q$. Como $a$ é um múltiplo de $p$, concluímos que, neste caso, $p$ divide $a$. □

**Definição 4.3.8.** Diz-se que um anel de integridade $(A, +, \cdot)$ é um *anel fatorial* se as seguintes condições se cumprem:

(i) Todo elemento $a \in A$, não nulo e não inversível, pode ser escrito como um produto de elementos irredutíveis de $A$.

(ii) Se $a = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$ são duas fatorações de $a$ em elementos irredutíveis de $A$, então $r = s$ e, para uma conveniente permutação $\sigma$ dos índices, $p_i$ e $q_{\sigma(i)}$ estão associados.

Para finalizar este capítulo, vamos mostrar que todo Domínio Principal é também um Domínio Fatorial. Para tanto, faremos um lema preliminar.

**Lema 4.3.9.** *Toda cadeia ascendente de ideais $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots \subseteq I_k \subseteq \cdots$ num Domínio Principal é estacionária, isto é, existe algum inteiro positivo $n$ tal que $I_k = I_n$ para todo $k \geq n$.*

*Demonstração.* Sejam $I_1 \subseteq I_2 \subseteq I_3 \cdots$ um cadeia ascendente de ideais num Domínio Principal $A$ e $I = \bigcup_{i \in \mathbb{N}} I_i$. Facilmente vemos que $I$ é um ideal. Como $A$ é um Domínio Principal, segue que $I$ é um ideal principal e, portanto, existe um elemento $a \in A$ tal que $I = Aa$. Observamos que $a = 1_A \cdot a \in Aa = I$. Uma vez que $I$ é a união dos ideais acima, $a$ deve ser um elemento de um dos ideais da cadeia, digamos $a \in I_n$. Desse modo, $I_n \subseteq I = Aa \subseteq I_n$ e, assim, $I = I_n$. Portanto, $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots \subseteq I_n = I_{n+1} = I_{n+3} = \cdots$ é uma cadeia estacionária. □

**Proposição 4.3.10.** *Todo Domínio Principal é Fatorial*

*Demonstração.* Seja $(A, +, \cdot)$ um Domínio Principal e seja $a \neq 0$ um elemento de $A$ não inversível. Devemos mostrar primeiro que $a$ pode ser escrito como um produto finito de elementos irredutíveis de $A$ e, depois, devemos verificar que esta decomposição é única. O método de prova da primeira parte é precisamente análogo à determinação da decomposição em fatores primos de um número inteiro.

Se $a$ for irredutível, então terminamos. Se não, $a$ pode ser escrito como um produto $a = a_1a_2$ onde nem $a_1$ e nem $a_2$ são inversíveis. Se ambos os elementos são irredutíveis, então novamente terminamos, tendo escrito $a$ como um produto de elementos irredutíveis. Caso contrário, pelo menos um dos dois elementos, digamos $a_1$ é redutível, portanto pode ser escrito como um produto de dois elementos não inversíveis, $a_1 = a_{11}a_{12}$ e, assim, por diante. O que devemos verificar é que esse processo termina, ou seja, devemos necessariamente chegar a um ponto em que todos os elementos obtidos como fatores de $a$ sejam irredutíveis.

Suponha que este não seja o caso. Da fatoração $a = a_1a_2$ obtemos uma inclusão própria de ideais:

$$aA \subseteq a_1A \subseteq A.$$

A primeira inclusão é própria porque $a_2$ não é inversível, e a última inclusão é própria porque $a_1$ não é inversível. Da fatoração de $a_1$ obtemos de forma semelhante

$$aA \subseteq a_1A \subseteq a_{11}A \subseteq A.$$

Se esse processo de fatoração não terminasse após um número finito de etapas, obteríamos uma cadeia ascendente infinita de ideais:

$$Aa \subseteq a_1A \subseteq a_{11}A \subseteq \cdots \subseteq A.$$

onde todas as inclusões são próprias. Pelo Lema 4.3.9, todo cadeia é estacionária. Isso significa que $a$ pode ser escrito como produto de fatores irredutíveis. Portanto, todo elemento diferente de zero de $A$ que não é inversível tem alguma fatoração em irredutíveis em $A$.

Resta provar que a decomposição acima é essencialmente única. Procedemos por indução no número $k$ de fatores irredutíveis em alguma fatoração do elemento $a$. Se $k = 0$, então $a$ é inversível. Se tivéssemos $a = qc$ (alguma outra fatoração) para algum $q$ irredutível, então $1 = aa^{-1} = q(ca^{-1})$. Portanto, $q$ seria um inversível, uma contradição.

Como hipótese de indução, suponhamos agora que se um elemento $a \in A$ tem $k$ fatores irredutíveis em alguma fatoração de $a$, então a fatoração de $a$ é única conforme o item (ii) da Definição 4.3.8.

Suponhamos que $a$ seja igual a dois produtos

$$a = p_1p_2 \cdots p_{k+1} = q_1q_2 \cdots q_m,$$

onde $p_i$ e $q_i$ são irredutíveis (não necessariamente distintos). Então, $p_1$ divide o produto à direita e, consequentemente, $p_1$ divide um dos fatores, uma vez que qualquer elemento irredutível é primo num Domínio Principal. Renumerando se necessário, podemos assumir que $p_1$ divide $q_1$. Logo, $q_1 = p_1 u$, para algum $u \in A$. Observamos que $u$ deve ser inversível, pois $q_1$ é irredutível. Além disso, temos que $p_1 = qu^{-1}$, ou seja, $p_1$ divide $q_1$ e, assim, esses dois elementos são associados. Agora, temos que

$$a = p_1 p_2 \cdots p_k = u p_1 q_2 \cdots q_m.$$

Lembramos que num Anel de Integridade a lei do cancelamento do produto é válida e, então, cancelando $p_1$ obtemos a igualdade

$$p_2 \cdots p_k = u q_2 \cdots q_s = q_2' \cdots q_m \tag{4.3}$$

onde $q_2' = u q_2$ é também um irredutível, associado a $q_2$. Pela indução sobre $k$, concluímos que o número de fatores irredutíveis do lado esquerdo e direito em (4.3) coincide e que cada um dos fatores à esquerda corresponde bijetivamente (sendo associados) com os fatores da direita. Como, já mostramos que $p_1$ e $q_1$ são associados após a renumeração inicial, temos que isso completa a etapa de indução e a prova do teorema. □

Das Proposições 4.2.12, 4.2.12 e 4.3.10, temos as seguintes inclusões entre as classes de anéis comutativos com identidade:

Corpos ⊆ Domínios Euclidianos ⊆ Domínios Principais ⊆ Domínios Fatoriais

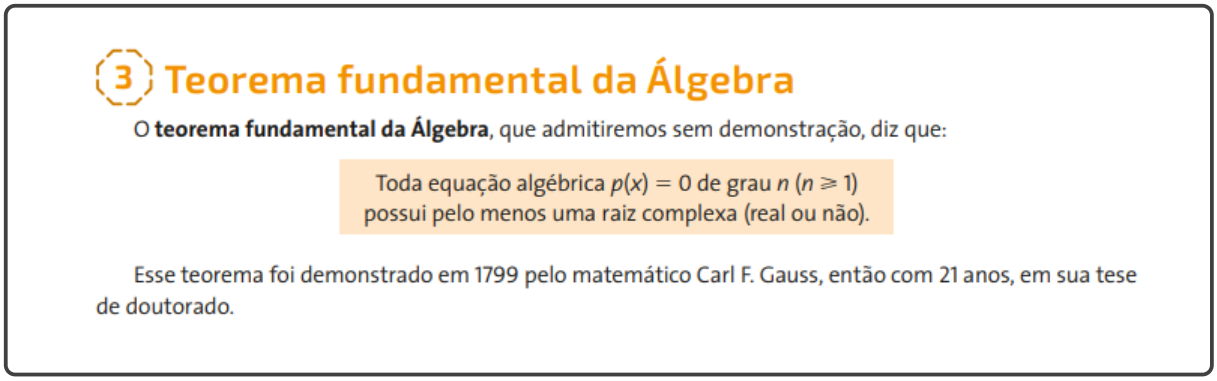
Segue dos Teoremas 4.1.3 e 4.1.5 que os anéis de inteiros e os anéis de polinômios com coeficiente num corpo são Domínios Euclidianos e, consequentemente, são Domínios Fatoriais.

Esse caminho longo prova o Teorema Fundamental da Aritmética. Para finalizar este capítulo, vamos discutir brevemente sobre a fatoração de polinômios de $\mathbb{C}[x]$.

**Definição 4.3.11.** Seja $\mathbb{K}$ um corpo. Se todo polinômio não constante de $\mathbb{K}[x]$ tem pelo menos uma raiz em $\mathbb{K}$, dizemos que $\mathbb{K}$ é um corpo *algebricamente fechado*.

O exemplo mais familiar de corpo algebricamente fechado é o corpo dos números complexos $\mathbb{C}$. O teorema que assegura esse fato é conhecido como *Teorema Fundamental da Álgebra*. Veja a Figura 33.

Figura 33 – Teorema Fundamental da Decomposição




Fonte: DANTE (2016b, p. 219)

Esse assegura que todo polinômio com grau maior do que zero pode ser decomposto em polinômios de primeiro grau com coeficientes complexos, o que implica que ele possuirá ao menos uma raiz complexa. Trata-se de um resultado essencial em álgebra, com aplicações relevantes em diversas áreas da matemática e da ciência. Para uma análise detalhada dessa demonstração, é possível encontrá-la em Hefez e Villela (2012, p. 192), visto que tais detalhes excedem o propósito deste texto.

**Proposição 4.3.12.** *Um polinômio sobre um corpo $\mathbb{C}$ é irredutível se, e somente se, tem grau 1.*

*Demonstração.* Seja $p \in \mathbb{C}[x]$ um polinômio irredutível. Pelo Teorema Fundamental da Álgebra, $\mathbb{C}$ é algebricamente fechado, ou seja, existe $u \in \mathbb{C}$ tal que $p(u) = 0$. Pelo algoritmo da divisão euclidiana, na divisão de $p$ pelo polinômio $x - u$, existem polinômios $q, r$ tais que

$$p(x) = (x - u)q(x) + r(x), \quad r(x) = 0 \text{ ou } \partial(r) < \partial(x - u).$$

Assim, $r(x)$ é um polinômio constante. No entanto, $0 = p(u) = (u - u)q(u) + r = r$, ou seja, o resto é o polinômio nulo. Temos que

$$p(x) = (x - u)q(x).$$

Como $p$ é irredutível, segue que o polinômio $q$ é constante não nulo (vimos que os polinômios inversível em $\mathbb{C}[x]$ são os constantes). Logo, existe $a \in \mathbb{C}$ tal que $q(x) = a$, para todo $x \in \mathbb{C}$. Portanto,

$$p(x) = a(x - u)$$

e $\partial(p) = 1$.

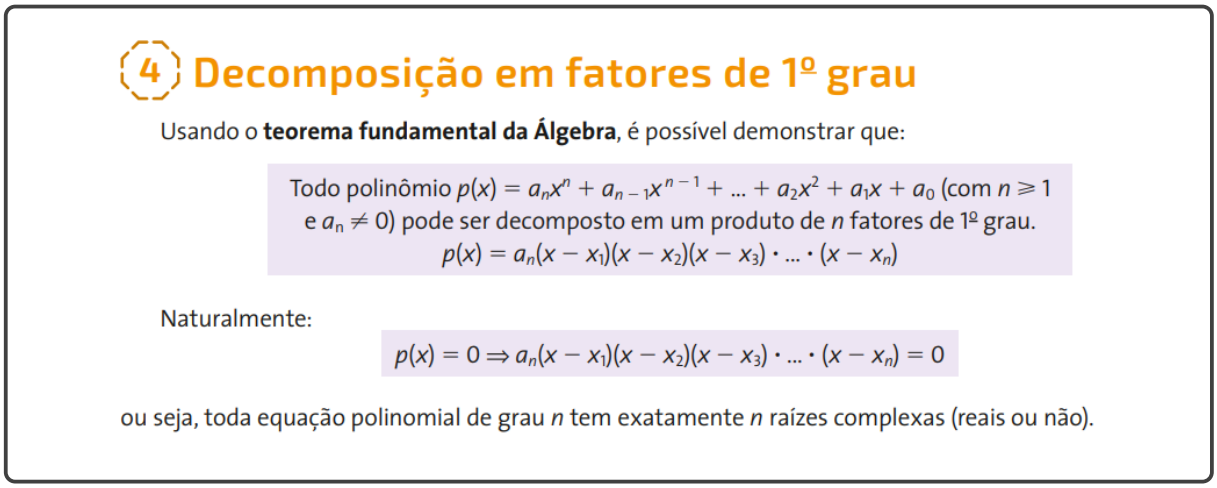
A recíproca foi feita no item (b) do Exemplo 4.3.4. □

Seja $p(x) \in \mathbb{C}[x]$ um polinômio não nulo e não constante. Já sabemos que o anel de polinômios $\mathbb{C}[x]$ é um Domínio Fatorial e que os polinômios irredutíveis desse anel são de grau 1. Logo, existem $x - u_1$, $x - u_2, \cdots, x - u_n \in \mathbb{C}[x]$ e $a \in \mathbb{C}$ tal que

$$p(x) = a(x - u_1)(x - u_2) \cdots (x - u_n).$$

Esse resultado é conhecido como o Teorema da Decomposição. Veja figura 34.

Figura 34 – Teorema da Decomposição



**4 Decomposição em fatores de 1º grau**

Usando o **teorema fundamental da Álgebra**, é possível demonstrar que:

Todo polinômio $p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_2x^2 + a_1x + a_0$ (com $n \geqslant 1$ e $a_n \neq 0$) pode ser decomposto em um produto de $n$ fatores de 1º grau.

$$p(x) = a_n(x - x_1)(x - x_2)(x - x_3) \cdot \ldots \cdot (x - x_n)$$

Naturalmente:

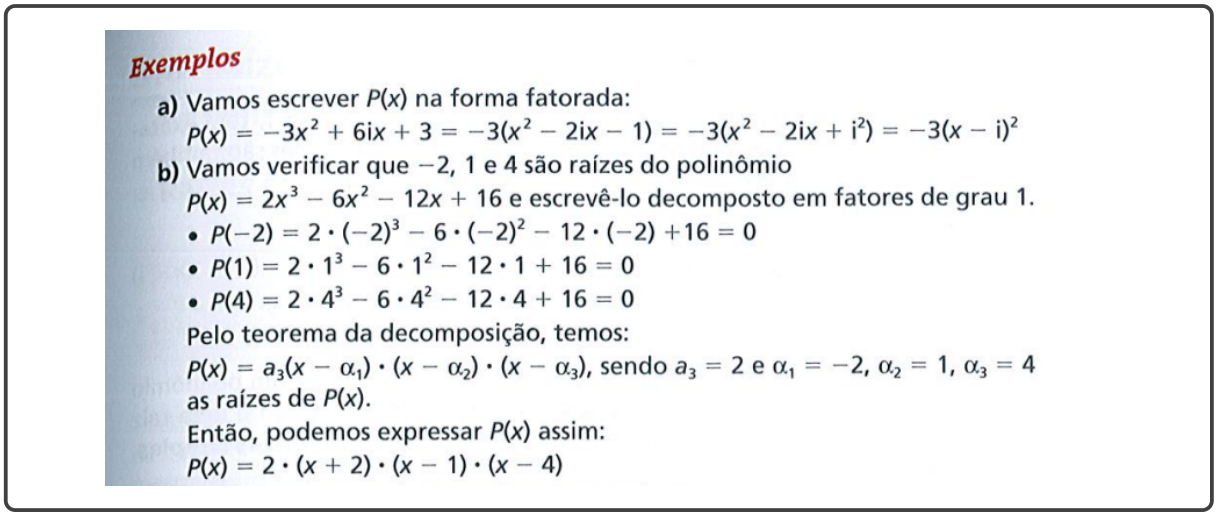
$$p(x) = 0 \Rightarrow a_n(x - x_1)(x - x_2)(x - x_3) \cdot \ldots \cdot (x - x_n) = 0$$

ou seja, toda equação polinomial de grau $n$ tem exatamente $n$ raízes complexas (reais ou não).

Fonte: DANTE (2016b, p. 219)

Observamos que o teorema acima afirma que todo polinômio complexo não constante pode ser fatorado em fatores irredutíveis, de forma semelhante com a fatoração em primos em $\mathbb{Z}$.

Figura 35 – Fatoração de polinômio



**Exemplos**

**a)** Vamos escrever $P(x)$ na forma fatorada:

$P(x) = -3x^2 + 6ix + 3 = -3(x^2 - 2ix - 1) = -3(x^2 - 2ix + i^2) = -3(x - i)^2$

**b)** Vamos verificar que $-2$, 1 e 4 são raízes do polinômio $P(x) = 2x^3 - 6x^2 - 12x + 16$ e escrevê-lo decomposto em fatores de grau 1.

- $P(-2) = 2 \cdot (-2)^3 - 6 \cdot (-2)^2 - 12 \cdot (-2) + 16 = 0$
- $P(1) = 2 \cdot 1^3 - 6 \cdot 1^2 - 12 \cdot 1 + 16 = 0$
- $P(4) = 2 \cdot 4^3 - 6 \cdot 4^2 - 12 \cdot 4 + 16 = 0$

Pelo teorema da decomposição, temos:

$P(x) = a_3(x - \alpha_1) \cdot (x - \alpha_2) \cdot (x - \alpha_3)$, sendo $a_3 = 2$ e $\alpha_1 = -2$, $\alpha_2 = 1$, $\alpha_3 = 4$ as raízes de $P(x)$.

Então, podemos expressar $P(x)$ assim:

$P(x) = 2 \cdot (x + 2) \cdot (x - 1) \cdot (x - 4)$

Fonte: LEONARDO (2016, p. 199)

Como podemos ver, os inteiros e os polinômios têm muito em comum. Isso mostra que a interseção entre os campos da Aritmética e a Álgebra é muito ampla.

Finalizando nossa análise sobre o Domínio Fatorial, voltamos agora nossa atenção para o próximo capítulo, o qual se dedicará à abordagem pedagógica referente ao Ensino da Matemática.

# 5 O Ensino da Matemática

A educação matemática desempenha um papel importante na vida do estudante, pois é responsável por fornecer habilidades como o raciocínio lógico, a resolução de problemas e a capacidade de analisar e interpretar informações.

## 5.1 Processos de Ensino e de Aprendizagem

De acordo com os Parâmetros Curriculares Nacionais os processos de ensino e aprendizagem da matemática deve ir além da simples transmissão de informações.

> A forma de trabalhar os conteúdos deve sempre agregar um valor formativo no que diz respeito ao desenvolvimento do pensamento matemático. Isso significa colocar os alunos em um processo de aprendizagem que valorize o raciocínio matemático, nos aspectos de formular questões, perguntar-se sobre a existência de solução, estabelecer hipóteses e tirar conclusões, apresentar exemplos e contraexemplos, generalizar situações, abstrair regularidades, criar modelos, argumentar com fundamentação lógico - dedutiva. (BRASIL, 2006, p.69-70).

Conforme afirmado por Fainguelert e Nunes (2012), é preciso permitir um ensino que integre uma dimensão mais dinâmica, para que a prática não seja meramente reprodutiva. Os alunos devem ser capazes de se envolver em atividades relevantes e desafiadoras que envolvam seus interesses e, dessa forma, serem encorajados a estimular sua curiosidade para facilitar uma aprendizagem mais significativa.

Para Meyer (2011), os alunos devem saber aprender, afinal, os professores não podem ensinar toda a matemática de que precisam, mas podem permitir que eles tenham confiança em si mesmos, para que desenvolvam aptidões suficientes para formular e resolver uma situação e interpretar criticamente a realidade com base nisso.

Entender a relevância da base de conhecimento do professor é essencial para alcançar uma educação mais significativa e eficaz. Ao reconhecer a influência desses elementos nos processos de ensino e de aprendizagem, podemos promover uma abordagem pedagógica mais sensível e apropriada, o que resultará no crescimento intelectual e pessoal dos alunos de maneira mais abrangente.

Analisando os parâmetros Curriculares Nacionais (Brasil, 2022), no nível do Ensino Médio, podemos identificar seus objetivos: desenvolver a capacidade de pesquisar, buscar

informações, realizar análises; ser capaz de aprender, criar, formular, ao invés do simples exercício de memorização.

Conforme Loyo (2018), quando um professor decide seguir determinada prática pedagógica a fim de facilitar a absorção do conhecimento por seus alunos, mesmo que inconscientemente, ele se vale de sua formação epistemológica, que seria a soma de suas crenças, conhecimentos e suas experiências quanto aluno.

> É preciso trazer o encantamento para a sala de aula e transgredir as fronteiras que foram criadas entre as disciplinas. Tornar a sala de aula de Matemática um ambiente que encoraje cada vez mais os alunos a propor soluções, explorar possibilidades, levantar hipóteses, justificar seus raciocínios e validar suas próprias conclusões. E é só dessa forma que abriremos espaço para uma educação mais significativa e dialógica. (FAINGUELERNT e NUNES, 2012, p.24).

Ao estabelecer conexões entre a matemática e situações do cotidiano, os estudantes percebem que ela deixa de ser algo complexo e distante, o que facilita a compreensão.

Loyo e Cabral, (2018), sugere que aproximar situações da vida real é uma forma interessante de usar o conteúdo. Desta forma, os alunos podem ter em conta a sua experiência quotidiana, perceber a matemática de uma forma menos abstrata e aproximá-la das suas vidas.

> Cabe ao professor ter o domínio dos métodos e trabalhar em constante inovação. Assim, ele terá plena capacidade para decidir qual é o método ideal para cada contexto. Tal decisão deve ser pautada pelo nível dos alunos, pelo contexto sociocultural em que estão envolvidos, pelos objetivos a serem alcançados, entre outros aspectos. (LOYO; CABRAL, 2018, p.31).

A educação é uma área em constante evolução, e o papel do professor como mediador do conhecimento é fundamental para o sucesso do processo de ensino e aprendizagem.

Nesse contexto, o saber pedagógico vai além de apenas passar um conteúdo, conforme destacado por Loyo e Cabral (2018), o professor deve demonstrar empatia e carisma para estabelecer uma conexão significativa com os alunos, tornando-se essas características indispensáveis ao transmitir um determinado conteúdo.

## 5.2 Planejamento

A adoção de métodos de ensino contextualizados e interativos pode facilitar no processo de ensino e aprendizagem. De acordo com Fainguelernt e Nunes (2012), a aplicação de aulas fragmentadas, desvinculadas e baseadas apenas na transmissão oral do conhecimento favorece a memorização e revela-se extremamente deficiente. Práticas que negligenciam o papel do professor como questionador e mediador no processo de apropriação do conhecimento pelos alunos apresentam graves deficiências.

Ou seja, proporcionar métodos de ensino que promovam o desenvolvimento dos alunos, contribuindo para uma formação mais completa e preparada para o contexto social em que estão inseridos. Loyo e Cabral (2018) destacam o papel do professor em oferecer aulas que possibilitem despertar nos alunos um aspecto investigativo na busca por soluções alternativas para a resolução de problemas, permitindo assim que se tornem cidadãos mais críticos e conscientes de seu papel na sociedade moderna.

É perceptível que o professor não tem controle sobre todas as variáveis envolvidas no aprendizado de cada aluno, mas precisa estar ciente de que pode facilitar o processo de ensino-aprendizagem em sua sala de aula.

Dar aos alunos a oportunidade de adquirir habilidades que permitam identificar o uso da matemática na resolução de problemas, aplicar conceitos, e verificar o procedimento em busca de resultados para obter solução e interpretá-los de acordo com o contexto das situações. “A dedução de algumas propriedades e a verificação de conjecturas, a partir de outras, podem ser estimuladas, sobretudo ao final do Ensino Fundamental.” (BRASIL, 2019, p.265)

Por meio de um planejamento cuidadoso, o professor tem a oportunidade de exercer um papel fundamental na condução do aprendizado, estabelecendo metas claras e alinhadas com os objetivos pedagógicos. Além disso, o planejamento permite ao educador preparar atividades relevantes e significativas, que estimulem a participação dos alunos, criando um ambiente propício para a aprendizagem.

Conforme mencionado por Sutherland (2008), o planejamento possibilita ao professor refletir sobre sua atitude em sala de aula, reconhecendo que suas ações e posturas influenciam diretamente no que os alunos irão aprender. Embora seja impossível prever exatamente o que os estudantes absorverão de cada atividade, um planejamento cuidadoso e bem estruturado aumenta as chances de sucesso no processo educativo.

Dessa forma, o professor se torna um facilitador do conhecimento, buscando promover uma aprendizagem significativa e enriquecedora para seus alunos.

Para Loyo e Cabral (2018), as estratégias de ensino estão em constante desenvolvimento com o objetivo de aproximar os alunos e a matemática ensinada na escola.

Assim, a utilização de jogos e brincadeiras é uma forma de ensino que está sendo bastante difundida.

Conforme afirmam Chambers e Timlin (2015), ao acompanhar a evolução da matemática ao longo dos séculos, verifica-se que esse campo do conhecimento está em contínuo progresso. Além disso, é relevante ressaltar que por trás das teorias e descobertas matemáticas encontram-se mentes humanas, o que torna essa ciência uma construção em constante desenvolvimento. Nesse sentido, abordaremos mais detalhadamente esse contexto.

### 5.2.1 História da Matemática: uma direção educacional

> Ao revelar a Matemática como uma criação humana, ao mostrar necessidades e preocupações de diferentes culturas, em diferentes momentos históricos, ao estabelecer comparações entre os conceitos e processos matemáticos do passado e do presente, o professor tem a possibilidade de desenvolver atitudes e valores mais favoráveis do aluno diante do conhecimento matemático. Além disso, conceitos abordados em conexão com sua história constituem-se veículos de informação cultural, sociológica e antropológica de grande valor formativo. A História da Matemática é, nesse sentido, um instrumento de resgate da própria identidade cultural. Em muitas situações, o recurso à História da Matemática pode esclarecer ideias matemáticas que estão sendo construídas pelo aluno, especialmente para dar respostas a alguns "porquês" e, desse modo, contribuir para a constituição de um olhar mais crítico sobre os objetos de conhecimento (BRASIL, 1997, p. 34).

Segundo Loyo e Cabral (2018), a história da matemática pode ser considerada uma direção educacional capaz de despertar nos seus alunos o mesmo deslumbramento que Einstein expressava. Essa tendência visa estabelecer os fundamentos cognitivos dos alunos nos processos históricos envolvidos na construção de cada tema que estudam.

> O conhecimento matemático deve ser apresentado aos alunos como historicamente desenvolvido e em constante desenvolvimento. O contexto histórico permite ver a matemática em sua prática filosófica, científica e social e contribui para a compreensão de seu lugar no mundo. É importante que, nas aulas e em atividades de Matemática, passemos de problemas com respostas definidas para situações sem "perguntas matemáticas". O objetivo e o subjetivo evidentemente se relacionam, e pretendemos que sejamos capazes de concatenar o mundo real em que os nossos alunos vivem com o universo matemático abstrato. (MEYER, 2019, p. 27).

Percebe-se que a abordagem da história da matemática é um método de ensino que permite ao aluno desempenhar um papel ativo na construção do seu conhecimento. Loyo e Cabral (2018) afirma que é possível apresentar a história da matemática nas séries iniciais do Ensino Fundamental. Qualquer atividade baseada em histórias estimula o pensamento investigativo. Nos primeiros anos escolares, esse estímulo pode aumentar a curiosidade e inspirar o desejo de explorar. Esse processo de aprendizagem ativo e reflexivo é essencial para a vida acadêmica do aluno.

A utilização de fatos históricos em sala de aula auxilia a compreensão dos aspectos históricos dos temas abordados, desperta o interesse dos alunos e ainda os motiva na busca pelo conhecimento. Segundo Loyo e Cabral (2018), a utilização de conceitos históricos como ferramentas pedagógicas permite a sistematização de abordagens pedagógicas que contribuem para o processo educacional. Isso possibilita aos alunos não apenas um aprendizado isolado, mas uma estrutura conceitual básica dos conceitos matemáticos sem memorizar definições, além de reviver as descobertas e obter uma compreensão mais profunda do conteúdo.

Cury e Ribeiro (2014) nos apresenta problemas com aplicação da matemática dos Egípcios.

> Na Matemática dos egípcios, por meio de muitos problemas encontrados nos papiros de Rhind e de Moscou, pôde ser detectada a presença de situações problemas de origem prática, com questões sobre pão, cerveja, balanceamento de rações para o gado e aves, entre outros. Muitos desses problemas eram resolvidos por uma equação linear com uma incógnita, nas quais os egípcios utilizavam-se de um método que, mais tarde na Europa, ficou conhecido por regra da falsa posição. Tais problemas eram normalmente simples e não iam além de equações lineares com uma incógnita. Além disso, suas soluções não exigiam grandes métodos e raciocínios, sendo que o mais empregado, o da falsa posição, assemelha-se bastante com o que conhecemos hoje como "método das tentativas". A partir disso, pode-se observar que tanto babilônios como egípcios trabalhavam, basicamente, com equações originárias de problemas de ordem prática, buscando as soluções de tais equações por métodos basicamente aritméticos, nos quais procuravam igualar duas ou mais quantidades conhecidas, com a finalidade de encontrar o valor da quantidade desconhecida. Observa-se ainda que, durante esse período da história das equações, a maior parte das soluções relacionava-se a equações particulares, no intuito de resolver problemas específicos, não apresentando como preocupação a busca por soluções gerais para todos os tipos de equações conhecidas. (CURY; RIBEIRO, 2015, p.30 - 31).

Assim como a história da matemática é um recurso educacional, também é importante destacar outra abordagem no ensino: a tecnologia educacional. Ao integrar a tecnologia no planejamento pedagógico, torna-se possível desenvolver aulas mais dinâmicas e interativas.

### 5.2.2 Ferramenta de Ensino: Tecnologia

Meyer (2019) enfatiza a preocupação existente em relação ao aprendizado da matemática. Mais do que isso, os alunos precisam adquirir ferramentas matemáticas relevantes. Entendemos que esse aprendizado será mais eficaz, embora seja apenas uma hipótese, se os alunos encontrarem sentido naquilo que estão aprendendo. Em outras palavras, é fundamental que o que é ensinado em sala de aula faça sentido para eles, como indivíduos que participam da prática social. Isso promove uma aprendizagem matemática crítica e engajada.

Com os avanços científicos e tecnológicos e a criação de novos campos do conhecimento a importância da matemática tornaram-se ainda mais evidente.

Segundo Fainguelernt e Nunes (2012), a matemática é uma ciência viva, uma ferramenta para o avanço de outras ciências. Inclui um amplo leque de relações e regularidades, que despertam a curiosidade e, ao mesmo tempo, aumentam a capacidade de generalização, projeção, previsão e abstração, condições essenciais para o exercício de qualquer atividade profissional.

Com a evolução das tecnologias digitais, os recursos disponíveis no ambiente de aprendizagem se expandem, proporcionando novas oportunidades de interação, colaboração e acesso a conteúdos diversificados.

Para Sutherland (2008), desenvolver o conteúdo matemático é possuir habilidades que possibilitem a utilização de novas ferramentas capazes de resolver problemas que até então eram considerados difíceis ou impossíveis de resolver com as ferramentas anteriores.

Consta nos parâmetros Curriculares Nacionais

> [...] em relação às competências a serem desenvolvidas pela Matemática, a abordagem proposta para esse tema permite ao aluno usar e interpretar modelos, perceber o sentido de transformações, buscar regularidades, conhecer o desenvolvimento histórico e tecnológico de parte de nossa cultura e adquirir uma visão sistematizada de parte do conhecimento matemático (BRASIL,2019, p.119).

De acordo com Sutherland (2008), as tecnologias digitais acrescentam uma nova dimensão ao feedback na educação, especialmente na matemática. Com o auxílio do computador, os estudantes podem receber retornos mais precisos e imediatos sobre suas construções matemáticas. Isso não apenas aprimora sua compreensão dos conceitos, mas também incentiva a autonomia e a autorregulação no processo de aprendizagem.

Portanto, a tecnologia usada de forma correta pelo professor torna-se valiosa no aperfeiçoamento do ensino, capacitando os estudantes a explorar, experimentar e consolidar seus conhecimentos de forma mais efetiva.

## 5.3 Competências no Ensino da Álgebra - Base Nacional Comum Curricular

As competências possuem um papel de orientação da Base Nacional Comum Curricular, possibilitando criar conexões entre a aprendizagem o mundo social e o mundo cultural em que habitamos, sendo assim, vamos citar as competências específicas para o ensino de matemática no ensino fundamental. (BRASIL, 2017):

1. Reconhecer que a matemática é uma ciência humana, fruto das necessidades e preocupações de diferentes culturas, em diferentes momentos históricos, e é uma ciência viva, que contribui para solucionar problemas científicos e tecnológicos e para alicerçar descobertas e construções, inclusive com impactos no mundo do trabalho.

2. Desenvolver o raciocínio lógico, o espírito de investigação e a capacidade de produzir argumentos convincentes, recorrendo aos conhecimentos matemáticos para compreender e atuar no mundo.

3. Compreender as relações entre conceitos e procedimentos dos diferentes campos da matemática (aritmética, álgebra, geometria, estatística e probabilidade) e de outras áreas do conhecimento, sentindo segurança quanto à própria capacidade de construir e aplicar conhecimentos matemáticos, desenvolvendo a autoestima e a perseverança na busca de soluções.

4. Fazer observações sistemáticas de aspectos quantitativos e qualitativos presentes nas práticas sociais e culturais, de modo a investigar, organizar, representar e comunicar informações relevantes, para interpretá-las e avaliá-las crítica e eticamente, produzindo argumentos convincentes.

5. Utilizar processos e ferramentas matemáticas, inclusive tecnologias digitais disponíveis, para modelar e resolver problemas cotidianos, sociais e de outras áreas de conhecimento, validando estratégias e resultados.

6. Enfrentar situações-problema em múltiplos contextos, incluindo situações imaginadas, não diretamente relacionadas com o aspecto prático–utilitário; expressar suas respostas e sintetizar conclusões, utilizando diferentes registros e linguagens (gráficos, tabelas, esquemas, além de texto escrito na língua materna e outras linguagens para descrever algoritmos, como fluxogramas e dados).

7. Desenvolver e/ou discutir projetos que abordem, sobretudo, questões de urgência social, com base em princípios éticos, democráticos, sustentáveis e solidários, valorizando a diversidade de opiniões de indivíduos e de grupos sociais, sem preconceitos de qualquer natureza.

8. Interagir com seus pares de forma cooperativa, trabalhando coletivamente no planejamento e no desenvolvimento de pesquisas para responder a questionamentos e na busca de soluções para problemas, de modo a identificar aspectos consensuais ou não na discussão de determinada questão, respeitando o modo de pensar dos colegas e aprendendo com eles.

Segundo a BNCC, o Ensino Fundamental tem o compromisso com o letramento matemático:

> O Ensino Fundamental deve ter compromisso com o desenvolvimento do letramento matemático, definido como as competências e habilidades de raciocinar, representar, comunicar e argumentar matematicamente, de modo a favorecer o estabelecimento de conjecturas, a formulação e a resolução de problemas em uma variedade de contextos, utilizando conceitos, procedimentos, fatos e ferramentas matemáticas. É também o letramento matemático que assegura aos alunos reconhecer que os conhecimentos matemáticos são fundamentais para a compreensão e a atuação no mundo e perceber o caráter de jogo intelectual da matemática, como aspecto que favorece o desenvolvimento do raciocínio lógico e crítico, estimula a investigação e pode ser prazeroso (BRASIL, 2017, documento on-line).

Sutherland (2008), considera a álgebra como uma ferramenta que auxilia na resolução de problemas difíceis utilizando apenas o conhecimento aritmético. Infelizmente, os benefícios a longo prazo de aprender a usar novas ferramentas matemáticas nem sempre podem ser apreciados a curto prazo. Paradoxalmente, uma ênfase excessiva na abordagem informal do aluno pode reduzir ainda mais a necessidade de os alunos aprenderem a usar novas ferramentas matemáticas. Isso levanta a questão de qual é a melhor forma de introduzir novas ferramentas matemáticas de forma que os alunos mudem de ferramentas antigas para novas.

> A matemática é uma das disciplinas, como as línguas modernas, na qual a aprendizagem é hierárquica. É impossível fazer cálculos sem uma compreensão detalhada da álgebra. Mesmo em se tratando de um tema como a álgebra, as habilidades necessárias para resolver equações quadráticas dependem do entendimento de como combinar os termos algébricos e do uso de parênteses.(CHAMBERS e TIMLIN, 2015, p.51).

Na perspectiva do ensino, o professor se aproprie dos objetos de conhecimento e aptidões necessários para o seu planejamento.

Assim como ocorre no ensino fundamental, a álgebra também é abordada no ensino médio. Quando o professor identifica claramente as competências que serão desenvolvidas e as habilidades que deseja cultivar, isso facilita a formulação de seu planejamento. Considerando essa perspectiva, fornecemos as competências destacadas na Base Nacional Comum Curricular (BNCC), acompanhadas de um quadro que detalha as habilidades correspondentes.

Competências específicas de matemática e suas tecnologias para o ensino médio.

1. Utilizar estratégias, conceitos e procedimentos matemáticos para interpretar situações em diversos contextos, sejam atividades cotidianas, sejam fatos das Ciências da Natureza e Humanas, ou ainda questões econômicas ou tecnológicas, divulgados por diferentes meios, de modo a consolidar uma formação científica geral.

2. Articular conhecimentos matemáticos ao propor e/ou participar de ações para investigar desafios do mundo contemporâneo e tomar decisões éticas e socialmente responsáveis, com base na análise de problemas de urgência social, como os voltados a situações de saúde, sustentabilidade, das implicações da tecnologia no mundo do trabalho, entre outros, recorrendo a conceitos, procedimentos e linguagens próprios da Matemática.

3. Utilizar estratégias, conceitos e procedimentos matemáticos, em seus campos – Aritmética, Álgebra, Grandezas e Medidas, Geometria, Probabilidade e Estatística –, para interpretar, construir modelos e resolver problemas em diversos contextos, analisando a plausibilidade dos resultados e a adequação das soluções propostas, de modo a construir argumentação consistente.

4. Compreender e utilizar, com flexibilidade e fluidez, diferentes registros de representação matemáticos (algébrico, geométrico, estatístico, computacional etc.), na busca de solução e comunicação de resultados de problemas, de modo a favorecer a construção e o desenvolvimento do raciocínio matemático.

5. Investigar e estabelecer conjecturas a respeito de diferentes conceitos e propriedades matemáticas, empregando recursos e estratégias como observação de padrões, experimentações e tecnologias digitais, identificando a necessidade, ou não, de uma demonstração cada vez mais formal na validação das referidas conjecturas.

## 5.4 Produto Educacional - Caderno Pedagógico

O caderno pedagógico foi desenvolvido com o propósito de oferecer atividades direcionadas ao ensino da Álgebra. Isso é feito tanto por meio da contextualização do conteúdo quanto pela utilização dos conhecimentos de Aritmética já adquiridos pelos alunos como ponto de partida. Essa abordagem visa estabelecer conexões entre a Álgebra e os conceitos matemáticos que os estudantes já aprenderam na Aritmética, tornando a Álgebra mais acessível e familiar para eles. O objetivo principal é assegurar que os estudantes compreendam o conteúdo de forma sólida e significativa.

O caderno pedagógico está dividido em duas seções distintas: uma voltada para o professor, que contém sugestões de atividades aplicáveis em suas aulas; e outra direcionada ao aluno, contendo o material sem comentários ou sugestões. Isso é feito com o propósito

de dar ao professor a liberdade de aplicar as atividades propostas de acordo com sua preferência e estilo.

Na Proposta 01, intitulada “Conexões aritméticas e algébricas”, buscamos transformar o próprio professor em um personagem de história em quadrinhos por meio de um aplicativo gratuito. Isso visa atrair a atenção dos alunos de forma simples para a consistência das propriedades compartilhadas entre a Aritmética e a Álgebra, permitindo que eles apliquem as regras previamente aprendidas. Essa abordagem contribuirá para o desenvolvimento de uma base sólida na compreensão dos conceitos algébricos.

Na Proposta 02, “ Estudo das operações com polinômios”, abordamos o estudo das operações com polinômios com o objetivo de promover a compreensão dessas operações. Essa abordagem visa capacitar os alunos a aplicar as regras necessárias para manipular o conteúdo de polinômios.

Na Proposta 03, “Fatoração de polinômios”, tratamos da fatoração com polinômios, um conteúdo que demanda raciocínio abstrato por parte dos alunos. Diante desse desafio, propomos a atividade de Fatoração de Polinômios. A ideia é que os alunos respondam a perguntas que os ajudem a distinguir os diferentes tipos de fatoração e identificar a maneira adequada de escrever cada expressão como um produto de fatores.

Na próxima Proposta, “Desafio de fatoração em um jogo de perguntas e respostas”, apresentamos um desafio de fatoração em um jogo de perguntas e respostas, onde utilizamos a tecnologia como uma ferramenta de avaliação para o professor. Basta acessar o link no laboratório de informática para que o professor tenha acesso ao jogo. O objetivo é que o professor possa diagnosticar se os alunos compreenderam o conteúdo de fatoração algébrica. Caso perceba que os alunos tiveram dificuldades em algum tipo de fatoração, ele poderá revisitar esse ponto.

Proposta 05: “Divisão de polinômios pelo método da chave, aplicação na terceira série do Ensino Médio”, utilizamos o método da chave, baseado nos inteiros que os alunos já dominam, para relacioná-lo aos procedimentos necessários na divisão de polinômios. Dessa forma, buscamos apresentar a Álgebra como uma extensão natural dos conceitos matemáticos previamente aprendidos na Aritmética.

Para concluir, a última Proposta “Expressões algébricas e divisão” possui o objetivo de despertar o interesse dos alunos por meio da criptografia RSA. A provocação é a seguinte: ‘Você já se perguntou como é possível manter mensagens privadas em um mundo digital repleto de ameaças?’ No material destinado ao professor, demonstramos como criptografar e descriptografar a palavra PARABÉNS. Isso é feito por meio do conteúdo de congruência. Para os leitores interessados, recomendamos consultar o Capítulo 9 do livro-texto da disciplina MA14 - Aritmética do PROFMAT. Para a realização desta atividade, sugerimos levar os alunos ao laboratório de informática e utilizar a calculadora

dos computadores como ferramenta educacional.

# CONSIDERAÇÕES FINAIS

> A formação para ser professor é desafiadora e difícil, mas proporciona enormes gratificações. Uma das maiores satisfações é o momento em que os olhos de um aluno iluminam-se com uma sensação de entendimento, e você sabe que uma pequena parte da aprendizagem se deve a você. (CHAMBERS e TIMLIN, 2015, p.21).

Nesta dissertação, procuramos estabelecer conexões entre a Aritmética e a Álgebra no contexto do Ensino Básico. Com esse propósito, conduzimos uma investigação histórica e buscamos aprofundar a compreensão desse conteúdo, utilizando a Teoria de Anéis, e visando contribuir para uma formalização mais abrangente do conhecimento por parte dos professores. Com o suporte de uma pesquisa relacionada ao ensino da matemática, elaboramos o produto educacional.

Foi realizada uma breve pesquisa sobre a história da matemática, abordando a conexão entre Aritmética e Álgebra, na qual encontramos importantes contribuições de matemáticos como Euclides, Diofante e Gauss para o desenvolvimento dessas áreas. Dante (2018), ressalta que a ideia é conceder um espaço a uma educação que reconheça e valorize a história e os conhecimentos gerados por diversas comunidades, permitindo uma compreensão profunda das características naturais e culturais presentes em sociedades e regiões diversas.

Dada a importância da formação continuada dos professores, especialmente no contexto do programa PROFMAT, e considerando que um conhecimento sólido por parte dos professores contribui de forma significativa para o processo educacional, nossa pesquisa está direcionada aos Anéis de Integridade. Abordamos os conceitos iniciais, como, por exemplo, os Anéis de Polinômios. Adicionalmente, aprofundamos nossos conhecimentos em Domínios Euclidianos, estudando tanto os Domínios Principais quanto o Domínio Fatorial. Percebemos que as semelhanças, por exemplo, entre os inteiros e os polinômios com coeficientes complexos partem do fato de que para ambos existe um algoritmo da divisão.

Quando o professor detém um conhecimento profundo e abrangente sobre determinado assunto, ele adquire maior flexibilidade para elaborar seu planejamento e adaptar suas estratégias pedagógicas. Segundo Chambers e Timlin (2015), estar ciente de que a aula está bem planejada possibilita que o docente a aborde com mais confiança do que se estivesse preparada apenas parcialmente, sendo a própria confiança um fator relevante na percepção que os alunos terão dele.

Posteriormente, conduzimos uma pesquisa relacionada ao ensino da matemática na educação básica, com o propósito de investigar a importância do planejamento das aulas alinhado ao uso de ferramentas e estratégias de aprendizagem.

> Se o professor é um dos grandes responsáveis pela apresentação de um novo conteúdo, de uma nova estratégia ou ainda difusor de um termo específico desconhecido pela turma, faz-se necessário que ele saiba não só o que vai ensinar, mas para quem está ensinando. Nesse sentido, é imprescindível sondar o conhecimento prévio dos alunos sobre os assuntos que serão formalmente trabalhados na escola, bem como considerar o desenvolvimento das habilidades e a realidade em que vivem e estudam. (GIOVANNI JÚNIOR, 2018, p.26).

Neste trabalho, meu objetivo é enfatizar a importância do professor como mediador do conteúdo em sala de aula. Defendo a utilização do método de resolução de listas de exercícios, mas antes disso, acredito que o professor deve despertar a curiosidade dos alunos por meio de um conteúdo contextualizado que estimule a investigação. A incorporação de ferramentas educacionais, como a tecnologia, pode tornar as aulas mais dinâmicas.

Com o Caderno Pedagógico, buscamos oferecer uma abordagem estruturada e flexível para o ensino da álgebra, com foco na compreensão profunda dos conceitos e no envolvimento dos alunos. Espero que isso sirva como uma contribuição e fonte de inspiração para que os professores encontrem alternativas no desenvolvimento das aulas de matemática, especialmente quando se trata do conteúdo de expressões algébricas e polinômios.

# Referências


[1] BECKER, Fernando. *Educação e Construção do Conhecimento*. 2a. ed. Porto Alegre: Penso, 2012.

[2] BIANCHINI, Edwaldo. *Matemática Bianchini*. 8a. ed. São Paulo: Editora Moderna, 2015.

[3] BONJORNO, José Roberto; GIOVANNI, José Ruy; SOUSA, Paulo Roberto Câmara de. *Matemática Completa 3º Ano*. 4a. ed. São Paulo: Editora FTD, 2016.

[4] BOYER, Carl B. *História da matemática*. 3a. ed. São Paulo: Editora Blucher, 2018.

[5] BRASIL, Ministério da Educação. *Base Comum Curricular*. Brasília: MEC, 2018. Acesso em: 19 out. 2022.

[6] BRASIL. *Parâmetros Curriculares Nacionais: Matemática*. Brasília: Secretaria de Educação Ensino Fundamental, 1997.

[7] BRASIL. *Parâmetros Curriculares Nacionais: Matemática*. Brasília: Secretaria de Educação. Ensino Médio, v.2 Brasília: MEC, 2006.

[8] CHAMBERS, Paul. e TIMLIN, Robert. *Ensinando matemática para adolescentes.*. 2a. ed. Porto Alegre: Penso, 2015.

[9] CONTADOR, Paulo Roberto Martins. *Matemática uma breve história*. 5a. ed. São Paulo: LF Editorial, 2014.

[10] CURY, Helena N.; RIBEIRO, Alessandro Jacques. *Álgebra para a Formação do Professor: explorando os conceitos de equação e de função.*. 1a. ed. Belo Horizonte: Autêntica, 2015.

[11] DANTE, Luiz Roberto. *Matemática: Contexto e Aplicações, 2ª Série*. 3a. São Paulo: Ática, 2016a.

[12] DANTE, Luiz Roberto. *Matemática: Contexto e Aplicações, 3ª Série*. 3a. São Paulo: Ática, 2016b.

[13] DANTE, Luiz Roberto. *Teláris Matemática 7º ano*. 3a. São Paulo: Ática, 2015a.

[14] DANTE, Luiz Roberto. *Teláris Matemática 7º ano*. 3a. São Paulo: Ática, 2018.

[15] DANTE, Luiz Roberto. *Teláris Matemática 9º ano*. 3a. São Paulo: Ática, 2015b.

[16] DOMINGUES, Hygino H. e IEZZI, Gelson. *Álgebra Moderna*. 4a. São Paulo: Atual, 2003.

[17] DOMINGUES, Hygino H.*Fundamentos da Aritmética*. Florianópolis: Edufsc, 2017.

[18] DUMMIT, David; FOOTE, Richard M.*Abstract Algebra*. 3a. Hoboken: John Wiley e Sons, 2004.

[19] FAINGUELERNT, Estela; NUNES, Kátia Regina A. *Matemática: Práticas Pedagógicas para o Ensino Médio*. 1 ed. Porto Alegre: Penso, 2012.

[20] GIOVANNI JÚNIOR, José Ruy. *A Conquista da Matemática: 7o ano: Ensino Fundamental*. 4ed. São Paulo: FTD, 2018.

[21] GONÇALVES, Adilson. *Introdução à Álgebra*. Rio de Janeiro: IMPA, 2017.

[22] HEFEZ, Abramo. *Aritmética*. 2.ed. Rio de Janeiro: SBM, 2016. (Coleção PROFMAT)

[23] HEFEZ, Abramo; VILLELA, Maria Lúcia Torres. *Polinômios e Equações Algébricas.*. Rio de Janeiro: SBM, 2012.

[24] IEZZI, Gelson; DOLCE, Osvaldo; DEGENSZAJN, David; PÉRIGO, Roberto; ALMEIDA, Nilze de. *Matemática: Ciência e Aplicações, Volume 2*. 9.ed. São Paulo: Saraiva, 2016.

[25] IEZZI, Gelson; MACHADO, Antônio; DOLCE, Osvaldo. *Matemática e realidade 6º ano*. 9.ed. São Paulo: Atual, 2018a.

[26] IEZZI, Gelson; MACHADO, Antônio; DOLCE, Osvaldo. *Matemática e realidade 7º ano*. 9.ed. São Paulo: Atual, 2018b.

[27] IEZZI, Gelson; MACHADO, Antônio; DOLCE, Osvaldo. *Matemática e realidade 8º ano*. 9.ed. São Paulo: Atual, 2018c.

[28] JANESCH, Oscar; TANEJA Inder Jeet. *Àlgebra I*. 2.ed. Florianópolis: Editora UFSC/EAD, 2011.

[29] KLEIN, Felix. *Matemática elementar de um ponto de vista superior*. 1.ed. Lisboa: Editora SPM, 2009.

[30] KLEINER, Israel. *A History of Abstract Algebra*. 1.ed. Boston: Editora Birkhauser, 2007.

[31] KLEINER, Israel. *From Numbers to Rings: The Early History of Ring Theory*. Elemente der Mathematik: Birkhauser Verlag, Basel, v. 53, p.18-35, 1998.

[32] LEONARDO, Fabio Martins de. *Conexões com a Matemática 2*. 3.ed. São Paulo: Moderna, 2016.

[33] LOYO, Tiago; CABRAL, Viviane R. S.. *Metodologia do ensino de matemática*. 1.ed. Porto Alegre: Penso, 2018.

[34] MEYER, João Frederico da Costa de; CALDEIRA, Ademir Donizeti; MALHEIROS, Ana Paula dos Santos. *Modelagem em educação matemática*. 4ed. Porto Alegre: Autêntica, 2019.

[35] MOL, Rogério S. *Introdução a história da matemática*. Belo Horizonte: CAED/UFMG, 2013.

[36] MORGADO, Augusto César; CARVALHO, Paulo Cezar Pinto. *Matemática Discreta*. Rio de Janeiro: SBM, 2013. (Coleção PROFMAT)

[37] ROQUE, Tatiana. *História da matemática: uma visão crítica, desfazendo lendas*. 1ed. Rio de Janeiro: Zahar, 2013.

[38] SUTHERLAND, Rosamund. *Ensino eficaz de matemática*. 1ed. Porto Alegre: Artmed, 2009.

[39] STEWART, Ian. e TALL, Davi. *Algebraic Number and Fermat's Last Theorem*. 3rd ed. Massachusetts: A K Peters, 2002.

# Apêndices

# APÊNDICE A – Produto Educacional

UNIVERSIDADE DO ESTADO DE SANTA CATARINA
CENTRO DE CIÊNCIAS TECNOLÓGICAS - CCT
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

VANESSA KLEIN SZABUNIA

## EXPLORANDO A ÁLGEBRA

JOINVILLE - SC
2023

# Explorando a Álgebra

## Conexões e Tecnologia no Ensino de Matemática

Vanessa Klein Seaburia

# SUMÁRIO

# 1 Introdução

A busca por abordagens inovadoras que tornem o processo de aprendizagem mais atrativo e significativo muitas vezes se torna um desafio ao professor. Assim, o caderno pedagógico destinado aos professores do ensino básico, pode ser usado como uma ferramenta acessível para enriquecer suas aulas no ensino do conteúdo algébrico.

A proposta central deste guia é utilizar os conhecimentos aritméticos prévios dos alunos como ponto de partida para introduzir e explorar os conceitos da Álgebra, estabelecendo conexões que facilitem o processo de aprendizagem. Ao abordar a Álgebra como uma extensão natural dos conceitos matemáticos já vistos na Aritmética, busca-se tornar esse campo de estudo mais próximo e familiar aos estudantes, proporcionando-lhes uma compreensão mais sólida e significativa do conteúdo.

Para atingir esse objetivo, o caderno pedagógico será estruturado em duas perspectivas: uma visão inicial do professor e uma visão complementar voltada para o aluno. A partir dessa abordagem, serão fornecidas orientações claras aos professores sobre como introduzir os conceitos de forma envolvente, aproveitando as conexões com a Aritmética.

Na perspectiva do aluno, serão apresentadas as atividades sem os comentários voltados aos professores. Essa abordagem interativa tem como objetivo estimular o raciocínio lógico-matemático dos estudantes, tornando o aprendizado da álgebra envolvente e prazeroso. Além disso, serão explorados recursos tecnológicos acessíveis, evidenciando como a utilização de calculadoras e a realização de aulas diferenciadas no laboratório de informática podem enriquecer a experiência de aprendizagem.

Dessa forma, pretende-se desenvolver nos estudantes habilidades essenciais, como o pensamento crítico, a resolução de problemas e a aplicação do conhecimento matemático em situações reais.

Neste sentido, espera-se que esta obra possa contribuir para a construção de uma educação matemática mais significativa e prazerosa, trazendo benefícios tanto para os educadores quanto para os estudantes.

# 2 Visão professor

Neste capítulo serão apresentadas as atividades para os professores, sendo fornecidas orientações aos professores sobre os conceitos matemáticos e as conexões entre a Aritmética e a Álgebra.

## Proposta 01: Conexões Aritméticas e Algébricas: Descobrindo paralelos matemáticos

Enfatizar a consistência das propriedades entre a Aritmética e a Álgebra permite que os alunos apliquem as regras já aprendidas, o que contribuirá para a construção de uma base sólida para a compreensão dos conceitos algébricos. Essa abordagem facilita a transição entre esses dois domínios matemáticos.

**Objetivos a serem alcançados:**

- Reconhecer semelhanças e conexões entre conceitos e propriedades numéricas e algébricas.
- Observar que muitas das regras e propriedades da Aritmética se aplicam à Álgebra.
- Usar suas habilidades Aritméticas existentes para resolver problemas e simplificar expressões algébricas.
- Perceber que os conceitos matemáticos podem ser generalizados para além de situações específicas, permitindo-lhes resolver problemas mais complexos e abstratos.
- Compreender que a Álgebra é uma extensão natural dos conceitos aritméticos.
- Dominar as propriedades a fim de desenvolver habilidades fundamentais de manipulação de expressões matemáticas

**Sugestão ao professor:** Compreender que através do anel de integridade as propriedades básicas definidas na adição e a multiplicação possuem conexões e consistência na Aritmética e na Álgebra. Os alunos podem usar as regras que já conhecem para simplificar expressões algébricas, resolver equações e realizar operações polinomiais. O professor pode se transformar em um personagem nas explicações do seu conteúdo, utilizar a tecnologia para prender positivamente a atenção do aluno despertando seu interesse. Para essa atividade foi utilizado um aplicativo gratuito chamado: *Toon Face*.

**Como utilizar esse aplicativo:**

1. Baixe e instale o aplicativo Toon Face em seu dispositivo móvel. O link para fazer a instalação na Play Store é o seguinte: https://play.google.com/store/apps/details?id=com.darkgalaxy.client.app_toonface&hl=en_US

2. Abra o aplicativo e permita o acesso à câmera. Ou selecione uma imagem da galeria do seu dispositivo.

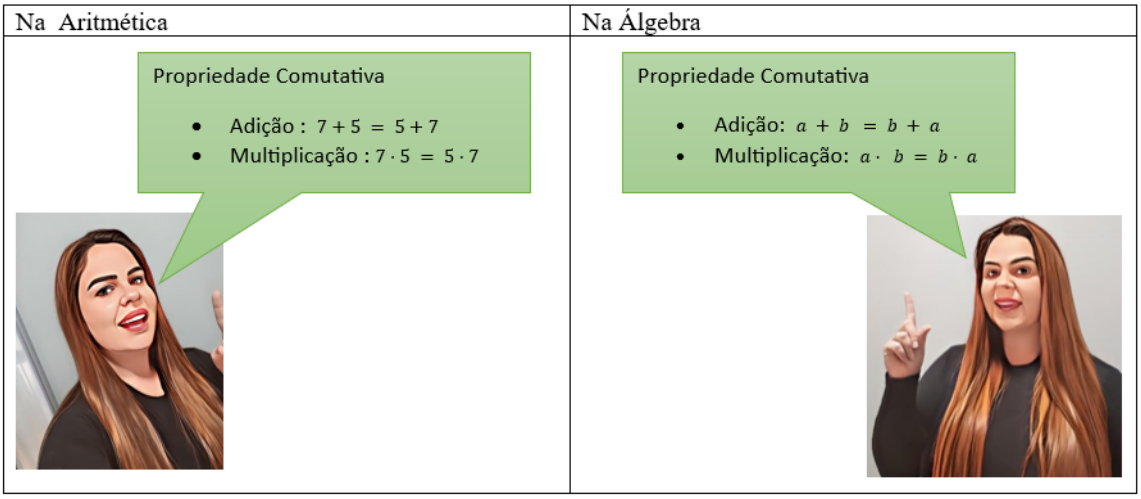
3. Escolha uma opção para criar um avatar animado.

4. Faça as alterações que desejar em seu avatar e personalize os detalhes ao seu gosto.

**Início da aula:** Para começar a aula, é recomendado retomar a introdução e os objetivos que foram enfatizados no início da atividade. Utilize o quadro disponível abaixo como uma ferramenta para comparar as propriedades Aritméticas e Algébricas. (Seria interessante se o professor criasse seu próprio avatar como parte da interação).

Mostre que as propriedades Aritméticas dos inteiros, que os alunos já conhecem, podem ser aplicadas e generalizadas para o contexto algébrico. Nesse estágio inicial, é recomendado utilizar exemplos simples para facilitar a compreensão das conexões entre as propriedades Aritméticas e como essas conexões se traduzem em expressões algébricas.

Figura 2.1 – Propriedade Comutativa




*Questão 1:* Diga se a afirmação é verdadeira ou falsa.

(a) As ações de calçar as meias e calçar os sapatos são comutativas. Não

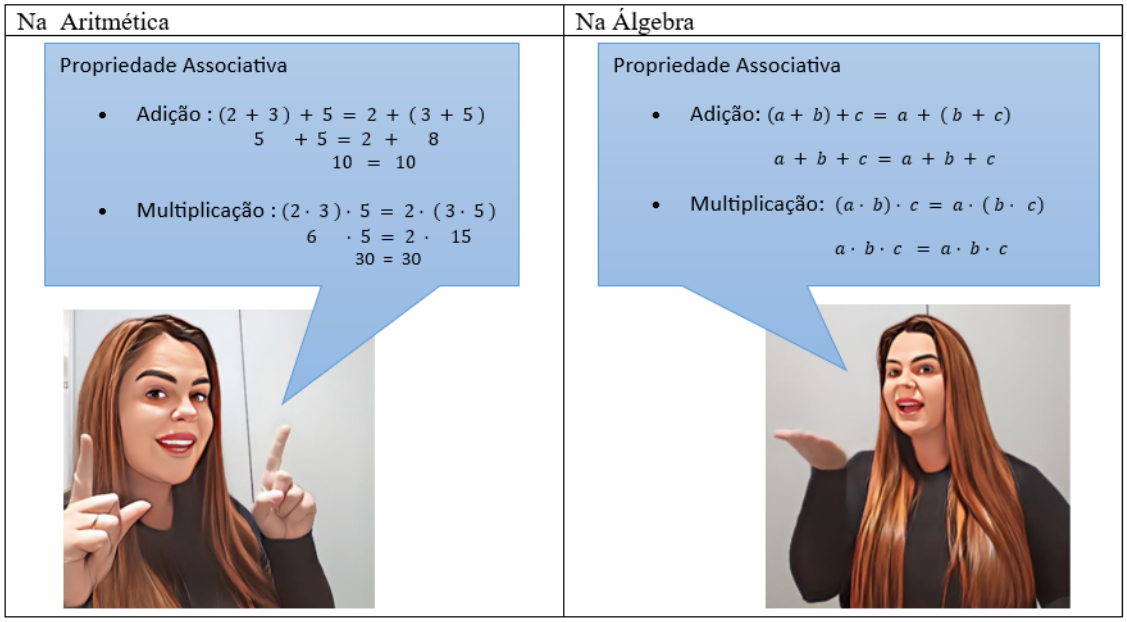
(b) As ações de colocar o chapéu e o casaco são comutativas. Sim

(c) As ações de lavar roupa e secar são comutativas. Não

*Questão 2:* Reflita se a subtração nos número inteiros é comutativa.

A subtração não é comutativa, pois $3-1=2$ e $1-3=-2$. Portanto, $3-1 \neq 1-3$.

Figura 2.2 – Propriedade Associativa




*Questão 2:* Use as propriedades dos números inteiros para escrever as expressões algébricas sem parênteses:

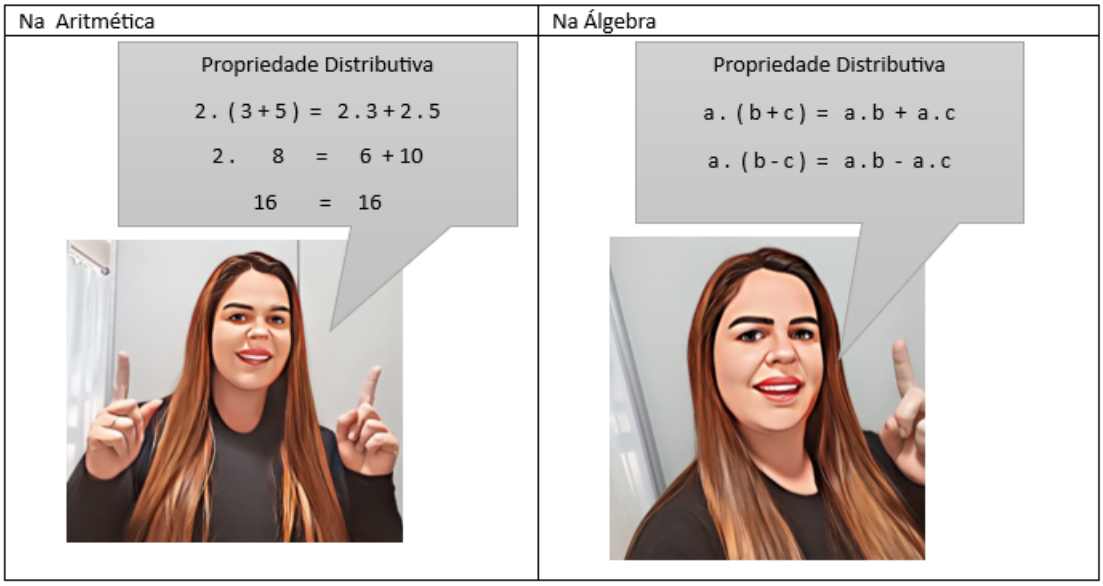
(a) $(x-1)+4 = x+3$ (propriedade associativa)

(b) $3 \cdot (5 \cdot x) = 15x$ (propriedade associativa)

(c) $(2+y)+5 = y+7$ (propriedade comutativa + propriedade associativa)

(d) $3 \cdot (x \cdot 6) = 3x+3y$ (propriedades comutativa e associativa)

Figura 2.3 – Propriedade Distributiva



*Questão 3:* Use as propriedades dos números inteiros para escrever as expressões algébricas sem parênteses:

(a) $4(x-1) = 4x - 4$ (propriedade associativa)

(b) $5(2a+1) = 10a + 5$ (propriedades distributiva e associativa)

(c) $4(2+b) + 5 = 13 + b$ (propriedades distributiva, comutativa e associativa)

(d) $3(x+2)+2(2y-1) = 3x+4y+4$ (propriedades distributiva, comutativa e associativa)

*Questão 4:* Use as propriedades dos números inteiros para simplificar as expressões algébricas:

(a) $2x + 4x = 6x$ (propriedade distributiva)

(b) $-y + 1 + 3y = 1 + 2y$ (propriedades comutativa e distributiva)

(c) $3a - 6a - a = -4a$ (propriedade distributiva e associativa)

(d) $4z + 5 + 2 + 2z = 6z + 7$ (propriedades associativa, comutativa e distributiva)

Figura 2.4 – Elemento neutro

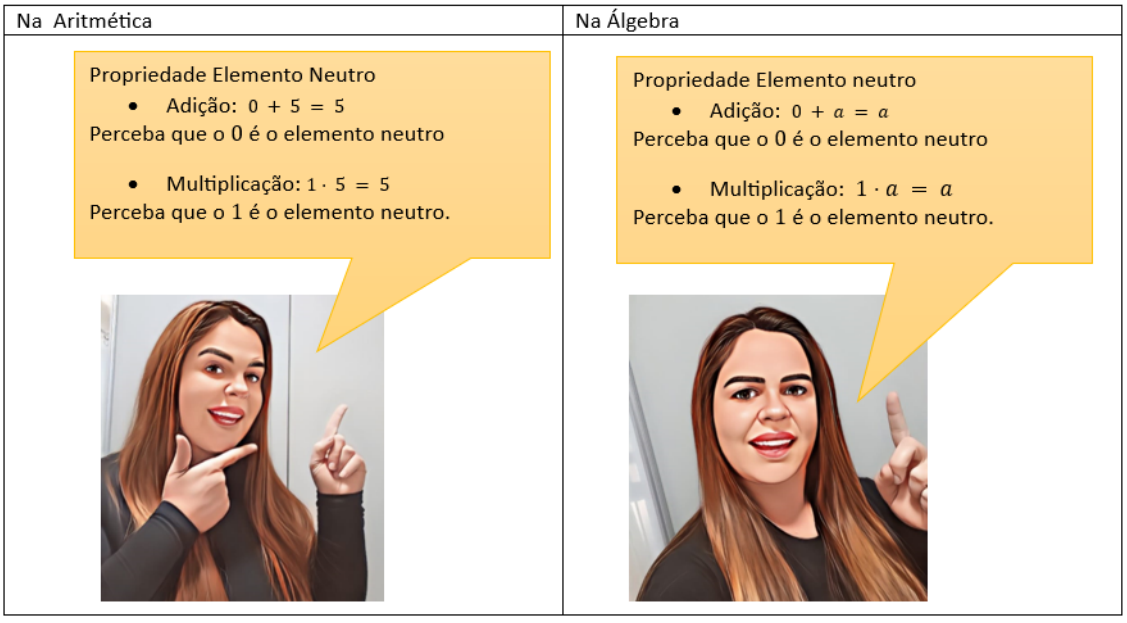
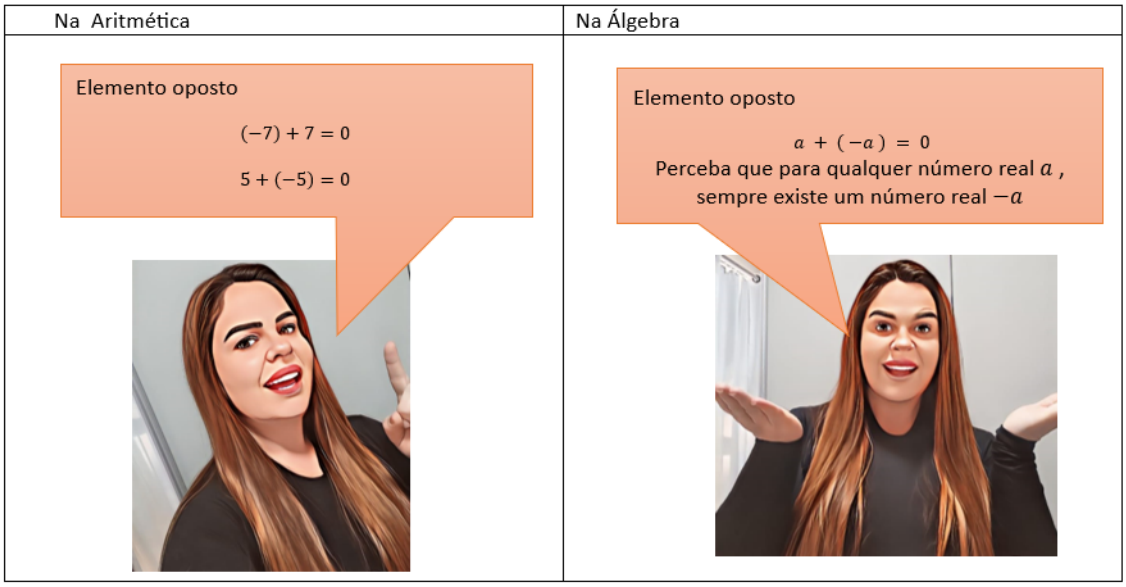


Figura 2.5 – Elemento oposto




*Questão 5:* Use as propriedades dos números inteiros para simplificar as expressões algébricas:

(a) $a^2 - a(a+b) = -ab$ (propriedade distributiva + elemento oposto)

(b) $-xy + x(1+y) = x$ (propriedade distributiva + elemento oposto)

(c) $1(a+b)-1(a+b) = 0$ (propriedade distributiva + associativa+comutativa+elemento oposto+elemento neutro)

(d) $-2a + 4 + 1(2a-3) = 1$ (propriedade distributiva + associativa + comutativa + elemento oposto + elemento neutro)

**Observação:** Nas questões acima, apresentamos as propriedades utilizadas para a compreensão do professor. Entretanto, não é necessário que o aluno identifique os nomes das propriedades. O foco não está na memorização dos nomes das propriedades, mas sim em desenvolver a habilidade de trabalhar com letras (variáveis), da mesma forma que ele já fazia com números.

## Proposta 02: Estudo das operações com polinômios

A adição e a subtração de polinômios exigem a combinação adequada de termos semelhantes, enquanto a multiplicação envolve a distribuição de cada termo de um polinômio sobre todos os termos do outro polinômio.

Já vimos que monômios de uma variável, na variável $x$, são expressões algébricas como

$$5 \qquad 2x \qquad -6x^2 \qquad 31x^3 \qquad -12x^6 \qquad -x^{11}$$

Ou seja, um monômio pode ser um número ou uma expressão algébrica que represente apenas multiplicações de números e potências naturais $x$.

Além disso, vimos que polinômios na variável $x$ são expressões algébricas como

$$5 \qquad -4x \qquad 2x-1 \qquad 3x^2-4x+1 \qquad -5x^4+10x \qquad -3x^5-6x^3-2x^2+1$$

Ou seja, polinômios são somas finitas de monômios (*poli=vários*).

**Observação:** Para o Ensino Médio é importante adicionar a seguinte definição:

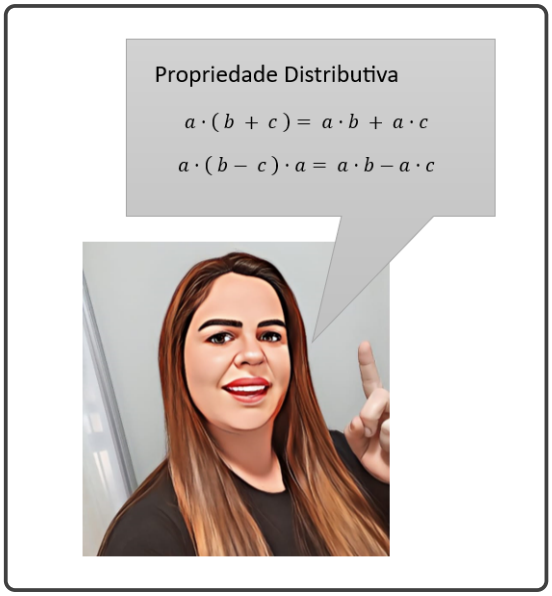
De modo geral, um polinômio na variável $x$ é uma expressão da forma

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0,$$

em que $a_n, a_{n-1}, \cdots, a_1$ e $a_0$ são números reais ou complexos denominados coeficientes.

### Adição e Subtração de monômios

Aplicando a propriedade distributiva da multiplicação em relação à adição, podemos adicionar e subtrair monômios semelhantes.




Observe os exemplos:

- $3x + 5x = (3 + 5)x = 8x$
- $12x^2 - 3x^2 = (12 - 3)x^2 = 9x^2$
- $-x^5 - 7x^5 = (-1 - 7)x^5 = -8x^5$

### Adição e Subtração de polinômios

Denominamos soma de dois ou mais polinômios ao polinômio que se obtém adicionando todos os termos semelhantes dos polinômios dados. Observe os exemplos:

- Se $p(x) = 3x + 12x^2$ e $q(x) = 5x - 3x^2$, então

$$\begin{aligned} p(x) + q(x) &= (3x + 12x^2) + (5x - 3x^2) \\ &= 3x + 5x + 12x^2 - 3x^2 \\ &= (3 + 5)x + (12 - 3)x^2 \\ &= 8x + 9x^2. \end{aligned}$$

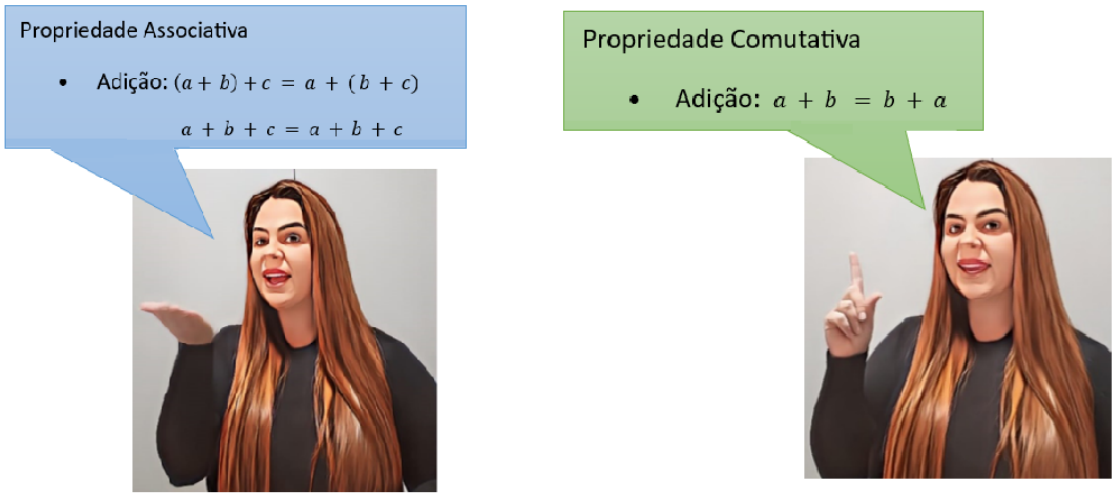
- Se $p(x) = 3x^2 - 5x + 8$ e $q(x) = 2x^3 + 5x^2 - 2x - 9$, então

$$\begin{aligned} p(x) + q(x) &= (3x^2 - 5x + 8) + (2x^3 + 5x^2 - 2x - 9) \\ &= (0x^3 + 3x^2 - 5x + 8) + (2x^3 + 5x^2 - 2x - 9) \\ &= 0x^3 + 2x^3 + 3x^2 + 5x^2 - 5x - 2x + 8 - 9 \\ &= (0 + 2)x^3 + (3 + 5)x^2 + (-5 - 2)x + (8 - 9) \\ &= 2x^3 + 8x^2 - 7x - 1 \end{aligned}$$

- Se $p(x) = -x^5 + 2x - 1$ e $q(x) = -7x^5 + 4x^3 + 2$, então

$$\begin{aligned} p(x) + q(x) &= (-x^5 + 2x - 1) + (-7x^5 + 4x^3 + 2) \\ &= (-x^5 + 0x^3 + 2x - 1) + (-7x^5 + 4x^3 + 0x + 2) \\ &= -x^5 + (-7x^5) + 4x^3 + 0x^3 + 2x + 0x + (-1) + 2 \\ &= (-1 - 7)x^5 + (4 + 0)x^3 + (2 + 0)x + (-1 + 2) \\ &= -8x^5 + 4x^3 + 2x + 1. \end{aligned}$$

Percebam que para efetuar a adição de polinômios usamos as propriedades associativa e comutativa da adição, além da distributiva para adicionar os termos semelhantes.




**Observação:** Para os alunos do Ensino Médio deve-se adicionar a seguinte definição:

Considere dois polinômios $p(x)$ e $q(x)$, sendo eles na forma:

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0$$

e

$$q(x) = b_n x^n + b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \cdots + b_1 x + b_0.$$

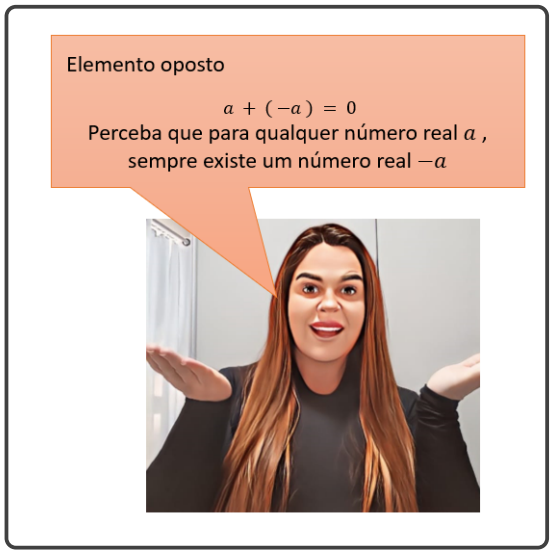
Define-se a adição $p(x) + q(x)$ como

$$p(x) + q(x) = (a_n + b_n)x^n + (a_{n-1} + b_{n-1})x^{n-1} + \cdots + (a_1 + b_1)x + (a_0 + b_0)$$

Pode-se também definir a subtração entre dois polinômios $p(x)$ e $q(x)$ por

$$p(x) - q(x) = p(x) + (-q(x)),$$

em que $-q(x)$ é o polinômio oposto de $q(x)$.




Observe os seguintes exemplos: Se $p(x) = 3x^2 - 5x + 8$ e $a(x) = 2x^3 + 5x^2 - 2x - 9$, então:

$$\begin{aligned} p(x) - q(x) &= (3x^2 - 5x + 8) - (2x^3 + 5x^2 - 2x - 9) \\ &= -2x^3 + (3-5)x^2 + (-5-(-2))x + (8-(-9)) \\ &= -2x^3 - 2x^2 - 3x + 17 \end{aligned}$$

e

$$\begin{aligned} q(x) - p(x) &= (2x^3 + 5x^2 - 2x - 9) - (3x^2 - 5x + 8) \\ &= 2x^3 + (5-3)x^2 + (-2-(-5))x + (-9-8) \\ &= 2x^3 + 2x^2 + 3x - 17 \end{aligned}$$

Observe que, assim como nos inteiros, a subtração de polinômios não é comutativa, pois no exemplo acima temos que $p(x) - q(x) \neq q(x) - p(x)$.

**Observação:** Para os alunos do Ensino Médio pode-se adicionar a seguinte definição:

Considere dois polinômios $p(x)$ e $q(x)$, sendo eles na forma

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0$$

e

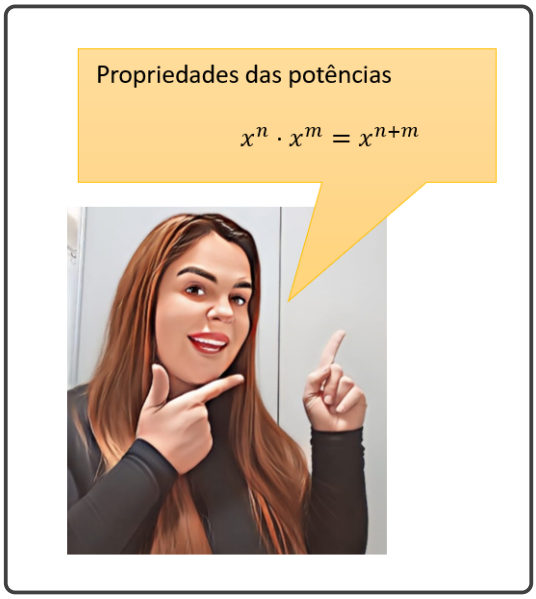
$$q(x) = b_n x^n + b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \cdots + b_1 x + b_0.$$

Temos que a diferença (subtração) $p(x) - q(x)$ é dada por

$$p(x) - q(x) = (a_n - b_n)x^n + (a_{n-1} - b_{n-1})x^{n-1} + \cdots + (a_1 - b_1)x + (a_0 - b_0)$$

### Multiplicação de monômios

Aplicando a propriedade da potenciação da figura abaixo podemos multiplicar monômios.




Observe os seguintes exemplos:

- $x^7 \cdot (3x^7) = 3x^{7+7} = 3x^{14}$
- $(3x^3)\cdot(5x^2) = 3\cdot5\cdot x^3\cdot x^2 = 15\cdot x^{3+2} = 15x^5$
- $(12x) \cdot (-3x^5) = 12 \cdot (-3) \cdot x^1 \cdot x^5 = -36x^{1+5} = -36x^6$

### Multiplicação de polinômios

Para efetuar a multiplicação de dois ou mais polinômios, utilizamos a propriedade distributiva da multiplicação em relação à adição. Devemos multiplicar dois a dois todos os termos do primeiro polinômio com todos os termos do segundo. Veja exemplos:

- Se $p(x) = 3x + 5$ e $q(x) = x^3 + 2x - 3$, então

$$\begin{aligned} p(x) \cdot q(x) &= (3x+5) \cdot (x^3 + 2x - 3) \\ &= 3x \cdot x^3 + 3x \cdot 2x + 3x \cdot (-3) + 5 \cdot x^3 + 5 \cdot 2x + 5 \cdot (-3) \\ &= 3x^4 + 6x^2 - 9x + 5x^3 + 10x - 15 \\ &= 3x^4 + 5x^3 + 6x^2 + (-9+10)x - 15 \\ &= 3x^4 + 5x^3 + 6x^2 + x - 15 \end{aligned}$$

- Se $p(x) = 2x^2 + 3x + 1$ e $q(x) = 4x^4 - x^2$, então

$$\begin{aligned} p(x) \cdot q(x) &= (2x^2 + 3x + 1) \cdot (4x^4 - x^2) \\ &= 2x^2 \cdot 4x^4 + 2x^2 \cdot (-x^2) + 3x \cdot 4x^4 + 3x \cdot (-x^2) + 1 \cdot 4x^4 + 1 \cdot (-x^2) \\ &= 8x^6 - 2x^4 + 12x^5 - 3x^3 + 4x^4 - x^2 \\ &= 8x^6 + 12x^5 + (-2+4)x^4 - 3x^3 - x^2 \\ &= 8x^6 + 12x^5 + 2x^4 - 3x^3 - x^2 \end{aligned}$$

**Observação:** Note que se $\text{gr}(p)$ é grau de $p(x)$ e $\text{gr}(q)$ é grau de $q(x)$, então $\text{gr}(p \cdot q) = \text{gr}(p) + \text{gr}(q)(p)$.

### Atividade de Fixação

*Questão 1:* Considere os polinômios $p(x) = 2x^3 + 3x^2 - 7$ e $q(x) = x^2 + 5x + 3$.

(a) Determine $p(x) + q(x)$ , apresente a resposta em sua forma simplificada.

Resolução:

$$\begin{aligned} p(x) + q(x) &= (2x^3 + 3x^2 - 7) + (x^2 + 5x + 3) \\ &= 2x^3 + 3x^2 + x^2 + 5x - 7 + 3 \\ &= 2x^3 + (3+1)x^2 + 5x + (-7+3) \\ &= 2x^3 + 4x^2 + 5x - 4. \end{aligned}$$

(b) Determine $p(x) - q(x)$ , apresente a resposta em sua forma simplificada.

Resolução:

$$\begin{aligned} p(x) - q(x) &= (2x^3 + 3x^2 - 7) - (x^2 + 5x + 3) \\ &= 2x^3 + 3x^2 - 7 - x^2 - 5x - 3 \\ &= 2x^3 + (3-1)x^2 - 5x + (-7-3) \\ &= 2x^3 + 2x^2 - 5x - 10. \end{aligned}$$

*Questão 2:* Calcule o produto dos polinômios $p(x) = 3x^2 + 1$ e $q(x) = x^3 - 3x$, em seguida, apresente a resposta em sua forma simplificada.

Resolução:

$$\begin{aligned} p(x) \cdot q(x) &= (3x^2 + 1) \cdot (x^3 - 3x) \\ &= 3x^2 \cdot x^3 + 3x^2 \cdot (-3x) + 1 \cdot x^3 + 1 \cdot (-3x) \\ &= 3x^5 - 9x^3 + x^3 - 3x \\ &= 3x^5 + (-9+1)x^3 - 3x \\ &= 3x^5 - 8x^3 - 3x. \end{aligned}$$

## Proposta 03: Fatoração de polinômios

Por meio desta atividade, pretendemos resgatar os conhecimentos já adquiridos em anos anteriores, especificamente em relação à fatoração de números naturais, e relacioná-los à fatoração de expressões algébricas. Visto que fatorar uma expressão algébrica significa transformá-la em um produto de fatores, ampliaremos os estudos sobre operações com polinômios. Estudaremos alguns casos de fatoração de expressões algébricas, tais como: fator comum em evidência, agrupamento, diferença de dois quadrados e trinômio quadrado perfeito.

**Fatoração de números naturais:** Os números primos, ao mesmo tempo tão simples e essenciais, possuem a capacidade de gerar todos os números naturais maiores que 1.

Vocês já aprenderam que fatorar um número natural ou inteiro consiste em escrevê-lo como um produto de dois ou mais fatores primos. Vamos relembrar esse conceito, fatorando o número 60.

$$60 \div 2 = 30$$

$$30 \div 2 = 15$$

$$15 \div 3 = 5$$

$$5 \div 5 = 1.$$

Assim,

$$60 = 2^2 \cdot 3 \cdot 5.$$

**Observação:** Professor, lembre que de acordo com o Teorema Fundamental da Aritmética temos o seguinte resultado:

> Todo número natural maior do que 1 ou é primo ou se escreve de modo único (a menos da ordem de fatores) como um produto de fatores primos,
>
> $$p = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n},$$
>
> em que $p_i$ são números primos e $\alpha_i$ são números naturais.

Vocês já perceberam que a fatoração pode ser utilizada para simplificar uma divisão? Veja o exemplo a seguir:

$$\frac{60}{15} = \frac{2^2 \cdot 3 \cdot 5}{3 \cdot 5} = 2^2 = 4.$$

**Fatoração algébrica para auxiliar a simplificação de expressões racionais**

É possível realizar a fatoração de uma expressão racional, como vemos na quociente entre dois monômios:

$$\frac{60x^2y^3}{15xy^2} = \frac{2^2 \cdot 3 \cdot 5 \cdot x \cdot x \cdot y \cdot y \cdot y}{3 \cdot x \cdot y \cdot y} = 2^2 \cdot x \cdot y = 4xy.$$

Observe que utilizamos a fatoração para efetuar a divisão entre monômios.

Apresentaremos a seguir as regras que podemos utilizar para realizar esse cálculo de maneira simplificada.

Na divisão de monômios, realizamos a divisão dos coeficientes do numerador pelo coeficiente do denominador. Ao lidarmos com a parte algébrica, utilizamos a regra da potenciação quando as bases são iguais. Dessa forma, ao dividirmos $x^2$ por $x$, mantemos a letra $x$ como base e subtraímos os expoentes. Da mesma forma, ao dividirmos $y^3$ por $y^2$, conservamos a letra e subtraímos os expoentes.

**Fatoração de Polinômios**

De acordo com o dicionário, encontramos o significado da palavra "fatorar".

- ✓ Na Aritmética: decompor (um número) em seus fatores primos.
- ✓ Na Álgebra: decompor (um polinômio) em um produto de fatores irredutíveis.

Com base nessas informações, vamos adquirir conhecimento sobre alguns tipos distintos de fatoração de polinômios.

**Fator Comum em evidência**

Quando uma expressão algébrica apresenta um fator comum em todos os seus termos, é possível colocá-lo em evidência, obtendo uma forma fatorada do polinômio.

Há duas dicas importantes a serem consideradas:

- ✓ Para encontrar o fator comum entre os coeficientes, é recomendado calcular o máximo divisor comum (mdc) entre eles. Dessa forma, é possível identificar o maior divisor comum que divide todos os coeficientes.
- ✓ No caso do fator comum na parte literal, quando as letras são iguais, devemos selecionar aquela com o menor expoente para evidenciá-la.

Veja o exemplo a seguir: Dada a expressão

$$18x^5 - 24x^3 + 12x^2 - 6x^6$$

temos que o mdc dos coeficientes é

$$\text{mdc}(18, 24, 12, 6) = 6.$$

Ao identificarmos as letras comuns, devemos selecionar aquela que possui o expoente menor, neste caso é $x^2$.

Dessa forma, o fator a ser evidenciado é determinado por $6x^2$.

O fator comum deve ser escrito fora dos parênteses. Em seguida, é necessário dividir cada termo do polinômio pelo fator comum. O resultado dessa divisão deve ser colocado dentro dos parênteses.

$$18x^5 - 24x^3 + 12x^2 - 6x^6 = 6x^2(3x^3 - 4x + 2 - x^4).$$

Podemos empregar a propriedade distributiva na resposta final como um meio concreto para verificar a correção do resultado.

**Agrupamento**

Conforme o próprio termo "agrupamento" sugere, essa técnica é utilizada quando a expressão algébrica apresenta grupos de termos que podem ser combinados devido a fatores em comum. Além disso, ao fatorar cada grupo, esses grupos revelam um novo fator comum, que pode ser identificado, finalizando assim o processo de fatoração.

Como exemplo, vamos fatorar a expressão a seguir:

$$ab + 3b - 7a - 21.$$

Observem que $ab + 3b = b(a + 3)$ e $-7a - 21 = -7(a + 3)$, sendo assim,

$$ab + 3b - 7a - 21 = b(a + 3) - 7(a + 3).$$

Dessa forma, constatamos a presença de um novo fator comum: $a + 3$. Ao evidenciá-lo, obtemos:

$$ab + 3b - 7a - 21 = b(a + 3) - 7(a + 3) = (a + 3) \cdot (b - 7).$$

Novamente, podemos empregar a propriedade distributiva na resposta final como um meio concreto para verificar a correção do resultado.

**Diferença entre Quadrados**

A forma fatorada da diferença de dois quadrados segue a regra do produto da soma pela diferença das bases, na ordem dada. Aqui está um exemplo:

$$a^2 - b^2 = (a + b)(a - b).$$

É importante notar que essa fatoração é aplicada nas seguintes condições:

- A expressão é um binômio;
- Há um sinal de "subtração" entre os termos.
- Para resolver, é necessário extrair a raiz quadrada dos termos e, em seguida, seguir a regra como apresentada no exemplo.

Vamos fatorar a expressão a seguir:

$$x^2 - 16 = (x + 4)(x - 4).$$

Empregamos a propriedade distributiva na resposta final como um meio concreto para verificar a correção do resultado.

### Trinômio Quadrado Perfeito

Esse procedimento é aplicado para fatorar ou decompor expressões algébricas que são trinômios quadrados perfeitos.

Um trinômio é chamado de trinômio quadrado perfeito, pois é igual ao quadrado de um binômio. Em outras palavras, é um trinômio que pode ser escrito na forma $(a+b)^2$ ou na forma $(a-b)^2$, em que $a$ e $b$ são termos ou coeficientes.

Analisem os exemplos a seguir:

$$(a + b)^2 = a^2 + 2ab + b^2$$

$$(a - b)^2 = a^2 - 2ab + b^2$$

Identificamos um trinômio quadrado perfeito e obtemos a sua forma fatorada ao observarmos os seguintes aspectos:

- ✓ O trinômio é composto por três termos.
- ✓ Dois dos termos são quadrados perfeitos ($a^2$ e $b^2$)
- ✓ O terceiro termo é equivalente a "mais" ou "menos" duas vezes o produto das bases desses quadrados.

Vamos analisar mais um exemplo e responder algumas perguntas.

$$x^2 - 16x + 64.$$

1. Possui três termos?
   Resposta: Sim.

2. Quais desses termos são quadrados perfeitos?
   Resposta: Sim, $x^2$ e $64$.

3. Quais são as bases desses quadrados perfeitos?
   Resposta: $x$ e $8$.

4. Se multiplicarmos por dois os resultados dos termos anteriores, obtemos o resultado do termo que não é um quadrado perfeito?
   Resposta: Sim, pois $2 \cdot x \cdot 8 = 16x$, o termo que não teve a raiz extraída.

Se todas as respostas forem "Sim", significa que é um trinômio quadrado perfeito. Vamos para a solução.

1. Abra parênteses e escreva a base de um dos quadrados perfeitos.

2. Utilize o sinal do termo que não é um quadrado perfeito.

3. Escreva a base do outro quadrado perfeito e feche os parênteses.

4. Eleve tudo ao quadrado.

Sendo assim:

$$x^2 - 16x + 64 = (x - 8)^2.$$

**Simplificação de Frações Algébricas**

As simplificações algébricas podem desempenhar um papel relevante na divisão de polinômios.

Embora a simplificação algébrica não seja diretamente uma forma de dividir polinômios, ela tem o potencial de simplificar as expressões utilizadas na divisão e tornar o processo mais acessível.

Observem os exemplos de simplificação de algumas expressões:

- $\dfrac{35}{7a - 7x} = \dfrac{7 \cdot 5}{7(a - x)} = \dfrac{5}{(a - x)}$;
- $\dfrac{15a + 5b}{3a + b} = \dfrac{5(3a + b)}{3a + b} = 5$;
- $\dfrac{x^2 - 9}{x^2 - 6x + 9} = \dfrac{(x + 3)(x - 3)}{(x - 3)(x - 3)} = \dfrac{(x + 3)}{(x - 3)}$;
- $\dfrac{a^2 + 8a}{ab + 8b + a + 8} = \dfrac{a(a + 8)}{b(a + 8) + 1(a + 8)} = \dfrac{a(a + 8)}{(a + 8)(b + 1)} = \dfrac{a}{b + 1}$.

## Proposta 04: Desafio de Fatoração em um Jogo de Perguntas e Respostas

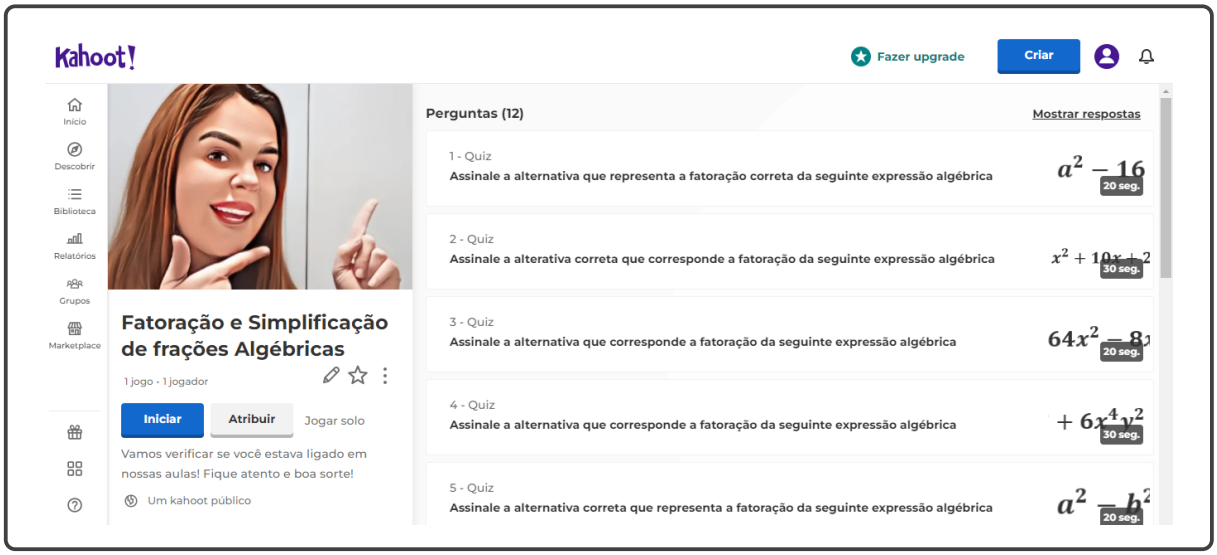
Essa atividade adota uma abordagem investigativa com o objetivo de avaliar o nível de compreensão dos estudantes em relação ao conteúdo relacionado à fatoração algébrica. A meta é fornecer ao professor a oportunidade de avaliar o aprendizado dos alunos em relação à fatoração de expressões algébricas.

Para esta atividade, empregaremos a plataforma Kahoot!. Trata-se de um ambiente educacional fundamentado em jogos, consistindo em questionários de múltipla escolha que possibilitam a criação por parte dos usuários. Estes questionários podem ser acessados via navegador web ou pela aplicação Kahoot. A plataforma pode ser utilizada como ferramenta didática nas escolas, seja para a revisão do conhecimento dos estudantes, para avaliação formativa ou como uma pausa nas atividades tradicionais da sala de aula. Portanto, esta atividade deverá ser realizada num laboratório de informática.

Professor, você deverá acessar o seguinte link da atividade: https://create.kahoot.it/share/fatoracao-e-divisao-algebrica/dda2e8b1-f64b-4be5-a225-9d3eecbeecff

A visão que o professor terá ao acessar o link acima, é representado pela Figura 2.6.

Figura 2.6 – Visão do professor ao acessar o site Kahoot

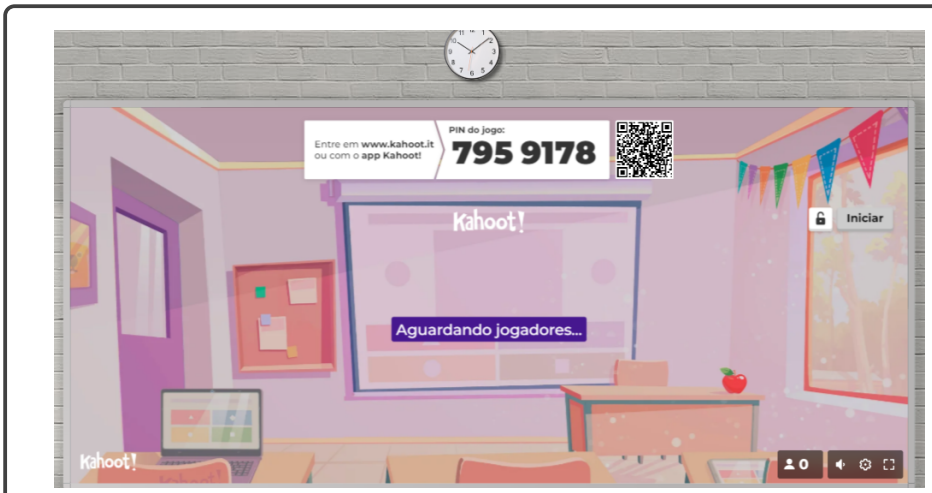



Após clicar no botão iniciar surgirá na tela uma imagem como ilustrada pela Figura 2.7.

Figura 2.7 – Visão do professor ao iniciar o jogo

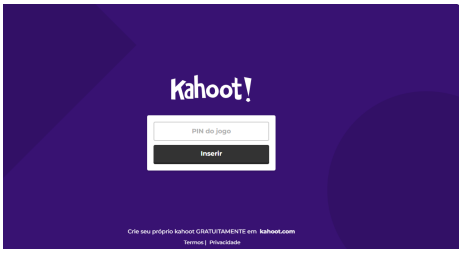

O professor pode escolher entre o modo clássico, no qual os alunos jogam individualmente, ou o modo em equipe, onde os alunos jogam em grupos. Após a escolha, uma nova tela será exibida com o código PIN do jogo, que os alunos deverão digitar em seus computadores, como mostrado na Figura 2.8.

Figura 2.8 – Número PIN do jogo.



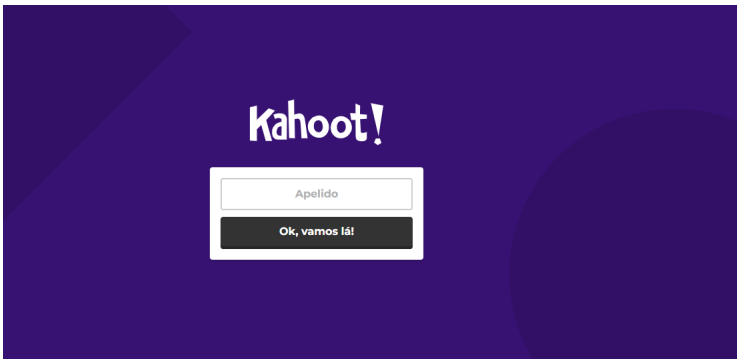

Os alunos deverão acessar link: https://kahoot.it/. Uma vez que os estudantes acessem o link, uma imagem será exibida em suas telas, como ilustrado na Figura 2.9. Nessa tela, os alunos devem inserir o número PIN do jogo.

Figura 2.9 – PIN



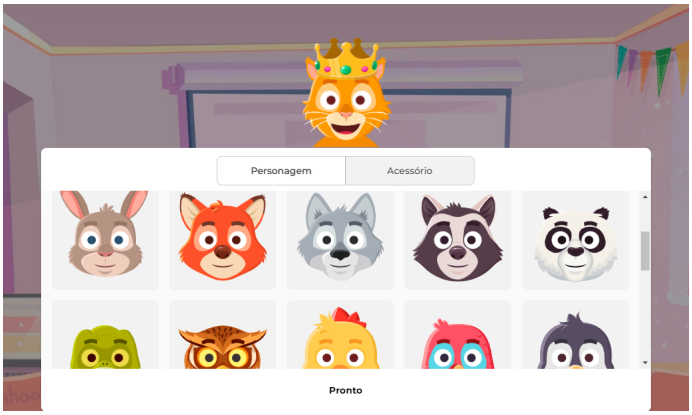

Posteriormente, os alunos serão solicitados a criar um nome ou apelido para participar do jogo. Para isso, eles verão a Figura 2.10 em suas telas.

Figura 2.10 – Aluno insere nome ou apelido




Logo depois, os alunos têm a opção de personalizar seu avatar no jogo. Para fazer isso, basta clicar no ícone de lápis e escolher o avatar desejado, conforme ilustrado na Figura 2.11.

Figura 2.11 – Escolha do Avatar



### O Jogo

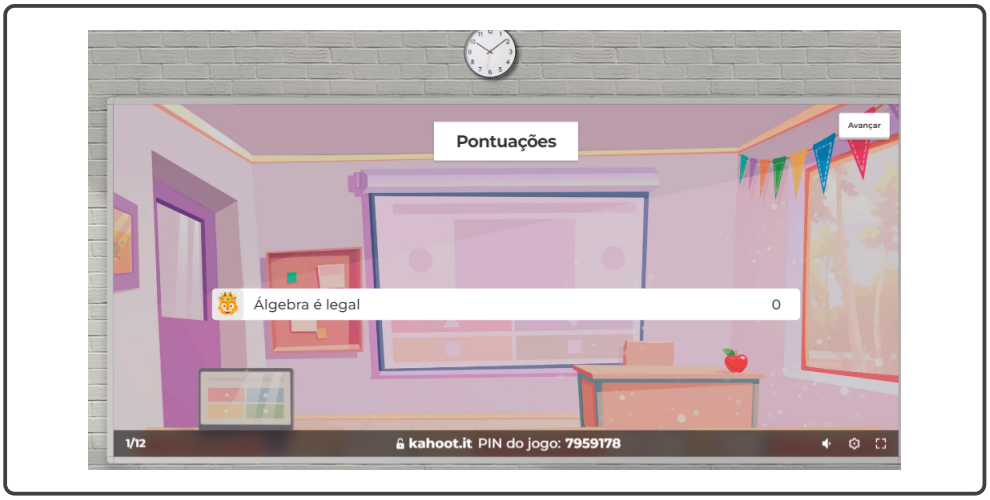
Quando todos os alunos estiverem na seção, o professor deve clicar no botão “Iniciar”, conforme demonstrado na Figura 2.12.

Figura 2.12 – Iniciaando o jogo.


Fonte: Acervo da Autora

A cada questão, a pontuação dos jogadores com a melhor classificação é exibida, como ilustrado na Figura. 2.13. Durante o jogo, os alunos acumulam pontos ao fornecerem respostas corretas e rápidas. Aqueles que respondem de forma precisa e ágil obtêm mais pontos. No entanto, cometer erros ou não responder dentro do prazo estabelecido não resulta em pontuação. Nesse contexto, é relevante destacar a importância tanto da precisão quanto da agilidade na conquista de pontos.

Figura 2.13 – Classificação por pontuação




Fonte: Acervo da Autora

### Questões do jogo

*Questão 01:* Assinale a alternativa que representa a fatoração correta da seguinte expressão algébrica

$$a^2 - 16.$$

Aternativas:

( ) $(a+4)(a-4)$ (resposta correta)

( ) $a^2 - 8a + 4$

( ) $(a+8)(a-8)$

( ) $a^2 - 4a + 16$

Os alunos terão o tempo de 60 segundos para resolver e a valor da pontuação será Padrão.

*Questão 02:* Assinale a alternativa que representa a fatoração correta da seguinte expressão algébrica

$$x^2 + 10x + 25.$$

Alternativas:

( ) $(x+5)(x-5)$

( ) $(x+25)^2$

( ) $5(2x+5)$

( ) $(x+5)^2$ (resposta correta)

Os alunos terão o tempo de 90 segundos para resolver a questão. O valor da pontuação é Padrão.

*Questão 03:* Assinale a alternativa que representa a fatoração correta da seguinte expressão algébrica

$$64x^2 - 8x.$$

Alternativas:

( ) $8x(8x-0)$

( ) $(8x+1)(8x-1)$

( ) $8x(8x-1)$ (resposta correta)

( ) $4(16x+2)$

Os alunos terão o tempo de resolução de 90 segundos. A pontuação é Padrão.

*Questão 04:* Assinale a alternativa que representa a fatoração correta da seguinte expressão algébrica

$$12x^2y^3 + 6x^4y^2 + 18xy^4.$$

Alternativas:

( ) $12x^2y^3(2 + x^2y + 3y)$

( ) $18xy(xy^2 + x^3y + y^3)$

( ) $6xy^2(2xy + x^3 + 3y^2)$ (resposta correta)

( ) $2xy(6xy^2 + 3x^2y + 9xy^3)$

Os alunos terão o tempo de 90 segundos para resolver a questão e a sua pontuação será Padrão.

*Questão 05:* Assinale a alternativa que representa a fatoração correta da seguinte expressão algébrica

$$a^2 - b^2.$$

Alternativas:

( ) $(a + b)^2$

( ) $(a - b)^2$

( ) $ab(a - b)$

( ) $(a + b)(a - b)$ (resposta correta)

Os alunos terão o tempo para resolver é de 60 segundos e a sua pontuação é Padrão.

*Questão 06:* Assinale a alternativa que representa a fatoração correta da seguinte expressão algébrica

$$a^2 - 2ab + b^2.$$

Alternativas:

( ) $(a + b)(a - b)$

( ) $ab(a - b)$

( ) $(a - b)^2$ (resposta correta)

( ) $(a + b)^2$

Os alunos terão o tempo de 90 segundos para responder a questão e a pontuação é Padrão.

*Questão 07:* Assinale a alternativa que representa a fatoração correta da seguinte expressão algébrica

$$4x^2 - 1.$$

Alternativas:

( ) $(2x-1)^2$

( ) $(2x+1)^2$

( ) $2x(2x-1)$

( ) $(2x-1)(2x+1)$ (resposta correta)

Os alunos terão o tempo de resolução de 90 segundos e a pontuação é Padrão.

*Questão 08:* Assinale a alternativa que representa a fatoração correta da seguinte expressão algébrica

$$4x^2 + 4x + 1.$$

Alternativas:

( ) $(2x-1)(2x-1)$

( ) $2x(2x+1)$

( ) $(2x+1)(2x+1)$ (resposta correta)

( ) $(2x-1)^2$

Os alunos terão o tempo de 90 segundos para resolver e a pontuação é Padrão.

*Questão 09:* Assinale a alternativa que representa a fatoração correta da seguinte expressão algébrica

$$\frac{4x^2 - 1}{4x^2 + 4x + 1}.$$

Alternativas:

( ) $\frac{2x+1}{x}$

( ) $\frac{2x+1}{2x-1}$

( ) $\frac{2x-1}{2x+1}$ (resposta correta)

( ) $\frac{1}{2x+1}$

Os alunos terão o tempo de 120 segundos para resolver e a sua pontuação é Padrão.

*Questão 10:* Assinale a alternativa que representa a fatoração correta da seguinte expressão algébrica

$$\frac{a^2 - b^2}{a^2 - 2ab + b^2}.$$

Alternativas:

( ) $\dfrac{a+b}{a}$

( ) $\dfrac{1}{a+b}$

( ) $\dfrac{a-b}{a+b}$

( ) $\dfrac{a+b}{a-b}$ (resposta correta)

Os alunos terão o tempo de 120 segundos para resolução e a pontuação é Padrão.

*Questão 11:* Assinale a alternativa que representa a fatoração correta da seguinte expressão algébrica

$$\frac{(a+b)^2 - 4ab}{a^2 - b^2}.$$

Alternativas:

( ) $\dfrac{a+b}{a}$

( ) $\dfrac{a+b}{a-b}$

( ) $\dfrac{a-b}{a+b}$ (resposta correta)

( ) $\dfrac{1}{a+b}$

Os alunos terão o tempo de 180 segundos para solucionar e a pontuação é Dupla.

*Questão 12:* Assinale a alternativa que representa a fatoração correta da seguinte expressão algébrica

$$\frac{x^2 - 5x}{x^2 - 25}.$$

Alternativas:

( ) $\dfrac{x-5}{x+5}$

( ) $\dfrac{x(x-5)}{x+5}$

( ) $\dfrac{x}{x+5}$ (resposta correta)

( ) $\dfrac{x}{x-5}$

Os alunos terão o tempo de 120 segundos para resolver e a pontuação é padrão.

Ao término do jogo, teremos um pódio que exibirá a colocação dos três destaques da partida, como ilustrado na Figura. 2.14.

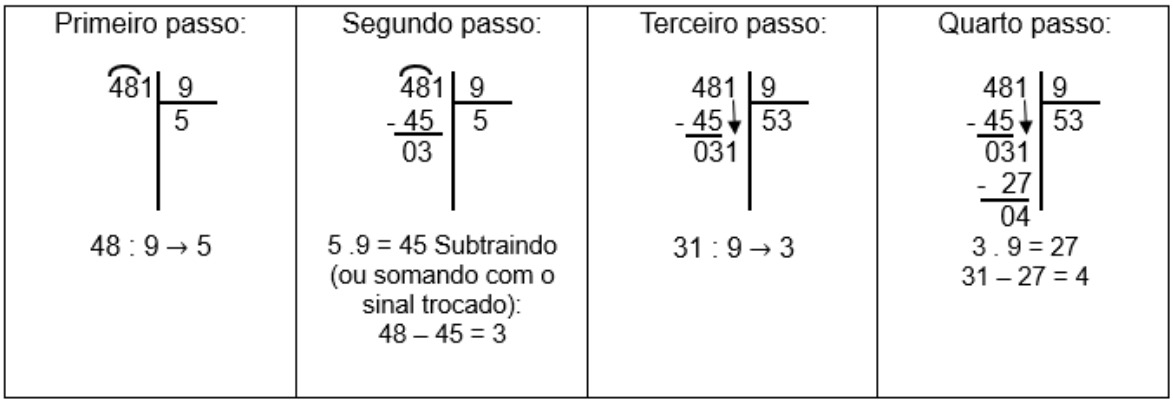
Figura 2.14 – Pódio


Fonte: Acervo da Autora

## Proposta 05: Divisão de polinômios pelo método da chave, aplicação na terceira série do Ensino Médio

Antes de iniciarmos a divisão entre polinômios vamos lembrar como resolvemos a divisão empregando nos números inteiros. Consideremos a seguinte divisão de números inteiros:

Figura 2.15 – Método da chave




Fonte: Acervo da Autora

Pela divisão acima, temos que

$$481 = 9 \cdot 53 + 4,$$

em que 481 é o dividendo, 9 é o divisor, 53 é o quociente e 4 é o resto.

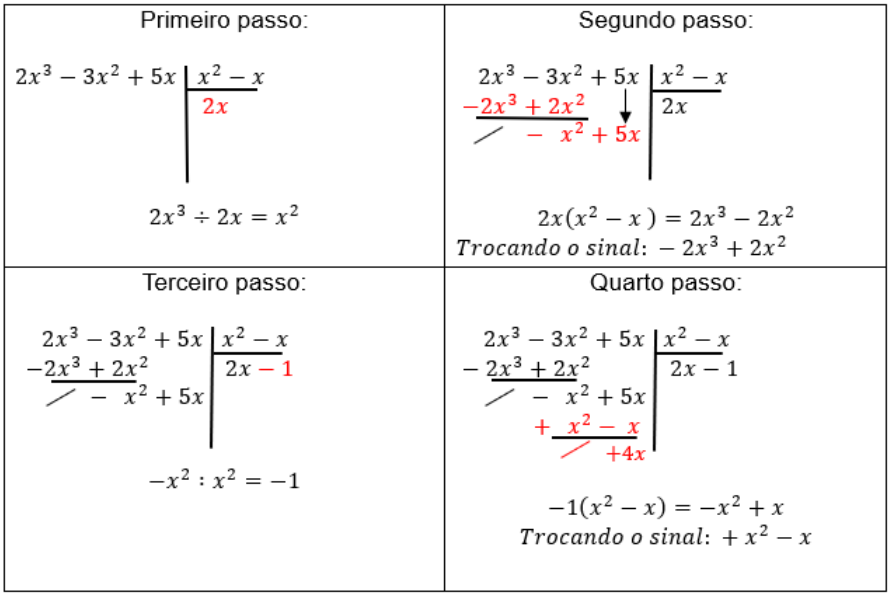
Vamos utilizar a mesma regra prática na divisão de polinômios.

Sejam $p(x)$ e $d(x)$ dois polinômios, com $d(x)$ não nulo, e gr$(p)$ o grau de $p(x)$ e d$(d)$ o grau de $d(x)$. Ao dividir $p(x)$ por $q(x)$, encontramos dois polinômios, $q(x)$, denominado quociente, e $r(x)$, denominado o resto. Esses dois polinômios devem satisfazer as seguintes condições:

- $p(x) = d(x) \cdot q(x) + r(x)$
- $r(x)$ é o polinômio nulo ou o grau de $r(x)$ deve satisfazer $0 \leq gr(r) \leq gr(d)$.

Aplicaremos o método da chave na divisão de $2x^3 - 3x^2 + 5x$ por $x^2 - x$. Veja a Figura 2.16.

Figura 2.16 – Método da chave para os polinômios

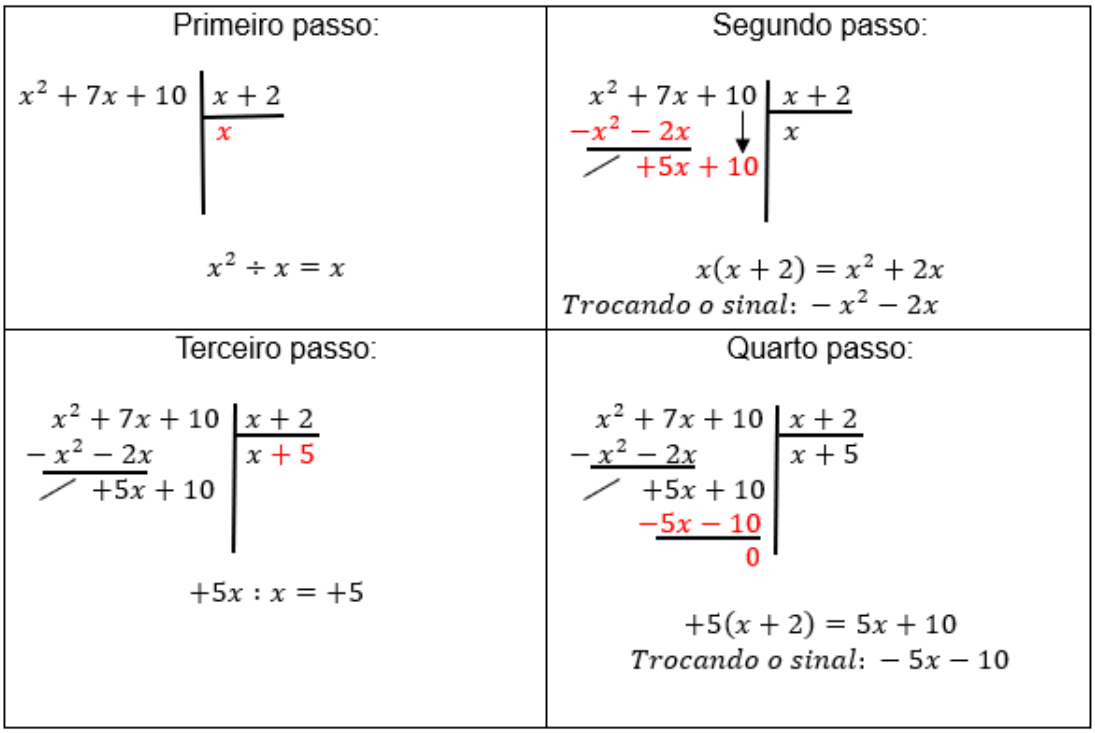



Lembre-se que $p(x) = d(x) \cdot q(x) + r(x)$. Assim,

$$2x^3 - 3x^2 + 5x = (x^2 - x) \cdot (2x - 1) + 4x.$$

Novamente, aplicaremos o método da chave na divisão de $x^2 + 7x + 10$ por $x + 2$. Veja a Figura 2.17.

Figura 2.17 – Método da chave para os polinômios



Lembre-se que $p(x) = d(x) \cdot q(x) + r(x)$. Assim,

$$x^2 + 7x + 10 = (x + 2) \cdot (x + 5) + 0.$$

Nesse caso, temos que $x^2 + 7x + 10$ é o dividendo, $x + 2$ é o divisor, $x + 5$ é o quociente e o polinômio nulo, 0, é o resto.

**Observações:**

- Quando o resto é nulo, $r(x) = 0$, dizemos que o polinômio $p(x)$ é divisível por $q(x)$, ou seja, a divisão é exata.
- O grau do quociente $q(x)$ sempre será a diferença entre os graus do dividendo $p(x)$ e do divisor $d(x)$ quando $\text{gr}(p) \geq \text{gr}(q)$.

**Atividade de Fixação**

*Questão 1:* Divida o polinômio $p(x) = 4x^2+6x-12$ pelo polinômio $q(x) = 2x-1$ utilizando o método da chave, em seguida, determine o quociente e o resto da divisão.

Resolução:

$$\begin{array}{r|l} 4x^2 + 6x - 12 & 2x - 1 \\ \underline{-\,4x^2 + 2x\phantom{\,-12}} & \overline{2x + 4} \\ \phantom{-\,4x^2 +}\ +8x - 12 & \\ \phantom{-\,4x^2 +}\ \underline{-8x + 4} & \\ \phantom{-\,4x^2 + 8x -}\ -8 & \end{array}$$

Resposta: Quociente: $2x + 4$ e Resto: $-8$.

*Questão 2:* Divida o polinômio $p(x) = 3x^2+10x-8$ pelo polinômio $q(x) = x+4$ utilizando o método da chave, em seguida, determine o quociente e o resto da divisão.

Resolução:

$$\begin{array}{r|l} 3x^2 + 10x - 8 & x + 4 \\ \underline{-\,3x^2 - 12x\phantom{\,-8}} & \overline{3x - 2} \\ \phantom{-\,3x^2 -}\ -2x - 8 & \\ \phantom{-\,3x^2 -}\ \underline{+2x + 8} & \\ \phantom{-\,3x^2 - 2x -}\ 0 & \end{array}$$

Resposta: Quociente: $3x - 2$ e Resto: 0.

## Proposta 06: Expressões algébricas e divisão

Com o objetivo de despertar o interesse dos alunos no que diz respeito ao conteúdo de expressões algébricas vamos propor uma atividade referente à criptografia RSA, com o intuito de estabelecer a importância da fatoração na segurança da informação.

**Início da aula:** Começar a aula realizando uma pergunta que seja provocativa "Você já se perguntou como é possível manter mensagens privadas em um mundo digital repleto de ameaças?".

**Próxima etapa:** Sugestão de texto e imagem para explicar de forma breve o que é criptografia RSA.[1]

Figura 2.18 – Criptografia

Fonte: Pixabay[1]

A Criptografia RSA é responsável pela segurança do sistema RSA, e é um algoritmo de criptografia assimétrica que permite a segurança e a confidencialidade das informações disponibilizadas pela internet e outras comunicações.

Os responsáveis pelo desenvolvimento foram Ron Rivest, Adi Shamir e Leonard Adleman, em 1977, e tal algoritmo vem sendo aceito em sistemas criptográficos. Assim, percebemos como a matemática, especialmente na Álgebra, garante a segurança das comunicações digitais, um tópico relevante no contexto atual de tecnologia e informação.

[1] Disponível em: <https://pixabay.com/illustrations/cyber-attack-encryption-smartphone-4444448/>. Acesso em: 16 jun. 2023

Em resumo, chamamos essa criptografia de assimétrica pois existe um par de chaves diferentes em que uma delas tem a função de criptografar, enquanto a outra tem a função de descriptografar as informações. Tais chaves são conhecidas como chave pública e chave privada.

A chave pública pode ser compartilhada com qualquer pessoa, ela é usada para criptografar dados antes de enviar, já a chave privada é secreta, sendo utilizada para descriptografar os dados recebidos.

O algoritmo está conectado à dificuldade de fatorar grandes números, ou seja, a segurança RSA consiste no fato de que a fatoração de grandes números primos é, computacionalmente ou não, um processo extremamente complicado e demorado.

A fatoração de números é a chave para quebrar a criptografia RSA, pois ele permitiria identificar os fatores primos essenciais para descobrir a chave privada e descriptografar uma mensagem.

E vocês? Estão prontos para decodificar a seguinte mensagem?

**[ 25, 1, 6, 1, 29, 14, 20, 13 ]**

**Objetivos a serem alcançados:**

- Introduzir a linguagem simbólica através do uso de símbolos e letras para representar quantidades desconhecidas;
- Resolver situações-problema que envolvam o cálculo do valor numérico de expressões algébricas;
- Compreender a relação entre a divisão aritmética e expressões algébricas através da criptografia;
- Explorar o processo de descriptografia usando equações;
- Usar a calculadora científica para calcular potências e divisão com resto;
- Interpretar os resultados na calculadora como letras do texto original;
- Analisar a relação entre os números criptografados, e as chaves pública e privada.

**Sugestão ao professor:** Perceba que o objetivo desta introdução é despertar o interesse dos alunos, através da criptografia, o cálculo de expressões algébricas e divisão. O texto base foi escolhido para chamar a atenção dos alunos quanto a tecnologia, desta forma, sugiro a aplicação da atividade no laboratório de informática com o uso da calculadora científica, visto que utilizar ferramentas ligadas a tecnologia pode tornar a aula mais produtiva e prazerosa.

Abordaremos a ideia de divisão de números inteiros com resto. Além disso, proporcionaremos a oportunidade de utilizar calculadoras científicas, o que tornará essa experiência mais agradável aos alunos. Afinal, no oitavo ano, muitos alunos nunca tiveram acesso a uma calculadora desse tipo. A orientação é levar os alunos até o laboratório de informática para acessar a calculadora científica dos computadores.

Para mostrar a importância da fatoração na criptografia sugiro ao professor realizar a decodificação da primeira letra utilizando congruência, além de apresentar um conteúdo novo o professor pode apresentar a importância da fatoração.

**Para o desenvolvimento da atividade:**

- Lápis, borracha e caderno de matemática;
- Tabela com as letras do alfabeto e suas respectivas posições;
- Calculadora.
- Realizar a atividade num laboratório de informática.

Atividade proposta no início do conteúdo é decodificar a palavra

PARABENS.

Para isso, o professor primeiro precisará codificar a palavra seguindo as Etapas 01 e 02.

**Observação ao professor:** Para realizar a criptografia e a descriptografia, utilizamos o conteúdo de congruência. Para os leitores interessados, recomendamos consultar o Capítulo 9 do livro-texto da disciplina MA14 - Aritmética do PROFMAT.

**Etapa 01: Gerando a chave:** Para gerar a chave, siga os seguintes passos:

1. Escolha dois números primos $p$ e $q$. Sugestão: $p = 3$ e $q = 11$
2. Determine o número $n = p \cdot q$. Neste caso, $n = 3 \cdot 11 = 33$
3. Determine o número $m = (p-1)(q-1)$. Utilizando $p = 3$ e $q = 11$, temos $m = (3-1)(11-1) = 20$.
4. Escolha um número inteiro $e$ que satisfaça as seguintes condições:
   - $1 \leq e < m$;
   - $\text{mdc}(e, m) = 1$. Com $p = 3$ e $q = 11$, podemos tomar $e = 7$, pois $1 \leq 7 < 20$ e $mdc(7, 20) = 1$.

5. Agora encontre o número $d$ tal que

   - $1 \leq d \leq m$;
   - $d \cdot e \equiv 1 \mod m$, isto é, $m \mid (d \cdot e - 1)$. Utilizando os valores acima, temos $d = 3$.

Professores, percebam que:

- $n$ é um número composto pela multiplicação de dois primos grandes. O número $n$ é utilizado tanto na codificação como na decodificação.
- $e$ é um número inteiro escolhido como o expoente de criptografia público.

Dessa forma, a **chave pública** é representada pelo par $(n, e) = (33, 7)$, enquanto a **chave privada** corresponde ao valor $d = 3$.

**Etapa 02: Codificação.** Nesta etapa será realizado o processo para decodificar a mensagem.

Tabela 1 – Letras do alfabeto e suas respectivas posições

| **A** | **B** | **C** | **D** | **E** | **F** | **G** | **H** | **I** | **J** | **K** | **L** | **M** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |

| **N** | **O** | **P** | **Q** | **R** | **S** | **T** | **U** | **V** | **W** | **X** | **Y** | **Z** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |

Fonte: Acervo da Autora

A mensagem escolhida é a palavra “PARABENS”. Utilizando a seguinte Tabela 1, convertemos essa palavra em números, obtendo:

**[16, 1, 18, 1, 2, 5,14, 19]**.

Para cada número $x$ encontrado no primeiro passo será gerado um novo número, através da seguinte relação:

$$c \equiv x^e \mod n.$$

Dessa forma, obtemos a palavra codificada. Vamos iniciar criptografando cada um dos números, para esse procedimento será utilizado o conteúdo de congruência.

- O primeiro número é 16. Assim,

$$c \equiv 16^7 \mod 33.$$

Observamos que $c \equiv 16^7 \mod 33 \equiv 16^3 \cdot 16^4 \mod 33$ e realizando os cálculos para potências menores, temos

$$16^1 \bmod 33 \equiv 16 \bmod 33$$
$$16^2 \bmod 33 \equiv 256 \bmod 33 \equiv 25 \bmod 33$$
$$16^3 \bmod 33 \equiv (16^2 \cdot 16) \bmod 33 \equiv 25 \cdot 16 \bmod 33 \equiv 400 \bmod 33 \equiv 4 \bmod 33$$
$$16^4 \bmod 33 \equiv 25^2 \bmod 33 \equiv 625 \bmod 33 \equiv 31 \bmod 33.$$

Assim,

$$c \equiv 16^7 \bmod 33 \equiv 16^4 \cdot 16^3 \bmod 33 \equiv 31 \cdot 4 \bmod 33 \equiv 124 \bmod 33 \equiv 25 \bmod 33.$$

Logo, o número 16 foi codificado para o número 25.

- O segundo número é 1. Como

$$c \equiv 1^7 \bmod 33 \equiv 1 \bmod 33,$$

segue que 1 é a própria codificação do número 1.

- O terceiro número é 18. Logo,

$$c \equiv 18^7 \bmod 33.$$

Temos que $c \equiv 18^7 \bmod 33 \equiv 18^3 \cdot 18^4 \bmod 33$. Utilizando os cálculos de potências menores temos,

$$18^1 \bmod 33 \equiv 18 \bmod 33$$
$$18^2 \bmod 33 \equiv 324 \bmod 33 \equiv 27 \bmod 33$$
$$18^3 \bmod 33 \equiv 18^2 \cdot 18 \bmod 33 \equiv 27 \cdot 18 \bmod 33 \equiv 486 \bmod 33 \equiv 24 \bmod 33$$
$$18^4 \bmod 33 \equiv 27^2 \bmod 33 \equiv 729 \bmod 33 \equiv 3 \bmod 33.$$

Então,

$$c \equiv 18^7 \bmod 33 \equiv 18^4 \cdot 18^3 \bmod 33 \equiv 3 \cdot 24 \bmod 33 \equiv 72 \bmod 33 \equiv 6 \bmod 33,$$

e a codificação do número 18 é 6.

- Temos que o quarto número é 1. Já criptografamos esse número e vimos que é 1.

- O quinto número é 2. Assim,

$$c \equiv 2^7 \bmod 33 \equiv 128 \bmod 33 \equiv 29 \bmod 33.$$

Portanto, 29 é a codificação do número 2.

- Sexto numero é 5. Desta forma,

$$c \equiv 5^7 \bmod 33.$$

Vendo que $c \equiv 5^7 \bmod 33 \equiv 5^3 \cdot 5^4 \bmod 33$ e, utilizando os cálculos de potências menores, temos:

$$\begin{aligned}
5^1 \bmod 33 &\equiv 5 \bmod 33 \\
5^2 \bmod 33 &\equiv 25 \bmod 33 \\
5^3 \bmod 33 &\equiv (5^2 \cdot 5) \bmod 33 \equiv 25 \cdot 5 \bmod 33 \equiv 125 \bmod 33 \equiv 26 \bmod 33 \\
5^4 \bmod 33 &\equiv 25^2 \bmod 33 \equiv 625 \bmod 33 \equiv 31 \bmod 33.
\end{aligned}$$

Logo,

$$c \equiv 5^7 \bmod 33 \equiv 5^4 \cdot 5^3 \bmod 33 \equiv 31 \cdot 6 \bmod 33 \equiv 806 \bmod 33 \equiv 14 \bmod 33.$$

Concluímos que o número 5 é codificado para o números 14.

- O sétimo número é 14. Logo,

$$c \equiv 14^7 \bmod 33.$$

Sabemos que $c \equiv 14^7 \bmod 33 \equiv 14^3 \cdot 14^4 \bmod 33$. Fazendo o uso dos cálculos de menores, obtemos

$$\begin{aligned}
14^1 \bmod 33 &\equiv 14 \bmod 33 \\
14^2 \bmod 33 &\equiv 196 \bmod 33 \equiv 31 \bmod 33 \\
14^3 \bmod 33 &\equiv 14^2 \cdot 14 \bmod 33 \equiv 31 \cdot 14 \bmod 33 \equiv 434 \bmod 33 \equiv 5 \bmod 33 \\
14^4 \bmod 33 &\equiv 31^2 \bmod 33 \equiv 961 \bmod 33 \equiv 4 \bmod 33.
\end{aligned}$$

Então,

$$c \equiv 14^7 \bmod 33 \equiv 14^4 \cdot 14^3 \bmod 33 \equiv 4 \cdot 5 \bmod 33 \equiv 20 \bmod 33.$$

O número 14 foi codificado para o número 20.

- Oitavo número é 19. Logo,

$$c \equiv 19^7 \bmod 33.$$

Temos $c \equiv 19^7 \bmod 33 \equiv 19^3 \cdot 19^4 \bmod 33$. Novamente, utilizando os cálculos de potências menores, obtemos

$$\begin{aligned}
19^1 \bmod 33 &\equiv 19 \bmod 33 \\
19^2 \bmod 33 &\equiv 361 \bmod 33 \equiv 31 \bmod 33 \\
19^3 \bmod 33 &\equiv (19^2 \cdot 19) \bmod 33 \equiv 31 \cdot 19 \bmod 33 \equiv 589 \bmod 33 \equiv 28 \bmod 33 \\
5^4 \bmod 33 &\equiv 31^2 \bmod 33 \equiv 961 \bmod 33 \equiv 4 \bmod 33.
\end{aligned}$$

Assim,

$$c \equiv 19^7 \bmod 33 \equiv 19^4 \cdot 19^3 \bmod 33 \equiv 4 \cdot 28 \bmod 33 \equiv 112 \bmod 33 \equiv 13 \bmod 33,$$

e a codificação do número 19 é 13.

Portanto, a palavra "PARABENS" foi codificada para

**[25, 1, 6, 1, 29, 14, 20, 13].**

**Etapa 03: Decodificação.** Os alunos recebem uma mensagem codificada. No nosso exemplo, os alunos recebem a seguinte mensagem

$$[25, 1, 6, 1, 29, 14, 20, 13].$$

Para facilitar a decodificação os alunos podem receber a Tabela 1.

Neste momento, é necessário adaptar a atividade de decodificação para alunos do oitavo ano do Ensino Fundamental, pois no processo de decodificação é utilizado congruência módulo $n$:

$$x \equiv c^d \bmod n.$$

Iniciamos mostrando o significado de cada letra da equação.

$$x \equiv c^d \bmod n.$$

Na qual:

- $x$: é o resultado da operação de descriptografia. Representa a mensagem original que queremos obter.
- $c$: é o texto criptografado, ou seja, a mensagem que foi previamente criptografada usando a chave pública do destinatário.
- $d$: é a chave privada de descriptografia, essa chave é mantida em segredo pelo destinatário e é usada para descriptografar o texto criptografado c.
- $n$: é a chave pública e o módulo utilizado na operação de criptografia. É um número composto pela multiplicação de dois primos grandes, geralmente denominados $p$ e $q$. O valor de $n$ é utilizado tanto na criptografia quanto na descriptografia.

Para a decodificação desta mensagem é necessário disponibilizar dos valores que foram desenvolvidos na Etapa 01, sendo assim: $c \in \{25, 1, 6, 1, 29, 14, 20, 13\}$, $d = 3$ e $n = 33$.

Para determinar a primeira letra, temos os seguintes valores: $c = 25$, $d = 3$ e $n = 33$. Sendo assim:

$$x \equiv c^d \bmod n.$$

Portanto:

$$x \equiv 25^3 \bmod 33.$$

Sabemos que

$$x \equiv 25^3 \bmod 33 \equiv 25 \cdot 25^2 \bmod 33$$

Utilizando cálculos de valores menores, temos:

$$25^1 \equiv 25 \bmod 33$$

$$25^2 \equiv 625 \bmod 33 \equiv 31 \bmod 33$$

$$25^3 \equiv 25 \cdot 25^2 \bmod 33 \equiv 25 \cdot 31 \bmod 33 \equiv 775 \bmod 33 \equiv 16 \bmod 33.$$

Agora o professor pode desenvolver o processo através da divisão. Como primeiro passo resolva $c^d$. O resultado deverá ser dividido por 33, e o resto da divisão será o código referente a primeira letra. Temos

$$25^3 = 15625$$

Agora, efetuando a divisão por 33 obtemos:

$$\begin{array}{r|l} 15625 & 33 \\ \cline{2-2} -\,132 & 473 \\ \cline{1-1} 242 & \\ -\,231 & \\ \cline{1-1} 115 & \\ -\,99 & \\ \cline{1-1} 16 & \end{array}$$

Temos que o resto é 16. Logo, a letra desejada é a que está na posição 16 da Tabela 1. Assim, a primeira letra da palavra é **P**.

A partir desse momento o desafio é com os alunos, eles devem chegar nos demais valores.

- Segundo número a ser decodificado é $c = 1$.
  Temos os seguintes números: $c = 1$, $d = 3$ e $n = 33$. Assim, $1^3 = 1$. Na divisão de 1 por 33, temos que 0 é o quociente e o resto é 1. Como o resto é 1, a letra desejada é a que está na primeira posição da Tabela 1. Assim, a segunda letra da palavra é **A**.

- Terceiro número a ser decodificado é $c = 6$.
  Temos os seguintes números: $c = 6$, $d = 3$ e $n = 33$. Logo, $6^3 = 216$. Dividindo 216 por 33, chegamos no quociente 6 e o resto 18. Como o resto é 18, a letra desejada é a que está na posição 18 da Tabela 1. Assim, a terceira letra da palavra é **R**.

- Quarto número a ser decodificado $c = 1$.
  Já vimos que $c = 1$ corresponde a letra **A**.

- Quinto número a ser codificado: $c = 29$
  Temos os seguintes valores: $c = 29$, $d = 3$ e $n = 33$. Notamos que $29^3 = 24389$ e 2 é o resto na divisão 24389 por 33. Sendo 2 o resto, a letra desejada é a que está na posição 2 da Tabela 1. Assim, a quinta letra da palavra é **B**.

- Sexto valor a ser codificado: $c = 14$.
  Temos os seguintes valores: $c = 14$, $d = 3$ e $n = 3$. Realizando as contas, obtemos $14^3 = 2744$ e, na divisão de 2744 por 33 o resto é 5. Portanto, a letra desejada é a que está na posição 5 da Tabela 1. Assim, a sexta letra da palavra é **E**.

- Sétimo Valor a ser codificado: $c = 20$.
  Temos os seguintes valores: $c = 20$, $d = 3$ e $n = 33$. Seguindo o processo, obtemos $20^3 = 8000$ e o resto na divisão de 8000 por 33 o quociente é 242 e resto é 14. Desse modo, a letra desejada é a que está na posição 14 da Tabela 1. Assim, a sétima letra da palavra é **N**.

- Oitavo Valor a ser codificado: c = 13
  Temos os seguintes valores: $c = 13$, $d = 3$ e $n = 33$. Como $13^3 = 2197$, então ao dividir esse valor por 33 chegamos no quociente 66 e no resto 19. Segue que a letra desejada é a que está na posição 19 da Tabela 1. Assim, a oitava letra da palavra é **S**.

Essa atividade pode se transformar em um projeto para a feira do conhecimento ou até mesmo ser apresentada em uma feira de matemática, caso haja alunos interessados no tema. Como requer algum tempo de preparação adicional para outras codificações, seria algo a ser desenvolvido no contraturno..

# 3 Ao estudante

Neste capítulo serão apresentadas as propostas de atividades com aplicação para estudantes do Ensino Básico.

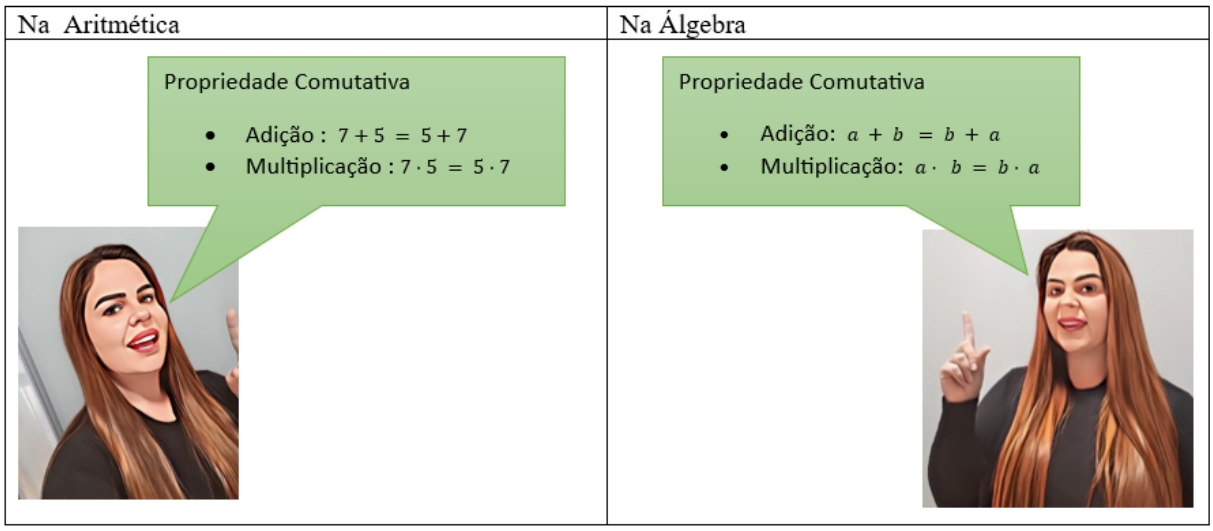
## Proposta 01: Conexões Aritméticas e Algébricas: Descobrindo paralelos matemáticos

**Objetivos a serem alcançados:**

- Reconhecer semelhanças e conexões entre conceitos e propriedades numéricas e algébricas.
- Observar que muitas das regras e propriedades da Aritmética se aplicam à Álgebra.
- Usar suas habilidades aritméticas existentes para resolver problemas e simplificar expressões algébricas.
- Perceber que os conceitos matemáticos podem ser generalizados para além de situações específicas, permitindo-lhes resolver problemas mais complexos e abstratos.
- Compreender que a Álgebra é uma extensão natural dos conceitos aritméticos.
- Dominar as propriedades a fim de desenvolver habilidades fundamentais de manipulação de expressões algébricas.

Vamos analisar as propriedades que vocês já aprenderam na Aritmética em anos anteriores e compará-las com as propriedades utilizadas no ensino de polinômios. Nesta atividade, iremos explorar as semelhanças e diferenças entre esses dois campos da matemática, buscando ampliar nosso entendimento e estabelecer conexões entre os conceitos estudados. Para isso observe e analise as figuras a seguir.

Figura 3.1 – Propriedade Comutativa




*Questão 1:* Diga se a afirmação é verdadeira ou falsa.

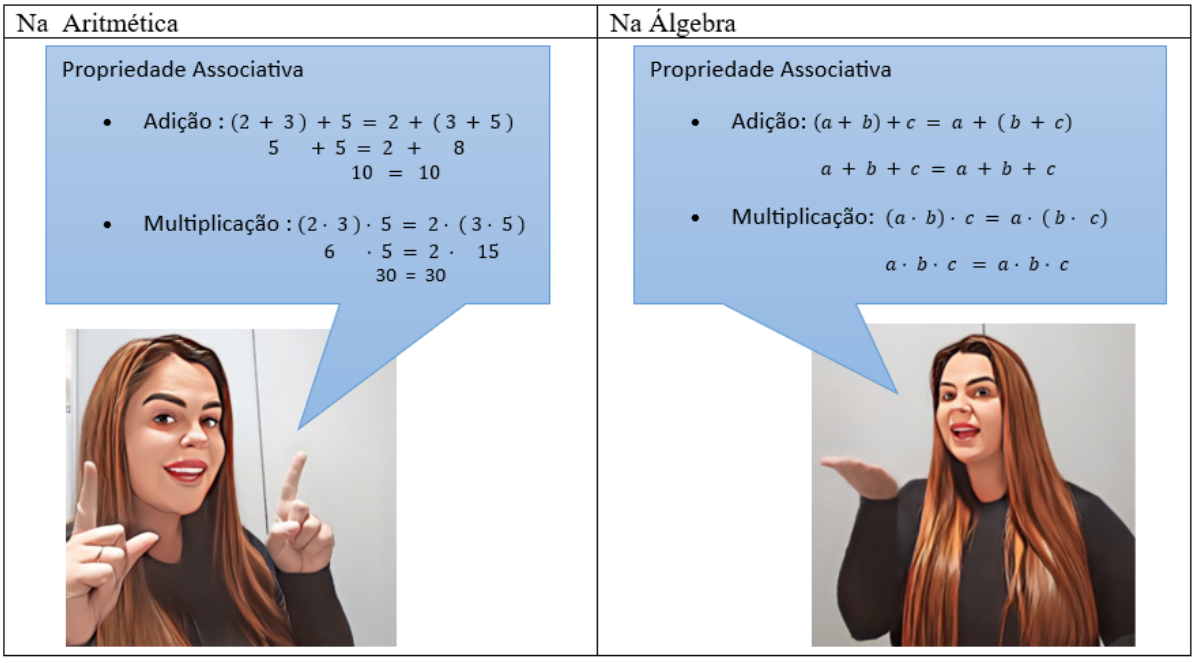
(a) As ações de calçar as meias e calçar os sapatos são comutativas.

(b) As ações de colocar o chapéu e o casaco são comutativas.

(c) As ações de lavar roupa e secar são comutativas.

*Questão 2:* Reflita se a subtração nos número inteiros é comutativa.

Figura 3.2 – Propriedade Associativa



*Questão 3:* Use as propriedades dos números inteiros para escrever as expressões algébricas sem parênteses:

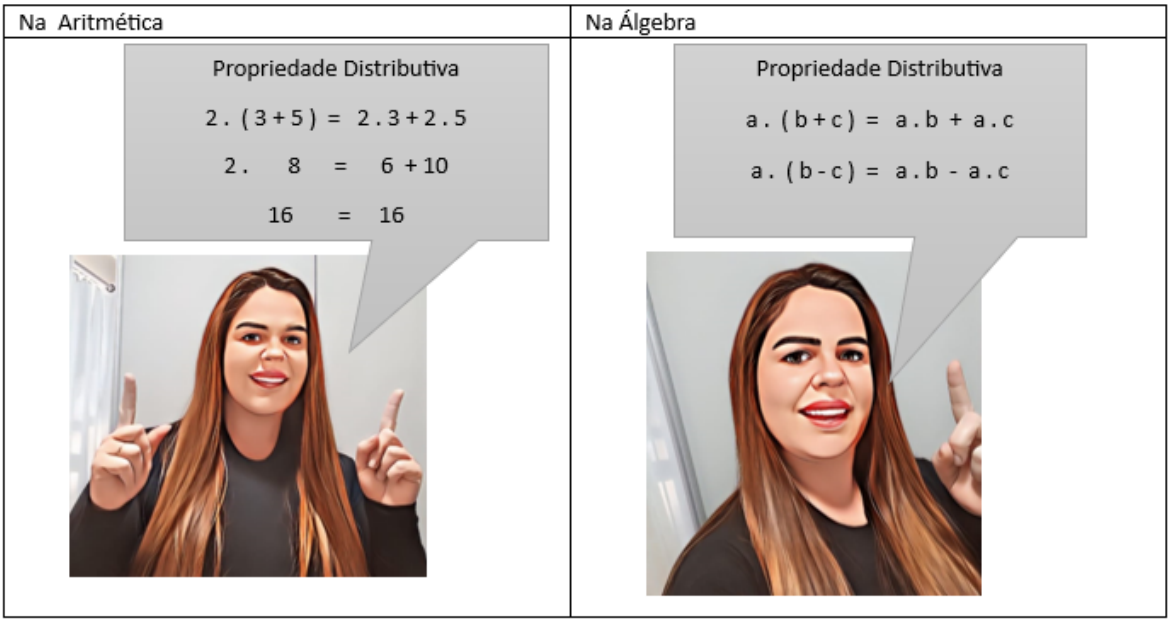
(a) $(x-1)+4$

(b) $3 \cdot (5 \cdot x)$

(c) $(2+y)+5$

(d) $3 \cdot (x \cdot 6)$

Figura 3.3 – Propriedade Distributiva




*Questão 4:* Use as propriedades dos números inteiros para escrever as expressões algébricas sem parênteses:

(a) $4(x-1)$

(b) $5(2a+1)$

(c) $4(2+b)+5$

(d) $3(x+2)+2(2y-1)$

*Questão 5:* Use as propriedades dos números inteiros para simplificar as expressões algébricas:

(a) $2x+4x$

(b) $-y + 1 + 3y$

(c) $3a - 6a - a$

(d) $4z + 5 + 2 + 2z$

Figura 3.4 – Elemento Neutro

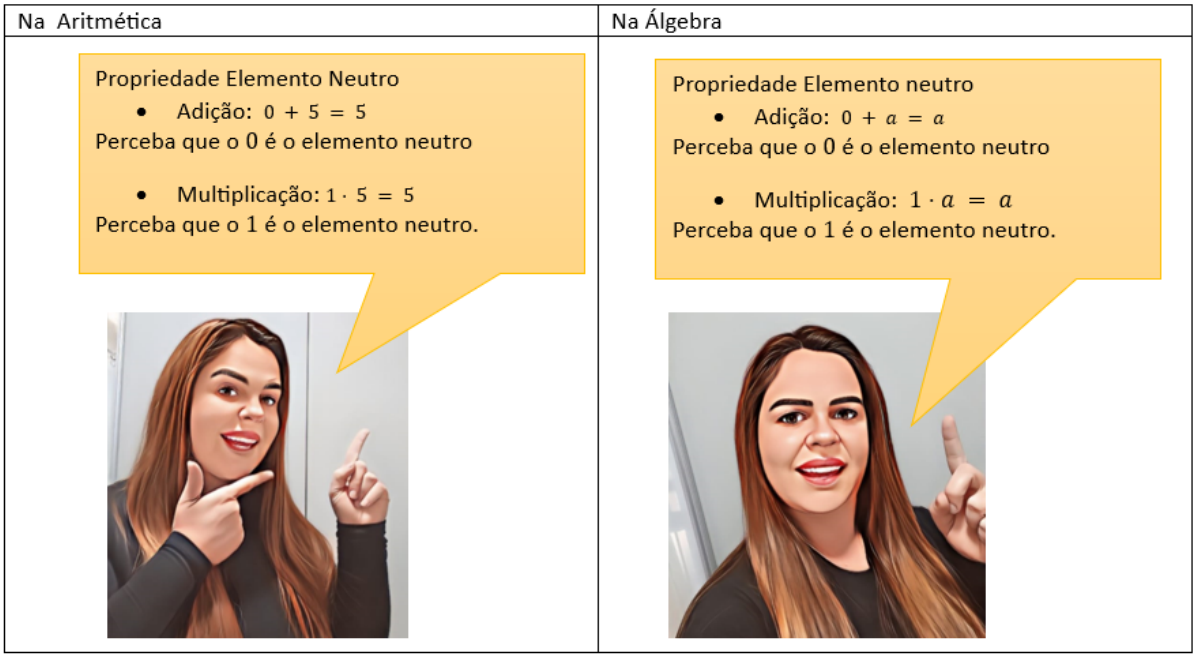
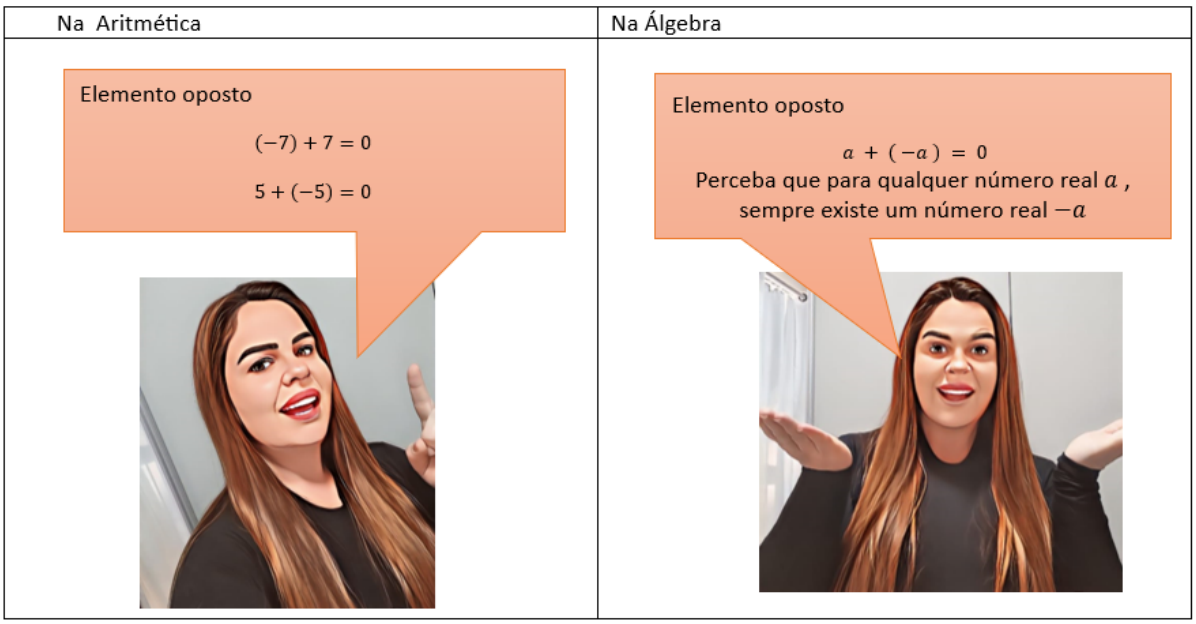



Figura 3.5 – Elemento Oposto




*Questão 6:* Use as propriedades dos números inteiros para simplificar as expressões algébricas:

(a) $a^2 - a(a + b)$

(b) $-xy + x(1 + y)$

(c) $1(a + b) - 1(a + b)$

(d) $-2a + 4 + 1(2a - 3)$

Com esta atividade, eu aprendi a:

- ☐ Reconhecer semelhanças e conexões entre conceitos e propriedades numéricas e algébricas.
- ☐ Observar que muitas das regras e propriedades da aritmética se aplicam à Álgebra.
- ☐ Dominar as propriedades a fim de desenvolver habilidades fundamentais de manipulação de expressões algébricas.

## Proposta 02: Estudo das operações com polinômios

**Introdução:** A adição e a subtração de polinômios exigem a combinação adequada de termos semelhantes, enquanto a multiplicação envolve a distribuição de cada termo de um polinômio sobre todos os termos do outro polinômio.

Já vimos que monômios de uma variável, na variável $x$, são expressões algébricas como

$$5 \qquad 2x \qquad -6x^2 \qquad 31x^3 \qquad -12x^6 \qquad -x^{11}$$

Ou seja, um monômio pode ser um número ou uma expressão algébrica que represente apenas multiplicações de números e potências naturais de $x$.

Além disso, vimos que polinômios na variável $x$ são expressões algébricas como

$$5 \qquad -4x \qquad 2x-1 \qquad 3x^2-4x+1 \qquad -5x^4+10x \qquad -3x^5-6x^3-2x^2+1$$

Ou seja, polinômios são somas finitas de monômios (*poli=vários*).

**Observação:** Para o Ensino Médio é importante adicionar a seguinte definição:

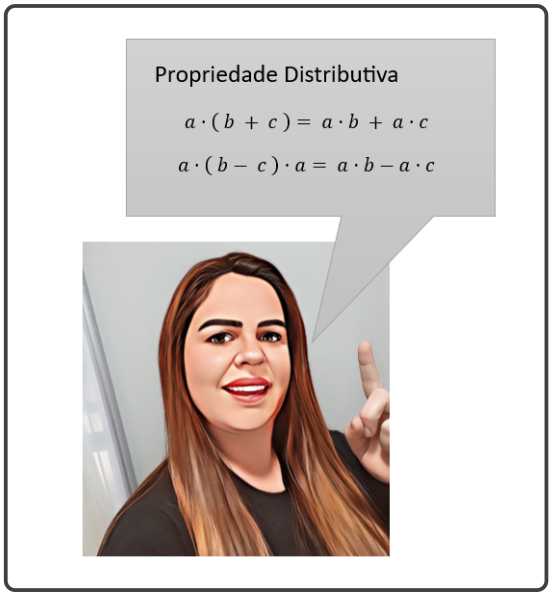
De modo geral, um polinômio na variável $x$ é uma expressão da forma

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0,$$

em que $a_n, a_{n-1}, \cdots, a_1$ e $a_0$ são números reais ou complexos denominados coeficientes.

**Adição e Subtração de monômios**

Aplicando a propriedade distributiva da multiplicação em relação à adição, podemos adicionar e subtrair monômios semelhantes.




Observe os exemplos:

- $3x + 5x = (3 + 5)x = 8x$
- $12x^2 - 3x^2 = (12 - 3)x^2 = 9x^2$
- $-x^5 - 7x^5 = (-1 - 7)x^5 = -8x^5$

### Adição e Subtração de polinômios

Denominamos soma de dois ou mais polinômios ao polinômio que se obtém adicionando todos os termos semelhantes dos polinômios dados. Observe os exemplos:

- Se $p(x) = 3x + 12x^2$ e $q(x) = 5x - 3x^2$, então

$$\begin{aligned} p(x) + q(x) &= (3x + 12x^2) + (5x - 3x^2) \\ &= 3x + 5x + 12x^2 - 3x^2 \\ &= (3 + 5)x + (12 - 3)x^2 \\ &= 8x + 9x^2. \end{aligned}$$

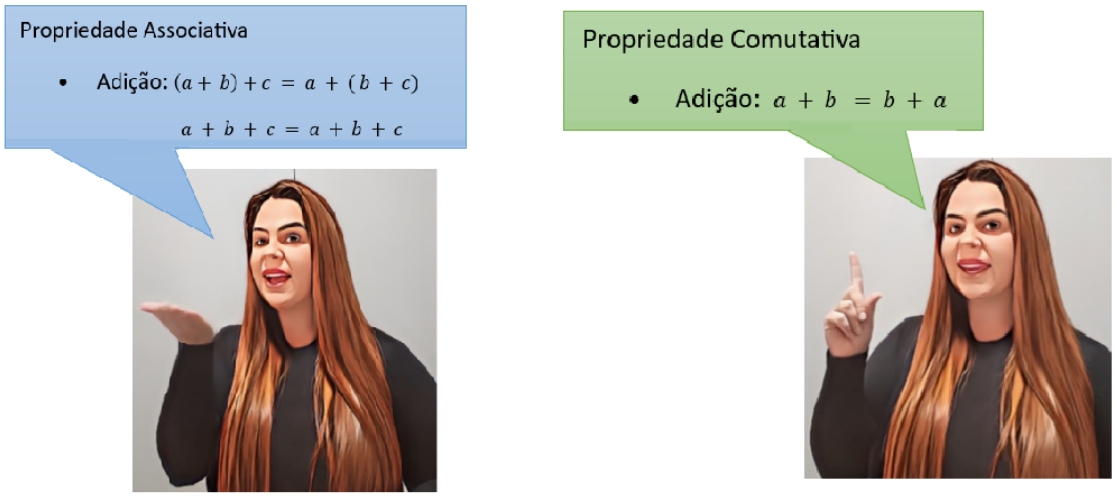
- Se $p(x) = 3x^2 - 5x + 8$ e $q(x) = 2x^3 + 5x^2 - 2x - 9$, então

$$\begin{aligned} p(x) + q(x) &= (3x^2 - 5x + 8) + (2x^3 + 5x^2 - 2x - 9) \\ &= (0x^3 + 3x^2 - 5x + 8) + (2x^3 + 5x^2 - 2x - 9) \\ &= 0x^3 + 2x^3 + 3x^2 + 5x^2 - 5x - 2x + 8 - 9 \\ &= (0 + 2)x^3 + (3 + 5)x^2 + (-5 - 2)x + (8 - 9) \\ &= 2x^3 + 8x^2 - 7x - 1 \end{aligned}$$

- Se $p(x) = -x^5 + 2x - 1$ e $q(x) = -7x^5 + 4x^3 + 2$, então

$$\begin{aligned} p(x) + q(x) &= (-x^5 + 2x - 1) + (-7x^5 + 4x^3 + 2) \\ &= (-x^5 + 0x^3 + 2x - 1) + (-7x^5 + 4x^3 + 0x + 2) \\ &= -x^5 + (-7x^5) + 4x^3 + 0x^3 + 2x + 0x + (-1) + 2 \\ &= (-1 - 7)x^5 + (4 + 0)x^3 + (2 + 0)x + (-1 + 2) \\ &= -8x^5 + 4x^3 + 2x + 1. \end{aligned}$$

Percebam que para efetuar a adição de polinômios usamos as propriedades associativa e comutativa da adição, além da distributiva para adicionar os termos semelhantes.




**Observação:** Para os alunos do Ensino Médio deve-se adicionar a seguinte definição:

Considere dois polinômios $p(x)$ e $q(x)$, sendo eles na forma:

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0$$

e

$$q(x) = b_n x^n + b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \cdots + b_1 x + b_0.$$

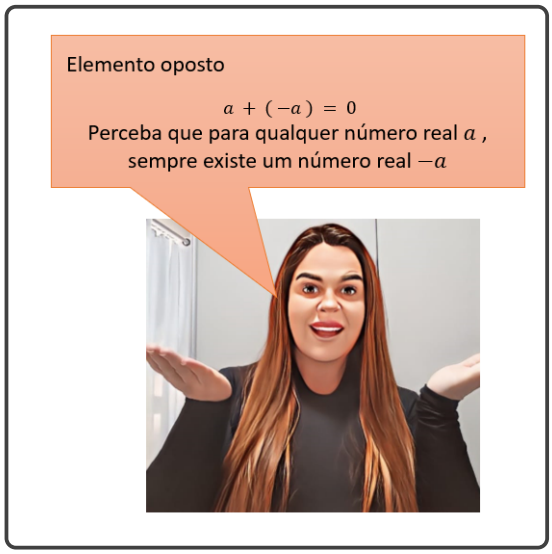
Define-se a adição $p(x) + q(x)$ como

$$p(x) + q(x) = (a_n + b_n)x^n + (a_{n-1} + b_{n-1})x^{n-1} + \cdots + (a_1 + b_1)x + (a_0 + b_0)$$

Pode-se também definir a subtração entre dois polinômios $p(x)$ e $q(x)$ por

$$p(x) - q(x) = p(x) + (-q(x)),$$

em que $-q(x)$ é o polinômio oposto de $q(x)$.




Observe os seguintes exemplos: Se $p(x) = 3x^2 - 5x + 8$ e $a(x) = 2x^3 + 5x^2 - 2x - 9$, então:

$$\begin{aligned} p(x) - q(x) &= (3x^2 - 5x + 8) - (2x^3 + 5x^2 - 2x - 9) \\ &= -2x^3 + (3-5)x^2 + (-5-(-2))x + (8-(-9)) \\ &= -2x^3 - 2x^2 - 3x + 17 \end{aligned}$$

e

$$\begin{aligned} q(x) - p(x) &= (2x^3 + 5x^2 - 2x - 9) - (3x^2 - 5x + 8) \\ &= 2x^3 + (5-3)x^2 + (-2-(-5))x + (-9-8) \\ &= 2x^3 + 2x^2 + 3x - 17 \end{aligned}$$

Observe que a subtração de polinômios não é comutativa, pois no exemplo acima temos que $p(x) - q(x) \neq q(x) - p(x)$.

**Observação:** Para os alunos do Ensino Médio pode-se adicionar a seguinte definição:

Considere dois polinômios $p(x)$ e $q(x)$, sendo eles na forma

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0$$

e

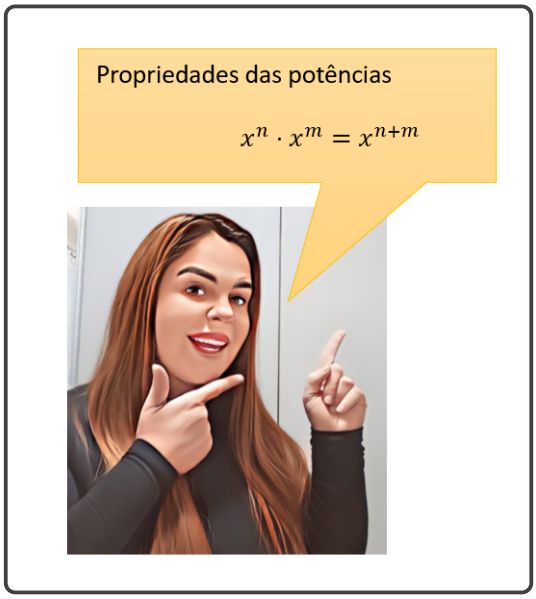
$$q(x) = b_n x^n + b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \cdots + b_1 x + b_0.$$

Temos que a diferença (subtração) $p(x) - q(x)$ é dada por

$$p(x) - q(x) = (a_n - b_n)x^n + (a_{n-1} - b_{n-1})x^{n-1} + \cdots + (a_1 - b_1)x + (a_0 - b_0)$$

### Multiplicação de monômios

Aplicando a propriedade da potenciação da figura abaixo podemos multiplicar monômios.




Observe os seguintes exemplos:

- $(3x^3)\cdot(5x^2) = 3\cdot 5\cdot x^3\cdot x^2 = 15\cdot x^{3+2} = 15x^5$
- $(12x)\cdot(-3x^5) = 12\cdot(-3)\cdot x^1\cdot x^5 = -36x^{1+5} = -36x^6$
- $x^7\cdot 3x^7 = 3x^{7+7} = 3x^{14}$

### Multiplicação de polinômios

Para efetuar a multiplicação de dois ou mais polinômios, utilizamos a propriedade distributiva da multiplicação em relação à adição. Devemos multiplicar dois a dois todos os termos do primeiro polinômio com todos os termos do segundo. Veja exemplos:

- Se $p(x) = 3x + 5$ e $q(x) = x^3 + 2x - 3$, então

$$\begin{aligned} p(x)\cdot q(x) &= (3x+5)\cdot(x^3+2x-3) \\ &= 3x\cdot x^3 + 3x\cdot 2x + 3x\cdot(-3) + 5\cdot x^3 + 5\cdot 2x + 5\cdot(-3) \\ &= 3x^4 + 6x^2 - 9x + 5x^3 + 10x - 15 \\ &= 3x^4 + 5x^3 + 6x^2 + (-9+10)x - 15 \\ &= 3x^4 + 5x^3 + 6x^2 + x - 15 \end{aligned}$$

- Se $p(x) = 2x^2 + 3x + 1$ e $q(x) = 4x^4 - x^2$, então

$$\begin{aligned} p(x)\cdot q(x) &= (2x^2+3x+1)\cdot(4x^4-x^2) \\ &= 2x^2\cdot 4x^4 + 2x^2\cdot(-x^2) + 3x\cdot 4x^4 + 3x\cdot(-x^2) + 1\cdot 4x^4 + 1\cdot(-x^2) \\ &= 8x^6 - 2x^4 + 12x^5 - 3x^3 + 4x^4 - x^2 \\ &= 8x^6 + 12x^5 + (-2+4)x^4 - 3x^3 - x^2 \\ &= 8x^6 + 12x^5 + 2x^4 - 3x^3 - x^2 \end{aligned}$$

**Observação:** Note que se $\text{gr}(p)$ é grau de $p(x)$ e $\text{gr}(q)$ é grau de $q(x)$, então $\text{gr}(p \cdot q) = \text{gr}(p) + \text{gr}(q)(p)$.

**Atividade de Fixação**

*Questão 1:* Considere os polinômios $p(x) = 2x^3 + 3x^2 - 7$ e $q(x) = x^2 + 5x + 3$.

(a) Determine $p(x) + q(x)$ , apresente a resposta em sua forma simplificada.

Resolução:

(b) Determine $p(x) - q(x)$ , apresente a resposta em sua forma simplificada.

Resolução:

*Questão 2:* Calcule o produto dos polinômios $p(x) = 3x^2 + 1$ e $q(x) = x^3 - 3x$, em seguida, apresente a resposta em sua forma simplificada.

Resolução:

Com esta atividade, eu aprendi a:

- ☐ Somar e subtrair polinômios semelhantes combinando os termos correspondentes.
- ☐ Identificar o grau de um polinômio e entender como ele afeta as operações.
- ☐ Reduzir expressões polinomiais ao combinar termos semelhantes e aplicar as propriedades da álgebra.
- ☐ Aplicar os conceitos aprendidos para resolver problemas práticos que envolvem operações com polinômios.

# Proposta 03: Fatoração de polinômios

**Fatoração Algébrica**

Os números primos, ao mesmo tempo tão simples e essenciais, possuem a capacidade de gerar todos os números naturais maiores que 1.

Vocês já aprenderam que fatorar um número natural ou inteiro consiste em escrevê-lo como um produto de dois ou mais fatores primos. Vamos relembrar esse conceito, fatorando o número 60.

$$60 \div 2 = 30$$

$$30 \div 2 = 15$$

$$15 \div 3 = 5$$

$$5 \div 5 = 1.$$

Assim,

$$60 = 2^2 \cdot 3 \cdot 5.$$

> Todo número natural maior do que 1 ou é primo ou se escreve de modo único (a menos da ordem de fatores) como um produto de fatores primos,
>
> $$p = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n},$$
>
> em que $p_i$ são números primos e $\alpha_i$ são números naturais.

Vocês já perceberam que a fatoração pode ser utilizada para simplificar uma divisão? Veja o exemplo a seguir:

$$\frac{60}{15} = \frac{2^2 \cdot 3 \cdot 5}{3 \cdot 5} = 2^2 = 4.$$

**Fatoração algébrica para auxiliar a simplificação de expressões racionais**

É possível realizar a fatoração de uma expressão racional, como vemos na quociente entre dois monômios:

$$\frac{60x^2y^3}{15xy^2} = \frac{2^2 \cdot 3 \cdot 5 \cdot x \cdot x \cdot y \cdot y \cdot y}{3 \cdot \cdot x \cdot y \cdot y} = 2^2 \cdot x \cdot y = 4xy.$$

Observe que utilizamos a fatoração para efetuar a divisão entre monômios.

Apresentaremos a seguir as regras que podemos utilizar para realizar esse cálculo de maneira simplificada.

Na divisão de monômios, realizamos a divisão dos coeficientes do numerador pelo coeficiente do denominador. Ao lidarmos com a parte algébrica, utilizamos a regra da

potenciação quando as bases são iguais. Dessa forma, ao dividirmos $x^2$ por $x$, mantemos a letra $x$ como base e subtraímos os expoentes. Da mesma forma, ao dividirmos $y^3$ por $y^2$, conservamos a letra e subtraímos os expoentes.

### Fatoração de Polinômios

De acordo com o dicionário, encontramos o significado da palavra "fatorar".

- ✓ Na Aritmética: decompor (um número) em seus fatores primos.
- ✓ Na Álgebra: decompor (um polinômio) em um produto de fatores irredutíveis.

Com base nessas informações, vamos adquirir conhecimento sobre alguns tipos distintos de fatoração de polinômios.

### Fator Comum em evidência

Quando uma expressão algébrica apresenta um fator comum em todos os seus termos, é possível colocá-lo em evidência, obtendo uma forma fatorada do polinômio.

Há duas dicas importantes a serem consideradas:

- ✓ Para encontrar o fator comum entre os coeficientes, é recomendado calcular o máximo divisor comum (mdc) entre eles. Dessa forma, é possível identificar o maior divisor comum que divide todos os coeficientes.
- ✓ No caso do fator comum na parte literal, quando as letras são iguais, devemos selecionar aquela com o menor expoente para evidenciá-la.

Veja o exemplo a seguir: Dada a expressão

$$18x^5 - 24x^3 + 12x^2 - 6x^6$$

temos que o mdc dos coeficientes é

$$\text{mdc}(18, 24, 12, 6) = 6.$$

Ao identificarmos as letras comuns, devemos selecionar aquela que possui o expoente menor, neste caso é $x^2$.

Dessa forma, o fator a ser evidenciado é determinado por $6x^2$.

O fator comum deve ser escrito fora dos parênteses. Em seguida, é necessário dividir cada termo do polinômio pelo fator comum. O resultado dessa divisão deve ser colocado dentro dos parênteses.

$$18x^5 - 24x^3 + 12x^2 - 6x^6 = 6x^2(3x^3 - 4x + 2 - x^4).$$

Podemos empregar a propriedade distributiva na resposta final como um meio concreto para verificar a correção do resultado.

### Agrupamento

Conforme o próprio termo "agrupamento" sugere, essa técnica é utilizada quando a expressão algébrica apresenta grupos de termos que podem ser combinados devido a fatores em comum. Além disso, ao fatorar cada grupo, esses grupos revelam um novo fator comum, que pode ser identificado, finalizando assim o processo de fatoração.

Como exemplo, vamos fatorar a expressão a seguir:

$$ab + 3b - 7a - 21.$$

Observem que $ab + 3b = b(a + 3)$ e $-7a - 21 = -7(a + 3)$, sendo assim,

$$ab + 3b - 7a - 21 = b(a + 3) - 7(a + 3).$$

Dessa forma, constatamos a presença de um novo fator comum: $a + 3$. Ao evidenciá-lo, obtemos:

$$ab + 3b - 7a - 21 = b(a + 3) - 7(a + 3) = (a + 3) \cdot (b - 7)$$

.

Novamente, podemos empregar a propriedade distributiva na resposta final como um meio concreto para verificar a correção do resultado.

### Diferença entre Quadrados

A forma fatorada da diferença de dois quadrados segue a regra do produto da soma pela diferença das bases, na ordem dada. Aqui está um exemplo:

$$a^2 - b^2 = (a + b)(a - b).$$

É importante notar que essa fatoração é aplicada nas seguintes condições:

- A expressão é um binômio;
- Há um sinal de "subtração" entre os termos.
- Para resolver, é necessário extrair a raiz quadrada dos termos e, em seguida, seguir a regra como apresentada no exemplo.

Vamos fatorar a expressão a seguir:

$$x^2 - 16 = (x + 4)(x - 4).$$

Empregamos a propriedade distributiva na resposta final como um meio concreto para verificar a correção do resultado.

### Trinômio Quadrado Perfeito

Esse procedimento é aplicado para fatorar ou decompor expressões algébricas que são trinômios quadrados perfeitos.

Um trinômio é chamado de trinômio quadrado perfeito, pois é igual ao quadrado de um binômio. Em outras palavras, é um trinômio que pode ser escrito na forma $(a+b)^2$ ou na forma $(a-b)^2$, em que $a$ e $b$ são termos ou coeficientes.

Analisem os exemplos a seguir:

$$(a+b)^2 = a^2 + 2ab + b^2$$

$$(a-b)^2 = a^2 - 2ab + b^2$$

Identificamos um trinômio quadrado perfeito e obtemos a sua forma fatorada ao observarmos os seguintes aspectos:

- ✓ O trinômio é composto por três termos.
- ✓ Dois dos termos são quadrados perfeitos ($a^2$ e $b^2$)
- ✓ O terceiro termo é equivalente a "mais" ou "menos" duas vezes o produto das bases desses quadrados.

Vamos analisar mais um exemplo e responder algumas perguntas.

$$x^2 - 16x + 64.$$

1. Possui três termos?
   Resposta:
2. Quais desses termos são quadrados perfeitos?
   Resposta:
3. Quais são as bases desses quadrados perfeitos?
   Resposta:
4. Se multiplicarmos por dois os resultados dos termos anteriores, obtemos o resultado do termo que não é um quadrado perfeito?
   Resposta:

Se todas as respostas forem "Sim", significa que é um trinômio quadrado perfeito. Vamos para a solução.

1. Abra parênteses e escreva a base de um dos quadrados perfeitos.
2. Utilize o sinal do termo que não é um quadrado perfeito.
3. Escreva a base do outro quadrado perfeito e feche os parênteses.
4. Eleve tudo ao quadrado.

Sendo assim:

$$x^2 - 16x + 64 =$$

**Simplificação de Frações Algébricas**

As simplificações algébricas podem desempenhar um papel relevante na divisão de polinômios.

Embora a simplificação algébrica não seja diretamente uma forma de dividir polinômios, ela tem o potencial de simplificar as expressões utilizadas na divisão e tornar o processo mais acessível.

Observem os exemplos de simplificação de algumas expressões:

- $\dfrac{35}{7a - 7x} = \dfrac{7 \cdot 5}{7(a - x)} = \dfrac{5}{(a - x)}$;
- $\dfrac{15a + 5b}{3a + b} = \dfrac{5(3a + b)}{3a + b} = 5$;
- $\dfrac{x^2 - 9}{x^2 - 6x + 9} = \dfrac{(x + 3)(x - 3)}{(x - 3)(x - 3)} = \dfrac{(x + 3)}{(x - 3)}$;
- $\dfrac{a^2 + 8a}{ab + 8b + a + 8} = \dfrac{a(a + 8)}{b(a + 8) + 1(a + 8)} = \dfrac{a(a + 8)}{(a + 8)(b + 1)} = \dfrac{a}{b + 1}$.

Com esta atividade, eu aprendi a:

- ☐ Reconhecer que fatorar uma expressão algébrica significa expressá-la como a multiplicação de dois ou mais fatores.
- ☐ Reconhecer as condições para aplicar diferentes técnicas de fatoração, como fator comum em evidência, diferença entre quadrados, agrupamentos e trinômios quadrados perfeitos.
- ☐ Utilizar diferentes técnicas de fatoração, como fator comum em evidência, diferença entre quadrados, agrupamentos e trinômios quadrados perfeitos.
- ☐ Simplificar expressões algébricas envolvendo frações, identificando fatores comuns e cancelando termos equivalentes.

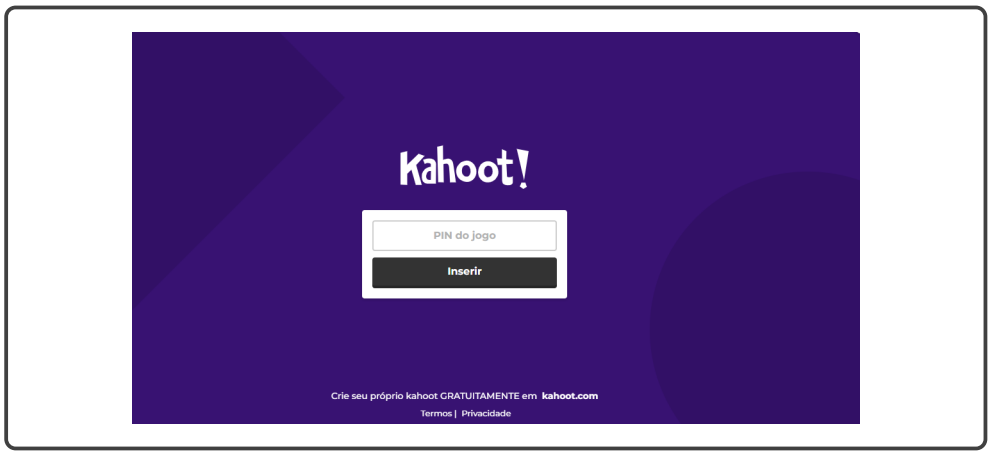
## Proposta 04: Desafio de Fatoração em um Jogo de Perguntas e Respostas

Querido aluno, está pronto para aplicar o conhecimento adquirido nas aulas de matemática sobre fatoração?

Acesse o link: `https://kahoot.it/`.

A imagem que está sendo exibida na sua tela será conforme ilustrado na Figura 3.6.

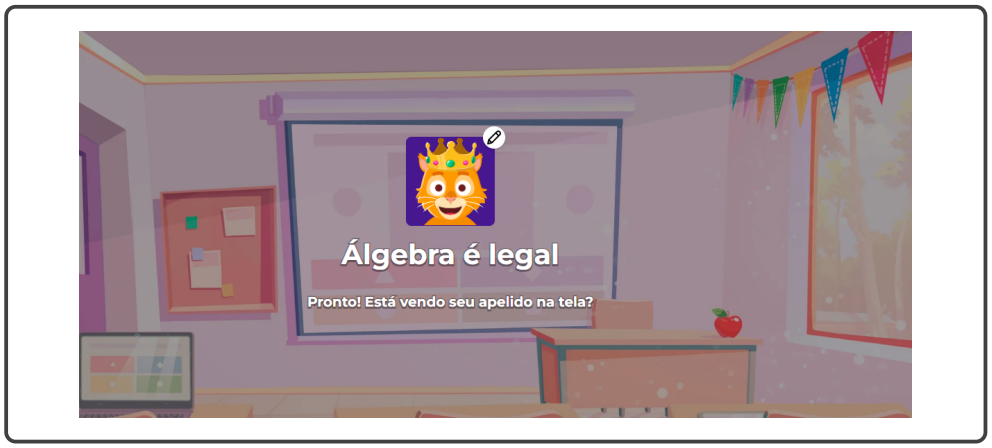
Figura 3.6 – PIN




Nessa tela, você deve inserir o número PIN do jogo, conforme o número informado pelo seu professor.

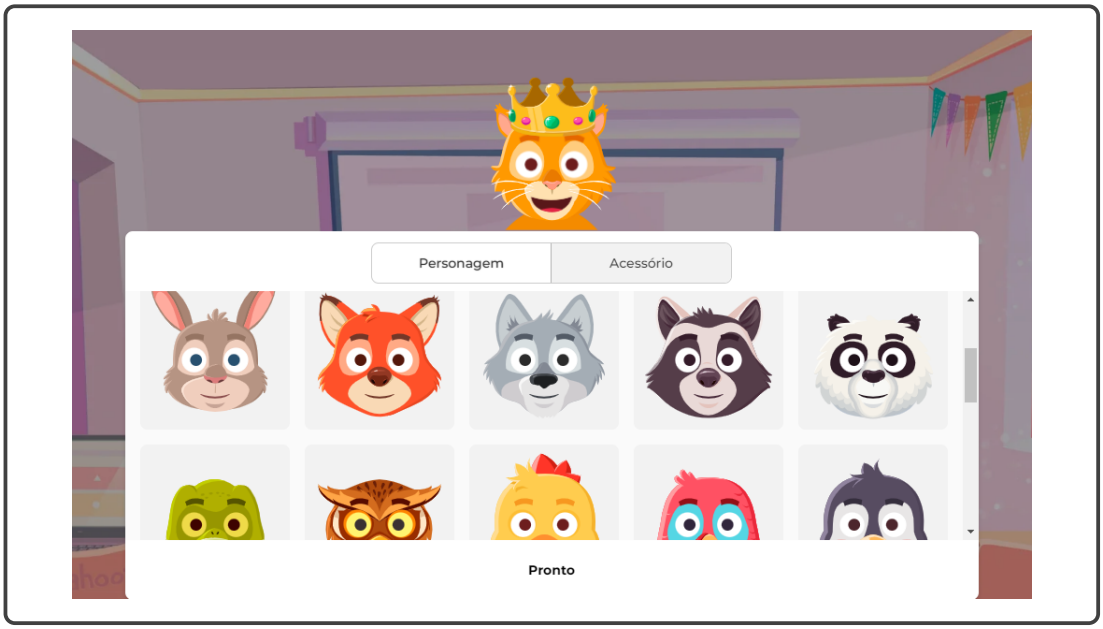
Agora, escolha um nome ou apelido para o seu avatar. Veja um exemplo de acordo com a Figura 3.7 em sua tela.

Figura 3.7 – Nome ou apelido do aluno



Logo depois, você pode personalizar seu avatar no jogo. Para fazer isso, basta clicar no ícone de lápis e escolher o avatar desejado, conforme ilustrado na Figura 3.8.

Figura 3.8 – Escolha do Avatar



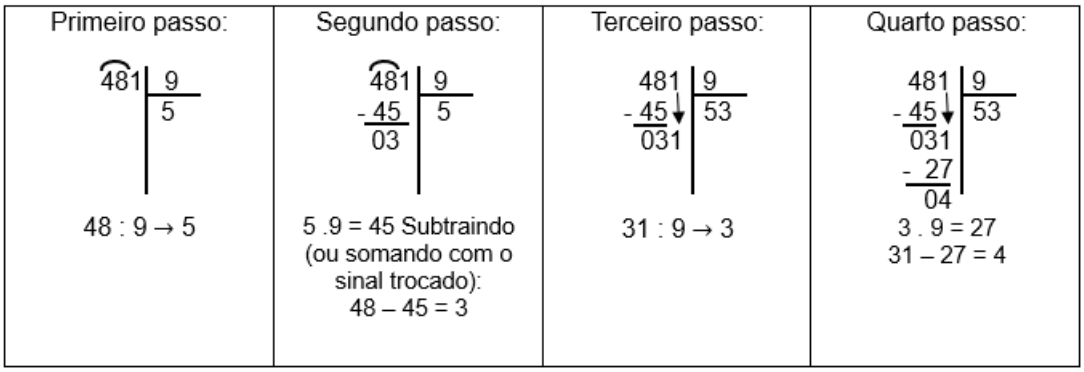

Avatar escolhido, pode clicar no botão iniciar, que seu avatar aparecerá na tela do seu professor. Aguarde todos os seus colegas entrarem no jogo.

Vamos jogar!

## Proposta 05: Divisão de polinômios pelo método da chave, aplicação na terceira série do Ensino Médio

Antes de iniciarmos a divisão entre polinômios vamos lembrar como resolvemos a divisão empregando números inteiros. Consideremos a seguinte divisão de números inteiros:

Figura 3.9 – Método da chave




Fonte: Acervo da Autora

Pela divisão acima, temos que

$$481 = 9 \cdot 53 + 4$$

em que 481 é o dividendo, 9 é o divisor, 53 é o quociente e 4 é o resto.

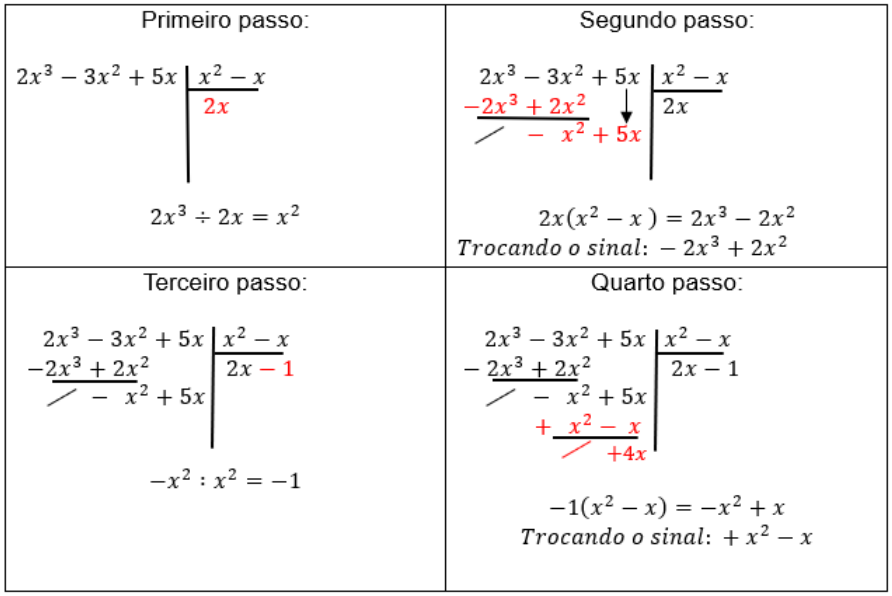
Vamos utilizar a mesma regra prática na divisão de polinômios.

Sejam $p(x)$ e $d(x)$ dois polinômios, com $d(x)$ não nulo, e gr($p$) o grau de $p(x)$ e d($d$) o grau de $d(x)$. Ao dividir $p(x)$ por $q(x)$, encontramos dois polinômios, $q(x)$, denominado quociente, e $r(x)$, denominado o resto. Esses dois polinômios devem satisfazer as seguintes condições:

- $p(x) = d(x) \cdot q(x) + r(x)$
- $r(x)$ é o polinômio nulo ou o grau de $r(x)$ deve satisfazer $0 \leq gr(r) \leq gr(d)$.

Aplicaremos o método da chave na divisão de $2x^3 - 3x^2 + 5x$ por $x^2 - x$. Veja a Figura 3.10.

Figura 3.10 – Método da chave para os polinômios



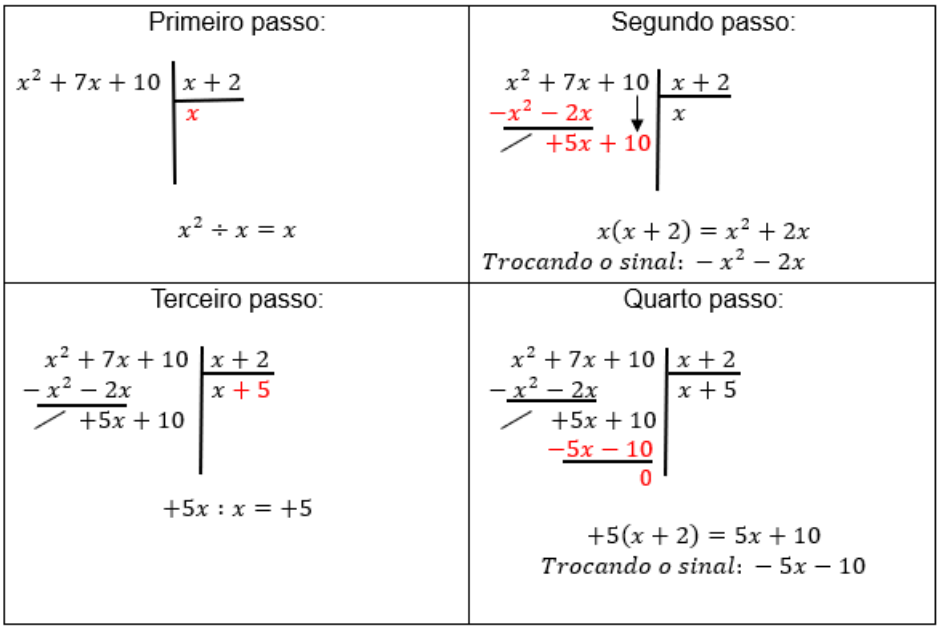

Fonte: Acervo da Autora

Lembre-se que $p(x) = d(x) \cdot q(x) + r(x)$. Assim,

$$2x^3 - 3x^2 + 5x = (x^2 - x) \cdot (2x - 1) + 4x.$$

Novamente, aplicaremos o método da chave na divisão de $x^2 + 7x + 10$ por $(x + 2)$. Veja a Figura 3.11.

Figura 3.11 – Método da chave para os polinômios




Fonte: Acervo da Autora

Lembre-se que $p(x) = d(x) \cdot q(x) + r(x)$. Assim,

$$x^2 + 7x + 10 = (x + 2) \cdot (x + 5) + 0.$$

Nesse caso, temos que $x^2 + 7x + 10$ é o dividendo, $x + 2$ é o divisor, $x + 5$ é o quociente e o polinômio nulo, 0, é o resto.

**Observações:**

- Quando o resto é nulo, $r(x) = 0$, dizemos que o polinômio $p(x)$ é divisível por $q(x)$, ou seja, a divisão é exata.
- O grau do quociente $q(x)$ sempre será a diferença entre os graus do dividendo $p(x)$ e do divisor $d(x)$ quando $\text{gr}(p) \geq \text{gr}(q)$.

### Atividade de Fixação

*Questão 1:* Divida o polinômio $p(x) = 4x^2+6x-12$ pelo polinômio $q(x) = 2x-1$ utilizando o método da chave, em seguida, determine o quociente e o resto da divisão.

Resposta:

*Questão 2:* Divida o polinômio $p(x) = 3x^2+10x-8$ pelo polinômio $q(x) = x+4$ utilizando o método da chave, em seguida, determine o quociente e o resto da divisão.

Resposta:

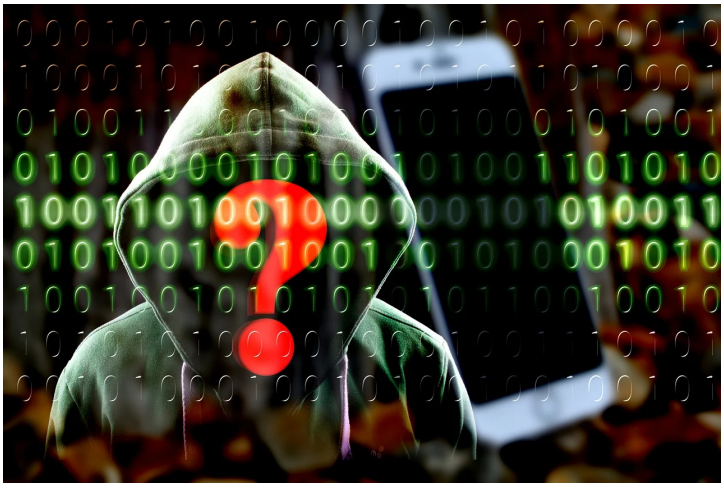
Com esta atividade, eu aprendi a:

- ☐ Compreender que na divisão de polinômios, a regra prática é semelhante ao método da chave utilizado para números inteiros.
- ☐ Realizar a divisão de polinômios, considerando $p(x)$ como o dividendo e $d(x)$ como o divisor, a fim de encontrar o quociente $q(x)$ e o resto $r(x)$ que atendam às condições $p(x) = d(x) \cdot q(x) + r(x)$.
- ☐ Observar que o polinômio resultante do quociente $q(x)$ deve ter um grau menor ou igual ao grau do dividendo $p(x)$ quando $\text{gr}(p) \geq \text{gr}(q)$.

## Proposta 06: Expressões algébricas e divisão

Você já se perguntou como é possível manter mensagens privadas em um mundo digital repleto de ameaças?

Figura 3.12 – Criptografia



Fonte: https://pixabay.com/illustrations/cyber-attack-encryption-smartphone-4444448/

A Criptografia RSA é responsável pela segurança do sistema RSA, e é um algoritmo de criptografia assimétrica que permite a segurança e a confidencialidade das informações disponibilizadas pela internet e outras comunicações.

Os responsáveis pelo desenvolvimento foram Ron Rivest, Adi Shamir e Leonard Adleman, em 1977, e tal algoritmo vem sendo aceito em sistemas criptográficos. Assim, percebemos como a matemática, especialmente na Álgebra, garante a segurança das comunicações digitais, um tópico relevante no contexto atual de tecnologia e informação.

Em resumo, chamamos essa criptografia de assimétrica pois existe um par de chaves diferentes em que uma delas tem a função de criptografar, enquanto a outra tem a função de descriptografar as informações. Tais chaves são conhecidas como: **chave pública** e **chave privada**.

A chave pública pode ser compartilhada com qualquer pessoa, ela é usada para criptografar dados antes de enviar, já a chave privada é secreta, sendo utilizada para descriptografar os dados recebidos.

O algoritmo está conectado à dificuldade de fatorar grandes números, ou seja, a segurança RSA consiste no fato de que a fatoração de grandes números primos é, computacionalmente ou não, um processo extremamente complicado e demorado.

A fatoração de números é a chave para quebrar a criptografia RSA, pois ele permitiria identificar os fatores primos essenciais para descobrir a chave privada e descriptografar uma mensagem.

E você? Está pronto para decodificar a seguinte palavra?

**[ 25, 1, 6, 1, 29, 14, 20, 13 ]**

**Objetivos a serem alcançados:**

- Introduzir a linguagem simbólica através do uso de símbolos e letras para representar quantidades desconhecidas;
- Resolver situações-problema que envolvam o cálculo do valor numérico de expressões algébricas;
- Compreender a relação entre a divisão aritmética e expressões algébricas através da criptografia;
- Explorar o processo de descriptografia usando equações;
- Usar a calculadora científica para calcular potências e divisão com resto;
- Interpretar os resultados na calculadora como letras do texto original;
- Analisar a relação entre os números criptografados, e as chaves pública e privada.

ATIVIDADE

Para essa atividade, uma palavra foi transformada em uma sequência de números utilizando a Tabela 2.

Tabela 2 – Letras do alfabeto e suas respectivas posições.

| **A** | **B** | **C** | **D** | **E** | **F** | **G** | **H** | **I** | **J** | **K** | **L** | **M** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |

| **N** | **O** | **P** | **Q** | **R** | **S** | **T** | **U** | **V** | **W** | **X** | **Y** | **Z** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |

Fonte: Acervo da Autora

Em seguida, foi utilizada a **chave pública**, $(n, e) = (33, 7)$, para codificar essa sequência de números, o que resultou na seguinte sequência de números:

**[ 25, 1, 6, 1, 29, 14, 20, 13 ]**.

Para decodificar essa palavra, ou seja, para descobrir qual palavra a sequência $[25, 1, 6, 1, 29, 14, 20, 13]$ representa, utilizamos a seguinte expressão:

$$x \equiv c^d \mod n.$$

Na qual:

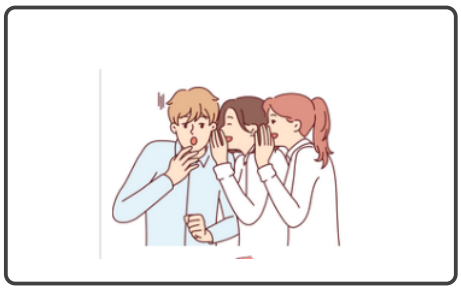
- $x$: é o resultado da operação de descriptografia. Representa a mensagem original que queremos obter.
- $c$: é o texto criptografado, ou seja, a mensagem que foi previamente criptografada usando a chave pública do destinatário.
- $d$: é a chave privada de descriptografia, essa chave é mantida em segredo pelo destinatário e é usada para descriptografar o texto criptografado c.
- $n$: é a chave pública e o módulo utilizado na operação de criptografia. É um número composto pela multiplicação de dois primos grandes, geralmente denominados $p$ e $q$. O valor de $n$ é utilizado tanto na criptografia quanto na descriptografia.

No entanto, o que significa a expressão $x \equiv c^d \mod n$? Significa que $x$ é o resto da divisão de $n$ por $c^d$.

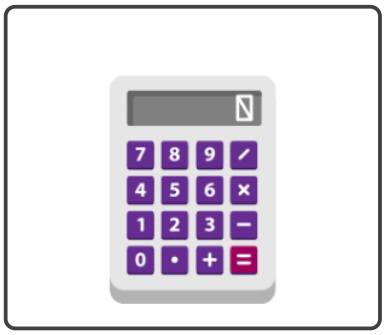
Vamos explicar como você deve proceder para completar o desafio de decodificar a palavra

$$[25, 1, 6, 1, 29, 14, 20, 13].$$

Para isso, vou te contar um segredo: "A chave privada é $d = 3$." Além disso, já sabemos que $n = 33$.



Com o uso de uma calculadora científica, calculamos $c^d$. Em seguida, o resultado obtido deverá ser dividido por $n$. O resto dessa divisão será o código referente à primeira letra, ou seja, o valor de $x$.



A agora, mostraremos como é o processo para realizar a decodificação da primeira letra da sequência. Nesse caso, temos os seguintes números: $c = 25$, $d = 3$ e $n = 33$. Temos que

$$25^3 = 15625$$

Em seguida, efetuando a divisão por 33 obtemos:

$$\begin{array}{r|l} 15625 & 33 \\ \cline{2-2} -\,132\phantom{00} & 473 \\ \cline{1-1} 242 & \\ -\,231 & \\ \cline{1-1} 115 & \\ -\,\phantom{1}99 & \\ \cline{1-1} 16 & \end{array}$$

Logo, o resto é 16. Temos que a letra desejada é a que está na posição 16 da Tabela **??**. Assim, a primeira letra da palavra é **P**.

Agora é com você!

Faça esse mesmo processo com os seguintes números da sequência

**[ 25, 1, 6, 1, 29, 14, 20, 13 ]**.

Com esta atividade, eu aprendi a:

- ☐ Explorar o processo de decodificação usando a equação para obter o número da mensagem original.
- ☐ Usar a calculadora científica para calcular potências e divisão com resto.
- ☐ Simplificar e desenvolver expressões algébricas.

# 4 Conclusão

Espero que o produto educacional desenvolvido possa contribuir com os professores que buscam aprimorar suas práticas pedagógicas no ensino da álgebra. A abordagem inovadora, a utilização de recursos tecnológicos e a integração da fatoração como ferramenta prática demonstram o potencial desse material para tornar o aprendizado da álgebra mais significativo para os estudantes.

Ao investir em metodologias que envolvam os alunos e promovam o desenvolvimento de habilidades essenciais, como o pensamento crítico e a resolução de problemas, os educadores estarão preparando os estudantes para enfrentar desafios futuros e utilizar a matemática de forma eficiente em suas vidas pessoais e profissionais.