UNIVERSIDADE FEDERAL DO ABC

PROFMAT

Dissertação de mestrado

Resolução de equações algébricas

Leandro Albino Mosca Rodrigues

Orientadora: Prof.ª Dr.ª Ana Carolina Boero

Santo André, outubro de 2014.

UNIVERSIDADE FEDERAL DO ABC

PROFMAT

Dissertação de mestrado

Resolução de equações algébricas

Leandro Albino Mosca Rodrigues

Trabalho apresentado como requisito parcial para obtenção do título de Mestre em Matemática (PROFMAT), sob orientação da Prof.ª Dr.ª Ana Carolina Boero.

Santo André, outubro de 2014.

MINISTÉRIO DA EDUCAÇÃO
Fundação Universidade Federal do ABC
Programa de Pós-Graduação em Mestrado Profissional em Matemática em Rede Nacional
Rua Abolição, s/nº – Vila São Pedro – Santo André – SP
CEP 09210-180 · Fone: (11) 4996-0017
profmat@ufabc.edu.br

FOLHA DE ASSINATURAS

Assinaturas dos membros da Banca Examinadora que avaliou e aprovou a Defesa de Dissertação de Mestrado do candidato Leandro Albino Mosca Rodrigues, realizada em 3 de outubro de 2014:

Prof.(a) Dr.(a) **Ana Carolina Boero** (UFABC) – Presidente

Prof.(a) Dr.(a) **Armando Caputi** (UFABC) – Membro Titular

Prof.(a) Dr.(a) **Renato Alessandro Martins** (UNIFESP) – Membro Titular

Prof.(a) Dr.(a) **Sinue Dayan Barbero Lodovici** (UFABC) – Membro Suplente

Prof.(a) Dr.(a) **Gleiciane da Silva Aragão** (UNIFESP) – Membro Suplente

Este exemplar foi revisado e alterado em relação à versão original, de acordo com as observações levantadas pela banca no dia da defesa, sob responsabilidade única do autor e com a anuência de seu orientador.

Santo André, 31 **de** outubro **de 20**14.

Assinatura do autor: Leandro Juliano Maia Rodrigues

Assinatura do orientador: _____

Aos meus pais José Manoel Rodrigues e Rita Helena Albino de Souza.

AGRADECIMENTOS

- Ao professor César Polcino Milies que me despertou o interesse pela álgebra em suas aulas ao longo do curso de graduação.

- Ao professor Armando Caputi pelas aulas no curso do PROFMAT.

- A grande ajuda indiscutível da professora Ana Carolina Boero que me recebeu sempre com um sorriso e uma enorme paciência ao longo dessa orientação.

- À professora Zélia Beletato que me despertou o interesse na mais bela das profissões.

- Aos meus amigos Ricardo A. Mori, Oertes A. Souza e Marcelo A. Souza sem os quais eu não teria começado esse curso.

"Só aqueles que desistiram de viver acham que os sonhos são impossíveis."
(Hyoga de Cisne)

RESUMO

Este trabalho se dedica ao estudo das equações algébricas. Foi feito um apanhado histórico do assunto, desde os tempos antigos até Galois. Estudamos métodos para resolver equações algébricas de grau menor ou igual a 4 e exibimos um exemplo de equação de grau 5 que não é solúvel por radicais. Apresentamos, também, uma proposta de abordagem do tema no Ensino Médio. Encerramos este trabalho com um capítulo dedicado aos professores do Ensino Médio que desejam se aprofundar no assunto. Nele, mostramos como alguns fatos do cálculo podem ser usados para explicar a natureza das raízes da equação $x^3 + px + q = 0$ a partir do sinal de seu discriminante.

Palavras-chave: equações algébricas, resolução por radicais

ABSTRACT

This work is dedicated to the study of algebraic equations. A historical overview of the subject has been done, from ancient times to Galois. We have studied methods for solving algebraic equations of degree less than or equal to 4 and we present an example of an equation of 5th degree that is not solvable by radicals. We also propose an approach to the subject in high school. Finally, there is a chapter dedicated to teachers who wish to deepen their knowledge in the subject. In it, we show how some facts of calculus can be used to explain the nature of the roots of the equation $x^3 + px + q = 0$ using the sign of its discriminant.

Keywords: algebraic equations, solution by radicals

SUMÁRIO

INTRODUÇÃO

Os primeiros problemas referentes à álgebra surgiram relacionados à problemas de geometria plana e espacial [13].

Algumas tábuas de argila como a Plimpton 322, que pode ser encontrada na Universidade de Columbia, apresentam alguns rudimentos de uma equação quadrática relacionada com o que viria mais tarde ser o Teorema de Pitágoras.

Nessa época não havia uma notação formal para álgebra como a conhecemos hoje e grande parte dos problemas eram escritos e resolvidos por palavras.

Um antigo texto hindu, escrito por Baudhayaba, por volta do século 8 a.C. resolve algumas equações quadráticas relacionadas com a construção de altares.

Durante os séculos seguintes a álgebra teve o seu desenvolvimento ligado sempre com a geometria durante todo o período helenístico na Grécia. Alguns grandes matemáticos surgiram nessa época como Pitágoras, Euclides, Diofanto, Arquimedes e Ptolomeu. [4]

Alguns séculos depois com o domínio árabe, o califa Al-Mamum (786-833) construiu a Casa da Sabedoria (House of Wisdom). Diz a lenda que Aristóteles apareceu em um sonho para ele e desde então ele ordenou a tradução de todos os textos gregos, entre eles *Os Elementos* de Euclides e o *Almagesto* de Ptolomeu. Com a criação do sistema hindu-arábico foi dado mais um passo para o desenvolvimento da álgebra e a constante necessidade de achar a direção de Meca fez-se natural o seu desenvolvimento.

O termo álgebra como conhecemos hoje veio do tratado escrito por Al-Khwarismi, chamado *Al-Kitab al-Jabr wa'l-Muqabala* (Livro da restauração e do balanceamento). Algumas equação quadráticas são desenvolvidas, porém eram considerados apenas números naturais tanto nos coeficientes como nas soluções.

Com o declínio do domínio árabe e início do renascimento na Europa, grande parte da transmissão de conhecimento se deu através de Omar Khayyan, por meio do seu tratado sobre demonstração de problemas de álgebra. Ele também foi

responsável pela resolução de algumas cúbicas usando geometria.

Na China no século 13, temos ainda que Zhu Shijie também desenvolveu soluções para algumas cúbicas.

Temos então o surgimento dos símbolos matemáticos como o conhecemos hoje (+, - , x, =) e o afastamento da álgebra com a geometria. François Viéte foi o responsável pela notação que usamos hoje, usando vogais para representar quantidades desconhecidas e consoante para quantidades conhecidas.

No capítulo 2 temos a discussão central deste trabalho no qual, mencionando o contexto histórico, começamos com as equações de grau 2 , 3 e 4 demonstrando que tais equações são solúveis por radicais. Para a equação de grau 5 faremos uso de algumas noções básicas de teoria de Galois.

O capítulo 1 trata de alguns pré-requisitos conhecidos como Álgebra Moderna ou Álgebra Abstrata. Em 1830 com a publicação de *Treatise on Álgebra* de Peacock, a álgebra libertou-se da artimética. Nesta obra Peacock tenta dar o mesmo tratamento axiomático que Euclides tinha dado a Geometria em *Os Elementos*. Para ele a álgebra era a ciência que trata das combinações de símbolos arbitrários cujo sentido é definido através de leis de combinação também arbitrárias. O mesmo pensamento é compartilhada por Augustus de Morgan no seu *Trigonometry and Double Algebra* [11], porém os axiomas que eles utilizavam eram extraídos da aritmética e apenas com o surgimento dos quatérnios por Hamilton foi dado mais um passo no rompimento total com a aritmética

O conjunto dos quatérnios seria o primeiro exemplo de anel não comutativo com divisão, porém sem essa terminologia. Com essa descoberta descobriu-se uma estrutura na qual "a ordem dos fatores altera o produto"o que levou a pensar nas definições e também em estender o conceito para outras álgebras.

O estudo das permutações se deu com Joseph Lagrange, seguido por Ruffini e Abel. O primeiro a usar o conceito mais explicitamente foi Galois. Todos os desenvolvimentos se deram para a resolução de equações álgebricas.

Logo em seguida Augustin Cauchy escreveu inúmeros tratados sobre grupo de permutações que mais tarde serviram de inspiração para Arthur Cayley formular o conceito de grupo abstrato em 1854 na obra *On the Theory of Groups as depending on the symbolical equation* $\theta^n = 1$.

O primeiro conceito de corpo foi usado por Galois ao tratar das extensões de corpos algébricos, porém a primeira definição formal de corpos foi dada por Richard

Dedekind. Em 1903, Leonard Eugene Dickson e Edward V. Huntington deram definições de corpos usando conjuntos e postulados. O termo *anel* foi introduzido por David Hilbert.

Alguns matemáticos consideram que os dois grandes pilares da álgebra abstrata são as publicações feitas por Ernst Steinitz em 1910 e por Emmy Noether em 1929.

Qualquer leitor que tenha familiaridade com Teoria de Grupos e Corpos pode omitir o capítulo 1, sem maiores problemas. Aqueles que desejarem se aprofundar no tema, grande parte das definições e demonstrações podem ser encontradas em [5].

O objetivo principal do capítulo 3 é mostrar como desenvolver com alunos do EM métodos que resolvam equações polinomiais. Inicialmente mostramos que grande parte dos exercícios recaem em equações de 2º grau, mostramos algumas técnicas de resolução que independem de fórmulas e terminamos com algumas noções de Cálculo Numérico que podem ser aplicadas com o nível de conhecimento obtido ao longo do curso. Os métodos de cálculo numérico podem ser melhores discutidos em [6] e [9].

O capítulo 4 traz um aprofundamento para o professor sobre discussão algébrica e gráfica das equações de grau 3 que foram extraídas de [9].

1 PRELIMINARES

O objetivo deste capítulo é apresentar as definições necessárias para a leitura do texto, bem como fixar as notações utilizadas ao longo do mesmo e enunciar resultados dos quais faremos uso mais adiante.

1.1 Grupos

Definição 1.1.1. Um *grupo* é um conjunto G munido de uma operação $*$ que satisfaz as seguintes condições:

1. $(a * b) * c = a * (b * c)$ para quaisquer $a, b, c \in G$;
2. existe (um único) $e \in G$ tal que $a * e = a = e * a$ para todo $a \in G$;
3. para cada $a \in G$ existe (um único) $a^{-1} \in G$ tal que $a * b = e = b * a$.

Exemplo: O conjunto das permutações de n elementos, denotado por S_n, com a operação de composição de função é um grupo. Tal grupo será melhor definido ao longo desse texto.

Um grupo G é dito *abeliano* se $a * b = b * a$ para quaisquer $a, b \in G$.

Definição 1.1.2. Dizemos que um grupo G é *finito* se G for um conjunto finito. Neste caso, definimos a *ordem* de G como o número de elementos de G e a denotamos por $|G|$.

Exemplo: O grupo S_5, formado pelas permutações de 5 elementos tem ordem $5! = 120$

Definição 1.1.3. Se G é um grupo e $a \in G$, definimos a *ordem* de a como o menor inteiro positivo n tal que $a^n = e$.

Teorema 1.1.4 (Cauchy). *Sejam G um grupo finito e p um número primo que divide $|G|$. Então G possui um elemento de ordem p.*

beginproof Considere o conjunto $S = (a_1, a_2, \ldots, a_{p-1}, a_p)$ sendo $a_1, a_2, \ldots, a_p \in G$ e $a_1 a_2 \ldots a_p = e$. Vamos primeiro provar que $|S| = |G|^{p-1}$.

Pensando em uma p-upla ordenada cada um dos $p-1$ primeiro elementos tem $|G|$ possibilidades, porém o p-ésimo elemento tem uma única opção dada por $(a_1 a_2 \ldots a_{p-1})^{-1}$, devido a restrição dada. Logo $|S| = |G|^{p-1}$ que será múltiplo de p, visto que p divide a ordem de $|G|$.

Vamos definir uma relação de equivalência $\sim$ de SxS dada por $(x, y) \in \sim \Leftrightarrow$ y pode ser obtido por uma permutação cíclica de x. Observe que qualquer uma desta permutações pertencem a S, pois dada a permutação $(a_p, a_1, \ldots, a_{p-1})$, temos que $a_p a_1 \ldots a_{p-1} = a_p a_1 \ldots a_{p-1} e = a_p a_1 \ldots a_{p-1} a_p {a_p}^{-1} = a_p (a_1 \ldots a_{p-1} a_p) {a_p}^{-1} = a_p e {a_p}^{-1} = e$.

Note ainda que nem sempre que permutamos geramos uma p-upla distinta, no caso $\epsilon = (e, e, \ldots, e)$ qualquer permutação gera ela própria. Logo a classe de equivalência (ϵ) tem apenas um elemento.

Vamos analisar as demais classes de equivalência agora. Se todas as demais classes de $\sim$ possuem p elementos então $|S|$ é congruente módulo 1 a p, o que é absurdo visto que p é múltiplo de $|S|$.

Portanto, em S, deve existir um $x = (a_1, a_2, \ldots, a_p)$ tal que exista uma quantidade menor que p na classe de equivalência deste elemento, ou seja, isto significa que há duas permutações cílicas diferentes de ϵ que são iguais.

Vamos considerar estas duas permutações dadas por $(a_{r+1}, \ldots, a_p, a_1, \ldots, a_r)$=$(a_{s+1}, \ldots, , a_p, a_1, \ldots, a_S)$. Sendo $r, s \in Z$ suponha, sem perda de generalidade, que $r > s$ e voltando as duas permutações $p-r$ vezes obtemos então que $(a_1, a_2, \ldots, a_p) = (a_{k+1}, \ldots, a_p, a_1, \ldots, a_k)$ sendo $k = p - r + s$. Igualando os valores note que $x_i = x_{k+i}$ para $1 \leq i \leq p$ e comparando módulo p os índices obtemos então que $x_1 = x_{k+1} = x_{2k+1} = x_{(p-1)k+1}$. Suponha então que dois índices $ak + 1$ e $bk + 1$ são congruentes módulo p, logo $p \mid k(a - b)$ mas como $a - b$ e k são ambos menores que p temos um absurdo pois p é primo. Logo, todos os números da sequência $1, k + 1, 2k + 1, \ldots (p - 1)k + 1$ são todos distintos módulo p e como temos p elementos nessa sequência, concluímos que numa determinada ordem $a_1 = a_2 = \cdots = a_p = a$ e portanto $a^p = e$ o que completa nossa demonstração.

Definição 1.1.5. Um subconjunto H de um grupo G é um *subgrupo* de G se, relativamente à operação de G, H é um grupo.

Proposição 1.1.6. *Sejam G um grupo e H um subconjunto de G. As seguintes condições são equivalentes:*

1. *H é um subgrupo de G.*
2. *a) $e \in H$;*
   b) se $a, b \in H$ então $a * b \in H$;
   c) se $a \in H$ então $a^{-1} \in H$.

Escreveremos $H \leq G$ para indicar que H é um subgrupo de um grupo G.

Definição 1.1.7. Sejam G um grupo e $H \leq G$. Um conjunto da forma

$$Hx = \{hx : h \in H\}$$

onde $x \in G$ é chamado de *coclasse à direita* de H em G. Analogamente, podemos definir o conjunto das coclasses à esquerda de H em G.

Definição 1.1.8. Seja $N \leq G$. Dizemos que N é *normal* em G se $Nx = xN$ para todo $x \in G$.

Escreveremos $N \lhd G$ para indicar que N é um subgrupo normal de G.
Note que todo subgrupo de um grupo abeliano é normal.

Proposição 1.1.9. *Seja $N \lhd G$. O conjunto $\frac{G}{N} = \{Nx : x \in G\}$ munido da operação*

$$(Nx) * (Ny) = N(xy)$$

é um grupo, denominado o grupo quociente *de G por H.*

Definição 1.1.10. Sejam G e G' grupos. Uma aplicação $f : G \to G'$ é um *homomorfismo (de grupos)* se

$$f(a * b) = f(a) * f(b)$$

para quaisquer $a, b \in G$. Um homomorfismo bijetor é denominado um *isomorfismo*. Se existe um isomorfismo de G em G', dizemos que G e G' são *isomorfos* e escrevemos $G \cong G'$.

Teorema 1.1.11 (Teorema do Isomorfismo)**.** *Sejam G e G' grupos e $f : G \to G'$ um homomorfismo. Então:*

1. $\mathrm{im}(f) = \{f(x) : x \in G\}$ *é um subgrupo de G'.*

2. $\ker(f) = \{x \in G : f(x) = e'\}$ *é um subgrupo normal de G.*

3. $\frac{G}{\ker f} \cong \mathrm{im}(f)$.

A demonstração do teorema abaixo foi extraída de [5].

Demonstração. (1) Temos que $f(e) = f(e \cdot e) = f(e) \cdot f(e) \Leftrightarrow f(e) \cdot (f(e) - e') = 0 \Leftrightarrow f(e) = 0$ ou $f(e) = e'$. Porém se $f(e) = 0$, temos que $f(a) = f(a \cdot e) = f(a) \cdot f(e) = 0$ o que é aburdo, pois f seria sempre nula, logo $f(e) = e'$ e portanto $Im(f) \neq \emptyset$. Note que $f(b \cdot b^{-1}) = f(e) = e' = f(b) \cdot f(b^{-1})$, ou seja $f(b^{-1}) = f^{-1}(b)$. Temos ainda que $f(a), f(b) \in Im(f)$, logo $f(a) \cdot f^{-1}(b) = f(a \cdot b^{-1}) \in Im(f), \forall a, b \in G$. Logo $Im(f)$ é um subgrupo de G'.

(2) Temos que $e \in ker(f)$, pois $f(e) = e'$. Note ainda que se $a, b \in ker(f) \Rightarrow f(a \cdot b) = f(a) \cdot f(b) = e' \cdot e' = e'$, portanto $a \cdot b \in ker(f)$. Por fim se $a \in Ker(f) \Rightarrow f(a^{-1}) = f^{-1}(a) = e'^{-1} = e'$, portanto $a^{-1} \in ker(f)$.

Finalmente se $a \in Ker(f)$ e $g \in G$, vem que $f(g^{-1} \cdot a \cdot g) = f(g^{-1}) \cdot f(a) \cdot f(g) = f^{-1}(g) \cdot e' \cdot f(g) = e'$, logo $g^{-1} \cdot a \cdot g \in ker(f), \forall g \in G$ e assim $Ker(f)$ é um subgrupo normal de G.

Vamos mostrar agora que f é injetiva se, e somente se, $ker(f) = \{e\}$.

Suponha que $a, b \in G$, temos que $f(a) = f(b) \Leftrightarrow f(a) \cdot f^{-1}(b) = e' \Leftrightarrow f(a \cdot b^{-1}) = e' \Leftrightarrow a \cdot b^{-1} \in ker(f)$. E daí segue a conclusão pois se f for injetiva temos que $a = b$ e assim $a \cdot b^{-1} = e$. De maneira analóga, se $Ker(f) = \{e\}$ segue que $b^{-1} = a^{-1} \Leftrightarrow b = a$.

(3) Vamos definir $\overline{G} = \frac{G}{ker(f)}$ e considerar a função $\overline{f} : \overline{G} \to Im(f)$ relacionando $\overline{g} \rightsquigarrow f(g)$. Primeiramente $\overline{f}$ está bem definida, pois $\overline{a} = \overline{b} \Rightarrow a \cdot b^{-1} \in ker(f) \Rightarrow f(a \cdot b^{-1}) = e' \Rightarrow f(a) = f(b)$. Note ainda que $Im(f) = Im(\overline{f})$ e portanto $\overline{f}$ é uma função sobrejetora.Agora se $\overline{a}, \overline{b} \in \overline{G}$, vem que $\overline{f}(\overline{a} \cdot \overline{b}) = f(a \cdot b) = f(a) \cdot f(b) = \overline{f}(\overline{a}) \cdot \overline{f}(\overline{b})$, ou seja, f é um homomorfismo sobrejetivo. Vamos agora mostrar que $\overline{f}$ é injetora.

$\overline{f}(\overline{a}) = e' \Leftrightarrow f(a) = e' \Leftrightarrow a \in Ker(f) \Leftrightarrow \overline{a} = \overline{e}$, logo $Ker(\overline{f}) = \{\overline{e}\}$ e portanto $\overline{f}$ é injetora. Logo $\overline{f}$ é um isomorfismo de $\overline{G}$ sobre $Im(f)$, ou seja $\frac{G}{Ker(f)} \backsimeq Im(f)$. □

Definição 1.1.12. Dizemos que um grupo G é *solúvel* se existem subgrupos $G_0, G_1, \ldots, G_n$ de G tais que

$$\{e\} = G_n \subseteq \ldots \subseteq G_1 \subseteq G_0 = G,$$

$G_{i+1} \lhd G_i$ para cada $i \in \{0, \ldots, n-1\}$ e $\frac{G_i}{G_{i+1}}$ é abeliano.

Proposição 1.1.13. *Seja G um grupo solúvel. Se $H \leq G$ e $N \lhd G$, então H e $\frac{G}{N}$ são solúveis.*

1.2 Permutações

Uma *permutação* de um conjunto X é uma função bijetora de X em X.

Proposição 1.2.1. *Seja $X = \{1, 2, \ldots, n\}$. O conjunto S_n das permutações de X munido da operação da composição de funções é um grupo.*

Definição 1.2.2. Dizemos que $\sigma \in S_n$ é um *k-ciclo* se existem k e $i \in \{1, \ldots, n\}$ tais que k é o menor inteiro positivo tal que $\sigma^k(i) = i$ e σ fixa cada $j \notin \{i, \sigma(i), \ldots, \sigma^{k-1}(i)\}$.

Um 2-ciclo é chamado de *transposição*.

Proposição 1.2.3. *Todo elemento de S_n escreve-se como um produto de transposições.*

A demonstração da proposição abaixo foi extraída de [5].

Proposição 1.2.4. *Se um subgrupo G de S_n contém uma transposição e um n-ciclo, então $G = S_n$.*

Demonstração. Sejam $t = (12)$ e $a = (12 \ldots n)$ e considere G o subgrupo de S_n gerado por a e t. Temos que $a^{-1}ta = (23), a^{-2}ta^2 = (34)$ e assim sucessivamente, de modo que $(m, m+1)$ pertence a G.

Portanto G contém as transposições: $(12)(23)(12) = (13), (13)(34)(13) = (14)$ e assim sucessivamente , de modo que $(1m)$ pertence a G.

Logo G contém todos os produtos $(1m)(1r)(1m) = (mr)$. Como todo elemento de S_n é um produto de transposições, temos que $G = S_n$. □

As demonstrações abaixo foram extraída de [1].

Lema 1.2.5. *Se um subgrupo U de S_n $(n > 4)$ contém todos os 3-ciclos e se u é um subgrupo normal de U de modo que $\frac{U}{u}$ é abeliano, então u contém todos os 3-ciclos.*

Demonstração. Considere o homomorfismo natural $f : U \to \frac{U}{u}$ e considere dois elementos $x = (abc)$ e $y = (cde)$ de U. Como $\frac{U}{u}$ é abeliano temos que $f(x^{-1}\cdot y^{-1}\cdot x\cdot y) = e$, mas como podemos reescrever $x^{-1}\cdot y^{-1}\cdot x\cdot y = (cba)(edc)(abc)(cde) = (cbe)$, e para cada c, b, e temos que o 3-ciclo $(cbe) \in u$. □

Proposição 1.2.6. *S_n não é um grupo solúvel para $n \geq 5$.*

Demonstração. Pelo lema, uma sequência de subgrupos que testemunha a solubilidade de S_n jamais poderia terminar na identidade, visto que S_n contém todos os 3-ciclos. □

1.3 Anéis

Definição 1.3.1. Considere um conjunto A nos qual estão definidas duas propriedades $(+, \cdot)$ dizemos que A é um *anel* se as seguintes condições forem satisfeitas:

- $(A, +)$ é um grupo abeliano
- $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (Associatividade do produto)
- $a \cdot (b + c) = a \cdot b + a \cdot c$ (Distributividade do produto)

Dizemos que A é um **anel com identidade** se existir um elemento $1 \in A$ tal que $1 \cdot a = a \cdot 1 = a \quad \forall a \in A$.

Um anel é dito **comutativo** se o produto for comutativo.

Exemplo: O conjunto dos inteiros módulo n, denotado por Z_n, é um anel comutativo com unidade.

Um anel é dito **sem divisores de zero** se $\forall a, b \in A$ temos que $a \cdot b = 0 \Leftrightarrow a = 0$ ou $b = 0$.

Exemplo: O conjunto $\mathbb{Z}$ é um anel sem divisores de zero.

Se $A(+, \cdot)$ for um anel comutativo, com unidade e sem divisores de zero chamamos A de um **domínio de integridade**.

Definição 1.3.2. Um domínio de integridade que satisfaz a propriedade $\forall b \neq 0 \in A, \exists a \in A$ tal que $b \cdot a = a \cdot b = 1$ é chamado de **corpo**.

Exemplo: O conjunto dos inteiros z_p com p primo é um corpo.

Definição 1.3.3 (Subcorpo)**.** Um subconjunto não vazio B, de um corpo A é um *subcorpo* de A, se relativo às operações $+, \cdot$ de A, B também for um corpo.

Exemplo: $\mathbb{R}$ é um subcorpo de $\mathbb{C}$

No decorrer deste texto iremos trabalhar apenas com subcorpos de $\mathbb{C}$

Se E e F são subcorpos de $\mathbb{C}$ tais que $F \subseteq E$, então E é um F-espaço vetorial. Denotaremos por $[E : F]$ a dimensão de E sobre F, caso esta seja finita.

1.4 Polinômios

Um *polinômio* com coeficientes em um subanel A de $\mathbb{C}$ é uma expresão da forma

$$a_n x^n + \ldots a_1 x + a_0$$

onde $n \in \mathbb{N}$, $a_0, a_1, \ldots, a_n \in A$ e x é uma variável. Os elementos $a_0, a_1, \ldots, a_n$ são denominados os seus *coeficientes*. Denotaremos por $A[x]$ o conjunto de todos os polinômios com coeficientes em A.

Se $f(x) \neq 0$ é um polinômio com coeficientes complexos, então o seu *grau* é a maior potência de x com coeficiente não nulo que ocorre em $f(x)$.

Proposição 1.4.1 (Algortimo da divisão)**.** *Sejam F um subcorpo de $\mathbb{C}$ e $f(x), g(x) \in F[x]$ com $g(x)$ não-nulo. Existem únicos $q(x), r(x) \in F[x]$ tais que $f(x) = g(x) \cdot q(x) + r(x)$ com $r(x) = 0$ ou $\partial r(x) < \partial g(x)$.*

Corolário 1.4.2. *Sejam F um subcorpo de $\mathbb{C}$, $f(x) \in F[x]$ e $a \in F$. Temos que $f(a) = 0$ se, e somente se, existe $p(x) \in F[x]$ tal que $f(x) = (x - a) \cdot p(x)$.*

Dizemos que um número complexo a é uma *raiz* de $f(x) \in \mathbb{C}[x]$ se $f(a) = 0$.

Teorema 1.4.3 (Teorema Fundamental da Álgebra)**.** *Seja $f(x) \in \mathbb{C}[x]$ com $\partial f(x) \geq 1$. Então $f(x)$ tem uma raiz em $\mathbb{C}$.*

Definição 1.4.4. Sejam F um subcorpo de $\mathbb{C}$ e $f(x) \in F[x]$ com $\partial f(x) \geq 1$. Dizemos que $f(x)$ é *irredutível sobre F* se $f(x)$ não puder ser expresso como um produto de dois polinômios em $F[x]$ ambos de grau menor que o grau de $f(x)$.

Proposição 1.4.5 (Lema de Gauss). *Seja $f(x) \in \mathbb{Z}[x]$ tal que $f(x)$ é irredutível sobre $\mathbb{Z}$ então $f(x)$ é irredutível sobre $\mathbb{Q}$.*

As demonstrações abaixo foram extraídas de [5]

Demonstração. Suponha que $f(x)$ seja irredutível sobre $\mathbb{Z}$ mas f$(x) = g(x) \cdot h(x)$, onde $g(x), h(x) \in \mathbb{Q}[x]$ e $\partial g(x) \geq 1$ $\partial h(x) < \partial f(x)$. Sendo m o mínimo múltiplo comum dos denominadores do produto $g(x) \cdot h(x)$, temos que o polinômio $mg(x) \cdot h(x) = mf(x) \in \mathbb{Z}[x]$. Considere então $mf(x) = g_1(x) \cdot h_1(x), g_1, h_1 \in \mathbb{Z}[x]$.

Temos então que $g_1(x) = a_0 + a_1x + \cdots + a_rx^r$ e $h_1(x) = b_0 + b_1x + \cdots + b_sx^s$, tal que $a_i, b_i \in \mathbb{Z}$. Suponha agora p um primo tal que $p|m$. Temos alguns casos a considerar:

1. p divide todos os coeficientes de $g_1(x)$ ou de $h_1(x)$.

2. Existe a_1 e b_j com i e j menores possíveis tais que $p \nmid a_i$ e $p \nmid b_j$.

   Porém p deve dividir o coeficiente de x^{j+i} de $g_1(x) \cdot h_1(x)$ que é $b_0 \cdot a_{i+j} + b_1 \cdot a_{i+j-1} + \cdots + b_j \cdot a_i + \cdots + b_{i+j-1} \cdot a_1 + b_{i+j} \cdot a_0$. Porém como escolhemos os menores i e j,temos que p divide toda as parcelas da expressão com exceção de $b_j \cdot a_i$. Mas p divide toda a expressão e portanto p também deve dividir $b_j \cdot a_i$ e sendo p primo temos que $p|b_j$ ou $p|a_i$ o que é uma contradição

Sem perda de generalidade podemos supor que p divide todos os coeficientes de $g_1(x)$. Escrevendo $m = m_1 \cdot p$ e $g_1(x) = p \cdot g_2(x)$, podemos reescrever $m_1 f(x) = g_2(x) \cdot h_1(x)$. Repetindo o processo com todos os fatores primos de m como feito acima, podemos em um dado momento cancelar todos os fatores primos de m chegando na expressão $f(x) = g^*(x) \cdot h^*(x), g^*(x), h^*(x) \in \mathbb{Z}[x]$ o que é absurdo pois $g(x)$ e $h(x)$ são irredutíveis em $\mathbb{Z}[x]$. □

Proposição 1.4.6 (Critério de Eisenstein). *Seja $f(x) = a_0 + a_1x + \ldots + a_nx^n \in \mathbb{Z}[x]$. Se existe um número primo p tal que*

- $p \nmid a_n$,
- $p \mid a_0, a_1, \ldots, a_{n-1}$ *e*
- $p^2 \nmid a_0$

então $f(x)$ é irredutível sobre $\mathbb{Q}$.

Demonstração. Pelo Lema de Gauss basta mostrarmos que $f(x)$ é irredutível em $\mathbb{Z}[x]$.

Suponha por contradição que $f(x) = g(x) \cdot h(x)$ e $g(x) = b_0 + b_1x + \cdots + b_rx^r$ e $h(x) = c_0 + c_1x + \cdots + c_sx^s$ e $s \geq 1, r \geq 1$ e $s + r = n$. Temos então que $a_0 = c_0 \cdot b_0$ e por (b) temos que $p \mid b_0$ ou $p \mid c_0$, porém por (c) p não pode dividir ambos, logo sem perda de generalidade suponha que $p \mid b_0$. Se todos os b_i são divisivéis por p temos uma contradição com (a). Suponha então que b_j é o primeiro coeficiente de $g(x)$ que não é divisível por p. Então $a_i = b_0 \cdot c_i + b_1 \cdot c_{i-1} + \cdots + b_i \cdot c_0$.

Como $p \mid a_i$ e $p \mid b_0, b_1, \ldots, b_{j-1}$ e $p \nmid b_j$ vem que $p \mid c_0$ o que é uma contradição e portanto $f(x)$ é irredutível em $\mathbb{Z}[x]$. □

Exemplo: Tomando $p = 2$ é fácil ver que o polinômio $p(x) = x^5 - 4x^3 + 2x - 2$ é irredutível pelo Critério de Eisenstein.

1.5 Extensões de corpos

Sejam E e F subcorpos de $\mathbb{C}$.

Definição 1.5.1. Dizemos que E é uma *extensão* de F se $F \subseteq E$.

Exemplo: $\mathbb{R}$ é uma extensão de $\mathbb{Q}$

Definição 1.5.2. Se $\alpha \in \mathbb{C}$, então a intersecção de todos os subcorpos de $\mathbb{C}$ que contêm F e α é uma extensão de F, a qual será denotada por $F(\alpha)$.

Exemplo: $Q(\sqrt{2}) = \{a + b\sqrt{2}, a, b \in \mathbb{Q}\}$

Definição 1.5.3. Seja E uma extensão de F. Dizemos que $\alpha \in E$ é *algébrico sobre* F se existe $f(x) \in F[x]$, $f(x) \neq 0$, tal que $f(\alpha) = 0$.

Exemplo: Considere $p(x) = x^2 - 2 \in \mathbb{Q}[x]$, logo $\sqrt{2}$ é algébrico sobre $\mathbb{Q}$.

Definição 1.5.4. Sejam E uma extensão de F e $\alpha \in E$ algébrico sobre F. O polinômio mônico de menor grau em $F[x]$ que tem α como raiz será denotado por $\mathrm{irr}(\alpha, F)(x)$.

Observe que $\mathrm{irr}(\alpha, F)(x)$ é irredutível sobre F e que $\mathrm{irr}(\alpha, F)(x)$ divide todo polinômio em $F[x]$ que tem α como raiz.

Exemplo: $irr(\sqrt{2}, \mathbb{Q})(x) = x^2 - 2$.

Proposição 1.5.5. *Seja $\alpha \in \mathbb{C}$ algébrico sobre F. Se n é o grau de $\mathrm{irr}(\alpha, F)$, então $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ é uma base de $F(\alpha)$ sobre F.*

Exemplo: A base de $\mathbb{Q}(\sqrt{2})$ sobre $\mathbb{Q}$ é dada por $\{1, \sqrt{2}\}$

Proposição 1.5.6. *Sejam K, L e M subcorpos de $\mathbb{C}$ tais que $K \subseteq L \subseteq M$ e $[M : L]$ e $[L : K]$ são finitos. Então $[M : K] = [M : L] \cdot [L : K]$.*

A demonstração abaixo foi extraída de [5]

Demonstração. Seja $v_1, v_2, \ldots, v_r$ uma base de M sobre L e seja $u_1, \ldots, u_s$ uma base de L sobre K. Considere $\beta = v_i \cdot u_j$, tal que $i = 1, \ldots, r$ e $j = 1, \ldots, s$. Precisamos provar que β é um conjunto $L.I.$ e que também é um gerador de M sobre K. Considerando $\alpha_{ij} \in K$, $1 \leq i \leq r$ e $1 \leq j \leq s$ e $\sum_{i,j} \alpha_{ij} v_i u_j = 0$

Reescrevendo a expressão acima temos que $\sum_i (\sum_j \alpha_{ij} u_j) v_i = 0$. Como $\sum_j \alpha_{ij} u_j$ está em L temos que $\sum_j \alpha_{ij} u_j = 0$, pois $v_1, \ldots, v_r$ é um conjunto $L.I.$ mas de maneira analóga, temos que $\alpha_{ij} \in K$ e como o conjunto $u_1, \ldots, u_s$ também é $L.I.$ segue que $\alpha_{ij} = 0$ para todo par (i, j), o q mostra que β é um conjunto $L.I.$ de M sobre K.

Vamos mostrar agora que β é o conjunto gerador de M sobre K.

Como $v_1, \ldots, v_r$ é a base de M sobre L, existem $\gamma_1, \ldots, \gamma_r \in L$ e $y \in M$ tal que $y = \gamma_1 v_1 + \cdots + \gamma_r v_r$.

Mas sendo $\gamma_i \in L$ e $u_1, \ldots, u_s$ a base de L sobre K existem $\alpha_{ij} \in K, 1 \leq i \leq r$, $1 \leq j \leq s$ tais que $\gamma_i = \alpha_{i1} u_1 + \cdots + \alpha_{is} u_s$, segue então que $y = \sum_{i,k} \alpha_{ij} v_i u_j$, para todo $\alpha_{ij} \in K$. □

Definição 1.5.7. Seja $f(x) \in F[x]$. O *corpo de decomposição de $f(x)$ sobre F* é o menor subcorpo de $\mathbb{C}$ que contém todas as raízes de $f(x)$ em $\mathbb{C}$.

Em outras palavras, se $\alpha_1, \ldots, \alpha_n$ são as raízes de $f(x)$ em $\mathbb{C}$, então o corpo de decomposição de $p(x)$ sobre F é $F(\alpha_1, \ldots, \alpha_n)$.

Exemplo: O corpo de decomposição de $f(x) = x^2 - 2 \in \mathbb{Q}[x]$ é dado por $\mathbb{Q}(\sqrt{2})$.

2 RESOLUÇÃO POR RADICAIS

O objetivo da álgebra clássica era expressar as raízes da equação geral de grau n

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

em termos dos coeficientes $a_0, a_1, \ldots, a_n$ usando uma quantidade finita de operações $+, -, \times, \div$ e radicais $\sqrt{\ }, \sqrt[3]{\ }, \ldots$

Por exemplo, as raízes x_1 e x_2 da equação

$$a_2 x^2 + a_1 x + a_0 = 0 \ \ (a_2 \neq 0)$$

são dadas pela fórmula

$$x_1, x_2 = \frac{-a_1 \pm \sqrt{a_1^2 - 4a_2 a_0}}{2a_2}$$

o que nos leva a dizer que equações quadráticas são *solúveis por radicais*.

Mostraremos que, assim como as equações quadráticas, as cúbicas e quárticas também são solúveis por radicais e exibiremos uma equação de grau 5 que não é solúvel por radicais.

2.1 Equações quadráticas

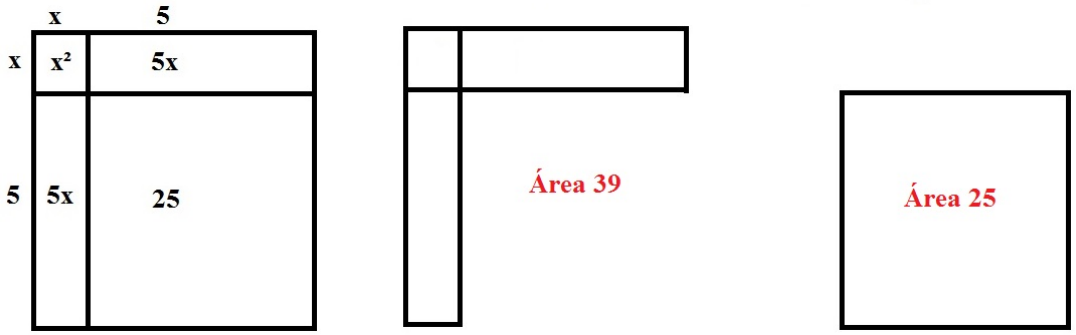
Os primeiros avanços na resolução dessas equações datam de 2000 a.C. e são atribuídos aos babilônios. Eles resolviam as equações pelo método de completar quadrados, porém sem uma fórmula específica. A grande maioria dos problemas tinha significado geométrico e, portanto, raízes negativas não faziam parte da solução. Vale ressaltar que números irracionais e complexos não faziam parte da matemática da época.

No século IX, com a expansão árabe, o califa Al-Mamum (786 + 47 = 833) decretou

o início das traduções dos textos gregos e estabeleceu a Casa da Sabedoria em Bagdá. Al-Khowarizmi (780 + 70 = 850), um dos mestres dessa casa, se propôs a fazer uma ponte entre duas áreas da matemática grega — a saber, os números e a geometria. Esse novo campo recebeu o nome *álgebra*. A palavra *álgebra* se origina de *Al-Jabr*, um dos livros de Al-Khowarizmi (cujo nome dá origem à palavra algarismo).

Figura 2.1: Al-Khowarizmi

Um dos problemas propostos por Al-Khowarizmi é a resolução da equação $x^2 + 10x = 39$.



(a) Fig.1 (b) Fig.2 (c) Fig.3

Figura 2.2: Resolução da equação $x^2 + 10x = 39$

Note que a expressão $x^2 + 10x = 39$ pode ser interpretada como a soma da área de um quadrado de lado x com a área de dois retângulos de lado x e 5. A figura 2, em "L"representa essa situação. Para completarmos o quadrado devemos adicionar um quadrado de lado 5 cuja área será 25, conforme a figura 3. Observando a figura 1, temos então que a soma das áreas é 64 e, portanto, a medida do lado do quadrado

maior deve ser 8. Para determinar o lado x do quadrado menor basta fazer $8-5=3$, que é uma solução de $x^2+10x=39$.

Uma outra grande contribuição para a resolução das equações quadráticas se deu com os hindus — em particular, com Bhaskara $(1114+71=1185)$ através da obra *Lilavati*. Diferentemente dos árabes, os hindus aceitavam números negativos e irracionais e conheciam a fórmula para a resolução das equações quadráticas obtendo as duas raízes reais quando estas existiam. O conjunto dos números complexos não havia surgido nesta época.

Através do método de completar quadrados, vamos demonstrar a fórmula da resolução das equações de segundo grau $ax^2+bx+c=0$, $a\neq 0$.

$$\begin{aligned} ax^2+bx+c=0 &\Leftrightarrow x^2+\tfrac{b}{a}x+\tfrac{c}{a}=0 \\ &\Leftrightarrow x^2+\tfrac{b}{a}x+\tfrac{b^2}{4a^2}=\tfrac{b^2}{4a^2}-\tfrac{c}{a} \\ &\Leftrightarrow \left(x+\tfrac{b}{2a}\right)^2=\tfrac{b^2-4ac}{4a^2} \\ &\Leftrightarrow x+\tfrac{b}{2a}=\pm\tfrac{\sqrt{b^2-4ac}}{2a} \\ &\Leftrightarrow \end{aligned}$$

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

2.2 Equações cúbicas

Assim como no caso das equações quadráticas, as primeiras contribuições para a resolução de equações cúbicas apareceram com os babilônios. É conhecida uma tábua que fornece o resultado de n^3+n^2 para valores de n variando de 1 a 10.

Em Bagdá, Omar Khayyan (1050 + 73 = 1123) resolve o problema das cúbicas através de métodos geométricos. Uma de suas raízes eram as abscissas dos pontos de intersecção de uma circunferência e uma hipérbole equilátera ou de duas hipérboles equiláteras.

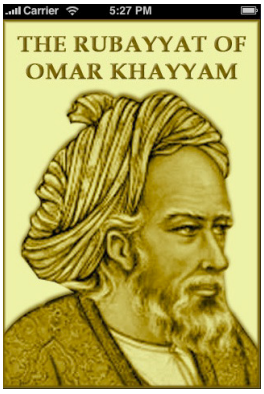


Figura 2.3: Omar Khayyan

Como exemplo considere a resolução do problema: "Um cubo, alguns lados e alguns números são iguais a alguns quadrados", que pode ser escrito da seguinte forma $x^3 + bc + c = ax^2$.

Os passos abaixo foram retirados de [15]

1. Trace três linhas de comprimento $\frac{c}{b}$, $\sqrt{b}$ e a, com um ângulo reto

2. Desenhe um semicírculo cujo diâmetro seja uma linha horizontal. Estenda a linha vertical até interceptá-lo. Se a linha sólida vertical tiver o comprimento d, faça uma linha grossa horizontal com o comprimento de $\frac{cd}{\sqrt{b}}$

3. Desenha uma hipérbole cujas assíntotas sejam linhas sombreadas, passando pelo ponto recém-encontrado

4. Localize onde a hipérbole intercepta o semicírculo. Os comprimentos das duas linhas sólidas, marcadas como x, serão as duas soluções (positivas) da cúbica.

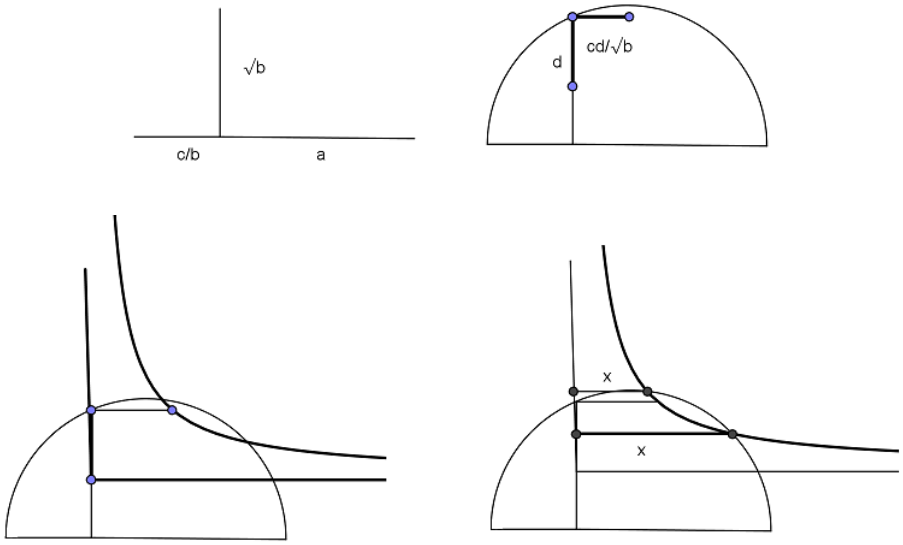


Figura 2.4: Solução da cúbica por Omar Khayyan

Daremos, agora, um enorme salto histórico até a Europa do século XV. Estamos na época da Renascença, onde a busca exacerbada pelo conhecimento ajudou a aflorar diversos talentos como Da Vinci, Michelângelo, Machiavel, Colombo, etc. Todas as áreas de estudos tiveram grandes avanços e a matemática não poderia ficar de fora. É o momento ideal para buscar a solução para problemas sem respostas há milhares de anos.

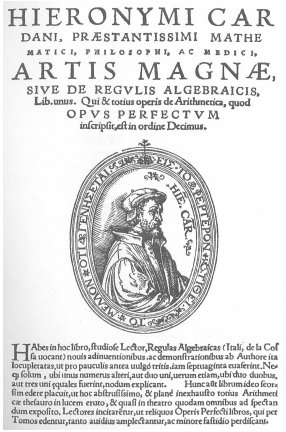
Nossa história começa em 1515, com Scipione Del Ferro (1465 + 61 = 1526), professor da Universidade de Bologna. Ele conseguiu resolver cúbicas da forma $x^3 + px + q = 0$ e, pouco antes de morrer, deu a regra (mas não a prova) a seu aluno Antonio de Fior. Simultaneamente, Niccolò Fontana (1499 + 58 = 1557), mais conhecido como Tartaglia, professor em Veneza, também conseguiu resolver cúbicas, porém da forma $x^3 + px^2 + q = 0$. Tartaglia também espalhou a notícia, porém sem revelar o método.

Imagine uma situação na qual um matemático recebe de outro um pedido de desafio para ver qual dos dois é o melhor perante toda a sociedade! Hoje pode parecer estranho pensar em tal situação de uma maneira pública, porém estes eram muito comuns na época. Alguns contratos de professores e mesmo a permanência na cátedra dependia de um bom desempenho em tais disputas. Podemos pensar que isso explicaria o motivo de Del Ferro não divulgar o seu trabalho, afinal de

contas caso ele fosse desafiado para uma disputa ele deveria ter algo grandioso em mãos para por em cheque o seu adversário. Em 1535, Fior resolveu fazer um desafio a Tartaglia no qual cada um iria propor ao outro uma lista com 30 problemas e daria 40 a 50 dias para o outro resolvê-lo. Faltando pouco tempo para o fim da competição Tartaglia descobriu não só como resolver as cúbicas da forma $x^3 + px + q = 0$ como descobriu uma fórmula para a resolução de todos os tipos de cúbicas. Tartaglia venceu a disputa, mas mesmo assim deixou seu método em segredo.

A notícia logo se espalhou pela Europa chegando aos ouvidos de Girolamo Cardano (1501 + 75 = 1576) que chamou Tartaglia e pediu que revelasse seu método, prometendo que o manteria em segredo. Porém, pouco tempo depois, Cardano publicou em 1545 a solução no seu livro chamado *Ars Magna*. Isso deu sequência a uma longa discussão entre Tartaglia e Cardano, no qual Cardano afirmou ter tido acesso aos manuscritos de Del Ferro. Targalia chegou a publicar *Quesiti e Inventioni Diverse*, livro no qual ele apresenta a solução para diversos problemas além de fatos autobiográficos como a suposta traição de Cardano. Ludovico Ferrari (1522 + 43 = 1565), um discípulo de Cardano, publicou no ano seguinte um panfleto no qual defendia o seu mestre e seguiu-se então uma longa troca de acusações através de 12 panfletos conhecidos como *Cartelli di Sfida Mathematica*. Por fim, Tartaglia aceitou um desafio para um debate matemático com Ferrari e, apesar do resultado não ter ficado muito claro, as autoridades universitárias não gostaram do desempenho de Tartaglia que acabou perdendo o emprego e morreu pobre e obscuro nove anos depois.

(a) Tartaglia



(b) Cardano: Ars Magna

Cabe ressaltar que o uso de letras para representar números teve início com Viète, em 1591. O que Cardano publicou eram receitas ou regras explicadas com exemplos numéricos para cada tipo de equação.

Segue abaixo um método para resolver a cúbica $x^3 + px + q = 0$.

Ele baseia-se na expressão

$$(u+v)^3 = 3uv(u+v) + (u^3 + v^3)$$

Relacionando-a com a equação cúbica $x^3 = -px - q$, passamos a buscar uma solução x da forma $x = u + v$, onde

$$\begin{cases} 3uv = -p \\ u^3 + v^3 = -q \end{cases}$$

As equações acima levam à equação quadrática

$$w^2 + qw - \left(\frac{p}{3}\right)^3 = 0$$

que tem u^3 e v^3 como raízes, uma vez que

$$\begin{cases} u^3 + v^3 = -q \\ u^3 v^3 = -\left(\frac{p}{3}\right)^3. \end{cases}$$

Aplicando o método de resolução para equações de grau 2 e usando o fato que $x = u + v$, obtemos a fórmula

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

Cardano desenvolveu um método de resolução para equações de grau 3 com o termo quadrático incluso. Fazendo $x = y - \frac{a}{3}$, ele transformou a equação $x^3 + ax^2 + bx + c = 0$ em

$$y^3 + py + q = 0$$

onde

$$p = -\frac{1}{3}a^2 + b$$
$$q = \frac{2}{27}a^3 - \frac{1}{3}ab + c$$

tornando possível aplicar o método de Tartaglia para a resolução. Subtraindo $\frac{a}{3}$ de cada raiz da equação reduzida, obtemos as raízes da cúbica completa.

O que parece ser um truque de "matemágica" tem origem nas relações entre coeficiente e raízes: se x_1, x_2 e x_3 são as raízes de $x^3 + ax^2 + bx + c = 0$ então $x_1 + x_2 + x_3 = -a$ e, portanto, $x_1 + \frac{a}{3} + x_2 + \frac{a}{3} + x_3 + \frac{a}{3} = 0$. Logo, a transformação $y = x + \frac{a}{3}$ elimina o termo de grau 2.

2.3 Equações quárticas

Os primeiros registros de resolução de quárticas datam de 1600 a.C. e encontram-se em algumas tábuas babilônicas da coleção de Yale. Elas apresentam equações simultâneas que caem em equações biquadradas. Um exemplo seria

$$\begin{cases} xy = 600 \\ 150(x - y) - (x + y)^2 = -1000 \end{cases}$$

Já na Europa, Cardano tinha dificuldades em resolver esse tipo de equação devido à falta de interpretação geométrica.

Cardano resolve então encorajar seu aluno, Ludovico Ferrari (1522 + 43 = 1565) a resolver tais equações. Ferrari consegue resolvê-las e Cardano também as publica no seu livro *Ars Magna*.

Ferrari era capaz de resolver uma equação da forma $x^4 + px^2 + qx + r = 0$ através de radicais.

Note que uma equação da forma

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

pode ser reescrita como

$$x^4 = -px^2 - qx - r.$$

Ferrari adicionou a ambos os lados da equação acima o termo $2x^2z+z^2$, completando assim um quadrado perfeito no lado esquerdo da equação:

$$(x^2+z)^2 = (2z-p)x^2 - qx + (z^2-r).$$

Podemos atribuir um comportamento de quadrado perfeito ao lado direito da equação desde que escolhamos z satisfazendo a condição

$$2\sqrt{2z-p}\sqrt{z^2-r} = -q.$$

Elevando ao quadrado ambos os lados da equação acima, obtemos

$$z^3 - \frac{p}{2}z^2 - rz + \left(\frac{pr}{2} - \frac{q^2}{8}\right) = 0$$

onde z pode ser obtido através da resolução da equação acima pelo método de Cardano e Tartaglia descrito anteriormente. Voltando então agora na nossa equação quártica temos que

$$(x^2+z)^2 = (\sqrt{2z-p}x + \sqrt{z^2-r})^2 \Leftrightarrow x^2+z = \pm(\sqrt{2z-p}x + \sqrt{z^2-r}).$$

Assim as raízes da equação $x^4+px^2+qx+r=0$ podem ser expressas através das fórmulas

$$x_{1,2} = \frac{1}{2}\sqrt{2z-p} \pm \sqrt{-\frac{1}{2}z - \frac{1}{4}p + \sqrt{z^2-r}}$$

$$x_{3,4} = -\frac{1}{2}\sqrt{2z-p} \pm \sqrt{-\frac{1}{2}z - \frac{1}{4}p - \sqrt{z^2-r}}.$$

Se tivermos uma equação quártica completa na forma $x^4+ax^3+bx^2+cx+d=0$ podemos transformá-la numa equação do tipo $y^4+py^2+qy+r=0$ usando a transformação $y = x + \frac{a}{4}$ como fizemos nas equações cúbicas.

Temos então que as equações quárticas são solúveis por radicais.

2.4 Equações de grau maior que 4

Com o avanço na resolução das cúbicas e quárticas, era natural que os matemáticos tentassem chegar em expressões que fornecessem as soluções para as

equações de grau 5.

Em 1799, Ruffini $(1765 + 57 = 1822)$ foi um dos pioneiros a propor que a equação geral de quinto grau não podia ser resolvida por radicais, porém foram observadas lacunas em sua demonstração.

Abel $(1802 + 27 = 1829)$ foi o primeiro a apresentar uma prova completa da impossibilidade da solução da equação de quinto grau por meio de radicais, em 1821. Devido a uma péssima saúde Abel veio a falecer de tuberculose e subnutrição aos 26 anos. Na Noruega podemos encontrar um monumento a Abel na igreja de Froland.

Figura 2.5: Abel

Ao lado de Abel, um outro matemático proeminente e de vida mais curta foi Évariste Galois $(1811 + 21 = 1832)$. Seus trabalhos sobre as soluções das equações algébricas por radicais foram concluídos quando ele tinha apenas 17 anos. Apesar de ser um gênio, Galois não conseguiu entrar na Escola Politécnica e foi expulso da Escola Normal e do exército por suas exacerbadas ideias democráticas para a época. Galois se apaixonou pela filha de um médico que o tratou de cólera o que acabou levando-o a um duelo com outro amante, no qual ele perdeu sua vida. Antes de morrer, Galois deixou uma carta testamento com algumas de suas descobertas não publicadas nas quais grande matemáticos deveriam se debruçar nos próximos anos. Tais manuscritos deram origem ao que hoje chamamos de *Teoria de Galois*.

Figura 2.6: Galois

Nessa secção, daremos exemplo de uma equação de grau 5 que não é solúvel por radicais.

Definição 2.4.1. Sejam E e F subcorpos de $\mathbb{C}$ tais que $F \subseteq E$. Dizemos que E é uma *extensão radical* de F se $E = F(a_1, \cdots, a_n)$ onde, para cada $i \in \{1, \cdots, n\}$, existe $m_i \in \mathbb{N}$ tal que $a_1^{m_1} \in F$ e $a_i^{m_i} \in F(a_1, \cdots, a_{i-1})$ se $i \geq 2$.

Exemplo: $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ é uma extensão radical de $\mathbb{Q}$.

Definição 2.4.2. Sejam F um subcorpo de $\mathbb{C}$ e $f(x) \in F[x]$. Dizemos que $f(x) = 0$ é *solúvel por radicais* se existe uma extensão radical E de F tal que E contém o corpo de decomposição de $f(x)$ sobre F.

Definição 2.4.3. Seja E um subcorpo de $\mathbb{C}$. Uma aplicação $\varphi : E \to E$ diz-se um *automorfismo* de E se φ é bijetora e as seguintes condições são satisfeitas:

- $\varphi(x + y) = \varphi(x) + \varphi(y) \quad \forall x, y \in E$
- $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y) \quad \forall x, y \in E$

O conjunto dos automorfismos de E é denotado por $\mathrm{Aut}(E)$.

Exemplo:A função $\varphi : \mathbb{C} \to \mathbb{C}$ dada por $\varphi(a + bi) = a - bi$ é um automorfismo

Definição 2.4.4. Sejam E e F subcorpos de $\mathbb{C}$ tais que $F \subseteq E$. Dizemos que $\varphi \in \mathrm{Aut}(E)$ *fixa* F se $\varphi(x) = x$ para todo $x \in F$.O conjunto dos automorfismos de E que fixam F será denotado por $\mathrm{Aut}(E, F)$. Munido da operação de composição, $\mathrm{Aut}(E, F)$ é um grupo.

Definição 2.4.5. Sejam F um subcorpo de $\mathbb{C}$, $f(x) \in F[x]$ e $K \subseteq \mathbb{C}$ o corpo de decomposição de f sobre F. Definimos o *grupo de Galois de f sobre F* como $\mathrm{Gal}(f, F) = \mathrm{Aut}(K, F)$.

Teorema 2.4.6. *Sejam F um subcorpo de $\mathbb{C}$ e $f(x) \in F[x]$. Se $f(x) = 0$ é solúvel por radicais, então $\mathrm{Gal}(f, F)$ é solúvel.*

Demonstração. Como $f(x) = 0$ é solúvel por radicais, existe uma extensão radical E de F tal que $K \subset E$, onde K é o corpo de decomposição de $f(x)$ sobre F.

Sejam $a_1, \ldots, a_n \in \mathbb{C}$ e $p_1, \ldots, p_n \in \mathbb{N}$ tais que $E = F(a_1, \ldots, a_n)$, $a_1^{p_1} \in F$ e $a_i^{p_i} \in F(a_1, \ldots, a_{i-1})$ se $i \geq 2$.

Podemos supor que cada p_i é primo, que F contém todas as raízes p_1-ésima da unidade e que $F(a_1, \ldots, a_{i-1})$ contém todas as raízes p_i-ésimas da unidade.

Considere $F_0 = F$ e $F_i = F(a_1, \ldots, a_i)$. Seja, ainda, $G_i = \mathrm{Aut}(E, F_i)$.

Note que

$$\{1\} = G_n < G_{n-1} < \ldots < G_1 < G_0 = \mathrm{Aut}(E, F).$$

Seja $i \in \{0, \ldots, n-1\}$. Vamos mostrar que $G_{i+1} \triangleleft G_i$ e que $\frac{G_i}{G_{i+1}}$ é abeliano. Disto decorrerá que $\mathrm{Aut}(E, F)$ é solúvel.

Começamos observando que se $f \in G_i$, então $f[F_{i+1}] \subseteq F_{i+1}$. De fato, se $y \in F_{i+1}$ então y é uma combinação linear de potências de a_{i+1} com coeficientes em F. Logo, $f(y)$ fica completamente determinado pelo valor $f(a_{i+1})$. Se a_{i+1} é uma raiz p_{i+1}-ésima da unidade, então $f(a_{i+1})^{p_{i+1}} = f(a_{i+1}^{p_{i+1}}) = f(1) = 1$. Portanto, $f(a_{i+1})$ também é uma raiz p_{i+1}-ésima da unidade. Logo, $f(a_{i+1}) = a_{i+1}^j \in F_{i+1}$. Se a_{i+1} não é uma raiz p_{i+1}-ésima da unidade, então $f(a_{i+1})^{p_{i+1}} = f(a_{i+1}^{p_{i+1}}) = a_{i+1}^{p_{i+1}}$, pois $a_{i+1}^{p_{i+1}} \in F_i$. Portanto, $f(a_{i+1}) = \zeta^j a_{i+1}$ para alguma raiz p_{i+1}-ésima da unidade ζ e algum j. Como $\zeta \in F_i$, temos que $f(a_{i+1}) \in F_{i+1}$.

Observamos, ainda, que $\mathrm{Aut}(F_{i+1}, F_i)$ é abeliano. De fato, sejam $f, g \in \mathrm{Aut}(F_{i+1}, F_i)$. A fim de concluir que $f \circ g = g \circ f$, temos que mostrar que $(f \circ g)(x) = (g \circ f)(x)$ para todo $x \in F_{i+1}$. Para isto, basta mostrar que $(f \circ g)(a_{i+1}) = (g \circ f)(a_{i+1})$. No parágrafo acima, vimos as possíveis "caras" de $f(a_{i+1})$ e $g(a_{i+1})$ e daí segue que $(f \circ g)(a_{i+1}) = (g \circ f)(a_{i+1})$.

Portanto, se mostrarmos que

$$\begin{array}{rccc} \varphi: & G_i & \to & \mathrm{Aut}(F_{i+1}, F_i) \\ & f & \mapsto & f \restriction_{F_{i+1}} \end{array}$$

é um homomorfismo tal que $\ker\varphi = G_{i+1}$ teremos que $G_{i+1} \triangleleft G_i$ e $\frac{G_i}{G_{i+1}} \cong \operatorname{im}\varphi$ será abeliano. Daí decorre que $\mathrm{Aut}(E,F)$ é solúvel.

Temos que $\varphi(f \circ g) = \varphi(f) \circ \varphi(g)$, pois $\varphi(f \circ g)(x) = (f \circ g)(x) = f(g(x))$ e $(\varphi(f) \circ \varphi(g))(x) = \varphi(f)(\varphi(g)(x)) = \varphi(f)(g(x)) = f(g(x))$.

Além disso, $f \in \ker\varphi \Leftrightarrow \varphi(f) = \mathrm{id}_{F_{i+1}} \Leftrightarrow f\restriction_{F_{i+1}} = \mathrm{id}_{F_{i+1}} \Leftrightarrow f \in G_{i+1}$.

Por fim, como

$$\mathrm{Gal}(f,F) = \mathrm{Aut}(K,F) \cong \frac{\mathrm{Aut}(E,F)}{\mathrm{Aut}(E,K)}$$

e o quociente de um grupo solúvel é solúvel, concluímos que $\mathrm{Gal}(f,F)$ é solúvel. □

Lema 2.4.7. *Sendo p primo e $f(x)$ irredutível sobre $\mathbb{Q}$ de grau p, se $f(x)$ tem exatamente 2 raízes complexas não reais, então $Gal(f,\mathbb{Q}) \cong S_p$.*

Demonstração. Considere $K = \mathbb{Q}(\alpha_1, \cdots, \alpha_p) \subseteq \mathbb{C}$ o corpo de decomposição de $f(x)$ sobre $\mathbb{Q}$. Como $[\mathbb{Q}(\alpha_1) : \mathbb{Q}] = p$ e $\mathbb{Q} \subseteq \mathbb{Q}(\alpha_1) \subseteq K$, temos que $[K : \mathbb{Q}]$ deve ser divisível por p. Como $\mathrm{Gal}(f,\mathbb{Q}) = \mathrm{Aut}(K,\mathbb{Q})$ temos então que $|\mathrm{Gal}(f,\mathbb{Q})| = [K : \mathbb{Q}]$ e portanto $|\mathrm{Gal}(f,\mathbb{Q})|$ também é divisível por p. Pelo Teorema de Cauchy, $\mathrm{Gal}(f,\mathbb{Q})$ deve ter um elemento de ordem p. Como $\mathrm{Gal}(f,\mathbb{Q})$ pode ser visto como um subgrupo de S_p (considerando as raízes $\alpha_1, \cdots, \alpha_p$), $\mathrm{Gal}(f,\mathbb{Q})$ contém um p-ciclo.

Note ainda que os automorfismos de $\mathbb{C}$ que mapeiam um complexo ao seu conjugado deixam as raízes reais fixas e trocam as raízes complexas. Pensando em termos de permutação, temos uma transposição.

Como S_p é gerado por uma transposição e um p-ciclo, concluímos que $\mathrm{Gal}(f,\mathbb{Q}) \cong S_p$. □

Proposição 2.4.8. *Seja $f(x) = x^5 - 6x + 3 \in \mathbb{Q}[x]$. A equação $f(x) = 0$ não é solúvel por radicais.*

Demonstração. Temos que $f(x)$ é irredutível sobre $\mathbb{Q}$ pelo critério de Eisenstein aplicado ao número primo $p = 3$. Note ainda que $f'(x) = 5x^4 - 6$ e que $mdc(f(x), f'(x)) = 1$, logo não há uma raiz comum de $f(x)$ e $f'(x)$ e portanto não temos raízes múltiplas.

Sejam então $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5$ as raízes em $\mathbb{C}$. Note ainda que $f'(x)$ não possui 4 raízes reais. Basta tomar $y = x^2$ e resolvendo $5y^2 - 6 = 0 \Leftrightarrow y^2 = \frac{6}{5} \Leftrightarrow y = \pm\frac{\sqrt{30}}{5}$ temos que $x^2 = \frac{\sqrt{30}}{5}$ ou $x^2 = -\frac{\sqrt{30}}{5}$, logo $f'(x)$ tem apenas 2 raízes reais e portanto $f(x)$ não tem cinco raízes reais. Como o polinômio tem coeficientes reais, as raízes complexas não reais aparecem aos pares, ou seja podemos ter 2 ou

4 raízes complexas não reais nesse caso. Note agora que $f(0) = 3$, $f(1) = -2$ e $f(-2) = -17$, logo o polinômio $f(x)$ tem pelo menos 3 raízes reais. Concluímos então que o polinômio tem 3 raízes reais e 2 raízes complexas conjugadas. Portanto pelo lema anterior o grupo de Galois é isomorfo a S_5 e como este grupo não é solúvel, concluímos que esta equação não é solúvel por radicais. □

3 ABORDAGEM EM SALA DE AULA

O objetivo principal do capítulo 3 é mostrar como desenvolver com alunos do EM métodos que resolvam equações polinomiais.

Na maioria das escolas no Brasil, o estudante começa a aprender equações de segundo grau no 9º EF. É o primeiro contato não só com uma fórmula que resolve uma equação mas também é introduzido o conceito de função de 2º grau, o que já faz uma pequena associação entre uma expressão polinomial de segundo grau e sua representação gráfica.

No 1º EM é iniciado um estudo mais detalhado de funções, incluindo termos como raízes, crescimento, paridade e sinal.

O aluno retoma e aprofunda o estudo das equações polinomiais no 3º EM. Nesse momento ele aprende o Teorema Fundamental da Álgebra, a pesquisa das raízes racionais, o teorema das raízes conjugadas, as relações de Girard, multiplicidade de raízes, algoritmo da divisão de Briot-Ruffini e o Teorema do Resto e de D'Alembert.

Vamos supor que todo esse trabalho será desenvolvido para alunos do 3º EM.

3.1 Motivação

Equações algébricas ocorrem naturalmente nas aplicações, como mostram os exemplos abaixo.

Exemplo 1. (FGV 2009) O conhecimento que temos da matemática na Antiguidade vem, em boa parte, de textos matemáticos redigidos por escribas, propondo problemas para os alunos ou outros escribas resolverem. Leia com atenção esta adaptação do texto "Sou o escriba, o chefe dos trabalhadores", e resolva o problema que o autor propõe como um desafio a outro escriba:

(a) Temos de resolver um problema e calcular certa taxa de juros. Um velho mercador emprestou um capital de 8 moedas de ouro, a certa taxa anual de

juros compostos, durante três anos. Passado esse tempo, o velho mercador ficou muito contente; somente de juros, ele recebeu 19 moedas de ouro!

Os escribas estarão todos reunidos para descobrir a taxa de juros da aplicação, mas nenhum saberá como fazê-lo. Voltar-se-ão para ti e dirão:" Tu és um escriba hábil, meu amigo! Responde rápido para nós, honra tua reputação, para que não se possa dizer que existe alguma coisa que o chefe dos escribas não saiba: a que taxa anual de juros compostos o mercador aplicou o seu dinheiro?"

(b) Para encontrar a taxa de juros você resolveu uma equação polinomial de terceiro grau. Quais são as outras duas raízes dessa equação?

Solução.

(a) Como o capital é 8 e o juros é 19, o montante obtido é de 27 moedas de ouro. Sendo x a taxa anual de juros temos que

$$8(1+x)^3 = 27.$$

Logo, $x = \frac{1}{2}$, ou seja, 50%.

(b) Podemos seguir por dois caminhos: tirar as outras raízes cúbicas do número $\frac{27}{8}$ no campo dos números complexos ou aplicar Briot-Ruffini com a raiz $x = \frac{1}{2}$. Vamos fazer do segundo modo!

$$(1+x)^3 = \frac{27}{8} \Leftrightarrow x^3 + 3x^2 + 3x - \frac{19}{8} = 0.$$

Aplicando Briot-Ruffini obtemos

$$x^3 + 3x^2 + 3x - \frac{19}{8} = \left(x - \frac{1}{2}\right)\left(x^2 - \frac{7}{2}x + \frac{19}{4}\right).$$

Logo, as demais raízes são raízes de

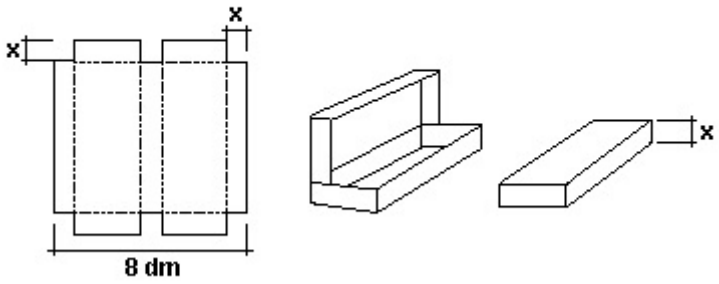
$$x^2 - \frac{7}{2}x + \frac{19}{4} = 0$$

e, portanto, são

$$x = \frac{-7 \pm 3\sqrt{3}i}{4}.$$

Note que, no caso do nosso problema, esses valores não representam respostas possíveis pois não são números reais.

Exemplo 2. (Uerj 2008) Para fazer uma caixa, foi utilizado um quadrado de papelão de espessura desprezível e $8dm$ de lado, do qual foram recortados e retirados seis quadrados menores de lado x. Em seguida, o papelão foi dobrado nas linhas pontilhadas, assumindo a forma de um paralelepípedo retângulo, de altura x, como mostram os esquemas.



Quando $x = 2dm$, o volume da caixa é igual a $8dm^3$. Determine outro valor de x para que a caixa tenha volume igual a $8dm^3$.

Solução. O volume da caixa é dado por

$$V = (\frac{8-3x}{2})(8-2x)x = 3x^3 - 20x^2 + 32x.$$

Fazendo $V = 8$, obtemos a equação polinomial

$$3x^3 - 20x^2 + 32x - 8 = 0.$$

Como 2 é raiz, segue que

$$3x^3 - 20x^2 + 32x - 8 = (x-2)(3x^2 - 14x + 4)$$

e portanto as outras raízes são

$$x = \frac{7 \pm \sqrt{37}}{3}.$$

Como $8 - 3x > 0 \Leftrightarrow x < \frac{8}{3}$ temos que a única solução possível seria

$$x = \frac{7 - \sqrt{37}}{3}.$$

3.2 Equações de 2º grau

Sugerimos que o professor recorde rapidamente como resolver equações de 2º grau.

Exemplos.

1. $x^2 - 5x + 6 = 0$

   $\Delta = (-5)^2 - 4 \cdot 1 \cdot 6 = 1$

   $x = \frac{-(-5) \pm \sqrt{1}}{2 \cdot 1} \Leftrightarrow x = 2$ ou $x = 3$.

   Neste caso, seria interessante incentivar o aluno a tentar resolver a equação por *soma* e *produto*. Como a soma das raízes da equação $ax^2 + bx + c = 0$ é dada por $S = -\frac{b}{a}$ e seu produto é dado por $P = \frac{c}{a}$, obtemos $S = 5$ e $P = 6$. É fácil ver que 2 e 3 são números que somados resultam em 5 e multiplicados resultam em 6. Logo, 2 e 3 são as raízes procuradas.

2. $2x^2 - 4x + 2 = 0$

   $2x^2 - 4x + 2 = 0 \Leftrightarrow x^2 - 2x + 1 = 0$

   $\Delta = (-2)^2 - 4 \cdot 1 \cdot 1 = 0$

   $x = \frac{-(-2) \pm \sqrt{0}}{2 \cdot 1} \Leftrightarrow x = 1$

   Por *soma* e *produto* temos $S = 2$ e $P = 1$. Logo as raízes são 1 e 1.

3. $x^2 + x - 1 = 0$

   $\Delta = (1)^2 - 4 \cdot 1 \cdot (-1) = 5$

   $x = \frac{-1 \pm \sqrt{5}}{2 \cdot 1} \Leftrightarrow x = \frac{-1 \pm \sqrt{5}}{2}$

   Por soma e produto temos $S = -1$ e $P = -1$, porém neste caso as respostas não são tão fáceis. Mas o professor deve mostrar ao aluno que mesmo a fórmula sendo o caso geral o método de *soma* e *produto* é mais rápido em determinados casos.

4. $x^2 - x + 1 = 0$

   $\Delta = (-1)^2 - 4 \cdot 1 \cdot 1 = -3 = (\sqrt{3}i)^2$

   $x = \frac{-(-1) \pm \sqrt{(\sqrt{3}i)^2}}{2 \cdot 1} \Leftrightarrow x = \frac{1 \pm \sqrt{3}i}{2}$

Seguem, abaixo, alguns casos de equações polinomiais de grau maior que podem ser reduzidas a grau 2 por meio de determinadas transformações:

5. $x^4 - 17x^2 + 16 = 0$

   Fazendo $y = x^2$ temos $y^2 - 17y + 16 = 0 \Leftrightarrow y = 16$ ou $y = 1$

   Logo $x^2 = 16$ ou $x^2 = 1 \Leftrightarrow x = \pm 4$ ou $x = \pm 1$

6. $x^4 - x^2 - 12 = 0$

   Sendo $y = x^2$ temos $y^2 - y - 12 = 0 \Leftrightarrow y = 4$ ou $y = -3$

   Logo $x^2 = 4$ ou $x^2 = -3 \Leftrightarrow x = \pm 2$ ou $x = \pm\sqrt{3}i$

7. $(x^2 - 5x + 7)^2 - (x - 2)(x - 3) = 1 \Leftrightarrow (x^2 - 5x + 7)^2 - (x - 5x + 7) = 0$

   Sendo $y = x^2 - 5x + 7$ temos $y^2 - y = 0 \Leftrightarrow y = 0$ ou $y = 1$

   Logo $x^2 - 5x + 7 = 0$ ou $x^2 - 5x + 7 = 1 \Leftrightarrow x = \frac{5 \pm i\sqrt{3}}{2}$ ou $x = 2$ ou $x = 3$

3.3 Fatoração

Uma das ferramentas mais poderosas que podemos utilizar é a fatoração.

Os métodos de fatoração são vistos pela primeira vez no 7º EF e ao longo do EM parecem ser algo à parte. Muitos alunos entendem que a fatoração deve ser usada apenas em exercícios do tipo "fatore a expressão" e não percebem as inúmeras aplicações que ela tem no cotidiano.

Vamos citar alguns exemplos de equações abaixo que são facilmente resolvidas em sua forma fatorada. O argumento que todos os estudantes devem ter em mente é que dado dois números complexos a e b temos que

$$ab = 0 \Leftrightarrow a = 0 \text{ ou } b = 0.$$

Exemplos.

1. $(x-2)(x-3)(x-4)=0 \Leftrightarrow \begin{cases} x-2=0 \\ x-3=0 \\ x-4=0 \end{cases} \Leftrightarrow \begin{cases} x=2 \\ \text{ou} \\ x=3 \\ \text{ou} \\ x=4 \end{cases}$

2. $x^3-1=0$

   Lembrando que $a^3-b^3=(a-b)(a^2+ab+b^2)$ temos que $x^3-1=(x-1)(x^2+x+1)$.

   Assim $x^3-1=0 \Leftrightarrow (x-1)(x^2+x+1)=0 \Leftrightarrow \begin{cases} x-1=0 \\ \text{ou} \\ x^2+x+1=0 \end{cases} \Leftrightarrow$

   $\begin{cases} x=1 \\ \text{ou} \\ x=\frac{-1\pm i\sqrt{3}}{2} \end{cases}$

3. $x^4-16=0$

   Lembrando que $a^4-b^4=(a^2-b^2)(a^2+b^2)=(a-b)(a+b)(a^2+b^2)$ temos que $x^4-16=(x-2)(x+2)(x^2+4)$. Assim

   $$x^4-16=0 \Leftrightarrow (x-2)(x+2)(x^2+4)=0 \Leftrightarrow \begin{cases} x-2=0 \\ \text{ou} \\ x+2=0 \\ \text{ou} \\ x^2+4=0 \end{cases} \Leftrightarrow \begin{cases} x=2 \\ \text{ou} \\ x=-2 \\ \text{ou} \\ x=\pm 2i \end{cases}$$

4. $x^3+5x^2+6x=0$

   Note que neste caso é possível colocar um fator comum em evidência!

$$x^3+5x^2+6x=0 \Leftrightarrow x(x^2+5x+6)=0 \Leftrightarrow \begin{cases} x=0 \\ \text{ou} \\ x^2+5x+6=0 \end{cases} \Leftrightarrow \begin{cases} x=0 \\ \text{ou} \\ x=-2 \\ \text{ou} \\ x=-3 \end{cases}$$

5. $x^3+x^2-2x-2=0$

   Neste caso podemos usar uma fatoração por agrupamento!

   $x^3+x^2-2x-2=x^2(x+1)-2(x+1)=(x^2-2)(x+1)$. Assim

$$x^3+x^2-2x-2=0 \Leftrightarrow (x^2-2)(x+1)=0 \Leftrightarrow \begin{cases} x^2-2=0 \\ \text{ou} \\ x+1=0 \end{cases} \Leftrightarrow \begin{cases} x=\pm\sqrt{2} \\ \text{ou} \\ x=-1 \end{cases}$$

3.4 Raízes racionais, raízes conjugadas e relações de Girard

Nesta seção, veremos como os seguintes resultados podem ajudar a resolver equações de grau maior que 2.

- Um polinômio $p(x)$ é divisível por $x-a$ se, e somente se, $p(a)=0$.

- Dada uma equação polinomial na forma $a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0=0$ com coeficientes inteiros, as possíveis raízes racionais são da forma $\frac{p}{q}$ sendo p um divisor de a_0 e q um divisor de a_n.

- Dada uma equação polinomial na forma $a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0=0$, onde $a_n,a_{n-1},\ldots,a_0\in\mathbb{R}$ se um número complexo $z=a+bi$ for raiz então $\overline{z}=a-bi$ também é raiz.

- Dada uma equação polinomial na forma $a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0=0$

de raízes $x_1, x_2, \ldots x_n$ as *relações de Girard* para estão equação são dadas por:

$$\begin{cases} x_1 + x_2 + \cdots + x_n = -\frac{a_{n-1}}{a_n} \\ x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n = \frac{a_{n-2}}{a_n} \\ x_1x_2x_3 + x_1x_2x_4 + \cdots + x_{n-2}x_{n-1}x_n = -\frac{a_{n-3}}{a_n} \\ \\ \ldots \\ x_1x_2x_3 \ldots x_n = (-1)^n \frac{a_0}{a_n} \end{cases}$$

Algumas equações polinomiais podem ser resolvidas aplicando os resultados acima, como mostram os seguintes exemplos: (Vamos supor nas equações abaixo que $U = \mathbb{C}$).

Exemplos. 1. $3x^3 + 8x^2 - 33x + 10 = 0$

Note que as possíveis raízes racionais são da forma $\frac{p}{q}$ sendo $p \in \{\pm 10, \pm 5, \pm 2, \pm 1\}$ e $q \in \{\pm 1, \pm 3\}$. Testando os possíveis valores temos que 2 é raiz, pois $3 \cdot 2^3 + 8 \cdot 2^2 - 33 \cdot 2 + 10 = 0$.

Por Briot-Ruffini, vem que $3x^3 + 8x^2 - 33x + 10 = (x-2)(3x^2 + 14x - 5)$, logo $3x^3 + 8x^2 - 33x + 10 = 0 \Leftrightarrow (x-2)(3x^2 + 14x - 5) = 0$

$$\Leftrightarrow \begin{cases} x - 2 = 0 \\ \quad \text{ou} \\ 3x^2 + 14x - 5 = 0 \end{cases} \Leftrightarrow \begin{cases} x = 2 \\ \quad \text{ou} \\ x = -5 \text{ ou } x = \frac{1}{3} \end{cases}$$

2. $-x^4 + 2x^3 + 6x^2 + 2x - 1 = 0$

Note que as possíveis raízes racionais são da forma $\frac{p}{q}$ sendo $p \in \{\pm 1\}$ e $q \in \{\pm 1\}$. Testando os possíveis valores temos que -1 é raiz.

Por Briot-Ruffini, vem que $-x^4 + 2x^3 + 6x^2 + 2x - 1 = (x+1)(-x^3 + 3x^2 + 3x - 1)$. Porém pelo mesmo processo -1 é raiz de $-x^3 + 3x^2 + 3x - 1$, logo $-x^4 + 2x^3 + 6x^2 + 2x - 1 = (x+1)^2(-x^2 + 4x^2 - 1)$. Assim, temos que:

$-x^4 + 2x^3 + 6x^2 + 2x - 1 = 0 \Leftrightarrow (x+1)^2(-x^2 + 4x^2 - 1) = 0 \Leftrightarrow$

$$\begin{cases} x + 1 = 0 \\ \quad \text{ou} \\ -x^2 + 4x - 1 = 0 \end{cases} \Leftrightarrow \begin{cases} x = -1 \\ \quad \text{ou} \\ x = 2 + \sqrt{3} \text{ ou } x = 2 - \sqrt{3} \end{cases}$$

3. $x^4 - 2x^3 + 4x - 4 = 0$, sabendo que $1 + i$ é raiz.

   Como os coeficientes são reais se $1 + i$ é raiz então $1 - i$ também é raiz. Sendo $a, b, 1 + i$ e $1 - i$ as raízes, pelas relações de Girard temos:

   $$\begin{cases} a + b + 1 + i + 1 - i = -(\frac{-2}{1}) \\ ab(1 + i)(1 - i) = \frac{-4}{1} \end{cases} \Leftrightarrow \begin{cases} a + b = 0 \\ ab = -2 \end{cases} \Leftrightarrow a = \sqrt{2} \text{ e } b = -\sqrt{2}$$

4. $x^3 - 4x^2 + 8 = 0$, sendo que uma das raízes é igual a soma das outras duas

   Sendo a, b e c as raízes temos que $a = b + c$. Pelas relações de Girard $a + b + c = -(\frac{-4}{1}) \Leftrightarrow 2a = 4 \Leftrightarrow a = 2$.

   Por Briot-Ruffini, vem que $x^3 - 4x^2 + 8 = (x - 2)(x^2 - 2x - 4)$, logo
   $x^3 - 4x^2 + 8 = 0 \Leftrightarrow (x - 2)(x^2 - 2x - 4) = 0 \Leftrightarrow$
   $$\begin{cases} x - 2 = 0 \\ \quad \text{ou} \\ x^2 - 2x - 4 = 0 \end{cases} \Leftrightarrow \begin{cases} x = 2 \\ \quad \text{ou} \\ x = 1 \pm \sqrt{5} \end{cases}$$

5. $-x^3 + 7x^2 - 14x + 8 = 0$, sabendo que as raízes estão em progressão geométrica

   Sendo a, b e c as raízes temos que $b^2 = ac$. Pelas relações de Girard temos que $abc = -(\frac{8}{-1}) \Leftrightarrow b^3 = 8 \Leftrightarrow b = 2$.

   Por Briot-Ruffini, vem que $-x^3 + 7x^2 - 14x + 8 = (x - 2)(-x^2 + 5x - 4)$, logo
   $-x^3 + 7x^2 - 14x + 8 = 0 \Leftrightarrow (x - 2)(-x^2 + 5x - 4) = 0$
   $$\Leftrightarrow \begin{cases} x - 2 = 0 \\ \quad \text{ou} \\ -x^2 + 5x - 4 = 0 \end{cases} \Leftrightarrow \begin{cases} x = 2 \\ \quad \text{ou} \\ x = 1 \text{ ou } x = 4 \end{cases}$$

Exemplo. Resolva em $U = \mathbb{C}$ a equação $x^3 - 2x + 3 = 0$.

Note que neste caso as possíveis raízes racionais são ± 1 e ± 3 e por inspeção temos que nenhum destes números é raiz. Portanto, dentre os métodos conhecidos no EM ficamos um pouco limitado para resolver tal equação, já que as técnicas apresentadas não funcionam.

Neste ponto cabe ao professor parar um pouco e mencionar que existe uma fórmula para resolver a equação de terceiro grau. Neste momento muitos alunos ficariam ansiosos pela fórmula mágica que resolve tudo. E quando o professor mostrar a fórmula digamos que a maior parte já desistiria de tentar memorizar.

Abriria aqui uma pequena discussão ao professor para falar um pouco do contexto histórico das equações e dizer que as equações de quarto grau também tem uma fórmula específica, porém um pouco maior e que a partir daí não existe mais fórmulas.

O que deve ser feito no momento é mostrar ao aluno outras maneiras de resolver tais equações que não são solúveis por fórmulas.

3.5 Gráficos

Nesta secção, vamos nos prender a problemas nos quais o aluno tem o gráfico de uma função polinomial real f e a partir daí quer determinar o número de soluções reais da equação $f(x) = g(x)$ num intervalo dado, sendo $g(x)$ uma função polinomial real tal que $g(x) = 0$ ou $\partial g(x) \leq 2$.

A ideia é que o aluno perceba que o número de soluções reais da equação $f(x) = g(x)$ é exatamente igual ao número de intersecções dos gráficos de f e g. Em particular, o número de raízes reais da equação $f(x) = 0$ é a quantidade de vezes que o gráfico de f corta o eixo das abscissas.

Como exemplo, vamos supor que tenhamos o gráfico da função polinomial

$$f(x) = x^5 + x^4 - x^3 + x^2 - 2x - 2.$$

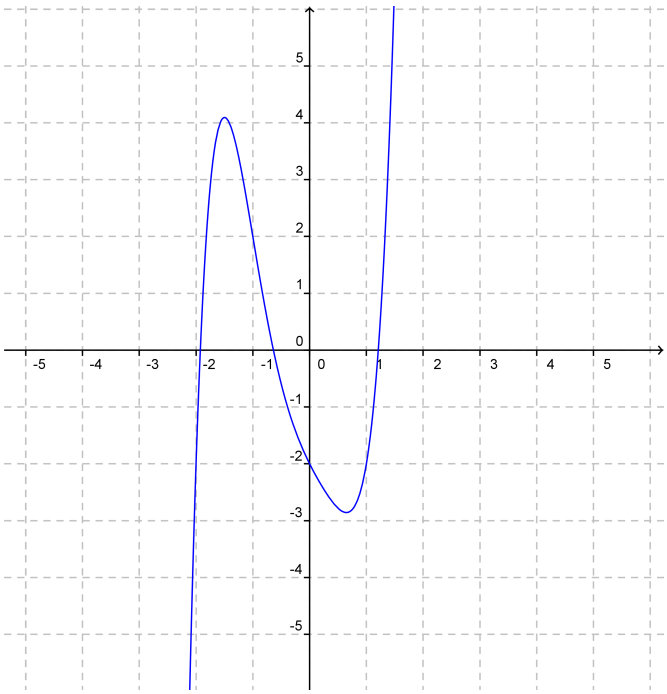
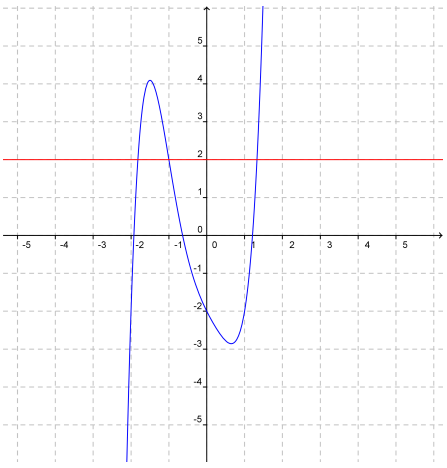


Figura 3.1: Gráfico de $f(x) = x^5 + x^4 - x^3 + x^2 - 2x - 2$

A função f possui apenas 3 raízes reais no intervalo $[-5, 5]$ visto que ela tem 3 intersecções com o eixo das abscissas.

Suponha agora que vamos determinar a quantidade de soluções de $f(x) = 2$ no intervalo $[-5, 5]$.

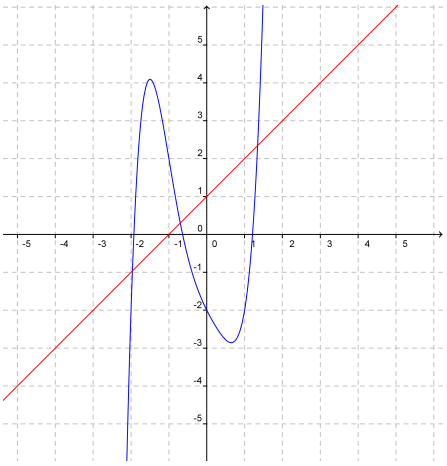
Neste caso basta contar as intersecções do gráfico de $f(x)$ com a reta $y = 2$.



Note que temos 3 intersecções e portanto temos 3 soluções no intervalo em questão. O problema anterior poderia ter sido reescrito como "Determinar o número

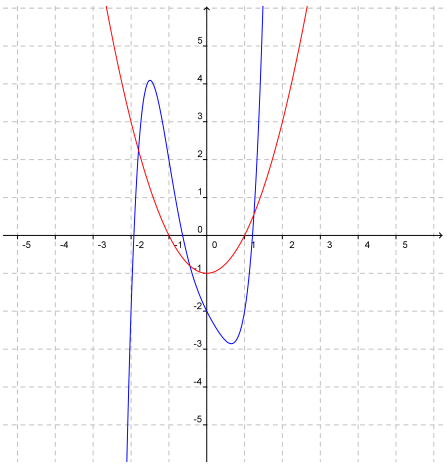
de raízes reais da equação $x^5 + x^4 - x^3 + x^2 - 2x - 4 = 0$".

Analogamente vamos determinar o número de raízes reais de $f(x) = x + 1$ em $[-5, 5]$.



Neste caso temos 3 intersecções também e portanto teríamos apenas 3 raízes reais no intervalo dado. Novamente este problema poderia ser reescrito como "Determine o número de raízes reais de $x^5 + x^4 - x^3 + x^2 - 2x - 2 = x + 1$
$\Leftrightarrow x^5 + x^4 - x^3 + x^2 - 3x - 3 = 0$".

E por fim gráficos de funções quadráticas também são de conhecimento comum aos alunos do Ensino Médio e portanto podemos ainda descobrir a quantidade de raízes da equação $f(x) = x^2 - 1$ no intervalo $[-5, 5]$.



E novamente temos 3 intersecções e portanto temos 3 raízes no intervalo dado. Note ainda que o problema anterior é dado por "Determine o número de raízes

reais de $x^5 + x^4 - x^3 + x^2 - 2x - 2 = x^2 - 1 \Leftrightarrow x^5 + x^4 - x^3 - 2x - 1 = 0$.

Caso uma aproximação para a raiz seja pedida, podemos usar alguns dos métodos numéricos apresentados na próxima seção.

3.6 Métodos numéricos

Nesta secção, estudaremos dois métodos que fornecem uma sequência de valores que aproximam, com o grau de precisão desejado, a raiz que se deseja obter.

3.6.1 Método da bissecção

Em primeiro lugar, recordamos que se f é uma função polinomial real e a e b são números reais tais que $f(a) \cdot f(b) < 0$, então f possui uma raiz no intervalo $[a, b]$.

O método da bissecção é um método iterativo no qual começamos com dois pontos x_0 e x_1 tais que $f(x_0) \cdot f(x_1) < 0$. Sabemos, da observação acima, que existe uma raiz no intervalo $]x_0, x_1[$.

Consideramos agora o ponto $x_2 = \frac{x_0+x_1}{2}$. Temos três possibilidades:

- $f(x_2) = 0$, logo x_2 é raiz
- $f(x_2) \cdot f(x_0) < 0$, neste caso temos uma raiz no intervalo $]x_0, x_2[$
- $f(x_2) \cdot f(x_0) > 0$, neste caso temos uma raiz no intervalo $]x_2, x_1[$

Ao determinar o novo intervalo podemos repetir esse processo indefinidamente, sempre gerando novos intervalos contendo as raízes até obtermos a aproximação desejada.

Exemplo. Determine uma raiz real da equação $x^3 - 5 = 0$.

Solução. Seja $f(x) = x^3 - 5$, note que $f(1) = -4$ e $f(2) = 3$, logo há uma raiz real no intervalo $]1, 2[$.

n	x_n	sinal de $f(x_n)$
0	1	< 0
1	2	> 0
2	$1,5$	< 0
3	$1,75$	> 0
4	$1,625$	< 0

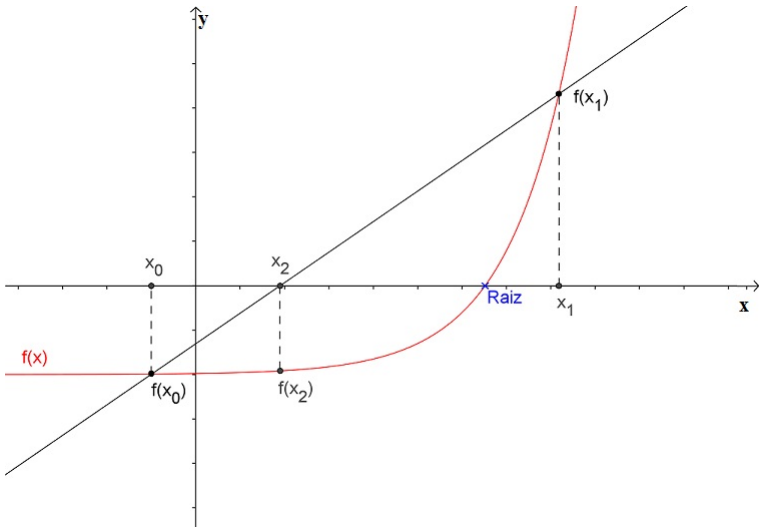
Podemos repetir esse processo até obtermos a aproximação desejada, usando a expressão do **erro relativo** dada por:

$$\frac{|x_{k+1} - x_k|}{|x_{k+1}|} < \varepsilon$$

3.6.2 Método das secantes

Outro método para obtermos a raiz de um polinômio $f(x)$ é o chamado *método das secantes*. A vantagem desse método em relação ao anterior é que ele converge mais rápido para a raiz. Tal método pode ser facilmente explicado aos alunos de EM com conhecimentos básicos de equações de retas estudados em Geometria Analítica.

Supondo duas aproximações iniciais x_0 e x_1 tais que $f(x_0) \neq f(x_1)$ neste método não é necessário que a raiz procurada esteja no intervalo $]x_0, x_1[$. Consideramos a reta que passa por $(x_0, f(x_0))$ e $(x_1, f(x_1))$, cuja equação pode ser dada por $y = f(x_0) + \frac{f(x_1)-f(x_0)}{x_1-x_0}(x - x_0)$. A abscissa x_2 de seu ponto de intersecção com o eixo x nos dá nossa primeira aproximação. A partir daí consideramos a reta que passa por $(x_1, f(x_1))$ e $(x_2, f(x_2))$, sendo tomado o cuidado de que a condição $f(x_2) \neq f(x_1)$ deve ser satisfeita.



O algoritmo geral para tal método é descrito por

$$x_{n+1} = x_n - \frac{(x_n - x_{n-1}) \cdot f(x_n)}{f(x_n) - f(x_{n-1})},$$

para $n = 1, 2, 3, \ldots$

O **erro relativo** pode ser calculado pela mesma epxressão vista na seção anterior.

Vamos dar um exemplo considerando $f(x) = x^3 - 5$ e $x_0 = 1$ e $x_1 = 2$. Aplicando o método obtemos a tabela de valores abaixo:

n	x_n
0	1
1	2
2	1,57
3	1,68
4	1,71

Uma variação deste método é conhecida como *método das tangentes* ou *método de Newton*, porém tal processo depende do conhecimento de derivadas que não faz parte do currículo de EM. Para maiores informações sobre este método o leitor pode consultar qualquer livro básico de Cálculo Numérico.

3.7 Comentários gerais sobre os métodos

Dos métodos aqui descritos vimos que muitas equações podem ser redutíveis a equações de segundo grau. Neste caso a maior dificuldade que um aluno do EM pode encontrar seria fazer a substituição adequada. Seria interessante que o professor em sala de aula ressaltasse a importância da resolução por soma e produto em alguns casos para agilizar cálculos.

Com relação ao método de fatoração, ele é extremamente útil e talvez um dos mais úteis, porém ele requer certa prática com as técnicas de fatoração. Nem sempre uma "fatoração por agrupamento" é facilmente identificada, bem como somar e subtrair termos para alguns alunos pode acabar virando uma "matemágica".

O método talvez mais prático para os alunos seriam as relações de Girard com o auxílio do dispositivo de Briot-Ruffini. Esse processo, no final das contas, é algo mais mecânico pois basta seguir um determinado algoritmo para resolver uma equação polinomial.

Com relação aos gráficos, muitos alunos do EM não têm o domínio de limites e derivadas para sua construção, porém uma boa análise ajuda em muito na resolução de alguns exercícios. É uma saída que se aplica em alguns poucos casos, mas nem por isso deve ser deixada de lado.

E, por fim, os métodos da bissecção e da secante são poderosos, porém exaustivos e impraticáveis sem o uso de uma calculadora. Como em muitas provas e nos grandes concursos não é permitido seu uso, esses métodos serviriam mais como um aprofundamento para os alunos do EM.

Porém o mais importante é mostrar que mesmo não tendo fórmulas prontas para determinar as raízes de equações polinomiais de grau maior que 5, temos muitas outras saídas para resolver este problema. Basta o aluno saber quando e como aplicar tais métodos.

4 APROFUNDAMENTO PARA O PROFESSOR

Como o próprio nome sugere, este capítulo tem por finalidade aprofundar os conhecimentos do professor no que se refere às equações cúbicas. Nosso principal objetivo é mostrar como alguns fatos do cálculo podem ser usados para explicar a natureza das raízes da equação $x^3+px+q=0$ a partir do sinal de seu discriminante.

O método de resolução da cúbica $x^3+px+q=0$ apresentado no capítulo 2 fornece a seguinte fórmula:

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

O radicando

$$D=\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3$$

recebe o nome de *discriminante* da equação $x^3+px+q=0$.

Exemplos.

1. $x^3-3x-2=0$.

   Neste caso, $D=0$. Testando as possíveis raízes racionais, chegamos à conclusão de que 2 é raiz e -1 é raiz dupla.

   Aplicando a fórmula, obtemos $x=2$.

2. $x^3+3x-14=0$.

   Neste caso, $D=50>0$. Testando as possíveis raízes racionais, chegamos à conclusão de que 2 é raiz. As outras duas são raízes de $x^2+2x+7=0$ porque $x^3+3x-14=(x-2)(x^2+2x+7)$ e, portanto, são complexas conjugadas.

   Aplicando a fórmula, obtemos $x=\sqrt[3]{7+5\sqrt{2}}+\sqrt[3]{7-5\sqrt{2}}$. Logo,

   $$\sqrt[3]{7+5\sqrt{2}}+\sqrt[3]{7-5\sqrt{2}}=2.$$

3. $x^3 - 6x - 4 = 0$.

Neste caso, $D = -4 < 0$. Testando as possíveis raízes racionais, chegamos à conclusão de que -2 é raiz. As outras duas são raízes de $x^2 - 2x - 2 = 0$ e, portanto, são $1 + \sqrt{3}$ e $1 - \sqrt{3}$.

Aplicando a fórmula obtemos $x = \sqrt[3]{2 + 2i} + \sqrt[3]{2 - 2i}$. Note que, quando z é um número complexo, o símbolo $\sqrt[3]{z}$ representa qualquer número complexo cujo cubo seja igual a z. Com exceção de $z = 0$, há sempre três números complexos que elevados ao cubo resultam em z. Na expressão

$$x = \sqrt[3]{2 + 2i} + \sqrt[3]{2 - 2i}$$

cada radical tem três valores. Contudo, é importante lembrar que $x = u + v$ com $uv = -p/3 = 2$ e, portanto, $v = 2/u$. Assim, escolhido um valor para u, o de v fica determinado.

Note que

$$2 + 2i = \sqrt{8}(\cos 45^\circ + i \operatorname{sen} 45^\circ).$$

Portanto, os valores de $u = \sqrt[3]{2 + 2i}$ são

$$u_1 = \sqrt{2}(\cos 15^\circ + i \operatorname{sen} 15^\circ),$$

$$u_2 = \sqrt{2}(\cos 135^\circ + i \operatorname{sen} 135^\circ),$$

$$u_3 = \sqrt{2}(\cos 255^\circ + i \operatorname{sen} 255^\circ).$$

Os valores correspondentes de $v = \sqrt[3]{2 - 2i}$ são

$$v_1 = \frac{2}{u_1} = \frac{2}{|u_1|^2}\bar{u_1} = \sqrt{2}(\cos 15^\circ - i \operatorname{sen} 15^\circ),$$

$$v_2 = \sqrt{2}(\cos 135^\circ - i \operatorname{sen} 135^\circ),$$

$$v_3 = \sqrt{2}(\cos 255^\circ - i \operatorname{sen} 255^\circ).$$

Logo,

$$u_1 + v_1 = 2\sqrt{2}\cos 15^\circ = 2\sqrt{2}\left(\frac{\sqrt{2} + \sqrt{6}}{4}\right) = 1 + \sqrt{3},$$

$$u_2 + v_2 = -2,$$

$$u_3 + v_3 = 1 - \sqrt{3}.$$

Proposição. *Seja D o discriminante da equação $x^3 + px + q = 0$. Temos que:*

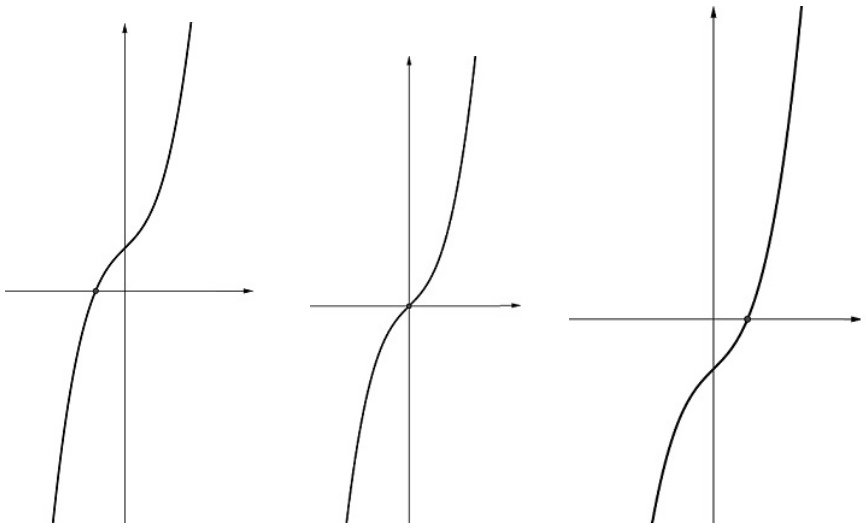
- *se $D > 0$, então a equação tem uma raiz real e duas complexas conjugadas;*
- *se $D = 0$, tem-se três raízes reais, sendo uma de multiplicidade maior que 1;*
- *se $D < 0$, então as três raízes são reais e distintas.*

Demonstração. Considere a função $f : \mathbb{R} \to \mathbb{R}$ dada por

$$\begin{aligned} f(x) &= x^3 + px + q \\ &= x^3 \left(1 + \frac{p}{x^2} + \frac{q}{x^3}\right). \end{aligned}$$

Sabemos que f tem pelo menos uma raiz real.

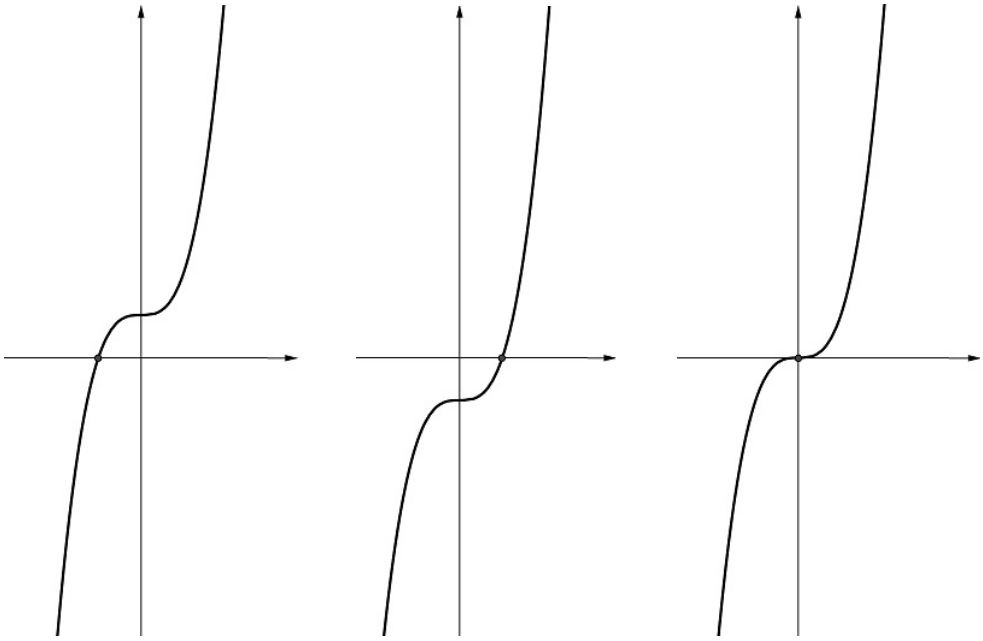
A derivada de f é dada por $f'(x) = 3x^2 + p$. Quando $p > 0$, a função é estritamente crescente e, assim, f corta o eixo das abscissas em único valor real. Neste caso temos uma raiz real e duas raízes complexas conjugadas. Note que $p > 0$ implica $D > 0$.



(a) 1 raiz real negativa (b) 1 raiz real nula (c) 1 raiz real positiva

Figura 4.1: Caso $p > 0$.

Quando $p = 0$, a equação se torna $x^3 + q = 0$. No caso $q \neq 0$, há uma raiz real e duas complexas conjugadas. No caso $q = 0$, há uma raiz real tripla — a saber, 0. Observe que se $p = 0$ e $q > 0$ então $D > 0$.



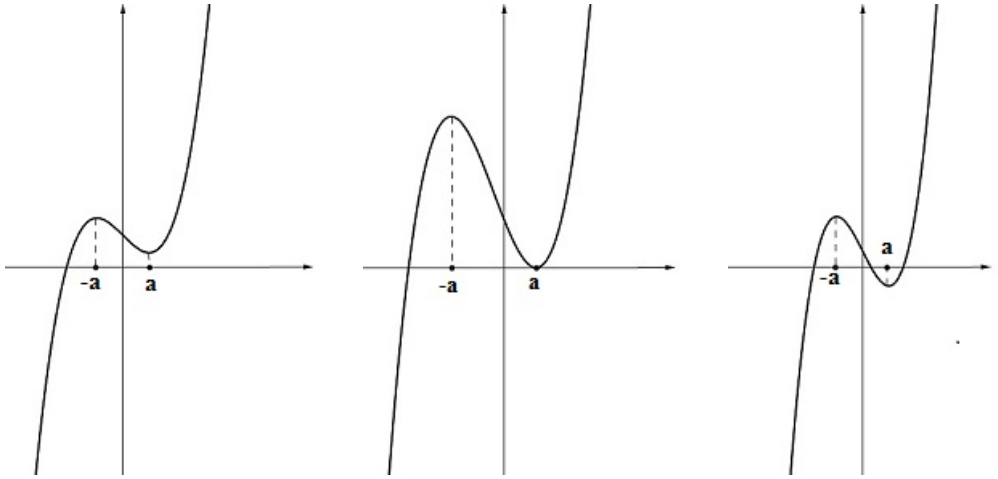
(a) Gráfico de $y = x^3 + q$, $q < 0$ (b) Gráfico de $y = x^3 + q$, $q > 0$ (c) Gráfico de $y = x^3$

Figura 4.2: Caso $p = 0$.

Considere, agora, $p < 0$. Podemos escrever $p = -3a^2$ para algum $a > 0$. Neste caso, $f(x) = x^3 - 3a^2x + q$ e, portanto, $f'(x) = 3x^2 - 3a^2$ e $f''(x) = 6x$. Como a primeira derivada se anula em $x = \pm a$, $f''(a) > 0$ e $f''(-a) < 0$ temos que $x = a$ será um ponto de mínimo local e $x = -a$ será um ponto de máximo local de f. Note que

$$f(a) \cdot f(-a) = (q - 2a^3)(q + 2a^3) = q^2 - 4a^6 = q^2 + \frac{4}{27}p^3 = 4\left(\frac{q^2}{4} + \frac{p^3}{27}\right) = 4D$$

e, portanto, o sinal de D é o mesmo de $f(a) \cdot f(-a)$. Logo, $D > 0$ implica $f(a) \cdot f(-a) > 0$ e, portanto, os sinais de $f(a)$ e $f(-a)$ são iguais o que garante que a função cresce e decresce num mesmo lado em relação ao eixo x, o que garante a existência de uma única raiz real. Se $D = 0$ então $f(a) \cdot f(-a) = 0$ e, portanto, a ou $-a$ é uma raiz dupla. Por fim, $D < 0$ implica $f(a) \cdot f(-a) < 0$ e, portanto, $f(a)$ e $f(-a)$ possuem sinais contrário o que garante a existência de três raízes reais distintas. Os gráficos abaixo ajudam a ilustrar melhor o que ocorre em tais situações.



(a) 1 raiz real e 2 complexas conjugadas

(b) 1 raiz real simples e uma dupla

(c) 3 raízes reais distintas

Figura 4.3: Caso $p < 0$.

□

Referências Bibliográficas

[1] E. Artin, *Galois Theory*, Dover Publications, Milwaukee, 1998.

[2] J. Bewersdorff, *Galois Theory for Beginners: A Historical Perspective*, AMS, Providence, 2006.

[3] H. M. Edwards, *Galois Theory*, Springer-Verlag, Harrisonburg, 1984.

[4] H. Eves, *Introdução à História da Matemática*, UNICAMP, Campinas, 2004.

[5] A. Gonçalves, *Introdução à Álgebra*, IMPA, Rio de Janeiro, 2011.

[6] A. F. P. C. Humes, *Noções de Cálculo Numérico*, McGraw-Hill, São Paulo, 1984

[7] G. Iezzi, *Conecte, Matemática: Ciências e Aplicações*, Saraiva, , 2011.

[8] E. L. Lima, *A Equação do Terceiro Grau*, Revista Matemática Universitária **5** (1987), 9-23.

[9] E. L. Lima, *A Matemática do Ensino Médio*, SBM, Rio de Janeiro, 2006.

[10] P. A. Martin, *Grupos, Corpos e Teoria de Galois*, Livraria da Física, São Paulo, 2010.

[11] C. P. Milies, *Breve História da Álgebra Abstrata*, IME USP, São Paulo.

[12] O. E. Nicodemi, M. A. Sutherland, G. W. Towsley, *An Introduction to Abstract Algebra with Notes to the Future Teacher*, Pearson Prentice Hall, Upper Saddle River, 2007.

[13] A. Rooney, *A História da Matemática*, M. Books, São Paulo, 2012.

[14] I. Stewart, *Galois Theory*, Chapman & Hall/CRC, Boca Raton, 2004.

[15] I. Stewart, *Uma história da Simetria na Matemática*, Zahar, Rio de Janeiro, 2012.

[16] J. Stillwell, *Galois Theory for Beginners*, Amer. Math. Monthly **101** (1994), 22-27.

[17] G. Tewani, *Mathematics for IIT-JEE 2012-13*, Cengage Learning, Delhi, 2012.