UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
INSTITUTO DE GEOCIÊNCIAS E CIÊNCIAS EXATAS

Programa de Pós-Graduação em Matemática em Rede Nacional

Um Estudo sobre Polinômios Aplicado a Reticulados e à Resolução de Problemas no Ensino Médio

Flávio Faria Massarioli

PROFMAT

Rio Claro - SP
2022

Universidade Estadual Paulista "Júlio de Mesquita Filho"
Instituto de Geociências e Ciências Exatas
Câmpus de Rio Claro

Um Estudo sobre Polinômios Aplicado a Reticulados e à Resolução de Problemas no Ensino Médio

Flávio Faria Massarioli

Dissertação apresentada como parte dos requisitos para obtenção do título de Mestre em Matemática, junto ao Programa de Pós-Graduação – Mestrado Profissional em Matemática em Rede Nacional, do Instituto de Geociências e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", Câmpus de Rio Claro.

Orientadora
Profa. Dra. Carina Alves

Rio Claro - SP
2022

M414e

Massarioli, Flávio Faria

Um estudo sobre polinômios aplicado a reticulados e à resolução de problemas no ensino médio / Flávio Faria Massarioli. -- Rio Claro, 2022

80 p. : il.

Dissertação (mestrado) - Universidade Estadual Paulista (Unesp), Instituto de Geociências e Ciências Exatas, Rio Claro

Orientadora: Carina Alves

1. Algebra. 2. Polinomios. 3. Teoria dos reticulados. I. Título.

Sistema de geração automática de fichas catalográficas da Unesp. Biblioteca do Instituto de Geociências e Ciências Exatas, Rio Claro. Dados fornecidos pelo autor(a).

Essa ficha não pode ser modificada.

TERMO DE APROVAÇÃO

Flávio Faria Massarioli

Um Estudo sobre Polinômios Aplicado a Reticulados e à Resolução de Problemas no Ensino Médio

Dissertação APROVADA como requisito parcial para a obtenção do grau de Mestre no Curso de Pós-Graduação – Mestrado Profissional em Matemática em Rede Nacional, do Instituto de Geociências e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", pela seguinte banca examinadora:

Profa. Dra. Carina Alves
Orientadora

Profa. Dra. Marta Cilene Gadotti
Departamento de Matemática - UNESP-Rio Claro

Prof. Dr. Wladimir Seixas
Departamento de Matemática - UFSCar-São Carlos

Rio Claro, 21 de setembro de 2022

Aos meus pais, João e Natália.

Agradecimentos

A Deus, em quem vivemos, nos movemos e existimos.

À minha esposa Adna, pelo amor verdadeiro e pela alegria de viver ao seu lado.

Às minhas filhas, Lívia e Cecília, por tornarem meus dias muito mais felizes e divertidos.

Aos meus pais, João e Natália, pelo amor provado no cuidado e dedicação que sempre tiveram para comigo.

Ao meu irmão Lucas, por ser para mim exemplo de lealdade, responsabilidade e confiança em Deus, e à sua linda família.

Aos meus familiares pelo apoio e incentivo.

Aos colegas de turma do PROFMAT, por terem sido verdadeiros companheiros, ajudando e incentivando sempre.

Aos meus irmãos em Cristo da Casa de Oração do Bairro Santa Terezinha, por serem verdadeiramente irmãos.

Aos colegas de trabalho pela ajuda, incentivo e compreensão.

Aos professores deste curso e em especial à minha orientadora, Professora Doutora Carina Alves, por sua dedicação e por me ajudar a dar este passo tão importante na minha carreira.

Ao Departamento de Matemática da Unesp de Rio Claro, por promover o PROFMAT no campus de Rio Claro conciliando seriedade e humanidade.

Em todo trabalho há proveito; meras palavras, porém, levam à penúria.
Provérbios 14.6

Resumo

O presente trabalho mostra como o estudo dos Polinômios nos fornece resultados importantes para a modelagem e resolução de problemas diversos. Dentre esses resultados estão a Divisão Euclidiana, as Relações de Girard, as Equações Polinomiais de 2º e 3º graus e suas fórmulas resolutivas. Mostramos aplicações desses resultados no desenvolvimento de um método alternativo às fórmulas de Cardano e na construção de reticulados densos e reticulados bem arredondados estabelecendo assim uma interessante relação entre a Álgebra e a Geometria. Apresentamos ainda a sugestão de diversos problemas e atividades para serem desenvolvidos com os alunos do Ensino Médio.

Palavras-chave: Álgebra, Polinômios, Equações Polinomiais, Fórmulas de Cardano, Reticulados.

Abstract

The present work shows how the study of Polynomials provides us with important results for the modeling and resolution of diverse problems. Among these results are the Euclidean Division, the Girard Relations, the 2nd and 3rd degree Polynomial Equations and their solving formulas. We show applications of these results in the development of an alternative method to Cardano's formula and in the construction of dense lattices and well-rounded lattices, thus establishing an interesting relationship between Algebra and Geometry. We also present the suggestion of several problems and activities to be developed with high school students.

Keywords: Algebra, Polynomials, Polynomial Equations, Cardano's Formula, Lattices.

Lista de Figuras

Sumário

1 Introdução

Neste trabalho apresentamos um estudo sobre polinômios com aplicações na resolução de problemas diversos e na construção de reticulados em $\mathbb{R}^2$ e $\mathbb{R}^3$. Além disso, ao final do trabalho, apresentamos sugestões de exercícios e atividades para serem aplicadas no Ensino Médio.

Na BNCC, o estudo dos polinômios e equações polinomiais está previsto tanto para o Ensino Fundamental como para o Ensino Médio. Em seu texto é dito que "No Ensino Fundamental – Anos Finais, os estudos de Álgebra retomam, aprofundam e ampliam o que foi trabalhado no Ensino Fundamental – Anos Iniciais." [7, p. 270]. Embora no Ensino Médio não haja essa divisão das habilidades em unidades temáticas, nas considerações sobre a organização dos currículos de matemática para o Ensino Médio, encontramos a sugestão de organizar esses currículos em unidades semelhantes às do Ensino Fundamental, sendo uma delas Números e Álgebra. Além disso, são descritas habilidades que apontam claramente para o estudo dos polinômios e equações polinomiais no Ensino Médio como, por exemplo, a habilidade "(EM13MAT302) Construir modelos empregando as funções polinomiais de 1º ou 2º graus, para resolver problemas em contextos diversos, com ou sem apoio de tecnologias digitais." [7, p. 536].

Para o que diz respeito as aplicações do estudo dos polinômios na resolução de equações polinomiais de 3º grau e na construção de reticulados em $\mathbb{R}^2$ e $\mathbb{R}^3$, consideramos a Lei nº 13.415/2017, conhecida como a lei do Novo Ensino Médio, a qual estabelece que o currículo de Ensino Médio deve ser composto pela BNCC e por itinerários formativos que podem servir, dentre outras opções, ao aprofundamento acadêmico em uma ou mais dessas áreas.

Considerando o que está previsto sobre o estudo de polinômios na BNCC e a existência de itinerários formativos de matemática onde esse estudo pode ser aprofundado, apresentamos, ao final do trabalho, sugestões de problemas e atividades relacionadas a polinômios para serem aplicadas no Ensino Médio e que sirvam tanto ao desenvolvimento das habilidades previstas na BNCC quanto ao aprofundamento acadêmico num itinerário formativo de matemática.

Com relação à estrutura do trabalho, no Capítulo 2 apresentamos alguns resultados sobre polinômios e equações polinomiais que serão importantes para a compreensão e desenvolvimento dos capítulos posteriores. No Capítulo 3 aprofundamos a análise das equações polinomiais do 3º grau, apresentando um método alternativo às fórmulas de Cardano que torna mais simples, de um ponto de vista computacional, a resolução de equações do 3º grau com coeficientes reais onde não configuram o termo do 2º grau. No Capítulo 4 aplicamos os conceitos estudados no Capítulo 2 para obter reticulados densos e reticulados bem arredondados, via raízes de polinômios de 2º e 3º graus. Finalmente, no Capítulo 5 sugerimos atividades para serem desenvolvidas por alunos do Ensino Médio.

2 Polinômios

Neste capítulo apresentamos alguns resultados elementares sobre polinômios com coeficientes em $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$. Tais resultados são, sempre que possível, estendidos para polinômios sobre $\mathbb{Z}$ e outros resultados para polinômios sobre esse conjunto são apresentados a fim de propiciar uma melhor compreensão dos capítulos posteriores. Em seu desenvolvimento, toda vez que uma propriedade for válida para polinômios sobre $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$, escreveremos apenas $\mathbb{K}$ para de denotar tais conjuntos. Para a elaboração deste capítulo usamos as seguintes referências: [21], [20], [16], [15], [6], e [5].

2.1 Definições e propriedades básicas

Definição 2.1. Uma sequência infinita $(a_0, a_1, a_2, \dots)$ de elementos de $\mathbb{K}$ é dita quase toda nula se existir $n \geqslant -1$ tal que

$$a_{n+1} = a_{n+2} = a_{n+3} = \cdots = 0.$$

Em palavras, uma sequência $(a_0, a_1, a_2, \dots)$ é quase toda nula se todos os seus termos, de uma certa posição em diante, forem iguais a zero. Por exemplo, as sequências

$$(0, 0, 0, 0, 0, 0, \dots) \text{ e } (1, 2, 3, \dots, n, 0, 0, 0, \dots)$$

são quase todas nulas; por outro lado, a sequência $(1, 0, 1, 0, 1, \dots)$, com 1's e 0's se alternando indefinidamente, não é quase toda nula.

Definição 2.2. Um polinômio sobre (ou com coeficientes em) $\mathbb{K}$ é uma soma formal $f = f(X)$ do tipo

$$f(X) = a_0 + a_1X + a_2X^2 + a_3X^3 + \cdots = \sum_{k\geqslant 0} a_kX^k,$$

onde $(a_0, a_1, a_2, \dots)$ é uma sequência quase toda nula de elementos de $\mathbb{K}$ e convencionamos $X^0 = 1$ e $X^1 = X$ no somatório acima.

Observação 2.3. Na Definição 2.2 , X é um símbolo qualquer. Em particular, X não representa uma variável.

Definição 2.4. Os polinômios $f(X) = \sum_{k\geqslant 0} a_kX^k$ e $g(X) = \sum_{k\geqslant 0} b_kX^k$ sobre $\mathbb{K}$ são **iguais** se, e só se, $a_k = b_k$, para todo $k \geqslant 0$.

Dado um polinômio $f(X) = a_0 + a_1X + a_2X^2 + a_3X^3 + \cdots$ sobre $\mathbb{K}$, adotamos as seguintes convenções:

1. Os elementos $a_i \in \mathbb{K}$ são chamados de os **coeficientes** de f. As parcelas a_iX^i são chamadas de termos e os termos a_iX^i, tais que $a_i \neq 0$ são chamados **monômios** de grau i do polinômio f.

2. Quando $a_i = 0$ omitiremos, sempre que for conveniente, o termo a_iX^i. Em particular, como a sequência $(a_0, a_1, a_2, \dots)$ é quase toda nula, existe um inteiro $n \geqslant 0$ para o qual podemos escrever

$$f(X) = \sum_{k=0}^{n} a_k X^k.$$

3. Quando $a_i = \pm 1$, escreveremos $\pm X^i$ em vez de $(\pm 1)X^i$, para o termo correspondente de f.

4. O polinômio $0 = 0 + 0X + 0X^2 + \cdots$ é denominado o polinômio identicamente nulo sobre $\mathbb{K}$. Sempre que não houver confusão com $0 \in \mathbb{K}$, denotaremos o polinômio identicamente nulo sobre $\mathbb{K}$ por 0.

5. Mais geralmente (e consoante 2), dado $\alpha \in \mathbb{K}$, denotamos o polinômio $\alpha + 0X + 0X^2 + \cdots$ simplesmente por α e o denominamos o **polinômio constante** α; em cada caso, o contexto deixará claro se estamos nos referindo ao polinômio constante e igual a α ou ao elemento $\alpha \in \mathbb{K}$.

Denotamos por $\mathbb{K}[X]$ o conjunto de todos os polinômios sobre $\mathbb{K}$. A partir do item 5 acima, convencionamos que

$$\mathbb{K} \subset \mathbb{K}[X].$$

Por outro lado, as inclusões $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ fornecem as inclusões

$$\mathbb{Q}[X] \subset \mathbb{R}[X] \subset \mathbb{C}[X].$$

Exemplo 2.5. Se $f(X) = 2 - 3X^2 + \sqrt{5}X^4 - \frac{3}{4}X^6$, então $f \notin \mathbb{Q}[X]$ (uma vez que $\sqrt{5} \notin \mathbb{Q}$) mas $f \in \mathbb{R}[X]$. Já a expressão $g = X + X^3 + X^5 + X^7 + \cdots$ não é um polinômio, uma vez que a sequência $(0, 1, 0, 1, \dots)$ não é quase toda nula.

Definiremos sobre $\mathbb{K}[X]$ as operações

$$\oplus\colon \mathbb{K}[X] \times \mathbb{K}[X] \to \mathbb{K}[X] \quad \text{e} \quad \odot\colon \mathbb{K}[X] \times \mathbb{K}[X] \to \mathbb{K}[X]$$

denominadas, respectivamente, de **adição** e **multiplicação**. Antes, contudo, necessitamos do seguinte resultado.

Lema 2.6. *Se $(a_k)_{k\geqslant 0}$ e $(b_k)_{k\geqslant 0}$, são sequências quase todas nulas de elementos de $\mathbb{K}$, então também são quase todas nulas as sequências $(a_k \pm b_k)_{k\geqslant 0}$ e $(c_k)_{k\geqslant 0}$, onde*

$$c_k = \sum_{\substack{i+j=k \\ i,j\geq 0}} a_i b_j = \sum_{i=0}^{k} a_i b_{k-i}.$$

Demonstração. Mostremos primeiramente que a sequência $(a_k \pm b_k)_{k\geqslant 0}$ é quase toda nula. Sejam $m, n \in \mathbb{Z}_+$ tais que $a_i = 0$ para $i > n$ e $b_j = 0$ para $j > m$. Sem perda de generalidade, suponhamos $m \geqslant n$. Se $k > m$, então $a_k = b_k = 0$ e consequentemente $a_k \pm b_k = 0$.

Agora mostremos que a sequência $(c_k)_{k\geqslant 0}$ é quase toda nula. Sejam $m, n \in \mathbb{Z}_+$ tais que $a_i = 0$ para $i > n$ e $b_j = 0$ para $j > m$. Se $k > m+n$ e $i+j = k$, com $i, j \geqslant 0$, então $i > n$ ou $j > m$, do contrário, teríamos $k = i+j \leqslant n+m$, o que não é o caso. Mas, como $i > n$, então $a_i = 0$ e $j > m$, e então $b_j = 0$. Em qualquer caso temos $a_i b_j = 0$, e assim,

$$c_k = \sum_{\substack{i+j=k \\ i,j\geq 0}} a_i b_j = 0.$$

□

A partir do Lema 2.6 apresentamos a seguir as definições das operações de adição e multiplicação de polinômios.

Definição 2.7. Dados em $\mathbb{K}[X]$ os polinômios

$$f(X) = \sum_{k\geqslant 0} a_k X^k \quad \text{e} \quad g(X) = \sum_{k\geqslant 0} b_k X^k,$$

a **soma** e o **produto** de f e g, denotados respectivamente por $f \oplus g$ e $f \odot g$, são os polinômios

$$(f \oplus g)(X) = \sum_{k\geqslant 0} (a_k + b_k) X^k$$

e

$$(f \odot g)(X) = \sum_{k\geqslant 0} c_k X^k,$$

onde $c_k = \sum_{\substack{i+j=k \\ i,j\geq 0}} a_i b_j$.

Embora não pareça, a definição do produto de dois polinômios é bastante natural: a fórmula para o coeficiente c_k de $f \odot g$ é necessária a fim de que valham a distributividade da operação $\odot$ em relação à operação $\oplus$, assim como a regra de potenciação $X^m \odot X^n = X^{m+n}$. De fato, se tais propriedade forem válidas, então, calculando o produto

$$(a_0 + a_1 X + a_2 X^2 + \cdots) \odot (b_0 + b_1 X + b_2 X^2 + \cdots)$$

distributivamente obtemos

$$a_0 b_0 = \sum_{\substack{i+j=0 \\ i,j\geqslant 0}} a_i b_j$$

para coeficiente de X^0,

$$a_0 b_1 + a_1 b_0 = \sum_{\substack{i+j=1 \\ i,j\geqslant 0}} a_i b_j$$

para coeficiente de X,

$$a_0 b_2 + a_1 b_1 + a_2 b_0 = \sum_{\substack{i+j=2 \\ i,j\geqslant 0}} a_i b_j$$

para coeficiente de X^2 e assim por diante.

Proposição 2.8. *Sejam f, g e h polinômios em $\mathbb{K}[X]$. Então valem as seguintes propriedades:*

1. ***Comutatividade:*** *$f \oplus g = g \oplus f$ e $f \odot g = g \odot f$;*

2. ***Associatividade:*** $(f \oplus g) \oplus h = f \oplus (g \oplus h)$ *e* $(f \odot g) \odot h = f \odot (g \odot h)$*;*

3. ***Distributividade:*** $f \odot (g \oplus h) = f \odot g \oplus f \odot h$*.*

Demonstração. Sejam $f(X) = \sum_{k=0}^{n} a_k X^k$, $g(X) = \sum_{k=0}^{m} b_k X^k$ e $h(X) = \sum_{k=0}^{l} c_k X^k$, polinômios em $\mathbb{K}[X]$.

1.1. Comutatividade da adição:

$$(f \oplus g)(X) = \sum_{k \geqslant 0} (a_k + b_k) X^k = \sum_{k \geqslant 0} (b_k + a_k) X^k = (g \oplus f)(X)$$

pois em $\mathbb{K}$, temos $a_i + b_j = b_j + a_i$, para quaisquer i e j.

1.2. Comutatividade da multiplicação:

$$(f \odot g)(X) = \sum_{k=0}^{n+m} \Big(\sum_{\substack{i+j=k \\ i,j \geqslant 0}} a_i b_j \Big) X^k = \sum_{k=0}^{n+m} \Big(\sum_{\substack{i+j=k \\ i,j \geqslant 0}} b_i a_j \Big) X^k = (g \odot f)(X),$$

pois em $\mathbb{K}$, temos $a_i b_j = b_j a_i$, para quaisquer i e j.

2.1. Associatividade da adição: Podemos supor que $n = m = l$, após reescrever $f(X)$, $g(X)$ e $h(X)$ com as mesmas potências de X:

$$\begin{aligned}
((f \oplus g) \oplus h)(X) &\overset{(1)}{=} \sum_{k=0}^{n} (a_k + b_k) X^k \oplus \sum_{k=0}^{n} c_k X^k \\
&\overset{(2)}{=} \sum_{k=0}^{n} \Big((a_k + b_k) + c_k \Big) X^k \\
&\overset{(3)}{=} \sum_{k=0}^{n} \Big(a_k + (b_k + c_k) \Big) X^k \\
&\overset{(4)}{=} \sum_{k=0}^{n} a_k X^k \oplus \sum_{k=0}^{n} (b_k + c_k) X^k \\
&\overset{(5)}{=} (f \oplus (g \oplus h))(X),
\end{aligned}$$

onde, nas igualdades (1) e (2) usamos a definição da adição em $\mathbb{K}[X]$; na igualdade (3) usamos a associatividade da adição em $\mathbb{K}$; e, nas igualdades (4) e (5) usamos, novamente, a definição de adição em $\mathbb{K}[X]$.

2.2. Associatividade da multiplicação: Podemos supor que $n = m = l$, após reescrever

$f(X)$, $g(X)$ e $h(X)$ com as mesmas potências de X:

$$\begin{aligned}
((f \odot g) \odot h)(X) &\overset{(1)}{=} \sum_{k=0}^{n+m} \Big(\sum_{\substack{h+i=k \\ h,i \geqslant 0}} a_h b_i \Big) X^k \odot \sum_{k=0}^{l} c_k X^k \\
&\overset{(2)}{=} \sum_{k=0}^{n+m+l} \left[\sum_{s=0}^{k} \left(\sum_{\substack{h+i=s \\ h,i \geqslant 0}} a_h b_i \right) c_{k-s} \right] X^k \\
&\overset{(3)}{=} \sum_{k=0}^{n+m+l} \left(\sum_{\substack{i+j+h=k \\ h,i,j \geqslant 0}} a_h b_i c_j \right) X^k \\
&\overset{(4)}{=} \sum_{k=0}^{n+m+l} \left[\sum_{s=0}^{k} \left(\sum_{\substack{i+j=s \\ i,j \geqslant 0}} b_i c_j \right) a_{k-s} \right] X^k \\
&\overset{(5)}{=} \sum_{k=0}^{n+m} \Big(\sum_{\substack{i+j=k \\ i,j \geqslant 0}} b_i c_j \Big) X^k \odot \sum_{k=0}^{l} a_k X^k \\
&\overset{(6)}{=} ((g \odot h) \odot f)(X) \\
&\overset{(7)}{=} ((f \odot g) \odot h)(X),
\end{aligned}$$

onde, nas igualdades (1) e (2) usamos a definição da multiplicação em $\mathbb{K}[X]$; nas igualdades (3) e (4) usamos a distributividade em $\mathbb{K}$; nas igualdades (5) e (6) usamos, novamente, a definição da multiplicação em $\mathbb{K}[X]$ e na igualdade (7) usamos a comutatividade da multiplicação em $\mathbb{K}[X]$.

3. Distributividade: Podemos supor $l = m$, após reescrever $g(X)$ e $h(X)$ com as mesmas potências de X:

$$\begin{aligned}
((f \odot (g \oplus h))(X) &\overset{(1)}{=} \Big(\sum_{k=0}^{n} a_k X^k \Big) \odot \Big(\sum_{k=0}^{m} (b_k + c_k) X^k \Big) \\
&\overset{(2)}{=} \sum_{k=0}^{n+m} \Big(\sum_{\substack{i+j=k \\ i,j \geq 0}} a_i (b_j + c_j) \Big) X^k \\
&\overset{(3)}{=} \sum_{k=0}^{n+m} \Big(\sum_{\substack{i+j=k \\ i,j \geq 0}} a_i b_j + a_i c_j) \Big) X^k \\
&\overset{(4)}{=} \sum_{k=0}^{n+m} \Big(\sum_{\substack{i+j=k \\ i,j \geq 0}} a_i b_j \Big) X^k \oplus \sum_{k=0}^{n+m} \Big(\sum_{\substack{i+j=k \\ i,j \geq 0}} a_i c_j \Big) X^k \\
&\overset{(5)}{=} ((f \odot g \oplus f \odot h))(X),
\end{aligned}$$

onde, na igualdade (1) usamos a definição da adição em $\mathbb{K}[X]$; na igualdade (2) usamos a definição da multiplicação em $\mathbb{K}[X]$; na igualdade (3)usamos a distributividade em $\mathbb{K}$; na igualdade (4), a definição da adição em $\mathbb{K}[X]$; e, na igualdade (5) usamos, novamente, a definição da multiplicação em $\mathbb{K}[X]$. □

Exemplo 2.9. Considere os polinômios de coeficientes reais $f(X) = 1 - 2X + \sqrt{3}X^2$ e $g(X) = 3X - 2X^2$. Então

$$(f \oplus g)(X) = 1 + X + (\sqrt{3} - 2)X^2$$

e

$$\begin{aligned}(f \odot g)(X) &= (1 - 2X + \sqrt{3}X^2) \odot (3X - 2X^2) \\ &= [1 \odot (3X - 2X^2)] \oplus [-2X \odot (3X - 2X^2)] \oplus [\sqrt{3}X^2 \odot (3X - 2X^2)] \\ &= (3X - 2X^2) \oplus (-6X^2 + 4X^3) \oplus (3\sqrt{3}X^3 - 2\sqrt{3}X^4) \\ &= 3X - 8X^2 + (4 + 3\sqrt{3})X^3 - 2\sqrt{3}X^4.\end{aligned}$$

Observação 2.10. Denotaremos, a partir de agora, as operações de adição e multiplicação de polinômios simplesmente por $+$ e $\cdot$. Assim, sempre que adicionarmos dois polinômios, os sinais $+$ representarão duas operações diferentes: a adição de elementos de $\mathbb{K}$, efetuada sobre os coeficientes dos polinômios em questão, e a adição de elementos de $\mathbb{K}[X]$. O contexto sempre deixará claro a qual operação o sinal $+$ se refere. Observe, ainda, que um comentário análogo é válido para o sinal $\cdot$ de multiplicação.

Observação 2.11. Todas as definições acima podem ser estendidas para incluir polinômios de coeficientes inteiros. De agora em diante, sempre que necessário, denotaremos o conjunto de tais polinômios por $\mathbb{Z}[X]$.

Seja 0 o polinômio identicamente nulo. Então, $f + 0 = 0 + f = f$ para todo $f \in \mathbb{K}[X]$, o que significa que o polinômio identicamente nulo é o **elemento neutro** da adição de polinômios. Além disso, dado $f \in \mathbb{K}[X]$, exite um único polinômio $g \in \mathbb{K}[X]$ tal que $f + g = g + f = 0$. De fato, sendo $f(X) = a_0 + a_1X + a_2X^2 + \cdots$, é imediato que

$$g(X) = -a_0 - a_1X - a_2X^2 - \cdots$$

é esse único polinômio. De agora em diante, denotaremos esse polinômio por $-f$. Desse modo,

$$(-f)(X) = -a_0 - a_1X - a_2X^2 - \cdots$$

e, para $f, g \in \mathbb{K}[X]$, é possível definir a diferença $f - g$ entre f e g por $f - g = f + (-g)$.

Sendo $\alpha \in \mathbb{K}$ e $g(X) = b_0 + b_1X + b_2X^2 + \cdots \in \mathbb{K}[X]$, é imediata a verificação de que

$$\alpha \cdot g(X) = \alpha b_0 + \alpha b_1X + \alpha b_2X^2 + \cdots ;$$

em particular, temos $1 \cdot g = g$ para todo $g \in \mathbb{K}[X]$, de maneira que o polinômio constante 1 é o elemento neutro da multiplicação de polinômios.

De agora em diante, para denotar o produto $f \cdot g$, de $f, g \in \mathbb{K}[X]$, escreveremos simplesmente fg, sempre que não houver perigo de confusão. Em particular, se $\alpha \in \mathbb{K}$, escreveremos αf para denotar o produto de α e f, onde α é compreendido como um polinômio constante.

Definição 2.12. Se $f(X) = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{K}[X] \setminus \{0\}$, com $a_n \neq 0$, dizemos que o inteiro não negativo n é o **grau** de f, e denotamos $\partial f = n$ (lê-se "o grau de f é igual a n").

Observe que o grau não está definido para o polinômio identicamente nulo; por outro lado, $\partial f = 0$ para todo polinômio constante $f(X) = \alpha$, com $\alpha \in \mathbb{K} \setminus \{0\}$. De agora em diante, sempre que nos referirmos a $f \in \mathbb{K}[X] \setminus \{0\}$ escrevendo

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

suporemos, salvo menção em contrário, que $a_n \neq 0$. Nesse caso, diremos que a_n é o **coeficiente** líder de f. Além disso, diremos que f é **mônico** quando tiver coeficiente líder 1.

O item (b) da proposição a seguir é conhecido como **propriedade multiplicativa do grau**.

Proposição 2.13. *Para $f, g \in \mathbb{K}[X] \setminus \{0\}$, temos:*

(a) $\partial(f+g) \leqslant \max\{\partial f, \partial g\}$ *se* $f + g \neq 0$.

(b) $fg \neq 0$ *e* $\partial(fg) = \partial f + \partial g$.

Demonstração. Sejam $\partial f = n$ e $\partial g = m$, com $f(X) = a_0 + a_1 X + \cdots + a_n X^n$ e $g(X) = b_0 + b_1 X + \cdots + b_m X^m$.

(a) Se $m \neq n$, podemos supor, sem perda de generalidade, que $m > n$. Então

$$(f+g)(X) = (a_0 + b_0) + \cdots + (a_n + b_n)X^n + b_{n+1}X_{n+1} + \cdots + b_m X^m,$$

de forma que $\partial(f+g) = m = \max\{\partial f, \partial g\}$. Se $m = n$ mas $f + g \neq 0$, então

$$(f+g)(X) = (a_0 + b_0) + \cdots + (a_n + b_n)X^n$$

e há duas possibilidades: $a_n + b_n = 0$ ou $a_n + b_n \neq 0$. No primeiro caso, $\partial(f+g) < n = \max\{\partial f, \partial g\}$. No segundo, $\partial(f+g) = n = \max\{\partial f, \partial g\}$. Em qualquer caso, ainda teremos $\partial(f+g) \leqslant \max\{\partial f, \partial g\}$.

(b) Seja $fg = c_0 + c_1 X + c_2 X^2 + \cdots$. Se $k > m + n$, vimos, na prova do Lema 2.6, que $c_k = 0$. Portanto, se mostrarmos que $c_{m+n} \neq 0$ seguirá que $fg \neq 0$ e $\partial(fg) = m + n = \partial f + \partial g$. Mas, como $a_i = 0$ para $i > n$ e $b_j = 0$ para $j > m$, é imediato que

$$c_{m+n} = \sum_{\substack{i+j=m+n \\ i,j \geq 0}} a_i b_j = a_n b_m \neq 0.$$

□

2.2 Divisão euclidiana

Nesta seção apresentamos o conceito de divisibilidade em $\mathbb{K}[X]$ e mostramos que é possível fazer **de modo único** uma divisão com **resto controlado** em $\mathbb{K}[X]$.

Definição 2.14. Sejam $f, g \in \mathbb{K}[X]$. Quando existe $h \in \mathbb{K}[X]$ tal que $f = gh$, dizemos que f é múltiplo de g. Nesse caso, se $g \neq 0$, dizemos que g divide f.

Exemplo 2.15. Tanto $X^2 - 2X + 2$ como $X^2 + 2X + 2$ dividem $X^4 + 4$ em $\mathbb{Z}[X]$, pois $X^4 + 4 = (X^2 - 2X + 2)(X^2 + 2X + 2)$.

O seguinte resultado é uma consequência da Proposição 2.13 item (b) (propriedade multiplicativa do grau) em $\mathbb{K}[X]$.

Proposição 2.16. *Dados $f, g \in \mathbb{K}[X] \setminus \{0\}$, se g divide f, então $\partial g \leqslant \partial f$.*

Demonstração. Como g divide f e ambos são não nulos, então existe $h \in \mathbb{K} \setminus \{0\}$ tal que $f = gh$. Pelo item (b) da Proposição 2.13, temos

$$\partial f = \partial gh = \partial g + \partial h \geqslant \partial g.$$

□

Apresentamos, na proposição seguinte, a divisão em $\mathbb{K}[X]$, conhecida como **divisão euclidiana**.

Proposição 2.17. *Se $f, g \in \mathbb{K}[X]$, com $g \neq 0$, então existem únicos $q, r \in \mathbb{K}[X]$ tais que*

$$f = gq + r, \text{ com } r = 0 \text{ ou } 0 \leqslant \partial r < \partial g.$$

Demonstração. Seja $g(X) = b_0 + b_1X + \cdots + b_mX^m$, onde b_m tem inverso $b_m^{-1} \in \mathbb{K}$.

Existência: Se $f(X) = 0$, então considere $q(X) = r(X) = 0$. Suponhamos que $f(X) \neq 0$. Seja $n = \partial f$ e escreva $f(X) = a_0 + a_1X + \cdots + a_nX^n$, com $a_n \neq 0$.

Se $n < m$, então considere $q(X) = 0$ e $r(X) = f(X)$.

Podemos supor $n \geqslant m$. A demonstração é por indução sobre $n = \partial f$. Se $n = 0$, então $0 = n \geqslant m = \partial g$, logo $m = 0$, $f(X) = a_0 \neq 0$, $g(X) = b_0$, com $b_0^{-1} \in \mathbb{K}$. Assim, $f(X) = a_0b_0^{-1}g$, com $q(X) = a_0b_0^{-1}$ e $r(X) = 0$.

Suponhamos o resultado válido para polinômios com grau menor do que $n = \partial f$. Vamos mostrar que vale para f.

Seja $f_1(X)$ o polinômio definido por $f_1(X) = f(X) - a_nb_m^{-1}X^{n-m}g(X)$. O polinômio $a_nb_m^{-1}X^{n-m}g(X)$ tem grau n e coeficiente líder a_n. Logo, $\partial f_1 < \partial f$. Por hipótese de indução, existem $q_1, r_1 \in \mathbb{K}[X]$ tais que

$$f_1 = q_1g + r_1,$$

onde $r_1 = 0$ ou $\partial r_1 < \partial g$. Logo,

$$\begin{aligned} f(X) &= f_1(X) + a_nb_m^{-1}X^{m-n}g(X) \\ &\overset{(1)}{=} \Big(q_1(X)g(X) + r_1(X)\Big) + a_nb_m^{-1}X^{m-n}g(X) \\ &\overset{(2)}{=} \Big(q_1(X) + a_nb_m^{-1}X^{m-n}\Big)g(X) + r_1(X). \end{aligned}$$

onde, em (1), substituímos a expressão de $f_1(X)$ e, em (2), usamos a comutatividade da adição e a distributividade em $\mathbb{K}[X]$.

Escrevemos $q(X) = q_1(X) + a_nb_m^{-1}x^{m-n}$ e $r(X) = r_1(X)$.

Unicidade: Sejam q_1, r_1, q_2, r_2 tais que

$$f(X) = q_1(X)g(X) + r_1(X) \overset{(3)}{=} q_2(X)g(X) + r_2(X), \text{onde}$$

$$(4) \begin{cases} r_1(X) = 0 \quad \text{ou} \quad \partial r_1 < \partial g \text{ e} \\ r_2(X) = 0 \quad \text{ou} \quad \partial r_2 < \partial g. \end{cases}$$

De (3), segue que $\Big(q_1(X) - q_2(X)\Big)g(X) = r_2(X) - r_1(X)$.

Se $q_1 \neq q_2$, então $q_1(X) - q_2(X) \neq 0$, assim, $r_2(X) - r_1(X) \neq 0$ e, da Proposição 2.16 e do item (a) da Proposição 2.13, obtemos

$$\partial g \leqslant \partial(r_2 - r_1) \leqslant \max\{\partial r_1, \partial r_2\} \overset{(4)}{<} \partial g,$$

uma contradição. Portanto, $q_1 = q_2$ e, consequentemente, $r_1 = r_2$. □

Definição 2.18. Sejam f, g, q e r como na Proposição 2.17. Chamamos f de **dividendo**, g de **divisor**, q de **quociente** e r de **resto**. Além disso, se $r = 0$, dizemos que f é divisível por g ou, o que é o mesmo, que g divide f, e denotamos por $g \mid f$.

Observação 2.19. Na Proposição 2.16 e Proposição 2.17, se considerarmos que g tem coeficiente líder invertível então a divisão euclidiana é válida em $\mathbb{A}[X]$, onde $\mathbb{A}$ é um anel. Lembramos que no anel $\mathbb{Z}$ os únicos elementos que têm inverso são 1 e -1. Em $\mathbb{K}$, todo elemento não nulo tem inverso.

2.3 Raízes de polinômios

Até este ponto, em nosso trabalho, temos considerado polinômios como expressões formais com as quais aprendemos a operar sem, no entanto, atribuir a **indeterminada** X um significado aritmético.

A partir desta seção, passamos a considerar a indeterminada X de um ponto de vista aritmético, apresentando o conceito de raiz de um polinômio e de função polinomial associada a um polinômio.

Definição 2.20. Para $f(X) = a_nX^n + \cdots + a_1X + a_0 \in \mathbb{K}[X]$, a **função polinomial** associada a f é a função $\widetilde{f}\colon \mathbb{K} \to \mathbb{K}$ dada, para $x \in \mathbb{K}$ por

$$\widetilde{f}(x) = a_nx^n + \cdots + a_1x + a_0.$$

Quando $f(X) = c$, observe que a função polinomial associada $\widetilde{f}$ será a função constante $\widetilde{f} = c$, para todo $x \in \mathbb{K}$, justificando o nome *constante* imputado anteriormente a um polinômio de grau 0.

Definição 2.21. Seja $f \in \mathbb{K}[X]$ um polinômio, com função polinomial associada $\widetilde{f}\colon \mathbb{K} \to \mathbb{K}$. Um elemento $\alpha \in \mathbb{K}$ é uma raiz de f se $\widetilde{f}(\alpha) = 0$.

Exemplo 2.22. Seja $f(X) = X - 5 \in \mathbb{C}[X]$. É fácil verificar que $x = 5$ é a única raiz de f em $\mathbb{C}$. De fato, a função polinomial associada a f é

$$\begin{aligned} \widetilde{f}\colon \mathbb{C} &\to \mathbb{C} \\ x &\mapsto x - 5 \end{aligned}$$

logo, $\widetilde{f}(x) = 0$ se, e somente se, $x = 5$.

O item (a) da Proposição 2.23 é conhecida como o **teste da raiz**.

Proposição 2.23. *Se $f \in \mathbb{K}[X] \setminus \{0\}$ e $\alpha \in \mathbb{K}$, então:*

(a) α é raiz de f se, e só se, $(X - \alpha) \mid f(X)$ em $\mathbb{K}[X]$.

(b) Se α for raiz de f, então existe um maior inteiro positivo m tal que $(X-\alpha)^m$ divide f. Ademais, sendo $f(X) = (X-\alpha)^m q(X)$, com $q \in \mathbb{K}[X]$, tem-se $\widetilde{q}(\alpha) \neq 0$, onde $\widetilde{q}\colon \mathbb{K} \to \mathbb{K}$ é a função polinomial associada a q.

(c) Se $\alpha_1, \ldots, \alpha_k$ forem raízes duas a duas distintas de f, então o polinômio $(X-\alpha_1)\cdots(X-\alpha_k)$ divide $f(X)$ em $\mathbb{K}[X]$.

Demonstração. (a) Segue da Proposição 2.17 (divisão euclidiana) a existência de polinômios $q, r \in \mathbb{K}[X]$ tais que

$$f(X) = (X-\alpha)q(X) + r(X),$$

com $r = 0$ ou $0 \leq \partial r < \partial(X-\alpha) = 1$. Portanto, $r(X) = c$, um polinômio constante. Por outro lado, sendo $\widetilde{f}$ e $\widetilde{q}$ as funções polinomiais respectivamente associadas a f e q, segue da igualdade acima que

$$\widetilde{f}(\alpha) = (\alpha-\alpha)\widetilde{q}(\alpha) + c = c,$$

ou seja, $f(X) = (X-\alpha)q(X) + \widetilde{f}(\alpha)$. Assim,

$$\alpha \text{ é raiz de } f \Leftrightarrow \widetilde{f}(\alpha) = 0 \Leftrightarrow f(X) = (X-\alpha)q(X).$$

(b) Se $m > \partial f$, então $(X-\alpha)^m$ não divide $f(X)$, uma vez que $\partial(X-\alpha)^m = m > \partial f$. Daí e do item *(a)*, existe um maior inteiro positivo m tal que $(X-\alpha)^m \mid f(X)$, digamos $f(X) = (X-\alpha)^m q(X)$. Passando para funções polinomiais, obtemos, a partir daí, a igualdade

$$\widetilde{f}(x) = (x-\alpha)^m \widetilde{q}(x), \forall x \in \mathbb{K};$$

se $\widetilde{q}(\alpha) = 0$, seguiria de *(a)* que $q(X) = (X-\alpha)q_1(X)$, para algum polinômio $q_1 \in \mathbb{K}[X]$. Mas aí, teríamos

$$f(X) = (X-\alpha)^{m+1} q_1(X),$$

contrariando a maximalidade de m.

(c) Façamos a prova deste item para o caso $k = 2$ (a prova do caso geral é inteiramente análoga). Como α_1 é raiz de f, pelo item *(a)* existe um polinômio $g \in \mathbb{K}[X]$ tal que $f(X) = (X-\alpha_1)g(X)$. Seja $\widetilde{g}$ a função polinomial associada ao polinômio g. Como $\alpha_1 \neq \alpha_2$ e α_2 também é raiz de f, segue da última igualdade que

$$0 = \widetilde{f}(\alpha_2) = (\alpha_2 - \alpha_1)\widetilde{g}(\alpha_2),$$

e α_2 é raiz de g. Daí, novamente pelo item *(a)*, existe um polinômio $h \in \mathbb{K}[X]$ tal que $g(X) = (X-\alpha_2)h(X)$ e, assim,

$$f(X) = (X-\alpha_1)(X-\alpha_2)h(X).$$

□

Se $f(X) = (X-\alpha)^m q(X)$, com $\widetilde{q}(\alpha) \neq 0$ como na Proposição 2.23. Chamamos m de a **multiplicidade** de α como raiz de f. Em particular, se $m = 1$, α é uma raiz **simples** de f, já se $m > 1$, α é uma raiz **múltipla** de f.

Exemplo 2.24. Sendo $f(X) = X^3 - 3X + 2$ um polinômio de coeficientes reais, temos que 1 é raiz dupla e -2 é raiz simples de f, uma vez que $f(X) = (X-1)^2(X-(-2))$.

Uma consequência importante do teste da raiz e que esta explicitada no corolário seguinte é que o número de raízes de um polinômio não identicamente nulo não pode exceder seu grau. Observe que consideramos a multiplicidade das raízes.

Corolário 2.25. *Se $f \in \mathbb{K}[X] \setminus \{0\}$, então f possui no máximo ∂f raízes em $\mathbb{K}$, contadas de acordo com suas multiplicidades.*

Demonstração. Façamos indução sobre o grau de f. Se $\partial f = 0$, então existe $c \in \mathbb{K} \setminus \{0\}$ tal que $f(X) = c$. Daí, a função polinomial associada $\widetilde{f}$ é a função constante $x \mapsto c$, e segue que o número de raízes de f é 0, igual a seu grau.

Seja, agora, f um polinômio de grau positivo e suponha a afirmação do enunciado válida para todos os polinômios não nulos de graus menores do que ∂f. Se f não tiver raízes em $\mathbb{K}$, nada há nada a fazer. Senão, seja $\alpha \in \mathbb{K}$ uma raiz de f e (de acordo com a Proposição 2.23) m o maior natural tal que $f(X) = (X-\alpha)^m q(X)$, para algum polinômio $q \in \mathbb{K}[X]$. Como

$$\partial q = \partial f - m < \partial f,$$

segue da hipótese de indução que q tem no máximo ∂q raízes em $\mathbb{K}$, contadas de acordo com suas multiplicidades. Agora, se $\beta \neq \alpha$ é raiz de f, temos

$$0 = \widetilde{f}(\beta) = (\beta - \alpha)^m \widetilde{q}(\beta)$$

e, daí, β é raiz de q. Portanto, o número máximo de raízes de f é igual a m (a multiplicidade de α) mais o número de raízes de q, e segue, por hipótese de indução, que f possui no máximo

$$m + \partial q = \partial f$$

raízes em $\mathbb{K}$. □

Utilizamos frequentemente o corolário acima em uma das formas a seguir.

Corolário 2.26. *Se $f(X) = a_n X^n + \cdots + a_1 X + a_0 \in \mathbb{K}[X]$ admite pelo menos $n+1$ raízes distintas em $\mathbb{K}$, então f é identicamente nulo, ou seja, $a_n = \cdots = a_0 = 0$.*

Demonstração. Se $f \in \mathbb{K}[X] \setminus \{0\}$, então, pelo Corolário 2.25, f teria no máximo n raízes em $\mathbb{K}$. □

Corolário 2.27. *Sejam $f(X) = a_n X^n + \cdots + a_1 X + a_0$ e $g(X) = b_m X^m + \cdots + b_1 X + b_0$ polinômios sobre $\mathbb{K}$, com $m \geqslant n$. Se $\widetilde{f}(x) = \widetilde{g}(x)$ para ao menos $m+1$ valores distintos $x \in \mathbb{K}$, então $f = g$, ou seja, $m = n$ e $a_i = b_i$, para $0 \leqslant i \leqslant n$.*

Demonstração. Basta aplicar o Corolário 2.26 ao polinômio $f - g$, notando que a função polinomial associada a tal polinômio é $\widetilde{f} - \widetilde{g}$. □

Considere a aplicação

$$\begin{array}{ccc} \mathbb{K}[X] & \to & \Phi \\ f & \mapsto & \widetilde{f} \end{array}, \tag{2.1}$$

onde Φ é o conjunto das funções de $\mathbb{K}$ em $\mathbb{K}$. O Corolário 2.27 garante que a aplicação (2.1) é injetiva, ou seja, se $f, g \in \mathbb{K}[X]$ e $\widetilde{f}, \widetilde{g} \in \Phi$, então $\widetilde{f} = \widetilde{g} \Rightarrow f = g$.

Por esse motivo, de agora em diante, quando quisermos nos referir quer seja a um polinômio sobre $\mathbb{K}$, quer seja à função polinomial associada a esse polinômio, escreveremos apenas f. De modo particular, ao escrevermos $f(X)$, estaremos fazendo referência ao polinômio f; ao escrevermos $f(x)$, estaremos fazendo referência ao elemento de $\mathbb{K}$, imagem de $x \in \mathbb{K}$ pela função polinomial associada ao polinômio f. Em qualquer caso, o contexto deixará claro a que estamos nos referindo.

Observação 2.28. O Corolário 2.27 garante que os coeficientes de um polinômio $f \in \mathbb{K}[X]$ são determinados pelos valores $f(x)$, com $x \in \mathbb{K}$.

2.4 O Teorema Fundamental da Álgebra

Uma consequência do Corolário 2.25 é que todo polinômio de coeficientes complexos e grau n possui no máximo n raízes complexas. No entanto, o polinômio $f(X) = X^2 - 5 \in \mathbb{Q}[X]$ tem coeficientes racionais mas não possui raízes racionais; semelhantemente, o polinômio $g(X) = X^2 + 3 \in \mathbb{R}[X]$ tem coeficientes reais mas não possui raízes reais. Isso ocorre, devido ao fato de que em $\mathbb{Q}$ ou $\mathbb{R}$ não é possível realizarmos certas extrações de raízes. Diferentemente do que ocorre nesses conjuntos, todo polinômio sobre $\mathbb{C}$ possui raízes também em $\mathbb{C}$. Esse fato é conhecido na literatura como o **teorema fundamental da álgebra**. Para a sua demonstração é necessário utilizar dois lemas, que apresentamos a seguir.

Lema 2.29. *Dado um polinômio $f \in \mathbb{C}[X] \setminus \mathbb{C}$, existe $z_0 \in \mathbb{C}$ tal que*

$$|f(z_0)| \leqslant |f(z)|, \ \forall z \in \mathbb{C}.$$

Demonstração. Basta provar o resultado para polinômios mônicos. Por comodidade de notação, escrevamos $f(z) = a_n z^n + \cdots + a_1 z + a_0$ para denotar a função polinomial associada a f. Pelas desigualdades triangulares [16, p. 15-16], temos para todo $z \in \mathbb{C}$,

$$|f(z)| = |z|^n \left|1 + \frac{a_{n-1}}{z} + \frac{a_{n-2}}{z^2} + \cdots + \frac{a_0}{z^n}\right| \geqslant |z|^n \left(1 - \frac{|a_{n-1}|}{|z|} - \frac{|a_{n-2}|}{|z|^2} - \cdots - \frac{|a_0|}{|z|^n}\right),$$

mostrando que

$$\lim_{|z| \to +\infty} |f(z)| = +\infty.$$

Assim, existe $R > 0$, tal que $|f(z)| > |f(0)|$ para todo z com $|z| > R$. Se $D_f = \{z \in \mathbb{C}; |z| \leqslant R\}$, pelo Teorema de Weierstrass [18, p. 19], temos a existência de $z_0 \in D_f$, tal que $|f(z_0)| \leq |f(z)|$ para todo $z \in D_f$. Como $|f(z_0)| \leq |f(0)|$, temos que $|f(z_0)| \leq |f(z)|$ para todo $z \in \mathbb{C}$. □

Lema 2.30. *Seja $f \in \mathbb{C}[X] \setminus \mathbb{C}$. Se $z_0 \in \mathbb{C}$ é tal que $f(z_0) \neq 0$, então existe $z_1 \in \mathbb{C}$ tal que $|f(z_1)| < |f(z_0)|$.*

Demonstração. Também aqui basta provar o resultado para polinômios mônicos. Seja $f(x) = x + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ e sejam z_0 e h números complexos tais que $f(z_0) \neq 0$ e h a ser determinado de modo que $|f(z_0 + h)| < |f(z_0)|$.

Com o auxílio do binômio de Newton, podemos escrever

$$f(z_0 + h) = (z_0 + h)^n + a_{n-1}(z_0 + h)^{n-1} + \cdots + a_0 = f(z_0) + q(h),$$

onde q é um polinômio não identicamente nulo, pois f é um polinômio não constante, de grau n e sem termo constante. Seja bx^n o termo de menor grau em q. Assim, podemos escrever $q(x) = bx^n + x^{m+1}r(x)$, onde r é um outro polinômio.

Podemos escolher o argumento de h de modo que $\lambda = \frac{bh}{f(z_0)}$ tenha argumento igual a π (lembre que $f(z_0) \neq 0$). Portanto, λ é um número real negativo. Podemos garantir que a desigualdade $-1 \leq \lambda \leq 0$ se mantém para $|h|$ suficientemente pequeno. Escolhemos, ainda, $|h|$ suficientemente pequeno para que $|h^{m+1}r(h)| < |bh^m|$. Pela desigualdade triangular [16, p. 15], para todo $h \in \mathbb{C}$, nas condições acima, temos que

$$\begin{aligned} |f(z_0+h)| &= |f(z_0)| + bh^m + h^{m+1}r(h)| \\ &\leqslant |f(z_0) + bh^m| + |h^{m+1}r(h)| \\ &\overset{(1)}{=} |f(z_0)| - |bh^m| + |h^{m+1}r(h)| \\ &< |f(z_0)|. \end{aligned}$$

Portanto, existe $z_1 = z_0 + h$, com h como acima, tal que $|f(z_1)| < |f(z_0)|$.

Observamos que na igualdade (1) usamos o seguinte resultado, que pode ser encontrado em [16, p. 18]: Dados $z, w \in \mathbb{C}$ e $t \in \mathbb{R}$, então, $|z+w| = |z| - |w|$ se, e somente se, $w = tz$, $-1 \leqslant t \leqslant 0$. □

Munidos do Lema 2.29 e Lema 2.30 estamos em condições de enunciar e demonstrar o **Teorema Fundamental da Álgebra**.

Teorema 2.31 (Teorema Fundamental da Álgebra)**.** *Todo polinômio $f \in \mathbb{C}[X] \setminus \mathbb{C}$ possui ao menos uma raiz complexa.*

Demonstração. Seja $f \in \mathbb{C}[X] \setminus \mathbb{C}$. Pelo Lema 2.29, temos a existência de $z_0 \in \mathbb{C}$ tal que $|f(z_0)| \leq |f(z)|$ para todo $z \in \mathbb{C}$. Se $f(z_0) \neq 0$,então, pelo Lema 2.30, existe $z_1 \in \mathbb{C}$ tal que $|f(z_1)| < |f(z_0)|$, o que é um absurdo. Portanto, $f(z_0) = 0$. □

O Corolário 2.32 fornece uma consequência imediata do Teorema Fundamental da Álgebra.

Corolário 2.32. *Se $f(X) = a_nX^n + \cdots + a_1X + a_0$ é um polinômio de coeficientes complexos e grau $n \geqslant 1$, então existem n números complexos $z_1, \ldots, z_n$ tais que*

$$f(X) = a_n(X - z_1)\ldots(X - z_n).$$

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

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

Se $z_1 \in \mathbb{C}$ é uma raiz de f, o teste da raiz garante a existência de um polinômio g, também de coeficientes complexos, tal que $f(X) = (X - z_1)g(X)$. Observe que g 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 $g(X) = a_n(X - z_2)\ldots(X - z_n)$. Logo, $f(X) = (X - z_1)g(X) = a_n(X - z_2)\ldots(X - z_n)$ e nada mais há a fazer. □

Exemplo 2.33. Dado $f(X) = X^2 + 1$, os números $-i, i \in \mathbb{C}$ são tais que $(X + i)(X - i) = X(X - i) + i(X - i) = X^2 - iX + iX - i^2 = X^2 + 1 = f(X)$. Logo, $f(X) = (X + i)(X - i)$ é a forma fatorada de f para $z_1 = -i$ e $z_2 = i$.

Retornando ao caso geral, seja $f(X) = a_n X\, n + \cdots + a_1 X + a_0$ um polinômio não nulo sobre $\mathbb{K}$. Se existirem elementos $\alpha_1, \ldots, \alpha_n \in \mathbb{K}$ para os quais

$$f(X) = a_n(X - \alpha_1) \ldots (X - \alpha_m)$$

também diremos que tal expressão é a **forma fatorada** de f sobre $\mathbb{K}$.

Considerando que alguns dos α_j podem se repetir, depois de reordená-los, se necessário, e considerando apenas os α_j distintos, podemos concluir que existem $1 \leqslant m \leqslant n$ e $k_1, \ldots, k_m$ inteiros positivos tais que

$$f(X) = a_n(X - \alpha_1)^{k_1} \ldots (X - \alpha_m)^{k_m},$$

com $k_1 + \cdots + k_m = n$ e $\alpha_1, \ldots, \alpha_m$ elementos dois a dois distintos de $\mathbb{K}$.

Exemplo 2.34. A forma fatorada de $f(X) = X^6 - 8X^5 + 25X^4 - 38X^3 + 28X^2 - 8X$ é $f(X) = (X-0)(X-1)(X-1)(X-2)(X-2)(X-2) = X(X-1)(X-1)(X-2)(X-2)(X-2)$. Considerando $k_1 = 1$, $k_2 = 2$ e $k_3 = 3$ e, $\alpha_1 = 0$, $\alpha_2 = 1$ e $\alpha_3 = 2$ podemos escrever $f(X) = X(X-1)^2(X-2)^3$.

2.5 Relações entre coeficientes e raízes

Nesta seção apresentamos importantes relações entre as raízes de um polinômio em uma indeterminada, comumente chamadas de *relações entre coeficientes e raízes* de um polinômio.

2.5.1 Polinômios em várias indeterminadas

Fixado $n \in \mathbb{N}$, um **polinômio f a n indeterminadas** sobre $\mathbb{K}$ é uma soma de termos

$$a_{i_1 \ldots i_n} X_1^{i_1} \ldots X_n^{i_n},$$

denominados **monômios**, onde $a_{i_1 \ldots i_n} \in \mathbb{K}$ e $i_1, \ldots, i_n$ variam em $\mathbb{Z}_+$, sendo $a_{i_1 \ldots i_n} = 0$ para quase todas (ou seja, para todas, exceto um número finito de) sequências $(i_1, \ldots, i_n)$ de inteiros não negativos. Nesse caso escrevemos

$$f = f(X_1, X_2, \ldots, X_n) = \sum_{i_1, \ldots, i_n \geq 0} a_{i_1 \ldots i_n} X_1^{i_1} \ldots X_n^{i_n}.$$

O **grau** de um polinômio f como acima é o maior valor possível para a soma $i_1 + \cdots + i_n$, tal que $a_{i_1 \ldots i_n} \neq 0$.

Denotamos por $\mathbb{K}[X_1, \ldots, X_n]$ o conjunto dos polinômios a n indeterminadas sobre $\mathbb{K}$. Sobre tal conjunto definimos, de maneira óbvia, operações

$$+ \colon \mathbb{K}[X_1, \ldots, X_n] \times \mathbb{K}[X_1, \ldots, X_n] \to \mathbb{K}[X_1, \ldots, X_n]$$

e

$$\cdot \colon \mathbb{K}[X_1, \ldots, X_n] \times \mathbb{K}[X_1, \ldots, X_n] \to \mathbb{K}[X_1, \ldots, X_n],$$

respectivamente denominadas **adição** e **multiplicação**, as quais se reduzem às operações de adição e multiplicação sobre $\mathbb{K}[X]$ quando $n = 1$ e continuam gozando das mesmas propriedades dessas operações. Por exemplo, se $f(X_1, X_2) = X_1^2 + X_1 X_2 + X_2^3$ e $g(X_1, X_2) = X_1^3 - \sqrt{2} X_1 X_2$, então

$$f(X_1, X_2) + g(X_1, X_2) = X_1^2 + (1 - \sqrt{2}) X_1 X_2 + X_1^3 + X_2^3$$

e

$$f(X_1, X_2) \cdot g(X_1, X_2) = X_1^5 - \sqrt{2}X_1^3X_2 + X_1^4X_2 - \sqrt{2}X_1^2X_2^2 + X_1^3X_2^3 - \sqrt{2}X_1X_2^4.$$

Dado $f \in \mathbb{K}[X_1, \ldots, X_n]$, podemos considerar f como um polinômio em X_i, com coeficientes em $\mathbb{K}[X_1, \ldots, \widehat{X_i}, \ldots, X_n]$, onde usamos o *circunflexo* $\wedge$ sobre X_i para indicar que todas as indeterminadas, menos X_i, estão presentes. Por exemplo, seja

$$f(X_1, X_2, X_3) = X_1^3X_2X_3^4 - X_1^3 - 5X_1X_2 + 10X_1X_2^5X_3^2,$$

um polinômio em $\mathbb{K}[X_1, X_2, X_3]$; escrevendo

$$f(X_1, X_2, X_3) = X_1^3X_2 \cdot X_3^4 + 10X_1X_2^5 \cdot X_3^2 - (X_1^3 + 5X_1X_2),$$

consideramos f como um polinômio em X_3, cujos coeficientes estão em $\mathbb{K}[X_1, X_2]$.

Se $f, g \in \mathbb{K}[X_1, \ldots, X_n]$ são dados por

$$f(X_1, X_2, \ldots, X_n) = \sum_{i_1,\ldots,i_n \geq 0} a_{i_1\ldots i_n} X_1^{i_1} \ldots X_n^{i_n}$$

e

$$g(X_1, X_2, \ldots, X_n) = \sum_{i_1,\ldots,i_n \geq 0} b_{i_1\ldots i_n} X_1^{i_1} \ldots X_n^{i_n},$$

dizemos que f e g são *iguais* quando $a_{i_1\ldots i_n} = b_{i_1\ldots i_n}$, para todas as escolhas possíveis de índices $i_1, \ldots, i_n \in \mathbb{Z}_+$.

Fixados $x_1, x_2, \ldots, x_n \in \mathbb{K}$, definimos o elemento $f(x_1, x_2, \ldots, x_n) \in \mathbb{K}$ por

$$f(x_1, x_2, \ldots, x_n) = \sum_{i_1,\ldots,i_n \geq 0} a_{i_1\ldots i_n} x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}.$$

A proposição a seguir nos dá uma relação entre tais elementos de $\mathbb{K}$ e a noção de igualdade de polinômios em várias indeterminadas.

Proposição 2.35. *Sejam $f, g \in \mathbb{K}[X_1, \ldots, X_n]$. Se $A_1, \ldots, A_n \subset \mathbb{K}$ são conjuntos infinitos, então*

$$f = g \Leftrightarrow f(x_1, x_2, \ldots, x_n) = g(x_1, x_2, \ldots, x_n),$$

para todos $x_1 \in A_1, x_2 \in A_2, \ldots, x_n \in A_n$.

Demonstração. Se $f = g$, é claro que $f(x_1, x_2, \ldots, x_n) = g(x_1, x_2, \ldots, x_n)$, para todos $x_1, x_2, \ldots, x_n \in \mathbb{K}$ e, em particular, para $x_1 \in A_1, x_2 \in A_2, \ldots, x_n \in A_n$.

Reciprocamente, suponhamos que esta última condição seja satisfeita e provemos que $f = g$ usando indução sobre o número n de indeterminadas. Já temos a validade da proposição para $n = 1$, pelo Corolário 2.27. Por hipótese de indução, suponha o resultado válido para polinômios em $n - 1$ indeterminadas e escreva

$$\begin{cases} f(X_1, X_2, \ldots X_n) = \sum_{j=0}^{m} f_j(X_2, \ldots, X_n) X_1^j \\ g(X_1, X_2, \ldots X_n) = \sum_{j=0}^{p} f_j(X_2, \ldots, X_n) X_1^j \end{cases}, \tag{2.2}$$

com $f_i, g_j \in \mathbb{K}[X_2, \ldots, X_n]$ para todos $0 \leq i \leq m$, $0 \leq j \leq p$.

Fixados $x_2 \in A_2, \ldots, x_n \in A_n$, temos por hipótese de indução que

$$f(x_1, x_2, \ldots, x_n) = g(x_1, x_2, \ldots, x_n),$$

para todo $x_1 \in A_1$, ou seja, que

$$\sum_{j=0}^{m} f_j(x_2, \ldots, x_n)x_1^j = \sum_{j=0}^{p} g_j(x_2, \ldots, x_n)x_1^j,$$

para todo $x_1 \in A_1$. Como o conjunto A_1 é infinito, aplicando o Corolário 2.27 aos polinômios

$$f(X_1, x_2, \ldots, x_n) = \sum_{j=0}^{m} f_i(x_2, \ldots, x_n)X_1^j$$

e

$$g(X_1, x_2, \ldots x_n) = \sum_{j=0}^{p} f_j(x_2, \ldots, x_n)X_1^j$$

concluímos que $m = p$ e

$$f_j(x_2, \ldots, x_n) = g_j(x_2, \ldots, x_n) \tag{2.3}$$

para $0 \leq j \leq m$. Mas, como os elementos $x_2 \in A_2, \ldots, x_n \in A_n$ fixados foram escolhidos arbitrariamente, concluímos que (2.3) é válida para todos $x_2 \in A_2, \ldots, x_n \in A_n$. Portanto, pela hipótese de indução segue que $f_j = g_j$ para $0 \leq j \leq m$, e (2.2) garante que $f = g$. □

Observação 2.36. De agora em diante, para polinômios f em duas indeterminadas, escrevemos $f(X, Y)$ em vez de $f(X_1, X_2)$. Semelhantemente, para polinômios f em três indeterminadas, escreveremos $F(X, Y, Z)$ em lugar de $f(X_1, X_2, X_3)$.

2.5.2 Polinômios simétricos

Definição 2.37. Um polinômio $f \in \mathbb{K}[X_1, \ldots X_n]$ é **simétrico** quando

$$f(X_1, X_2, \ldots, X_n) = F(X_{\sigma(1)}, X_{\sigma(2)}, \ldots, X_{\sigma(n)},)$$

para toda permutação σ de I_n.

Exemplo 2.38. Seja $f \in \mathbb{K}[X, Y]$, dado por

$$f(X, Y) = -2X^3 - 2Y^3 - X^2Y^2 - X - Y.$$

Como

$$f(Y, X) = -2Y^3 - 2X^3 - Y^2X^2 - Y - X = f(X, Y),$$

concluímos que f é um polinômio simétrico.

Dentre os polinômios simétricos destacamos os da definição a seguir.

Definição 2.39. Para $0 \leqslant j \leqslant n$, o $j-$ésimo **polinômio simétrico elementar** em $X_1, \ldots, X_n$, denotado por $s_j = s_j(X_1, \ldots, X_n)$, é definido como

$$s_j(X_1, \ldots, X_n) = \begin{cases} 1, & \text{se } j = 0 \\ \sum_{1 \leqslant i_1 < \cdots < i_j \leqslant n} X_{i_1}X_{i_2} \ldots X_{i_j}, & \text{se } 1 \leqslant j \leqslant n \end{cases}.$$

No caso $n = 3$, por exemplo, temos

$$s_0 = 1,\ s_1 = X + Y + Z,\ s_2 = XY + YZ + XZ,\ s_3 = XYZ.$$

Proposição 2.40. *Se* $f(X) = a_nX^n + \cdots + a_1X + a_0 \in \mathbb{K}[X] \setminus \mathbb{K}$ *se fatora completamente sobre* $\mathbb{K}$*, com raízes* $\alpha_1, \ldots, \alpha_n$*, então, para* $1 \leqslant j \leqslant n$*, temos*

$$s_j(\alpha_1, \ldots, \alpha_n) = (-1)^j \frac{a_{n-j}}{a_n}. \tag{2.4}$$

Demonstração. Por simplicidade de notação, denote $s_j(\alpha_1, \ldots, \alpha_n)$ simplesmente por $s_j(\alpha_i)$. Escrevendo $f(X) = a_n(X-\alpha_1)(X-\alpha_2)\ldots(X-\alpha_n)$ e expandindo os parênteses, obtemos

$$f(X) = a_nX^n - a_ns_1(\alpha_i)X^{n-1} + a_ns_2(\alpha_i)X^{n-2} - \cdots + a_n(-1)s_n(\alpha_i).$$

Igualando os coeficientes correspondentes nessa expressão para f e naquela do enunciado, obtemos o resultado desejado. □

As igualdades provenientes de (2.4), que relacionam coeficientes e raízes de um polinômio f não constante, são conhecidas como as **relações de Girard**. Elas nos permitem conhecer, com relação às raízes de f, a sua soma, a soma de seus produtos dois a dois, a soma de seus produtos três a três e assim por diante, além da soma de seus quadrados e a soma de seus inversos.

Embora as relações de Girard sejam úteis na resolução de vários tipos de problemas envolvendo as raízes de um polinômio, elas não são suficientes para determinar essas raízes.

Exemplo 2.41. Sejam α_1, α_2 e α_3 as raízes complexas do polinômio $f(X) = X^3+3X^2-2$. Pelas relações de Girard, temos

$$\alpha_1 + \alpha_2 + \alpha_3 = -3, \quad \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = 0 \quad \text{e} \quad \alpha_1\alpha_2\alpha_3 = 2.$$

Multiplicando a segunda igualdade acima por α_2, obtemos $\alpha_1{\alpha_2}^2 + \alpha_1\alpha_2\alpha_3 + {\alpha_2}^2\alpha_3 = 0$ e, como $\alpha_1\alpha_2\alpha_3 = 2$, podemos escrever ${\alpha_2}^2(\alpha_1+\alpha_3)+2 = 0$. Agora, como $\alpha_1+\alpha_3 = -3-\alpha_2$, temos que ${\alpha_2}^2(-3-\alpha_2)+2 = 0$, o que é equivalente à $f(\alpha_2) = 0$. De modo análogo, ao tentarmos determinar α_1 e α_3, obtemos expressões equivalentes a $f(\alpha_1) = 0$ e $f(\alpha_3) = 0$. Mas, para fins de determinação das raízes de f não há diferença entre as expressões $f(\alpha_1)$, $f(\alpha_2)$, $f(\alpha_3)$ e $f(X)$.

Nas notações da Proposição 2.40, nos referimos a $s_j(\alpha_1, \ldots, \alpha_n) \in \mathbb{K}$ como a $j-$ésima **soma simétrica elementar** das raízes de f. Sempre que $\alpha_1, \ldots, \alpha_n$ estiverem subentendidos e não houver perigo de confusão com o polinômio simétrico elementar $s_j = s_j(X_1, \ldots, X_n)$, denotaremos a soma simétrica elementar $s_j(\alpha_1, \ldots, \alpha_n)$ simplesmente por s_j.

2.6 Fatoração de polinômios

Diante do exposto até agora e notando que há similaridades entre as noções de divisibilidade em $\mathbb{K}[X]$ e em $\mathbb{Z}$, poderíamos nos perguntar se existem em $\mathbb{K}[X]$ polinômios *primos*, por meio dos quais seria possível obter uma *fatoração única* com propriedades semelhantes às da fatoração única de inteiros. Nesta seção apresentamos respostas para tal pergunta.

2.6.1 Fatoração única em $\mathbb{Q}[X]$

Definição 2.42. Sejam $f, g \in \mathbb{K}[X] \setminus \{0\}$. Se existir $a \in \mathbb{K} \setminus \{0\}$ tal que $f = ag$, dizemos que f e g são **associados** em $\mathbb{R}[X]$.

Exemplo 2.43. Os polinômios de coeficientes reais

$$f(X) = 3X^3 + 9X^2 - 3 \text{ e } g(X) = \frac{3}{\sqrt{3}}X^3 + 3\sqrt{3}X^2 - \sqrt{3}$$

são associados em $\mathbb{R}[X]$, uma vez que $f = \sqrt{3}g$ e $\sqrt{3} \in \mathbb{R} \setminus \{0\}$.

Definição 2.44. Dados $f, g \in \mathbb{K}[X] \setminus \{0\}$, dizemos que um polinômio $p \in \mathbb{K}[X] \setminus \{0\}$ é um **divisor comum** de f e g quando $p \mid f, g$.

Observe que f e g sempre têm divisores comuns: os polinômios constantes e não nulos sobre $\mathbb{K}$, por exemplo.

Definição 2.45. Dados $f, g \in \mathbb{K}[X] \setminus \{0\}$, dizemos que $d \in \mathbb{K}[X] \setminus \{0\}$ é um **máximo divisor comum** de f e g, e denotamos $d = \text{mdc}(f, g)$, se as duas condições a seguir forem satisfeitas:

(a) $d \mid f, g$ em $\mathbb{K}[X]$.

(b) Se $d' \in \mathbb{K}[X] \setminus \{0\}$ divide f e g em $\mathbb{K}[X]$, então $d' \mid d$ em $\mathbb{K}[X]$.

A existência de um mdc para dois polinômios não nulos sobre $\mathbb{K}$ é garantida pelo Teorema 2.46, chamado **teorema de Bézout** para polinômios. Tal mdc é único a menos de associação.

Teorema 2.46. *Sejam $f, g \in \mathbb{K}[X] \setminus \{0\}$. Se*

$$S = \{af + bg; a, b \in \mathbb{K}[X]\},$$

então existe um polinômio $d \in \mathbb{K}[X] \setminus \{0\}$ satisfazendo as seguintes condições:

(a) $S = d\mathbb{K}[X]$, onde $d\mathbb{K}[X] = \{ad; a \in \mathbb{K}[X]$. Em particular, $d \mid f, g$ em $\mathbb{K}[X]$.

(b) Todo polinômio em $\mathbb{K}[X] \setminus \{0\}$ que divide f e g também divide d.

Ademais, tal polinômio d é único, a menos de associação.

Demonstração. (a) Se $d \in S \setminus \{0\}$ é tal que

$$\partial d = \min\{\partial h; h \in S \setminus \{0\}\},$$

afirmamos inicialmente que $S = d\mathbb{K}[X]$. De fato, sendo $d = a_0 f + b_0 g$, com a_0, b_0 e $c \in \mathbb{K}[X]$, então

$$cd = (ca_0)f + (cb_0)g \in S,$$

ou seja, $d\mathbb{K}[X] \subset S$. Reciprocamente, escolha $h \in S$, digamos $h = af + bg$, com $a, b \in \mathbb{K}[X]$. Pela Divisão Euclidiana, temos $h = dq + r$, com $q, r \in \mathbb{K}[X]$ e $r = 0$ ou $0 \leq \partial r < \partial d$. Mas, se $r \neq 0$, então $\partial r < \partial d$ e

$$r = h - dq = (af + bg) - (a_0 f + b_0 g)q = (a - a_0 q)f + (b - b_0 q)g \in S,$$

uma contradição à minimalidade do grau de d em S. Logo, $r = 0$ e, daí, $h = dq \in d\mathbb{K}[X]$.

Para a segunda parte do item (a) basta ver que $f, g \in S = d\mathbb{K}[X]$, de forma que, em particular, f e g são múltiplos de d em $\mathbb{K}[X]$.

(b) Seja $d_1 \in \mathbb{K}[X] \setminus \{0\}$ um polinômio que divide f e g, digamos $f = d_1 f_1$ e $g = d_1 g_1$, com $f_1, g_1 \in \mathbb{K}[X]$. Se $a, b \in \mathbb{K}[X]$, então

$$af + bg = (af_1 + bg_1)d_1 \in d_1\mathbb{K}[X].$$

Mas, como $af + bg$ é um elemento genérico do conjunto S, segue então que

$$d \in d\mathbb{K}[x] = S \subset d_1\mathbb{K}[X];$$

em particular, d é um múltiplo de d_1, conforme desejado.

Agora, para a parte da unicidade, considere um outro polinômio $d' \in \mathbb{K}[X] \setminus \{0\}$ satisfazendo (a) e (b). Então, $d \mid d'$ e $d' \mid d$. Logo, $\partial d = \partial d'$ e assim há apenas duas possibilidades: d e d' são iguais ou diferem apenas pela multiplicação por uma constante. Em qualquer dos dois casos, existe $a \in \mathbb{K} \setminus \{0\}$ tal que $d' = ad$, ou seja, d e d' são associados. □

Devido à unicidade do mdc de dois polinômios não nulos sobre $\mathbb{K}$, convencionamos que tal mdc é sempre mônico. Além disso, dizemos que dois polinômios $f, g \in \mathbb{K}[X] \setminus \{0\}$ são **primos entre si**, ou **relativamente primos**, quando $\text{mdc}(f, g) = 1$.

Corolário 2.47. *Se $f, g \in \mathbb{K}[X] \setminus \{0\}$, então f e g são primos entre si se, e só se, existem polinômios $a, b \in \mathbb{K}[X]$ tais que $af + bg = 1$.*

Demonstração. Se mdc $(f, g) = 1$, a existência de $a, b \in \mathbb{K}[X]$ como no enunciado segue do teorema de Bézout. Reciprocamente, se $d = \text{mdc}\ (f, g)$ e existem $a, b \in \mathbb{K}[X]$ tais que $af + bg = 1$, então, novamente pelo teorema de Bézout, temos que $1 \in d\mathbb{K}[X]$, ou seja, d é um divisor do polinômio constante 1. Mas, uma vez que d é mônico, segue que $d = 1$. □

Corolário 2.48. *Sejam $f, g \in \mathbb{K}[X] \setminus \{0\}$ primos entre si e $h \in \mathbb{K}[X] \setminus \{0\}$ tal que $\partial h < \partial(fg)$. Então, existem $a, b \in \mathbb{K}[X]$ tais que $a = 0$ ou $\partial a < \partial g$, $b = 0$ ou $\partial b < \partial f$ e $af + bg = h$.*

Demonstração. Pelo Corolário 2.47, existem $a_1, b_1 \in \mathbb{K}[X]$ tais que $a_1 f + b_1 g = 1$. Daí, fazendo $a_2 = a_1 h$ e $b_2 = b_1 h$, temos $a_2 f + b_2 g = h$. Agora, fazendo a divisão euclidiana entre a_2 e g, segue que $a_2 = gq + a$, com $a = 0$ ou $\partial a < \partial g$. Assim,

$$h = (gq + a)f + b_2 g = af + (qf + b_2)g$$

e, fazendo $b = qf + b_2$, temos $h = af + bg$, com $a = 0$ ou $\partial a < \partial g$. Por fim, como $bg = h - af$, se $b \neq 0$, temos

$$\partial b + \partial g = \partial(bg) = \partial(h - af) \leq \partial h < \partial(fg) = \partial f + \partial g,$$

de sorte que $\partial b < \partial f$. □

Apresentamos a seguir uma definição que será de grande importância para o restante desta seção.

Definição 2.49. Um polinômio $p \in \mathbb{K}[X] \setminus \mathbb{K}$ é **irredutível** sobre $\mathbb{K}$ se p não puder ser escrito como produto de dois polinômios não constantes e com coeficientes em $\mathbb{K}$. Um polinômio $p \in \mathbb{K}[X] \setminus \mathbb{K}$ que não é irredutível é dito **redutível** sobre $\mathbb{K}$.

Enunciando de forma contrapositiva a condição de irredutibilidade, temos que um polinômio $p \in \mathbb{K}[X] \setminus \mathbb{K}$ é irredutível se, e somente se, a seguinte condição for satisfeita:

$$p = gh, \text{ com } g, h \in \mathbb{K}[X] \Rightarrow g \in \mathbb{K} \text{ ou } h \in \mathbb{K}. \tag{2.5}$$

Os exemplos a seguir ajudam a compreender melhor o conceito de polinômio irredutível.

Exemplo 2.50. Uma consequência imediata da expressão (2.5) é que todo polinômio $p \in \mathbb{K}[X]$ de grau 1 é irredutível; de fato, sendo $p = gh$, com $g, h \in \mathbb{K}[X]$, pelo item *(b)* da Proposição 2.13, temos que $\partial g + \partial h = \partial p = 1$, logo, $\partial g = 0$ ou $\partial h = 0$, ou seja, g ou h é constante. Por outro lado, pela Proposição 2.31 (Teorema Fundamental da Álgebra), os polinômios irredutíveis em $\mathbb{C}[X]$ são precisamente aqueles de grau 1.

Para o Exemplo 2.51 considere que dado o número complexo $z = a + bi$, o número complexo $\overline{z} = a - bi$ é o **conjugado** de z.

Exemplo 2.51. Se $p \in \mathbb{R}[X]$ é irredutível sobre $\mathbb{R}$, então $\partial p = 1$ ou $\partial p = 2$. De fato, de acordo com [16, p. 114], as raízes complexas não reais de p ocorrem aos pares (cada raiz com sua conjugada). Assim, há dois casos a considerar:

(a) $\partial p \geqslant 3$ e p tem pelo menos uma raiz real: sendo α essa raiz, pelo item (b) da Proposição 2.23 (teste da raiz) temos $p(X) = (X-\alpha)h(X)$, para algum $h \in \mathbb{R}[X]$ de grau pelo menos 2, logo, p é redutível sobre $\mathbb{R}$.

(b) $\partial p \geqslant 3$ e p tem duas raízes não reais conjugadas: sendo z e $\overline{z}$ essas raízes, novamente pelo teste da raiz, temos $p(X) = (X - z)(X - \overline{z})h(X)$, para algum polinômio $h \in \mathbb{C}[X]$ de grau pelo menos 1. Mas, se $z = a + bi$ e $g(X) = (X - z)(X - \overline{z})$, então

$$g(X) = (X - a - bi)(X - a + bi) = (X - a)^2 + b^2 \in \mathbb{R}[X].$$

Portanto, fazendo a Divisão Euclidiana de p por g, concluímos que $h \in \mathbb{R}[X]$. Assim, $p = gh$, com $g, h \in \mathbb{R}[X] \setminus \mathbb{R}$, logo, p é redutível sobre $\mathbb{R}$.

Vamos a partir de agora voltar nossa atenção para a irredutibilidade de polinômios sobre $\mathbb{Q}$.

Proposição 2.52. *Se $p \in \mathbb{Q}[X]$ tem grau 2 ou 3, então p é redutível sobre $\mathbb{Q}$ se, e somente se, tiver raiz em $\mathbb{Q}$.*

Demonstração. Seja α uma raiz racional de p. Pela Proposição 2.23 temos $p(X) = (X - \alpha)h(X)$, para algum $h \in \mathbb{Q}[X]$ de grau pelo menos 1, logo, p é redutível sobre $\mathbb{Q}$. Reciprocamente, se p é redutível sobre $\mathbb{Q}$ então, existem $g, h \in \mathbb{Q}[X] \setminus \mathbb{Q}$, tal que $p = gh$. Como $\partial p = 2$ ou 3, pela Proposição 2.13, ao menos um dentre g e h tem grau 1. Sem perda de generalidade, seja $\partial g = 1$. Então $g = aX + b$ com $a, b \in \mathbb{Q}$ e $a \neq 0$, e assim, p possui uma raiz racional igual a $\frac{-b}{a}$, uma vez que $p\left(\frac{-b}{a}\right) = g\left(\frac{-b}{a}\right)h\left(\frac{-b}{a}\right) = 0 \cdot h(\frac{-b}{a}) = 0$. □

Observe que, em $\mathbb{Q}[X]$, os únicos divisores de um polinômio $p \in \mathbb{Q}[X] \setminus \mathbb{Q}$, irredutível sobre $\mathbb{Q}$, são os polinômios constantes e aqueles associados a p. Diante disso, temos o seguinte resultado.

Proposição 2.53. *Seja $p \in \mathbb{Q}[X] \setminus \mathbb{Q}$ irredutível. Se $f_1, \ldots, f_k \in \mathbb{Q}[X] \setminus \{0\}$ são tais que $p \mid f_1 \cdots f_k$, então existe $1 \leqslant i \leqslant k$ tal que $p \mid f_i$.*

Demonstração. Por indução, basta mostrarmos que, se $p \mid fg$, com $f, g \in \mathbb{Q}[X] \setminus \{0\}$, então $p \mid f$ ou $p \mid g$. Se $p \nmid f$, afirmamos inicialmente que $\text{mdc}(f, p) = 1$. De fato, se $d = \text{mdc}\,(f, p)$, então $d \mid p$, de forma que $d \in \mathbb{Q}$ ou d é associado a p em $\mathbb{Q}[X]$. Mas, se d for associado a p, então segue de $d \mid f$ que $p \mid f$, o que é uma contradição. Logo, $d \in \mathbb{Q}$ e, daí, $d = 1$.

Agora, pelo Corolário 2.47, existem polinômios $a, b \in \mathbb{Q}[X]$ tais que $af + bp = 1$, de sorte que

$$a(fg) + (bg)p = g.$$

Como $p \mid (fg)$, existe $m \in \mathbb{Q}[X] \setminus \{0\}$ tal que $fg = pm$. Então,

$$g = a(pm) + (bg)p = p(am + bg).$$

Logo, $p \mid g$, conforme desejado. □

Mostraremos agora, que todo polinômio $f \in \mathbb{Q}[X] \setminus \mathbb{Q}$ pode ser escrito de forma única, a menos de associação, como o produto de um número finito de polinômios irredutíveis. De forma mais precisa, mostraremos que:

(i) Existem polinômios irredutíveis $p_1, \ldots, p_k \in \mathbb{Q}[X] \setminus \mathbb{Q}$ tais que $f = p_1 \cdots p_k$.

(ii) Se $q_1, \ldots, q_l \in \mathbb{Q}[X] \setminus \mathbb{Q}$ são também irredutíveis e tais que $f = q_1 \cdots q_l$, então $k = l$ e, a menos de uma reordenação, p_i e q_i são associados em $\mathbb{Q}[X]$.

Comecemos examinando a parte de existência.

Proposição 2.54. *Todo polinômio $f \in \mathbb{Q}[X] \setminus \mathbb{Q}$ pode ser escrito como produto de um número finito de polinômios irredutíveis sobre $\mathbb{Q}$.*

Demonstração. Façamos indução sobre ∂f, sendo o caso $\partial f = 1$ imediato (já vimos que, nesse caso, f é irredutível). Por hipótese de indução, suponha o resultado válido para todo polinômio em $\mathbb{Q}[X] \setminus \mathbb{Q}$ de grau menor do que n, e considere $f \in \mathbb{Q}[X] \setminus \mathbb{Q}$ tal que $\partial f = n$. Se f for irredutível, nada há a fazer. Senão, podemos escrever $f = gh$, com $g, h \in \mathbb{Q}[X] \setminus \mathbb{Q}$. Logo, $\partial g, \partial h < n$ e a hipótese de indução garante que g e h podem ser ambos escritos como produtos de um número finito de polinômios irredutíveis sobre $\mathbb{Q}$, digamos $g = p_1 \cdots p_j$ e $h = p_{j+1} \cdots p_k$. Então $f = gh = p_1 \cdots p_j p_{j+1} \cdots p_k$, um produto de um número finito de polinômios irredutíveis sobre $\mathbb{Q}$. □

A Proposição 2.55 garante que um polinômio $f \in \mathbb{Q}[X] \setminus \mathbb{Q}$ pode ser escrito de forma única, a menos de associação, como produto de polinômios irredutíveis sobre $\mathbb{Q}$.

Proposição 2.55. *Se $p_1, \ldots, p_k, q_1, \ldots, q_l \in \mathbb{Q}[X] \setminus \mathbb{Q}$ são irredutíveis e tais que $p_1 \cdots p_k = q_1 \cdots q_l$, então $k = l$ e, a menos de uma reordenação, p_i e q_i são associados sobre $\mathbb{Q}$.*

Demonstração. Se $k = 1$, temos $p_1 = q_1 \cdots q_l$, e a irredutibilidade de p_1 garante que $l = 1$. Analogamente, $l = 1 \Rightarrow k = 1$. Suponha, pois, $k, l > 1$; como $p_k \mid q_1 \cdots q_l$, a Proposição 2.53 garante a existência de $1 \leqslant j \leqslant l$ tal que $p_k \mid q_j$. Suponha, sem perda de generalidade, $j = l$. Como q_l é irredutível e $p_k \notin \mathbb{Q}$, a única possibilidade é que p_k e q_l sejam associados, digamos $p_k = uq_l$ com $u \in \mathbb{Q} \setminus \{0\}$. Então

$$p_1 \cdots p_{k-1} = q_1 \cdots q_{l-2} u q_{l-1} = q_1' \cdots q_{l-1}',$$

com $q_i' = q_i$ para $1 \leq i < l - 2$ e $q_{l-1}' = uq_{l-1}$, todos irredutíveis sobre $\mathbb{Q}$.

Por indução sobre $\max\{k, l\}$, temos $k - 1 = l - 1$ e, a menos de uma reordenação, p_i é associado a q_i' para $1 \leqslant i \leqslant l - 1$. Portanto, a menos de uma reordenação, p_i e q_i são também associados sobre $\mathbb{Q}$. □

A Proposição 2.54 e Proposição 2.55 nos permitem afirmar que em $\mathbb{Q}[X]$ temos *fatoração única*. Semelhantemente ao que ocorre em $\mathbb{Z}$, se $f \in \mathbb{Q}[X] \setminus \mathbb{Q}$ pode ser escrito como $f = p_1 \cdots p_k$, com $p_1, \ldots, p_k \in \mathbb{Q}[X] \setminus \mathbb{Q}$ irredutíveis, então, reunindo os fatores p_i iguais a menos de associação, obtemos

$$f = q_1^{\alpha_1} \cdots q_l^{\alpha_l}, \tag{2.6}$$

com $q_1, \ldots, q_l \in \mathbb{Q}[X] \setminus \mathbb{Q}$ irredutíveis e dois a dois não associados, e $\alpha_1, \ldots, \alpha_l \in \mathbb{N}$. A expressão 2.6 (também única a menos de associação) é a **fatoração canônica** de f em $\mathbb{Q}[X]$, e $q_1, \ldots, q_l$ são os **fatores irredutíveis** de f em $\mathbb{Q}[X]$.

2.6.2 Fatoração única em $\mathbb{Z}[X]$

Nesta seção, consideraremos o problema da fatoração única para polinômios com coeficientes inteiros. Para isso, a seguinte definição será de grande utilidade.

Definição 2.56. Se $f \in \mathbb{Z}[X] \setminus \{0\}$, o **conteúdo** $c(f)$ de f é o mdc de seus coeficientes não nulos. Se $c(f) = 1$, dizemos que f é um **polinômio primitivo** em $\mathbb{Z}[X]$.

Por simplicidade de notação, se $f = a_n X^n + \cdots + a_1 X + a_0 \in \mathbb{Z}[X] \setminus \{0\}$, denotamos

$$c(f) = \text{mdc}(a_0, \ldots, a_n).$$

Lema 2.57. *(a) Se $f \in \mathbb{Z}[X]\setminus\{0\}$ e $a \in \mathbb{Z}\setminus\{0\}$, então $c(af) = |a|\cdot c(f)$. Em particular, existe $g \in \mathbb{Z}[X] \setminus \{0\}$ primitivo tal que $f = c(f)g$.*

(b) Se $f \in \mathbb{Q}[X] \setminus \{0\}$, então, a menos de multiplicação por -1, existem únicos $a, b \in \mathbb{Z} \setminus \{0\}$ primos entre si e $g \in \mathbb{Z}[X]$ primitivo tais que $f = (\frac{a}{b})g$.

Demonstração. (a) Sejam $f(X) = a_n X^n + \cdots + a_1 X + a_0 \in \mathbb{Z}[X] \setminus \{0\}$, $a \in \mathbb{Z}\setminus\{0\}$ e $d = c(af) = \text{mdc}(aa_0, \ldots, aa_n)$. Como $c(f) \mid a_0, \ldots, a_n$ temos que $|a|c(f) \mid aa_0, \ldots, aa_n$, ou seja, $|a|c(f)$ é um divisor comum de $aa_0, \ldots, aa_n$, logo, $|a|c(f) \leqslant d$. Por outro lado, como $d = aa_0v_0 + \cdots + aa_nv_n$, com $v_i \in \mathbb{Z} \setminus \{0\}$, temos que $a \mid d$ e, como $d \mid aa_0, \ldots, aa_n$, $\frac{d}{|a|}$ é um inteiro positivo que divide $a_0, \ldots, a_n$, logo, $\frac{d}{|a|} \leqslant c(f)$, ou seja, $d \leqslant |a|c(f)$. Portanto $d = |a|c(f)$.

Em particular, se f é primitivo, podemos escrever $f = 1f = c(f)f$. Caso contrário, escrevemos $f = c(f)g$ onde $g(X) = \frac{a_n}{c(f)}X^n + \cdots + \frac{a_1}{c(f)}X + \frac{a_0}{c(f)}$. Como $c(f) = \text{mdc}(a_0, \ldots, a_n)$, temos que $g \in \mathbb{Z}[X]\setminus\{0\}$. Além disso, como $c(f) = a_0v_0 + \cdots + a_nv_n$, com $v_i \in \mathbb{Z} \setminus \{0\}$, temos $\frac{a_0}{c(f)}v_0 + \cdots + \frac{a_n}{c(f)}v_n = 1$, ou seja, $c(g) = 1$.

(b) Seja m o mmc dos denominadores dos coeficientes não nulos de f. Então, $mf \in \mathbb{Z}[X] \setminus \{0\}$. Seja $d = c(mf)$, então, pelo item (a), existe $h \in \mathbb{Z}[X] \setminus \{0\}$ primitivo tal que $mf = dh$, logo, $f = \frac{d}{m}h$ onde $\frac{d}{m}$ é um racional positivo. Agora, escolhendo $d' = \text{mdc}(d, m)$, $d = d'|a|$ e $m = d'|b|$, com $a, b \in \mathbb{Z} \setminus \{0\}$, temos que

$$f = \frac{d'|a|}{d'|b|}h = \frac{|a|}{|b|}h,$$

onde a e b são primos entre si. De fato, como $d' = dv_1 + mv_2$, com $v_1, v_2 \in \mathbb{Z}$, então, $\frac{d}{d'}v_1 + \frac{m}{d'}v_2 = 1$. Se a e b tem sinais iguais, escolhemos $g = h$ e assim, $\frac{a}{b}g = \frac{|a|}{|b|}h = f$; caso contrário, escolhemos $g = -h$, e assim, $\frac{a}{b}g = \frac{|a|}{|b|}h = f$.

Para a parte da unicidade basta notar que

$$|a| = \frac{d}{d'} \Leftrightarrow a = \frac{d}{d'} \text{ ou } a = -\frac{d}{d'},$$

e

$$|b| = \frac{m}{d'} \Leftrightarrow b = \frac{m}{d'} \text{ ou } b = -\frac{m}{d'},$$

e a unicidade de d, m e d' garantem a unicidade de a e b, a menos de multiplicação por -1.

□

O conceito de conteúdo de um polinômio de coeficientes inteiros é determinante para o estudo de polinômios irredutíveis sobre $\mathbb{Z}$, desde a sua definição.

Definição 2.58. Um polinômio $p \in \mathbb{Z}[X] \setminus \mathbb{Z}$ é **irredutível** sobre $\mathbb{Z}$ se p for primitivo e não puder ser escrito como produto de dois polinômios não constantes em $\mathbb{Z}[X]$. Um polinômio primitivo $p \in \mathbb{Z}[X] \setminus \mathbb{Z}$ que não é irredutível é dito **redutível** sobre $\mathbb{Z}$.

Novamente, é útil reescrever a condição de irredutibilidade de polinômios de coeficientes inteiros de forma contra-positiva, de modo que um polinômio primitivo $p \in \mathbb{Z}[X] \setminus \mathbb{Z}$ é irredutível se, e somente se, a seguinte condição for satisfeita:

$$p = gh, \text{ com } g, h \in \mathbb{Z}[X] \Rightarrow g = \pm 1 \text{ ou } h = \pm 1. \tag{2.7}$$

Proposição 2.59 (Lema de Gauss)**.** *Para $f, g \in \mathbb{Z}[X] \setminus \mathbb{Z}$, temos que:*

(a) $c(fg) = c(f)c(g)$. Em particular, fg é primitivo se, e só se, f e g o forem.

(b) Se f é primitivo, então f é irredutível em $\mathbb{Z}[X]$ se, e só se, o for em $\mathbb{Q}[X]$.

(c) Se f e g forem primitivos e associados em $\mathbb{Q}[X]$, então $f = \pm g$.

Demonstração. (a) Pelo Lema 2.57, se $f = c(f)f_1$ e $g = c(g)g_1$, então $f_1, g_1 \in \mathbb{Z}[X]$ são primitivos e $fg = c(f)c(g)f_1g_1$, de modo que $c(fg) = c(f)c(g)c(f_1g_1)$. Portanto, basta mostrarmos que f_1g_1 é primitivo, ou, o que é o mesmo, que

$$f, g \text{ primitivos } \Leftrightarrow fg \text{ é primitivo.}$$

Se f não for primitivo, existe $p \in \mathbb{Z}$ primo tal que p divide todos os coeficientes de f. Então, p divide todos os coeficientes de fg, e fg não é primitivo. Analogamente, se g não for primitivo, então fg também não é primitivo.

Reciprocamente, suponha que $f(X) = a_mX^m + \cdots + a_1X + a_0$ e $g(X) = b_nX^n + \cdots + b_1X + b_0$ são primitivos mas fg não o é. Considere $p \in \mathbb{Z}$ primo tal que p divide todos os coeficientes de fg, e sejam $k, l \geqslant 0$ os menores índices tais que p não divide a_k, b_l (tais k e l existem, uma vez que f e g são primitivos). Denotando por c_{k+l} o coeficiente de X^{k+l} em fg, segue que

$$c_{k+l} = \cdots + a_{k-2}b_{l+2} + a_{k-1}b_{l+1} + a_kb_l + a_{k+1}b_{l-1} + a_{k+2}b_{l-2} + \cdots .$$

Agora, como $p \mid c_{k+l}$ e $p \mid a_0, \ldots, a_{k-1}, b_0, \ldots, b_{l-1}$, a igualdade acima garante que $p \mid a_kb_l$, o que é uma contradição.

(b) Primeiramente, considere $f \in \mathbb{Z}[X] \setminus \mathbb{Z}$ primitivo e suponha que f é redutível em $\mathbb{Q}[X]$, digamos $f = gh$, com $g, h \in \mathbb{Q}[X] \setminus \mathbb{Q}$. Pelo Lema 2.57, podemos escolher $a, b, c, d \in \mathbb{Z} \setminus \{0\}$ tais que $g = (\frac{a}{b})g_1$ e $h = (\frac{c}{d})h_1$, com $g_1, h_1 \in \mathbb{Z}[X]$ primitivos. Então,

$$bdf = bg \cdot dh = ag_1 \cdot ch_1 = acg_1h_1.$$

Mas, como g_1h_1 é primitivo pelo item (a), considerando conteúdos na igualdade acima obtemos $|bd| \cdot c(f) = |ac|$. Logo, $\frac{ac}{bd} = \pm c(f) \in \mathbb{Z}$, e segue novamente da igualdade acima que $f = \pm c(f)g_1h_1$, ou seja, f é redutível em $\mathbb{Z}[X]$. Reciprocamente, se $f \in \mathbb{Z}[X] \setminus \mathbb{Z}$ é primitivo e irredutível em $\mathbb{Z}[X]$, então, dados $g, h \in \mathbb{Z}[X] \subset \mathbb{Q}[X]$, temos que $f = gh \Rightarrow g = \pm 1$ ou $h = \pm 1$. Logo, f é irredutível em $\mathbb{Q}[X]$.

(c) Se $f = (\frac{a}{b})g$, com $a, b \in \mathbb{Z} \setminus \{0\}$, então $bf = ag$ e, considerando conteúdos, obtemos $|b| \cdot c(f) = |a| \cdot c(g)$. Mas, uma vez que $c(f) = 1$ e $c(g) = 1$, segue que $|a| = |b|$, de sorte que $\frac{a}{b} = \pm 1$. □

O seguinte resultado sobre polinômios de coeficientes inteiros é semelhante à Proposição 2.54 e Proposição 2.55.

Teorema 2.60. *Todo polinômio primitivo $f \in \mathbb{Z}[X] \setminus \{0\}$ pode ser escrito como produto de um número finito de polinômios irredutíveis em $\mathbb{Z}[X]$. Ademais, tal maneira de escrever f é única a menos de uma reordenação dos fatores e de multiplicação de alguns dos mesmos por -1.*

Demonstração. Mostremos primeiramente a existência da fatoração em irredutíveis: vendo f como polinômio em $\mathbb{Q}[X]$, segue da Proposição 2.54 a existência de polinômios irredutíveis $p_1, \ldots, p_k \in \mathbb{Q}[X] \setminus \mathbb{Q}$ tais que $f = p_1 \cdots p_k$. Escreva $p_i = (\frac{a_i}{b_i})q_i$, com $a_i, b_i \in \mathbb{Z} \setminus \{0\}$ relativamente primos e $q_i \in \mathbb{Z}[X] \setminus \mathbb{Z}$ primitivo. Como q_i também é obviamente irredutível em $\mathbb{Q}[X]$, segue do item (b) da Proposição 2.59 que q_i também é obviamente irredutível em $\mathbb{Z}[X]$. Sendo $a = a_1 \cdots a_k$ e $b = b_1 \cdots b_k$, temos então que

$$f = (\frac{a}{b})q_1 \cdots q_k.$$

Mas como $q_1 \cdots q_k$ são todos primitivos, o item (a) da Proposição 2.59 garante que $q_1 \cdots q_k$ também é primitivo. Assim, considerando conteúdos na igualdade acima, obtemos

$$|b| = |b| \cdot c(f) = |a| \cdot c(q_1 \cdots q_k) = |a|.$$

Portanto, segue que $\frac{a}{b} = \pm 1$ e, daí, $f = q_1 \cdots q_k$ é um produto de polinômios irredutíveis de $\mathbb{Z}[X]$.

A prova da parte de unicidade do enunciado é essencialmente idêntica à prova da Proposição 2.55, uma vez que provemos o seguinte: se $p, f, g \in \mathbb{Z}[X] \setminus \mathbb{Z}$ são tais que p é irredutível e $p \mid fg$ em $\mathbb{Z}[X]$, então $p \mid f$ ou $p \mid g$ em $\mathbb{Z}[X]$. Para tanto, observe inicialmente (novamente pelo item (b) da Proposição 2.59) que p também é irredutível em $\mathbb{Q}[X]$ e, assim sendo, já sabemos que $p \mid f$ ou $p \mid g$ em $\mathbb{Q}[X]$. Se $p \mid f$ em $\mathbb{Q}[X]$ (o outro caso é análogo), existe $f_1 \in \mathbb{Q}[X]$ tal que $f = f_1p$. Considerando $a, b \in \mathbb{Z}$ tais que $f_1 = (\frac{a}{b})f_2 \in \mathbb{Z}[X] \setminus \mathbb{Z}$ primitivo, temos

$$bf = bf_1p = af_2p.$$

Agora, p e f_2 primitivos implica (uma vez mais pelo item (a) da Proposição 2.59) em f_2p primitivo e, considerando conteúdos na igualdade acima, obtemos $|b| \cdot c(f) = |a| \cdot c(f_2p) = |a|$. Portanto, $\frac{a}{b} = \pm c(f) \in \mathbb{Z}$, de maneira que $f_1 \in \mathbb{Z}[X]$ e $p \mid f$ em $\mathbb{Z}[X]$. □

Expomos a seguir o **Critério de Eisenstein**, um importante critério que permite determinar a irredutibilidade de vários polinômios em $\mathbb{Q}[X]$.

Teorema 2.61 (Critério de Eisenstein)**.** *Seja $f(X) = a_nX^n + \cdots + a_1X + a_0$ um polinômio de grau $n \geq 1$ e com coeficientes inteiros. Sejam ainda $p \in \mathbb{Z}$ primo e $1 \leq k < n$ inteiro tais que $p \mid a_0, a_1, \ldots, a_k$, p^2 não divide a_0 e p não divide a_n. Então, f é irredutível sobre $\mathbb{Q}$.*

Demonstração. Seja f_1 primitivo tal que $f(X) = c(f)f_1$. Como p não divide $c(f)$, as condições do enunciado continuam válidas para os coeficientes de f_1. Podemos supor que f é primitivo. Pelo item (b) da Proposição 2.59, basta provar que $f(X)$ é irredutível em $\mathbb{Z}[X]$.

Suponhamos, por absurdo, que $f(X) = g(X)h(X)$, com $1 \leqslant \partial g, \partial h < n = \partial f$ e $g, h \in \mathbb{Z}[X]$. Sejam $g(X) = b_rX^r + \cdots + b_1X + b_0$, com $b_j \in \mathbb{Z}$ para $0 \leqslant j \leqslant r$, e $h(X) = c_sX^s + \cdots + c_1X + c_0$, com $c_j \in \mathbb{Z}$ para $0 \leqslant j \leq s$.

Como $a_0 = b_0c_0$ e $p \mid a_0$, então $p \mid b_0$ ou $p \mid c_0$. Entretanto, p^2 não divide a_0, logo p divide apenas um deles, isto é,

$$p \mid b_0 \text{ e } p \text{ não divide } c_0, \text{ ou } p \text{ não divide } b_0 \text{ e } p \mid c_0.$$

Suponhamos, sem perda de generalidade, que p não divide b_0 e $p \mid c_0$.

Como $a_n = b_rc_s$ e p não divide a_n, então p não divide b_r. Seja l o menor natural $l \leq r$ tal que p não divide b_l. Então, $p \mid b_{l-1}, \ldots, b_0$ e $a_l = b_lc_0 + b_{l-1}c_1 + \cdots + b_0c_l$, onde p não divide b_lc_0 e $p \mid b_{l-1}c_1 + \cdots + b_0c_l$. Logo, p não divide a_l e, por hipótese, $l = n = \partial f > r$, o que é uma contradição. □

Exemplo 2.62. $f(X) = 5X^4 - 6X^2 + 9X - 3$ é irredutível sobre $\mathbb{Q}$. De fato, para $p = 3$, temos que $p \mid a_0$, $p \mid a_1$, $p \mid a_2$, $p \mid a_3$, p não divide a_4 e p^2 não divide a_0, satisfazendo as hipóteses do Critério de Eisenstein.

2.7 Equações polinomiais ou algébricas

Equação polinomial ou **algébrica** com solução em $\mathbb{K}$ é toda equação da forma $f(X) = 0$. Denominamos de conjunto solução ao conjunto das raízes de $f(X)$. O grau do polinômio $f(X)$ determina o grau da equação $f(X) = 0$. Neste capítulo estudaremos métodos de obtenção das raízes nos casos em que $f(X)$ possui graus 2 e 3, o que será de fundamental importância na compreensão do capítulo posterior.

2.7.1 Equação polinomial de grau 2

Considere a equação $aX^2 + bX + c = 0$ com coeficientes em $\mathbb{C}$ e $a \neq 0$. É possível deduzir a fórmula resolutiva desta equação, em função dos seus coeficientes, completando quadrados em $f(X)$ como a seguir:

$$aX^2+bX+c = a\left(X^2+\frac{b}{a}X\right)+c = a\left(X^2+2\frac{b}{2a}X+\frac{b^2}{4a^2}\right)+c-\frac{b^2}{4a} = a\left(X+\frac{b}{2a}\right)^2+c-\frac{b^2}{4a}$$

Portanto, α é raiz da equação se, e somente se,

$$a\left(\alpha+\frac{b}{2a}\right)^2+c-\frac{b^2}{4a}=0 \Leftrightarrow \left(\alpha+\frac{b}{2a}\right)^2=\frac{b^2}{4a^2}-\frac{c}{a} \Leftrightarrow \left(\alpha+\frac{b}{2a}\right)^2=\frac{b^2-4ac}{4a^2}$$

de onde, por extração das raízes, obtemos

$$\alpha + \frac{b}{2a} = \pm\sqrt{\frac{b^2-4ac}{4a^2}} \Leftrightarrow \alpha = \pm\sqrt{\frac{b^2-4ac}{4a^2}} - \frac{b}{2a} \Leftrightarrow \alpha = \frac{-b \pm \sqrt{b^2-4ac}}{2a},$$

onde $\sqrt{b^2-4ac}$ é uma das raízes quadradas do número complexo $\Delta = b^2 - 4ac$, chamado usualmente de discriminante da equação.

Observe que, a condição necessária e suficiente para que a equação do segundo grau tenha uma raiz dupla, igual a $\frac{-b}{2a}$, é que o discriminante da equação seja nulo.

Se os coeficientes a, b e c da equação $aX^2 + bX + c = 0$ são reais, então, pela fórmula resolutiva, temos os seguintes resultados:

i. $\Delta > 0$ se, e somente se, a equação tem duas raízes reais;

ii. $\Delta = 0$ se, e somente se, a equação tem uma raiz real dupla;

iii. $\Delta < 0$ se, e somente se, a equação tem duas raízes complexas conjugadas.

2.7.2 Equação polinomial de grau 3

Considere a equação geral do terceiro grau com coeficientes complexos, que vamos supor, sem perda de generalidade, que esteja na forma:

$$X^3 + a_2X_2X^2 + a_1X + a_0 = 0. \tag{2.8}$$

Por meio de uma mudança de variável, vamos colocar o polinômio em (2.8) numa forma onde não figure o termo do segundo grau.

Substituindo X por $Y + d$ na Equação (2.8) temos

$$(Y+d)^3+a_2(Y+d)^2+a_1(Y+d)+a_0 = Y^3+(3d+a_2)Y^2+(3d^2+2da_2+a_1)Y+(d^3+d^2a_2+da_1+a_0).$$

Pondo $d = -\frac{a_2}{3}$, na expressão acima, temos que

$$X^3 + a_2X^2 + a_1X + a_0 = Y^3 + pY + q,$$

onde

$$X = Y - \frac{a_2}{3}, \quad p = a_1 - \frac{a_2^2}{3} \quad \text{e} \quad q = \frac{2a_2^3}{27} - \frac{a_1a_2}{3} + a_0. \tag{2.9}$$

Portanto, para achar as raízes da Equação (2.8), basta achar as raízes da equação

$$Y^3 + pY + q = 0, \tag{2.10}$$

com p e q como em (2.9) e delas subtrair $\frac{a_2}{3}$.

Vamos agora, nos concentrar na resolução da Equação (2.10).

Sejam U e V duas novas indeterminadas. Façamos em (2.10) a mudança de variáveis: $Y = U + V$. Obtemos, então,

$$0 = (U+V)^3 + p(U+V) + q = (U^3 + V^3 + q) + (U+V)(p+3UV). \tag{2.11}$$

Segue daí que cada solução (U, V) do sistema

$$\begin{cases} U^3 + V^3 = -q \\ U \cdot V = -\frac{p}{3} \end{cases}$$

nos fornece uma solução (U, V) de (2.11) e, portanto, uma solução da forma $Y = U + V$ de (2.10).

Elevando ao cubo a segunda equação do sistema acima, segue que se (U, V) é uma solução do sistema, então U^3 e V^3 são soluções da seguinte equação do segundo grau:

$$Z^2 + qZ - \frac{p^3}{27} = 0. \tag{2.12}$$

Fixando uma das raízes quadradas de $\frac{q^2}{4} + \frac{p^3}{27}$ e denotando-a por $\sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$, temos que as raízes de (2.12) são:

$$Z_1 = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} \quad \text{e} \quad Z_2 = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}.$$

Pela simetria do papel que desempenham U e V, podemos supor que $U^3 = Z_1$ e $V^3 = Z_2$.

Escolhendo uma das raízes cúbicas de Z_1 e denotando-a por $\sqrt[3]{Z_1}$, segue que as soluções de $U^3 = Z_1$ são $\sqrt[3]{Z_1}$, $\zeta_3\sqrt[3]{Z_1}$ e $\zeta_3^2\sqrt[3]{Z_1}$, em que $\zeta_3 = \frac{-1+i\sqrt{3}}{2}$ é uma das raízes cúbicas da unidade.

Agora, denotando por $\sqrt[3]{Z_2}$ a raiz cúbica de Z_2, tal que $\sqrt[3]{Z_1}\sqrt[3]{Z_2} = -\frac{p}{3}$, de modo que a segunda equação do sistema acima seja satisfeita, o referido sistema admite as seguintes soluções:

$$\begin{aligned}
&U_1 = \sqrt[3]{Z_1}, \quad V_1 = \sqrt[3]{Z_2};\\
&U_2 = \zeta_3\sqrt[3]{Z_1}, \quad V_2 = \zeta_3^2\sqrt[3]{Z_2};\\
&U_3 = \zeta_3^2\sqrt[3]{Z_1}, \quad V_3 = \zeta_3\sqrt[3]{Z_2}.
\end{aligned}$$

Finalmente, a equação cúbica (2.10) possui como soluções as chamadas **fórmulas de Cardano**:

$$\begin{aligned}
Y_1 &= U_1 + V_1 = \sqrt[3]{Z_1} + \sqrt[3]{Z_2} = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}},\\
Y_2 &= U_2 + V_2 = \zeta_3\sqrt[3]{Z_1} + \zeta_3^2\sqrt[3]{Z_2} = \zeta_3\sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \zeta_3^2\sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} \quad \text{e}\\
Y_3 &= U_3 + V_3 = \zeta_3^2\sqrt[3]{Z_1} + \zeta_3\sqrt[3]{Z_2} = \zeta_3^2\sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \zeta_3\sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}.
\end{aligned}$$

Exemplo 2.63. Resolvendo pelas fórmulas de Cardano a equação $X^3 + 6X - 20 = 0$, obtemos as seguintes raízes:

$$\begin{aligned}
X_1 &= \sqrt[3]{10 + 6\sqrt{3}} + \sqrt[3]{10 - 6\sqrt{3}};\\
X_2 &= -\frac{1}{2}\left(\sqrt[3]{10 + 6\sqrt{3}} + \sqrt[3]{10 - 6\sqrt{3}}\right) + \frac{i\sqrt{3}}{2}\left(\sqrt[3]{10 + 6\sqrt{3}} - \sqrt[3]{10 - 6\sqrt{3}}\right),\\
X_3 &= -\frac{1}{2}\left(\sqrt[3]{10 + 6\sqrt{3}} + \sqrt[3]{10 - 6\sqrt{3}}\right) - \frac{i\sqrt{3}}{2}\left(\sqrt[3]{10 + 6\sqrt{3}} - \sqrt[3]{10 - 6\sqrt{3}}\right),
\end{aligned}$$

sendo X_1 uma raiz real e, X_2 e X_3 raízes complexas conjugadas. Não é difícil notar que 2 é raiz da equação, donde conclui-se que $\sqrt[3]{10+6\sqrt{3}}+\sqrt[3]{10-6\sqrt{6}}=2$.

3 Método para resolução de equações do tipo $Y^3 + pY + q = 0$

O método que apresentamos neste capítulo fornece fórmulas que permitem determinar as raízes de uma equação do tipo $Y^3+pY+q=0$ com coeficientes reais e $p, q \neq 0$, de uma forma mais simples do que quando usamos as fórmulas de Cardano. Para tanto usamos as referências [17], [11] e [27].

Para a aplicação desse método, na equação de coeficientes reais $Y^3 + pY + q = 0$, fazemos $p = -3rs$ e $q = rs(r + s)$, obtendo a equação $Y^3 - 3rsY + rs(r + s) = 0$. Como $-3rs$ e $rs(r + s)$ são reais, há apenas dois casos há considerar: o caso em que r e s são números reais e o caso em que r e s são um par de complexos conjugados.

3.1 Resolvendo a equação $Y^3 - 3rsY + rs(r + s) = 0$ quando r e s são reais

No caso em que r e s são números reais há dois casos há considerar: $r = s$ e $r \neq s$. Comecemos pelo caso em que $r = s$.

3.1.1 Caso $r = s$

Teorema 3.1. *Seja $Y^3 - 3rsY + rs(r + s) = 0$ uma equação com coeficientes reais. Se $r = s$ então três raízes da equação são $\sqrt{rs}, \sqrt{rs}, -2\sqrt{rs}$.*

Demonstração. O polinômio $Y^3 - 3rsY + rs(r + s)$ pode ser fatorado como segue:

$$\begin{aligned} Y^3 - 3r^2Y + 2r^3 &= (Y^3 - r^3) - 3r^2(Y - r) \\ &= (Y - r)(Y^2 + rY - 2r^2) \\ &= (Y - r)^2(Y + 2r) \end{aligned}$$

Logo, as raízes são $r, r, -2r$, que podem ser escritas, já que $r = s$, como $\sqrt{rs}, \sqrt{rs}, -2\sqrt{rs}$. □

Exemplo 3.2. Resolva $Y^3 - 27Y + 54 = 0$.

Como $rs = 9$ e $rs(r + s) = 54$, segue que $r + s = 6$. Logo r e s são as duas raízes de $T^2 - 6T + 9 = 0$. Resolvendo esta equação temos $r = s = 3$. Pelo Teorema 3.1 as três raízes de $Y^3 - 27Y + 54 = 0$ são $3, 3, -6$.

3.1.2 Caso $r \neq s$

Para o caso em que $r \neq s$ usaremos a seguinte identidade que pode ser encontrada em [11]:

$$Y^3 - 3rsY + rs(r+s) = \frac{s}{s-r}(Y-r)^3 + \frac{r}{r-s}(Y-s)^3, \tag{3.1}$$

Como temos $r \neq s$, da identidade (3.1) segue que

$$\frac{s}{s-r}(Y-r)^3 + \frac{r}{r-s}(Y-s)^3 = Y^3 - 3rsY + rs(r+s) = 0,$$

então,

$$\frac{s(Y-r)^3 - r(Y-s)^3}{s-r} = 0 \Leftrightarrow s(Y-r)^3 = r(Y-s)^3.$$

Logo,

$$\left(\frac{Y-r}{Y-s}\right)^3 = \frac{r}{s}. \tag{3.2}$$

Observe que temos $s \neq 0$ já que $p \neq 0$.

Teorema 3.3. *Seja a equação $Y^3 - 3rsY + rs(r+s) = 0$ com coeficientes reais e $r \neq s$. Se r e s são reais, então a equação possui uma raiz real e um par de raízes complexas conjugadas, sendo elas*

$$-r^{\frac{1}{3}}s^{\frac{1}{3}}(r^{\frac{1}{3}} + s^{\frac{1}{3}}),\ -r^{\frac{1}{3}}s^{\frac{1}{3}}(\zeta_3^2 r^{\frac{1}{3}} + \zeta_3 s^{\frac{1}{3}})\ e\ -r^{\frac{1}{3}}s^{\frac{1}{3}}(\zeta_3 r^{\frac{1}{3}} + \zeta_3^2 s^{\frac{1}{3}}).$$

Demonstração. Suponha r, s reais. Então $\frac{r}{s}$ também é real. Logo, pela Equação (3.2) temos $\frac{Y-r}{Y-s} = \sqrt[3]{\frac{r}{s}},\ \sqrt[3]{\frac{r}{s}}\zeta_3,\ \sqrt[3]{\frac{r}{s}}\zeta_3^2$, onde $\zeta_3 = \frac{-1+i\sqrt{3}}{2}$. Quando $\frac{Y-r}{Y-s} = \sqrt[3]{\frac{r}{s}}$, então $\sqrt[3]{s}(Y-r) = \sqrt[3]{r}(Y-s) \Rightarrow (\sqrt[3]{s} - \sqrt[3]{r}Y) = \sqrt[3]{s}r - \sqrt[3]{r}s$. Portanto,

$$Y = \frac{\sqrt[3]{s}r - \sqrt[3]{r}s}{\sqrt[3]{s} - \sqrt[3]{r}} = \frac{r^{\frac{1}{3}}s^{\frac{1}{3}}(r^{\frac{2}{3}} - s^{\frac{2}{3}})}{s^{\frac{1}{3}} - r^{\frac{1}{3}}} = -r^{\frac{1}{3}}s^{\frac{1}{3}}(r^{\frac{1}{3}} + s^{\frac{1}{3}}).$$

De modo semelhante, quando $\frac{Y-r}{Y-s} = \sqrt[3]{\frac{r}{s}}\zeta_3$, temos $\sqrt[3]{s}(Y-r) = \sqrt[3]{r}\zeta_3(Y-s) \Rightarrow (\sqrt[3]{s} - \zeta_3\sqrt[3]{r})Y = \sqrt[3]{s}r - \zeta_3\sqrt[3]{r}s$. Donde segue que

$$\begin{aligned} Y &= \frac{\sqrt[3]{s}r - \zeta_3\sqrt[3]{r}s}{\sqrt[3]{s} - \zeta_3\sqrt[3]{r}} = \frac{r^{\frac{1}{3}}s^{\frac{1}{3}}(r^{\frac{2}{3}} - \zeta_3 s^{\frac{2}{3}})}{s^{\frac{1}{3}} - \zeta_3 r^{\frac{1}{3}}} = \frac{r^{\frac{1}{3}}s^{\frac{1}{3}}(r^{\frac{2}{3}} - \zeta_3 s^{\frac{2}{3}})\zeta_3^2}{(s^{\frac{1}{3}} - \zeta_3 r^{\frac{1}{3}})\zeta_3^2} \\ &= -\frac{r^{\frac{1}{3}}s^{\frac{1}{3}}(\zeta_3^2 r^{\frac{2}{3}} - s^{\frac{2}{3}})}{\zeta_3^2(\zeta_3 r^{\frac{1}{3}} - s^{\frac{1}{3}})} = -\zeta_3 r^{\frac{1}{3}}s^{\frac{1}{3}}(\zeta_3 r^{\frac{1}{3}} + s^{\frac{1}{3}}) \\ &= -r^{\frac{1}{3}}s^{\frac{1}{3}}(\zeta_3^2 r^{\frac{1}{3}} + \zeta_3 s^{\frac{1}{3}}). \end{aligned}$$

Quando $\frac{Y-r}{Y-s} = \sqrt[3]{\frac{r}{s}}\zeta_3^2$, um argumento semelhante nos fornece $Y = -r^{\frac{1}{3}}s^{\frac{1}{3}}(\zeta_3 r^{\frac{1}{3}} + \zeta_3^2 s^{\frac{1}{3}})$. □

Exemplo 3.4. Determine as soluções de $Y^3 - 9Y - 28 = 0$.

Temos $3rs = 9$ e $rs(r+s) = -28$, logo $rs = 3$ e $r + s = \frac{-28}{3}$. Pelas relações de Girard temos que r e s são as raízes de $T^2 + \frac{28}{3}T + 3 = 0$, o que nos dá $r = \frac{-1}{3}$ e $s = -9$. Como $r \neq s$, pelo Teorema 3.3 as raízes da equação $Y^3 - 9Y - 28 = 0$ são

$$-3^{\frac{1}{3}}\left(\left(\frac{-1}{3}\right)^{\frac{1}{3}} + (-9)^{\frac{1}{3}}\right) = -((-1)^{\frac{1}{3}} + (-27)^{\frac{1}{3}}) = 4,$$

$$-3^{\frac{1}{3}}\left(\left(\frac{-1-i\sqrt{3}}{2}\right)\left(\frac{-1}{3}\right)^{\frac{1}{3}} + \left(\frac{-1+i\sqrt{3}}{2}\right)(-9)^{\frac{1}{3}}\right) = -\left(\frac{1+i\sqrt{3}}{2} + \frac{3-3i\sqrt{3}}{2}\right) = -2+i\sqrt{3},$$

$$-3^{\frac{1}{3}}\left(\left(\frac{-1+i\sqrt{3}}{2}\right)\left(\frac{-1}{3}\right)^{\frac{1}{3}} + \left(\frac{-1-i\sqrt{3}}{2}\right)(-9)^{\frac{1}{3}}\right) = -\left(\frac{1-i\sqrt{3}}{2} + \frac{3+3i\sqrt{3}}{2}\right) = -2-i\sqrt{3}.$$

3.2 Resolvendo a equação $Y^3 - 3rsY + rs(r+s) = 0$ quando r e s são um par de complexos conjugados

Para considerarmos o segundo caso, quando r e s são um par de complexos conjugados, estabeleceremos algumas notações.

Qualquer número complexo $z = a + bi \neq 0$ pode ser escrito como $z = |z|e^{i\theta} = |z|(\cos\theta + i\,\mathrm{sen}\,\theta)$, onde θ é o argumento de z no intervalo $(-\pi, \pi]$. Escreveremos $\overline{z} = a - bi$ para denotar o conjugado de z e $\mathrm{Re}(z)$ para denotar a parte real de z.

Para algum inteiro positivo m, o número complexo z tem m-ésimas raízes $\alpha, \alpha\zeta_1, \alpha\zeta_2^2, \ldots, \alpha\zeta_{m-1}^{m-1}$, onde $\alpha = \sqrt[m]{|z|}e^{i\frac{\theta}{m}}$ e $\zeta_m = e^{i\frac{2\pi}{m}}$. Escreveremos α como $z^{\frac{1}{m}}$. Em particular, quando $\theta = 0$, $z^{\frac{1}{m}} = \sqrt[m]{z} \in \mathbb{R}$.

Teorema 3.5. *Seja a equação $Y^3 - 3rsY + rs(r+s) = 0$ com coeficientes reais e $r \neq s$. Se r e s são um par de complexos conjugados, então a equação possui três raízes reais, sendo elas*

$$-2\sqrt{rs}\cos\frac{\theta}{3},\ -2\sqrt{rs}\cos\Big(\frac{\theta}{3} + \frac{2\pi}{3}\Big)\ e\ -2\sqrt{rs}\cos\Big(\frac{\theta}{3} + \frac{4\pi}{3}\Big).$$

Demonstração. Da expressão (3.2), segue que $\frac{Y-r}{Y-s} = \left(\frac{r}{s}\right)^{\frac{1}{3}}, \left(\frac{r}{s}\right)^{\frac{1}{3}}\zeta_3, \left(\frac{r}{s}\right)^{\frac{1}{3}}\zeta_3^2$. Mediante cálculos análogos aos do primeiro caso em que r e s são reais, vemos que as soluções são dadas pelas mesmas expressões

$$-r^{\frac{1}{3}}s^{\frac{1}{3}}(r^{\frac{1}{3}} + s^{\frac{1}{3}}),\ -r^{\frac{1}{3}}s^{\frac{1}{3}}(\zeta_3 r^{\frac{1}{3}} + \zeta_3^2 s^{\frac{1}{3}})\ \text{e}\ -r^{\frac{1}{3}}s^{\frac{1}{3}}(\zeta_3^2 r^{\frac{1}{3}} + \zeta_3 s^{\frac{1}{3}}).$$

No entanto, como $r = |r|e^{i\theta}$ e $s = |s|e^{-i\theta}$ com $|r| \neq |s|$, segue que $r^{\frac{1}{3}} = |r|^{\frac{1}{3}}e^{i\frac{\theta}{3}} = (rs)^{\frac{1}{6}}e^{i\frac{\theta}{3}}$ e, de modo semelhante, $s^{\frac{1}{3}} = (rs)^{\frac{1}{6}}e^{-i\frac{\theta}{3}} = r^{\frac{1}{3}}$. Desse modo, podemos reescrever as soluções como

$$-r^{\frac{1}{3}}s^{\frac{1}{3}}(r^{\frac{1}{3}} + s^{\frac{1}{3}}) = -(rs)^{\frac{1}{3}+\frac{1}{6}}\left(e^{i\frac{\theta}{3}} + e^{-i\frac{\theta}{3}}\right) = -2\sqrt{rs}\cos\frac{\theta}{3},$$

$$-r^{\frac{1}{3}}s^{\frac{1}{3}}(\zeta_3 r^{\frac{1}{3}} + \zeta_3^2 s^{\frac{1}{3}}) = -(rs)^{\frac{1}{3}}\left(\zeta_3 r^{\frac{1}{3}} + \overline{\zeta_3 r^{\frac{1}{3}}} + \right) = -2(rs)^{\frac{1}{3}}\,\mathrm{Re}(\zeta_3 r^{\frac{1}{3}}) = -2\sqrt{rs}\cos\Big(\frac{\theta}{3} + \frac{2\pi}{3}\Big),$$

$$-r^{\frac{1}{3}}s^{\frac{1}{3}}(\zeta_3^2 r^{\frac{1}{3}} + \zeta_3 s^{\frac{1}{3}}) = -(rs)^{\frac{1}{3}}\left(\zeta_3^2 r^{\frac{1}{3}} + \overline{\zeta_3^2 r^{\frac{1}{3}}}+\right) = -2(rs)^{\frac{1}{3}}\,\mathrm{Re}(\zeta_3^2 r^{\frac{1}{3}}) = -2\sqrt{rs}\cos\Big(\frac{\theta}{3}+\frac{4\pi}{3}\Big).$$

□

Exemplo 3.6. Determine as raízes da equação $Y^3 - 48Y - 64\sqrt{2} = 0$.

Temos $3rs = 48$ e $rs(r+s) = -64\sqrt{2}$, logo $rs = 16$ e $r+s = -4\sqrt{2}$. Pelas relações de Girard temos que r e s são as raízes de $T^2 - 4\sqrt{2}T + 16$, o que nos dá $r = \frac{-4\sqrt{2}+\sqrt{-32}}{2} = -2\sqrt{2} + 2i\sqrt{2} = 4e^{i\frac{3\pi}{4}}$ e $s = 4e^{-i\frac{3\pi}{4}}$. Logo, r e s são dois complexos conjugados e $\theta = \frac{3\pi}{4}$. Portanto, pelo Teorema 3.5 as raízes da equação $Y^3 - 48Y - 64\sqrt{2} = 0$ são

$$-2\cdot 4\cos\frac{\pi}{4} = -8\cdot\frac{1}{\sqrt{2}} = -4\sqrt{2},$$

$$-2\cdot 4\left(\cos\frac{\pi}{4}+\frac{2\pi}{3}\right) = 8\cos\frac{\pi}{12} = 8\cdot\frac{1+\sqrt{3}}{2\sqrt{2}} = 2\sqrt{2}+2\sqrt{6},$$

$$-2\cdot 4\left(\cos\frac{\pi}{4}+\frac{4\pi}{3}\right) = -8\cos\frac{19\pi}{12} = -8\cdot\frac{-1+\sqrt{3}}{2\sqrt{2}} = 2\sqrt{2}-2\sqrt{6}.$$

Comparando as fórmulas de Cardano com o método apresentado neste capítulo, vemos que quando r e s são números reais, a solução real obtida pelas fórmulas de Cardano tem a seguinte forma para $a = \frac{-q}{2}$ e $b = \frac{q^2}{4} + \frac{p^3}{27}$:

$$Y = \sqrt[3]{a+\sqrt{b}} + \sqrt[3]{a-\sqrt{b}},$$

enquanto o método apresentado neste capítulo fornece

$$Y = -(rs)^{\frac{1}{3}}(r^{\frac{1}{3}} + s^{\frac{1}{3}}).$$

Logo, considerando o aspecto computacional, o método que apresentamos neste capítulo é mais simples do que as fórmulas de Cardano.

4 Reticulados

Um dos parâmetros para se encontrar bons códigos corretores de erros [24] está ligado ao problema do empacotamento de esferas, que surgiu a partir do 18^o Problema de Hilbert, que é uma forma de dispor esferas no espaço euclidiano de modo a cobrir a maior parte do espaço. Este problema é denominado de empacotamento esférico, e quando o conjunto de centros das esferas formam um subgrupo discreto do $\mathbb{R}^n$, estes empacotamentos passam a se chamar empacotamentos reticulados. A partir daí, passaram a associar o estudo dos códigos aos reticulados e surgiram várias famílias de reticulados.

Um método ainda pouco explorado de obter reticulados que será apresentado neste trabalho, consiste em obter reticulados via polinômios irredutíveis sobre o corpo dos racionais. Assim, neste trabalho apresentamos construções a partir de polinômios de grau 2 e de grau 3 com raízes reais de versões rotacionadas dos reticulados A_2 e D_3, que são os reticulados com densidade de empacotamento ótimas em dimensão 2 e 3, respectivamente [12]. O método utilizado neste trabalho foi proposto em [25] e espera-se que ele possa ser estendido para outras dimensões.

A dificuldade desse tipo de construção está em encontrar vetores linearmente independentes e identificar o determinante da matriz geradora e a norma de um ponto do reticulado em termos dos coeficientes dos polinômios considerados.

Um outro problema semelhante ao empacotamento de esferas é o número de contato. Configurações esféricas que dão bons números de contato sempre vêm de reticulados bem arredondados.

Muitos reticulados importantes na matemática e na física são bem arredondados. Por exemplo, o reticulado hexagonal e o reticulado $\mathbb{Z}^2$ em $\mathbb{R}^2$ e o reticulado cúbico em $\mathbb{R}^3$ são bem arredondados, assim como o reticulado hipercúbico e o reticulado A_4 em $\mathbb{R}^4$, que são importantes em quase cristalografia (quasicrystallography).

Como estamos interessados em construir reticulados com boa densidade de empacotamento nas dimensões 2 e 3 via polinômios, vamos analisar aqui em quais condições reticulados construídos via polinômios nessas dimensões são bem arredondados. Para isso, nos baseamos na teoria do artigo [1].

Construímos reticulados que são gerados por vetores cujas coordenadas são as raízes de um polinômio com coeficientes inteiros e raízes reais.

Usaremos as fórmulas de Girard para provar a independência linear dos vetores considerados e para obter a norma euclidiana em termos dos coeficientes do polinômio. Uma vantagem é que podemos estabelecer condições envolvendo tais coeficientes a fim de aumentar o número de vetores mínimos do reticulado.

4.1 Definição e propriedades elementares

Nesta seção faremos um breve estudo sobre os reticulados, definindo-os e apresentando suas principais propriedades.

Definição 4.1. Sejam $\{v_1, v_2, ..., v_m\}$ vetores linearmente independentes do $\mathbb{R}^n$. O conjunto de pontos

$$\Lambda = \left\{ x = \sum_{i=1}^{m} \lambda_i v_i, \lambda_i \in \mathbb{Z} \right\}$$

é chamado reticulado de dimensão m e $\{v_1, v_2, ..., v_m\}$ é chamado de base do reticulado.

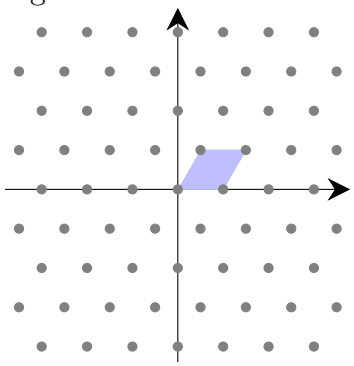
Definição 4.2. Seja $\{v_1, \ldots, v_m\}$ uma base de um reticulado. O paralelepípedo formado pelos pontos

$$\lambda_1 v_1 + \cdots + \lambda_m v_m, \ 0 \leqslant \lambda_i < 1$$

é chamado de **paralelepípedo fundamental** ou **região fundamental do reticulado**.

Exemplo 4.3. O reticulado Λ_{hex} é gerado pelos vetores $e_1 = (1, 0)$, $e_2 = (\frac{1}{2}, \frac{\sqrt{3}}{2})$ e é chamado de reticulado hexagonal.

Figura 4.1: Região fundamental do reticulado Λ_{hex}



Fonte: Elaborada pelo autor

Dado $n \geq 2$, utilizando elementos de $\mathbb{Z}^{n+1}$, definimos o reticulado A_n como

$$A_n = \{(x_0, \cdots, x_n) \in \mathbb{Z}^{n+1} : x_0 + \cdots + x_n = 0\}.$$

Considerando $n \geq 3$, definimos

$$D_n = \{(x_1, \cdots, x_n) \in \mathbb{Z}^n : x_1 \cdots x_n \equiv 0 \mod 2\}.$$

Em outras palavras, o reticulado D_n é formado por todos os elementos de $\mathbb{Z}^n$ tal que a soma das coordenadas é par.

Definição 4.4. Seja $\{v_1, \ldots, v_m\}$ uma base de Λ. Se $v_i = (v_{i1}, \ldots, v_{in})$, para $i = 1, \cdots, m$, a matriz

$$M = \begin{pmatrix} v_{11} & v_{12} & \ldots & v_{1n} \\ v_{21} & v_{22} & \ldots & v_{2n} \\ & & \ddots & \\ v_{m1} & v_{m2} & \ldots & v_{mn} \end{pmatrix}$$

é chamada de **matriz geradora** do reticulado Λ. A matriz $G = MM^t$ é chamada de **matriz de Gram** do reticulado, onde t denota a transposição.

Assim, os pontos do reticulado são formados por

$$\Lambda = \{\mathbf{x} = \lambda M \mid \lambda \in \mathbb{Z}^m\}.$$

Definição 4.5. O **determinante** do reticulado Λ é definido como sendo o determinante da matriz G, ou seja,

$$\det(\Lambda) = \det(G).$$

Um reticulado Λ é dito ter posto máximo se $m = n$, e neste caso M é uma matriz quadrada. Assim,

$$\det(\Lambda) = (\det(M))^2.$$

Definição 4.6. Para reticulados de posto máximo, a raiz quadrada do determinante do reticulado é o volume da região fundamental, também chamado **volume do reticulado**, e denotado por $Vol(\Lambda)$.

É importante observar que o mesmo reticulado pode ser representado por mais de uma matriz, e o fato de dois reticulados terem o mesmo determinante não é suficiente para que eles sejam isomorfos.

Definição 4.7. Dois reticulados $\Lambda_1,\ \Lambda_2 \subset \mathbb{R}^n$ de posto n são ditos **semelhantes** ou **equivalentes** se existe uma matriz ortogonal A, de ordem n com entradas em $\mathbb{R}$, e uma constante real α tal que $\Lambda_1 = \alpha A \Lambda_2$.

Exemplo 4.8. Os reticulados

$$\Lambda_1 = \left\{ \begin{pmatrix} 6 & 3 \\ 0 & 12 \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \lambda_2 \end{pmatrix} \mid \lambda_1,\ \lambda_2 \in \mathbb{Z} \right\} \text{ e}$$

$$\Lambda_2 = \left\{ \begin{pmatrix} 2 & 1 \\ 0 & 4 \end{pmatrix} \begin{pmatrix} \lambda_3 \\ \lambda_4 \end{pmatrix} \mid \lambda_3, \lambda_4 \in \mathbb{Z} \right\}$$

do $\mathbb{R}^2$ são semelhantes, pois

$$\begin{pmatrix} 6 & 3 \\ 0 & 12 \end{pmatrix} = 3 \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 0 & 4 \end{pmatrix}.$$

Em outras palavras, reticulados semelhantes têm a mesma configuração mas não a mesma escala.

Exemplo 4.9. É possível mostrar que os reticulados A_2 e o reticulado hexagonal Λ_{hex} são equivalentes [22].

Definição 4.10. Um **empacotamento esférico**, ou simplesmente um empacotamento no $\mathbb{R}^n$, é uma distribuição de esferas de mesmo raio no $\mathbb{R}^n$ de forma que a interseção de quaisquer duas esferas tenha no máximo um ponto. Um empacotamento reticulado é um empacotamento em que o conjunto dos centros das esferas formam um reticulado Λ no $\mathbb{R}^n$. Além disso, $\rho = \frac{1}{2}\min\{||v|| : v \in \Lambda_f, v \neq 0\}$ é o maior raio para o qual é possível distribuir esferas centradas nos pontos de Λ e obter um empacotamento, este raio é então chamado de **raio de empacotamento.**

Seja $\Lambda \subset \mathbb{R}^n$ um reticulado. Denotando por $B(\rho)$ a esfera com centro na origem e raio ρ, podemos obter uma expressão para calcular a densidade de empacotamento de Λ. Temos que

$$\Delta(\Lambda) = \frac{\text{volume da região coberta por uma esfera}}{\text{volume da região fundamental}} = \frac{Vol(B(\rho))}{Vol(\Lambda)} = \frac{Vol(B(1))(\rho)^n}{Vol(\Lambda)}.$$

Como o valor de $Vol(B(1))$ é conhecido, podemos reduzir nosso estudo ao cálculo de $\frac{\rho^n}{Vol(\Lambda)}$ que definiremos a seguir.

Definição 4.11. Seja $\Lambda \subset \mathbb{R}^n$ um reticulado. Definimos a **densidade de centro** de Λ por

$$\delta(\Lambda) = \frac{\rho^n}{Vol(\Lambda)},$$

onde ρ é o raio de empacotamento de Λ e $Vol(\Lambda)$ seu volume.

Um dos problemas de empacotamento esférico de um reticulado no $\mathbb{R}^n$ é encontrar o empacotamento com maior densidade de centro. Na dimensão um, temos que os pontos de coordenadas inteiras da reta formam um $\mathbb{Z}$-reticulado cuja a densidade de centro é a melhor possível dada por $\delta = 1$.

Na dimensão dois o reticulado A_2 é o de maior densidade de centro, dada por $\delta = \frac{1}{\sqrt{12}} \approx 0,28868$.

Na dimensão 3 o reticulado D_3 é o de maior densidade de centro, sendo essa $\delta = \frac{1}{\sqrt{32}} \approx 0,17678$.

É conhecido e provado que as densidades de centro dos reticulados A_1, A_2, D_3, D_4, D_5, E_6, E_7, E_8 e Λ_{24}, de dimensões 1 a 8 e 24, respectivamente, são ótimas. Para outras dimensões não se sabe as ótimas.

4.2 Reticulados densos via polinômios

Nesta seção utilizamos a referência [1] e apresentamos como construir reticulados com maior densidade de centro nas dimensões 2 e 3.

4.2.1 Reticulados em $\mathbb{R}^2$ via polinômios de grau 2 com raízes reais distintas

Para dar início à construção, seja $f(x) = x^2 + ax + b \in \mathbb{Z}[x]$ com $a^2 - 4b > 0$ e raízes distintas $\alpha, \beta \in \mathbb{R}$. Agora, sejam os vetores $v_1 = (\alpha, \beta)$ e $v_2 = (\beta, \alpha)$ e consideremos o reticulado definido por

$$\Lambda_f = \{\lambda_1 v_1 + \lambda_2 v_2 : \lambda_1, \lambda_2 \in \mathbb{Z}\} \ ,$$

ou seja, um reticulado gerado por v_1 e v_2.

Como $\alpha, \beta \in \mathbb{R}$, então a matriz geradora de Λ_f é dada por

$$M = \begin{pmatrix} \alpha & \beta \\ \beta & \alpha \end{pmatrix}.$$

Observe que, pela Definição 4.11,

$$\delta(\Lambda_f) = \frac{\rho^2}{Vol(\Lambda_f)} = \frac{\rho^2}{|\det(M)|},$$

onde $\rho = \frac{1}{2}\min\{||x|| : x \in \Lambda_f, x \neq 0\}$. Por outro lado,

$$\alpha = \frac{-a + \sqrt{a^2 - 4b}}{2}$$

e

$$\beta = \frac{-a - \sqrt{a^2 - 4b}}{2}.$$

Daí,

$$\begin{aligned}
|\det(M)| &= \left|\det \begin{pmatrix} \alpha & \beta \\ \beta & \alpha \end{pmatrix}\right| \\
&= \left|\left(\frac{-a + \sqrt{a^2 - 4b}}{2}\right)^2 - \left(\frac{-a - \sqrt{a^2 - 4b}}{2}\right)^2\right| \\
&= \left|\frac{a^2 - 2a\sqrt{a^2 - 4b} + a^2 - 4b}{4} - \frac{a^2 + 2a\sqrt{a^2 - 4b} + a^2 - 4b}{4}\right| \\
&= |-a\sqrt{a^2 - 4b}| \\
&= |a|\sqrt{a^2 - 4b}.
\end{aligned}$$

Assim,

$$\delta(\Lambda_f) = \frac{\rho^2}{|a|\sqrt{a^2 - 4b}},$$

o que é suficiente para enunciar o próximo resultado.

Proposição 4.12. *Sejam $f(x) = x^2 + ax + b \in \mathbb{Z}[x]$, com $a^2 - 4b > 0$ e $\Lambda_f \subset \mathbb{R}^2$ o reticulado de base $\{(\alpha, \beta), (\beta, \alpha)\}$, onde α e β são raízes distintas de f. Então*

$$\delta(\Lambda_f) = \frac{\rho^2}{|a|\sqrt{a^2 - 4b}},$$

onde $\rho = \frac{1}{2}\min\{||x|| : x \in \Lambda_f, x \neq 0\}$.

No entanto, não é prático identificar numericamente o parâmetro ρ na Proposição 4.12. Deste modo, é necessário que adotemos uma estratégia que simplifique tal tarefa.

Proposição 4.13. *Sejam $f(x) = x^2+ax+b \in \mathbb{Z}[x]$, com $a^2-4b > 0$ e $\Lambda_f \subset \mathbb{R}^2$ o reticulado de base $\{(\alpha, \beta), (\beta, \alpha)\}$, onde α e β são raízes distintas de f. Se $v = z_1(\alpha, \beta) + z_2(\beta, \alpha) \in \Lambda_f$, com $z_1, z_2 \in \mathbb{Z}$, então*

$$||v||^2 = a^2({z_1}^2 + {z_2}^2) - 2b(z_1 - z_2)^2.$$

Demonstração. Basta fazer uma verificação direta. Se $\Delta = a^2 - 4b$, então

$$\begin{aligned}
||v||^2 &= {z_1}^2\alpha^2 + 2\alpha\beta(z_1z_2) + {z_2}^2\beta^2 + {z_1}^2\beta^2 + 2\alpha\beta(z_1z_2) + {z_2}^2\alpha^2 \\
&= (\alpha^2 + \beta^2)({z_1}^2 + {z_2}^2) + 4\alpha\beta(z_1z_2) \\
&= \left(\left(\frac{-a + \sqrt{\Delta}}{2}\right)^2 + \left(\frac{-a - \sqrt{\Delta}}{2}\right)^2\right)({z_1}^2 + {z_2}^2) + 4\left(\frac{-a + \sqrt{\Delta}}{2}\right)\left(\frac{-a - \sqrt{\Delta}}{2}\right)(z_1z_2) \\
&= \frac{2a^2 + 2|\Delta|}{4}({z_1}^2 + {z_2}^2) + 4\left(\frac{a^2 - |\Delta|}{4}\right)(z_1z_2) \\
&= (a^2 - 2b)({z_1}^2 + {z_2}^2) - 4b(z_1z_2) \\
&= a^2({z_1}^2 + {z_2}^2) - 2b(z_1 - z_2)^2.
\end{aligned}$$

□

Exemplo 4.14. Sejam $f(x) = x^2 - x$ e Λ_f o reticulado gerado por $(1,0)$ e $(0,1)$. Se $v = z_1(1,0) + z_2(0,1) \in \Lambda_f$, com $z_1, z_2 \in \mathbb{Z}$, então

$$||v||^2 = ({z_1}^2 + {z_2}^2)$$

cujo valor mínimo 1 é atingido quando $z_1 = \pm 1$ e $z_2 = 0$ ou quando $z_1 = 0$ e $z_2 = \pm 1$. Assim,

$$\delta(\Lambda_f) = \frac{\left(\frac{1}{2}\right)^2}{1} = \frac{1}{4}.$$

Exemplo 4.15. Sejam $f(x) = x^2 - 4x + 3$ e Λ_f o reticulado gerado por $(3,1)$ e $(1,3)$. Se $v = z_1(3,1) + z_2(1,3) \in \Lambda_f$, com $z_1, z_2 \in \mathbb{Z}$, então

$$||v||^2 = 16({z_1}^2 + {z_2}^2) - 6({z_1}^2 - {z_2}^2)^2 = 2(8({z_1}^2 + {z_2}^2) - 3(z_1 - z_2)^2)$$

cujo valor mínimo 8 é atingido quando $z_1 = 1$ e $z_2 = -1$ ou quando $z_1 = -1$ e $z_2 = 1$. Assim,

$$\delta(\Lambda_f) = \frac{\left(\frac{\sqrt{8}}{2}\right)^2}{4\sqrt{4}} = \frac{8}{32} = \frac{1}{4},$$

O próximo resultado identifica uma condição para a e b de modo que o reticulado obtido tenha a maior densidade de centro possível em $\mathbb{R}^2$.

Teorema 4.16. *[25] Sejam $f(x) = x^2 + ax + b \in \mathbb{Z}[x]$, com $a^2 - 4b > 0$ e $\Lambda_f \subset \mathbb{R}^2$ o reticulado de base $\{(\alpha,\beta),(\beta,\alpha)\}$, onde α e β são raízes reais distintas de f. Se $a^2 = 6b$ $(b > 0)$ ou $a^2 = -2b$ $(b < 0)$, então Λ_f possui a maior densidade de centro possível para a dimensão 2.*

Demonstração. Prossegue-se por verificação direta.

Seja $v = z_1(\alpha,\beta) + z_2(\beta,\alpha) \in \Lambda_f$, com $z_1, z_2 \in \mathbb{Z}$. Daí,

$$||v||^2 = a^2({z_1}^2 + {z_2}^2) - 2b(z_1 - z_2)^2 = 2b(3({z_1}^2 + {z_2}^2) - (z_1 - z_2)^2)\ ,$$

que assume menor valor $4b$ quando $z_1 = 1$ e $z_2 = 0$. Daí,

$$\delta(\Lambda_f) = \begin{cases} \dfrac{\left(\dfrac{\sqrt{4b}}{2}\right)^2}{\sqrt{6b}\sqrt{2b}} = \dfrac{1}{2\sqrt{3}} & \text{se } b > 0 \\ \\ \dfrac{\left(\dfrac{\sqrt{4b}}{2}\right)^2}{\sqrt{-2b}\sqrt{-6b}} = \dfrac{1}{2\sqrt{3}} & \text{se } b < 0 \end{cases}$$

o que conclui a demonstração. □

Assim, conseguimos um método via polinômios de grau 2, para gerar reticulados com boa densidade de centro em $\mathbb{R}^2$.

A seguir, explicitamos o Teorema 4.16 para $a = -18$ e $a = 24$ com $b > 0$.

Exemplo 4.17. Sejam $f(x) = x^2-18x+54$, $\alpha, \beta \in \mathbb{R}$ as raízes de f e $v = z_1v_1+z_2v_2 \in \Lambda_f$, onde $v_1 = (\alpha, \beta)$ e $v_2 = (\beta, \alpha)$. Temos que

$$||v||^2 = 324({z_1}^2 + {z_2}^2) - 108(z_1 - z_2)^2,$$

que assume o valor mínimo 216. Temos ainda que

$$|\det(M)| = |a|\sqrt{a^2 - 4b} = 18\sqrt{108} = 108\sqrt{3}.$$

Portanto,

$$\delta(\Lambda_f) = \frac{(\frac{\sqrt{216}}{2})^2}{108\sqrt{3}} = \frac{54}{108\sqrt{3}} = \frac{1}{2\sqrt{3}},$$

que é a densidade ótima para dimensão 2.

Exemplo 4.18. Sejam $f(x) = x^2+24x+96$, $\alpha, \beta \in \mathbb{R}$ as raízes de f e $v = z_1v_1+z_2v_2 \in \Lambda_f$, $v_1 = (\alpha, \beta)$ e $v_2 = (\beta, \alpha)$. Temos que

$$||v||^2 = 576({z_1}^2 + {z_2}^2) - 192(z_1 - z_2)^2$$

assume valor mínimo 384. Temos ainda que,

$$|\det(M)| = |a|\sqrt{a^2 - 4b} = 24\sqrt{192} = 192\sqrt{3}.$$

Com isso

$$\delta(\Lambda_f) = \frac{(\frac{\sqrt{384}}{2})^2}{192\sqrt{3}} = \frac{96}{192\sqrt{3}} = \frac{1}{2\sqrt{3}},$$

que é a densidade ótima para dimensão 2.

A seguir, explicitamos o Teorema 4.16 para $a = 2$ e $b < 0$.

Exemplo 4.19. Sejam $f(x) = x^2+4x-8$, $\alpha, \beta \in \mathbb{R}$ as raízes de f e $v = z_1v_1+z_2v_2 \in \Lambda_f$, $v_1 = (\alpha, \beta)$ e $v_2 = (\beta, \alpha)$. Temos que

$$||v||^2 = 16({z_1}^2 + {z_2}^2) + 16(z_1 - z_2)^2$$

assume valor mínimo 32. Temos ainda que,

$$|\det(M)| = |a|\sqrt{a^2 - 4b} = 4\sqrt{48} = 16\sqrt{3}.$$

Com isso

$$\delta(\Lambda_f) = \frac{(\frac{\sqrt{32}}{2})^2}{16\sqrt{3}} = \frac{8}{16\sqrt{3}} = \frac{1}{2\sqrt{3}},$$

que é a densidade ótima para dimensão 2.

4.2.2 Reticulados de dimensão 3 via polinômios de grau 3 com raízes reais

Aqui apresentamos uma construção de reticulados de dimensão 3 via polinômios de grau 3 com 3 raízes reais. O Teorema 4.26 mostrará que é possível obter reticulados que são versões rotacionadas do reticulado D_3 via tais polinômios, que como vimos é o reticulado com a melhor densidade de centro na dimensão 3.

Seja $f(x) = x^3 + ax^2 + bx + c$ um polinômio mônico com coeficientes inteiros e sejam $\alpha, \beta, \gamma \in \mathbb{C}$ as raízes de f. Queremos que f possua somente raízes reais.

Para tal, primeiramente precisaremos de uma restrição para os parâmetros a, b, c do polinômio $f(x) = x^3 + ax^2 + b + c \in \mathbb{Z}[x]$ para que este tenha raízes reais. A proposição a seguir nos dá essa restrição.

Proposição 4.20. *([25]) Seja $f(x) = x^3 + ax^2 + bx + c$ um polinômio mônico com coeficientes inteiros. Para que as raízes de f sejam reais é necessário e suficiente que*

$$a^2 - 3b > 0 \quad e \quad (\sqrt{a^2 - 3b})^3 > \left| \frac{2a^3 - 9ab + 27c}{2} \right|.$$

Demonstração. Uma condição necessária e suficiente para que as raízes de f sejam todas reais é que sua derivada se anule em dois pontos distintos e que a função f aplicada nestes pontos tenham sinais distintos. Assim, se $f(x) = x^3 + ax^2 + bx + c$, com $a, b, c \in \mathbb{Z}$ temos que sua derivada é dada por $f'(x) = 3x^2 + 2ax + b$ cujas raízes são

$$x_1 = \frac{-a - \sqrt{a^2 - 3b}}{3} \quad \text{e} \quad x_2 = \frac{-a + \sqrt{a^2 - 3b}}{3}.$$

Daí, segue que $a^2 - 3b > 0$ deve ser um número positivo. Agora,

$$\begin{aligned} f(x_1) &= x_1^3 + ax_1^2 + bx_1 + c \\ &= \left(\frac{-a - \sqrt{a^2 - 3b}}{3} \right)^3 + a \left(\frac{-a - \sqrt{a^2 - 3b}}{3} \right)^2 + b \left(\frac{-a - \sqrt{a^2 - 3b}}{3} \right) + c \\ &= \frac{1}{27}(2a^3 + 2(\sqrt{a^2 - 3b})^3 - 9ab + 27c) \end{aligned}$$

e, portanto, $f(x_1) > 0$ se, e somente se,

$$(\sqrt{a^2 - 3b})^3 > \frac{-2a^3 + 9ab - 27c}{2}.$$

Analogamente,

$$f(x_2) = \frac{1}{27}(2a^3 - 2(\sqrt{a^2 - 3b})^3 - 9ab + 27c)$$

e, portanto, $f(x_2) < 0$ se, e somente se,

$$(\sqrt{a^2 - 3b})^3 > \frac{2a^3 - 9ab + 27c}{2}.$$

Logo, para que as raízes de f sejam reais devemos ter

$$a^2 - 3b > 0 \quad \text{e} \quad (\sqrt{a^2 - 3b})^3 > \left| \frac{2a^3 - 9ab + 27c}{2} \right|,$$

como queríamos. □

Sejam $\alpha, \beta, \gamma \in \mathbb{R}$ as raízes de $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$ que satisfazem as condições da Proposição 4.20. Podemos definir $\Lambda_f \subset \mathbb{R}^3$ como o reticulado gerado pela base $\{v_1, v_2, v_3\}$, onde $v_1 = (\alpha, \beta, \gamma)$, $v_2 = (\gamma, \alpha, \beta)$ e $v_3 = (\beta, \gamma, \alpha)$. Temos que uma matriz geradora de Λ_f será

$$M = \begin{pmatrix} \alpha & \beta & \gamma \\ \gamma & \alpha & \beta \\ \beta & \gamma & \alpha \end{pmatrix}, \tag{4.1}$$

desde que $\det(M) \neq 0$, e sua densidade de centro será dada por:

$$\delta(\Lambda_f) = \frac{\rho^3}{|\det(M)|},$$

onde ρ é o raio de empacotamento de Λ_f.

Da mesma forma como para dimensão 2, queremos encontrar expressões para o calcular ρ e $\det(M)$. No resultado a seguir veremos uma expressão para o cálculo de $\det(M)$.

Proposição 4.21. *([25]) Seja $f(x) = x^3 + ax^2 + bx + c$ um polinômio mônico com coeficientes inteiros e sejam α, β, γ as raízes de f, satisfazendo a condição da Proposição 4.20. Se Λ_f é o reticulado obtido a partir de f com matriz geradora M como dada em (4.1), então o módulo do determinante de M é dado por*

$$|\det(M)| = |a(a^2 - 3b)|.$$

Demonstração. Temos que o determinante de M será dado por

$$\det(M) = \alpha^3 + \beta^3 + \gamma^3 - 3\alpha\beta\gamma.$$

Das relações de Girard, apresentada em (2.40), segue que:

$$\begin{cases} \alpha + \beta + \gamma = -a \\ \alpha\beta + \alpha\gamma + \beta\gamma = b \\ \beta\gamma\alpha = -c \end{cases}$$

Assim,

$$(\alpha + \beta + \gamma)^2 = \alpha^2 + \beta^2 + \gamma^2 + 2(\alpha\beta + \alpha\gamma + \beta\gamma) = a^2,$$

logo,

$$\alpha^2 + \beta^2 + \gamma^2 = a^2 - 2b. \tag{4.2}$$

Como $\alpha + \beta + \gamma = -a$, multiplicando o lado esquerdo da Equação (4.2) por $\alpha + \beta + \gamma$ e o lado direito por $-a$ teremos

$$\begin{aligned} &\alpha^3 + \beta^3 + \gamma^3 + \alpha\beta^2 + \beta\alpha^2 + \beta\gamma^2 + \gamma\alpha^2 + \gamma\beta^2 \\ &= \alpha^3 + \beta^3 + \gamma^3 + \alpha\beta(\alpha + \beta) + \alpha\gamma(\alpha + \gamma) + \beta\gamma(\beta + \gamma) \\ &= \alpha^3 + \beta^3 + \gamma^3 - \alpha\beta(\gamma + a) - \alpha\gamma(\beta + a) - \beta\gamma(\alpha + a) \\ &= \alpha^3 + \beta^3 + \gamma^3 - 3\alpha\beta\gamma - a(\alpha\beta + \alpha\gamma + \beta\gamma) \\ &= -a(a^2 - 2b). \end{aligned}$$

Logo,

$$\alpha^3 + \beta^3 + \gamma^3 - 3\alpha\beta\gamma = -a(a^2 - 2b) + ab = -a^3 + 3ab.$$

Portanto, $|\det(M)| = |a(a^2 - 3b)|$ o que prova a proposição. □

Exemplo 4.22. Sejam $f(x) = x^3 - 9x^2 + 23x - 15$ um polinômio de grau 3 com raízes reais α, β, γ. Se Λ_f é o reticulado com base $\{v_1, v_2, v_3\}$ e matriz geradora M, segue pela Proposição 4.21 que

$$|\det(M)| = |a(a^2 - 3b)| = 108.$$

Agora, veremos um resultado que nos dará uma expressão para o cálculo da norma de um vetor de Λ_f.

Proposição 4.23. *([25]) Seja $f(x) = x^3 + ax^2 + bx + c$ um polinômio mônico com coeficientes inteiros e sejam α, β, γ as raízes de f, satisfazendo a condição da Proposição 4.20. Se Λ_f é o reticulado de dimensão 3 gerado pela base $\{v_1, v_2, v_3\}$, onde $v_1 = (\alpha, \beta, \gamma)$, $v_2 = (\gamma, \alpha, \beta)$, $v_3 = (\beta, \gamma, \alpha)$, e $v \in \Lambda_f$, tal que $v = z_1v_1 + z_2v_2 + z_3v_3$, com $z_1, z_2, z_3 \in \mathbb{Q}$. Então,*

$$||v||^2 = (a^2 - 2b)(z_1^2 + z_2^2 + z_3^2) + 2b(z_1z_2 + z_1z_3 + z_2z_3).$$

Demonstração. Temos que:

$$\begin{aligned} v &= z_1v_1 + z_2v_2 + z_3v_3 \\ &= z_1(\alpha, \beta, \gamma) + z_2(\gamma, \alpha, \beta) + z_3(\beta, \gamma, \alpha) \\ &= (\alpha z_1 + \gamma z_2 + \beta z_3, \beta z_1 + \alpha z_2 + \gamma z_3, \gamma z_1 + \beta z_2 + \alpha z_3). \end{aligned}$$

Então,

$$\begin{aligned} ||v||^2 &= (\alpha z_1 + \gamma z_2 + \beta z_3)^2 + (\beta z_1 + \alpha z_2 + \gamma z_3)^2 + (\gamma z_1 + \beta z_2 + \alpha z_3)^2 \\ &= (\alpha^2 + \beta^2 + \gamma^2)(z_1^2 + z_2^2 + z_3^2) + 2(\alpha\beta + \alpha\gamma + \beta\gamma)(z_1z_2 + z_1z_3 + z_2z_3) \\ &= (a^2 - 2b)(z_1^2 + z_2^2 + z_3^2) + 2b(z_1z_2 + z_1z_3 + z_2z_3), \end{aligned}$$

como queríamos mostrar. Observe que para obter a última igualdade usamos as relações de Girard, apresentadas em (4.2). □

A partir das Proposições 4.21 e 4.23, a densidade de centro do reticulado Λ_f é dada por

$$\delta(\Lambda_f) = \frac{\left(\frac{\sqrt{\psi}}{2}\right)^3}{|a(a^2 - 3b)|}, \tag{4.3}$$

onde $\psi = \min\{||v||^2 = (a^2 - 2b)(z_1^2 + z_2^2 + z_3^2) + 2b(z_1z_2 + z_2z_3 + z_1z_3) \mid z_1, z_2, z_3 \in \mathbb{Z}\}$.

Exemplo 4.24. Nas condições do Exemplo 4.22, seja $v = z_1v_1 + z_2v_2 + z_3v_3 \in \Lambda_f$. Pela Proposição 4.23 segue que

$$||v||^2 = 35(z_1^2 + z_2^2 + z_3^2) + 46(z_1z_2 + z_1z_3 + z_2z_3)$$

e, este vetor assume o valor mínimo 24 quando fazemos $z_1 = 1$, $z_2 = -1$ e $z_3 = 0$. Portanto, a densidade de centro do reticulado Λ_f é dada por

$$\delta(\Lambda_f) = \frac{(\sqrt{6})^3}{108} = \frac{\sqrt{6}}{18}.$$

Exemplo 4.25. Sejam $f(x) = x^3 + 3x^2 + x - 1$ e Λ_f o reticulado de base

$$\{(-\sqrt{2} - 1, \sqrt{2} - 1, -1), (-1, -\sqrt{2} - 1, \sqrt{2} - 1), (\sqrt{2} - 1, -1, -\sqrt{2} - 1)\}.$$

Se $v = z_1(-\sqrt{2}-1, \sqrt{2}-1, -1) + z_2(-1, -\sqrt{2}-1, \sqrt{2}-1) + z_3(\sqrt{2}-1, -1, -\sqrt{2}-1) \in \Lambda_f$, com $z_1, z_2, z_2 \in \mathbb{Z}$, então

$$||v||^2 = 7({z_1}^2 + {z_2}^2 + {z_3}^2) + 2(z_1z_2 + z_1z_3 + z_2z_3)$$

cujo valor mínimo 7 é atingido quando $z_i = \pm 1$ e $z_j = z_k = 0$, com $i, j, k \in \{1, 2, 3\}$ e $i \neq j$, $i \neq k$ e $j \neq k$. Assim,

$$\delta(\Lambda_f) = \frac{\left(\frac{\sqrt{7}}{2}\right)^3}{18} = \frac{7\sqrt{7}}{144}.$$

O próximo resultado identifica uma condição para a, b e c de modo que o reticulado obtido tenha a maior densidade de centro possível em $\mathbb{R}^3$.

Teorema 4.26. *([25]) Seja $f(x) = x^3+ax^2+bx+c$ um polinômio mônico com coeficientes inteiros e sejam α, β, γ as raízes de f, satisfazendo a condição da Proposição 4.20. Se f satisfaz*

$$a^2 = 4b,$$

então o reticulado Λ_f gerado pela base $\{v_1, v_2, v_3\}$, onde $v_1 = (\alpha, \beta, \gamma)$, $v_2 = (\gamma, \alpha, \beta)$ e $v_3 = (\beta, \gamma, \alpha)$, possui densidade de centro ótima.

Demonstração. Pela Proposição (4.23) temos que

$$\begin{aligned} ||v||^2 &= (a^2 - 2b)(z_1^2 + z_2^2 + z_3^2) + 2b(z_1z_2 + z_1z_3 + z_2z_3) \\ &= 2b(z_1^2 + z_2^2 + z_3^2 + z_1z_2 + z_1z_3 + z_2z_3). \end{aligned}$$

Observe que esta forma quadrática assume valor mínimo $2b$ quando $z_1 = 1$ e $z_2 = z_3 = 0$. Logo,

$$\psi = \min\{||v||^2 = (a^2-2b)(z_1^2+z_2^2+z_3^2)+2b(z_1z_2+z_2z_3+z_1z_3) \mid z_1, z_2, z_3 \in \mathbb{Z}\} = 2b. \quad (4.4)$$

Agora, pela Proposição 4.21, temos

$$|\det(M)| = |a(a^2 - 3b)| = |ab|. \quad (4.5)$$

Por, (4.3), (4.4) e (4.5) segue que a densidade de centro de Λ_f será dada por

$$\delta(\Lambda_f) = \frac{\left(\frac{\sqrt{2b}}{2}\right)^3}{|ab|} = \frac{1}{4\sqrt{2}} \approx 0,17678,$$

que é a mesma densidade de centro do reticulado D_3. Portanto, Λ_f possui densidade de centro ótima para dimensão 3. □

Exemplo 4.27. Sejam $f(x) = x^3 - 6x^2 + 9x - 1$ com raízes reais α, β, γ, Λ_f um reticulado de dimensão 3 gerado pela base $\{v_1, v_2, v_3\}$, onde $v_1 = (\alpha, \beta, \gamma)$, $v_2 = (\gamma, \alpha, \beta)$, $v_3 = (\beta, \gamma, \alpha)$, e $v \in \Lambda_f$, tal que $v = z_1v_1 + z_2v_2 + z_3v_3$, com $z_1, z_2, z_3 \in \mathbb{Q}$. Temos que

$$||v||^2 = 18(z_1^2 + z_2^2 + z_3^2) + 18(z_1z_2 + z_1z_3 + z_2z_3),$$

que assume o valor mínimo 18, quando $z_1 = 1$ e $z_2 = z_3 = 0$. Temos ainda que

$$|\det(M)| = |a(a^2 - 3b)| = 54.$$

Portanto,

$$\delta(\Lambda_f) = \frac{\left(\frac{3\sqrt{2}}{2}\right)^3}{54} = \frac{\sqrt{2}}{8} = \frac{1}{4\sqrt{2}} \approx 0,17677,$$

que é a densidade de centro ótima para essa dimensão.

4.3 Reticulados bem arredondados

Nesta seção investigamos sob quais condições reticulados em $\mathbb{R}^2$ e $\mathbb{R}^3$ construídos via polinômios com coeficientes inteiros e raízes reais são *bem arredondados*, do inglês, *well-rounded*. Em outras palavras, vamos analisar a propriedade do bem arredondamento nos reticulados construídos através do método apresentado na Seção 4.2.1 e Seção 4.2.2.

Tal investigação é importante para o estudo de empacotamentos esféricos, problemas referentes ao número de contato (do inglês, *kissing number*) e outras propriedades de reticulados que são interessantes na aplicação prática.

Para o seu desenvolvimento, as referências utilizadas foram [9], [14], [13] e [26].

4.3.1 Definições iniciais

Definição 4.28. Seja Λ um reticulado de posto completo em $\mathbb{R}^d$, com $d \geq 2$. O **conjunto dos vetores mínimos** de Λ é definido por

$$S(\Lambda) = \{\mathbf{x} \in \Lambda : \|\mathbf{x}\|^2 = |\Lambda|\},$$

onde $|\Lambda| = \min\{\|\mathbf{x}\|^2 : \mathbf{x} \in \Lambda, \mathbf{x} \neq 0\}$

Definição 4.29. Seja Λ um reticulado de posto completo em $\mathbb{R}^d$, com $d \geq 2$. Dizemos que Λ é um **reticulado *bem arredondado*** se $S(\Lambda)$ gera $\mathbb{R}^d$.

Observação 4.30. A propriedade de bem arredondamento é preservada com relação à semelhança. Em outras palavras, se dois reticulados de posto completo Λ_1, $\Lambda_2 \subset \mathbb{R}^n$ são semelhantes e Λ_1 é *bem arredondado* então Λ_2 também é *bem arredondado*.

Lema 4.31 ([14], p. 192)**.** *Seja $\Lambda \subset \mathbb{R}^2$ um reticulado de posto completo. Então Λ contém 2, 4 ou 6 vetores mínimos e é bem arredondado se, e somente se, $\#S(\Lambda) = 4$ ou $\#S(\Lambda) = 6$. Além disso, $\#S(\Lambda) = 6$ se, e somente se, Λ é semelhante ao reticulado hexagonal Λ_{hex}.*

Demonstração. Seja $v \in S(\Lambda)$. Como $-v \in \Lambda$ e $||v||^2 = ||-v||^2$, então $-v \in S(\Lambda)$. Observe ainda que se $v_1, v_2 \in S(\Lambda)$ são vetores distintos e linearmente dependentes, ou seja, $v_1 = \lambda v_2$ para algum $\lambda \in \mathbb{R}$, então v_1 e v_2 são opostos entre si, uma vez que

$$||v_1|| = ||\lambda v_2|| = |\lambda|||v_2|| \Rightarrow |\lambda| = 1 \Rightarrow \lambda = \pm 1.$$

Como v_1 e v_2 são distintos, segue que $\lambda = -1$. Dessa forma, $S(\Lambda)$ possui um número par de elementos e contém dois vetores linearmente independentes se, e somente se, $\#S(\Lambda) \geq 4$.

Sejam $v, u \in S(\Lambda)$ vetores distintos e suponhamos que o ângulo θ entre estes dois vetores seja tal que $0 < \theta < \dfrac{\pi}{3}$. Pela Lei dos cossenos,

$$||v-u||^2 = ||v||^2 - 2||v||||u||cos(\theta) + ||u||^2 < ||v||^2 - ||v||||u|| + ||u||^2$$

e como $||v|| = ||u||$, uma vez que são vetores de $S(\Lambda)$, temos

$$||v-u||^2 < ||v||^2 = ||u||^2,$$

o que é uma contradição, visto que encontramos um vetor $v - u \in \Lambda$, com $v - u \neq 0$ e norma menor do que $||v|| = ||u||$. Portanto o ângulo entre dois vetores distintos de

$S(\Lambda)$ é necessariamente maior ou igual à $\frac{\pi}{3}$. Por definição, os vetores de $S(\Lambda)$ estão compreendidos na circunferência de centro na origem e raio $|\Lambda|$, então

$$\frac{2\pi}{\#S(\Lambda)} \geq \frac{\pi}{3}.$$

A desigualdade acima também nos permite concluir que $\#S(\Lambda) \leq 6$. Assim,

$$\#S(\Lambda) = 2, 4 \text{ ou } 6.$$

Se $\#S(\Lambda) = 2$, então Λ não é bem arredondado, uma vez que dois vetores linearmente dependentes não geram $\mathbb{R}^2$. Portanto Λ é bem arredondado se, e somente se, $\#S(\Lambda) = 4$ ou 6.

Nos resta garantir que se $\#S(\Lambda) = 6$, então $\Lambda \sim \Lambda_{hex}$. De fato, suponhamos que Λ possua 6 vetores de norma mínima, então necessariamente $S(\Lambda) = \{\pm v_1, \pm v_2, \pm v_3\}$ e podemos escolher um par de vetores v_i e v_j, com $1 \leq i, j \leq 3$ e $i \neq j$, tal que o ângulo entre esses vetores seja $\frac{\pi}{3}$, por conseguinte, v_i e v_j são linearmente independentes. Logo, como Λ tem posto 2, os vetores v_i e v_j formam uma base para Λ. Dessa forma, Λ_{hex} pode ser obtido através de rotação e dilatação dos vetores escolhidos, o que nos permite concluir a primeira implicação, isto é, $\Lambda \sim \Lambda_{hex}$.

Em contrapartida, se $\Lambda \sim \Lambda_{hex}$, então $\#S(\Lambda) = \#S(\Lambda_{hex}) = 6$, concluindo o resultado. □

4.3.2 Reticulados bem arredondados via polinômios de grau 2

Na Seção 4.2.1 apresentamos um método via polinômios de grau 2, para gerar reticulados com boa densidade de centro em $\mathbb{R}^2$.

A ideia agora será investigar, em quais condições, reticulados obtidos via polinômios de grau 2 são bem arredondados. Para facilitar a notação, defina

$$\begin{array}{rcl} g : \mathbb{Z}^2 & \to & \mathbb{R}_+ \\ v & \mapsto & g(v) = g(x_1, x_2) = a^2(x_1^2 + x_2^2) - 2b(x_1 - x_2)^2, \end{array}$$

isto é, $\|v\|^2 = g(x_1, x_2)$. A fim de identificar quando $g(x_1, x_2)$ assume valor mínimo, é suficiente verificar seus valores quando x_1e x_2 variam entre 0, 1 e -1. Observe que

(i) $g(\pm 1, 0) = g(0, \pm 1) = a^2 - 2b$;

(ii) $g(1, 1) = g(-1, -1) = 2a^2$;

(iii) $g(-1, 1) = g(1, -1) = 2a^2 - 8b$.

Sabemos do Lema 4.31 que $\Lambda_f \subset \mathbb{R}^2$ é bem arredondado se, e somente se, $|S(\Lambda)| = 4$ ou $|S(\Lambda)| = 6$. Neste último caso, Λ_f tem a maior densidade de empacotamento em dimensão 2. Observe que $|S(\Lambda)| = 4$ se, e somente se, $min\{a^2 - 2b, 2a^2, 2a^2 - 8b\} = a^2 - 2b$, isto é, $a^2 - 2b \leq 2a^2$ e $a^2 - 2b \leq 2a^2 - 8b$. Portanto, $-2b \leq a^2$ e $6b \leq a^2$. Quando $b \geq 0$ (respectivamente, $b < 0$) a desigualdade acima é satisfeita se, e somente se, $a^2 \geq 6b$ (respectivamente, $a^2 \geq -2b$). É fácil ver que $|S(\Lambda)| = 6$ se, e somente se, $a^2 - 2b = 2a^2$ ou $a^2 - 2b = 2a^2 - 8b$ que é equivalente a $a^2 = -2b$ ($b < 0$)ou $a^2 = 6b$ ($b > 0$). Consequentemente, provamos o seguinte teorema.

Teorema 4.32. *Seja $f(x) = x^2 + ax + b \in \mathbb{Z}[x]$,com $a \neq 0$, um polinômio com raízes reais distintas. Se $\alpha, \beta \in \mathbb{R}$ são as raízes distintas de $f(x)$, então o reticulado Λ_f gerado pela base $\{(\alpha, \beta), (\beta, \alpha)\}$ é bem arredondado se, e somente se, $a^2 \geq -2b$ (com $b < 0$) ou $a^2 \geq 6b$ (com $b \geq 0$).*

4.3.3 Reticulados bem arredondados via polinômios de grau 3

Na Seção 4.2.2 conseguimos um método via polinômios de grau 3 para gerar reticulados com boa densidade de centro em $\mathbb{R}^3$.

O objetivo agora é estabelecer em quais condições entre os coeficientes de um polinômio de grau 3 e raízes reais para que o reticulado correspondente seja bem arredondado.

Teorema 4.33. *Seja $f(x) = x^3+ax^2+bx+c \in \mathbb{Z}[x]$, com $a \neq 0$. Se $\alpha, \beta, \gamma \in \mathbb{R}$ são as raízes reais distintas de $f(x)$, então o reticulado Λ_f gerado pela base $\{(\alpha, \beta, \gamma), (\gamma, \alpha, \beta), (\beta, \gamma, \alpha)\}$ é bem arredondado se, e somente se, $a^2 \geq 4b$ (com $b \geq 0$) ou $a^2 \geq -b$ (com $b < 0$). Além disso, Λ_f tem a maior densidade de empacotamento na dimensão 3 se, e somente se, $a^2 = 4b$.*

Demonstração.

$$\begin{array}{rcl} g : \mathbb{Z}^3 & \to & \mathbb{R}_+ \\ v & \mapsto & g(v) = g(x_1, x_2, x_3) = (a^2 - 2b)(x_1^2 + x_2^2 + x_3^2) + 2b(x_1x_2 + x_1x_3 + x_2x_3), \end{array}$$

isto é, $\|v\|^2 = g(x_1, x_2, x_3)$. Para identificar quando $g(x_1, x_2, x_3)$ assume valor mínimo é suficiente verificar seus valores quando x_1, x_2 e x_3 variam entre 0, 1 e -1. Então,

(i) $g(\pm 1, 0, 0) = g(0, \pm 1, 0) = g(0, 0, \pm 1) = a^2 - 2b$;

(ii) $g(1, 1, 0) = g(-1, -1, 0) = g(1, 0, 1) = g(-1, 0, -1) = g(0, 1, 1) = g(0, -1, -1) = 2a^2 - 2b$;

(iii) $g(1, -1, 0) = g(-1, 1, 0) = g(1, 0, -1) = g(-1, 0, 1) = g(0, 1, -1) = g(0, -1, 1) = 2a^2 - 6b$;

(iv) $g(1, 1, 1) = g(-1, -1, -1) = 3a^2$;

(v) $g(1, \pm 1, -1) = g(1, -1, 1) = g(-1, \pm 1, 1) = g(-1, 1, -1) = 3a^2 - 8b$.

Seja $m = \min\{a^2 - 2b, 2a^2 - 2b, 2a^2 - 6b, 3a^2, 3a^2 - 8b\}$. Observe que, se

$$a^2 - 2b = m, \tag{4.6}$$

então Λ_f é bem arredondado, pois os vetores $v \in \Lambda_f$ tal que $\|v\|^2 = a^2-2b$ são linearmente independentes. Por outro lado, vamos mostrar que (4.6) também é uma condição necessária para Λ_f ser bem arredondado. Primeiro, Observe que $3a^2-8b = (a^2-2b)+(2a^2-6b) > m$ e $2a^2 - 2b = a^2 + (a^2 - 2b) > m$. Assim,

$$3a^2 - 8b,\ 2a^2 - 2b \neq m. \tag{4.7}$$

Suponha que Λ_f é bem arredondado e (4.6) não é válida, isto é,

$$a^2 - 2b \neq m. \tag{4.8}$$

Claramente, $b \neq 0$ pois caso contrário $a^2 - 2b = m$. Se $b > 0$, então $2a^2 - 6b < 3a^2$. De (4.7) e (4.8), segue que $2a^2 - 6b = m$. Como os vetores $v \in \Lambda_f$ tal que $\|v\|^2 = 2a^2 - 6b$ são linearmente dependentes, segue que o conjunto $S(\Lambda_f)$ não gera $\mathbb{R}^3$, o que é uma contradição. Se $b < 0$,então $m < 2a^2 - 2b < 2a^2 - 6b$. Novamente, de (4.7) e (4.8), segue que $m = 3a^2$ e então o conjunto $S(\Lambda_f)$ não gera $\mathbb{R}^3$, o que é uma contradição. Portanto, Λ_f é bem arredondado, se e somente se, $a^2 - 2b = m$.

Quando $b \geq 0$ (respectivamente, $b < 0$) a última equação é satisfeita se, e somente se, if $a^2 - 2b \leq 2a^2 - 6b$ (respectivamente, $a^2 - 2b \leq 3a^2$), isto é, se, e somente se, $a^2 \geq 4b$ ($a^2 \geq -b$). Quando $a^2 = -b$ ou $a^2 = 4b$, segue que $|S(\Lambda_f)|$ aumenta. Isto significa que Λ_f tem maior densidade de centro quando as igualdades são satisfeitas.

Observe que se $a^2 = -b$, onde $b < 0$, então

$$\delta(\Lambda_f) = \frac{(\sqrt{3(-b)}/2)^3}{a(4b)} = \frac{3\sqrt{3}}{32} \approx 0,16238.$$

Por outro lado, se $a^2 = 4b$, então

$$\delta(\Lambda_f) = \frac{(\sqrt{4b}/2)^3}{|ab|} = \frac{1}{4\sqrt{2}} \approx 0,7679$$

correspondendo a maior densidade de centro na dimensão 3. □

5 Sugestão de atividades

Apresentamos neste capítulo sugestões de problemas e atividades relacionadas aos assuntos abordados neste trabalho para serem desenvolvidas com os alunos do Ensino Médio.

Inicialmente, sugerimos uma coletânea de dez problemas sobre polinômios que foram extraídos das provas da American Mathematics Competitions (AMC), do American Invitational Mathematics Examination (AIME) e do vestibular do Instituto Tecnológico de Aeronáutica (ITA) [1]. Em seguida, sugerimos um problema que pode ser modelado por uma equação polinomial do 3º grau. Finalmente, sugerimos duas atividades interligadas sobre reticulados que exploram a relação entre álgebra e geometria.

5.1 Coletânea de problemas sobre polinômios

Sugerimos a aplicação desta coletânea na 3ª série do Ensino Médio dentro de um Itinerário Formativo para aprofundamento em Matemática ou numa classe de preparação para olimpíadas de Matemática. Os problemas extraídos das provas da AMC e do AIME foram adaptados de [2]. Já as questões do ITA foram adaptadas de [23]. Sugestões de resolução podem ser encontradas no Apêndice A.

Essas questões auxiliam no desenvolvimento destas habilidades:

i. (EF09MA09) Compreender os processos de fatoração de expressões algébricas, com base em suas relações com os produtos notáveis, para resolver e elaborar problemas que possam ser representados por equações polinomiais do 2o grau.

ii. (EM13MAT302) Construir modelos empregando as funções polinomiais de 1o ou 2o graus, para resolver problemas em contextos diversos, com ou sem apoio de tecnologias digitais

Problema 1 (AMC 2017): Para certos números reais a, b, e c, o polinômio $g(x) = x^3 + ax^2 + x + 10$ possui três raízes distintas, e cada raiz de $g(x)$ é também uma raiz do polinômio $f(x) = x^4 + x^3 + bx^2 + 100x + c$. Qual o valor de $f(1)$?

(A) -9009 **(B)** -8008 **(C)** -7007 **(D)** -6006 **(E)** -5005

Problema 2 (AMC 2021): Um polinômio quadrático com coeficientes reais e coeficiente líder 1 é chamado de *desrespeitoso* se a equação $p(p(x)) = 0$ é satisfeita por

[1] AMC e AIME são exames que consistem nas duas primeiras etapas, de um total de quatro, para a formação da equipe dos Estados Unidos para a Olimpíada Internacional de Matemática (IMO). Já o ITA é uma instituição universitária pública ligada ao Comando da Aeronáutica e especializado nas áreas de ciência e tecnologia no Setor Aeroespacial.

exatamente três números reais. Entre todos os polinômios quadráticos desrespeitosos, há um único polinômio $\tilde{p}(x)$ para o qual a soma das raízes é maximizada. Qual o valor de $\tilde{p}(1)$?

(A) $\frac{5}{16}$ **(B)** $\frac{1}{2}$ **(C)** $\frac{5}{8}$ **(D)** 1 **(E)** $\frac{9}{8}$

Problema 3 (AMC 2021) Sejam $Q(z)$ e $R(z)$ os únicos polinômios tais que $z^{2021} + 1 = (z^2 + z + 1)Q(z) + R(z)$ e o grau de $R(z)$ é menor do que 2. Qual o valor de $R(z)$?

(A) $-z$ **(B)** -1 **(C)** 2021 **(D)** $z + 1$ **(E)** $2z + 1$

Problema 4 (AMC 2021): Seja $g(x)$ um polinômio com coeficiente líder 1 cujas três raízes são os inversos das três raízes de $f(x) = x^3 + ax^2 + bx + c$, com $1 < a < b < c$. Qual o valor de $g(1)$ em termos de a, b, e c?

(A) $\frac{1+a+b+c}{c}$ **(B)** $1 + a + b + c$ **(C)** $\frac{1+a+b+c}{c^2}$ **(D)** $\frac{a+b+c}{c^2}$ **(E)** $\frac{1+a+b+c}{a+b+c}$

Problema 5 (AIME 2022): Os polinômios quadráticos $P(x)$ e $Q(x)$ têm coeficiente líder 2 e -2, respectivamente. Os gráficos de ambos passam pelos pontos $(16, 54)$ e $(20, 53)$. Determine $P(0) + Q(0)$.

Problema 6 (AIME 2021): Há números reais a, b, c, e d tais que -20 é uma raiz de $x^3 + ax + b$ e -21 é uma raiz de $x^3 + cx^2 + d$. Esses dois polinômios compartilham uma raiz complexa $m + \sqrt{n} \cdot i$, onde m e n sõ inteiros positivos e $i = \sqrt{-1}$. Determine $m + n$.

Problema 7 (ITA 2020): Considere o polinômio $p(X) = X^3 - mX^2 + X + 5 + n$, sendo m, n números reais fixados. Sabe-se que toda raiz $z = a + bi$, com $a, b \in \mathbb{R}$, da equação $p(z) = 0$ satisfaz a igualdade $a = mb^2 + nb - 1$. Então, a soma dos quadrados das raízes de $p(z) = 0$ é igual a **(A)** 6 **(B)** 7 **(C)** 8 **(D)** 9 **(E)** 10

Problema 8 (ITA 2020): Seja $p(x) = ax^4 + bx^3 + cx^2 + dx + e$ um polinômio com coeficientes reais. Sabendo que:

I. $p(x)$ é divisível por $x^2 - 4$;

II. a soma das raízes de $p(x)$ é igual a 1;

III. o produto das raízes de $p(x)$ é igual a 3;

IV. $p(-1) = \frac{-15}{4}$;

então, $p(1)$ é igual a

(A) $\frac{-17}{2}$ **(B)** $\frac{-19}{4}$ **(C)** $\frac{-3}{2}$ **(D)** $\frac{9}{4}$ **(E)** $\frac{9}{2}$

Problema 9 (ITA 2022): Considere o polinômio $p(z) = z^4 - 6z^3 + 14z^2 - 6z + 13$ e observe que $p(i) = 0$. Considere no plano complexo o quadrilátero cujos vértices são as raízes de $p(z)$. Podemos afirmar que a área desse quadrilátero é

(A) 4 **(B)** 6 **(C)** 8 **(D)** 9 **(E)** 10

Problema 10 (ITA 2015): Considere o polinômio p dado por $p(x) = 2x^3 + ax^2 + bx - 16$, com $a, b \in \mathbb{R}$. Sabendo-se que p admite raiz dupla e que 2 é uma raiz de p, então o valor de $b - a$ é igual a

(A) -36 **(B)** -12 **(C)** 6 **(D)** 12 **(E)** 24

5.2 Resolvendo um problema pelo método apresentado no Capítulo 3 e pelas fórmulas de Cardano

Sugerimos a aplicação deste problema na 3ª série do Ensino Médio dentro de um Itinerário Formativo para aprofundamento em Matemática.

O caminho escolhido para solucionar o problema apresentado nesta seção passa pela resolução de uma equação do tipo $Y^3 + pY + q = 0$. Ao chegarmos nessa equação, nós a resolveremos, primeiramente, pelo método apresentado no Capítulo 3, e em seguida, pelas fórmulas de Cardano.

Esse problema auxilia o aluno no desenvolvimento das competências específicas 3 e 4 para o Ensino Médio e que são explicitadas a seguir:

i. Utilizar estratégias, conceitos, definições e procedimentos matemáticos para interpretar, construir modelos e resolver problemas em diversos contextos, analisando a plausibilidade dos resultados e a adequação das soluções propostas, de modo a construir argumentação consistente.

ii. Compreender e utilizar, com flexibilidade e precisão, diferentes registros de representação matemáticos (algébrico, geométrico, estatístico, computacional etc.), na busca de solução e comunicação de resultados de problemas.

Problema: Uma caixa de papelão de formato cúbico teve sua altura reduzida, passando a ter o formato de um bloco retangular de volume 9 cm^3. Com a redução de sua altura houve também uma redução de 24 cm^2 em sua área total. Qual a altura da caixa após a redução?

Solução: Seja Y a aresta da caixa cúbica. Com a redução da altura da caixa houve a redução de uma área equivalente a área de quatro retângulos congruentes com um de seus lados medindo Y, logo cada um desses retângulos possui área 6 cm^2 e seu outro lado mede $\frac{6}{Y}$. Assim, as dimensões do bloco retangular são Y, Y e $Y - \frac{6}{Y}$, sendo esse último a sua altura. Como o volume do bloco retangular é 9 cm^3, temos que

$$Y \cdot Y \cdot \left(Y - \frac{6}{Y}\right) = 9,$$

logo, o valor de Y deve ser dado pela equação $Y^3 - 6Y - 9 = 0$.

Resolvendo a equação pelo método apresentado no Capítulo 3: Reescrevendo a equação como $Y^3 - 3rs + rs(r + s) = 0$, temos que $-3rs = -6$ e $rs(r + s) = -9$, então $rs = 2$ e $r + s = \frac{-9}{2}$. Assim, r e s são as raízes de $t^2 + \frac{9}{2} + 2 = 0$, o que nos dá $r = \frac{-1}{2}$ e $s = -4$. Como $r \neq s$, a raiz real da equação é

$$-\sqrt[3]{\frac{-1}{2}} \cdot \sqrt[3]{-4}\left(\sqrt[3]{\frac{-1}{2}} + \sqrt[3]{-4}\right) = -\sqrt[3]{2}\left(\sqrt[3]{\frac{-1}{2}} + \sqrt[3]{-4}\right) = -(-1 - 2) = 3.$$

Portanto, a altura da caixa após a redução é $Y - \frac{6}{Y} = 3 - 2 = 1$ cm.

Resolvendo a equação pelas fórmulas de Cardano: Como $p = -6$ e $q = -9$, temos

$$\sqrt[3]{\frac{9}{2} + \sqrt{\frac{81}{4} + \frac{(-216)}{27}}} + \sqrt[3]{\frac{9}{2} - \sqrt{\frac{81}{4} + \frac{(-216)}{27}}},$$

então

$$\sqrt[3]{\frac{9}{2}+\sqrt{\frac{49}{4}}}+\sqrt[3]{\frac{9}{2}-\sqrt{\frac{49}{4}}}=\sqrt[3]{\frac{9}{2}+\frac{7}{2}}+\sqrt[3]{\frac{9}{2}-\frac{7}{2}}=\sqrt[3]{8}+\sqrt[3]{1}=3.$$

Portanto, a altura da caixa após a redução é $Y-\frac{6}{Y}=3-2=1$ cm.

5.3 Atividades sobre reticulados

As duas atividades aqui sugeridas são complementares uma da outra e foram elaboradas de forma a haver condições de aplica-las já na 1ª série do Ensino Médio. Logo, a linguagem e notação utilizadas são simplificadas. Um exemplo disso é a notação utilizada na Atividade 2 onde evitamos propositadamente o uso da palavra "vetor" e a notação usual de vetores, preferindo usar uma linguagem mais leve e uma notação mais simples aceita pelo software GeoGebra [2]. A Atividade 2 pode ser desenvolvida em um nível maior de profundidade do que foi originalmente proposto, explorando os conceitos de vetor e as transformações geométricas resultantes das operações com os mesmos. O professor poderá fazer as devidas adaptações na linguagem, notação e desenvolvimento dessa atividade conforme o nível de conhecimento dos alunos permitir.

As habilidades desenvolvidas através dessas atividades são:

i. (EF07MA19) Realizar transformações de polígonos representados no plano cartesiano, decorrentes da multiplicação das coordenadas de seus vértices por um número inteiro.

ii. (EM13MAT302) Construir modelos empregando as funções polinomiais de 1o ou 2o graus, para resolver problemas em contextos diversos, com ou sem apoio de tecnologias digitais.

iii. (EM13MAT505) Resolver problemas sobre ladrilhamento do plano, com ou sem apoio de aplicativos de geometria dinâmica, para conjecturar a respeito dos tipos ou composição de polígonos que podem ser utilizados em ladrilhamento, generalizando padrões observados.

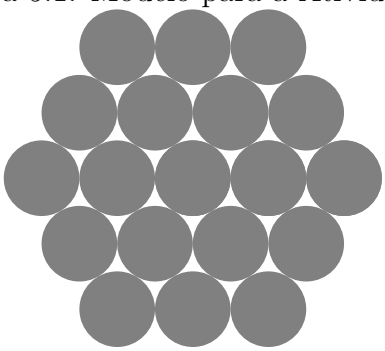
Orientações ao professor para realização da Atividade 1:
Atividade 1: Empacotamento esférico do plano.

Objetivo: O objetivo desta atividade é instigar os alunos à investigação e a construção de modelos a fim de resolver o problema proposto. Para isso, os alunos serão desafiados a dar resposta a seguinte questão: Como dispor discos idênticos no plano de modo a obter a maior densidade de empacotamento possível, sem que haja sobreposição de discos? Para responder a essa questão os alunos terão em mãos alguns discos de mesmo raio e a informação de que a maior proporção do plano que pode ser coberta sob tais condições é $\frac{\pi}{\sqrt{12}}\approx 0,907$.

Material:

- Pequenos discos de mesmo raio.
- Cópias da Figura 5.1 .

Figura 5.1: Modelo para a Atividade 1



Fonte: Elaborada pelo autor

Organização Divida os alunos em grupos distribuindo para cada grupo aproximadamente 20 discos de mesmo raio e então apresente aos alunos o texto a seguir para que leiam e tentem responder à questão apresentada.

Texto da **Atividade 1**: **Empacotamento esférico e transmissão de dados**

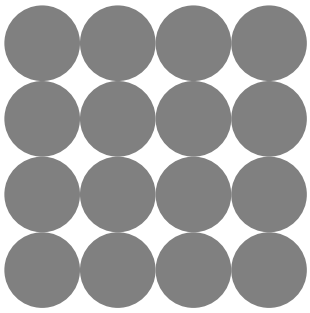
No processo de transmissão e recebimento de dados, em um sistema de comunicação digital, há interferências (ruídos) que podem prejudicar a comunicação entre o transmissor e o receptor dos sinais. Uma importante contribuição matemática à Teoria da Informação é o estudo do problema chamado empacotamento esférico que aplicado à teoria dos códigos corretores de erros fornece formas de minimizar os efeitos desses ruídos. Para isso, busca-se empacotar os sinais de transmissão dentro de *esferas* da forma mais densa possível. Para termos uma pequena noção do que isso significa vamos abordar o problema do empacotamento esférico do ponto de vista geométrico, considerando apenas o plano e o espaço. Sob esse ponto de vista, o problema do empacotamento esférico consiste em buscar uma maneira de dispor discos, no plano, ou esferas, no espaço, sem que haja sobreposição e de forma a cobrir a maior proporção possível do espaço em questão. Tal proporção é denominada densidade de empacotamento. Quando os discos são todos idênticos, a maior densidade de empacotamento do plano que se pode obter é $\frac{\pi}{\sqrt{12}} \approx 0,907$, o que significa que os discos cobrem aproximadamente $90,7\%$ do plano. De posse destas informações e seguindo as orientações do professor, responda: Como dispor discos idênticos no plano de modo a obter a maior densidade de empacotamento possível, sem que haja sobreposição de discos? (Nota: o termo *esferas*, em destaque, tem aqui um significado mais amplo do que o usual pois considera *esferas* para além do espaço tridimensional.)

Recomendações ao professor: É importante lembrar aos alunos que a extensão do plano é infinita e embora a quantidade de discos de que dispomos é finita, podemos imaginar que dispomos de uma quantidade infinita de discos para cobri-lo. Outro ponto a ser observado é que espera-se que os alunos construam a solução do problema de forma intuitiva o que pode ser favorecido pela manipulação dos discos distribuídos a cada grupo.

Desenvolvimento: Espera-se, inicialmente, que os alunos usem os discos que receberam, dispondo-os sobre uma superfície plana na tentativa de encontrar uma forma de cobrir o máximo possível dessa superfície e assim obter um protótipo do empacotamento esférico que corresponde à solução do problema. Espera-se que os alunos percebam que para cobrir a maior área possível, respeitando a condição de não sobrepor os discos, é necessário (mas não suficiente) que estes sejam dispostos no plano de forma que cada dois discos sejam

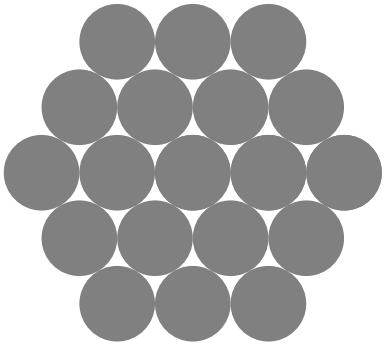
[2]Software de matemática dinâmica gratuito que combina, dentre outras coisas, álgebra e geometria.

Figura 5.2: Empacotamento com 4 discos ao redor de cada interstício



Fonte: Elaborada pelo autor

Figura 5.3: Empacotamento com 3 discos ao redor de cada interstício.



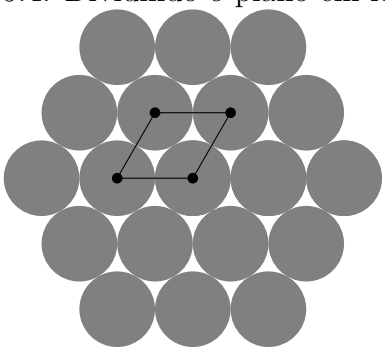
Fonte: Elaborada pelo autor

tangentes e não formem uma única fileira de discos. Dessa forma, haverá entre os discos espaços não cobertos por eles que são chamados de interstícios. Isso só pode ser feito de duas formas como exemplificado pela Fig. 5.2 e Fig. 5.3.

Observação: Caso nenhum dos grupos de alunos chegue a tal conclusão o professor pode tentar conduzi-los a ela sugerindo, por exemplo, que deixem o menor espaço possível entre os discos. Em último caso o professor poderá apresentar essas duas formas como candidatas ao empacotamento com densidade ótima.

A esta altura o professor pode questionar os alunos se um desses empacotamentos é mais denso do que o outro pedindo que justifiquem suas respostas. Não é difícil perceber que o empacotamento da Fig. 5.3 cobre uma proporção maior do plano, uma vez que os interstícios são menores do que o empacotamento da Fig. 5.2 Sendo assim, o empacotamento proposto na Fig. 5.3 parece ser um bom candidato à solução do problema. Para conferir se de fato esta é a solução, os alunos devem calcular a proporção do plano coberta por este empacotamento e verificar se tal proporção corresponde à proporção máxima apresentada no texto da **Atividade 1**. O professor pode auxiliar os alunos nessa tarefa instigando-os com a seguinte afirmação: Se dividirmos o plano em figuras iguais e de modo que a área coberta pelos discos em cada uma destas figuras seja a mesma, então a razão $\frac{\text{área coberta pelos discos em cada figura}}{\text{área de cada figura}}$ nos fornece a proporção do plano coberta pelos discos, ou seja, a densidade de empacotamento. Nesse momento o professor pode distribuir entre os alunos cópias da Fig. 5.1, desafiando-os a desenhar sobre elas algum polígono capaz de ladrilhar o plano, e de tal modo que as porções de cada polígono cobertas pelos discos da figura sejam sempre as mesmas. Há muitas maneiras de se fazer isso e todas elas levam a solução do problema. Apresentamos duas soluções possíveis:

Figura 5.4: Dividindo o plano em losangos



Fonte: Elaborada pelo autor

1. Uma maneira de dividir o plano em figuras iguais é usando losangos como o da Fig. 4, uma vez que é possível ladrilhar o plano pela translação dessa figura.

Observe que a área do losango coberta pelos discos corresponde a área de exatamente um destes discos (há quatro setores circulares de raio igual ao raio r do disco e a soma dos ângulos dos setores é 360°). Já a área do losango é igual a $2r \cdot r\sqrt{3} = 2\sqrt{3}r^2$. Logo, a densidade de empacotamento é igual a $\frac{\pi r^2}{2\sqrt{3}r^2} = \frac{\pi}{\sqrt{12}} \approx 0,907$ que é a densidade de empacotamento ótima para o plano. Portanto, dispor os discos no plano desta maneira nos permite obter a maior densidade de empacotamento possível usando discos idênticos.

2. Ligando os centros dos discos como na Fig. 5.5, obtemos um hexágono regular de lado $2r$ cuja área coberta pelos discos equivale a área de exatamente três discos (um disco inteiro no centro da figura mais dois discos repartidos em seis setores circulares de raio r com 120° cada um). Por translação do hexágono é possível ladrilhar o plano de forma que a área da região coberta pelos discos em cada hexágono é a mesma. Logo, a densidade desse empacotamento é $\frac{\text{área do hexágono coberta pelos discos}}{\text{área do hexágono}} = \frac{3\pi r^2}{6\sqrt{3}r^2} = \frac{\pi}{\sqrt{12}} \approx 0,907.$ que é a densidade de empacotamento ótima para o plano. Portanto, dispor os discos no plano desta desta maneira nos permite obter a maior densidade de empacotamento possível usando discos idênticos.

Figura 5.5: Dividindo o plano em hexágonos

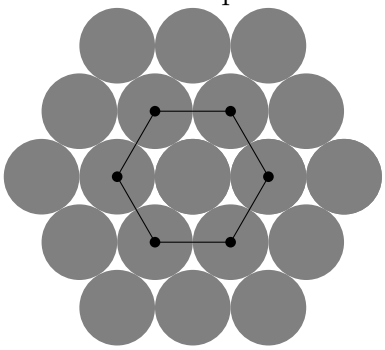


Figura 5.6: Dividindo o plano em hexágonos
Fonte: Elaborada pelo autor

Atividade 2: Construção de um reticulado denso em $\mathbb{R}^2$ via um polinômio de grau 2, usando o GeoGebra.

Orientações ao professor para realização da Atividade 2:

Considerações iniciais Depois de ter realizado a Atividade 1 os alunos devem ter percebido como foi importante, no processo de divisão do plano, desenhar os polígonos escolhidos tendo seus vértices coincidindo com os centros dos discos. O professor deve ressaltar que um modelo que considerasse apenas os centros dos discos seria suficiente para resolução dessa atividade e informar aos alunos que um tal modelo é chamado de reticulado. Além disso, deve-se ressaltar também que um reticulado com densidade de empacotamento ótima é chamado de reticulado denso e é exatamente a representação de um reticulado como esse que os alunos terão a oportunidade de construir nesta atividade.

Objetivo: O objetivo desta atividade é mostrar que um mesmo objeto matemático pode ser representado de diferentes formas sendo possível fazer a conversão de uma forma para outra. Para isso faremos uso de alguns conceitos básicos de geometria analítica que nos permitirão explicitar aos alunos a proximidade entre álgebra e geometria.

Material:

- lápis e caderno,
- software GeoGebra.

Organização: O professor distribuirá entre os alunos o seguinte roteiro de cinco passos contendo informações sobre a construção de uma representação de um reticulado usando o software GeoGebra.

Roteiro para construção da representação de um reticulado usando o geogebra:

Passo 1: Primeiro escolha dois números inteiros, m e n, que satisfaçam $m^2 = 6n$, se $n > 0$ ou $m^2 = -2n$, se $n < 0$. Com esses números escolhidos escreva o polinômio $x^2 + mx + n$ e determine suas raízes x_1 e x_2. Na janela de álgebra do software GeoGebra faça as duas entradas $A = (x_1, x_2)$ e $B = (x_2, x_1)$, gerando na janela de visualização os pontos A e B.

Passo 2: Na janela de álgebra faça as 25 entradas:

$$\begin{gathered} A+B,\ A+2B,\ A+3B,\ A+4B,\ A+5B,\\ 2A+B,\ 2A+2B,\ 2A+3B,\ 2A+4B,\ 2A+5B,\\ 3A+B,\ 3A+2B,\ 3A+3B,\ 3A+4B,\ 3A+5B,\\ 4A+B,\ 4A+2B,\ 4A+3B,\ 4A+4B,\ 4A+5B,\\ 5A+B,\ 5A+2B,\ 5A+3B,\ 5A+4B,\ 5A+5B. \end{gathered}$$

Essas 25 entradas devem gerar na janela de visualização 25 pontos de um reticulado, além dos pontos A e B que também pertencem ao reticulado.

Nota: Você pode gerar mais pontos do reticulado fazendo outras entradas do tipo $xA+yB$ com $x, y \in \mathbb{Z}$. Caso decida fazer isso procure seguir a mesma lógica das primeiras 25 entradas a fim de não deixar "buracos" no reticulado.

Passo 3: Com o auxílio da ferramenta de desenho "Polígono" desenhe um quadrilátero cujos vértices sejam pontos do reticulado e que não tenha pontos do reticulado em seu interior. Observe que esse quadrilátero é um losango.

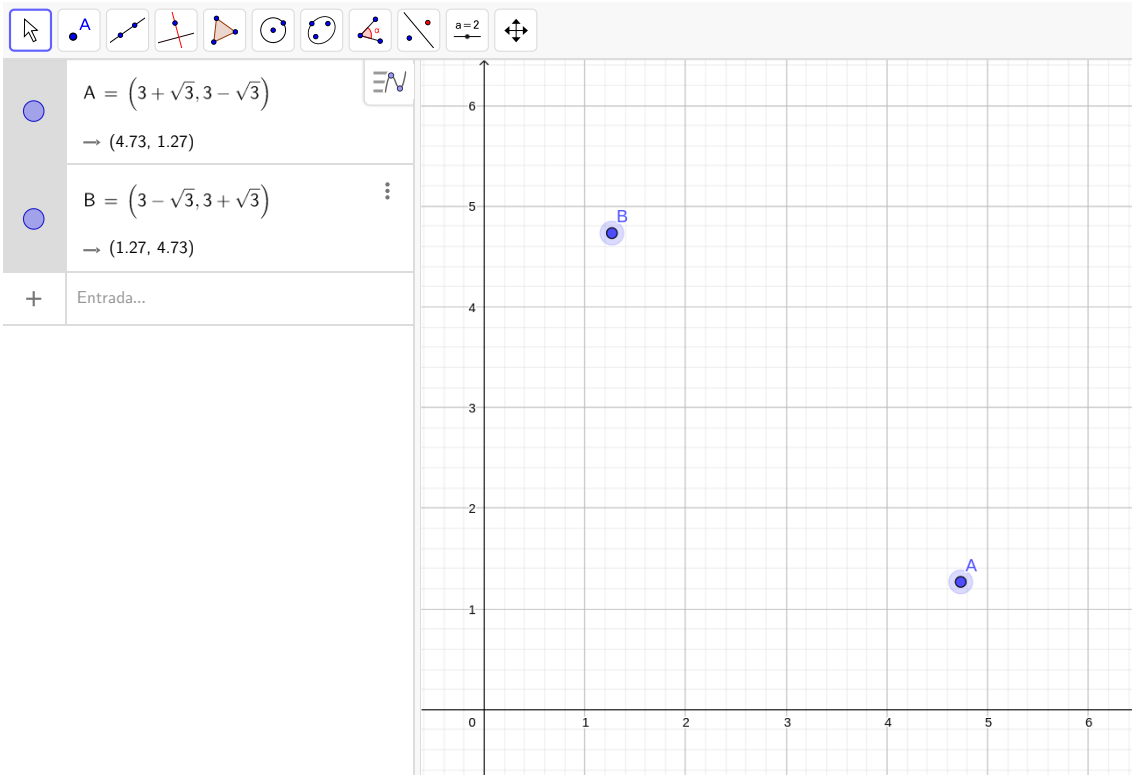
Passo 4: Com o auxílio da ferramenta de desenho "Círculo: Centro & Raio", desenhe quatro círculos cujos centros sejam cada um dos vértices do losango desenhado no **Passo 3** e cujos raios sejam a metade do lado desse losango.

Nota: Você pode repetir os Passos 3 e 4 para desenhar vários losangos justapostos e círculos sobre seus vértices (veja a Fig 5.11) a fim de melhor compreender o conceito de empacotamento do plano e seu ladrilhamento por meio de losangos.

Passo 5: Na janela de álgebra faça as entradas $a = Área(\text{“nome do polígono”})$ e $b = Área(\text{“nome do círculo”})$, onde no lugar de “nome do polígono” e “nome do círculo” você deve inserir o nome dado pelo GeoGebra a um dos losangos e a um dos círculos desenhados. Em seguida faça a entrada b/a (b dividido por a) para determinar o fator de empacotamento do reticulado desenhado. Observe que o valor obtido corresponde à densidade de empacotamento máxima para o plano conforme visto na **Atividade 1**.

Seguem algumas imagens para exemplificar a construção de um reticulado seguindo os passos deste roteiro para a escolha de $m = -6$ e $n = 6$, ou seja, para o polinômio $x^2 - 6x + 6$.

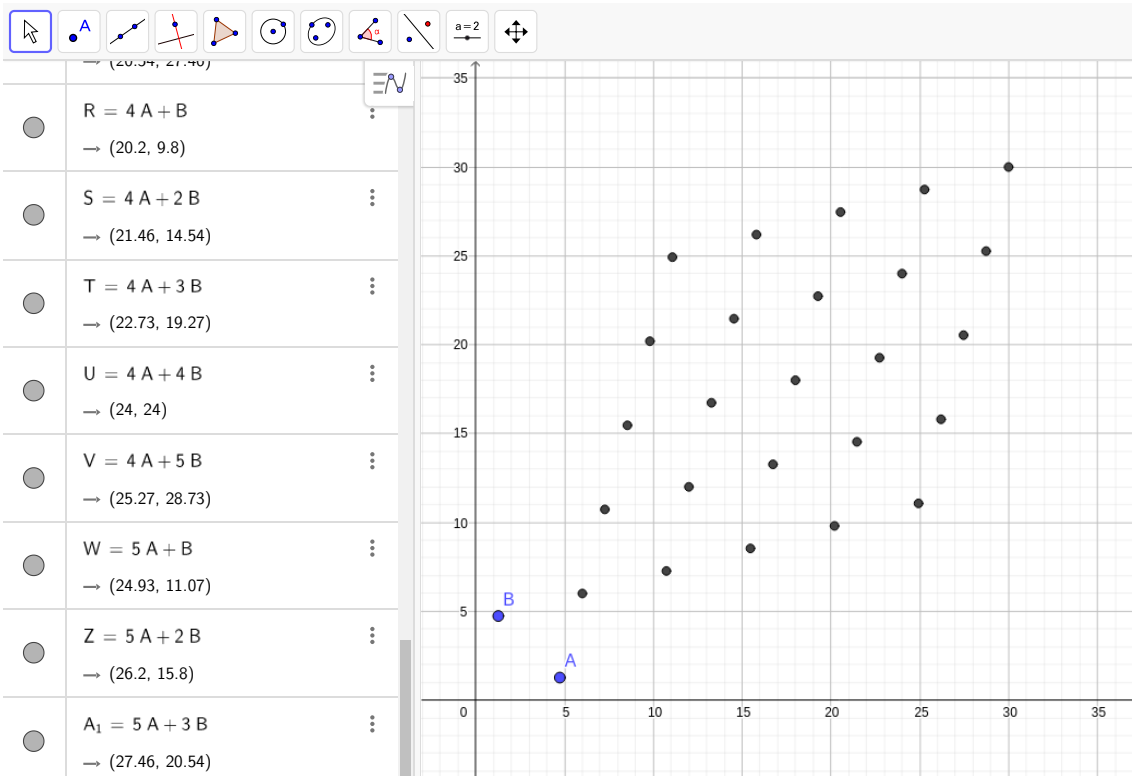
Figura 5.7: Gerando os pontos A e B conforme o **Passo 1**



Fonte: Elaborada pelo autor

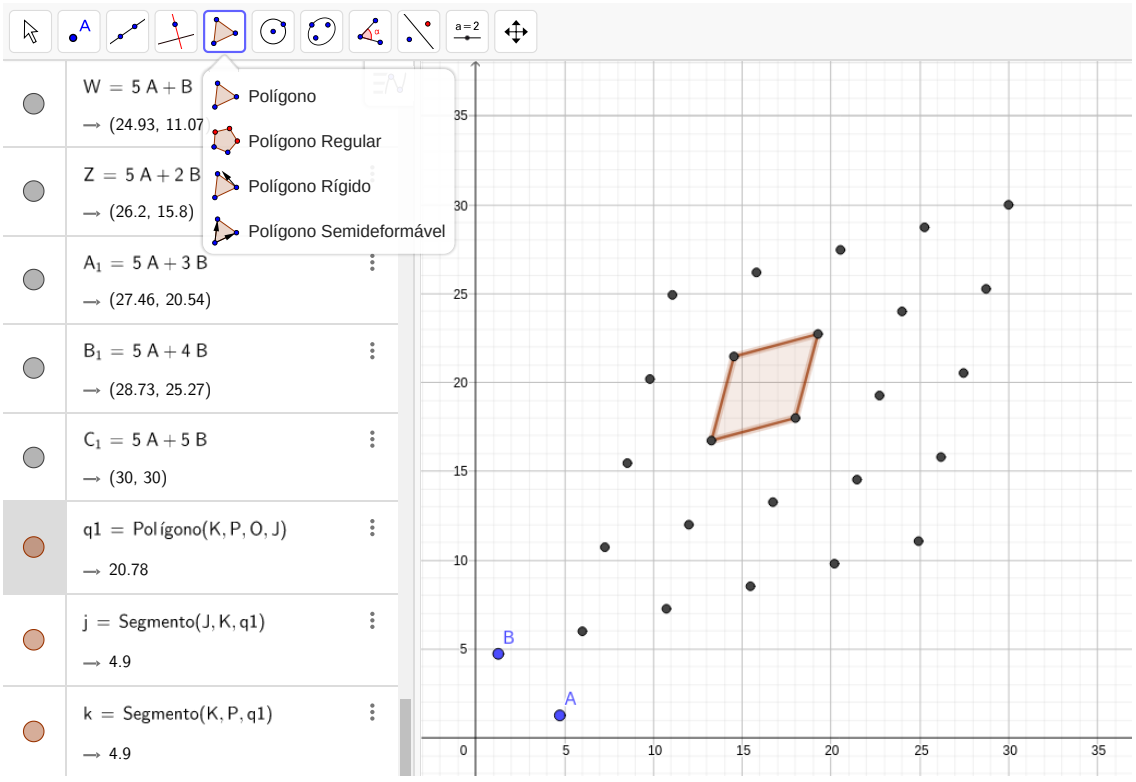
Observação 5.1. Sugerimos que as imagens exemplificando a construção do reticulado façam parte do roteiro dado aos alunos a fim de facilitar a realização da atividade.

Figura 5.8: Gerando 25 pontos do reticulado conforme o **Passo 2**



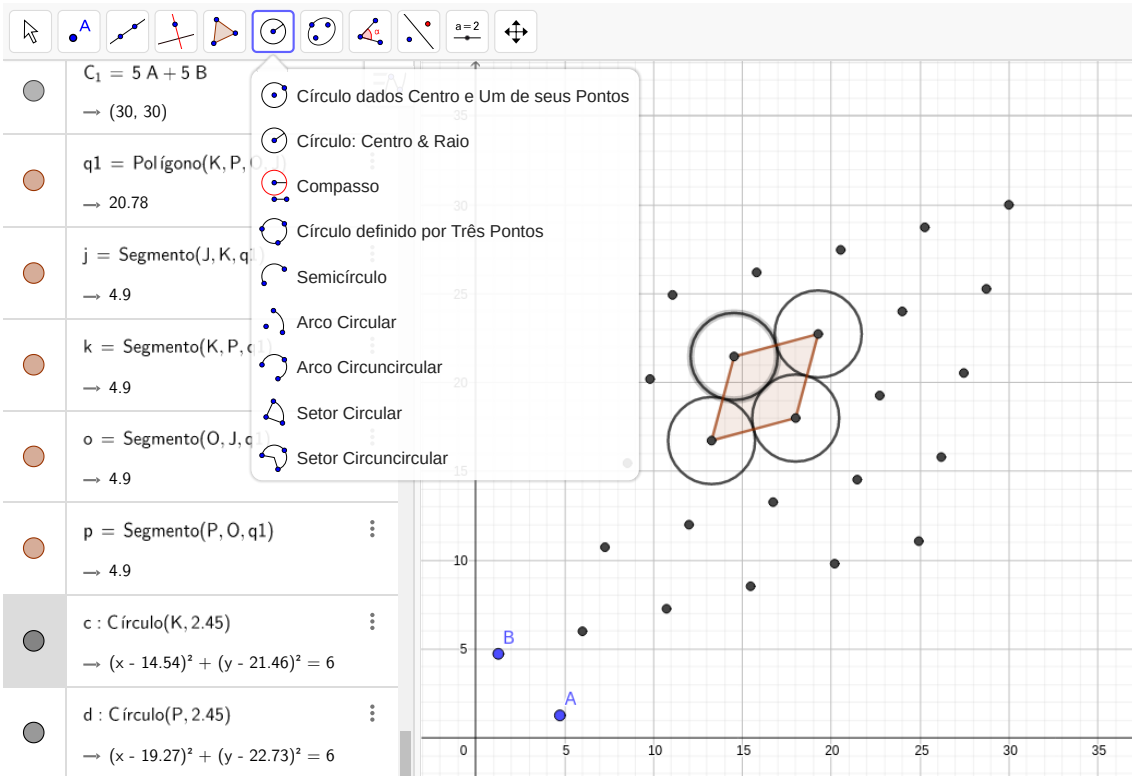
Fonte: Elaborada pelo autor

Figura 5.9: Desenhando um quadrilátero conforme o **Passo 3**



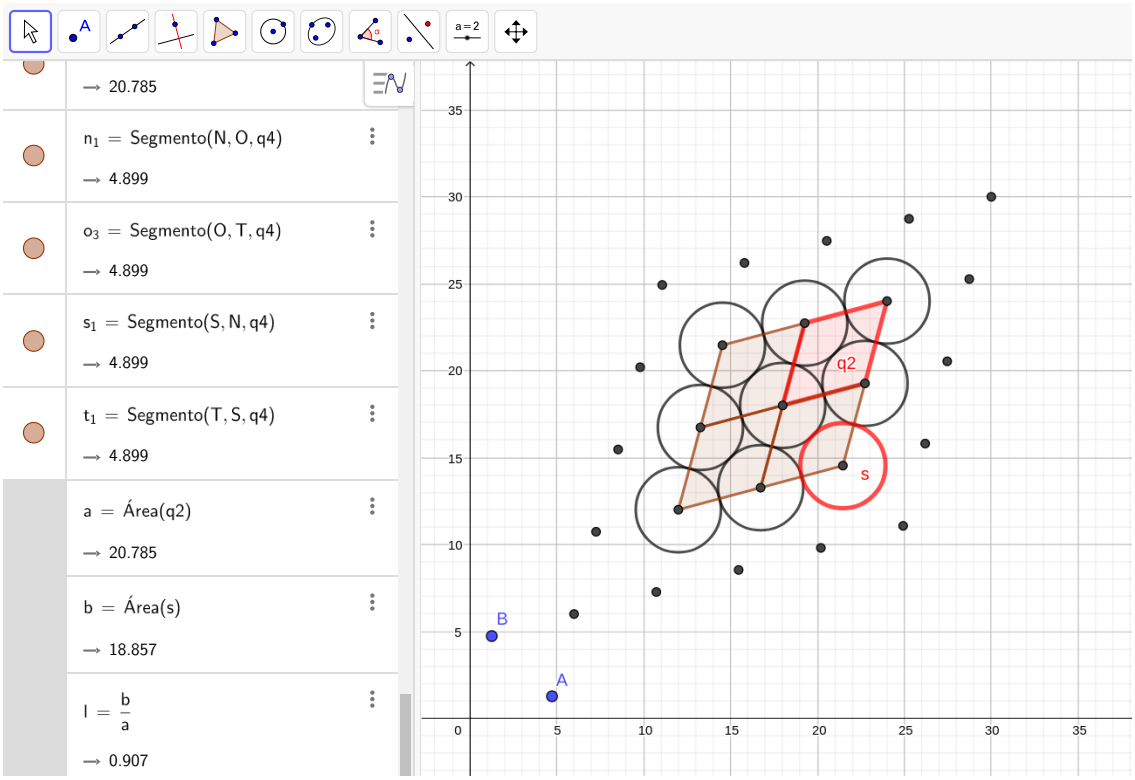
Fonte: Elaborada pelo autor

Figura 5.10: Desenhando círculos conforme o **Passo 4**



Fonte: Elaborada pelo autor

Figura 5.11: Calculando a densidade de empacotamento conforme o **Passo 5**



Fonte: Elaborada pelo autor

6 Considerações finais

Em nosso trabalho estudamos resultados sobre polinômios e equações polinomiais de 2^o e 3^o graus, úteis para o desenvolvimento desses assuntos no Ensino Médio, como a divisão euclidiana para polinômios, a fatoração canônica de um polinômio, as relações de Girard, a fórmula resolutiva da equação do 2^o grau e as fórmulas de Cardano para equações do 3^o grau. Além disso, ampliamos e aprofundamos o tema estudando sua aplicação no desenvolvimento de um método para facilitar a resolução da equação $Y^3 + pY + q = 0$ bem como, na construção de reticulados densos e reticulados bem arredondados em $\mathbb{R}^2$ e $\mathbb{R}^3$.

Ao final do trabalho, apresentamos a sugestão de uma coletânea de problemas extraídos de competições norte americanas de matemática e de um importante vestibular nacional, relacionadas ao tema estudado, além de um problema e duas atividades para serem desenvolvidas com os alunos do Ensino Médio.

Referências

[1] ALVES, Carina.; PINTO, Willian L.S.; ANDRADE, Antonio A. Well-rounded lattices via polynomials with real roots. **International Journal of Applied Mathematics**, v. 33, n. 4, p. 663-672, jan. 2020.

[2] AMC problems and solutions. **AoPS Online**, c2022. Disponível em <https://artofproblemsolving.com/wiki/index.php/AMC_Problems_and_Solutions>. Acesso em: 11 de jul. de 2022

[3] ANDRADE, Antonio A.; PALAZZO Jr., Reginaldo: *Construction and decoding of BCH codes over finite commutative rings*. **Linear Algebra and its Applications**, 286, 69-85, 1999.

[4] ARAUJO, Robson R.; COSTA, Sueli I. R.: *Well-rounded algebraic lattices in odd prime dimension.* Arch. Math., **112**, 139-148, feb. 2019.

[5] BEDOYA, Hernando; CAMELIER, Ricardo **Álgebra II**: v. único. Rio de Janeiro: Fundação CECIERJ, 2010.

[6] BIAZZI, Ricardo Neves. **Polinômios irredutíveis: critérios e aplicações**. 2014. 74 f. Dissertação - (Mestrado) - Universidade Estadual Paulista, Instituto de Geociências e Ciências Exatas, Rio Claro, 2014. Disponível em: <http://hdl.handle.net/11449/108811>. Unesp, Rio Claro, 2014.

[7] BRASIL. Ministério da Educação. **Base Nacional Comum Curricular**. Brasília, 2020.

[8] BRASIL. **Parâmetros Curriculares Nacionais** – Ensino Médio. Brasília: Ministério da Educação, 1998

[9] BUELL, Duncan A. **Binary Quadratic Forms**. New York: Springer-Verlag, 1989.

[10] CAMPELLO, Antonio; STRAPASSON, João E.; Costa, Sueli I.R. On projections of arbitrary lattices. **Linear Algebra and its Applications**, v.439, n. 9, 2577-2583, nov. 2013.

[11] CHEN, Willian Y.C. Cubic Equations Through the Looking Glass of Sylvester. **College Math. J.**, to appear, arXiv preprint: 2103.15051, mar. 2021.

[12] CONWAY, J. H.; SLOANE, N. J. A. **Sphere Packings, Lattices and Groups.** 3. ed. New York: Springer, 1999.

[13] FUKSHANSKY, Lenny. On similarity classes of well-rounded sublattices of $\mathbb{Z}^2$. **Journal of Number Theory**, vol. 129, n. 10, 2530–2556, 2009.

[14] FUKSHANSKY, Lenny; PETERSEN, Kathleen. On Well-Rounded Ideal Lattices. **International Journal of Number Theory**, vol. 8, n. 1, 189–206, 2012.

[15] GONÇALVES, Adilson. **Introdução à álgebra**. Rio de Janeiro: IMPA, 2006.

[16] HEFEZ, Abramo.; VILLELA, Maria L. T. **Polinômios e Equações Algébricas.** 2. ed. Rio de Janeiro: Sociedade Brasileira de Matemática, 2018.

[17] LIAO, Hsin-C.; SAUL, Mark, SHIUE, Peter J.-S.Revisiting the general cubic: A simplification of Cardano's solution. **The Mathematical Gazette**, to appear, arXiv:2204.07507v1, apr. 2022

[18] LIMA, Elon L. **Análise Real, vol. 2**: Funções de n Variáveis. 6ed. Rio de Janeiro: IMPA, 2016.

[19] LU, Peter; STEINHARDT, Paul J. Decagonal and quasicrystalline tilings in Medieval Islamic architecture. **Science**, v. 315, 1106-1110, feb. 2007.

[20] NETO, Antonio C. M. **Tópicos de Matemática Elementar**: Teoria dos Números. 2. ed. Rio de Janeiro: Sociedade Brasileira de Matemática, 2014.

[21] NETO, A. C. M. **Tópicos de Matemática Elementar**: Polinômios. 2. ed. Rio de Janeiro: Sociedade Brasileira de Matemática, 2016.

[22] PINTO, Willian L.S. **Construção de reticulados circulantes densos**. 2022, 102 f. Dissertação (Mestrado em Matemática) - Universidade Estadual Paulista "Júlio de Mesquita Filho", São José do Rio Preto, 2022..

[23] RESOLUÇÃO comentada ITA. **Curso Objetivo Vestibulares**, c2022. Disponível em: <https://www.curso-objetivo.br/vestibular/resolucao_comentada/ita.asp>. Acesso em: 15 de jul. de 2022

[24] SHANNON, C. E. A mathematical theory of communication. **The Bell System Technical Journal.** vol. 27, p. 379–423 and 623–656, 1948.

[25] SOUZA, Taciana M. **Reticulados algébricos em corpos de números abelianos**. 2004, 119 f. Dissertação (Mestrado em Matemática) - Universidade Estadual Paulista "Júlio de Mesquita Filho", São José do Rio Preto, 2004.

[26] STEWART, Ian.; TALL,D. **Algebric Number Theory.** New York:Chapman & Hall, 1987.

[27] SYLVESTER, J.J. On a remarkable discovery in the theory of canonical forms and of hyperdeterminants. **Philosophical Magazine and Journal of Science.** vol. 2, 391-410, n. 12, 1851.

A Soluções das questões propostas na Seção 5.1

As soluções aqui apresentadas foram adaptadas de [2] e [23].

Solução do Problema 1: Sejam r_1, r_2, e r_3 as raízes de $g(x)$. Seja r_4 a raiz adicional de $f(x)$. Aplicando as relações de Girard ao termo quadrátrico de $g(x)$ e ao termo cúbico de $f(x)$, obtemos:

$$\begin{cases} r_1 + r_2 + r_3 = -a \\ r_1 + r_2 + r_3 + r_4 = -1 \end{cases}$$

Então, $r_4 = a - 1$.

Agora, aplicando as relações de Girard aos termos constante e linear de $g(x)$ e ao termo linear de $f(x)$, obtemos:

$$\begin{cases} r_1 r_2 r_3 = -10 \\ r_1 r_2 + r_2 r_3 + r_3 r_1 = 1 \\ r_1 r_2 r_3 + r_2 r_3 r_4 + r_3 r_4 r_1 + r_4 r_1 r_2 = -100 \end{cases} \tag{A.1}$$

Substituibndo $r_1 r_2 r_3$ na terceira equação do sistema (A.1) e fatorando o restante da expressão, obtemos:

$$-10 + (r_1 r_2 + r_2 r_3 + r_3 r_1) r_4 = -10 + r_4 = -100.$$

Donde segue que $r_4 = -90$. Mas $r_4 = a - 1$, então $a = -89$.

Podemos agora fatorar $f(x)$ em termos de $g(x)$ como

$$f(x) = (x - r_4) g(x) = (x + 90) g(x).$$

Logo, $f(1) = 91 g(1)$ onde

$$g(1) = 1^3 - 89 \cdot 1^2 + 1 + 10 = -77.$$

Portanto, $f(1) = 91 \cdot (-77) = \boxed{\textbf{(C)} \ -7007}$.

Solução do Problema 2: Sejam r_1 e r_2 as raízes de $\tilde{p}(x)$. Então, $\tilde{p}(x) = (x - r_1)(x - r_2) = x^2 - (r_1 + r_2)x + r_1 r_2$. As raízes de $\tilde{p}(\tilde{p}(x)) = 0$ são dadas pela união das raízes de

$$\tilde{p}(x) - r_1 = x^2 - (r_1 + r_2)x + (r_1 r_2 - r_1) = 0$$

e

$$\tilde{p}(x) - r_2 = x^2 - (r_1 + r_2)x + (r_1 r_2 - r_2) = 0.$$

Como devemos ter exatamente três raízes, uma dessas equações quadráticas deve possuir uma única raiz real (uma raiz dupla) e a outra, duas raízes reais distintas. Digamos que $x^2 - (r_1 + r_2)x + (r_1r_2 - r_1) = 0$ seja a equação com uma raiz dupla. Então seu discriminante é 0, e assim

$$\begin{aligned}(r_1 + r_2)^2 = 4r_1r_2 - 4r_1 &\Leftrightarrow r_1^2 + 2r_1r_2 + r_2^2 = 4r_1r_2 - 4r_1\\ &\Leftrightarrow r_1^2 - 2r_1r_2 + r_2^2 = -4r_1\\ &\Leftrightarrow (r_1 - r_2)^2 = -4r_1\\ &\Leftrightarrow |r_1 - r_2| = \sqrt{-4r_1}\\ &\Leftrightarrow r_1 - r_2 = \pm 2\sqrt{-r_1}\end{aligned}$$

onde $r_1 \leqslant 0$, pois r_1 e r_2 são reais.

Agora, para que $x^2 - (r_1 + r_2)x + (r_1r_2 - r_2) = 0$ tenha duas raízes reais distintas, é necessário que seu discriminante seja maior do que 0. Assim,

$$\begin{aligned}(r_1 + r_2)^2 > 4r_1r_2 - 4r_2 &\Leftrightarrow r_1^2 + 2r_1r_2 + r_2^2 > 4r_1r_2 - 4r_2\\ &\Leftrightarrow r_1^2 - 2r_1r_2 + r_2^2 > -4r_2\\ &\Leftrightarrow (r_1 - r_2)^2 > -4r_2.\end{aligned}$$

E como $|r_1 - r_2| = \sqrt{-4r_1}$ temos, $-4r_1 > -4r_2$, de onde segue que $r_1 < r_2$. Logo,

$$r_1 - r_2 = -2\sqrt{-r_1}, \tag{A.2}$$

donde $r_2 = r_1 + 2\sqrt{-r_1}$. Assim, somando $2r$ em ambos os membros da equação (A.2) e substituindo r_2 no membro da direita, obtemos uma expressão para a soma das raízes de $\tilde{p}(x)$ em termos de r_1:

$$r_1 + r_2 = 2r_1 + 2\sqrt{-r_1}. \tag{A.3}$$

Para determinar o valor máximo de (A.3), podemos reescrever seu membro da direita em termos de X, onde $X = \sqrt{-r_1}$, obtendo $-2X^2 + 2X$, cujo valor máximo ocorre quando $X = \frac{1}{2}$ ou, de modo equivalente, $r_1 = \frac{-1}{4}$. Substituindo r_1 em (A.3), obtemos $r_2 = \frac{3}{4}$.

Portanto, $\tilde{p}(x) = x^2 - \left(\frac{-1}{4} + \frac{3}{4}\right)x - \left(\frac{-1}{3} \cdot \frac{3}{4}\right) = x^2 - \frac{1}{2}x - \frac{3}{16}$. E assim, $\tilde{p}(1) = \boxed{\textbf{(A)}\ \dfrac{5}{16}}$.

Solução do Problema 3: Primeiramente observe que $z^3 - 1 = (z^2 + z + 1)(z - 1)$. Seja s uma raiz de $z^2 + z + 1$. Então,

$$(s - 1)\left(s^2 + s + 1\right) = s^3 - 1 = 0,$$

de onde $s^3 = 1$, mas $s \neq 1$.

Observe também que

$$\begin{aligned}s^{2021} + 1 &= s^{3\cdot 673 + 2} + 1\\ &= (s^3)^{673} \cdot s^2 + 1\\ &= s^2 + 1\\ &= \left(s^2 + s + 1\right) - s\\ &= -s.\end{aligned}$$

Desse modo, quando $z = s$ temos $(s^2 + s + 1)Q(s) + R(s) = s^{2021} + 1 \Leftrightarrow R(s) = -s$

Como $z^{2021}+1=-z$ para cada raiz $z=s$ de z^2+z+1,, o resto da divisão de $z^{2021}+1$ por z^2+z+1 é $R(z)=\boxed{\textbf{(A) } -z}$.

Solução do Problema 4: Sejam p, q, e r as três raízes de $f(x)$. Então, $f(x) = (x-p)(x-q)(x-r)$ e $g(x) = (x-\frac{1}{p})(x-\frac{1}{q})(x-\frac{1}{r})$. Logo,

$$g(1) = (1-\frac{1}{p})(1-\frac{1}{q})(1-\frac{1}{r}) = \frac{(p-1)(q-1)(r-1)}{pqr}$$

Agora observe que $(p-1)(q-1)(r-1) = -(1-p)(q-1)(r-1) = (1-p)(1-q)(r-1) = -(1-p)(1-q)(1-r) = -f(1)$. Além disso, pelas relações de Girard em f, temos que $pqr = -c$. Portanto,

$$g(1) = \frac{-f(1)}{-c} = \boxed{(\mathbf{A})\frac{1+a+b+c}{c}}$$

Solução do Problema 5: Sejam $P(x) = 2x^2+ax+b$, $Q(x) = -2x^2+cx+d$ e $R(x) = P(x)+Q(x)$. Então, $R(x) = P(x)+Q(x) = (a+c)x+(b+d)$. Fazendo $a+c=m$ e $b+d=n$ podemos escrever $R(x) = P(x)+Q(x) = mx+n$.

Como os gráficos de ambos passam pelos pontos $(16, 54)$ e $(20, 53)$, temos

$$R(16) = P(16)+Q(16) = 54+54 = 108,$$
$$R(20) = P(20)+Q(20) = 53+53 = 106.$$

Por outro lado,

$$\begin{cases} R(16) = 16m+n, \\ R(20) = 20m+n. \end{cases}$$

de onde segue que $m = \frac{-1}{2}$ e $n = 116$. Logo,

$$R(x) = \frac{-1}{2}x + 116$$

Portanto, $P(0)+Q(0) = R(0) = \frac{-1}{2}\cdot 0 + 116 = 116$.

Solução do Problema 6:

Pelo teste da raiz podemos escrever

$$x^3+ax+b = (x+20)P(x)$$

e

$$x^3+cx^2+d = (x+21)Q(x)$$

para alguns polinômios $P(x)$ e $Q(x)$.

Fazendo a divisão euclidiana de x^3+ax+b e x^3+cx^2+d, respectivamente, por $P(x)$ e $Q(x)$, e desprezando os restos (pois são iguais a 0), obtemos $P(x) = x^2-20x+(400+a)$, e $Q(x) = x^2+(c-21)x+(441-21c)$.

A raiz complexa não real compartilhada por x^3+ax+b e x^3+cx^2+d é também compartilhada por $P(x)$ e $Q(x)$. Como ambos têm no máximo duas raízes e, como as raízes complexas não reais ocorrem aos pares, $P(x)$ e $Q(x)$ possuem exatamente as duas mesmas raízes. Além disso, como seu coeficientes líderes são iguais, segue que $P(x) = Q(x)$. Desse

modo, $c - 21 = -2$ e $441 - 21c = 400 + a$, de onde segue que $a = 20$ and $c = 1$. Logo, $P(x) = Q(x) = x^2 - 20x + 420$.

Pela fórmula resolutiva da equação polinomial do 2º grau, obtemos

$$\frac{20 \pm i\sqrt{400 - 1680}}{2} = 10 \pm i\sqrt{320}.$$

Logo, $m = 10$ e $n = 320$ e, portanto, $m + n = 330$.

Solução do Problema 7: Sejam z_1, z_2 e z_3 as raízes de p. Como toda raiz não real ocorre ao pares, p deve ter ao menos uma raiz real, z_1 digamos. Nesse caso, $b = 0$ e assim, $z_1 = a_1 = -1$.

Se $b \neq 0$, $z_2 = a_2 + b_2 i$ e $z_3 = a_2 + (-b_2)i$. Logo, da igualdade $a = mb^2 + nb - 1$, segue que $mb_2^2 + nb_2 - 1 = a_2 = m(-b_2)^2 + n(-b_2) - 1$. Então,

$$mb_2^2 + nb_2 - 1 = m(-b_2)^2 + n(-b_2) - 1 \Leftrightarrow 2nb_2 = 0 \Leftrightarrow n = 0.$$

Substituindo $n = 0$ e $z_1 = -1$ em $p(z) = 0$, temos

$$p(-1) = (-1)^3 - m(-1)^2 - 1 + 5 + 0 \Leftrightarrow -1 - m - 1 + 5 = 0 \Leftrightarrow m = 3$$

Pelas relações de Girard, temos

$$\begin{cases} z_1 + z_2 + z_3 = m = 3 \\ z_1z_2 + z_1z_3 + z_2z_3 = 1 \\ z_1z_2z_3 = -5. \end{cases}$$

Elevando a primeira equação ao quadrado, temos

$$z_1^2 + z_2^2 + z_3^2 + 2(z_1z_2 + z_1z_3 + z_2z_3) = 9.$$

Finalmente, substituindo $z_1z_2 + z_1z_3 + z_2z_3$ obtemos

$$z_1^2 + z_2^2 + z_3^2 = \boxed{\textbf{(B) } 7}.$$

Solução do Problema 8: Como $p(x)$ é divisível por $x^2 - 4 = (x+2)(x-2)$, então -2 e 2 são raízes de $p(x)$. Sejam $x_1, x_2, -2$ e 2 as raízes de $p(x)$. Como a soma e o produto das raízes de $p(x)$ são, respectivamente, iguais a 1 e 3, segue que

$$\begin{cases} -2 + 2 + x_1 + x_2 = 1 \\ -2 \cdot 2 \cdot x_1 \cdot x_2 = 3, \end{cases}$$

de onde

$$\begin{cases} x_1 + x_2 = 1 \\ x_1 \cdot x_2 = \frac{-3}{4}, \end{cases}$$

Logo, x_1, x_2 são as raízes da equação $t^2 - t - \frac{3}{4} = 0$. Pela fórmula resolutiva da equação polinomial do 2º grau obtemos $t = \frac{1 \pm \sqrt{1+3}}{2}$. Logo, as raízes de $p(x)$ são $\frac{-1}{2}, \frac{3}{2}, -2$ e 2, e assim, podemos escrever $p(x) = a\left(x + \frac{1}{2}\right)\left(x - \frac{3}{2}\right)(x+2)(x-2)$.

Como $p(-1) = \frac{-15}{4}$, temos

$$a\left(-1+\frac{1}{2}\right)\left(-1-\frac{3}{2}\right)(-1+2)(-1-2) = \frac{-15}{4},$$

de onde $a = 1$. Portanto, $p(x) = \left(x+\frac{1}{2}\right)\left(x-\frac{3}{2}\right)(x+2)(x-2)$, e assim, $p(1) = \left(1+\frac{1}{2}\right)\left(1-\frac{3}{2}\right)(1+2)(1-2) = \boxed{\textbf{(D)}\ \frac{9}{4}}$.

Solução do Problema 9: Como as raízes não reais ocorrem ao pares (raízes conjugadas), as raízes de $p(z)$ são i, $-i$, z_1 e $\overline{z}_1$. Das relações de Girard segue que

$$\begin{cases} i + (-i) + z_1 + \overline{z}_1 = 6 \\ i \cdot (-i) \cdot z_1 \cdot \overline{z}_1 = 13 \end{cases}$$

donde,

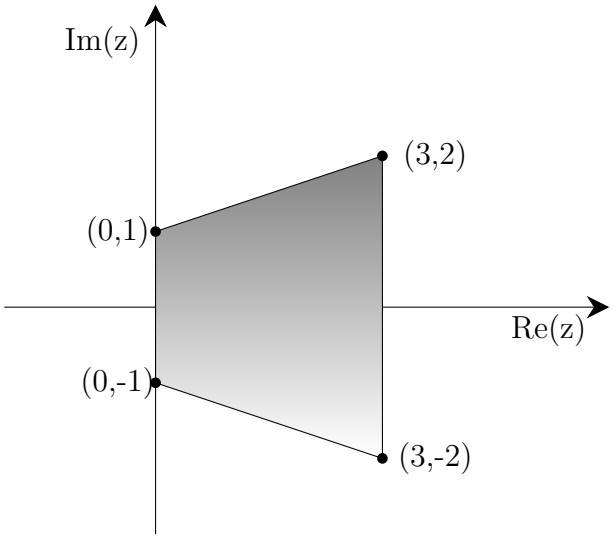
$$\begin{cases} z_1 + \overline{z_1} = 6 \\ z_1\overline{z_1} = 13 \end{cases}.$$

Logo, z_1 e $\overline{z_1}$ são as raízes de $t^2 - 6t + 13 = 0$. Pela fórmula resolutiva da equação polinomial do 2º grau, obtemos:

$$t = \frac{6 \pm \sqrt{-16}}{2} = \frac{6 \pm 4i}{2} = 3 \pm 2i.$$

Logo as raízes de $p(z) = 0$ são i, $-i$, $3+2i$ e $3-2i$.

Representando no plano complexo o quadrilátero cujos vértices são as raízes de $p(z) = 0$, obtemos:



O quadrilátero em questão é um trapézio cuja área é igual a $\frac{4+2}{2} \cdot 3 = \boxed{\textbf{(D)}\ 9}$.

Solução do Problema 10:

Se p admite raiz dupla, então p possui uma raiz dupla e uma raiz simples. Suponhamos que 2 seja a raiz dupla de p e seja $r \neq 2$ a outra raiz. Pelas relações de Girard temos $2 \cdot 2 \cdot r = \frac{16}{2}$, de onde $r = 2$. Mas isso não pode ocorrer, pois supomos $r \neq 2$.

Seja $r \neq 2$ a raiz dupla de p. Pelas relações de Girard temos que $2 \cdot r \cdot r = \frac{16}{2}$, donde $r = \pm 2$ e, como $r \neq 2$, temos $r = -2$.

Novamente pelas relações de Girard, temos

$$(-2) + (-2) + 2 = \frac{-a}{2}$$

e

$$2 \cdot (-2) + 2 \cdot (-2) + (-2) \cdot (-2) = \frac{b}{2},$$

de onde obtemos, respectivamente, $a = 4$ e $b = -8$.

Portanto, $b - a = -8 - 4 =$ **(B) -12**