UNIVERSIDADE ESTADUAL DE FEIRA DE SANTANA

Departamento de Ciências Exatas e da Terra

Mestrado Profissional em Matemática em Rede Nacional - PROFMAT

Dissertação de mestrado

RELAÇÕES DE GIRARD E ARITMÉTICA: CONSTRUÇÃO DOS CONCEITOS BÁSICOS E ATIVIDADES PARA O ENSINO FUNDAMENTAL E MÉDIO

Rosipléia Souza dos Santos

Orientador: Prof. Dr. Kisnney Emiliano de Almeida

Feira de Santana

Abril de 2014

UNIVERSIDADE ESTADUAL DE FEIRA DE SANTANA

Departamento de Ciências Exatas e da Terra

Mestrado Profissional em Matemática em Rede Nacional - PROFMAT

RELAÇÕES DE GIRARD E ARITMÉTICA: CONSTRUÇÃO DOS CONCEITOS BÁSICOS E ATIVIDADES PARA O ENSINO FUNDAMENTAL E MÉDIO

Dissertação apresentada ao Projeto de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT do Departamento de Ciências Exatas, UEFS, como requisito parcial para a obtenção do título de **Mestre**.

Orientador: Prof. Dr. Kisnney Emiliano de Almeida

Feira de Santana

Abril de 2014

Ficha Catalográfica – Biblioteca Central Julieta Carteado

Santos, Rosipléia Souza dos
S238r Relações de Girard e Aritmética : construção dos conceitos básicos e atividades para o ensino fundamental e médio / Rosipléias Souza dos Santos. – Feira de Santana, 2014.
65 f. : il.

Orientador: Kisnney Emiliano de Almeida.

Mestrado (dissertação) – Universidade Estadual de Feira de Santana, Programa de Pós-Graduação em Matemática, 2014.

1. Matemática – Estudo e ensino. 2. Relações de Girard. 3. Aritmética. 4. Ensino fundamental. 5. Ensino médio. I. Almeida, Kisnney Emiliano de, orient. II. Universidade Estadual de Feira de Santana. III. Título.

CDU: 51.09

UNIVERSIDADE ESTADUAL DE FEIRA DE SANTANA
DEPARTAMENTO DE CIÊNCIAS EXATAS
Mestrado Profissional em Matemática em Rede Nacional

PROFMAT

ATA DA SESSÃO PÚBLICA DE DEFESA DE DISSERTAÇÃO DA DISCENTE ROSIPLÉIA SOUZA DOS SANTOS DO PROGRAMA DE MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL DA UNIVERSIDADE ESTADUAL DE FEIRA DE SANTANA

Aos oito dias do mês de abril de dois mil e quatorze às 8:00 horas na sala MT55, Módulo 5, UEFS, ocorreu a Sessão pública de defesa de dissertação apresentada sob o título **"Relações de Girard e aritmética: construção dos conceitos básicos e atividades para o ensino fundamental e médio"**, da discente **Rosipléia Souza dos Santos**, do Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, UEFS, para obtenção do título de MESTRE. A Banca Examinadora foi composta pelos professores: Kisnney Emiliano de Almeida (Orientador, UEFS), Sérgio Mota Alves (UESC) e Maurício de Araujo Ferreira (UEFS). A sessão de defesa constou da apresentação do trabalho pela discente e das arguições dos examinadores.
Em seguida, a Banca Examinadora se reuniu em sessão secreta para julgamento final do trabalho e atribuiu o conceito: aprovado.
Sem mais a tratar, foi lavrada a presente ata, que segue assinada pelos membros da Banca Examinadora e pelo Coordenador Acadêmico Institucional do PROFMAT. Feira de Santana, 08 de abril de 2014.

Prof. Dr. Kisnney Emiliano de Almeida (UEFS)
Orientador

Prof. Dr. Sérgio Mota Alves (UESC)

Prof. Dr. Maurício de Araujo Ferreira (UEFS)

Visto do Coordenador:

Prof. Dr. Maurício de Araujo Ferreira
Coordenador do PROFMAT / UEFS

Agradeço

Ao meu Deus por ter me encorajado e capacitado durante esta jornada.

Aos meus pais, Domingos e Roselita, pela educação que me proporcionaram, pelo apoio incondicional e pelo carinho e cuidado de sempre.

Ao meu esposo, Anselmo Miranda, pela paciência, apoio e por todo amor a mim dedicado.

Ao meu filho, Juan Carlos, por trazer felicidade aos meus dias e por ser minha motivação.

Ao meu professor orientador Dr Kisnney Emiliano de Almeida pela dedicação, por estar sempre disponível independente de dia e horário e por não duvidar da minha capacidade em desenvolver este trabalho.

Aos demais professores que com suas aulas enriqueceram nosso saber.

Aos meus colegas de turma, em especial à Anatália, Joilma e Tenivâm, pelo companheirismo e amizade. Juntos as dificuldades tornaram-se bem menores.

À CAPES pelo apoio financeiro.

Resumo

Este trabalho tem por primeiro objetivo construir uma proposta didática de como ensinar métodos de encontrar as raízes inteiras ou racionais de polinômios de grau superior a dois utilizando propriedades de números inteiros, com mínima aplicação de fórmulas prontas. Dessa maneira, é dada ao aluno a oportunidade de exercitar simultaneamente e de maneira dinâmica os conceitos básicos de álgebra e aritmética presentes no ensino básico. Além disso, fazemos a construção cuidadosa dos conceitos envolvidos, à luz da álgebra abstrata moderna, sempre tentando relacionar os diferentes conceitos das áreas de álgebra e aritmética.

Palavras-chaves: Ensino de matemática, Relações de Girard, Aritmética.

Abstract

This work has a primary objective to build a didatic proposal for teaching methods to find the integer or rational roots of polynomials of degree greater than two,using properties of integers with minimal application of formulas. Thus the student is given the opportunity to exercise simultaneously and dynamically the basics of algebra and arithmetic present in basic education. In addition, we added a careful construction of the concepts involved in the light of the modern abstract algebra always, trying to relate the different concepts in the areas of algebra and arithmetic.

Keywords: Mathematics teaching, Girard's Relations, Arithmetic.

Conteúdo

Capítulo 1

Introdução

O ensino da álgebra na educação básica tem sido um desafio para nós professores da rede pública. Nossos alunos demonstram uma certa recusa por acharem que matemática está diretamente ligada a números e que as letras apenas atrapalham.

Em se tratando de polinômios, conteúdo estudado inicialmente no oitavo ano do ensino fundamental e aprofundado no terceiro ano do ensino médio, uma das maiores dificuldades é encontrar as raízes quando este polinômio tem grau superior a dois, visto que as fórmulas para encontrar tais raízes não fazem parte do conteúdo programático. Como uma abordagem alternativa, apresentaremos neste trabalho sugestões de atividades que exploram as relações de Girard, conteúdo visto completamente no terceiro ano do ensino médio, mas que pode ser parcialmente introduzido desde a primeira noção de raízes de polinômios; as principais propriedades de múltiplos e divisores inteiros; além de conteúdos que o aluno já deva ter visto em sua vida acadêmica como divisão e fatoração de polinômios, resolução de sistemas, entre outros.

Organizado em cinco capítulos, iniciamos falando um pouco de matemáticos como Bhaskara, Tartaglia, Cardano e Ferrari que contribuíram muito para o avanço do estudos dos polinômios descobrindo as fórmulas que, embora bastante trabalhosas, nos dão as raízes das equações do terceiro e quarto graus.

No segundo capítulo, faremos um estudo sobre Teoria de Anéis, abordando definições, proposições e apresentando alguns exemplos que são importantes para a construção dos conceitos de polinômios e números inteiros.

No terceiro capítulo é feito um estudo mais aprofundado sobre o anel dos números inteiros, as operações com suas propriedades, além de abordar alguns dos mais importantes teoremas. Falamos também sobre os números primos, que nos levam ao Teorema Fundamental da Aritmética.

O quarto capítulo é destinado ao estudo dos polinômios, suas operações, alguns teoremas e proposições. Fazemos uma abordagem sobre as relações entre as raízes e os coeficientes dos

polinômios, relações estas que são a principal ferramenta na resolução das atividades propostas.

Como um dos nossos objetivos é desenvolver o raciocínio lógico do educando levando-o a encontrar estratégias para resolução de problemas por caminhos que não sejam apenas aplicação de fórmulas prontas, destinamos o quinto capítulo para isto. Temos algumas propostas pedagógicas de atividades com as devidas resoluções, que podem ser facilmente adaptadas de modo a servirem como modelo para construção de muitas outras atividades. São estratégias de encontrar raízes de polinômios de grau três, quatro, e até seis usando apenas as relações de Girard e conhecimentos aritméticos que os educandos devem trazer de sua vida acadêmica. Temos também algumas atividades onde deve-se encontrar o polinômio dadas algumas informações acerca do mesmo entre outras.

A metodologia utilizada para conclusão deste trabalho foi a pesquisa bibliográfica, enriquecida com pesquisa em ambiente virtual.

1.1 Breve histórico

Dentre os matemáticos hindus que se destacaram com contribuições do desenvolvimento da álgebra, o que mais facilmente nos lembramos é Bhaskara, por estar ligado à fórmula geral da solução das equações polinomiais do segundo grau. No entanto, a fórmula que leva seu nome não foi descoberta por ele, conforme o próprio relatou no século XII. Um século antes, o matemático hindu Sridhara (c. 870, Índia – c. 930 Índia) teria encontrado a mencionada fórmula e publicado em uma obra que se perdeu.

A ideia de encontrar uma forma de reduzir uma equação polinomial de 2^o grau para o primeiro através da extração de raízes quadradas foi o instrumento usado com sucesso pelos hindus na busca pela fórmula geral que conhecemos hoje. Segundo Eves (2002), em textos babilônicos, escritos há cerca de 4000 anos, encontram-se descrições de procedimentos para resolução de problemas envolvendo equações do segundo grau. O autor menciona também que na Grécia, utilizava-se geometria para resolver tais equações. A partir do início do século IX, matemáticos árabes já haviam se empenhado na resolução de equações do segundo grau, cujos procedimentos utilizaram álgebra e geometria dos gregos, e, em decorrência, fórmulas específicas para tipos diferentes de equação surgiram. Contudo, o aparecimento de uma fórmula geral para se obter as raízes de uma equação do segundo grau está situado por volta do final do século XVI.

Eis, então, a fórmula de Bhaskara, que, embora não tenha sido deduzida por ele, imortalizou seu nome.

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Segundo Garbi (1997), vencidas as equações do segundo grau, a inesgotável curiosidade dos

matemáticos levou-os a conjecturar sobre as formas de resolver as do terceiro. Apesar de não terem encontrado a solução para o problema, os árabes tiveram um importante papel no estudo dessas equações. Girolamo Cardano, nascido em Pavia em 1501 e falecido em Roma em 1576, e Nicoló Fontana, apelidado Tartaglia, nascido em Bréscia em 1500, disputaram pelas equações do terceiro grau.

Por volta de 1510, Scipione Del Ferro, matemático italiano, encontrou uma forma geral de resolver equações polinomiais de terceiro grau do tipo $x^3 + px + q = 0$, mas não a publicou até sua morte. Seu aluno, Antonio Maria Fior, para o qual Del Ferro revelou a solução antes de morrer, aproveitando-se desse conhecimento desafiou Tartaglia visando ganhar notoriedade, já que este era bastante conhecido por seu talento nos estudos. Sabendo da intenção de Fior, Tartaglia dedicou-se entusiasticamente em encontrar uma solução para as equações das quais seria submetido ao desafio, e foi mais longe, encontrando também a fórmula geral para a resolução das equações do tipo $x^3 + px^2 + q = 0$.

O resultado do desafio não poderia ter sido diferente: Tartaglia venceu resolvendo corretamente todos os problemas propostos, enquanto Fior saiu humilhado por não conseguir resolver nenhum dos que lhe foi proposto por se tratar de equações do tipo $x^3 + px^2 + q = 0$, sobre as quais não detinha conhecimento algum.

Cardano, que estava escrevendo a *Prática Arithmeticae Generalis* nesta época, acreditando na impossibilidade de uma solução geral para as equações do terceiro grau, ficou sabendo do ocorrido e resolveu pedir a Tartaglia que revelasse a solução encontrada a fim de publicar em sua obra. Tartaglia não concordou e diante da recusa Cardano o insultou gravemente. Algum tempo depois, Cardano investiu em formas de conseguir convencer Tartaglia a revelar as tão cobiçadas fórmulas, até que conseguiu sob juramento de jamais revelá-las, contudo, não foi exatamente o que aconteceu. Quebrando suas promessas e juramentos, Cardano, em 1545, publicou a fórmula revelada por Tartaglia que, nada contente por ter sua obra revelada, publicou sua versão dos fatos e denunciou Cardano por haver traído um sagrado juramento sobre a Bíblia.

Assim como ocorreu com a fórmula de Bhaskara, a fórmula da resolução das equações polinomiais de terceiro grau não recebeu o nome do seu verdadeiro criador, e hoje é conhecida como Fórmula de Cardano.

Vejamos a ideia de Tartaglia: supondo que a solução procurada era composta de duas parcelas, escreveu $x = A + B$ e elevou ambos os membros ao cubo. Assim, obteve

$$x^3 = (A + B)^3$$

$$x^3 = A^3 + B^3 + 3AB(A + B)$$

como $x = A + B$, substituindo

$$x^3 = A^3 + B^3 + 3ABx,$$

donde

$$x^3 - 3ABx - (A^3 + B^3) = 0$$

fazendo $p = -3AB$, ou melhor, $A^3B^3 = -\frac{p^3}{27}$ e

$$q = -(A^3 + B^3) \Longrightarrow A^3 + B^3 = -q$$

assim, conhecemos a soma e o produto de A^3 e B^3, recaindo no clássico problema que se resolve com equações de segundo grau.

$$A^3 = -\frac{q}{2} \pm \sqrt{(\frac{q}{2})^2 + (\frac{p}{3})^3} \quad \text{e} \quad B^3 = -\frac{q}{2} \mp \sqrt{(\frac{q}{2})^2 + (\frac{p}{3})^3}.$$

Como $x = A + B$,

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{(\frac{q}{2})^2 + (\frac{p}{3})^3}} + \sqrt[3]{-\frac{q}{2} + \sqrt{(\frac{q}{2})^2 - (\frac{p}{3})^3}}.$$

E chegamos à fórmula de Cardano, que não foi descoberta por ele, e sim por Tartaglia.

Submetido ao desafio de resolver uma equação de quarto grau, Cardano, após inúmeras tentativas sem sucesso, passou a questão para seu jovem e prodigioso discípulo Ludovico Ferrari. Nascido em 1522 na cidade de Bolonha, Ferrari teve sua brilhante inteligência reconhecida muito cedo por seu mestre e, com sua genialidade, encontrou o método geral para a solução das citadas equações, o qual foi publicado por seu mestre, Cardano, na *Ars Magna*. Olhando a equação

$$x^4 + px^2 + qx + r = 0$$

Ferrari, segundo Garbi (1997), procurou reagrupar os termos de modo que nos dois lados da igualdade houvesse polinômios quadrados perfeitos. Se tal reagrupamento fosse possível, seriam extraídas as raízes quadradas, cair-se-ia em equações do 2º grau e o problema estaria resolvido.

Reescrevendo a equação, chega-se a

$$x^4 + (p + \alpha)x^2 + (r + \beta) = \alpha x^2 - qx + \beta$$

E então, fazendo os cálculos e substituições convenientes chegamos à fórmula de Ferrari:

$$\sqrt{x^4 + (p + \alpha)x^2 + (r + \beta)} = \pm\sqrt{\alpha x^2 - qx + \beta}$$

Embora muito trabalhoso, o método desenvolvido por Ferrari nos fornece as soluções de uma equação polinomial de quarto grau apenas com operações algébricas, fato que merece destaque.

Para o caso de equações de grau 5, Abel provou que não existem soluções por radicais para encontrar suas raízes, como nos casos anteriores. Posteriormente Galois generalizou esse resultado, mostrando que o mesmo valia para equações de grau maior. Mesmo para equações de grau pequeno, os métodos acima podem ser muito trabalhosos e pouco interessantes para o aprendizado do aluno do ensino básico. Ao restringirmos o problema para encontrar raízes inteiras, o mesmo se torna bem mais interessante, por permitir a utilização e exercício de conceitos básicos de aritmética. A partir do próximo capítulo, desenvolveremos a fundamentação teórica para a exposição de algumas atividades com esse intuito.

Capítulo 2

Conceitos básicos de Teoria de Anéis

Nesse capítulo está a fundamentação teórica do trabalho: definições e resultados preliminares de teoria de anéis, que, com as devidas adaptações, podem ser aplicados tanto aos conjuntos numéricos ($\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$) quanto aos conjuntos de polinômios e suas operações. Nossas principais referências são Gonçalves (2008), Domingues e Iezzi (1982) e Lequain e Garcia (2008).

2.1 Definições e Exemplos

Seja A um conjunto não vazio. Vamos definir duas operações, as quais chamaremos de *soma* e *produto* em A e denotaremos por $+$ e $\cdot$. Assim,

$$+ : A \times A \to A \qquad \cdot : A \times A \to A$$

$$(a, b) \rightsquigarrow a + b \qquad (a, b) \rightsquigarrow a \cdot b.$$

Definição 2.1.1. O trio $(A, +, \cdot)$ é um *Anel* se são verificadas as seguintes propriedades:

A1) $(a + b) + c = a + (b + c)$ (associatividade da soma);

A2) Existe $0 \in$ A tal que $a + 0 = 0 + a = a$ (existência do elemento neutro da soma);

A3) Para todo $x \in A$ existe um único y pertencente a A, denotado por $y = -x$, tal que $x + y = y + x = 0$ (existência do inverso aditivo);

A4) $a + b = b + a$ (comutatividade da soma);

A5) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (associatividade do produto);

A6) $a \cdot (b + c) = a \cdot b + a \cdot c$; $(a + b) \cdot c = a \cdot c + b \cdot c$ (distributividade à esquerda e à direita).

Se um anel $(A, +, \cdot)$ satisfaz a propriedade:

A7) Existe $1 \in A, 0 \neq 1$ tal que $x \cdot 1 = 1 \cdot x = x$ para todo $x \in A$,

dizemos que $A, +, \cdot$ é um *anel com unidade*.

Se um anel $(A, +, \cdot)$ satisfaz a propriedade:

A8) Para quaisquer $x, y \in A, x \cdot y = y \cdot x$,

dizemos que $A, +, \cdot$ é um *anel comutativo*.

Se um anel $(A, +, \cdot)$ satisfaz a propriedade:

A9) $x, y \in A, x \cdot y = 0 \Rightarrow x = 0$ ou $y = 0$, dizemos que $(A, +, \cdot)$ é um *anel sem divisores de zero*.

Se $(A, +, \cdot)$ é um anel comutativo, com unidade e sem divisores de zero, dizemos que $(A, +, \cdot)$ é um *Domínio de Integridade*.

Se um Domínio de Integridade $(A, +, \cdot)$ satisfaz a propriedade:

A10) Para todo $x \in A, x \neq 0$, existe $y \in A$ tal que $x \cdot y = y \cdot x = 1$, dizemos que $(A, +, \cdot)$ é um *Corpo*.

Por uma questão de praticidade, quando não houver ambiguidade com relação às operações representaremos o anel $(A, +, \cdot)$ apenas por A.

Exemplo 2.1.2. Alguns exemplos de anéis comutativos com unidade são os conhecidos anéis numéricos, com as operações usuais: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Mais ainda, é fácil ver que são todos domínios de integridade e que $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ são corpos.

Exemplo 2.1.3. Um exemplo de anel numérico menos conhecido é

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

com p sendo um número natural primo, que, com as operações usuais, também é um domínio de integridade. Definimos as operações de soma e produto em $Z[\sqrt{p}]$ da seguinte forma:

Dados $r, s \in \mathbb{Z}[\sqrt{p}]$, então existem inteiros a, b, c, d tais que $r = a + b\sqrt{p}$ e $s = c + d\sqrt{p}$, assim,

$$r + s := (a + c) + (b + d)\sqrt{p}$$

$$r \cdot s := (ac + pbd) + (ad + bc)\sqrt{p}.$$

Podemos também definir o anel

$$\mathbb{Q}[\sqrt{p}] = \{a + b\sqrt{p} \,|\, a, b \in \mathbb{Q}\},$$

que nesse caso é um corpo, com operações análogas.

Para mais detalhes sobre esses anéis, ver [10], p. 35.

Exemplo 2.1.4. As classes de congruência de inteiros módulo n, com $n \geq 2$, com as operações usuais de soma e produto, também formam um anel comutativo com unidade:

$$\mathbb{Z}_n := \left\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\right\}.$$

O anel $\mathbb{Z}_n$ é um domínio de integridade se e somente se é um corpo se e somente se n é primo. Para mais detalhes, ver [4] (1982), p. 141.

Se n não é primo, então $\mathbb{Z}_n$ possui divisores de zero. Por exemplo, em $\mathbb{Z}_6$ temos $\overline{2} \cdot \overline{3} = 0$, logo $\overline{2}$ e $\overline{3}$ são divisores de zero.

Exemplo 2.1.5. $n\mathbb{Z}$, o anel dos inteiros múltiplos de n, com as operações usuais, é um anel comutativo. Se $n \geq 2$, é anel comutativo que não possui unidade.

Exemplo 2.1.6. $M_2(\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} ; a, b, c, d \in \mathbb{R} \right\}$, o anel de matrizes quadradas de ordem 2, com as operações usuais de matrizes, é um exemplo de anel com unidade não comutativo.

Definição 2.1.7. Seja $(A, +, \cdot)$ um anel. Dizemos que um subconjunto $B \subset A$, $B \neq \emptyset$, é um *subanel* de A se B é um anel com as mesmas operações de A. Usaremos a notação $B \leq A$ para representar que B é um subanel de A.

Exemplo 2.1.8. É fácil ver que $2\mathbb{Z}$ é um subanel de $\mathbb{Z}$. De fato, a soma e o produto de dois números pares são números pares. Além disso tanto a adição como a multiplicação de números pares são associativas, a adição é comutativa, o número zero é par e o oposto de um número par também é um número par. Finalmente, a multiplicação de números pares é distributiva em relação à adição.

Este exemplo mostra que um subanel de um anel com unidade não possui necessariamente unidade.

Exemplo 2.1.9. Seja $n \in \mathbb{N}$. Então,

1. $$n\mathbb{Z} \leq Z \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}.$$

2. $$n\mathbb{Z} \leq \mathbb{Z} \leq \mathbb{Z}[\sqrt{p}] \leq \mathbb{Q}[\sqrt{p}] \leq \mathbb{R}.$$

2.2 Ideais

Ideais compõem um tipo de subanel que é especialmente importante para o estudo de teoria de anéis.

Definição 2.2.1. Seja A um anel comutativo com unidade. Dizemos que um subconjunto $I \subset A$, $I \neq \emptyset$, é um ideal de A se

(i) $x, y \in I \Rightarrow x + y \in I$;

(ii) $x \in I$ e $a \in A \Rightarrow ax \in I$.

Exemplo 2.2.2. No anel $\mathbb{Z}$ dos números inteiros todos os subconjuntos

$$n\mathbb{Z} = \{nq \,|\, q \in \mathbb{Z}\},$$

onde n é um número inteiro dado, são ideais. De fato:

$0 \in n\mathbb{Z}$ uma vez que $0 = n0$;

(i) $nq_1 + nq_2 = n(q_1 + q_2) \in n\mathbb{Z}$;

(ii) $a(nq) = n(aq) \in n\mathbb{Z}, \forall a \in \mathbb{Z}$

.

Exemplo 2.2.3. Para todo anel A, são ideais em A os subconjuntos $\{0\}$ e A. São os chamados *ideais triviais* de A.

Observação 2.2.4. É fácil ver que todo ideal de um anel A é um subanel de A. Contudo, a reciproca não vale. Por exemplo, $\mathbb{Z}$ é um subanel de $\mathbb{Q}$ mas não é um ideal em $\mathbb{Q}$. Basta notar que $1 \in \mathbb{Z}$, $\frac{1}{2} \in \mathbb{Q}$, mas $\frac{1}{2} \cdot 1 = \frac{1}{2} \notin \mathbb{Z}$.

Um elemento $u \neq 0$ de um anel com unidade A é invertível se e somente se existe um elemento $v \in A$, chamado inverso multiplicativo de u, tal que $u \cdot v = v \cdot u = 1$. É fácil ver que, se o inverso de um elemento existe, ele é único. Denotaremos por u^{-1} o inverso multiplicativo de u.

Proposição 2.2.5. *Seja I um ideal num anel comutativo com unidade A. Se existe um elemento inversível $u \in A$ tal que $u \in I$, então $I = A$.*

Demonstração. Seja $a \in A$. Podemos escrever $a = a \cdot 1$. Como u é inversível, existe um elemento $v \in A$ de maneira que $uv = 1$. Donde $a = a(uv) = u(av)$, e, pela definição de ideal,

$$av \in A \text{ e } u \in I \Rightarrow a = u(av) \in I,$$

e podemos concluir que $a \in I$. Provamos assim que $A \subset I$. Como obviamente $I \subset A$, temos então que $I = A$. □

Definição 2.2.6. Seja A um anel comutativo com unidade. Tomemos $a_1, a_2, a_3, ..., a_n \in A$, com $n \geq 1$. Indiquemos por $\langle a_1, a_2, a_3, ..., a_n \rangle$ o seguinte subconjunto de A:

$$\langle a_1, a_2, a_3, ..., a_n \rangle := \{x_1a_1 + x_2a_2 + x_3a_3 + \cdots + x_na_n \,|\, x_i \in A \ \forall i \in \mathbb{N}\}.$$

Tal subconjunto é um ideal em A.

Verifiquemos:

✓ $0 = 0a_1 + 0a_2 + \cdots + 0a_n \Rightarrow 0 \in \langle a_1, a_2, a_3, \ldots, a_n \rangle$.

✓ $r, s \in \langle a_1, a_2, a_3, \ldots, a_n \rangle \Rightarrow \begin{cases} \exists x_1, \ldots, x_n \in A \,|\, r = x_1a_1 + \cdots + x_na_n \\ \exists y_1, \ldots, y_n \in A \,|\, s = y_1a_1 + \cdots + y_na_n \end{cases}$

Daí,

$$r + s = (x_1 + y_1)a_1 + (x_2 + y_2)a_2 + ... + (x_n + y_n)a_n \in \langle a_1, a_2, a_3, ..., a_n \rangle.$$

✓ Seja $y \in A$ e $r \in \langle a_1, a_2, a_3, ..., a_n \rangle$. Então,

$$yr = (yx_1)a_1 + (yx_2)a_2 + (yx_3)a_3 + ... + (yx_n)a_n \in \langle a_1, a_2, a_3, ..., a_n \rangle.$$

Definição 2.2.7. O ideal $\langle a_1, a_2, a_3, ..., a_n \rangle$ obtido segundo as considerações acima é chamado *ideal gerado* por $a_1, a_2, a_3, ..., a_n$. Um ideal gerado por um único elemento $a \in A$ é chamado *ideal principal* gerado por a. Neste caso, além da notação $\langle a \rangle$, usaremos também aA.

Se todos os ideais de um domínio de integridade são principais, então este anel é chamado de *domínio principal*.

Exemplo 2.2.8. $\mathbb{Z}$ é um domínio principal (*cf.* Teorema 3.1.7).

Exemplo 2.2.9. Se K é um corpo, então $K[x]$, o anel de polinômios com coeficientes em K, é um domínio principal (*cf.* Teorema 4.1.10). A hipótese de que K é um corpo é necessária: por exemplo, $\mathbb{Z}[x]$, o anel de polinômios com coeficientes em $\mathbb{Z}$, é um domínio que não é principal (*cf.* Exemplo 4.1.13).

Exemplo 2.2.10. $Z[i] := \{a + bi \,|\, a, b \in Z\} \leq \mathbb{C}$, o anel dos inteiros de Gauss, é um domínio principal (ver [8], 2008 p.22).

Exemplo 2.2.11. $K[x, y]$, o anel de polinômios com duas variáveis com coeficientes em um corpo K, não é domínio principal. (ver [8], 2008 p.48)

Se I e J são ideais em A, indicaremos por $I + J$ o seguinte subconjunto de A:

$$I + J := \{x + y \,|\, x \in I \text{ e } y \in J\}$$

Trata-se também de um ideal de A, porque, além de não ser vazio (pois $0 \in I$ e $0 \in J \Rightarrow 0 \in I + J$),

$0 = 0 + 0 \ \in \ I + J$;

(i) $r, s \in I + J \Rightarrow r = x_1 + y_1$ e $s = x_2 + y_2$ com $x_1, x_2 \in I$ e $y_1, y_2 \in J$. Então,

$$r + s = (x_1 + x_2) + (y_1 + y_2) \in I + J.$$

(ii) $t \in I + J$ e $a \in A \Rightarrow t = x + y \in I + J$ com $x \in I$ e $y \in J$. Então,

$$at = ax + ay \in I + J.$$

Dados os ideais I e J num anel comutativo A pode-se mostrar que

$$I \cap J := \{a \in A \,|\, a \in I \text{ e } a \in J\}$$

também é um ideal em A. De fato,

$0 \in I$ e $0 \in J \Rightarrow 0 \in I \cap J$.

(i) Se $x, y \in I \cap J \Rightarrow x, y \in I$ e $x, y \in J \Rightarrow$

$$x + y \in I \text{ e } x + y \in J \Rightarrow x + y \in I \cap J.$$

(ii) Se $x \in I \cap J$ e $a \in A \Rightarrow x \in I, x \in J$ e $a \in A$

$$ax \in I \text{ e } ax \in J \Rightarrow ax \in I \cap J.$$

Proposição 2.2.12. *Sejam I e J ideais num anel comutativo A. Então:*

a) $I \cap J$ é o maior ideal contido em I e em J;

b) $I + J$ é o menor ideal que contém I e J.

Demonstração. Naturalmente o "maior" e o "menor" que figuram no enunciado referem-se à relação de ordem "inclusão".

(a) Seja L um ideal em A tal que $L \subset I$ e $L \subset J$. Então $L \subset I \cap J$.

(b) Seja L um ideal em A tal que $I \subset L$ e $J \subset L$. Então:

$r \in I + J \Rightarrow \exists\ x \in I$ e $\exists\ y \in J$ tal que $r = x + y \Rightarrow r \in L$ pois,

$$x, y \in L \Rightarrow x + y \in L.$$

Logo $I + J \subset L$. □

Exemplo 2.2.13. Quem é o ideal $2\mathbb{Z} + 3\mathbb{Z}$?

Temos que $2\mathbb{Z} + 3\mathbb{Z} = \{x + y \,|\, x \in 2\mathbb{Z},\ y \in 3\mathbb{Z}\}$. Assim, todo elemento de $\mathbb{Z}$ que se escreve como uma soma de um múltiplo de 2 e um múltiplo de 3 está neste ideal. Como sabemos escrever 1=-2+3, segue que $1 \in 2\mathbb{Z} + 3\mathbb{Z}$, ou seja $2\mathbb{Z} + 3\mathbb{Z} = \mathbb{Z}$ (pela Proposição 2.2.5).

Exemplo 2.2.14. a) $\langle \frac{3}{8} \rangle$ em $\mathbb{Q}$ será igual a $\mathbb{Q}$, pois $\frac{3}{8}$ é inversível em $\mathbb{Q}$.

b) $\langle -\frac{2}{5} \rangle$ em $\mathbb{R}$ será igual a $\mathbb{R}$, pois $-\frac{2}{5}$ é inversível em $\mathbb{R}$.

c) $\langle 3 \rangle$ em $2\mathbb{Z}$ será igual a $3 \cdot 2\mathbb{Z} = 6\mathbb{Z}$.

d) Em $\mathbb{Z}$, $\langle 6, 21 \rangle = \langle 6 \rangle + \langle 21 \rangle = \{x + y \,|\, x \in 6\mathbb{Z}, y \in 21\mathbb{Z}\}$.

e) Em $\mathbb{Z}$, $\langle 6 \rangle \cap \langle 2 \rangle = \{x \in \mathbb{Z} \,|\, x \in 6\mathbb{Z}$ e $y \in 21\mathbb{Z}\}$.

f) $\langle \sqrt{2} \rangle = \{0a + b\sqrt{2} \in \mathbb{Z} \,|\, a, b \in \mathbb{Z}\}$ é um ideal de $\mathbb{Z}[\sqrt{2}]$ que representa os múltiplos de $\sqrt{2}$.

g) Em $\mathbb{Z}$, $\langle 4, 6, 10 \rangle = \langle 4 \rangle + \langle 6 \rangle + \langle 10 \rangle = \{x + y + z \in \mathbb{Z} \,|\, x \in 4\mathbb{Z}, y \in 6\mathbb{Z}, z \in 10\mathbb{Z}\}$.

Capítulo 3

Inteiros

O conjunto dos números inteiros, suas operações e propriedades foram fonte de inspiração para muitos conceitos de teoria de anéis. Neste capítulo, faremos uma revisão das principais propriedades dos números inteiros, apresentando, sempre que possível, demonstrações utilizando os conceitos de teoria de anéis desenvolvidos no capítulo anterior.

É fácil ver que, com as definições usuais de soma e produto, $\mathbb{Z}$ é um domínio de integridade.

3.1 Divisibilidade e divisão eucliciana

Definição 3.1.1. Diz-se que um número inteiro a *divide* um inteiro b se $b = ac$, para algum $c \in \mathbb{Z}$. Neste caso diz-se também que a é *divisor* de b e que b é *múltiplo* de a. Ou ainda que b é *divisível* por a. Indicaremos por $a \mid b$ o fato de a dividir b; e se a não divide b, escrevemos $a \nmid b$. O elemento $c \in \mathbb{Z}$ tal que $b = ac$, onde $a \neq 0$ é indicado por $c = \frac{b}{a}$ e é chamado quociente de b por a.

Exemplo 3.1.2. a) $2 \mid 6$ pois $6 = 2 \cdot 3$;

b) $-5 \mid 20$ pois $20 = -5 \cdot 4$;

c) $1 \mid a$ $(\forall a \in \mathbb{Z})$ pois $a = 1 \cdot a$ para todo $a \in \mathbb{Z}$;

d) Se $b \neq 0$, então $0 \nmid b$ pois $0 \cdot c = 0$ para todo $c \in \mathbb{Z}$.

Proposição 3.1.3. *A relação de divisibilidade possui as seguintes propriedades:*

(d_1) Se $a \neq 0$ então $a \mid 0$ e $a \mid a$.

(d_2) Se $a \neq 0$, $b \neq 0$, $a \mid b$ e $b \mid c$ então $a \mid c$.

(d_3) Se $a \neq 0$, $a \mid (b + c)$ e $a \mid b$, então $a \mid c$.

(d_4) Se $a \neq 0$, $a \mid b_1, \ldots, a \mid b_n$, então $a \mid b_1c_1 + \cdots + b_nc_n$ para quaisquer $c_1, \ldots, c_n$.

(d_5) $1 \mid a$ para todo $a \in \mathbb{Z}$.

(d_6) Se $a \neq 0$, $c \neq 0$, $a \mid b$ e $c \mid d$ então $a \cdot c \mid b \cdot d$.

A demonstração dessas tópicos é simples e pode ser encontrada em [3] p.31-32.

Observação 3.1.4. a) Se a e b são inteiros positivos e $a \mid b$ então $a \leq b$.

b) $a|b$ se e somente se $b\mathbb{Z} \subset a\mathbb{Z}$. De fato, se $a|b$, então $\exists\ n \in \mathbb{Z}$ tal que $b = a \cdot n$ logo $b \in a\mathbb{Z}$. Como todo elemento de $b\mathbb{Z}$ é escrito na forma bx, então $bx = a(nx)$ e todo elemento de $b\mathbb{Z}$ está em $a\mathbb{Z}$, logo $b\mathbb{Z} \subset a\mathbb{Z}$ Reciprocamente, $b\mathbb{Z} \subset a\mathbb{Z}$ então b pode ser escrito na forma an para algum $n \in \mathbb{Z}$. Desta forma, $b = an \Rightarrow a \mid b$.

Uma propriedade conhecida dos números inteiros é o **Princípio da Boa Ordenação (PBO)**: Todo subconjunto não vazio S de $\mathbb{Z}$ de elementos não negativos possui um primeiro elemento, isto é, $\exists\ x_0 \in S$ tal que $x_0 \leq x,\ \forall x \in S$.

A partir dessa propriedade, podemos estabelecer o algoritmo de divisão de Euclides.

Teorema 3.1.5 (Algoritmo da Divisão)**.** *Sejam a e b, tais que $a \geq 0$ e $b > 0$ então existem inteiros q e r tais que $a = bq + r$, e $0 \leq r < b$. Os inteiros q e r, nas condições acima, são únicos e são chamados, respectivamente, de quociente e resto da divisão euclidiana de a por b.*

Demonstração. (**Existência**) Considere o conjunto

$$S := \{a - bx \mid x \in \mathbb{Z} \text{ e } a - bx \geq 0\}.$$

Observe que $a \in S$, pois $a = a - b \cdot 0$ e $a \geq 0$. Logo S não é vazio. Assim, temos que S é um subconjunto dos números naturais, não vazio. Então, pelo Princípio da Boa Ordenação, existe em S um elemento mínimo, o qual denotaremos por r.

$$r \in S \Rightarrow r \geq 0 \text{ e } r = a - bq \text{ para algum } q \in \mathbb{Z}.$$

Falta mostrar que $r < b$. De fato, suponha por absurdo que $r \geq b$.

$r \geq b \Rightarrow a - bq \geq b \Rightarrow a - bq - b \geq 0 \Rightarrow a - b(q+1) \geq 0 \Rightarrow a - bq - b \in S \Rightarrow a - bq - b \geq r \Rightarrow r - b \geq r \Rightarrow -b \geq 0 \Rightarrow b \leq 0$, o que é um absurdo, pois por hipótese $b > 0$.

(**Unicidade**) Suponha que existam $q, q', r, r' \in \mathbb{Z}$, com $q \neq q'$ e $r \neq r'$, tais que

$$a = bq + r = bq' + r'$$

com $0 \leq r, r' < b$.

$$bq + r = bq' + r' \Rightarrow b(q - q') = r - r'$$

$$0 \leq r \text{ e } 0 \leq r' \Rightarrow |\, r' - r \,| < b$$

Assim, $b(q - q') = r' - r \Rightarrow |\, b(q - q') \,| = |\, r' - r \,| \Rightarrow b\,|\, q - q' \,| = |\, r' - r \,| < b \Rightarrow |\, q - q' \,| < 1$

Como $q - q'$ é um número inteiro, temos que $q - q' = 0$ e assim, $r' - r = 0 \Rightarrow q = q'$ e $r = r'$. □

Exemplo 3.1.6. Sejam $n = 39$ e $d = 7$, então $39 = 5 \cdot 7 + 4$, assim, $q = 5$ e $r = 4$.

O teorema a seguir evidencia uma importante propriedade do anel dos números inteiros.

Teorema 3.1.7. *Todo ideal de $\mathbb{Z}$ é principal, logo $\mathbb{Z}$ é um domínio principal.*

Demonstração. Sabemos que $I = n\mathbb{Z}$ é um ideal de $\mathbb{Z}$ para todo $n \in \mathbb{Z}$, pelo Exemplo 2.2.2.

Vejamos que todo ideal de $\mathbb{Z}$ é desta forma.

Se $I = 0$, então $I = 0\mathbb{Z}$. Suponhamos $I \neq 0$, então existe $a \in I$ tal que $a \neq 0$. Consideremos

$$S = \{x \in I \,|\, x > 0\}.$$

Como $a \in S$ ou $-a \in S$, temos que $S \neq \emptyset$. Logo, pelo Princípio da Boa Ordenação dos números inteiros, S possui um menor elemento, digamos a_0. Então, $a_0\mathbb{Z} \subseteq I$, pois I é ideal de $\mathbb{Z}$. Reciprocamente, seja $b \in I$. Segue do algoritmo da divisão (teorema 3.1.5) que existem $q, r \in \mathbb{Z}$ tais que

$$b = a_0 q + r,$$

com $0 \leq r \leq a_0$. Assim, $r = b - a_0 q \in I$, de onde segue que $r = 0$, pela minimalidade de a_0. Logo, $b = a_0 q$ e segue que $I = a_0\mathbb{Z}$. □

Mostraremos agora que existe o máximo divisor comum, ou simplesmente mdc no conjunto $\mathbb{Z}$.

Definiremos, a seguir, o máximo divisor comum entre números inteiros.

Definição 3.1.8. Dados dois números inteiros a e b com $a \neq 0$ ou $b \neq 0$, a cada um deles pode-se associar seu conjunto de divisores positivos $D(a)$ e $D(b)$ respectivamente, e a intersecção de tais conjuntos $D(a) \cap D(b)$ é finita e não vazia (já que 1 pertence à intersecção). Por ser finito, $D(a) \cap D(b)$ possui elemento máximo que é chamado de *máximo divisor comum* (mdc) dos números a e b. Para $a = b = 0$ convencionamos $\text{mdc}(0, 0) = 0$. Quando $\text{mdc}(a, b) = 1$ dizemos que a e b são primos entre si.

Podemos estender a definição de mdc em $\mathbb{Z}$ para k elementos, ou seja, dados k números inteiros $n_1, n_2, \ldots, n_k$, pode-se associar o conjunto dos divisores positivos

$$D(n_1), D(n_2), \ldots, D(n_k)$$

respectivamente e a intersecção $D(n_1) \bigcap D(n_2) \bigcap, \ldots, \bigcap D(n_k)$ é finita e não vazia. Logo, possui um elemento máximo d tal que $\text{mdc}(n_1, n_2, \ldots, n_k) = d$.

O teorema a seguir contextualiza o conceito de mdc dentro da teoria de anéis e lista algumas propriedades importantes do mesmo.

Teorema 3.1.9. *Sejam $n_1, n_2, \ldots, n_k$ inteiros não nulos e seja*

$$J = n_1\mathbb{Z} + n_2\mathbb{Z} + \cdots + n_k\mathbb{Z}$$

o ideal gerado por $n_1, n_2, \ldots, n_k$. Pelo Teorema 3.1.7, existe um número inteiro positivo $d \in \mathbb{Z}$ tal que $J = d\mathbb{Z}$. Então,

(i) $\exists\ r_1, r_2, \ldots, r_k \in \mathbb{Z}$ *tais que* $d = n_1r_1 + n_2r_2 + \cdots + n_kr_k$.

(ii) d *é um divisor comum de* $n_1, n_2, \ldots, n_k$.

(iii) Se d' *é um divisor qualquer de* $n_1, n_2, \ldots, n_k$, *então* d' *é também um divisor de* d.

(iv) $d = \text{mdc}(n_1, n_2, \ldots, n_k)$.

Demonstração. (i) Como $1 \in \mathbb{Z}$, então $d \in d\mathbb{Z}$. Uma vez que

$$J = d \cdot \mathbb{Z} = n_1\mathbb{Z} + n_2\mathbb{Z} + \cdots + n_k\mathbb{Z},$$

temos que existem $r_1, \ldots, r_k \in \mathbb{Z}$ tais que $d = n_1r_1 + \cdots + n_kr_k$.

(ii) Seja $i \in \{1 \ldots, k\}$. Claro que

$$n_i \in n_i\mathbb{Z} \subset n_1\mathbb{Z} + \cdots + n_i\mathbb{Z} + ... + n_k\mathbb{Z} = d\mathbb{Z},$$

e, portanto, $\exists r_i \in \mathbb{Z}$ tal que $n_i = dr_i$, isto é, d é um divisor de cada n_i, para cada $i = 1, \ldots, k$.

(iii) Seja d' um divisor comum qualquer de $n_1, n_2, \ldots, n_k$. Assim, para cada $i = 1, \ldots, k$, existe r_i tal que $n_i = d' \cdot r_i$, ou seja, $n_i\mathbb{Z} \subseteq d'\mathbb{Z}\ \forall i \in \{1, 2, \ldots, k\}$ (*cf.* observação 3.1.4 ítem b) e daí segue imediatamente que:

$$n_1\mathbb{Z} + n_2\mathbb{Z} + \cdots + n_k\mathbb{Z} = d\mathbb{Z} \subseteq d'\mathbb{Z}$$

e portanto: $d \in d'\mathbb{Z}$, isto é, $\exists r \in \mathbb{Z}$ tal que $d = d'r$.

(iv) Por (ii) d é divisor comum de $n_1, n_2, \ldots, n_k$ então $d \in D(n_1) \bigcap D(n_2) \bigcap \ldots \bigcap D(n_k)$. Por (iii), qualquer outro divisor comum de $n_1, n_2, \ldots, n_k$ também divide d, logo d é o maior divisor comum de $n_1, n_2, \ldots, n_k$. □

Observação 3.1.10. a) Se $a = 0$ e $b \neq 0$, então $d = |\, b \,|$.

b) Se d é máximo divisor comum entre a e b, então d também é máximo divisor comum entre $-a$ e b, entre a e $-b$ e entre $-a$ e $-b$.

Exemplo 3.1.11. Sejam os inteiros 30 e 66, então

$D(30) = \{1, 2, 3, 5, 6, 10, 15, 30\}$

$D(66) = \{1, 2, 3, 6, 11, 33, 66\}$

$D(30) \cap D(66) = \{1, 2, 3, 6\}$

Logo, de acordo com a Definição 3.1.8, $\text{mdc}(30, 66) = 6$.

Exemplo 3.1.12. Sendo n um inteiro qualquer, achar os possíveis valores do máximo divisor comum dos números n e $n + 10$.

Resolução: Seja $d := \text{mdc}(n, n + 10)$.

Como $d \,|\, n + 10$ e $d \,|\, n$, então, pela propriedade 4 da proposição 3.1.3

$$d \,|\, [(n + 10) - n] \Rightarrow d \in \{1, 2, 5, 10\}.$$

Corolário 3.1.13. *Sejam $a, b \in \mathbb{Z}$ não simultaneamente nulos. Então, existem inteiros x e y tais que* $\text{mdc}(a, b) = ax + yb$. *Portanto, se $c \in \mathbb{Z}$ é tal que $c \,|\, a$ e $c \,|\, b$ então $c \,|\, \text{mdc}(a, b)$.*

Este corolário é consequencia do Teorema 3.1.9 para $k = 2$.

Exemplo 3.1.14. Dados os inteiros 12 e 21, temos:

$D(12) = \{1, 2, 3, 4, 6, 12\}$

$D(28) = \{1, 2, 4, 7, 14, 28\}$

$D(12) \cap D(28) = \{1, 2, 4\}$

Pela Definição 3.1.8, temos que $\text{mdc}(12, 28) = 4$, então existem $x, y \in \mathbb{Z}$ tais que $4 = 12x + 28y$.

A saber, para $x = -2$ e $y = 1$ teremos $12(-2) + 28(1) = 4$.

Exemplo 3.1.15. Consideremos o ideal de $\mathbb{Z}$ gerado por 3 e 4, a saber

$$\langle 3, 4\rangle = \{3x + 4y; x, y \in \mathbb{Z}\} = 3\mathbb{Z} + 4\mathbb{Z}.$$

Com $x = 1$ e $y = 0$ vemos que $3 = 3 \cdot 1 + 4 \cdot 0 \in I(3, 4)$. Analogamente com $x = 0$ e $y = 1$,temos que $4 = 3 \cdot 0 + 4 \cdot 1$. Portanto, todo elemento de $\mathbb{Z}$ que pode ser escrito como uma soma de um mútiplo de 3 e um múltiplo de 4 pertence a este anel. Como sabemos escrever $1 = -3 + 4$, segue que $1 \in \langle 3, 4\rangle$, ou seja, $3\mathbb{Z} + 4\mathbb{Z} = 1\mathbb{Z} = \mathbb{Z}$.

Proposição 3.1.16. *Se* $\text{mdc}(a, b) = 1$ *e $a \,|\, bc$, então $a \,|\, c$.*

Demonstração. Como $\text{mdc}(a,b) = 1$, existem $x, y \in \mathbb{Z}$ tais que $ax + by = 1$, assim

$$a \cdot cx + (bc) \cdot u = c.$$

Do fato de a dividir cada termo do lado esquerdo, temos que $a \,|\, c$. □

Teorema 3.1.17. *Para todo inteiro positivo t,* $\text{mdc}(ta, tb) = t\,\text{mdc}(a,b)$.

Demonstração. Seja $d = \text{mdc}(a,b)$. Então, pelo teorema 3.1.9, temos que

$$d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}.$$

Multiplicando por t, temos

$$td\mathbb{Z} = t(a\mathbb{Z} + b\mathbb{Z}) \Longrightarrow td\mathbb{Z} = ta\mathbb{Z} + tb\mathbb{Z}$$

e portanto,

$$td = \text{mdc}(ta, tb).$$

□

Proposição 3.1.18. *Se a, b e c são números inteiros tais que $a \,|\, c$, $b \,|\, c$ e se a e b são primos entre si, então $ab \,|\, c$.*

Demonstração. Como a e b são primos entre si, pela definição de mdc e pelo teorema 3.1.9, existem r e s tais que $ra + sb = 1$, de onde vem

$$r(ac) + s(bc) = c.$$

De $a \,|\, c$ e $b \,|\, c$ resulta que $ab \,|\, ac$ e $ab \,|\, bc$, portanto, pela propriedade 4 da proposição 3.1.3:

$$ab \,|\, acr + acs \Rightarrow ab \,|\, c.$$

□

Exemplo 3.1.19. Sejam os números 4,7 e 56. Temos que $4 \,|\, 56$ pois $56 = 4 \cdot 14$ e $7 \,|\, 56$ pois $56 = 7 \cdot 8$.

Como $\text{mdc}(4,7) = 1$ podemos concluir que $4 \cdot 7 \,|\, 56$. De fato $4 \cdot 7 = 28 \,|\, 56$.

Lema 3.1.20. *Se $a = bq + r$, então* $\text{mdc}(a,b) = \text{mdc}(b,r)$.

Demonstração. Basta mostrar que $D(a) \cap D(b) = D(a) \cap D(r)$, já que se estes conjuntos forem iguais, em particular seus máximos também serão iguais. Se $d \in D(a) \cap D(b)$ temos $d \,|\, a$ e $d \,|\, b$, logo $d \,|\, a - bq \Leftrightarrow d \,|\, r$ e portanto $d \in D(b) \cap D(r)$. Da mesma forma, se $d \in D(b) \cap D(r)$ temos $d \,|\, b$ e $d \,|\, r$, logo $d \,|\, bq + r \Leftrightarrow d \,|\, a$ e assim $d \in D(a) \cap D(b)$. □

O procedimento que usaremos no exemplo a seguir serve para calcular os r_i's no Teorema 3.1.9. É o chamado Algoritmo de Euclides Estendido que também serve para calcular o mdc.

Exemplo 3.1.21. Vamos calcular o $\text{mdc}(726, -275)$. Como o $\text{mdc}(726, -275) = \text{mdc}(726, 275)$, podemos aplicar o Algoritmo da Divisão (*cf.* teorema 3.1.5) a $\text{mdc}(726, 275)$:

$$726 = 2 \cdot 275 + 176$$

$$275 = 1 \cdot 176 + 99$$

$$176 = 1 \cdot 99 + 77$$

$$99 = 1 \cdot 77 + 22$$

$$77 = 3 \cdot 22 + 11$$

$$22 = 2 \cdot 11$$

e, portanto, segundo o lema 3.1.20 $\text{mdc}(726, -275) = \text{mdc}(22, 11) = 11$.

É importante notar que o máximo divisor comum de 726 e -275 pode ser escrito na forma

$$11 = 77 - 3 \cdot 22$$

$$= 77 - 3 \cdot (99 - 1 \cdot 77) = 4 \cdot 77 - 3 \cdot 99$$

$$= 4(176 - 1 \cdot 99) - 3 \cdot 99 = 4 \cdot 176 - 7 \cdot 99$$

$$= 4 \cdot 176 - 7(275 - 1 \cdot 176) = 11 \cdot 176 - 7 \cdot 275$$

$$11 = 11(726 - 2 \cdot 275) - 7 \cdot 275 = 11 \cdot 726 + 29(-275).$$

Corolário 3.1.22. *Sejam a e b inteiros positivos, com* $\text{mdc}(a, b) = d$. *Sejam x e y inteiros tais que $a = dx$ e $b = dy$. Então,* $\text{mdc}(x, y) = 1$, *ou seja, x e y são primos entre si.*

Demonstração. Como $d = \text{mdc}(a, b) = \text{mdc}(dx, dy) = d\,\text{mdc}(x, y)$ e $d \neq 0$ (pelo corolário 3.1.17), então:

$$\text{mdc}(x, y) = 1$$

□

O mínimo múltiplo comum de dois números inteiros a e b é o menor inteiro positivo m que é múltiplo de a e b simultaneamente. Vamos a uma definição formal de m.

Definição 3.1.23. Se denotarmos por $M(n)$ o conjunto dos múltiplos positivos de n, dados dois números inteiros a e b com $a \neq 0$ e $b \neq 0$, então a intersecção $M(a) \cap M(b)$ é não vazia (já que $|ab|$ está na intersecção). Pelo princípio da boa ordenação, $M(a) \cap M(b)$ possui elemento mínimo. Tal número é chamado *mínimo múltiplo comum* de a e b e o denotaremos $\text{mmc}(a, b)$.

Proposição 3.1.24. *Sejam a e b inteiros não-nulos e seja m o mínimo múltiplo comum de a e b. Então,*

(i) $m > 0$*;*

(ii) $a \mid m$ *e* $b \mid m$*;*

(iii) Se $c \in \mathbb{Z}$ *for tal que* $a \mid c,\ b \mid c$ *e* $c > 0$*, então* $m \leq c$*.*

Demonstração. De fato, segundo a definição 3.1.23, m é inteiro positivo e pertence à intersecção $M(a) \cap M(b)$, logo m é múltiplo de a e de b e, consequentemente, $a \mid m$ e $b \mid m$.

Novamente pela definição 3.1.23, temos que m é o menor elemento da intersecção $M(a) \cap M(b)$. Assim, se $a \mid c,\ b \mid c$ e $c > 0$ temos que, c também pertece à intersecção $M(a) \cap M(b)$, logo $m \leq c$. □

Proposição 3.1.25. *Sejam a e b dois números naturais, então*

$$\text{mdc}(a, b) \cdot \text{mmc}(a, b) = a \cdot b.$$

Demonstração. Escreva $d = \text{mdc}(a, b)$ e $m = \text{mmc}(a, b)$. Como $d \mid a$ então $d \mid ab$, ou seja, ab é múltiplo de d, logo $ab = dm_1$ onde m_1 é um número inteiro diferente de zero.

Pondo-se $a = a_1 d$ e $b = b_1 d$, com a_1, b_1 primos entre si (*cf.* corolário 3.1.22), temos que $a_1 d b_1 d \mid m_1 d \Rightarrow a_1 b_1 d \mid m_1$, donde:

$$ab_1 d = dm_1 \Longrightarrow ab_1 = m_1$$

$$a_1 db = dm_1 \Longrightarrow a_1 b = m_1.$$

Logo, m_1 é um múltiplo comum de a e b, portanto, pelo ítem (iii) da definição 3.1.23, $m \leq m_1$.

Por outro lado temos $m = m'd$, já que $d \mid a$ e $a \mid m$ (*cf.* ítem d_2 da proposição 3.1.3). E como $a \mid m$ e $b \mid m$, teremos:

$$a_1 d \mid m'd \text{ e } b_1 d \mid m'd,$$

logo

$$a_1 \mid m' \text{ e } b1 \mid m'$$

e pelo teorema 3.1.18 temos que

$$a_1 b_1 \mid m' \Rightarrow a_1 b_1 d \mid m'd \Rightarrow a_1 b \mid m,$$

ou seja, $m_1 \mid m$ e portanto $m_1 \leq m$. Fica assim demonstrado que $m_1 = m$ e portanto $ab = dm$. □

Proposição 3.1.26. *Sejam $a\mathbb{Z}$ o ideal gerado por a e $b\mathbb{Z}$ o ideal gerado por b. Então,*

$$a\mathbb{Z} \cap b\mathbb{Z} = \text{mmc}(a,b)\mathbb{Z}.$$

Demonstração. Seja $x \in a\mathbb{Z} \cap b\mathbb{Z}$ então $x \in a\mathbb{Z}$ e $x \in b\mathbb{Z}$. Seja $d = \text{mdc}(a,b)$ e sejam $a_1, b_1 \in \mathbb{Z}$ tais que $a = a_1 d$ e $b = b_1 d$.

Como $x \in a\mathbb{Z}$, então existe $q \in \mathbb{Z}$ tal que $x = aq = a_1 dq$. Como $x \in b\mathbb{Z}$, então

$$b = b_1 d | a_1 dq \Rightarrow b_1 | a_1 q \Rightarrow b_1 | q,$$

onde a última implicação segue do corolário 3.1.22 e da proposição 3.1.16.

Dessa forma, temos que

$$b|dq \Rightarrow ab|daq = dx \Rightarrow x|\frac{ab}{d} = \text{mmc}(a,b),$$

onde a última igualdade segue da proposição 3.1.25.

Reciprocamente, seja $m = \text{mmc}(a,b)$ então $m = r \cdot a = s \cdot b$ para algum $r, s \in \mathbb{Z}$ e seja $y \in \text{mmc}(a,b)\mathbb{Z}$. Deste modo, existe $c \in \mathbb{Z}$ tal que

$$y = c \cdot r \cdot a = c \cdot s \cdot b \Rightarrow y \in a\mathbb{Z} \; e \; y \in b\mathbb{Z} \Rightarrow y \in a\mathbb{Z} \cap b\mathbb{Z}.$$

Logo, $a\mathbb{Z} \cap b\mathbb{Z} = \text{mmc}(a,b)\mathbb{Z}$. □

Exemplo 3.1.27. Seja $a = -6$ e $b = 15$, então $\text{mmc}(-6,15) = 30$. Com efeito, o conjunto dos múltiplos de -6 é $M(-6) = \{6, 12, 18, 24, 30, \ldots\}$ e o dos múltiplos de 15 é $M(15) = \{15, 30, 45, 60, \ldots\}$. Portanto,

$$M(-6) \cap M(15) = \{30, 60, \ldots\},$$

donde $\text{mmc}(-6,15) = 30$.

Exemplo 3.1.28. Sendo a e b inteiros positivos, demonstrar que o $\text{mdc}(a,b)$ sempre divide o $\text{mmc}(a,b)$.

Resolução:Sendo $a = \text{mdc}(a,b) \cdot x$ e $b = \text{mdc}(a,b) \cdot y$, onde $\text{mdc}(x,y) = 1$ (*cf.* corolário 3.1.22). Pela proposição 3.1.25, $ab = \text{mdc}(a,b) \cdot \text{mmc}(a,b) \Rightarrow [\text{mdc}(a,b)]^2 \cdot x \cdot y = \text{mdc}(a,b) \cdot \text{mmc}(a,b) \Rightarrow \text{mdc}(a,b).x.y = \text{mmc}(a,b) \Rightarrow \text{mdc}(a,b) | \text{mmc}(a,b)$.

3.2 Números Primos

Os números primos têm fascinado os matemáticos desde os tempos mais remotos. Abordaremos aqui alguns importantes resultados acerca destes números.

Definição 3.2.1. Seja $p \in \mathbb{Z}$ com $p \neq 1$. Dizemos que um número natural p é um número primo se os seus únicos divisores (positivos) são 1 e p.

Esta definição é equivalente a dizer que $p \in \mathbb{Z}$ é um número primo se $p \neq 1$ e toda vez que $p = ab$, com $a, b \in \mathbb{Z}$, então $a = 1$ ou $a = p$.

Quando um número não é primo, dizemos que ele é composto. Ou seja, um número é composto quando tem mais de dois divisores naturais distintos.

Exemplo 3.2.2. a) 23 é primo, pois $D(23) = \{1, 23\}$.

b) 41 é primo, pois $D(41) = \{1, 41\}$.

c) 97 é primo, pois $D(97) = \{1, 97\}$.

Exemplo 3.2.3. Dados que p, $p + 10$ e $p + 14$ são números primos, encontre p.

Vamos analisar os possíveis restos na divisão de p por 3. Se p deixa resto 1, então 3 divide $p + 14$ e não poderá ser primo. Se o resto é 2, então 3 divide $p + 10$ e também não poderá ser primo. Assim, o resto da divisão p por 3 é 0 e, consequentemente, $p = 3$. Logo a sequencia de números será 3, 13 e 17.

Proposição 3.2.4. *Se um número primo p não é um divisor de um número inteiro n, então existem $r, s \in \mathbb{Z}$ tais que $rp + sn = 1$.*

Demonstração. Seja $d := \text{mdc}(p, n) > 0$. Pela definição de mdc, temos que d é um divisor de p e portanto $d = 1$ ou $d = p$. Mas como $d \mid n$ e p não é divisor de n, temos que $d = 1$ e a proposição segue, pois $1 \in d \cdot \mathbb{Z} = p \cdot \mathbb{Z} + n\mathbb{Z}$. □

Exemplo 3.2.5. Sejam os inteiros 7 e 20, temos que 7 é um número primo pois $D(7) = \{1, 7\}$ e 7 não divide 20, pois $D(20) = \{1, 2, 4, 5, 10, 20\}$ e pelo algoritmo da divisão:

$$20 = 7 \cdot 2 + 6$$

$$7 = 6 \cdot 1 + 1$$

$$6 = 1 \cdot 6 + 0$$

logo, pelo lema 3.1.20, $\text{mdc}(20, 7) = 1$, assim podemos escrever $20 \cdot (-1) + 7 \cdot 3 = 1$.

Proposição 3.2.6. *Todo número primo que divide um produto divide pelo menos um dos fatores.*

Demonstração. Suponhamos que $p \mid ab$ e que p não é divisor de a e vamos provar que $p \mid b$. De fato, pela proposição 3.2.4 segue que existem $r, s \in \mathbb{Z}$ tais que

$$p \cdot r + a \cdot s = 1.$$

Multiplicando ambos os membros da igualdade por b, temos que

$$p(rb) + (ab)s = b.$$

Como por hipótese $p \mid ab$ e $p \mid p$ então $p \mid p(rb) + (ab)s$, logo $p \mid b$. □

Teorema 3.2.7 (**Teorema Fundamental da Aritmética**). *Seja $n \geq 2$, um número natural. Podemos escrever n de forma única como um produto*

$$n = p_1 p_2 \dots p_m$$

onde $m \geq 1$ é um número natural e $p_1 \leq p_2 \leq \cdots \leq p_m$ são primos.

Demonstração. **Existência:** Mostraremos a existência da fatoração de n em primos por indução.

Seja $S \subset \mathbb{N}$ formado de naturais maiores que 1 que são primos ou um produto de primos. Claramente $2 \in S$. Suponha que para algum n natural, S contém todos os naturais k, com $1 < k < n$. Devemos mostrar que $n \in S$. Se n é primo não há o que provar (escrevemos $m = 1, p_1 = n$). Se n é composto podemos escrever $n = ab, a, b \in \mathbb{N},\ 1 < a < n,\ 1 < b < n$. Por hipótese de indução, a e b se decompõem como produto de primos. Juntando as fatorações de a e b (e reordenando os fatores) obtemos uma fatoração de n.

Unicidade: Suponha por absurdo que n possui duas fatorações diferentes

$$n = p_1 \cdots p_m = q_1 \cdots q_{m'},$$

com $p_1 \leq \ldots \leq p_m,\ q_1 \leq \ldots \leq q_{m'}$ e que n é mínimo com tal propriedade. Como $p_1 \mid q_1 \cdots q_{m'}$, pela proposição 3.2.6 temos que $p_1 \mid q_i$ para algum valor de i. Logo, como q_i é primo, $p_1 = q_i$ e $p_1 \geq q_1$. Analogamente temos $q_1 \leq p_1$, donde $p_1 = q_1$. Mas

$$\frac{n}{p_1} = p_2 \cdots p_m = q_2 \cdots q_{m'}$$

admite uma única fatoração, pela minimalidade de n donde $m = m'$ e $p_i = q_i$ para todo i, o que contradiz o fato de n ter duas fatorações. □

Seja a um número inteiro; se $a \geq 2$, pelo teorema fundamental da atitmética, existem números positivos $p_1 \leq \ldots \leq p_m, m \geq 1$ tais que $a = p_1 p_2 \ldots p_m$ e nesta decomposição os fatores não são necessariamente distintos dois a dois. Indiquemos por s o número de elementos do conjunto $\{p_1 \leq \ldots \leq p_m\}$ e representemos este conjunto por $q_1 \leq \ldots \leq q_s$ onde cada q_i é um número primo positivo e $p_i \neq p_j$ se $i \neq j$, $(i.j = 1, 2, \ldots, s)$. Com estas notações temos

$$a = q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_s^{\alpha_s}$$

onde $\alpha_i \geq 1$ e $\alpha_1 + \alpha_2 + \ldots + \alpha_s = m$.

Proposição 3.2.8. *Sejam a e b números inteiros tais que $a = q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_s^{\alpha_s}$ e $b = q_1^{\beta_1} q_2^{\beta_2} \ldots q_s^{\beta_s}$. Temos que $b \,|\, a$ se, e somente se, $\alpha_i \geq \beta_i$.*

Demonstração. Se $b \,|\, a$, então

$$q_1^{\beta_1} q_2^{\beta_2} \ldots q_s^{\beta_s} \,|\, q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_s^{\alpha_s}.$$

Consequentemente,

$$q_1^{\beta_1} \,|\, q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_s^{\alpha_s}$$

e pela proposição 3.2.6 temos que $q_1^{\beta_1} \,|\, q_1^{\alpha_1}$ já que $q_2, \ldots, q_s$ são primos distintos de q_1. Deste modo, temos que $\alpha_1 \geq \beta_1$.

Analogamente, temos que $q_2^{\beta_2} \,|\, q_2^{\alpha_2}$, $\ldots, q_s^{\beta_s} \,|\, q_s^{\alpha_s}$. Logo $\alpha_i \geq \beta_i$.

Reciprocamente, se $\alpha_i \geq \beta_i$, então $\alpha_i - \beta_i \geq 0$ que nos leva a concluir que $q_i^{\alpha_i - \beta_i}$ é um número inteiro $\forall i \in \{1, 2, \ldots, s\}$. Assim $q_1^{\alpha_1 - \beta_1} q_2^{\alpha_2 - \beta_2} \ldots q_s^{\alpha_s - \beta s} = \frac{a}{b}$ é inteiro. Logo temos que $b \,|\, a$. □

Pondo-se $\delta_i = \min\{\alpha_i, \beta_i\}$, para $i = 1, 2, \ldots, s$, verifica-se que o número

$$d = q_1^{\delta_1} q_2^{\delta_2} \ldots q_s^{\delta_s}$$

é o máximo divisor comum de a e b. Analogamente, se $\mu = \max\{\alpha_i, \beta_i\}$, o número inteiro

$$m = q_1^{\mu_1} q_2^{\mu_2} \ldots q_s^{\mu_s}$$

é o mínimo múltiplo comum de a e b. Obtivemos assim as regras usuais para a determinação do $\text{mdc}(a, b)$ e do $\text{mmc}(a, b)$ a partir das decomposições destes inteiros em fatores primos.

Para provar estas regras precisaremos do seguinte corolário:

Corolário 3.2.9. *Seja*

$$n = p_1^{e_1} \cdots p_k^{e_k}$$

a forma fatorada do número natural n em primos distintos p_i. Temos que os divisores naturais de n são os números da forma

$$d = p_1^{f_1} \cdots p_k^{f_k}$$

com $0 \leq f_i \leq e_i$ para todo i.

Este corolário é consequência da Proposição 3.2.8.

Provemos, agora, as regras básicas:

Demonstração. Segundo o corolário 3.2.9, os divisores de a são da forma $d_1 = q_1^{n_1} q_2^{n_2} \cdots q_s^{n_s}$, com $n_i \leq \alpha_i$ e os divisores de b são da forma $d_2 = q_1^{m_1} q_2^{m_2} \cdots q_s^{m_s}$, com $m_i \leq \beta_i$, logo os divisores comuns de a e b são da forma $d = q_1^{t_1} q_2^{t_2} \cdots q_s^{t_s}$, com $t_i \leq \alpha_i, \beta_i$.

Pela definição, o $\text{mdc}(a, b)$ será o maior elemento deste conjunto, assim

$$\text{mdc}(a, b) = q_1^{\delta_1} q_2^{\delta_2} \cdots q_s^{\delta_s},$$

onde $\delta_i = \min\{\alpha_i, \beta_i\}$.

Da definição de mínimo múltiplo comum, nenhum fator primo p_i deste mínimo poderá ter um expoente que seja inferior nem a α_i nem a β_i. Se tomarmos o maior destes dois para expoente de p_i teremos, não apenas um múltiplo comum, mas o menor possível dentre todos eles, o que conclui a demonstração. □

Exemplo 3.2.10. a) Podemos escrever 384=$2 \cdot 2 \cdot 3 \cdot 3 \cdot 3 \cdot 3 = 2^2 \cdot 3^4$.

b) O número 120 pode ser escrito na forma $2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 = 2^3 \cdot 3 \cdot 5$.

c) Vamos encontrar $\text{mdc}(120, 324)$ e o $\text{mmc}(120, 384)$ através do método da decomposição. Vejamos:

$$\text{mdc}(120, 384) = 2^2 \cdot 3 = 12$$

$$\text{mmc}(120, 384) = 2^3 \cdot 3^4 \cdot 5 = 3240$$

Capítulo 4

Polinômios

Seja A um anel comutativo com unidade. Chamamos de um *polinômio sobre A em uma indeterminada x* a uma expressão formal

$$p(x) = a_0 + a_1x + \cdots + a_mx^m + \cdots$$

onde $a_i \in A$, $\forall i \in \mathbb{N}$ e $\exists\ n \in \mathbb{N}$ tal que $a_j = 0\ \forall\ j \geq n$.

Dizemos que dois polinômios

$$p(x) = a_0 + a_1x + \cdots + a_mx^m + \cdots \text{ e } q(x) = b_0 + b_1x + \cdots + b_mx^m + \cdots$$

são iguais se, e somente se, $a_i = b_i$ em $K, \forall i \in \mathbb{N}$.

Se

$$p(0) = 0 + 0x + \cdots + 0x^m + \cdots$$

indicaremos $p(x)$ por 0 e o chamaremos de *polinômio identicamente nulo sobre A*. Assim um polinômio $p(x) = a_0 + a_1x + \cdots + a_mx^m + \cdots$ sobre A é identicamente nulo se e somente se $a_i = 0 \in A\ \forall i \in \mathbb{N}$.

Se $a \in A$ indicaremos por a o polinômio

$$p(x) = a_0 + a_1x + \cdots + a_mx^m + \cdots$$

onde $a_0 = a$ e $a_i = 0\ \forall i \geq 1$. O polinômio $p(x) = a, a \in k$ é o *polinômio constante.*

Se $p(x) = a_0 + a_1x + \cdots + a_mx^m + \cdots$ é tal que $a_n \neq 0$ e $a_j = 0\ \forall j > n$ dizemos que n é o *grau do polinômio* $p(x)$, e indicaremos $p(x) = a_0 + a_1x + \cdots + a_nx^n$ e o grau de $p(x)$ por $\text{gr}(p(x)) = n$. No termo a_nx^n, o a_n é chamado *coeficiente líder* do polinômio.

Os polinômios de grau n com coeficientes líder $a_n = 1$ são chamados de *polinômios mônicos.*

Vamos denotar por $A[x]$ o conjunto de todos os polinômios sobre A, em uma indeterminada x.

Exemplo 4.0.11. São polinômios em $\mathbb{Z}[x]$: $f(x) = -x^2 + 3x - 1$, $g(x) = 9 - 4x + 2x^4 - 3x^6$, $h(x) = 2x - 4 + x^3$.

Exemplo 4.0.12. São polinômios em $\mathbb{R}[x]$: $r(x) = \frac{1}{2}x + \sqrt{3}x^2 - 5x^3$, $s(x) = 2 - \pi x^3 + \sqrt[3]{6}x^5$.

Exemplo 4.0.13. Voltando aos exemplos 4.0.11 e 4.0.12 verificamos que $\text{gr}(f(x)) = 2$, $\text{gr}(g(x)) = 6$, $\text{gr}(h(x)) = 3$, $\text{gr}(r(x)) = 3$ $\text{gr}(s(x)) = 5$ e que $h(x)$ é o único polinômio mônico dentre eles.

Convencionaremos as regras: $x^0 = 1$ e $x^1 = x$

Definiremos abaixo operações de soma, produto e divisão no conjunto $A[x]$.

4.1 Operações

Sejam $p(x) = a_0 + a_1x + \cdots + a_mx^m + \cdots$ e $q(x) = b_0 + b_1x + \cdots + b_rx^r + \cdots$ dois elementos de $A[x]$.

Adição: Definimos:

$$p(x) + q(x) = c_0 + c_1x + \ldots + c_kx^k + \ldots$$

onde $c_i = (a_i + b_i) \in A$

Temos que $\text{gr}(f(x) + g(x)) \leq \max\{\text{gr}(f(x)), \text{gr}(g(x))\}$, quaisquer que sejam os polinômios não nulos $f(x), g(x) \in A[x]$ tais que $f(x) + g(x) \neq 0$

Exemplo 4.1.1. Sejam $f(x) = 3x^3 + 8x^2 - 2x + 1$ e $g(x) = x^3 - 10x^2 + 4x - 9$. Então,

$$f(x) + g(x) = (3 + 1)x^3 + (8 + (-10))x^2 + (-2 + 4)x + (1 + (-9))$$

$$= 4x^3 - 2x^2 + 2x - 8$$

Produto:

Definimos:

$$p(x) \cdot q(x) = c_0 + c_1x + \ldots + c_kx^k + \ldots,$$

onde

$$c_0 = a_0b_0$$

$$c_1 = a_0b_1 + a_1b_0$$

$$c_2 = a_0b_2 + a_1b_1 + a_2b_0$$

$$\vdots$$

$$c_k = a_0b_k + a_1b_{k-1} + \cdots + a_{k-1}b_1 + a_kb_0 = \sum_{i+j=k} a_ib_j$$

Denotaremos por $K[x]$ o conjuntos dos polinômios com coeficientes em K, onde K é corpo.

Propriedade multiplicativa do grau: Temos que $\text{gr}(f(x) \cdot g(x)) = \text{gr}(f(x)) + \text{gr}(g(x))$ quaisquer que sejam os polinômios não nulos $f(x), g(x) \in K[x]$.

Vale salientar que a propriedade multiplicativa do grau só é válida para polinômios com coeficientes em um corpo ou domínio de integridade. Por exemplo, tomando os polinômios $(\bar{2}x + \bar{1})$ e $(\bar{2}x + \bar{3})$ em $\mathbb{Z}_4$, temos

$$(\bar{2}x + \bar{1}) \cdot (\bar{2}x + \bar{3}) = \bar{3}$$

cujo grau é zero.

Note também que, como um elemento invertível nunca é um divisor de zero, então a propriedade vale se $f(x)$ ou $g(x)$ possui coeficiente líder invertível (por exemplo, se um dos polinômios é mônico).

Em consequencia das propriedades da adição e multiplicação do anel A, a adição e multiplicação $A[x]$ possuem as seguintes propriedades, para quaisquer que sejam $f(x), g(x)$ e $h(x)$ em $A[x]$:

(i) Associativa: $(f(x) + g(x)) + h(x) = f(x) + (g(x) + h(x))$ e

$$(f(x) \cdot g(x)) \cdot h(x) = f(x) \cdot (g(x) \cdot h(x));$$

(ii) Comutativa: $f(x) + g(x) = g(x) + f(x)$ e

$$f(x) \cdot g(x) = g(x) \cdot f(x);$$

(iii) Distributiva: $f(x) \cdot (g(x) + h(x)) = f(x) \cdot g(x) + f(x) \cdot h(x)$;

(iv) Existência do elemento neutro aditivo: O polinômio nulo é tal que $f(x) = 0 + f(x)$, para todo $f(x) \in A[x]$.

(v) Existência do elemento simétrico: Dado $f(x) = a_0 + a_1x + \cdots + a_nx^n$, o simétrico de $f(x)$ é o polinômio

$$-f(x) = (-a_0) + (-a_1)x + \cdots + (-a_n)x^n$$

(vi) Existência do elemento neutro multiplicativo: O polinômio constante 1 é tal que $1 \cdot f(x) = f(x)$, para todo $f(x) \in A[x]$.

As demonstrações destas propriedades podem ser encontradas em [11] p.100-101.

Com as operações de adição e multiplicação e suas propriedades, dizemos que $A[x]$ é um anel comutativo com unidade.

Para $f(x), g(x) \in A[x]$, podemos definir a **diferença** $f(x) - g(x)$ entre $f(x)$ e $g(x)$ por $f(x) - g(x) = f(x) + (-g(x))$.

Seja A um domínio de integridade e suponhamos que um polinômio $p(x) \neq 0$ possua um inverso multiplicativo em $A[x]$. Assim, existe $q(x) \neq 0 \in A[x]$ tal que $p(x) \cdot q(x) = 1$. Pela propriedade multiplicativa do grau, temos que $p(x) = a \neq 0$ é um polinômio constante. Portanto, os únicos polinômios invertíveis em $A[x]$ são os polinômios constantes não nulos.

Exemplo 4.1.2.

Sejam $p(x) = x + 2$ e $g(x) = 3x^2 + x - 5$, então:

$$f(x) \cdot g(x) = (x + 2) \cdot (3x^2 + x - 5)$$

$$= (1 \cdot 3)x^3 + (1 \cdot 1 + 2 \cdot 3)x^2 + (-5 \cdot 1 + 2 \cdot 1)x + [2 \cdot (-5)]$$

$$= 3x^3 + 7x^2 - 3x - 10$$

Divisão

Introduziremos o conceito de divisibilidade em $A[x]$ e mostraremos que é possível fazer uma divisão com resto, de modo único.

Sejam $f(x)$ e $g(x)$ em $A[x]$. Quando existe $h(x) \in A[x]$ tal que $f(x) = g(x) \cdot h(x)$, dizemos que $f(x)$ é múltiplo de $g(x)$. Nesse caso, se $g(x) \neq 0$, dizemos que $g(x)$ divide $f(x)$.

Proposição 4.1.3. *Sejam A um anel, $f(x), g(x) \in A[x] \setminus \{0\}$. Se $g(x)$ tem coeficiente líder invertível e divide $f(x)$, então* $\mathrm{gr}(g(x)) \leq \mathrm{gr}(f(x))$.

Demonstração. Como $g(x)$ divide $f(x)$ e ambos são não nulos, então existe $h(x) \in A[x] \setminus \{0\}$ tal que $f(x) = g(x)h(x)$. Pela propriedade multiplicativa do grau, temos

$$\mathrm{gr}(f(x)) = \mathrm{gr}(g(x)h(x))$$

$$= \mathrm{gr}(g(x)) + \mathrm{gr}(h(x)) \geq \mathrm{gr}(g(x)).$$

□

Teorema 4.1.4. ***(Algoritmo da Divisão)****Sejam K um corpo, $f(x), g(x) \in K[x]$ e $g(x) \neq 0$. Então existem únicos $q(x), r(x) \in K[x]$ tais que:*

$$f(x) = q(x) \cdot g(x) + r(x)$$

onde $r(x) = 0$ ou $\mathrm{gr}(r(x)) < \mathrm{gr}(g(x))$.

Demonstração. Mostraremos, inicialmente, que há no máximo um par de polinômios $q(x)$ e $r(x)$ satisfazendo as condições do teorema. Para tanto sejam $q_1(x), q_2(x), r_1(x), r_2(x) \in K[x]$ tais que

$$f(x) = g(x)q_1(x) + r_1(x) = g(x)q_2(x) + r_2,$$

com $r_1(x) = r_2(x) = 0$ ou $0 \leq \text{gr}(r_i(x)) < \text{gr}\, g(x)$, para $i = 1, 2$. Segue daí que $g(x)(q_1(x) - q_2(x)) = r_2(x) - r_1(x)$, de sorte que, se $q_1(x) \neq q_2(x)$, então $r_1(x) \neq r_2(x)$. Mas pela definição de adição de polinômios e pela propriedade multiplicativa do grau, temos

$$\text{gr}(g(x)) \leq \text{gr}(g(x)) + \text{gr}(q_1(x) - q_2(x)) = \text{gr}(g(x)(q_1(x) - q_2(x))$$

$$= \text{gr}(r_1(x) - r_2(x)) \leq \max\{\text{gr}(r_1(x), r_2(x)) < \text{gr}(g(x),$$

o que é um absurdo. Portanto, $q_1(x) = q_2(x)$ e daí $r_1(x) = r_2(x)$.

Façamos agora a prova da existência de polinômios $q(x)$ e $r(x)$.

Seja $g(x) = b_0 + b_1x + \cdots + b_mx^m$, onde b_m tem inverso $b_m^{-1} \in K$.

Se $f(x) = 0$, então tome $q(x) = r(x) = 0$.

Suponhamos que $f(x) \neq 0$. Seja $n = \text{gr}(f(x))$ e escreva

$$f(x) = a_0 + a_1x + \cdots + a_nx^n,$$

com $a_n \neq 0$.

Se $n < m$, então tome $q(x) = 0$ e $r(x) = f(x)$. Podemos, então, supor $n \geq m$.

Agora, seja $f_1(x)$ o polinômio definido por

$$f(x) = a_nb_m^{-1}x^{n-m} \cdot g(x) + f_1(x). \tag{4.1.1}$$

Observemos que $\text{gr}(f_1(x)) < \text{gr}(f(x))$. A demonstração será feita por indução sobre $n = \text{gr}(f(x))$.

Se $n = 0,\ n \geq m \Rightarrow m = 0$ e portanto $f(x) = a_0 \neq 0,\ g(x) = b_0$ e teremos, $f(x) = a_0b_0^{-1}g(x)$ e basta tomar $q(x) = a_0b_0^{-1}$ e $r(x) = 0$.

Pela equação (4.1.1), $f_1(x) = f(x) - a_nb_m^{-1}x^{n-m}g(x)$ e $\text{gr}(f_1(x) < \text{gr}(f(x)) = n$. Temos pela hipótese de indução que: $\exists\ q_1(x), r_1(x)$ tais que:

$$f_1(x) = q_1(x) \cdot g(x) + r_1(x)$$

onde $r_1(x) = 0$ ou $\text{gr}(r_1) < \text{gr}(g(x))$. Daí, segue que:

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

e portanto tomando $q(x) = q_1(x) + a_nb_m^{-1}x^{n-m}$ e $r_1(x) = r(x)$ provamos a existência dos polinômios $q(x)$ e $r(x)$ tais que $f(x) = q(x) \cdot g(x) + r(x)$, e $r(x) = 0$ ou $\text{gr}(r(x)) < \text{gr}(g(x))$. $\square$

Exemplo 4.1.5. **a)** Sejam $f(x) = 3x + 7$ e $g(x) = x^2 + 4x + 5$ em $\mathbb{Q}[x]$.

Temos que $\text{gr}(f(x)) = 1 < 2 = \text{gr}(g(x))$, portanto não temos nada a fazer. O quociente é $q(x) = 0$ e o resto é $r(x) = f(x) = 3x + 7$. Assim

$$x^2 + 4x + 5 = 0 \cdot (x^2 + 4x + 5) + (3x + 7)$$

b) Sejam $f(x) = 2x^2 + 3x + 3$ e $g(x) = x^2 + 2x + 2$ em $\mathbb{Q}[x]$.

$\text{gr}(g(x)) = \text{gr}(f(x))$, então a divisão é possível. Como o monônio de maior grau de $f(x)$ é $2x^2$ e o monômio de maior grau de $g(x)$ é x^2, efetuando a divisão entre esses dois monômios temos o quociente $q(x) = 2$. Fazendo o cálculo de $r(x)$

$$r(x) = f(x) - q(x)g(x) = (2x^2 + 3x + 3) - 2(x^2 + 2x + 2) = -x - 1$$

Como $1 = \text{gr}(r(x)) < \text{gr}(g(x)) = 2$, não podemos continuar a divisão. Logo, $q(x) = 2$ e $r(x) = -x - 1$.

c) Sejam $f(x) = 3x^4 + 5x^3 + 2x^2 + x - 3$ e $g(x) = x^2 + 2x + 1$ em $\mathbb{Q}[x]$.

Após uma série de operações obtemos $q(x) = 3x^2 - x + 1 = q_1(x) + q_2(x) + q_3(x)$ e $r(x) = r_3(x) = -4$.

Nem sempre é possível efetuar a divisão entre polinômios em um anel que não seja um corpo.

d) Tomando $f(x) = 3x^2$ e $g(x) = 2x$ em $\mathbb{Z}[x]$, não é possível obter $f(x) : g(x)$ em $\mathbb{Z}[x]$, pois $\frac{3}{2} \notin \mathbb{Z}$.

Definição 4.1.6. Seja $f(x) = a_0 + a_1x + \ldots + a_nx^n \in A[x]$, onde A é um anel, e seja $\beta \in A$. Dizemos que o *valor numérico* de $f(x)$ para $x = \beta$ é definido por

$$f(\beta) = a_0 + a_1\beta + \ldots + a_n(\beta)^n \in A.$$

Definição 4.1.7. Se $f(\beta) = 0$, dizemos que β é uma *raiz* de $f(x)$.

Proposição 4.1.8 (Teste da raiz). *Seja K um corpo, $f(x) \in K[x] \setminus \{0\}$. Então, $\beta \in K$ é uma raiz de $f(x)$ se, e somente se, $x - \beta$ divide $f(x)$.*

Demonstração. Suponhamos que $f(\beta) = 0$. Pela divisão euclidiana de $f(x)$ por $x - \beta$, existem $q(x), r(x) \in K[x]$ tais que

$$f(x) = q(x)(x - \beta) + r(x),$$

onde $r(x) = 0$ ou $\text{gr}(r(x)) < \text{gr}(x-\beta) = 1$. Assim, $r(x) = r$ pertence a A e $f(x) = q(x)(x-\beta)+r$. Avaliando $f(x)$ em β temos

$$0 = f(\beta) = q(\beta)(\beta - \beta) + r = r,$$

mostrando que $x - \beta$ divide $f(x)$.

Reciprocamente, suponhamos que $x - \beta$ divida $f(x)$. Então, existe $q(x) \in K[x]$ tal que $f(x) = q(x)(x - \beta)$. Portanto,

$$f(\beta) = q(\beta)(\beta - \beta) = q(\beta) \cdot 0 = 0$$

□

Proposição 4.1.9. *Seja K um corpo e seja $f(x) = a_0 + a_1x + \cdots + a_nx^n$ um polinômio não nulo em $K[x]$ de grau n. Então, o número de raízes de $f(x)$ em K é no máximo igual a $\text{gr}(f(x)) = n$.*

Demonstração. Faremos a prova por indução sobre $n = \text{gr}(f(x))$.

Se $n = 0$, então $f(x) = a \neq 0$ não tem raízes em A e o resultado é válido.

Seja $n > 0$. Suponhamos o resultado verdadeiro para polinômios de grau n e seja $f(x)$ um polinômio com $\text{gr}(f(x)) = n + 1$.

Se $f(x)$ não tem raízes em K, então não temos o que demonstrar. Digamos que $f(x)$ tenha uma raiz β em K. Pelo teste da raiz, $x - \beta$ divide $f(x)$ em $K[x]$, logo existe $q(x) \in K[x]$ tal que

$$f(x) = q(x)(x - \beta), \text{ com } \text{gr}(q(x)) = n.$$

Por hipótese de indução, $q(x)$ tem no máximo n raízes em K. Observamos que

$$\alpha \in K \text{ é raiz de } f(x) \Leftrightarrow 0 = f(\alpha) = q(\alpha)(\alpha - \beta)$$

$$\Leftrightarrow^{(\star)} \ q(\alpha) = 0 \text{ ou } \alpha - \beta = 0$$

$$\alpha \text{ é raiz de } q(x) \text{ ou } \alpha = \beta,$$

onde em $(\star)$ usamos o fato de K ser um domínio de integridade. Logo, $f(x)$ tem no máximo $n + 1$ raízes em K. □

Teorema 4.1.10. *Seja K um corpo. Então, $K[x]$ é um domínio principal.*

Demonstração. Basta mostrar que todo ideal de $K[x]$ é principal.

Seja J um ideal de $K[x]$. Se $J = 0$ então J é gerado por 0. Suponhamos que $J \neq 0$ e escolhemos $0 \neq p(x) \in J$ tal que $\text{gr}(p(x))$ seja o menor possível. Se $p(x) = a$ constante diferente de 0 então $1 = a^{-1} \cdot a \in J$ e assim pela proposição 2.2.5 segue que $J = K[x]$ é gerado por $1 \in K[x]$. Suponhamos, então, $\text{gr}(p(x)) > 0$.

Como $p(x) \in J$, claramente temos $p(x) \cdot K[x] \subseteq J$. Agora vamos mostrar que $J \subseteq p(x)K[x]$ e isto demonstra o teorema.

De fato, seja $f(x) \in J$. Pelo algoritmo da divisão (*cf.* teorema 4.1.4) temos que $\exists\, q(x), r(x) \in K[x]$ tais que $f(x) = q(x) \cdot p(x) + r(x)$ onde ou $r(x) = 0$ ou $\mathrm{gr}(r(x)) < \mathrm{gr}(p(x))$.

Agora, como $f(x), p(x) \in J$ segue imediatamente que $r(x) = f(x) - q(x) \cdot p(x) \in J$ e pela minimalidade da nossa escolha do polinômio $p(x) \in J$ não podemos ter $r(x) \in J$ e $\mathrm{gr}(r(x)) < \mathrm{gr}(g(x))$ o que resulta que só há uma alternativa, $r(x) = 0$ e portanto temos $f(x) = q(x) \cdot p(x) \in K[x] \cdot p(x)$ como queríamos demonstrar. □

Assim como vale o Algoritmo da divisão para $K[x]$, mostraremos que existe o mdc.

Teorema 4.1.11 (Existência de M.D.C.). *Seja K um corpo e sejam $p_1(x), \ldots, p_m(x) \in K[x] \setminus 0$ e seja o ideal $J = K[x] \cdot p_1(x) + \cdots + K[x] \cdot p_m(x)$ de $K[x]$ gerado pelos polinômios não nulos $p_1(x), \ldots, p_m(x)$.*

Se $d(x) \in K[x]$ é tal que $J = K[x] \cdot d(x)$ então são válidas as seguintes propriedades:

a) $\exists\, r_1, \ldots, r_m \in K[x]$ tais que $d(x) = r_1(x) \cdot p_1(x) + \cdots + r_m(x) \cdot p_m(x)$.

b) $d(x)$ é um divisor comum de $p_1(x), p_2(x), \ldots, p_m(x)$.

c) se $d'(x)$ é um divisor comum qualquer de $p_1(x), p_2(x), \ldots, p_m(x)$ então $d'(x)$ é também um divisor de $d(x)$.

Um polinômio satisfazendo as condições (b) e (c) chama-se um máximo divisor comum de $p_1(x), p_2(x), \ldots, p_m(x)$ em $K[x]$, ou

$$\mathrm{mdc}(p_1(x), p_2(x), \ldots, p_m(x)).$$

É claro que se $d(x)$ é um mdc *de $(p_1(x), p_2(x), \ldots, p_m(x))$ em $K[x]$ e $0 \neq a \in K$ então $a \cdot d(x)$ é também um* mdc *em $K[x]$ desses polinômios.*

Demonstração. Primeiramente observemos que, de acordo com o Teorema 4.1.10, $K[x]$ é um domínio principal, assim, sempre existirá um $d(x)$ satisfazendo o enunciado. Além disso, como já vimos no Teorema 2.2.6, toda soma de ideais é ideal.

a) Como K é corpo, temos que o polinômio constante $f(x) = 1 \in K[x]$, logo

$$d(x) \in d(x) \cdot K[x] = K[x] \cdot p_1(x) + \cdots + K[x] \cdot p_m(x)$$

logo, existem $r_1(x), \ldots, r_m(x) \in K[x]$ tais que $d(x) = r_1(x) \cdot p_1(x) + \cdots + r_m(x) \cdot p_m(x)$.

b) Seja $i \in \{1, \ldots, m\}$ e $K[x] \cdot d(x) = K[x] \cdot p_1(x) + \cdots + K[x] \cdot p_m(x)$. Então,

$$p_i \in K[x] \cdot p_i(x) \subset K[x] \cdot p_1(x) + \cdots + K[x] \cdot p_m(x) = K[x] \cdot d(x)$$

e portanto $\exists\ r_i(x) \in K[x]$ tal que $p_i(x) = r_i(x) \cdot d(x)$, isto é, $d(x)$ é um divisor de cada $p_i(x),\ i = 1, 2, \ldots, m$.

c) Seja $d'(x)$ um divisor comum em $K[x]$ de $p_1(x), \ldots, p_m(x)$, isto é, $\exists\ r_i \in K[x]$ tal que $p_i(x) = r_i(x) \cdot d'(x),\ i = 1, 2. \ldots . m$.

Assim,

$$K[x] \cdot p_i(x) \subset K[x] \cdot d'(x)\ \forall\ i \in \{1, 2, \ldots, m\}$$

daí segue que,

$$K[x] \cdot d(x) = K[x] \cdot p_1(x) + \ldots + K[x] \cdot p_m(x) \subset K[x] \cdot d'(x),$$

ou seja, $\exists\ r(x) \in K[x]$ tal que $d(x) = r(x) \cdot d'(x)$ e isto demonstra o teorema.

□

Exemplo 4.1.12. Sejam os polinômios $p(x) = x^2 - 16$ e $g(x) = x^3 + 2x^2 - 7x + 4$ em $\mathbb{R}[x]$. Vamos mostrar que o $\text{mdc}(p(x), g(x)) = (x + 4)$.

Como $\mathbb{R}[x]$ é corpo, podemos aplicar o Algoritmo de Euclides. Efetuando a divisão de $g(x)$ por $p(x)$, temos:

$$x^3 + 2x^2 - 7x + 4 = (x^2 - 16)(x + 2) + (9x + 36)$$
$$x^2 - 16 = (9x + 36)\left(\frac{1}{9}x - \frac{4}{9}\right)$$

Logo, o $\text{mdc}(p(x), g(x)) = (9x + 36)$. Como este mdc não é único, podemos dividi-lo por 9 e obteremos uma forma mais simplificada. Assim, podemos afirmar que $\text{mdc}(p(x), g(x)) = (x+4)$.

Exemplo 4.1.13. $\mathbb{Z}[x]$ não é domínio principal.

Verifiquemos: Seja $A = \mathbb{Z}[x]$ e I o ideal de A gerado por 2 e x, isto é, $\langle 2, x\rangle = \{2p(x) + x \cdot q(x) \,|\, p(x), q(x) \in \mathbb{Z}[x]\}$.

Suponhamos por absurdo que A é um domínio de ideais principais. Assim, existe $d(x) \in A$ tal que $I = A \cdot d(x)$, então $\langle 2, x\rangle = A \cdot d(x)$. Isto quer dizer que $2 \in \langle d(x)\rangle$ e $x \in \langle d(x)\rangle$. Então existem $f(x), g(x) \in \mathbb{Z}[x]$ tais que $2 = f(x)d(x),\ x = g(x)d(x)$ levando-nos a concluir que $\text{gr}(d(x)) = 0$. Deste modo $d(x) = 1$ ou $d(x) = 2$, mas 2 não divide x em $\mathbb{Z}[x]$, logo $d(x) = 1$ e pela proposição 2.2.5, $\langle 2, x\rangle = \mathbb{Z}[x]$ o que é um absurdo, pois o termo independente de $\langle 2, x\rangle$ será sempre par.

4.2 Raízes de Polinômios

Proposição 4.2.1. *Sejam K um corpo, β um elemento de K e $f(x) = a_0x^n+a_1x_{n-1}+\ldots+a_nx \in K[x]$ um polinômio de grau n. Nessas condições:*

a) *[**Teorema do resto**] O resto na divisão euclidiana e $f(x)$ por $x - \beta$ é $f(\beta)$;*

b) *[**Algoritmo do Briot-Ruffini**] Se $q(x) = b_0x^{n-1} + b_1x^{n-2} + \ldots + b_{n-1}$ e $r(x) = b_n$ são respectivamente, quociente e resto na divisão considerada, então $a_0 = b_0$ e $b_i = \beta b_{i-1} + a_i,\ (i = 1, 2, \ldots, n)$.*

Demonstração. (a) Vale o algoritmo da divisão para $f(x)$ e $x - \beta$ já que $\text{gr}(x - \beta) < \text{gr}(f(x))$. Suponhamos que

$$f(x) = (x - \beta)q(x) + r(x),$$

onde $r(x) = 0$ ou $\text{gr}(r(x)) = 0$ (pois $\text{gr}(x - \beta) = 1$).

Achando o valor numérico de $f(x)$ para $x = \beta$:

$$f(\beta) = (\beta - \beta)q(\beta) + r(\beta) = r(\beta)$$

Sendo $r(x)$ constante, consideremos $r(\beta) = r$. Assim, $r = f(\beta),\ \forall\beta \in A$.

(b) Calculemos $(x - \beta)q(x) + r$;

$$\begin{aligned}
&(x - \beta)(b_0x^{n-1} + b_1x^{n-2} + \ldots + b_{n-1}) + b_n = \\
&= b_0x^n + (b_1 - \beta b_0)x^{n-1} + \ldots + (b_{n-1} - \beta b_{n-2})x + (b_n - \beta b_{n-1}) = \\
&= \sum_{i=0}^{n} b_ix^{n-i} - \beta\sum_{i=1}^{n} b_{i-1}x^{n-i}
\end{aligned}$$

Levando em conta que $(x - \beta)q(x) + r = f(x)$, obtemos as seguintes igualdades:

$$b_0 = a_0,$$

$$b_1 - \beta b_0 = a_1,$$

$$\vdots$$

$$b_{n-1} - \beta b_{n-2} = a_{n-1} \text{ e}$$

$$b_n - \beta b_{n-1} = a_n.$$

Daí,

$$b_0 = a_0,$$

$$b_1 = \beta b_0 + a_1,$$

$$\vdots$$

$$b_{n-1} = \beta b_{n-2} + a_{n-1} \text{ e}$$

$$b_n = \beta b_{n-1} + a_n,$$

que são as igualdades pretendidas. □

Teorema 4.2.2 (**Teorema fundamental da Álgebra**). *Todo polinômio $f(x) \in \mathbb{C}[x]$ de grau maior ou igual a 1, possui ao menos uma raiz complexa.*

A prova deste teorema pode ser encontrada em [14], p. 75-77.

Uma consequencia imediata do teorema fundamental da álgebra é o seguinte

Corolário 4.2.3. *Se $f(x) = a_n x^n + \cdots + a_1 x + a_0$ é um polinômio de coeficientes complexos e grau $n \geq 1$, então existem n números complexos $z_1, \ldots, z_n$ tais que*

$$f(x) = a_n(x - z_1) \cdots (x - z_n).$$

*A expressão acima é a **forma fatorada** do polinômio f(x).*

Demonstração. Façamos a prova por indução sobre o grau n de $f(x)$, sendo o caso $n = 1$ imediato. Suponha, pois, $n > 1$ e o corolário válido para todo polinômio de coeficientes complexos e grau $n - 1$.

Se $z_1 \in \mathbb{C}$ é uma raiz de $f(x)$, o teste da raiz garante a existência de um polinômio $g(x)$, também de coeficientes complexos, tal que $f(x) = (x - z_1)g(x)$. Note que $g(x)$ tem grau $n - 1$ e coeficiente líder a_n; portanto por hipótese de indução existem $z_2, \ldots, z_n \in \mathbb{C}$, tais que $g(x) = a_n(x - z_2) \cdots (x - z_n)$. Logo, $f(x) = (x - z_1)g(x) = a_n(x - z_1)(x - z_2) \cdots (x - z_n)$. □

Exemplo 4.2.4. (i) A forma fatorada do polinômio $f(x) = x^2 + 6x + 8$ em $\mathbb{Z}[x]$ é $f(x) = (x + 2)(x + 4)$;

(ii) O polinômio $p(x) = 3x^2 - 15x + 12 \in \mathbb{Z}[x]$ tem forma fatorada $p(x) = 3(x - 1)(x - 4)$;

(iii) Para o polinômio $q(x) = x^3 + 2x^2 - x - 2$ em $\mathbb{C}[x]$ a forma fatorada é

$$q(x) = (x + 2)(x - i)(x + i);$$

(iv) A forma fatorada de $r(x) = 2x^2 - 3$ em $\mathbb{R}[x]$ é $r(x) = 2\left(x - \sqrt{\frac{3}{2}}\right)\left(x + \sqrt{\frac{3}{2}}\right)$;

(v) O polinômio $g(x) = x^4 - x^2 - 2$ de $\mathbb{C}[x]$ tem forma fatorada

$$g(x) = (x+1)(x-1)\left(x+\sqrt{2}\right)\left(x-\sqrt{2}\right).$$

Apresentaremos agora, um estudo do problema de pesquisa de raízes racionais de polinômios de coeficientes inteiros. A proposição a seguir nos dá este resultado.

Proposição 4.2.5. *Sejam $n > 1$ inteiro, $f(x) = a_n x^n + \ldots + a_1 x + a_0$ um polinômio de coeficientes inteiros e p e q inteiros não nulos primos entre si. Se $f\left(\frac{p}{q}\right) = 0$, então:*

(a) $p \,|\, a_0$ e $q \,|\, a_n$.

(b) Se f for mônico, então as possíveis raízes racionais de f são inteiras.

Demonstração. (a) A partir de $f(\frac{p}{q}) = 0$, obtemos

$$a_n p^n + a_{n-1} p^{n-1} q + \ldots + a_1 p q^{n-1} + a_0 q^n = 0$$

e daí,

$$\begin{cases} a_0 q^n = p(-a_n p^{n-1} - \ldots - a_1 q^{n-1}) \\ a_n p^n = q(-a_{n-1} p^{n-1} - \ldots - a_0 q^{n-1}) \end{cases}$$

Portanto, $p \,|\, a_0 q^n$ e $q \,|\, a_n p^n$. Mas desde que p e q são primos entre si, a proposição 3.2.6 nos garante que $p \,|\, a_0$ e $q \,|\, a_n$, como queríamos demonstrar.

(b) Se $f(x)$ é mônico, $a_n = 1$. Pelo item (a), $q \,|\, 1$, logo $\frac{p}{q}$ é um número inteiro.

□

4.3 Relações de Girard

Figura 4.1: Albert Girard (1595-1632)

Albert Girard (1595-1632), matemático francês, apresentou um importante teorema que relaciona as raízes com os coeficientes de um polinômio.

Consideremos inicialmente o polinômio do 2º grau $p(x) = ax^2 + bx + c$ em $K[x]$, com $a \neq 0$, cujas raízes são x_1 e x_2. Pelo Colorário 4.2.3, temos:

$$ax^2 + bx + c = a(x - x_1)(x - x_2)$$

$$x^2 + \frac{b}{a}x + \frac{c}{a} = (x - x_1)(x - x_2)$$

$$x^2 + \frac{b}{a}x + \frac{c}{a} = x^2 - (x_1 + x_2)x + x_1x_2$$

Igualando os coeficientes, obtemos:

$$x_1 + x_2 = -\frac{b}{a}$$

$$x_1x_2 = \frac{c}{a}$$

Tomemos, agora, o polinômio de grau 3 $p(x) = ax^3 + bx^2 + cx + d$ com $a \neq 0$ em $K[x]$, cujas raízes são x_1, x_2 e x_3. Novamente pelo Colorário 4.2.3, temos:

$$ax^3 + bx^2 + cx + d = a(x - x_1)(x - x_2)(x - x_3)$$

$$x^3 + \frac{b}{a}x_2 + \frac{c}{a}x + \frac{d}{a} = (x - x_1)(x - x_2)(x - x_3)$$

$$x^3 + \frac{b}{a}x_2 + \frac{c}{a}x + \frac{d}{a} = x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_1x_3 + x_2x_3)x - x_1x_2x_3$$

Igualando os coeficientes, temos:

$$x_1 + x_2 + x_3 = -\frac{b}{a}$$

$$x_1x_2 + x_1x_3 + x_2x_3 = \frac{c}{a}$$

$$x_1x_2x_3 = -\frac{d}{a}$$

Consideremos o polinômio $p(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_0$ sendo $a_n \neq 0$ e $n \geq 1$. Segundo o Colorário 4.2.3, podemos escrever

$$p(x) = a_n(x - x_1)(x - x_2)\cdots(x - x_n)$$

. Aplicando a propriedade distributiva, reduzindo os termos semelhantes e ordenando o polinômio, temos:

$$\begin{aligned} p(x) =& a_nx^n - x^{n-1}(x_1 + x_2 + \ldots + x_n) + \\ &+ x^{n-2}(x_1x_2 + x_1x_3 + \ldots + x_1x_n + x_2x_3 + \ldots + x_{n-1}x_n) - \\ &- x^{n-3}(x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 + \ldots + x_{n-2}x_{n-1}x_n) + \\ &\ldots + (-1)^n(x_1x_2\ldots x_{n-1}x_n) \end{aligned}$$

Dividindo a expressão por a_n e igualando os coeficientes deste último polinômio com o polinômio considerado inicialmente, chegaremos às seguintes relações, conhecidas como relações de Girard, ou ainda, *relações entre coeficientes e raízes.*

$$x_1 + x_2 + \ldots + x_{n-1} + x_n = -\frac{a_{n-1}}{a_n}$$

$$x_1x_2 + x_1x_3 + \ldots + x_1x_n + x_2x_3 + \ldots + x_{n-1}x_n = \frac{a_{n-2}}{a_n}$$

$$x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 + \ldots + x_{n-2}x_{n-1}x_n = -\frac{a_{n-3}}{a_n}$$

$$\vdots$$

$$x_1x_2 \ldots x_{n-1}x_n = (-1)^n \frac{a_0}{a_n}.$$

As relações aqui explicitadas serão utilizadas na resolução de atividades no capítulo a seguir.

Capítulo 5

Atividades

Neste capítulo mostraremos algumas propostas didáticas que vão muito além da aplicação de fórmulas. Aqui pretende-se incentivar o aluno a utilizar conhecimentos aritméticos já estudados na resolução de problemas e desafios.

As atividades aqui propostas podem ser aplicadas a alunos a partir do 8º ano do Ensino Fundamental e podem ser trabalhadas de forma individual ou em grupos. Comentamos cada questão e explicitamos os conteúdos que podem ser explorados em cada uma delas para que o leitor identifique qual atividade pode ser aplicada em cada série.

Iniciemos com alguns desafios que podem tranquilamente ser aplicados aos alunos do 8º ano, com uma pequena observação: as relações entre coeficientes e raízes (relações de Girard) são estudadas apenas no 3º ano do Ensino Médio, mas ao estudar polinômios, o professor pode acrescentar a primeira relação $\left(x_1 + x_2 + \cdots + x_n = -\frac{a_{n-1}}{a_n}\right)$ de forma natural quando falar de raízes de polinômios, sem precisar formalizar todas as outras relações. A partir daí trabalha-se fatoração de polinômios que não se enquadram nos casos estudados nesta série (diferença de quadrados, fator comum em evidência, trinômio quadrado perfeito e agrupamento).

Vejamos alguns exemplos onde abordaremos apenas a relação da soma das raízes, divisão de polinômios, potência e valor numérico. A esta altura o professor já deve ter comentado o teorema fundamental da álgebra e deve ter o cuidado de utilizar apenas polinômios com raízes reais. No nosso caso trabalharemos apenas raízes inteiras.

1. **Escrever a forma fatorada do polinômio $P(x) = x^3 - 4x^2 - 4x + 16$ sabendo que duas raízes são simétricas.**

   Neste polinômio, embora dê para aplicar a fatoração por agrupamento, utilizaremos a relação da soma das raízes para encontrar a solução.

   $$x_1 + x_2 + x_3 = -(-4)$$

Como x_1 e x_2 são simétricas, temos que $x_1 + x_2 = 0$, daí temos que $x_3 = 4$.

Se 4 é raiz, podemos dividir $P(x)$ por $x - 4$, assim:

$$x^3 - 4x^2 - 4x + 16 = (x^2 - 4)(x - 4)$$

Como $x^2 - 4$ é uma diferença de quadrados, sua forma fatorada é $(x - 2)(x + 2)$, logo, a forma fatorada é

$$P(x) = (x - 4)(x - 2)(x + 2).$$

2. **Certo polinômio de coeficiente líder -2 e grau 3, tem raízes -1, 3 e 4. Outro polinômio de coeficiente líder 1 e grau 3, tem raízes 0 e 3, sendo o 3 uma raiz dupla. Encontre os dois polinômios e detemine o** mmc **entre eles.**

   Sejam os polinômios $p(x)$ e $g(x)$, então:

$$p(x) = -2(x + 1)(x - 3)(x - 4) = -2x^3 + 12x^2 - 10x - 24$$

$$g(x) = x(x - 3)^2 = x^3 - 6x^2 + 9x$$

   Para encontrar o $\text{mmc}(p(x), g(x))$, vamos analisar sua forma fatorada e escolher o termos:

$$\begin{aligned}\text{mmc}(p(x), g(x)) &= -2x(x + 1)(x - 3)^2(x - 4) \\ &= -2x^5 + 18x^4 - 46x^3 + 6x^2 + 72x.\end{aligned}$$

3. **Marquinhos chegou na sala de aula e desafiou os colegas a dizer qual o resto da divisão do polinômio $g(x) = x^5 + x^4 + x^3 + x^2 + x - 10$ por $(x - 2)$. Aquele que acertasse mais rápido iria ganhar um ingresso para assistir o filme que acabara de estrear no cinema. Todos pegaram o papel e a caneta e iniciaram imediatamente a efetuar a divisão, enquanto Joãozinho, em poucos segundos de cálculo mental, arriscou: -O resto é 52.**

   Espantado com a rapidez do cálculo Marquinhos afirmou que o resto estaria correto e deu-lhe o ingresso, mas ficou curioso pra saber como ele acertara o resultado tão rápido, Joãozinho então explicou:

   - Simples: calculei todas as potências de 2 até a quinta, somei e subtraí 10.

   O raciocínio de Joãozinho está correto? Justifique.

   O raciocínio está correto. Joãozinho utilizou-se do Teorema do Resto, onde o resto da divisão de um polinômio qualquer por $(x - \beta)$ é igual a $f(\beta)$. Sendo assim, como os coeficientes dos termos do polinômio são todos iguais a 1 (exceto o termo independente),

bastou calcular as potências de 2 até a quinta que é o grau do polinômio, somá-las e subtrair o termo independente que é 10.

4. **Escreva a forma fatorada do polinômio $P(x) = x^3 - 3x^2 - 6x + 8$ sabendo que a soma de duas de suas raízes é igual a 5.**

   Suponhamos $x_1 + x_2 = 5$ e substituindo na relação $x_1 + x_2 + x_3 = 3$, temos:

   $$5 + x_3 = 3 \Longrightarrow x_3 = -2$$

   Como -2 é raiz, podemos dividir $P(x)$ por $(x + 2)$, daí segue que

   $$x^3 - 3x^2 - 6x + 8 = (x + 2)(x^2 - 5x + 4)$$

   Alguns livros trazem a fatoração do trinômio de 2º grau, além do trinômio quadrado perfeito, onde deve-se procurar as raízes através da soma e do produto das mesmas. Deste modo, para o polinômio $q(x) = x^2 - 5x + 4$ devemos ter duas raízes cuja soma seja 5 e o produto 4. Assim, as raízes do polinômio são $\{-2, 1, 4\}$ e sua forma fatorada é $P(x) = (x + 2)(x - 1)(x - 4)$.

5. **A professora do 8º ano colocou uma caixa de bombons num baú e trancou com um cadeado cujo segredo é formado por 3 algarismos. Ela disse que o aluno que acertasse primeiro o segredo ficaria com os bombons e lançou o seguinte desafio: Os algarismos estão em ordem crescente e são as raízes do polinômio $P(x) = x^3 - 11x^2 + 31x - 21$ e a soma de dois deles é 10.**

   Podemos escrever $x_1 + x_2 = 10$ e $x_1 + x_2 + x_3 = -(-11)$, então

   $$10 + x_3 = 11 \Longrightarrow x_3 = 1$$

   Efetuando a divisão de $P(x)$ por $x - 1$, encontramos:

   $$x^3 - 11x^2 + 31x - 21 = (x - 1)(x^2 - 10x + 21)$$

   Analisando a fatoração do polinômio $q(x) = x^2 - 10x + 21$, temos a soma igual a 10 e o produto igual a 21, logo as raízes procuradas são 3 e 7. Assim, o segredo do cadeado é 137.

6. **Questionada por um aluno a respeito do número de sua casa, a professora de matemática lançou o enigma: O número da minha casa é formado por quatro algarismos que são as raízes do polinômio**

   $$P(x) = x^4 - 13x^3 + 57x^2 - 99x + 54.$$

Os dois primeiros algarismos são iguais os dois últimos formam um quadrado perfeito e sua soma é 7.

Temos que $x_1 = x_2$ e $x_3 + x_4 = 7$, então:

$$x_1 + x_2 + x_3 + x_4 = 13 \Longrightarrow 2x_1 + 7 = 13 \Longrightarrow x_1 = 3$$

Logo, 3 é a raiz dupla, ou seja $(x-3)^2$ divide $P(x)$. Desenvolvendo o produto notável $(x-3)^2 = x^2 - 6x + 9$ e efetuando a divisão, temos:

$$x^4 - 13x^3 + 57x^2 - 99x + 54 = (x^2 - 6x + 9)(x^2 - 7x + 6).$$

Os quadrados perfeitos formados por dois algarismos cuja soma dos algarismos é 7 são 16 e 25. Substituindo 1 no polinômio:

$$P(1) = 1 - 13 + 57 - 99 + 54 = 0$$

Substituindo 2 no polinômio:

$$P(2) = 16 - 104 + 228 - 198 + 54 = -4$$

Logo, 1 é raiz do polinômio e o quadrado perfeito procurado é 16. Daí temos que o número da casa da professora é 3316.

Poderíamos também analisar o quociente da divisão $q(x) = x^2 - 7x + 6$. De acordo com a regra de fatoração do trinômio do 2º grau, devemos ter duas raízes cuja soma seja 7 e o produto 6 e chegamos aos números 1 e 6.

7. **Determine o valor de $n \in \mathbb{Z}^*$ de modo que o polinômio**

$$p(x) = x^6 + nx^4 + 2x^3 + 2nx^2 + nx + 1$$

seja quadrado de um polinômio mônico $f(x) \in \mathbb{Z}[x]$, sabendo que os coeficientes de $p(x)$ pertencem a $\mathbb{Z}_+$.

Como $\text{gr}(p(x)) = 6$, ele será o quadrado de um polinômio mônico de grau 3. Seja $f(x) = x^3 + ax^2 + bx + c$, então

$$(x^3 + ax^2 + bx + c)^2 = x^6 + a^2x^4 + b^2x^2 + c^2 + 2ax^5 + 2bx^4 + 2cx^3 + 2abx^3 + \\ + 2acx^2 + 2bcx$$

agrupando os termos semelhantes, temos:

$$x^6 + 2ax^5 + (a^2 + 2b)x^4 + (2c + 2ab)x^3 + (b^2 + 2ac)x^2 + 2bcx + c^2$$

Comparando $p(x)$ com o quadrado de $(f(x))$

$$2a = 0 \Rightarrow a = 0$$

$$c^2 = 1 \Rightarrow c = \pm 1$$

mas $-1 \notin \mathbb{Z}_+$, logo $c = 1$

$$\begin{cases} a^2 + 2b = n \Rightarrow 2b = n \\ b^2 + 2ac = 2n \Rightarrow b^2 = 2n \Rightarrow b^2 = 2 \cdot 2b \Rightarrow b^2 - 4b = 0 \Rightarrow b \in \{0, 4\} \end{cases}$$

Para $b = 0$ temos $n = 0$ que não serve pois $n \in \mathbb{Z}^*$.

Para $b = 4$ temos $n = 8$, assim,

$$p(x) = x^6 + 8x^4 + 2x^3 + 16x^2 + 8x + 1 = (x^3 + 4x + 1)^2$$

8. **Obtenha $a \in \mathbb{Z}$ de modo que $p(x) = x^4 + ax^3 + 7x^2 - ax + 1$ seja o quadrado de um polinômio mônico de coeficientes inteiros.**

   Como $\text{gr}(p(x)) = 4$, $p(x)$ será o quadrado de um polinômio mônico de grau 2. Seja este polinômio $f(x) = x^2 + bx + c$.

   $$x^4 + ax^3 + 7x^2 - ax + 1 = (x^2 + bx + c)^2$$

   $$(x^2 + bx + c)^2 = x^4 + b^2x^2 + c^2 + 2bx^3 + 2cx^2 + 2bcx$$

   $$= x^4 + 2bx^3 + (2c + b^2)x^2 + 2bcx + c^2$$

   Comparando a última expressão com $p(x)$, temos:

   $$c^2 = 1 \Rightarrow c = \pm 1$$

   Caso $c = 1$, temos $2c + b^2 = 7 \Rightarrow b^2 = 5 \Rightarrow b = \pm\sqrt{5}$ que não serve pois $b \in \mathbb{Z}$.

   Para $c = -1$ temos $-2 + b^2 = 7 \Rightarrow b^2 = 9 \Rightarrow b = \pm 3$, logo

   $$b = 3 \Rightarrow 2b = a \Rightarrow a = 6$$

   $$b = -3 \Rightarrow 2b = a \Rightarrow a = -6$$

   Assim, temos que os valores de a são 6 e -6.

9. **O polinômio $p(x) = x^4 - 8x^3 - 27x^2 + 182x + 392$ tem 4 raízes inteiras. Duas delas são positivas e iguais e é um número primo que divide 84. Encontre as quatro raizes de $p(x)$.**

Decompondo 84 em fatores primos temos $84 = 2^2 \cdot 3 \cdot 7$. Substituindo os 2, 3 e 7 no polinômio observamos que:

$$p(2) = 2^4 - 8(2)^3 - 27(2(^2+182(2) + 392 = 600$$

$$p(3) = 3^4 - 8(3)^3 - 27(3)^2 + 182(3) + 392 = 560$$

$$p(7) = 7^4 - 8(7)^3 - 27(7)^2 + 182(7) + 392 = 0$$

Logo, 7 é a raiz dupla e $(x-7)^2$ divide $p(x)$. Desenvolvendo o produto notável e efetuando a divisão, encontramos:

$$p(x) = (x^2 - 14x + 49)(x^2 + 6x + 8).$$

Analisando a fatoração do polinômio $q(x) = x^2 + 6x + 8$ temos que as duas raízes são números cuja soma seja -6 e o produto 8, logo esses números são -2 e -4. E a raízes do polinômio são $\{-4, -2, 3, 3\}$.

Observação 5.0.1. As atividades acima foram comentadas e direcionadas para turmas do 8º ano, podendo ser aplicadas à turmas mais avançadas. Neste caso os alunos já terão conhecimento da fórmula de Bhaskara que poderá ser aplicada nas três últimas questões.

Abaixo temos atividades direcionadas ao Ensino Médio onde as relações de Girard são bastante exploradas. Além delas trabalhamos também divisores, sistema de equações, progressões aritmética e geométrica.

10. **Calcular as raízes do polinômio** $p(x) = x^3 - 16x^2 + 61x - 66$ **sabendo que todas são naturais.**

    De acordo com as relações de Girard, temos:

$$x_1x_2x_3 = -\frac{-66}{1} = 66$$

$$x_1 + x_2 + x_3 = -\frac{-16}{1} = 16$$

    Podemos afirmar que as raízes são divisores de 66, assim

$$x_1, x_2, x_3 \in \{1, 2, 3, 6, 11, 22, 33, 66\}.$$

    Mas os valores, 22, 33 e 66 não servem pois são maiores que 16. Além disso o 6 também não serve pois a soma dele com outros dois valores quaisquer não dá 16. Sendo assim, como $66 = 2 \cdot 3 \cdot 11$ e 2+3+11=16, temos que as raízes são 2, 3 e 11.

11. **Encontre as raízes do polinômio $p(x) = x^3 - 11x^2 + 39x - 45$ sabendo que todas são inteiras positivas e uma delas é dupla.**

Pelas relações de Girard temos que:

$$x_1 + x_2 + x_3 = -\frac{-11}{1} = 11$$

$$x_1x_2 + x_1x_3 + x_2x_3 = \frac{39}{1} = 39$$

$$x_1x_2x_3 = -\frac{-45}{1} = 45$$

Pela terceira relação temos que $x_1, x_2, x_3 \in \{1, 3, 5, 9, 15, 45\}$. Mas 15 e 45 estão descartados, visto que a soma das três raízes deve ser igual a 11. Como uma raiz é dupla, façamos $x_1 = x_2$ e podemos reescrever a primeira relação da seguinte forma:

$$2x_1 + x_3 = 11 \Rightarrow x_3 = 11 - 2x_1 \tag{5.0.1}$$

Reescrevendo a segunda relação,

$$x_1^2 + 2x_1x_3 = 39 \tag{5.0.2}$$

Substituindo a equação (5.0.1) na equação (5.0.2), temos:

$$x_1^2 + 2x_1(11 - 2x_1) - 39 = 0 \Rightarrow x_1^2 + 22x_1 - 4x_1^2 - 39 = 0 \Rightarrow 3x_1^2 - 22x_1 + 39 = 0$$

Resolvendo a equação encontramos as raízes $\frac{13}{3}$ e 3. Mas x_1 não pode ser igual a $\frac{13}{3}$, pois este valor não é divisor de 45. Então $x_1 = 3$.

Como $x_1 = x_2$, a raiz dupla é 3, e substituindo em $x_3 = 11 - 2x_1$ encontramos $x_3 = 5$. Logo, as raízes procuradas são $\{3, 3, 5\}$.

Outra resolução: Outra opção de resolução envolve analisar a decomposição do 45.

Como uma raiz é dupla teremos $x_1^2x_2 = 45$, mas $45 = 3^2 \cdot 5$, sendo assim, as raízes são 5 e 3 ou -3. Para verificar se 3 ou -3 é a raiz dupla basta efetuar a divisão de $p(x)$ por $x - 5$, donde:

$$p(x) = (x - 5)(x^2 - 6x + 9),$$

que nos leva a concluir que a raiz dupla é 3.

12. **Qual deve ser o valor de k no polinômio $p(x) = x^3 - 6x^2 + 4x + k$ para que suas raizes estejam em P.A.?**

Como o polinômio é de grau 3 e as raízes devem estar em P.A., podemos escrever $x_1 = a-r$, $x_2 = a$ e $x_3 = a+r$, e usando as relações entre os coeficientes e raízes, temos que:

$$x_1 + x_2 + x_3 = a - r + a + a + r = 6 \Longrightarrow a = 2$$

Como 2 é raiz o teste da raiz nos garante que $(x-2)$ divide $p(x)$ e usando o algoritmo da divisão temos que

$$x^3 - 6x^2 + 4x + k = (x-2)(x^2 - 4x - 4) + (k-8)$$

Como a divisão deve ser exata, devemos ter $k - 8 = 0$, donde $k = 8$.

13. **Encontrar as raízes do polinômio $p(x) = x^3 - 9x^2 + 23x - 15$ sabendo que suas raízes estão em P.A.**

Como as raízes estão em P.A., podemos escrever $x_1 = a - r$, $x_2 = a$ e $x_3 = a + r$. Então, pelas relações de Girard, temos:

$$x_1 + x_2 + x_3 = 9,$$

substituindo x_1, x_2 e x_3,

$$a - r + a + a + r = 9 \Rightarrow 3a = 9 \Rightarrow a = 3.$$

Logo, $x_2 = 3$ e pelo teste da raiz, $(x-3)$ divide $p(x)$. Assim, pelo algoritmo da divisão,

$$x^3 - 9x^2 + 23x - 15 = (x-3)(x^2 - 6x + 5)$$

O polinômio $q(x) = x^2 - 6x + 5$ tem raízes 5 e 1 (pelas relações de Girard, a soma é 6 e o produto é 5). Assim, as raízes de $p(x)$ são $\{1, 3, 5\}$.

14. **Sabendo que o polinômio $p(x) = x^3 - 5x^2 + 7x - 3$ tem 3 raízes inteiras e uma raiz dupla, encontre suas raizes.**

Como a soma das três raízes deve ser 5 e o produto deve ser 3, afirmamos que a raiz dupla deve ser 1 ou -1 e a outra raiz é 3. Fazendo a substituição de 1 e -1 no polinômio, temos:

$$p(1) = 1^3 - 5(1)^2 + 7(1) - 3 = 0$$

$$p(-1) = (-1)^3 - 5(-1)^2 + 7(-1) - 3 = -16$$

Logo, a raiz dupla é 1.

Outra resolução: Como uma raiz é dupla, podemos considerar $x_1 = x_2$ e escrever as relações:

$$x_1 + x_2 + x_3 = 5 \Longrightarrow 2x_1 + x_3 = 5 \Longrightarrow x_3 = 5 - 2x_1 \tag{5.0.3}$$

$$x_1x_2 + x_1x_3 + x_2x_3 = 7 \Longrightarrow x_1^2 + 2x_1x_3 = 7 \tag{5.0.4}$$

$$x_1x_2x_3 = 3 \Longrightarrow x_1^2x_3 = 3 \tag{5.0.5}$$

Substituindo (5.0.3) em (5.0.4), temos:

$$x_1^2 + 2x_1(5 - 2x_1) = 7 \Longrightarrow x_1^2 + 10x_1 - 4x_1^2 - 7 = 0 \Longrightarrow -3x_1^2 + 10x_1 - 7 = 0$$

Resolvendo esta última equação, encontramos $x_1 = \frac{7}{3}$ e $x_1 = 1$. Vamos verificar qual dos valores é raiz da equação inicial. Para $x_1 = \frac{7}{3}$:

$$p(\frac{7}{3}) = \frac{343}{7} - \frac{5 \cdot 49}{9} + \frac{49}{3} - 3 = \frac{343 - 735 + 441 - 81}{27} = -\frac{32}{27}$$

Portanto $\frac{7}{3}$ não é raiz do polinômio.

Para $x_1 = 1$:

$$p(1) = 1 - 5 \cdot 1 + 7 \cdot 1 - 3 = 1 - 5 + 7 - 3 = 0$$

Logo, 1 é a raiz dupla. Substituindo 1 em (5.0.3), encontramos $x_3 = 3$.

Assim, as raízes de $p(x)$ são $\{1, 1, 3\}$.

15. **Escreva a forma fatorada do polinômio $P(x) = x^3 - 3x^2 - 6x + 8$ sabendo que as raízes são todas inteiras e a soma de duas de suas raízes é igual a 5.**

Esta é a questão 4 que já foi resolvida. Queremos aqui dar uma outra resolução com base nas relações entre os coeficientes e raízes do polinômio. Suponhamos $x_1 + x_2 = 5$ e substituindo na relação $x_1 + x_2 + x_3 = 3$, temos:

$$5 + x_3 = 3 \Longrightarrow x_3 = -2$$

Pela proposição 4.2.5, temos que x_1 e x_2 são inteiros e divisores de 8, logo $x_1, x_2 \in \{1, 2, 4, 8\}$ e $x_1 + x_2 = 5$, o que nos leva a concluir que $x_1 = 1$ e $x_2 = 4$. Assim, as raízes do polinômio são $\{-2, 1, 4\}$.

16. **As raízes do polinômio $p(x) = x^3 - 6x^2 + kx + 64$ estão em P.G. Nessas condições, calcule o coeficiente k.**

Como as raízes estão em P.G., podemos escrever $x_1 = \frac{a}{q}$, $x_2 = a$ e $x_3 = aq$.

Das relações de Girard, temos:

$$x_1x_2x_3 = -64 \Longrightarrow \frac{a}{q} \cdot a \cdot aq = -64 \Longrightarrow a^3 = -64 \Longrightarrow a = -4$$

Substituindo -4 no polinômio, encontramos:

$$(-4)^3 - 6(-4)^2 + k(-4) + 64 = 0$$

$$-64 - 96 - 4k + 64 = 0$$

$$4k = -96 \Longrightarrow k = -24$$

17. **Dona Leide foi ao shopping comprar presente do dia das crianças para seus netos menores. O número de presentes que ela vai comprar equivale ao número de raízes distintas do polinômio $p(x) = x^4 - 9x^3 + 30x^2 - 44x + 24$. Descubra o número de netos pequenos que dona Leide tem, sabendo que todas as raízes de $p(x)$ são inteiras.**

As possíveis raízes racionais do polinômio $p(x)$ pertencem ao conjunto dos divisores de 24: $D(24) = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 8, \pm 12, \pm 24\}$. Por substituição: $p(1) = 2,\ p(-1) = 108,\ p(2) = 0$. Logo, 2 é raiz de $p(x)$ e pelo algoritmo da divisão:

$$x^4 - 9x^3 + 30x^2 - 44x + 24 = (x - 2)(x^3 - 7x^2 + 16x - 12)$$

Encontremos, agora, as raízes do polinômio $q(x) = x^3 - 7x^2 + 16x - 12$. As possíveis raízes pertencem ao conjuntos dos divisores de 12:

$$D(12) = \{\pm 1, \pm 2 \pm 3, \pm 4, \pm 6, \pm 12\}.$$

Novamente por substituição: $q(1) = -2,\ q(-1) = -36,\ p(2) = 0$. Logo, 2 é raiz de $x^3 - 7x^2 + 16x - 12$ e pelo algoritmo da divisão, temos:

$$x^3 - 7x^2 + 16x - 12 = (x - 2)(x^2 - 5x + 6).$$

As raízes de $x^2 - 5x + 6$ são $\{2, 3\}$. Assim, as raízes distintas de $p(x)$ são 2 e 3. Logo, dona Leide tem 2 netos pequenos.

18. **O polinômio $p(x) = x^4 + x^3 - 7x^2 - x + 6$ tem quatro raízes inteiras, sendo duas simétricas. Quais são essas raízes?**

Sabemos que

$$x_1 + x_2 + x_3 + x_4 = -\frac{1}{1} = -1$$

Podemos escrever $x_2 = -x_1$. Substituindo na espressão acima,

$$x_1 - x_1 + x_3 + x_4 = -1 \Longrightarrow x_3 + x_4 = -1$$

Como $x_1, x_2, x_3, x_4 \in \{-1, 1, -2, 2, -3, 3, -6, 6\}$, temos quatro opções: $\{-1, 1, 2, -3\}$; $\{-3, 3, -2, 1\}$; $\{-6, 6, -3, 2\}$ ou $\{-6, 6, -2, 1\}$.

Mas, $x_1x_2x_3x_4 = 6$, logo apenas uma das opções satisfaz esta condição: $\{-1, 1, 2, -3\}$.

19. **Uma das raízes do polinômio $p(x) = x^3 + 11x^2 - 160x + 400$, que tem três raízes distintas, é -20. Sem usar a divisão de polinômios, encontre as outras duas raízes sabendo que estas são inteiras.**

Decompondo 400 em fatores primos temos: $400 = 2^4 \cdot 5^2$. Se uma raiz é -20, por Girard as outras são divisores de 20, pois o produto das 3 raízes é igual a -400 então só podem ser (1,20), (-1,-20), (2, 10), (-2, -10), (4, 5), (-4, -5). Dessa forma, é só testar se 1,-1, 2, -2, 4, -4 são raízes. Obtendo que, dessa lista, apenas o par (4,5) tem as raizes, do polinômo.

Outra solução: Seja $x_1 = -20$. Então

$$x_1 + x_2 + x_3 = -11 \Longrightarrow -20 + x_2 + x_3 = -11 \Longrightarrow$$

$$x_2 + x_3 = 9 \Longrightarrow x_2 = 9 - x_3 \tag{5.0.6}$$

$$x_1x_2 + x_1x_3 + x_2x_3 = -160 \Longrightarrow -20x_2 - 20x_3 + x_2x_3 = -160 \tag{5.0.7}$$

$$x_1x_2x_3 = -400 \Longrightarrow -20x_2x_3 = -400 \Longrightarrow x_2x_3 = 20 \tag{5.0.8}$$

Vamos analisar as substituições possíveis:

Substituindo (5.0.6) e (5.0.8) em (5.0.7),

$$-20(9 - x_3) - 20x_3 + 20 = -160$$

$$-180 + 20x_3 - 20x_3 + 20 = -160$$

$$-160 = -160$$

Observe que esta substituição não nos fornece valores para x_2 e x_3, portanto façamos a substituição apenas de (5.0.6) em (5.0.7).

$$-20(9 - x_3) - 20x_3 + (9 - x_3)x_3 = -160$$

$$-180 + 20x_3 - 20x_3 + 9x_3 - x_3^2 + 160 = 0$$

$$-x_3^2 + 9x_3 - 20 = 0$$

Resolvendo a equação quadrática encontramos $x_3 = 4 \Longrightarrow x_2 = 5$ ou $x_3 = 5 \Longrightarrow x_2 = 4$.

Em qualquer das situações, temos que as raízes serão $\{-20, 4, 5\}$.

20. **A diferença entre duas das raízes do polinômio $P(x) = x^3 - 4x^2 - 17x + 60$ é 2. Quais são as raízes desse polinômio sabendo que todas são inteiras?**

Com a diferença entre duas das raízes é 2, podemos escrever

$$x_1 - x_2 = 2 \Longrightarrow x_1 = 2 - x_2. \tag{5.0.9}$$

Pelas relações de Girard $x_1 + x_2 + x_3 = 4$, então

$$2 + x_2 + x_2 + x_3 = 4 \Longrightarrow 2x_2 + x_3 = 2 \Longrightarrow x_3 = 2 - 2x_2 \tag{5.0.10}$$

Além disso, temos que

$$x_1x_2 + x_1x_3 + x_2x_3 = -17 \tag{5.0.11}$$

Substituindo as equações (5.0.9) e (5.0.10) em (5.0.11), temos:

$$(2 + x_2)x_2 + (2 + x_2)(2 - 2x_2) + x_2(2 - 2x_2) = -17$$

$$2x_2 + x_2^2 + 4 - 4x_2 + 2x_2 - 2x_2^2 + 2x_2 - 2x_2^2 = -17$$

$$-3x_2^2 + 2x_2 + 21 = 0$$

Resolvendo a equação do segundo grau, encontramos $x_2 = -\frac{7}{3}$ e $x_2 = 3$. Mas $-\frac{7}{3}$ não pode ser raiz, logo, $x_2 = 3$.

Substituindo o valor de x_2 em (5.0.9) e(5.0.10), encontramos $x_1 = 5$ e $x_3 = -4$.

Outra resolução: Analisando a decomposição em fatores primos de 60, temos $60 = 2^2 \cdot 3 \cdot 5$. Como a soma das três raízes deve ser 4 e o produto -60, devemos ter 1 ou 3 raízes negativas. Mas se as três forem negativas, não poderemos ter soma 4, portanto teremos apenas uma raiz negativa e duas positivas.

Dentre os divisores de 60,

$$D(60) = \{\pm1, \pm2, \pm3, \pm4, \pm5, \pm6, \pm12, \pm15, \pm20, \pm30, \pm60\},$$

tomando um divisor negativo e fazendo a combinação com outros dois positivos, chegamos às raízes que só podem ser $\{-4, 3, 5\}$.

21. **O polinômio $p(x) = x^5 - 7x^4 + 10^3 + 18x^2 - 27x - 27$ tem raízes inteiras sendo uma dupla e uma tripla. Encontrar suas raízes.**

Pelas relações de Girard temos que a soma das raízes é 7 e o produto entre elas é 27. Observando a decomposição em fatores primos de $27 = 3^3$, temos que as raízes só podem ser ±1 a dupla e ±3 a tripla.

Para avaliarmos o sinal da raiz vamos substituir 1 e -1 no polinômio.

$$p(1) = 1 - 7 + 10 + 18 - 27 - 27 = -32$$

$$p(-1) = -1 - 7 - 10 + 18 + 27 - 27 = 0$$

Logo, -1 é a raiz dupla de $p(x)$ e como o produto é positivo, -3 não pode ser a raiz tripla, assim temos que a raiz tripla é 3.

22. **As raízes do polinômio** $p(x) = x^3 - 14x^2 + 64x - 96$ **são inteiras e positivas. Sabendo que o polinômio tem raiz dupla e que o** mmc **entre as raízes é igual a 12 e o** mdc **é igual a 2, determine-as.**

    Observemos a decomposição em fatores primos do número $96 = 2^5 \cdot 3$.

    Como o mdc é 2, o número 3 não pode ser raiz, e como o expoente do 3 na decomposição é 1, ele n pode ser fator da raiz dupla, logo temos as seguintes opções de raízes: (1,1,96); (2,2,24) ou (4,4,6).

    Como o mmc é 12, a opção que nos dá as raízes do polinômio é (4,4,6).

23. **O polinômio** $p(x) = x^5 - 26x^4 + 252x^3 - 1114x^2 + 2147x - 1260$ **tem cinco raízes inteiras positivas distintas. Encontre estas raízes sabendo que são duas a duas primas entre si.**

    Decompondo 1260 em fatores primos, encontramos $1260 = 2^2 \cdot 3^2 \cdot 5 \cdot 7$.

    Como as raízes são todas duas a duas primas entre si, a raiz que tiver um fator primo deve conter todos eles, logo duas prováveis raízes são 4 e 9. Também ñão podemos ter números com mais de um fator primo como 6, 15, 20, 35 ou 45 como raiz. Sendo assim, as possíveis raízes são 4,9,5,7 e 1. Como as raízes são todas positivas e a soma deve ser 26, temos 1+4+5+7+9=26.

    Assim as raízes do polinômio são (1,4,5,7,9).

24. **O polinômio** $p(x) = x^4 + 15x^3 + 80x^2 + 180x + 144$ **tem quatro raízes inteiras negativas. Sabendo que o mmc entre duas delas é 12 e que o mdc entre as mesmas duas raízes é 2, encontre todas as raízes deste polinômio.**

    Escrevamos a e b as duas raízes cujos valores do mmc e mdc são dados. Pela proposição 3.1.25 temos que $\text{mmc}(a,b) \cdot \text{mdc}(a,b) = a \cdot b$, logo $a \cdot b = 24$. Como o produto das quatro raízes deve ser igual a 144, temos que o produto das duas raízes restantes será 144:24=6, e assim temos as seguintes opções: $(-1,-6)$ ou $(-2,-3)$, já que são todas negativas.

Testando -1 e -2 verificamos que:

$$p(-1) = 1 - 15 + 80 - 180 + 144 = 30$$

$$p(-2) == (-2)^4 + 15(-2)^3 + 80(-2)^2 + 180(-2) + 144 = 0$$

Logo, duas raízes deste polinômio são -2 e -3.

Podemos, agora, efetuar a divisão de $p(x)$ por $(x+2)(x+3) = x^2 + 5x + 6$ e encontrar as raízes do quociente usando a fórmula de Bhaskara, ou ainda analisar que, como o produto de a e b é igual a 24, temos as opções $(-2, -12)$ ou $(-4, -6)$. Como a soma das quatro raízes deve ser -15 e já concluímos que -2 e -3 são raízes, temos que:$-2-3-2-12 = -19$ e $-2-3-4-6 = -15$.

Assim, as raízes de $p(x)$ são $(-2, -3, -4, -6)$.

25. **O polinômio $p(x) = x^4 - 28x^3 + 260x^2 - 89x + 960$ tem quatro raízes inteiras positivas e distintas. Sabendo que o mmc entre elas é 60 e o mdc é 2, encontre as raízes.**

    Como o mdc entre as raízes é 2, temos que todas são números pares. Pela decomposição do número $960 = 2^6 \cdot 3 \cdot 5$ observamos que os 6 fatores 2 estão assim distribuídos: três raízes com um fator 2 e uma com três fatores 2 ou duas raízes com um fator 2 e duas com dois fatores 2.

    Resta-nos distribuir os fatores 3 e 5. Para a primeira opção de distriuição do 2^6 só podemos ter as raizes $(2, 6, 8, 10)$, já que todas devem ser distintas. Para a segunda distribuição podemos ter $(2, 4, 6, 20)$ ou $(2, 4, 10, 12)$.

    Para decidirmos qual das três combinações forma as raízes do polinômio, observemos que a soma destas deve ser igual a 28, assim:

    $$2 + 6 + 8 + 10 - 26$$

    $$2 + 4 + 6 + 20 = 32$$

    $$2 + 4 + 10 + 12 = 28$$

    Logo, as raízes de $p(x)$ são $(2, 4, 10, 12)$.

Mostraremos aqui alguns exemplos de raízes racionais, onde além das relações de Girard, usaremos a proposição 4.2.5 que no ensino médio é trabalhada, normalmente logo após as relações entre raízes e coeficientes.

26. **As dimensões a, b e c, em cm, de um paralelepípedo retângulo, são as raízes do polinômio $p(x) = 6x^3 - 44x^2 + 103x - 77$.**

a) **Calcule o volume do paralelepípedo.**

b) **Calcule a soma das áreas das faces desse paralelepípedo.**

Pelas relações de Girard,

$$a + b + c = -\frac{-44}{6} = \frac{22}{3}$$

$$ab + ac + bc = \frac{103}{6}$$

$$abc = -\frac{-77}{6} = \frac{77}{6}$$

a) $V = abc = \frac{77}{6} cm^3$

b) $A_{total} = 2(ab + ac + bc) = 2 \cdot \frac{103}{6} = \frac{103}{3} cm^2$

27. **Pesquisar as raízes dos polinômios, sabendo que são todas distintas e racionais.**

a) $p(x) = 2x^3 - x^2 - 2x + 1$.

De acordo com a proposição 4.2.5, temos que as raízes pertencem ao conjunto $\{-1, 1, -\frac{1}{2}, \frac{1}{2}\}$. E pelas relações de Girard,

$$x_1 + x_2 + x_3 = -\frac{1}{2}$$

$$x_1 x_2 x_3 = \frac{1}{2}$$

Como temos 3 raízes distintas cuja soma é $-\frac{1}{2}$ e o produto é $\frac{1}{2}$, a única solução possível é $S = \{-1, 1, -\frac{1}{2}\}$.

b) $g(x) = 2x^3 - 7x^2 + 7x - 2$

O conjunto solução S pertence ao conjunto $\{-\frac{1}{2}, \frac{1}{2} - 1, 1, -2, 2\}$ de acordo com a proposição 4.2.5. E segundo as relações de Girard,

$$x_1 + x_2 + x_3 = \frac{7}{2}$$

$$x_1 x_2 x_3 = \frac{2}{2} = 1$$

Como o produto das três raízes deve ser 1, temos as opções: $\{-1, -\frac{1}{2}, 2\}$; $\{-1, \frac{1}{2}, -2\}$; $\{1, \frac{1}{2}, 2\}$ ou $\{-\frac{1}{2}, 1, -2\}$. Como a soma das raízes deve ser $\frac{7}{2}$, calculemos a soma das opções apresentadas:

$$-1 - \frac{1}{2} + 2 = \frac{1}{2}$$

$$-1 + \frac{1}{2} - 2 = -\frac{5}{2}$$

$$1 + \frac{1}{2} + 2 = \frac{7}{2}$$
$$1 - \frac{1}{2} - 2 = -\frac{3}{2}$$

Observando as somas, concluímos que as raízes de $g(x)$ são $\{\frac{1}{2}, 1, 2\}$.

c) $h(x) = 2x^3 + 3x^2 - 8x + 3$

Sabemos que a solução pertence ao conjunto

$$\{-\frac{1}{3}, \frac{1}{3}, -\frac{1}{2}, \frac{1}{2}, -1, 1, -3, 3\}.$$

Além disso temos as relações:

$$x_1 + x_2 + x_3 = -\frac{3}{2}$$

$$x_1 x_2 x_3 = -\frac{3}{2}$$

Assim, temos as seguintes possibilidades: $\{-3, \frac{1}{2}, 1\}$; $\{-\frac{1}{2}, 1, 3\}$ e $\{-1, \frac{1}{2}, 3\}$.

Analisemos as somas:

$$-3 + \frac{1}{2} + 1 = -\frac{3}{2}$$
$$-\frac{1}{2} + 1 + 3 = \frac{7}{2}$$

Pela soma, as raízes do polinômio $h(x)$ são $\{-3, \frac{1}{2}, 1\}$. Verifiquemos o produto:

$$-3 \cdot \frac{1}{2} \cdot 1 = -\frac{3}{2}.$$

Observação 5.0.2. É possível criar inúmeros problemas para explorar e estimular a habilidade dos alunos a partir dos modelos expostos no trabalho. Para tanto,basta um pouco de imaginação por parte do professor.

Bibliografia

[1] AYRES JR, Frank. **Álgebra Moderna**. São Paulo - Rio de Janeiro - Belo Horvizonte: Editora McGraw-Hill do Brasil Ltda, 1973.

[2] BOYER, Carl Benjamin. **História da Matemática**. 2ª ed. Trad. ELZA F. OMIDE. São Paulo: Edgard Blücher, 1996

[3] DOMINGUES, Hygino H. **Fundamentos de Aritmética**. São Paulo: Atual. 1991.

[4] DOMINGUES, Hygino H. e IEZZI, Gelson. **Álgebra Moderna**. 3ª ed. São Paulo: Atual editora, 1982.

[5] EVES, Howard Whitley. **Introdução à história da Matemática**. 5ª ed.Campinas: Unicamp, 1997.

[6] FERNANDES, Angela Maria Vidigal; et al. **Fundamentos de Álgebra**. Belo Horizonte: Editora UFMG, 2005.

[7] GARBI, Gilberto G. **O Romance das Equações Algébricas**. São Paulo: Makron Books, 1997.

[8] GARCIA, Arnaldo e LEQUIAN, Yves. **Elementos de álgebra**. 4ª ed. Rio de Janeiro: Impa, Projeto Euclides, 2008.

[9] GIOVANNI, José Ruy e BONJORNO, José Roberto. **Matemática: uma nova abordagem**: vol3. São Paulo: FTD, 2001.

[10] GONÇALVES, Adilson. **Introdução à Álgebra**. 5ª ed. Rio de Janeiro: Impa, Projeto Euclides, 2008.

[11] HEFEZ, Abramo e VILLELA, Maria Lúcia Torres. **Polinômios e Equações Algebricas**. 1ª ed. Rio de Janeiro: SBM, 2012. (Coleção Profmat)

[12] MARTINEZ, FABIO Brochero; et al. **Teoria dos Números**: um passeio com primos e outros números familiares pelo mundo inteiro. 3ª ed. Rio de Janeiro: IMPA, 2013.

[13] MONTEIRO, Luiz Henrique Jacy. **Elementos de Álgebra**. Rio de Janeiro: Ao Livro Técnico S.A., 1969.

[14] NETO, Antonio Caminha Muniz. **Tópicos de Matemática Elementar**: Volume 6 - Polinômios. 1ª ed. Rio de Janeiro: SBM, 2012. (Coleção Professor de Matemática)

[15] MARQUES, Maria Cristina. **Introdução à Teoria de Anéis**. UFMG. Disponível em ⟨ http//www.mat.ufmg.br/ marques/Apostila-Aneis.pdf⟩. Acesso em 01 nov. 2013.

[16] SANTOS, José Plinio de Oliveira. **Introdução à Teoria dos Números**. Rio de Janeiro: Impa, 1998. (Coleção Matemática Universitária)

[17] DIVISIBILIDADE e o Algoritmo da Divisão em $\mathbb{Z}$. Disponível em ⟨ http://www.dm.ufscar.br/ sampaio/itn2007cap03.pdf⟩ Acesso em 15 nov.2013.

[18] RELAÇÕES de Girard. Disponível em ⟨ http://www.colegioweb.com.br/trabalhos-escolares/matematica/equacoes-algebricas/relacoes-de-girard.html.⟩ Acesso em 19 dez. 2013.