5

Polinômios e Equações Algébricas

5.1 Introdução

É bem sabido que o uso de uma notação adequada é fundamental para o bom desenvolvimento de uma área da matemática. Porém, a história nos ensina que nem sempre é fácil chegar a uma tal notação.

A necessidade de uma notação mais sofisticada se manifestou pela primeira vez em relação à resolução de equações algébricas. Como já observamos, tanto os egípcios quanto que os babilônios e os gregos trabalharam com equações de primeiro ou segundo grau mas, em todos os casos, não tinham notações nem fórmulas gerais.

É no século IV d.C., na *Arithmetica* de Diofanto, que encontramos pela primeira vez o uso de uma letra para representar a incógnita de uma equação, que o autor chamava *o número do problema.* Como os manuscritos originas de Diofanto não chegaram até nós, não sabemos com toda certeza quais os símbolos que ele usava, mas acredita-se que representava a incógnita pela letra ς, uma variante da letra σ quando aparece no fim de uma palavra (por exemplo, em $\acute{\alpha}\rho\iota\theta\mu\acute{o}\varsigma$ – *arithmos*). Esta escolha se deve provavelmente ao fato de que, no sistema grego de numeração, as letras representavam também números conforme sua posição no alfabeto, mas a letra ς não fazia parte do sistema e não correspondia, assim, a nenhum valor numérico particular.

Ele usava também nomes para designar as várias potências da incógnita, como quadrado, cubo, quadrado-quadrado (para a quarta potência), quadrado-cubo (para a quinta) e cubo-cubo (para a sexta). O uso de potências superiores a três é notável uma vez que, como os gregos se apoiavam em interpretações geométricas, tais potências não tinham um significado concreto.

A notação de expoentes é usada por Nicolas Chuquet na sua *Tripary*, onde escreve expressões como $12^3, 10^3$ e 120^3 para representar o que hoje escreveríamos como $12x^3, 10x^3$ e $120x^3$ e também 12^0 e 7^{1m} para $12x^0$ e $7x^{-1}$.

Os primeiros passos para a introdução do conceito de *polinômio* e seu uso para a formulação de problemas de resolução de equações foram dados por Simon Stevin (1548–1620). Nascido em Bruges*, mudou para Leyden em 1582, foi tutor de Maurício de Nassau e serviu o exército holandês. Ele foi um defensor do sistema de Copérnico e o primeiro a discutir e sugerir o emprego de frações decimais (em oposição ao sistema sexagesimal defendido por outros), na sua obra mais conhecida *De Thiende*, publicada em Flamengo em 1585 e traduzida ao francês, sob o título *La Disme*, no mesmo ano.

Alí ele usou símbolos como ⓪, ①, ②, etc. para indicar as posições das unidades, dízimas, centésimas, respectivamente. Assim por exemplo, ele escreve $875,782$ como $875\ \ ⓪7\ ①8\ ②2\ \ ③$.

No seu livro seguinte, *L'Arithmetique*, publicado em 1585, ele introduz uma notação exponencial semelhante para denotar as várias potências de uma variável. As potências que nós escreveríamos com $x,\ x^2\ x^3$ etc. são denotadas por ele como ⓪, ①, ②, e assim, por exemplo, o polinômio $2x^3+4x^2+2x+5$ se escreveria, na sua notação como:

$$2\ ③+\ 4\ ②+\ 2\ ①+\ 5\ ⓪$$

Ele denomina estas expressões de *multinômios* e mostra como operar com eles. Entre outras coisas, observa que as operações com multinômios tem muitas propriedades em comum com as operações entre "números aritméticos". Ainda, ele mostra que o algorítmo de Euclides pode ser usado para determinar o máximo divisor comum de dois "multinômios".

* A época Bruges, que hoje é uma cidade da Bélgica, pertencia à Holanda.

É interessante destacar aqui que nos encontramos frente a dois progressos notáveis na direção da abstração. De um lado temos a percepção, cada vez mais clara, de que os métodos de resolução de equações dependem unicamente do grau da equação e não dos valores dos coeficientes numéricos. Mais importante ainda, vemos que Stevin trata seus multinômios como novos objetos matemáticos e estuda as operações entre eles.

O próximo passo importante é devido ao trabalho de François Viète (1540–1603). Nascido em Fontenay-le Comte, teve formação de advogado e, nesta condição, serviu ao parlamento de Bretania em Rennes e foi banido de suas atividades, devido à oposição política, entre 1584 e 1589, quando foi chamado por Henri III para ser conselheiro do parlamento, em Tours. Nos anos em que esteve afastado da atividade política, dedicou-se ao estudo da matemática e, em particular, aos trabalhos de Diofanto, Cardano, Tartaglia, Bombelli e Stevin. Da leitura destes trabalhos ele teve a idéia de utilizar letras para representar quantidades.

Sua principal contribuição à Álgebra aparece no seu livro *In Artem Analyticam Isagoge* – Introdução à Arte Analítica – impresso em 1591, onde trata das equações algébricas de um novo ponto de vista. Ele fez importantes progressos na notação e seu verdadeiro mérito está em ter usado letras *não somente para representar "incógnitas", mas também para representar os coeficientes ou quantidades conhecidas.* Ele usava consoantes para representar quantidades conhecidas e reservava as vogais para representar as incógnitas.

Viète chamava sua álgebra simbólica de *logística speciosa* por oposição à *logística numerosa*, que trata dos números. É importante observar que Viète tinha plena consciência de que seu emprego de letras lhe permitia trabalhar com *classes de equações*, por oposição ao emprego de números, que permite apenas trabalhar com um exemplo de cada vez. Com isso ele tornou explícita a diferença entre Álgebra e Artimética: para ele, a Álgebra – *logística speciosa* – era um método para operar com espécies ou formas de coisas e a Aritmética – *logística numerosa* – lidava apenas com números.

O uso de letras para representar classes de números e assim tratar das equações de forma mais geral demorou a ser aceito. Um aperfeiçoamento desta notação foi devido a René Descartes que, na sua obra intitulada *La Géométrie* utiliza pela primeira vez a prática hoje usual de utilizar as primeiras

letras do alfabeto para representar quantidades conhecidas e as últimas, como x, y e z para as incógnitas.

É precisamente nesta obra que Descartes apresenta as ideias que deram origem à Geometria Analítica, junto com as contribuições de Pierre de Fermat. Esse texto não foi apresentado como um livro independente mas como um apêndice da obra pela que seria mais conhecido, o *Discours de la méthode pour bien conduire sa raison et chercher la vérité dans les sciénces*, publicada em 1637*.

5.2 Polinômios

Como vimos na seção anterior, foram os progressos na notação que levaram à formulação da noção de *polinômios* como um conjunto de símbolos entre os quais é possível definir operações. No que segue, vamos formalizar estas ideias.

Para isso vamos utilizar o símbolo $\mathbb{K}$ para representar o conjunto $\mathbb{Q}$ dos números racionais, o conjunto $\mathbb{R}$ dos números reais ou o conjunto $\mathbb{C}$ dos números complexos. O símbolo $\mathbb{K}$ poderá representar também o conjunto $\mathbb{Z}_p$ dos inteiros módulo um inteiro primo p. Como ficará claro para o leitor, o estudo de polinômios sobre um determinado conjunto de coeficientes depende apenas das propriedades das operações entre coeficientes e não da natureza dos mesmos.

Provavelmente o leitor está acostumado a pensar nos polinômios como funções e, nesse sentido, o símbolo x é considerado uma variável. No ponto de vista que vamos adotar aqui, um polinômio é apenas um símbolo, um objeto de estudo da matemática e, para enfatizar esse ponto de vista, vamos chamar a letra X de uma *indeterminada*.

Naturalmente o leitor sabe, de sua experiência anterior, que um polinômio na indeterminada X é um símbolo da forma

$$f = a_0 + a_1X + a_2X^2 + \cdots + \alpha_nX^n.$$

* Neste livro ele descreve o uso da *dúvida metódica* como forma de tornar a ideias claras e precisas a partir das quais poderia-se chegar a conclusões válidas. Por esta e muitas outras contribuições, ele veio a ser considerado o "pai da filosofia moderna".

Há, porém, um pequeno problema em defini-lo assim: diferentes polinômios podem ter diferentes "comprimentos", o que dificulta a definição rigorosa das operações. Para evitar isto vamos formular a definição de um modo levemente diferente.

Definição 5.2.1 Um *polinômio* f com coeficientes em $\mathbb{K}$, na indeterminada X é um símbolo da forma

$$f = \sum_{i=0}^{\infty} a_i X^i = a_0 + a_1 X + a_2 X^2 + \cdots + \alpha_n X^n + \cdots ,$$

onde $a_i \in \mathbb{K}$, $0 \leq i \leq \infty$, e apenas um número finito deles é diferente de 0; isto é, existe um índice n tal que $a_n \neq 0$ e $a_i = 0$ se $i > n$.

O inteiro positivo n chama-se o *grau* de f, que denotaremos por $\mathrm{gr}\,(f)$, e o coeficiente a_n, o *líder* de f ou, por vezes, o *coeficiente dominante* de f. Um polinômio cujo coeficiente dominante é igual a 1 diz-se um *polinômio mônico*

Incluiremos também o *polinômio nulo*, que é o símbolo em que todos os coeficientes são 0 e que, por convenção, consideraremos de grau $-\infty$.

O conjunto de todos os polinômios na indeterminada X, com coeficientes em $\mathbb{K}$ será representado pelo símbolo $\mathbb{K}\,[X]$.

É claro que, se f é um polinômio de grau n, por vezes o escreveremos na forma

$$f = a_0 + a_1 X + a_2 X^2 + \cdots + \alpha_n X^n,$$

omitindo os termos da forma $a_i X^i$, para $i > n$, uma vez que estes são todos iguais a zero. Quando for conveniente, também escreveremos f ordenando seus termos por potências decrescentes de X, isto é, na forma:

$$f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0.$$

Da própria definição, segue que dois polinômios $f = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n$ e $g = b_0 + b_1 X + b_2 X^2 + \cdots + \beta_m X^m$ são iguais se e somente se $n = m$ e, para cada índice i, $1 \leq i \leq n$ tem-se que $a_i = b_i$.

Note que um polinômio f é de grau 0, então ele é da forma $f = a_0$, com $a_0 \in \mathbb{K} \setminus \{0\}$. Os polinômios de grau 0 são chamados *constantes*

identificando cada elemento $a \in \mathbb{K}$ com o polinômio de $f = a$, grau 0, podemos considerar que $\mathbb{K} \subset \mathbb{K}[X]$. Por convenção, consideraremos que o polinômio nulo também é um polinômio constante.

5.2.1 Operações entre polinômios

A seguir, vamos definir operações no conjunto $\mathbb{K}[X]$ de todos os polinômios com coeficientes em $\mathbb{K}$. Faremos isso formalmente, mas o leitor deverá observar que se trata das definições de soma e produto que lhe são familiares.

Definição 5.2.2 Sejam $f = \sum_{i=0}^{\infty} a_i X^i$ e $g = \sum_{i=0}^{\infty} b_i X^i$ dois polinômios de $\mathbb{K}[X]$. Chama-se *soma* de f e g ao polinômio

$$f + g = \sum_{i=0}^{\infty} (a_i + b_i) X^i.$$

Chama-se *produto* de f e g ao polinômio

$$fg = \sum_{k=0}^{\infty} c_k X^k,$$

onde cada coeficiente c_k, $1 \leq k \leq \infty$ é dado pela fórmula:

$$c_k = a_0 b_k + a_1 b_{k-1} + a_2 b_{k-2} + \cdots + a_k b_0 = \sum_{i+j=k} a_i b_j.$$

Exemplo 5.2.1 Considere os polinômios $f = 1 - X + X^2$ e $g = 3 + X^2 - X^3$ de $\mathbb{Q}[X]$. Então:

$$f + g = 4 - X + 2X^2 - X^3.$$

Calcular o produto seguindo a definição formal dará um pouco mais de trabalho, mas o leitor verificará facilmente que se trata do produto que lhe

é familiar. Vamos calcular os coeficientes do produto, um a um, aplicando diretamente a definição. Temos:

$$\begin{aligned}
c_0 &= a_0b_0 = 1 \cdot 3 = 3,\\
c_1 &= a_0b_1 + a_1b_0 = 1 \cdot 0 + (-1) \cdot 3 = -3,\\
c_2 &= a_0b_2 + a_1b_1 + a_2b_0 = 1 \cdot 1 + (-1) \cdot 0 + 1 \cdot 3 = 4,\\
c_3 &= a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0\\
&\quad = 1 \cdot (-1) + (-1) \cdot 1 + 1 \cdot 0 + 0 \cdot 3 = -2,\\
c_4 &= a_0b_4 + a_1b_3 + a_2b_2 + a_3b_1 + a_4b_0\\
&\quad = 1 \cdot 0 + (-1) \cdot (-1) + 1 \cdot 1 + 0 \cdot 1 + 0 \cdot 3 = 2,\\
c_5 &= a_0b_5 + a_1b_4 + a_2b_3 + a_3b_2 + a_4b_1 + a_5b_0\\
&\quad = 1 \cdot 0 + (-1) \cdot 0 + 1 \cdot (-1) + 0 \cdot 1 + 0 \cdot 0 + 0 \cdot 3 = -1,\\
c_6 &= a_0b_6 + a_1b_5 + a_2b_4 + a_3b_3 + a_4b_2 + a_5b_1 + a_6b_0\\
&\quad = 1 \cdot 0 + (-1) \cdot 0 + 1 \cdot 0 + 0 \cdot (-1) + 0 \cdot 1 + 0 \cdot (-1) + 0 \cdot 3 = 0,
\end{aligned}$$

e é fácil ver que, para $k > 6$, todos os coeficientes são iguais a 0. Assim,

$$fg = -X^5 + 2X^4 - 2X^3 + 4X^2 - 3X + 3.$$

Naturalmente, ao trabalhar com exemplos concretos escreveremos os polinômios na forma usual (sem considerar os infinitos coeficientes iguais a zero) e faremos as operações de modo que é familiar ao leitor.

Tal como observara Stevin, as operações com polinômios têm as mesmas propriedades que os operações entre números inteiros.

(i) (Propriedade associativa da soma) *Para toda terna de polinômios* f, g, h *de* $\mathbb{K}[X]$ *tem-se que*

$$(f + g) + h = f + (g + h).$$

(ii) (Existência de neutro da soma) *O polinômio nulo, é o elemento* neutro *da soma. No que segue denotaremos o polinômio nulo simplesmente por* 0*, e o significado deste símbolo estará sempre claro, do contexto. Ele é tal que*

$$f + 0 = 0 + f = f, \text{ para todo } f \in \mathbb{K}[X].$$

(iii) (EXISTÊNCIA DE OPOSTO) *Para cada polinômio* $f \in \mathbb{K}[X]$ *existe um outro elemento, que denotaremos por* $-f$*, que chamaremos de seu* oposto*, tal que*

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

(iv) (PROPRIEDADE COMUTATIVA DA SOMA) *Para cada par de polinômios* f *e* g *de* $\mathbb{K}[X]$ *tem-se que*

$$f + g = g + f.$$

(v) (PROPRIEDADE ASSOCIATIVA DO PRODUTO) *Para toda terna de elementos* f*,* g *e* h *de* $\mathbb{K}[X]$ *tem-se que:*

$$(fg)\,h = f\,(gh)\,.$$

(vi) (EXISTÊNCIA DE NEUTRO DO PRODUTO) *O polinômio* $\sum_{i=0}^{\infty} a_i X^i$*, em que* $a_0 = 1$ *e* $a_i = 0$ *para todo índice* $i > 0$*, é o* neutro multiplicativo *de* $\mathbb{K}[X]$*. Também denotaremos este elemento simplesmente por* 1 *e, novamente o significado do símbolo estará sempre claro, do contexto. Ele é tal que*

$$f \cdot 1 = 1 \cdot f = f, \text{ para todo } f \in \mathbb{K}[X]\,.$$

(viii) (PROPRIEDADE COMUTATIVA DO PRODUTO) *Para cada par de polinômios* f *e* g *de* $\mathbb{K}[X]$ *tem-se que*

$$fg = gf.$$

(ix) (PROPRIEDADE DISTRIBUTIVA) *Para toda terna de polinômios* f*,* g *e* h *de* $\mathbb{K}[X]$ *tem-se que:*

$$f\,(g + h) = fg + fh,$$
$$(f + g)\,h = fh + gh.$$

A demonstração de todas estas propriedades é muito simples, embora algo longa e tediosa, e a deixamos a cargo do leitor. A título de exemplo, demonstraremos a validade da primeira equação de *(ix)*.

Sejam $f = \sum_{i=0}^{\infty} a_i X^i$, $g = \sum_{i=0}^{\infty} b_i X^i$ e $h = \sum_{i=0}^{\infty} c_i X^i$, então

$$\begin{aligned}
f(gh) &= \sum_{i=0}^{\infty} a_i X^i \left[\sum_{i=0}^{\infty} (b_i + c_i) X^i \right] \\
&= \sum_{k=0}^{\infty} \left[\sum_{i+j=k} a_i (b_j + c_j) \right] X^k \\
&= \sum_{k=0}^{\infty} \left[\sum_{i+j=k} (a_i b_j + a_i c_j) \right] X^k \\
&= \sum_{k=0}^{\infty} \left[\sum_{i+j=k} a_i b_j + \sum_{i+j=k} a_i c_j \right] X^k \\
&= \left[\sum_{k=0}^{\infty} \left(\sum_{i+j=k} a_i b_j \right) + \sum_{k=0}^{\infty} \left(\sum_{i+j=k} a_i c_j \right) \right] X^k \\
&= \sum_{k=0}^{\infty} \left(\sum_{i+j=k} a_i b_j \right) X^k + \sum_{k=0}^{\infty} \left(\sum_{i+j=k} a_i c_j \right) X^k \\
&= fg + fh.
\end{aligned}$$

5.2.2 Divisibilidade em $\mathbb{K}[X]$

Definição 5.2.3 Sejam f e g polinômios de $\mathbb{K}[X]$, com $g \neq 0$. Diz-se que g *divide* f (ou que g é um *divisor* de f ou, ainda que f é *múltiplo* de g) se existe um polinômio $h \in \mathbb{K}[X]$ tal que $f = gh$.

Para indicar que g divide f usaremos a notação $g \mid f$ e para negar esta afirmação escreveremos $g \nmid f$.

Seja f um polinômio de $\mathbb{K}[X]$. Note que se g é um polinômio constante não nulo; isto é, se $g \in \mathbb{K}$, $g \neq 0$ então sempre podemos escrever

$f = g\left(g^{-1}\right) f$. Logo, todo polinômio constante é um divisor de f. Da mesma forma, é fácil ver que todo polinômio da forma af, com $a \in \mathbb{K}$, $a \neq 0$ é um divisor de f. Elementos desta forma chamam-se *associados* de f.

Definição 5.2.4 Dado um polinômio f, os polinômios constantes e os associados de f dizem-se os *divisores impróprios* de f. Um divisor de f que não é impróprio, diz-se um *divisor próprio* de f.

Um fato muito importante é que, no conjunto $\mathbb{K}[X]$ pode se definir divisão com quociente e resto, tal como ocorre no conjunto dos números inteiros, como veremos a seguir.

Teorema 5.2.1 (Algoritmo da divisão em $\mathbb{K}[X]$) *Dados dois polinômios $f, g \in \mathbb{K}[X]$, com $g \neq 0$, existem polinômios $q, r \in \mathbb{K}[X]$ tais que*

$$f = gq + r \quad \textit{com} \quad r = 0 \textit{ ou } \operatorname{gr}(r) < \operatorname{gr}(g).$$

Os polinômios q e r nestas condições são únicos.

Demonstração: Vamos provar inicialmente a existência de polinômios q e r nas condições do enunciado.

Claramente, se $\operatorname{gr}(f) < \operatorname{gr}(g)$, podemos tomar $q = 0$, $r = f$ e estes polinômios verificam as condições requeridas.

Podemos supor então que $\operatorname{gr}(f) \geq \operatorname{gr}(g)$.

Vamos fazer a demonstração por indução no grau de f, que denotaremos por n.

Se $n = 0$ então $\operatorname{gr}(g)$ também é igual a 0; logo g é uma constante e, portanto, tem inverso g^{-1}. É fácil ver que $q = fg^{-1}$ e $r = 0$ estão nas condições requeridas.

Vamos supor então que $\operatorname{gr}(f) = n$ e que o teorema vale para todo polinômio de grau menor que n.

Sejam $f = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$ e $g = b_m X^m + b_{m-1}X^{m-1} + \cdots + b_1 X + b_0$, onde, por hipótese, $m \leq n$.

Consideramos então o polinômio:

$$\begin{aligned} f_1 &= f - \frac{a_n}{b_m} X^{n-m} g \\ &= \left(a_{n-i} - \frac{a_n}{b_m} b_{m-1}\right) X^{n-m-1} + \cdots + \left(a_1 - \frac{a_n}{b_m} b_1\right) X + \left(a_0 - \frac{a_n}{b_m} b_0\right). \end{aligned}$$

Pode acontecer que $f_1 = 0$. Neste caso,

$$q = \frac{a_n}{b_m} X^{n-m} g \quad \text{e} \quad r = 0$$

são polinômios nas condições do enunciado.

Se $f_1 \neq 0$ então $\text{gr}\,(f_1) < \text{gr}\,(f)$ e, pela hipótese de indução, o enunciado vale para f_1. Então, existem q_1 e r_1 tais que

$$f_1 = q_1 g + r_1 \quad \text{com} \quad r_1 = 0 \text{ ou } \text{gr}\,(r_1) < \text{gr}\,(g)\,.$$

Temos então que

$$f = f_1 + \frac{a_n}{b_m} X^{n-m} g = \left(q_1 + \frac{a_n}{b_m} X^{n-m} \right) g + r_1$$

e, neste caso, os polinômios $q = q_1 + \frac{a_n}{b_m} X^{n-m}$ e $r = r_1$ estão nas condições do enunciado.

Vamos demonstrar agora a unicidade destes polinômios. Com efeito, suponha que existem q, r e também q_1, r_1 tais que

$$f = qg + r = q_1 g + r_1,$$

onde $r = 0$ ou $\text{gr}\,(r) < \text{gr}\,(g)$ e também $r_1 = 0$ ou $\text{gr}\,(r_1) < \text{gr}\,(g)$.

Temos então que $(q - q_1)\, q = r_1 - r$.

Se $r_1 - r = 0$ segue que $r_1 = r$ e $(q - q_1)g = 0$. Como $g \neq 0$, isto implica que $q - q_1 = 0$, onde $q = q_1$, como queríamos demonstrar.

Por outro lado, se $r_1 - r \neq 0$, então

$$\text{gr}\,(r_1 - r) \leq \min\{\text{gr}\,(r_1)\,, \text{gr}\,(r)\} < \text{gr}\,(g)\,.$$

Ainda, no primeiro membro da equação acima temos que

$$\text{gr}\,((q - q_1)\, q) > \text{gr}\,(g)\,,$$

uma contradição. □

Definição 5.2.5 Os polinômios q e r do teorema acima chamam-se respectivamente o *quociente* e o *resto* da divisão de f por g.

Exercícios

1. Calcular $f+g$ e fg nos seguintes casos de polinômios em $\mathbb{Q}[X]$:

   (a) $f = 1 + X + X^2, \quad g = 3 - 2X - X^2 + 2X^3$.

   (b) $f = 5 - X - X^2, \quad g = 1 - 2X + 2X^2 - 3X^3$.

   (c) $f = 1 - X, \quad g = 1 + X + X^2 + \cdots + X^n$.

2. Calcular $f+g$ e fg nos seguintes casos:

   (a) $f = 1 + X + X^2, \quad g = 3 - 2X - X^2 + 2X^3$ em $\mathbb{Z}_5[X]$.

   (b) $f = 3 + 2X + 2X^2, \quad g = 3 - 2X - 3X^2 + 3X^3$ em $\mathbb{Z}_7[X]$.

3. Sejam f e g polinômios de $\mathbb{K}[X]$. Provar que:

   (a) $\operatorname{gr}(f) + \operatorname{gr}(g) \leq \max\{\operatorname{gr}(f), \operatorname{gr}(g)\}$.

   (b) $\operatorname{gr}(fg) = \operatorname{gr}(f) + \operatorname{gr}(g)$.

   (c) Se $fg = 0$ então $f = 0$ ou $g = 0$.

4. Mostre através de exemplos que, se tomarmos polinômios com coeficientes em $\mathbb{Z}_m$, onde m é um inteiro não primo, então as propriedades (b) e (c) do exercício anterior não são necessariamente válidas.

5. (a) Determinar o número de polinômios de $\mathbb{Z}_5[X]$ cujo grau é menor o igual a 4.

   (b) Determinar o número de polinômios de $\mathbb{Z}_5[X]$ cujo grau é precisamente igual a 4.

6. Um polinômio $f \in \mathbb{K}[X]$ diz-se *inversível* se existe $g \in \mathbb{K}[X]$ tal que $fg = 1$. Determinar o conjunto de todos os elementos inversíveis de $\mathbb{K}[X]$.

7. Achar um polinômio não constante de $\mathbb{Z}_4[X]$ que é inversível.

8. Sejam f e g polinômios não nulos de $\mathbb{K}[X]$. Provar que

   (a) Se $g \mid f$ então $\operatorname{gr}(g) \leq \operatorname{gr}(f)$.

(b) Se $g \mid f$ e $f \mid g$ então g é um associado de f.

9. Sejam $f, g, h \in \mathbb{K}[X]$ (e sempre que afirmamos que um deles é um divisor, estaremos assumindo que é diferente de 0). Provar que:

   (a) $f \mid f$.

   (b) Se $f \mid g$ e $g \mid h$ então $f \mid h$.

   (c) Se $f \mid g$ e $f \mid h$ então $f \mid (g \pm h)$.

   (d) $f \mid g$ se e somente se $(fh) \mid (gh)$.

10. Determinar o quociente e o resto de dividir $f = 5X^4 + 3X^3 + 1$ por $g = 3X^2 + 2X + 1$ em $\mathbb{Z}_7[X]$.

11. Dados os polinômios $f = 3m^2X^4 - 11mX^3 - \left(m^2 - 10\right)X^2 + \left(6m^2 + 5m\right)X$ e $g = 3mX^3 - 5X^2 - mX + 6m + 3$, de $\mathbb{R}[X]$, determinar m para que f seja divisível por g.

12. Seja n um inteiro positivo, Achar o resto de dividir $(X-2)^{10n} + (X-1)^n + 2$ por $(X-1)(X-2)$ em $\mathbb{Q}[X]$.

13. Sejam $f, g \in \mathbb{K}[X]$ e seja r o resto da divisão de f por g. Provar que todo divisor comum a f e g é também um divisor comum a g e r.

14. Sejam $f, g \in \mathbb{K}[X]$. Um polinômio $d \in \mathbb{K}[X]$ diz-se um *máximo divisor comum* se:

    (i) $d \mid f$ e $d \mid g$.

    (ii) Se $d' \mid f$ e $d' \mid g$ então $d' \mid d$.

    Prove que:

    (a) Mostre que se d_1 e d_2 são ambos um máximo divisor comum de f e g então d_1 é associado a d_2.

    (b) Prove que existe um único máximo divisor comum de f e g que é mônico. Este polinômio será denotado por $\mathrm{mdc}(f, g)$.

15. Mostre que o máximo divisor comum de dois polinômios pode ser calculado da forma análoga ao máximo divisor comum de dois números inteiros, utilizando o Algoritmo de Euclides

16. Sejam $f, g \in \mathbb{K}[X]$ e seja $d = \text{mdc}(f, g)$. Provar que existem $r, s \in \mathbb{K}[X]$ tais que $d = rf + sg$. (*Sugestão:* Usar o exercício anterior).

17. Achar o máximo comum divisor dos polinômios f e g nos seguintes casos:

    (a) $f = X^4 + X^3 + 2X^2 - X - 3, \quad g = X^3 + X^2 - 4X + 2.$

    (b) $f = X^4 + 2X^3 - 3^2 + 5, \quad g = X^2 - 3X + 2.$

18. Seja $\mathcal{I}$ um subconjunto não vazio de $\mathbb{K}[X]$ que tem as seguintes propriedades:

    (i) Se $g, h \in \mathcal{I}$ então $g \pm h \in \mathcal{I}$.

    (ii) Se $g \in \mathcal{I}$ e f é qualquer polinômio de $\mathbb{K}[X]$ então $gh \in \mathcal{I}$.

    Provar que existe um polinômio $f_0 \in \mathbb{K}[X]$ tal que $\mathcal{I}$ é o conjunto de todos os múltiplos de f_0.

19. Sejam $f, g \in \mathbb{K}[X]$. Provar que o conjunto

$$\mathcal{I} = \{\alpha f + \beta g \mid \alpha, \beta \in K[X]\}$$

    tem as propriedades (i) e (ii) do exercício anterior.

    Utilizar este fato para provar que existem $r, s \in \mathbb{K}[X]$ tais que

$$\text{mdc}(f, g) = rf + sg.$$

20. Sejam $f, g \in \mathbb{K}[X]$, onde f é um polinômio irredutível. Provar que $f \mid g$ ou $\text{mdc}(f, g) = 1$.

21. Seja f um polinômio irredutível de $\mathbb{K}[X]$. Provar que, se f divide um produto gh, então $f \mid g$ ou $f \mid h$ (*Sugestão:* utilizar a propriedade demonstrada no Exercício 19).

22. Um polinômio $f \in \mathbb{K}[X]$ que não é um polinômio constante, diz-se *irredutível* se não tem divisores próprio. Em caso contrário, ele diz-se *redutível*.

    (a) Provar que um polinômio f não constante é irredutível se e somente se toda vez que f se escreve como um produto $f = gh$ tem-se que $\mathrm{gr}(g) = 0$ ou $\mathrm{gr}(h) = 0$.

    (b) Provar que todo polinômio f não constante tem pelo menos um divisor irredutível.

    (c) Provar que todo polinômio f não constante pode se escrever como um produto da forma:
    $$f = af_1 \cdots f_t,$$
    onde $a \in \mathbb{K}$ e cada f_i, $1 \leq i \leq t$ é um polinômio irredutível.

    (d) Utilizar o exercício anterior para provar que a expressão obtida acima para f é única.

23. Provar que o conjunto de polinômios irredutíveis de $\mathbb{K}[X]$ é infinito.

5.3 Raízes de Polinômios

Cardano observara, no *Ars Magna*, que uma equação de quarto grau pode ter, no máximo, quatro raízes. Depois, Peter Rothe num texto intitulado *Arithmetica Philosophica*, publicado em 1608, escreveu que um polinômio de grau n *pode* ter n raízes. A estrutura das equações algébricas foi devidamente explorada por **Alber Girard** num livro intitulado *Invention Nouvelle en l'Algebre* de 1629, onde escreve

> *Todas as equações em álgebra recebem tantas soluções quanto o expoente da maior quantidade* [...]

Mais adiante, Descartes faz uma afirmação semelhante, devidamente fundamentada, que é consequência do seu Teorema do Resto:

> *Cada equação pode ter tantas raízes diferentes quanto o número de dimensões da quantidade desconhecida na equação.*

Nesta seção vamos precisar conceitos e demonstrar estas afirmações.

Definição 5.3.1 Sejam $a \in \mathbb{K}$ e $f = \sum_{i=0}^{\infty} a_i X^i$ um polinômio de $\mathbb{K}[X]$. Chama-se **valor** de f em a ao elemento

$$f(a) = \sum_{i=0}^{\infty} a_i a^i \in \mathbb{K}[X].$$

Note que, como a soma $\sum_{i=0}^{\infty} a_i a^i$ é finita, pois apenas um número finito de coeficientes de f é diferente de 0, o elemento $f(a)$ está bem definido. Ainda, é fácil verificar que a função $\varphi_a : \mathbb{K}[X] \to \mathbb{K}$ que a cada polinômio $f \in \mathbb{K}[X]$ associa o valor $f(a)$ é tal que

$$\begin{aligned} \varphi_a(f+g) &= \varphi_a(f) + \varphi_a(g), \\ \varphi_a(fg) &= \varphi_a(f)\,\varphi_a(g). \end{aligned}$$

Em outras palavras, tem-se que

$$\begin{aligned} (f+g)(a) &= f(a) + g(a), \\ (fg)(a) &= f(a)\,g(a). \end{aligned}$$

Exemplo 5.3.1

Sejam $f = X^2 + X + 1, g = 2X^2 + X - 1 \in \mathbb{Q}[X]$. Então $f(1) = 3$ e $g(1) = 2$. Por outro lado temos que

$$\begin{aligned} f+g &= 3X^2 + 2X, \\ fg &= 2X^4 + 3X^3 + 2X^2 - 1, \end{aligned}$$

donde

$$\begin{aligned} (f+g)(1) &= 5 = 3 + 2 = f(1) + g(1), \\ (fg)(1) &= 6 = 3 \cdot 2 = f(1)\,g(1). \end{aligned}$$

Definição 5.3.2 Seja f um polinômio de $\mathbb{K}[X]$. Um elemento $a \in \mathbb{K}$ diz-se uma **raiz** de f se $f(a) = 0$.

O fato de existir em Algoritmo da divisão $\mathbb{K}[X]$ nos permitira discutir rigorosamente a questão de quantas raízes um polinômio pode ter. Os resultados a seguir são de demonstração muito simples, mas de grande importância para nosso objetivo.

Teorema 5.3.1 (Teorema do Resto) *Sejam f um polinômio de $\mathbb{K}[X]$ e a um elemento de $\mathbb{K}$. Então, o resto da divisão de f pelo polinômio $X-a$ é precisamente $f(a)$.*

Demonstração: Conforme o Algoritmo da Divisão, existem $q, r \in \mathbb{K}[X]$ tais que

$$f = (X-a)\,q + r \quad \text{com} \quad r = 0 \text{ ou } \operatorname{gr}(r) < \operatorname{gr}(X-a).$$

Calculando o valor de ambos os membros dessa igualdade em a temos:

$$f(a) = (a-a)\,q(a) + r = r,$$

como queríamos demonstrar. □

Corolário 5.3.1 (Teorema de Descartes) *Sejam f um polinômio de $\mathbb{K}[X]$ e a um elemento de $\mathbb{K}$. Então, a é raiz de f se e somente se f é divisível por $X-a$.*

Demonstração: Basta observar que a é raiz de f se e somente se o resto da divisão de f por $X-a$ é igual a 0. □

Definição 5.3.3 Sejam f um polinômio de $\mathbb{K}[X]$ e a um elemento de $\mathbb{K}$. Diz-se que a é uma raiz de f de **multiplicidade** m se $(X-a)^m$ divide f e $(X-a)^{m+1}$ não divide f.

Em outras palavras, se a é uma raiz de f sabemos, pelo Teorema de Descartes, que $(X-a)$ divide f. A multiplicidade de a como raiz de f é a *maior potência de $(X-a)$ que divide f*.

Teorema 5.3.2 *Um polinômio $f \in \mathbb{K}[X]$, de grau n tem, no máximo, n raízes (contadas com as respectivas multiplicidades) em $\mathbb{K}$.*

DEMONSTRAÇÃO: Vamos demonstrar o resultado por indução em n.

Se $n = 1$ então f é da forma $aX + b$ e é fácil ver que a única raiz de f em $\mathbb{K}$ é $X = -\frac{b}{a}$.

Seja então $\operatorname{gr}(f) = n$ e suponhamos, como hipótese de indução, que o resultado vale para todo polinômio de grau menor do que n.

Se f não tem raízes em $\mathbb{K}$, o resultado é trivialmente verdadeiro. Suponhamos então que f tem uma raiz $a \in \mathbb{K}$ e seja m a sua multiplicidade. Conforme à definição de multiplicidade, existe $g \in \mathbb{K}[X]$ tal que

$$f = (X - a)^m g.$$

Como $\operatorname{gr}(f) = m + \operatorname{gr}(g)$, temos que $m \leq n$ e $\operatorname{gr}(g) = n - m$. Se f não tem outras raízes, o resultado está demonstrado.

Note que, se $b \neq a$ é outra raiz de f então b é raiz de g. De fato, se b é raiz de f temos que

$$0 = f(b) = (b - a)\, g(b)$$

e, como $(b - a) \neq 0$ segue que $g(b) = 0$. Assim, todas as outras raízes de f são raízes de g e, pela hipótese de indução, g tem no máximo t raízes, onde

$$t \leq \operatorname{gr}(g) = n - m.$$

Logo, f tem ao todo $m + t$ raízes. Como $m + t \leq m + (n - m) = n$, o resultado está demonstrado. □

Em relação a este resultado, veja também o Exercício 10.

Exercícios

1. Sejam $f = X^2 + X + 1, g = 2X^2 + x - 1 \in \mathbb{Z}_5[X]$.

   (a) Calcular $f(-1)$ e $g(-1)$.

   (b) Achar os polinômios $f + g$ e fg.

   (c) Calcular $(f + g)(a)$ e $(fg)(a)$ e verificar que $(f + g)(a) = f(a) + g(a)$ e $(fg)(a) = f(a)\, g(a)$.

2. Determinar todas as raízes do polinômio $f = 2X^2 + X - 1 \in \mathbb{Z}_5[X]$ em $\mathbb{Z}_5$, testando todos os valores possíveis.

3. Mostre que o polinômio $f = X^2 + 5X + 6 \in \mathbb{Z}_6[X]$ tem mais que duas raízes em $\mathbb{Z}_6$.

4. (a) Provar que se um elemento $a \in \mathbb{K}$ é raiz dos polinômios $f, g \in \mathbb{K}[X]$, então a é raiz do resto de dividir f por g.

   (b) Deduzir que, se $f, g \in \mathbb{K}[X]$ têm raízes comuns, então $\mathrm{mdc}(f, g) \neq 1$.

5. Seja $f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \in \mathbb{Q}[X]$ um polinômio tal que todos seus coeficientes são números inteiros. Provar que, se $\alpha = \frac{p}{q} \in \mathbb{Q}$ é uma raiz de f, então $p \mid a_0$ e $q \mid a_n$.

6. Achar todas as raízes de $f = 3X^3 + X^2 + 6X + 2$ em $\mathbb{Q}$ e em $\mathbb{R}$.

7. Provar que o polinômio $f = X^4 - 2X^2 + 8X + 1$ é irredutível em $\mathbb{Q}[X]$.

8. Sejam $a, b \in \mathbb{K}$, com $a \neq b$. Provar que se um polinômio f é divisível por $X - a$ e por $X - b$ em $\mathbb{K}[X]$, então é divisível pelo produto $(X - a)(X - b)$.

9. Determinar todos os inteiros primos p tais que $X^4 + X^3 - X^2 - X + 24$ é divisível por $X + 2$ em $\mathbb{Z}_p[X]$.

10. Seja $f \in \mathbb{K}[X]$ um polinômio de grau n e sejam $\alpha_1, \ldots, \alpha_t$ todas as raízes de f em $\mathbb{K}$, com multiplicidades $m_1, \ldots m_t$ respectivamente. Provar que

$$f = (X - \alpha_1)^{m_1} \cdots (X - \alpha_t)^{m_t} g$$

    onde $g \in \mathbb{K}x$ é um polinômio que não tem raízes em $\mathbb{K}$.

11. Seja f um polinômio de $\mathbb{K}[X]$. Definimos uma função $\varphi_f : \mathbb{K} \to \mathbb{K}$ associando a cada elemento $a \in \mathbb{K}$ o valor $f(a) \in \mathbb{K}$. Esta função chama-se a **função polinomial** definida por f.

    (a) Provar que, quando $\mathbb{K}$ é um conjunto infinito, dados dois polinômios $f, g \in \mathbb{K}[X]$ tem-se que $\varphi_f = \varphi_g$ se e somente se $f = g$; isto é, dois

polinômios definem a mesma função se e somente se são iguais (este resultado era chamado, classicamente, de **Princípio da Identidade de Polinômios**).

(b) Seja p um inteiro primo. Mostrar que existem polinômios diferentes $f, g \in \mathbb{Z}_p[X]$ tais que $\varphi_f = \varphi_g$; isto é, tais que $f(a) = g(a)$ para todo $a \in \mathbb{Z}_p[X]$.

6

O Teorema Fundamental da Álgebra

6.1 Introdução

Desde a introdução dos números complexos, uma preocupação fundamental em matemática foi saber se estes números seriam suficientes para resolver todas as equações algébricas ou se a resolução de equações de graus maiores forçariam a introdução de novos conjuntos numéricos. Depois da demonstração da Fórmula de De Moivre, ficou claro que, se fosse possível resolver equações de graus maiores usando as operações algébricas e, eventualmente, radicais, então os números complexos seriam suficientes. Infelizmente não foi possível achar fórmulas dessa natureza e, com os trabalhos de Ruffini de 1805 e de Abel de 1825, ficou claro que tais fórmulas não existiam para equações algébricas de grau maior o igual a 5.

No entanto, esse não foi o único caminho a ser tentado. Também se procuraram caminhos alternativos para demonstrar o Teorema Fundamental da Álgebra, que pode se enunciar brevemente da seguinte forma:

Todo polinômio com coeficientes complexos tem n raízes complexas.

Em 1702, **Gottfried Wilhelm Leibniz** acreditou ter uma prova de que o teorema era falso. Ele afirmou que um polinômio da forma $X^4 + a^4$ não poderia ser escrito como produto de dois polinômios de segundo grau (o que necessariamente deveria acontecer se o teorema fosse verdadeiro). Em 1742,

Leonhard Euler, em correspondências com **N. Bernoulli** e **C. Goldbach**, mostrou que o contraexemplo estava errado, exibindo a fatoração correta (veja o Exercício 12).

A primeira tentativa séria de demonstrar o teorema é devida a **D'Alembert**, em 1746, mas ele usava sem demonstração um resultado que só foi provado em 1851 por Poiseaux e cuja prova depende deste teorema. Em 1749 Euler tentou dar outra prova mas sua demonstração é rigorosa para equações de quarto grau, mas apenas um esboço no caso geral.

Em 1772, **Joseph Louis Lagrange** deu um longo argumento, baseado no seu trabalho com permutações, tentando "completar" a prova de Euler. Porém, de certa forma, Lagrange assumia que existiam n raízes e que estas tinham as propriedades dos números. Nessas condições, ele conseguia provar que as raízes eram, de fato, números complexos.

Finalmente, a primeira prova realmente completa do Teorema Fundamental da Álgebra foi dada por **Carl Friederich Gauss** na sua tese de doutoramento, em 1799, intitulada *Nova demonstração do teorema que toda função algébrica racional inteira de uma variável pode ser decomposta em fatores reais de primeiro e segundo grau.* Como observaram diversos autores, a única incorreção da tese está no título, uma vez que não se trata de uma *nova demonstração* mas da *primeira demonstração* realmente correta (para os padrões da época) de tal fato.

Mesmo a prova de Gauss, que usa propriedades do tipo "topológico" não pareceria completamente rigorosa ao leitor moderno pois, embora o argumento seja altamente original, ele depende de determinar a interseção de duas curvas. A prova, porém, está substancialmente correta e nos resulta totalmente satisfatória quando a parte "analítica" e é feita com o rigor a que hoje estamos acostumados e que seria introduzido no século seguinte.

Ao longo de sua vida, Gauss deu mais três provas diferentes deste teorema. Em 1814 **Jean Robert Argand** publicou uma prova que é considerada por vários autores como a prova mais simples do teorema, embora não seja completamente elementar. Estas e outras demonstrações hoje conhecidas podem-se ver num texto totalmente dedicado ao assunto [8].

6.2 O Teorema

Nesta seção vamos enunciar o Teorema Fundamental da Álgebra e estudar algumas de suas consequências importantes. No Apêndice final deste capítulo damos uma demonstração deste resultado.

Teorema 6.2.1 (Teorema Fundamental da Álgebra) *Seja*

$$f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0 \in \mathbb{C}[X]$$

um polinômio com coeficientes complexos, tal que $a_n \neq 0$ *e* $n \geq 1$. *Então existe* $\alpha \in \mathbb{C}$ *tal que* $f(\alpha) = 0$; *isto é,* f *tem pelo menos uma raiz em* $\mathbb{C}$.

A seguinte é uma consequência importante deste teorema.

Proposição 6.2.1 *Dado um polinômio* $f \in \mathbb{C}[X]$, *de grau* $n > 1$, *existem* $\alpha_1, \ldots, \alpha_r \in \mathbb{C}$, *inteiros positivos* $n_1, \ldots n_r$ *e* $a \in \mathbb{C}$ *tais que*

$$f = a(X - \alpha_1)^{n_1} \cdots (X - \alpha_r)^{n_r},$$

onde $\alpha_1, \ldots, \alpha_r$ *são as raízes distintas de* f, *tem-se que* $n_1 + \cdots + n_r = n = \operatorname{gr}(f)$ *e* a *é o coeficiente dominante de* f.

Demonstração: Faremos a demonstração por indução em n.

Se $n = 1$ então f é da forma $f = aX + b$ e podemos escrever

$$f = a\left(X - \left(-\frac{b}{a}\right)\right).$$

Claramente, a é o coeficiente dominante de f e $-\frac{b}{a}$ é sua única raiz.

Suponhamos, como hipótese de indução que o teorema vale para todo polinômio de grau menor que $n = \operatorname{gr}(f)$. Pelo Teorema Fundamental da Álgebra, f tem uma raiz α_1 em $\mathbb{C}$. Seja n_1 a multiplicidade de α_1. Então f é divisível por $(X - \alpha_1)^{n_1}$, donde existe $g \in \mathbb{C}[X]$ tal que

$$f = (X - \alpha_1)^{n_1} g,$$

e tem-se que $n = \operatorname{gr}(f) = n_1 + \operatorname{gr}(g)$.

Pela hipótese de indução, existem $a \in \mathbb{C}$, $\alpha_2, \ldots, \alpha_r \in \mathbb{C}$ e inteiros positivos $n_2, \ldots, n_r$ tais que

$$g = a\,(X - \alpha_2)^{n_2} \cdots (X - \alpha_r)^{n_r}\,,$$

com $n_2 + \cdots + n_r = \operatorname{gr}(g)$.

Substituindo esta expressão de g na fórmula para f acima, a tese segue imediatamente. □

Este resultado pode-se enunciar equivalentemente, da seguinte forma.

Corolário 6.2.1 *Dado um polinômio $f \in \mathbb{C}[X]$, de grau $n > 1$ existem $\alpha_1, \ldots, \alpha_n$ (não necessariamente distintos) e $a \in \mathbb{C}$ tais que*

$$f = a\,(X - \alpha_1) \cdots (X - \alpha_n)\,.$$

Como consequência imediata temos o seguinte.

Corolário 6.2.2 *Um polinômio mônico $f \in \mathbb{C}[X]$ é irredutível se e somente se ele da forma $f = X - a$, para algum elemento $a \in \mathbb{C}$.*

O próximo resultado nos permitirá classificar também os polinômios irredutíveis de $\mathbb{R}[X]$.

Proposição 6.2.2 *Seja $f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$ um polinômio com coeficientes reais. Se $\alpha \in \mathbb{C}$ é uma raiz de f então o seu conjugado $\overline{\alpha}$ também é raiz de f.*

Demonstração: Com efeito, se α é raiz de f temos que

$$0 = f(\alpha) = a_n \alpha^n + a_{n-1} \alpha^{n-1} + \cdots + a_1 \alpha + a_0$$

e tomando conjugados

$$\begin{aligned} 0 \;=\; \overline{f(\alpha)} \;&=\; \overline{a_n \alpha^n + a_{n-1} \alpha^{n-1} + \cdots + a_1 \alpha + a_0} \\ &=\; \overline{a_n}\,\overline{\alpha}^n + \overline{a_{n-1}}\,\overline{\alpha}^{n-1} + \cdots + \overline{a_1}\,\overline{\alpha} + \overline{a_0} \\ &=\; a_n \overline{\alpha}^n + a_{n-1} \overline{\alpha}^{n-1} + \cdots + a_1 \overline{\alpha} + a_0 \;=\; f(\overline{\alpha})\,. \end{aligned}$$

Esta última equação mostra que $\overline{\alpha}$ é raiz de f. □

COROLÁRIO 6.2.3 *Seja $f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$ um polinômio com coeficientes reais. Se $\alpha = a + bi \in \mathbb{C}$, com $b \neq 0$, é uma raiz de f, então este é divisível pelo polinômio $X^2 + (\alpha + \overline{a})\, X + \alpha\overline{\alpha} \in \mathbb{R}[X]$.*

DEMONSTRAÇÃO: Como α é raiz de f, pelo Teorema de Descartes, podemos escrever $f = (X - \alpha) \cdot g$, para algum $g \in \mathbb{C}[X]$. Ainda, como $\overline{\alpha}$ também é raiz de f temos

$$0 = f(\overline{\alpha}) = (\overline{a} - \alpha) \cdot g(\overline{\alpha}).$$

Como assumimos que $b \neq 0$ temos que $(\overline{a} - \alpha) \neq 0$, donde $g(\overline{a}) = 0$.

Novamente pelo Teorema de Descartes podemos escrever

$$g = (X - \overline{\alpha}) \cdot h,$$

para algum $h \in \mathbb{C}[X]$; portanto

$$\begin{aligned} f &= ((X - \alpha)(X - \overline{\alpha}))\, h \\ &= \left(X^2 + (\alpha + \overline{\alpha})\, X + \alpha\overline{\alpha}\right) h. \end{aligned}$$

Finalmente, como $\alpha + \overline{\alpha} = 2a$ e $\alpha\overline{\alpha} = a^2 + b^2$, temos que

$$X^2 + (\alpha + \overline{a})\, X + \alpha\overline{\alpha} \in \mathbb{R}[X].$$

Note ainda que, como f e $X^2 + (\alpha + \overline{a})\, X + \alpha\overline{\alpha}$ pertencem ambos a $\mathbb{R}[X]$, temos também que $h \in \mathbb{R}[X]$. □

COROLÁRIO 6.2.4 *Seja $f \in \mathbb{R}[X]$ um polinômio irredutível. Então f tem grau igual a 1 ou 2.*

DEMONSTRAÇÃO: Se f é irredutível, então ele é não constante, donde $\operatorname{gr}(f) \geq 1$. Pelo Teorema Fundamental, existe $\alpha \in \mathbb{C}$ tal que $f(\alpha) = 0$.

Se α é real, então podemos escrever $f = (X - \alpha)\, g$ em $\mathbb{R}[X]$ e, como f é irredutível, g deve ser constante. Logo $\operatorname{gr}(f) = 1$.

Se α não é real, pela Corolário 6.2.3 acima, existe $h \in \mathbb{R}[X]$ tal que $f = \left(X^2 + (\alpha + \overline{\alpha})\, X + \alpha\overline{\alpha}\right) h$ e, novamente, como f é irredutível, h deve ser constante. Logo $\operatorname{gr}(f) = 2$. □

Claramente, todo polinômio de primeiro grau é irredutível. O próximo resultado permite distinguir quais polinômios de segundo grau de $\mathbb{R}[X]$ são irredutíveis.

Proposição 6.2.3 *O polinômio*

$$f = aX^2 + bX + c$$

é irredutível se e somente se $b^2 - 4ac < 0$.

Demonstração: Se $b^2 - 4ac \geq 0$ então os números reais

$$\alpha_1 = \frac{-b + \sqrt{b^2 - 4ac}}{2} \quad \text{e} \quad \alpha_2 = \frac{-b - \sqrt{b^2 - 4ac}}{2}$$

são raízes do polinômio e ambos são números reais. Logo, podemos escrever f na forma

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

Logo, f não é irredutível.

Reciprocamente, se f é redutível em $\mathbb{R}[X]$, ele só pode ser produto de dois polinômios de primeiro grau. Portanto, existem $\alpha_1, \alpha_2 \in \mathbb{R}$ tais que

$$f = a(X - \alpha_1)(X - \alpha_2) = a\left(X^2 - (\alpha_1 + \alpha_1)X + \alpha_1\alpha_2\right),$$

donde

$$b = -a(\alpha_1 + \alpha_2) \quad \text{e} \quad c = a\alpha_1\alpha_2.$$

Logo,

$$b^2 - 4ac = a^2(\alpha_1 + \alpha_2)^2 - 4a^2\alpha_1\alpha_2 = a^2(\alpha_1 - \alpha_2)^2 \geq 0.$$

□

Exercícios

1. (a) Mostrar que o polinômio $f = X^2 + X + 4$ é irredutível em $\mathbb{R}[X]$.
   (b) Escrever f como produto de fatores irredutíveis em $\mathbb{C}[X]$.
   (c) Escrever f como produto de fatores irredutíveis em $\mathbb{Z}_3[X]$.

2. Escrever o polinômio $X^4 + 4$ como produto de fatores irredutíveis de $\mathbb{Z}_5[X]$.

3. Escrever o polinômio $X^3 + 2X^2 + 2X + 1$ como produto de fatores irredutíveis de $\mathbb{Z}_7[X]$.

4. Achar o resto de dividir um polinômio f por $(X + 2)(X - 1)$ sabendo que $f(-2) = -1$ e $f(1) = 8$.

5. Escrever o polinômio $X^4 + X^2 + 1$ como produto de fatores irredutíveis de $\mathbb{R}[X]$ e de $\mathbb{C}[X]$.

6. De um polinômio $f \in \mathbb{K}[X]$ sabe-se que, quando dividido por $X + 1$ da resto 3; que seu termo independente é -8 e que uma de suas raízes é -4. Achar o resto da divisão de f pelo produto $X(X + 1)(X + 4)$.

7. (a) Determinar o valor de m para que o polinômio $f = 2X^3 + (1 - 2m)X^2 + (1 - m)X + 1$ seja divisível por $(2X + 1)$.
   (b) Para o valor de m achado, decompor f com produto de polinômios irredutíveis de $\mathbb{Q}[X]$ e de $\mathbb{R}[X]$.

8. (a) Provar que um polinômio $f \in \mathbb{K}[X]$, de terceiro grau, é redutível se e se somente se tem uma raiz em $\mathbb{K}$.
   (b) Provar que o polinômio $X^3 + X + 2$ é irredutível em $\mathbb{Z}_5[X]$.
   (c) Escrever o polinômio $X^3 + 2X + 3$ como produto de polinômios irredutíveis de $\mathbb{Z}_5[X]$.

9. Determinar todos os polinômios irredutíveis de grau 3 em $\mathbb{Z}_2[X]$.

10. Mostrar que, para todo primo p existem polinômios em $\mathbb{Z}_p[X]$ que não têm nenhuma raiz em $\mathbb{Z}_p$.

11. Provar, sem utilizar noções de cálculo (mas admitindo o Teorema Fundamental da Álgebra) que todo polinômio de $\mathbb{R}[X]$, de grau ímpar, tem pelo menos uma raiz real.

12. Em 1702, G.W. Leibniz observou que se a é um número real, então

$$X^4 + a^4 = \left(X^2 + a^2 i\right)\left(x^2 - a^2 i\right)$$

embora não usando o símbolo i que só foi introduzido por Euler em 1777. Ele afirmou que este polinômio não poderia ser escrito como o produto de dois fatores de segundo grau em $\mathbb{R}[X]$, o que contraria o Corolário 6.2.4 e produziria, portanto, um contraexemplo para o Teorema Fundamental da Álgebra.

(a) Prove que

$$\sqrt{i} = \pm\left(\frac{1+i}{\sqrt{2}}\right) \quad \text{e} \quad \sqrt{-i} = \pm\left(\frac{1-i}{\sqrt{2}}\right).$$

(b) Escreva $X^4 - a^4$ como produto de dois fatores de segundo grau em $\mathbb{R}[X]$.

13. O *Pequeno Teorema de Fermat* afirma que, se p é um número primo e a é um inteiro tal que $p \nmid a$ então $a^{p-1} \equiv 1 \pmod{p}$.

(a) Utilize esse resultado para provar que, em $\mathbb{Z}_p[X]$ tem-se que

$$X^{p-1} - 1 = (X-1)(X-2)\cdots(X-(p-1)).$$

(b) Prove o *Teorema de Wilson*: Para todo primo p tem-se que

$$(p-1)! \equiv p - 1 \pmod{p}.$$

Daremos uma demonstração de ambos teoremas no Capítulo 10.

6.3 Polinômios com coeficientes racionais

Na seção anterior vimos critérios para decidir quando um polinômio é irredutível em $\mathbb{R}[X]$ e $\mathbb{C}[X]$. Estudar irredutibilidade de polinômios em $\mathbb{Q}[X]$ é um problema bem mais complicado, porque, como veremos, não há limitação para o grau destes polinômios, como acontece nos dois casos anteriores (veja o Exercício 2). Mesmo assim, há alguns critérios que podem ser de grande utilidade.

Definição 6.3.1 Seja $f = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0$ um polinômio com coeficientes inteiros. Chama-se **conteúdo** de f ao máximo comum divisor dos seus coeficientes $a_0, a_1, \ldots, a_n$.

Um polinômio diz-se **primitivo** se o seu conteúdo é igual a 1.

Lema 6.3.1 (Lema de Gauss) *Se $f, g \in \mathbb{Z}[X]$ são polinômios primitivos, então o seu produto fg também é um polinômio primitivo.*

Demonstração: Sejam

$$f = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0,$$
$$g = b_mX^m + b_{m-1}X^{m-1} + \cdots + b_0.$$

Suponhamos, por absurdo, que o produto fg não é primitivo. Isso significa que existe algum primo p que divide todos os coeficientes deste produto.

Como f é primitivo, existe algum coeficiente de f que não é divisível por p. Seja então r o menor índice tal que o $p \nmid a_r$

Da mesma forma, podemos determinar o menor índice s tal que $p \nmid b_s$.

O coeficiente de X^{r+s} é:

$$c_{r+s} = a_0b_{r+s} + a_1b_{r+s-1} + \cdots + a_{r-1}b_{s+1} + a_rb_s + a_{r+1}b_{s-1} + \cdots + a_{r+s}b_0.$$

Como p divide $a_0, a_1, \ldots a_{r-1}$ temos que p divide a soma

$$a_0b_{r+s} + a_1b_{r+s-1} + \cdots + a_{r-1}b_{s+1}.$$

De modo análogo segue que p também divide

$$a_r b_s + a_{r+1} b_{s-1} + \cdots + a_{r+s} b_0.$$

Como assumimos que p divide todo coeficiente do polinômio produto, p também divide c_{r+s}. Consequentemente, p divide o produto $a_r b_s$. Porém, p não divide a_r nem divide b_s, uma contradição. □

LEMA 6.3.2 *Seja $f \in \mathbb{Q}[X]$ um polinômio não nulo. Então f pode-se escrever sob a forma*

$$f = \frac{a}{b} f^*,$$

onde $a, b \in \mathbb{Z}$ e f^* é um polinômio primitivo de $\mathbb{Z}[X]$.

DEMONSTRAÇÃO: Seja

$$f = \frac{a_0}{b_0} + \frac{a_1}{b_1} X + \cdots + \frac{a_n}{b_n} X^n \in \mathbb{Q}[X],$$

onde $a_i, b_i \in \mathbb{Z}$, $0 \leq i \leq n$.

Chamando $b = b_0 b_1 \cdots b_n$, podemos escrever

$$f = \frac{1}{b} f_1, \text{ com } f_1 = a_0' + a_1' X + \cdots + a_n' X^n \text{ onde } a_i' = a_i \frac{b}{b_i} \in \mathbb{Z}, \ 0 \leq i \leq n.$$

Ainda, se $a = \operatorname{mdc}(a_0, a_1, \ldots, a_n)$ podemos escrever $a_i' = a c_i$, $0 \leq i \leq n$, e temos que $\operatorname{mdc}(c_0, c_1, , \ldots, c_n) = 1$. Logo, $f = \frac{a}{b} f^*$, onde $f^* = c_o + c_1 X + \cdots + c_n X^n \in \mathbb{Z}[X]$ é um polinômio primitivo. □

TEOREMA 6.3.1 *Seja $f \in \mathbb{Z}[X]$ um polinômio primitivo. Se f pode ser fatorado como o produto de dois polinômios não constantes de $\mathbb{Q}[X]$ então também pode ser fatorado como o produto de dois polinômios não constantes de $\mathbb{Z}[X]$.*

DEMONSTRAÇÃO: Se f pode-se escrever na forma $f = gh$, onde $g, h \in \mathbb{Q}[X]$ são polinômios não constantes, aplicando o lema anterior a cada um dos fatores podemos escrever:

$$g = \frac{a}{b} g^*, \quad h = \frac{c}{d} h^*,$$

onde g^* e h^* são polinômios primitivos de $\mathbb{Z}[X]$. Então temos

$$(bd)\, f = (ac)\, g^* h^*.$$

Pelo Lema de Gauss, g^*h^* é um polinômio primitivo. Logo, ac é o conteúdo do polinômio $(ac)\, g^*h^*$. Da mesma forma, temos que bd é o conteúdo do polinômio $(bc)\, f$. Como ambos polinômios são iguais, temos que $ac = bd$ e, cancelando, $f = g^*h^*$, onde g^* e h^* são polinômios primitivos de $\mathbb{Z}[X]$. Ainda, temos que $\operatorname{gr}(g) = \operatorname{gr}(g^*)$ e $\operatorname{gr}(h) = \operatorname{gr}(h^*)$; logo, estes polinômios não são constantes. □

Teorema 6.3.2 (Critério de Irredutibilidade de Eisenstein) *Seja*

$$f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0,$$

um polinômio com coeficientes inteiros. Se existe um número primo p tal que

$$p \nmid a_n, \quad p \mid a_i,\ 0 \leq i \leq n-1, \quad e \quad p^2 \nmid a_0$$

então f é irredutível em $\mathbb{Q}[X]$.

Demonstração: De acordo com o Lema 6.3.1, será suficiente provar que f não pode ser fatorado como produto de dois polinômios não constantes em $\mathbb{Z}[X]$. Suponhamos então que

$$f = (b_r X^r + \cdots + b_0)(c_s X^s + \cdots + c_0), \text{ em } \mathbb{Z}[X], \text{ com } b_r \neq 0,\ c_s \neq 0.$$

Como $a_0 = b_0 c_0$ é divisível por p, mas não é divisível por p^2, segue que p divide um dos coeficientes b_0, c_o, mas não ambos. Suponhamos que $p \mid b_0$ e que $p \nmid c_0$.

Claramente, p não pode dividir todos os coeficientes $b_i, 0 \leq i \leq r$, pois, nesse caso, p dividiria todos os coeficientes de f, inclusive a_n.

Seja k o menor índice tal que $p \nmid b_k$. Note que $k \leq r < n$, . Calculamos então:

$$a_k = b_k c_0 + b_{k-1} c_1 + \cdots + b_0 c_k.$$

Como p divide $b_{k-1}, \ldots b_0$ segue que p divide a soma $b_{k-1}c_1 + \cdots + b_0c_k$. Ainda, como $k < n$ sabemos, por hipótese, que $p \mid a_k$, donde também $p \mid b_k c_0$.

Isto é uma contradição, pois $p \nmid b_k$ e $p \nmid c_0$. □

EXEMPLO 6.3.1

Consider o polinômio

$$f = 13X^5 + 6X^4 + 3X^3 + 9X - 15.$$

Como $3 \nmid 13$, mas $3 \mid 6$, $3 \mid 3$, $3 \mid 9$, $3 \mid 15$ mas $3^3 = 9$ não divide 15, segue que f é irredutível em $\mathbb{Q}[X]$.

Uma consequência importante do Critério de Eisenstein é a seguinte.

COROLÁRIO 6.3.1 *Para todo número primo p o p-ésimo* **polinômio ciclotômico***:*

$$\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1,$$

é irredutível em $\mathbb{Q}[X]$.

DEMONSTRAÇÃO: Inicialmente observamos que

$$\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1 = \frac{X^p - 1}{X - 1}.$$

Fazemos então a mudança de variável $X = x + 1$ e temos:

$$\begin{aligned} g(x) &= \Phi_p(x+1) \\ &= \frac{(x+1)^{p-1} - 1}{x + 1 - 1} \\ &= \frac{x^p + \binom{p}{1}x^{p-1} + \cdots + \binom{p}{1}x + 1 - 1}{x + 1 - 1} \\ &= x^p + \binom{p}{1}x^{p-1} + \binom{p}{2}x^{p-2} + \cdots + \binom{p}{1}. \end{aligned}$$

É claro que $g(x)$ é irredutível se e somente se $\Phi_p(X)$ é irredutível (pois se $\Phi_p(X)$ fosse redutível, a mudança de variável, efetuada em cada um dos fatores de $\Phi_p(X)$ daria uma decomposição para g).

Como os coeficientes $\binom{p}{i}$, $1 \leq i \leq p-1$, são todos múltiplos de p e $\binom{p}{1} = p$ não é múltiplo de p^2, pelo critério de Eisenstein, segue que g, e consequentemente também $\Phi_p(X)$, é irredutível. □

O próximo resultado também pode ser útil para decidir quando um polinômio de $\mathbb{Z}[X]$ é irredutível.

Teorema 6.3.3 *Sejam p um primo e*

$$f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0,$$

um polinômio com coeficientes inteiros e seja

$$\overline{f} = \overline{a_n} X^n + \overline{a_{n-1}} X^{n-1} + \cdots + \overline{a_1} X + \overline{a_0},$$

onde $\overline{a_i}$ indica a classe de a_i em $\mathbb{Z}_p$, $0 \leq i \leq n$.

Se $\overline{f}$ é irredutível em $\mathbb{Z}_p[X]$ e $\operatorname{gr}(\overline{f}) = n = \operatorname{gr}(f)$, então f é irredutível em $\mathbb{Q}[X]$.

Demonstração: Se f é redutível em $\mathbb{Q}[X]$, pelo Teorema 6.3.1 podemos escrever $f = g \cdot h$, com $g, h \in \mathbb{Z}[X]$ e $\operatorname{gr}(g) < \operatorname{gr}(f)$, $\operatorname{gr}(h) < \operatorname{gr}(f)$.

Sejam $\overline{g}$ e $\overline{h}$ os polinômios de $\mathbb{Z}_p[X]$ que se obtém tomando classes módulo p nos coeficientes de g e h respectivamente.

Então

$$\overline{f} = \overline{g} \cdot \overline{h}.$$

Como

$$\operatorname{gr}(\overline{g}) \leq \operatorname{gr}(g) < \operatorname{gr}(f),$$
$$\operatorname{gr}(\overline{h}) \leq \operatorname{gr}(h) < \operatorname{gr}(f),$$

e $\operatorname{gr}(f) = \operatorname{gr}(\overline{f})$, a decomposição acima mostra que f é redutível em $\mathbb{Z}_p[X]$, uma contradição. □

Exercícios

1. Seja $f \in \mathbb{Z}[X]$ e seja a um número racional tal que $(X-a)$ divide f em $\mathbb{Q}[X]$. Provar que a é inteiro.

2. Sejam p um inteiro primo e n um inteiro positivo. Provar que o polinômio $X^n - p$ é irredutível em $\mathbb{Q}[X]$.

3. Seja $f \in \mathbb{K}[X]$ um polinômio e $a \neq 0$ um elemento de $\mathbb{K}$.

   (a) Provar que $f(X)$ é irredutível se e somente se $f(aX)$ é irredutível.

   (b) Provar que $f(X)$ é irredutível se e somente se $f(a+X)$ é irredutível.

4. Decidir quais dos seguintes polinômios são irredutíveis em $\mathbb{Q}[X]$.

   (a) $X^3 + 2X^2 + 2X + 1$.

   (b) $X^7 + 25X^5 - 20X^2 + 15$.

   (c) $X^5 + 5X^2 + 3$.

5. Escrever o polinômio $X^4 - X^3 + 2X^2 - X + 1$ como produto de fatores irredutíveis de $\mathbb{R}[X]$ e de $\mathbb{C}[X]$.

6. Decidir se o polinômio $X^2 + X + 4$ é irredutível em $\mathbb{Z}_7[X]$.

7. Determinar todos os valores de m para os quais o polinômio $X^2 + mX + (m+1)$ é redutível em $\mathbb{Z}_5[X]$.

8. Provar que o polinômio $f = X^4 + 1$ é irredutível em $\mathbb{Q}[X]$ e escrever f como produto de polinômios irredutíveis de $\mathbb{R}[X]$ e de $\mathbb{C}[X]$.

9. Seja $p \neq 2$ um inteiro primo.

   (a) Provar que existe um elemento $b \in \mathbb{Z}_p$ tal que $b^2 = 1$.

   (b) Mostrar que o polinômio $X^4 + 1$ é redutível em $\mathbb{Z}_p$.

10. Escrever o polinômio $f = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$ como produto de fatores irredutíveis em $\mathbb{Q}[X]$, $\mathbb{R}[X]$ e $\mathbb{C}[X]$.

11. Seja p um inteiro primo. Provar que o polinômio

$$X^{p-1} - x^{p-2} + X^{p-3} - \cdots - X + 1$$

é irredutível em $\mathbb{Q}[X]$.

12. Utilizando as idéias da demonstração do Corolário 6.3.1, provar que os seguintes polinômios são irredutíveis em $\mathbb{Q}[X]$.

(a) $X^6 + X^3 + 1$.

(b) $X^3 + 3X + 2$.

(c) $X^3 + 6X^2 + 1$.

13. Seja $f = \sum_{i=0}^{n} a_i X^i$ um polinômio de grau ímpar, tal que

$$a_n = a_{n-2} = 1 \quad \text{e} \quad a_{n-1} = 0.$$

Provar que, para todo inteiro a, o polinômio $f(X + a)$ não satisfaz as condições do critério de irredutibilidade de Eisenstein.

6.4 Relações entre raízes e coeficientes

O leitor provavelmente sabe que se α_1, α_2 são as raízes da equação $aX^2 + bX + c$, então tem-se que

$$\begin{aligned} -b/a &= \alpha_1 + \alpha_2, \\ c/a &= \alpha_1\alpha_2. \end{aligned}$$

Da mesma forma, se $\alpha_1, \alpha_2, \alpha_3$ são as raízes do polinômio

$$a_3X^3 + a_2X^2 + a_1X + a_0$$

então:

$$\begin{aligned} -a_2/a_3 &= \alpha_1 + \alpha_2 + \alpha_3, \\ a_1/a_3 &= \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3, \\ -\alpha_0/a_3 &= \alpha_1\alpha_2\alpha_3. \end{aligned}$$

Relações semelhantes a estas valem no caso geral. Dados $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{C}$ definimos a k ésima **função simétrica elementar** nestes elementos como:

$$\sigma_k(\alpha_1, \alpha_2, \ldots, \alpha_n) = \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} \alpha_{i_1} \alpha_{i_2} \cdots \alpha_{i_k},$$

isto é, $\sigma_k(\alpha_1, \alpha_2, \ldots, \alpha_n)$ é a soma de todos os produtos de k fatores, nesses valores. Consequentemente, $\sigma_k(\alpha_1, \alpha_2, \ldots, \alpha_n)$ é uma soma de $\binom{n}{k}$ termos.

Exemplo 6.4.1

Para $n = 4$ as funções simétricas elementares são:

$$\begin{aligned}
\sigma_1(\alpha_1, \alpha_2, \alpha_3, \alpha_4) &= \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4, \\
\sigma_2(\alpha_1, \alpha_2, \alpha_3, \alpha_4) &= \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_3 + \alpha_2\alpha_4 + \alpha_3\alpha_4, \\
\sigma_3(\alpha_1, \alpha_2, \alpha_3, \alpha_4) &= a_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \alpha_1\alpha_3\alpha_4 + \alpha_2\alpha_3\alpha_4, \\
\sigma_4(\alpha_1, \alpha_2, \alpha_3, \alpha_4) &= \alpha_1\alpha_2\alpha_3\alpha_4.
\end{aligned}$$

A teoria das funções simétricas foi desenvolvida por Lagrange, Ruffini, Galois e outros, para discutir a resolução de equações algébricas. A expressão aparece explicitamente no texto de Lacroix [15, p. 277], onde diz:

> *As funções de que falo, são aquelas que contém todas as raízes combinadas de uma maneira semelhante, seja entre elas, seja com outras quantidades, e que por isso eu as chamei de funções simétricas.*

Incidentalmente, nesse mesmo texto ele introduz também, pela primeira vez, a expressão *geometria analítica* para se referir a teoria criada quase dois séculos antes por Descartes e Fermat que ele descreve da seguinte forma:

> *Existe uma maneira de ver a geometria que poderia ser chamada de geometria analítica, que consiste em deduzir as propriedades da extensão do menor número possível de princípios, por métodos verdadeiramente analíticos.*

Um cálculo direto - ou, mais formalmente, um argumento de indução (veja o Exercício 5) - mostra que

$$\begin{aligned}\prod_{i=1}^{n}(X-\alpha_i) &= X^n-\sigma_1(\alpha_1,\alpha_2,\ldots,\alpha_n)X^{n-1}+\sigma_{n-2}(\alpha_1,\alpha_2,\ldots,\alpha_n)X^{n-}\\ &\quad\cdots+(-1)^n\sigma_0(\alpha_1,\alpha_2,\ldots,\alpha_n).\end{aligned}$$

Podemos usar esta observação para estabelecer uma relação entre as raízes e os coeficientes de uma equação algébrica.

Teorema 6.4.1 *Seja*

$$f=a_nX^n+a_{n-1}X^{n-1}+\cdots+a_1X+a_0,$$

um polinômio de $\mathbb{C}[X]$ *e sejam* $\alpha_1,\alpha_2,\ldots,\alpha_n$ *suas raízes. Então:*

$$\frac{a_{n-k}}{a_n}=(-1)^k\sigma_k(\alpha_1,\alpha_2,\ldots,\alpha_n),\quad 1\leq k\leq n.$$

Demonstração: De fato, temos que $f=a_n\prod_{i=1}^{n}(X-\alpha_i)$ e, usando a fórmula acima, o resultado segue imediatamente. □

Estas relações podem ser usadas para resolver equações algébricas, quando temos informações adicionais sobre suas raízes.

Exemplo 6.4.2

Vamos determinar as raízes do polinômio $9X^3-36X^2+44X-16$ sabendo que uma delas é igual à soma das outras duas.

Usando as relações do teorema acima temos:

$$\begin{aligned}36/9 &= (\alpha_1+\alpha_2+\alpha_3), &(6.1)\\ 44/9 &= \alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3, &(6.2)\\ -16/9 &= \alpha_1\alpha_2\alpha_3. &(6.3)\end{aligned}$$

Ainda, sabemos que

$$\alpha_1=\alpha_2+\alpha_3. \tag{6.4}$$

De (6.1) e (6.4) temos que $2\alpha_1 = 36/9 = 4$ donde $\alpha_1 = 2$.
Substituindo em (6.2) segue que

$$2(\alpha_2 + \alpha_3) + \alpha_2\alpha_3 = 44/9$$

donde $\alpha_2\alpha_3 = 44/9 - 4 = 8/9$.

Como $\alpha_2 + \alpha_3 = 2$ α_2 e α_3 são as raízes da equação

$$X^2 - 2X + 8/9;$$

logo $\alpha_2 = 4/3$ e $\alpha_3 = 2/3$.

Exercícios

1. Dado o polinômio $X^3 + aX^2 + bX + c$ determinar relações entre a, b e c para que

   (a) As raízes formem uma progressão geométrica.

   (b) Uma raiz seja oposta de outra.

   (c) Uma raiz seja igual à soma das outras duas.

2. Dado o polinômio $f = X^2 + bX + c$, determinar os coeficientes do polinômio de segundo grau cujas raízes são os quadrados das raízes de f.

3. Dado o polinômio $f = X^3 + aX^2 + bX + c$, determinar os coeficientes do polinômio de terceiro grau cujas raízes são os cubos das raízes de f.

4. * Um estudante acordou no fim de uma aula de álgebra, justo a tempo de ouvir o professor dizer "e lhes digo, como sugestão, que as raízes desta equação formam uma progressão aritmética". Olhando o quadro, o aluno viu uma equação de quinto grau que devia ser resolvida como dever de casa, mas apenas teve tempo de copiar

$$X^5 - 5X^4 - 35X^3$$

* Este exercício aparece na página `http://www.cs.berkeley.edu/~oholtz/191/equations.pdf`.

antes de que o professor apagasse o quadro. Ele conseguiu encontrar todas as raízes, mesmo assim. Quais são essas raízes?

5. (a) Provar que

$$\sigma_k(\alpha_1, \alpha_2, \ldots, \alpha_{n-1}) + \sigma_{k-1}(\alpha_1, \alpha_2, \ldots, \alpha_n) = \sigma_k(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

(b) Provar, usando indução em n, que

$$\begin{aligned}\prod_{i=1}^{n}(X - \alpha_i) &= X^n - \sigma_1(\alpha_1, \alpha_2, \ldots, \alpha_n) X^{n-1} + \sigma_{n-2}(\alpha_1, \alpha_2, \ldots, \alpha_n \\ &\quad \cdots + (-1)^n \sigma_0(\alpha_1, \alpha_2, \ldots, \alpha_n).\end{aligned}$$

6.5 Apêndice: Uma demonstração do Teorema Fundamental da Álgebra

Nesta seção vamos dar uma prova do Teorema Fundamental da Álgebra que é razoavelmente elementar, devida a O.R.B. de Oliveira [19]. Uma característica interessante do teorema é que, apesar do seu nome, ele não é um teorema puramente algébrico; precisa de alguns resultados do cálculo. Para a nossa demonstração precisaremos de poucos fatos.

Em primeiro lugar, dado um polinômio $f \in \mathbb{C}[X]$, vamos considerar a *função polinomial* que a cada número complexo $z \in \mathbb{C}$ associa o valor de f em z, que denotaremos por $f(z)$ e vamos considerar também a função de $\mathbb{C}$ em $\mathbb{R}$ que a cada $z \in \mathbb{C}$ associa o número real $|f(z)|$ e admitiremos aqui, sem demonstração. que esta função é contínua.

Também admitiremos o fato intuitivamente óbvio de que, se a é um complexo fixado então, para cada inteiro positivo m tem-se que

$$\lim_{|z|\to\infty} \frac{|a|}{|z|^m} = 0.$$

Precisaremos ainda da seguinte versão simplificada do Teorema de Weierstrass, que assumimos conhecido do leitor, e que fazem parte dos cursos de Cálculo.

TEOREMA 6.5.1 (WEIERSTRASS) *Seja D um disco fechado do plano complexo. Toda função contínua $\varphi : D \to \mathbb{R}$ tem um mínimo em D.*

Admitidos estes fatos, estamos em condições de provar o teorema principal deste capítulo. Para isso precisamos um resultado preliminar.

LEMA 6.5.1 *A função $|f(z)|$ tem um mínimo absoluto num ponto $z_0 \in \mathbb{C}$.*

DEMONSTRAÇÃO: Pelo Exercício 22 da seção 4.3 (p. 86), para cada complexo $z \in \mathbb{C}$ temos

$$\begin{aligned} |f(z)| &= \left|a_n z^n + a_{n-1} z^{n-1} + \cdots + a_0\right| \\ &\geq |a_n|\,|z|^n - |a_{n-1}|\,|z|^{n-1} - \cdots - |a_0| \\ &= |z|^n \left(|a_n| - \frac{|a_{n-1}|}{|z|} - \cdots - \frac{|a_0|}{|z|^n}\right). \end{aligned}$$

Logo,

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

Seja então $\gamma = |f(0)|$. Como $|f(z)|$ tende a infinito, existe um disco fechado D, com centro na origem e raio k tal que, fora do disco, o valor de $|f(z)|$ é maior do que γ; isto é, tal que se $|z| > k$, então $|f(z)| > \gamma$.

Pelo Teorema 6.5.1, $|f(z)|$ tem um mínimo α_0 em D e seja z_0 um ponto em que esse mínimo é atingido, ou seja, um ponto em D tal que $|f(z_0)| = \alpha_0$. Se $z \in D$, então, por construção, $f(z) \geq \alpha_0$ e, em particular, também $\gamma = |f(0)| \geq \alpha_0$.

Ainda, se $z \notin D$, então $|f(z)| > \gamma \geq \alpha_0$. Este argumento mostra que para todo $z \in \mathbb{C}$ tem-se que $|f(z)| \geq a_0$, donde α_0 é um mínimo absoluto de $|f(z)|$. □

TEOREMA 6.5.2 (TEOREMA FUNDAMENTAL DA ÁLGEBRA) *Seja*

$$f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0 \in \mathbb{C}[X]$$

um polinômio com coeficientes complexos, tal que $a_n \neq 0$ e $n \geq 1$. Então existe $\alpha \in \mathbb{C}$ tal que $f(\alpha) = 0$; isto é, f tem pelo menos uma raiz em $\mathbb{C}$.

DEMONSTRAÇÃO: Fazendo a mudança de variável $\zeta = z - z_0$ segue que a função

$$h(\zeta) = f(z - z_0)$$

é tal que

$$h(0) = f(z_0).$$

Como o conjunto de todos os valores de $|h(\zeta)|$ é igual ao conjunto dos valores de $f(z)$ segue que a função $|h(\zeta)|$ tem um mínimo absoluto no ponto $\zeta = 0$ e $|h(0)| = \alpha_0$.

Queremos provar que $\alpha_0 = 0$, o que implicará que 0 e raiz de $h(\zeta)$ e, portanto, que z_0 é uma raiz de $f(z)$.

Suponhamos, por absurdo que $\alpha_0 > 0$.

Note que $h(\zeta)$ é um polinômio de grau n em ζ. Podemos escrevê-lo então sob a forma

$$h(\zeta) = b_0 + b_1\zeta + \cdots b_n\zeta^n, \quad \text{com} \quad b_i \in \mathbb{C},\ 0 \leq i \leq n.$$

Com esta notação, temos que $|b_0| = |h(0)| = \alpha_0 > 0$.

Pode acontecer que alguns coeficientes b_i, com $i > 0$ sejam nulos. Seja então $m > 0$ o menor índice tal que $b_m \neq 0$. Podemos escrever $h(\zeta)$ na forma

$$h(\zeta) = b_0 + b_m\zeta^m + \zeta^{m+1}g(\zeta),$$

onde $g(\zeta)$ é um polinômio.

Pela fórmula de Teorema 4.4.1, existe um complexo γ_1 tal que

$$\gamma_1^m = -\frac{b_m}{b_0}.$$

Fazendo a mudança de variável $\zeta = \gamma_1\zeta_1$ e denotando

$$\frac{1}{|b_0|\, g(\gamma_1\zeta_1)} = g_1(\zeta_1)$$

temos:

$$h(\zeta_1) = b_0 - b_0\zeta_1^m + b_0\zeta_1^{m+1}g_1(\zeta_1) = b_0\left(1 - \zeta_1^m + \zeta_1^{m+1}g_1(\zeta_1)\right),$$

e, pela desigualdade triangular:

$$|h(\zeta)| \leq |b_0| \left(|1 - \zeta_1^m| + \left| \zeta_1^{m+1} g_1(\zeta_1) \right| \right).$$

Como isto é verdadeiro para todo valor de ζ_1, tomando para ζ_1 um valor real positivo x e tal que $x^m < 1$, resulta:

$$|h(x)| \leq |b_0| \left(1 - x^m + x_1^{m+1} |g_1(x)| \right) = |b_0| \left(1 - x^m \left(1 + x |g_1(x)| \right) \right).$$

Podemos escolher x suficientemente pequeno, de modo que $x |g_1(x)| < 1$. Neste caso $x^m (1 + x |g_1(x)|) > 0$ donde $1 - x^m (1 + x |g_1(x)|) < 1$ e, portanto $|h(x)| < |b_0| = \alpha_0$, uma contradição. □