Parte 2

Polinômios sobre domínios e corpos

Pressupomos que o estudante tenha familiaridade com os anéis comutativos com unidade, em particular com domínios e corpos.

Alguns exemplos importantes são $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, $\mathbb{Z}_n$, onde n é um natural e $n \geq 2$, e, em particular, os corpos $\mathbb{Z}_p$, onde p é um natural primo.

Faremos o estudo dos anéis de polinômios com coeficientes em anéis comutativos com unidade, com ênfase nos domínios dos polinômios com coeficientes em domínios e corpos.

O objetivo principal é estudar a fatoração de polinômios em produto de potências de polinômios irredutíveis e chegar ao Teorema Fundamental da Álgebra.

O estudante deve estar familiarizado com os conceitos de anéis comutativos com unidade e de divisibilidade em domínios, tendo visto o Teorema Fundamental da Aritmética.

Relembraremos os conceitos de ideais, ideais principais, ideais primos e domínios principais, onde vale a fatoração única. Mostraremos que vale a divisão euclidiana no domínio $A[x]$, onde A é um domínio, quando a divisão é feita por polinômios com coeficiente líder invertível em A. Como conseqüência obteremos que $K[x]$ é um domínio principal. Vamos estudar os polinômios irredutíveis em $K[x]$, processo que depende do corpo K.

Vamos relacionar a existência de raízes complexas para polinômios $f(x)$ de coeficientes reais com a sua divisibilidade por polinômios quadráticos da forma $x^2 + bx + c$, com $b^2 - 4c < 0$, ou da forma $x - \beta$, com $\beta \in \mathbb{R}$. Com isso, obteremos o Teorema Fundamental da Álgebra, que dá a fatoração de

$f(x) \in \mathbb{R}[x]$ num produto de potências de fatores como descritos acima.

Estudaremos alguns critérios de irredutibilidade de polinômios em $\mathbb{Q}[x]$ e em $\mathbb{Z}[x]$.

Finalizaremos resolvendo por meio de radicais equações do segundo, terceiro e quarto graus, isto é, determinando as suas raízes por meio de radicais de funções algébricas racionais dos seus coeficientes.

O anel de polinômios

Nesta seção definiremos o anel dos polinômios com coeficientes em um anel comutativo com unidade. Veremos que as propriedades das operações dos polinômios estão relacionadas diretamente com as propriedades da adição e multiplicação do anel, e aprenderemos a efetuá-las na prática.

Vocês estão familiarizados com expressões do tipo $ax^2 + bx + c$ e $ax + b$, sendo a, b e c números reais fixados e $a \neq 0$, sob o ponto de vista geométrico. Estas expressões são *polinômios com coeficientes reais* e vão ser estudadas agora sob o ponto de vista algébrico, isto é, essas expressões serão manipuladas, usando operações de adição e multiplicação.

Seja A um anel comutativo com unidade 1_A. Seja x um símbolo não pertencente ao anel A, chamado uma *indeterminada ou variável sobre* A.

Para cada número natural $j \geq 1$, designamos a j-ésima potência de x por x^j e escrevemos $x^1 = x$.

Definição 1
Um *polinômio com coeficientes em* A é uma expressão do tipo

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n = \sum_{j=0}^{n} a_jx^j,$$

onde n é um número natural e $a_j \in A$, para $0 \leq j \leq n$.

O símbolo $\sum$ lê-se como somatório ou soma e convencionamos escrever $a_0x^0 = a_0$.

Para $0 \leq j \leq n$, os elementos a_j são chamados de *coeficientes*, as parcelas a_jx^j de *termos* e os termos a_jx^j tais que $a_j \neq 0$ de *monômios de grau* j do polinômio $f(x)$. O coeficiente a_0 é chamado de *termo constante*.

Convencionamos:

(a) Para cada número natural n, chamar $0(x) = 0+0x+\cdots+0x^n$ de *polinômio identicamente nulo* e escrever $0(x) = 0$.
(b) Chamar $f(x) = a_0$ de *polinômio constante*.
(c) Escrever o polinômio $f(x)$ com as j-ésimas potências de x em ordem crescente ou em ordem decrescente, a saber, $f(x) = a_0+a_1x+a_2x^2+\cdots+a_nx^n$ ou $f(x) = a_nx^n + \cdots + a_2x^2 + a_1x + a_0$.
(d) Não escrever o termo a_jx^j sempre que $a_j = 0$, quando houver algum termo não-nulo no polinômio.

Exemplo 1

(a) Dados os números reais $a_0 = \frac{3}{2}$, $a_1 = -1$, $a_2 = \sqrt{2}$ e $a_3 = 1$, temos $f(x) = \frac{3}{2} - x + \sqrt{2}x^2 + x^3 \in \mathbb{R}[x]$.

(b) Dados os números reais $a_0 = 2$, $a_1 = -\sqrt{5}$, $a_2 = 0$, $a_3 = -\pi$, $a_4 = 0$ e $a_5 = -2{,}4$, temos $g(x) = 2 - \sqrt{5}x - \pi x^3 - 2{,}4\,x^5 \in \mathbb{R}[x]$.

(c) Dados os números reais $a_0 = 0$, $a_1 = -1$, $a_2 = 3$, $a_3 = 0$ e $a_4 = -3$, temos $h(x) = -x + 3x^2 - 3x^4 \in \mathbb{R}[x]$.

(d) Dados os números reais $a_0 = 5$, $a_1 = -1$ e $a_2 = 3$, temos $r(x) = 5 - x + 3x^2 \in \mathbb{R}[x]$.

(e) Dados os números reais $a_0 = 2$, $a_1 = -1$, $a_2 = 3$, $a_3 = 0$ e $a_4 = -3$, temos $s(x) = 2 - x + 3x^2 - 3x^4 \in \mathbb{R}[x]$.

(f) Dados os números reais $a_0 = 2$, $a_1 = -1$, $a_2 = 3$, $a_3 = 0$, $a_4 = -3$ e $a_5 = a_6 = 0$, temos $t(x) = 2 - x + 3x^2 - 3x^4 \in \mathbb{R}[x]$.

(g) As expressões $u(x) = x^{-2} + 3\sqrt{x} + x^5$ e $v(x) = 6\sqrt{x^3} - 4x^2 + 5$ **não são polinômios** porque nem todos os expoentes da indeterminada x são números naturais.

O polinômio $f(x) = a_0 + a_1x + \cdots + a_nx^n \in A[x]$ pode também ser escrito como $f(x) = a_0 + a_1x + \cdots + a_nx^n + 0x^{n+1} + 0x^{n+2} + \cdots + 0x^{n+m}$, para todo número natural $m \geq 1$. Portanto, quando comparamos dois polinômios $f(x), g(x) \in A[x]$, é possível assumir que os termos de ambos têm as mesmas potências de x.

Definição 2 (Igualdade de polinômios)

Os polinômios $f(x) = a_0 + a_1x^1 + a_2x^2 + \cdots + a_nx^n \in A[x]$ e $g(x) = b_0 + b_1x^1 + b_2x^2 + \cdots + b_nx^n \in A[x]$ *são iguais* se, e somente se, $a_j = b_j$ para todo j, tal que $0 \leq j \leq n$. Escrevemos $f(x) = g(x)$.

Isto é, $f(x)$ e $g(x)$ são iguais apenas quando todos os coeficientes das correspondentes potências de x em $f(x)$ e $g(x)$ são iguais.

Observe que, se $f(x)$ e $g(x)$ *não são iguais*, então existe algum número natural j, com $0 \leq j \leq n$ e $a_j \neq b_j$. Nesse caso, dizemos que $f(x)$ e $g(x)$ *são diferentes* e escrevemos $f(x) \neq g(x)$.

No Exemplo 1, os coeficientes dos termos constantes dos polinômios $h(x) = -x + 3x^2 - 3x^4$ e $t(x) = 2 - x + 3x^2 - 3x^4$ são diferentes; logo $h(x) \neq t(x)$. Enquanto $s(x) = t(x)$, pois todos os coeficientes das mesmas potências de x em $s(x)$ e $t(x)$ são iguais.

Exemplo 2

Os polinômios $f(x) = x^4 - x^5 + 4x^2 + 3 - 2x$ e $g(x) = 3 + 4x^2 - 2x - x^5 + x^4$ são iguais, porque os seus coeficientes a_j da j-ésima potência x^j são: $a_0 = 3$, $a_1 = -2$, $a_2 = 4$, $a_3 = 0$, $a_4 = 1$ e $a_5 = -1$.

Escrevendo os polinômios com as potências de x em ordem crescente, visualizamos imediatamente a igualdade dos polinômios. Temos

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

Em todo polinômio não identicamente nulo, $f(x) \not\equiv 0$, algum coeficiente deve ser diferente de zero, então há um maior número natural n, tal que $a_n \neq 0$. Definimos o *grau* de $f(x)$ por $\text{grau}(f(x)) = n$ e, nesse caso, a_n é chamado de *coeficiente líder* de $f(x)$.

O símbolo $\not\equiv$ lê-se como não é idêntico.

O símbolo grau(f(x)) lê-se como grau de f de x.

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

Importante: Não definimos o grau do polinômio identicamente nulo, $0(x) \equiv 0$.

Exemplo 3

O polinômio constante $w(x) = 5$ não é identicamente nulo e $\text{grau}(w(x)) = 0$. Volte ao Exemplo 1 e observe que $\text{grau}(f(x)) = 3$, $\text{grau}(g(x)) = 5$, $\text{grau}(h(x)) = 4$, $\text{grau}(r(x)) = 2$, $\text{grau}(s(x)) = 4$, $\text{grau}(t(x)) = 4$ e que $f(x)$ é o único polinômio mônico.

Note que:

$$\boxed{\text{grau}(f(x)) = 0 \text{ se, e somente se, } f(x) = a \neq 0,\ a \in A.}$$

Denotamos o conjunto de todos os polinômios na variável x com coeficientes no anel comutativo com unidade 1_A por $A[x]$.

$$\boxed{A[x] = \{\, f(x) = a_0 + a_1 x + \cdots + a_n x^n \mid n \in \mathbb{N},\ a_j \in A,\ 0 \leq j \leq n \,\}.}$$

No conjunto $A[x]$ estão definidas as operações de adição e multiplicação de polinômios.

Definição 3 (Adição de polinômios)

Definimos a *adição* dos polinômios $f(x) = \sum_{j=0}^{n} a_j x^j$ e $g(x) = \sum_{j=0}^{n} b_j x^j$ de $A[x]$ por

$$\boxed{f(x) + g(x) = \sum_{j=0}^{n} c_j x^j, \text{ onde } c_j = a_j + b_j, \text{ para } 0 \leq j \leq n.}$$

O resultado da adição de dois polinômios é chamado de *soma*.

Exemplo 4

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

$$\begin{aligned} f(x) + g(x) &= (4+0)x^3 + (-3+2)x^2 + (4+(-5))x + (5+(-2)) \\ &= 4x^3 - x^2 - x + 3 \in \mathbb{Z}[x], \\ f(x) + h(x) &= (4-4)x^3 + (-3+5)x^2 + (4-3)x + (5+1) \\ &= 0x^3 + 2x^2 + x + 6 \\ &= 2x^2 + x + 6 \in \mathbb{Z}[x]. \end{aligned}$$

Lembre que $a - b = a + (-b)$, para quaisquer a e b no anel A.

No exemplo anterior, observamos que

$\text{grau}(f(x)) = \text{grau}(h(x)) = 3$ e $\text{grau}(f(x)+h(x)) = 2$, enquanto $\text{grau}(g(x)) = 2$ e $\text{grau}(f(x) + g(x)) = 3 =$ máximo$\{\,\text{grau}(f(x)),\, \text{grau}(g(x))\,\}$.

Na adição de polinômios vale a seguinte propriedade do grau.

Propriedade do grau: (Adição de polinômios)

Sejam $f(x) = \sum_{j=0}^{n} a_j x^j$, com $a_n \neq 0$, e $g(x) = \sum_{j=0}^{m} b_j x^j$, com $b_m \neq 0$.

Se $f(x) + g(x) \neq 0$, então

$$\boxed{\text{grau}(f(x) + g(x)) \leq \max\{\,\text{grau}(f(x)), \text{grau}(g(x))\,\} = \max\{\,n, m\,\}}$$

O símbolo max significa o maior ou o máximo dos números.

valendo a igualdade sempre que $\text{grau}(f(x)) = n \neq m = \text{grau}(g(x))$.

A adição de polinômios tem diversas propriedades, que são conseqüência das propriedades da adição no anel A, conforme veremos a seguir.

Propriedades da adição:

Sejam $f(x) = \sum_{j=0}^{n} a_j x^j$, $g(x) = \sum_{j=0}^{n} b_j x^j$ e $h(x) = \sum_{j=0}^{n} c_j x^j$ em $A[x]$.

(A1) Associativa: $(f(x) + g(x)) + h(x) = f(x) + (g(x) + h(x))$,

pois para quaisquer $a_j, b_j, c_j \in A$ e $0 \leq j \leq n$, temos que

$$(a_j + b_j) + c_j = a_j + (b_j + c_j).$$

Lembre que a adição no anel A é associativa (A1) e comutativa (A2).

(A2) Comutativa: $f(x) + g(x) = g(x) + f(x)$,

pois para quaisquer $a_j, b_j \in A$ e $0 \leq j \leq n$, temos $a_j + b_j = b_j + a_j$.

(A3) Existência de elemento neutro:

Como o polinômio identicamente nulo $0 = \sum_{j=0}^{n} 0x^j$, então $f(x) = 0 + f(x)$,

Lembre que no anel A 0 é o elemento neutro aditivo.

pois para qualquer $a_j \in A$, $0 \leq j \leq n$, temos $a_j = 0 + a_j$.

(A4) Existência de simétrico:

Dado $f(x) = \sum_{j=0}^{n} a_j x^j$, o polinômio $-f(x) = \sum_{j=0}^{n} (-a_j)x^j$ é o *simétrico* de $f(x)$, sendo

$$f(x) + (-f(x)) = \sum_{j=0}^{n} 0x^j,$$

pois $a_j + (-a_j) = 0$ para qualquer $a_j \in A$, $0 \leq j \leq n$.

Lembre que no anel A $-a$ é o simétrico de a.

Exemplo 5

Consideremos os polinômios $f(x) = 4x^3 - 3x^2 + 4x + 5$, $g(x) = 2x^2 - 5x - 2$ e $h(x) = -4x^3 + 5x^2 - 3x + 1$ em $\mathbb{Z}[x]$ do Exemplo 4.

(a) No Exemplo 4 determinamos $f(x) + g(x) = 4x^3 - x^2 - x + 3$.

Assim, $(f(x) + g(x)) + h(x) = (4x^3 - x^2 - x + 3) + (-4x^3 + 5x^2 - 3x + 1)$

$= (4-4)x^3 + (-1+5)x^2 + (-1-3)x + (3+1) = 0x^3 + 4x^2 - 4x + 4 = 4x^2 - 4x + 4$.

(b) A adição de polinômios pode ser feita facilmente se escrevemos os polinômios numa tabela, onde nas primeiras linhas estão cada um dos polinômios com as potências x^j em ordem decrescente, e na última linha o resultado da adição, de maneira similar à adição de números reais. Calcularemos $g(x) + h(x)$ desse modo.

$$\begin{array}{rrrrrrrrr} & & & & 2x^2 & - & 5x & - & 2 \\ (+) & - & 4x^3 & + & 5x^2 & - & 3x & + & 1 \\ \hline & - & 4x^3 & + & 7x^2 & - & 8x & - & 1 \end{array}$$

Nesse caso, $g(x) + h(x) = -4x^3 + 7x^2 - 8x - 1$.

(c) Podemos usar este processo para calcular a soma de m polinômios, construindo uma tabela com $m + 1$ linhas e tantas colunas quantas forem necessárias. Por exemplo, para calcular $f(x) + g(x) + h(x)$ a tabela terá quatro linhas

$$\begin{array}{rrrrrrrrr} & & 4x^3 & - & 3x^2 & + & 4x & + & 5 \\ & & & & 2x^2 & - & 5x & - & 2 \\ (+) & - & 4x^3 & + & 5x^2 & - & 3x & + & 1 \\ \hline & & 0x^3 & + & 4x^2 & - & 4x & + & 4 \end{array}$$

Logo, $f(x) + g(x) + h(x) = 4x^2 - 4x + 4$.

Definição 4 (Multiplicação de polinômios)

Definimos a *multiplicação* dos polinômios $f(x) = \sum_{j=0}^{n} a_j x^j$ e $g(x) = \sum_{j=0}^{m} b_j x^j$ em $A[x]$ por

O resultado da multiplicação de dois polinômios é chamado de *produto*.

$$\boxed{f(x)\cdot g(x)=\sum_{j=0}^{n+m} c_j x^j}$$

sendo

$$\begin{aligned}
c_0 &= a_0\cdot b_0\\
c_1 &= a_0\cdot b_1 + a_1\cdot b_0\\
c_2 &= a_0\cdot b_2 + a_1\cdot b_1 + a_2\cdot b_0\\
&\vdots\\
c_j &= a_0\cdot b_j + a_1\cdot b_{j-1} + \cdots + a_j\cdot b_0 = \sum_{\lambda+\mu=j} a_\lambda\cdot b_\mu\\
&\vdots\\
c_{n+m} &= a_n\cdot b_m\,.
\end{aligned}$$

Propriedade do grau: (Multiplicação de polinômios)

Sejam A um domínio e $f(x)=\sum_{j=0}^{n} a_j x^j$, com $a_n\neq 0$, e $g(x)=\sum_{j=0}^{m} b_j x^j$, com $b_m\neq 0$. Então,

$$\boxed{\text{grau}(f(x)\cdot g(x))=n+m}$$

pois o coeficiente líder de $f(x)\cdot g(x)$ é $c_{n+m}=a_n\cdot b_m\neq 0$.

Lembre que em um domínio $a\cdot b=0\Longleftrightarrow a=0$ ou $b=0$.

A multiplicação de polinômios tem as seguintes propriedades.

Propriedades da multiplicação:

Sejam $f(x)=\sum_{j=0}^{n} a_j x^j$, $g(x)=\sum_{j=0}^{m} b_j x^j$ e $h(x)=\sum_{j=0}^{r} c_j x^j$ elementos de $A[x]$.

(M1) Associativa: $(f(x)\cdot g(x))\cdot h(x)=f(x)\cdot(g(x)\cdot h(x))$.

(M2) Comutativa: $f(x)\cdot g(x)=g(x)\cdot f(x)$,

Lembre que no anel A a multiplicação é associativa e comutativa.

pois para todo j com $0\leq j\leq n+m$, vale a identidade

$$\sum_{\lambda+\mu=j} a_\mu b_\lambda=\sum_{\lambda+\mu=j} b_\lambda a_\mu\,.$$

Note que, em vista da definição das operações:

- Para quaisquer $j,k\in\mathbb{N}$, vale a identidade: $x^j\cdot x^k=x^{j+k}$.
- Se $f(x)=a$ e $g(x)=b_0+b_1x+\cdots+b_mx^m$, então

$$\begin{aligned}
f(x)\cdot g(x) &= a\cdot g(x)=a\cdot\left(\sum_{k=0}^{m} b_k x^k\right)=\sum_{k=0}^{m}(a\cdot b_k)x^k\\
&= (a\cdot b_0)+(a\cdot b_1)x+\cdots+(a\cdot b_m)x^m\,,
\end{aligned}$$

pois, nesse caso, $a_0 = a$, $n = 0$, e $c_j = a_0 \cdot b_j = a \cdot b_j$, para todo $j \in \mathbb{N}$.

Em particular, $A[x]$ tem a propriedade M3:

(M3) Existência de elemento neutro multiplicativo :

$1_A \cdot f(x) = f(x)$, para qualquer $f(x) \in A[x]$ e $1_{A[x]} = 1_A$.

Chamamos o elemento neutro multiplicativo de *unidade*.

- Se $f(x) = ax^j$ com $j \geq 1$, e $g(x) = b_0 + b_1x + \cdots + b_mx^m$, então

$$\begin{aligned} f(x) \cdot g(x) &= (ax^j) \cdot g(x) = (ax^j) \cdot \left(\sum_{k=0}^{m} b_k x^k \right) = \sum_{k=0}^{m} (a \cdot b_k) x^{k+j} \\ &= (a \cdot b_0)x^j + (a \cdot b_1)x^{j+1} + \cdots + (a \cdot b_m)x^{j+m}, \end{aligned}$$

pois, nesse caso, temos $a_0 = 0, \ldots, a_{j-1} = 0$ $a_j = a$, $n = j$, $n+m = j+m$, $c_0 = 0, \ldots, c_{j-1} = 0$, $c_j = a_j \cdot b_0 = a \cdot b_0$, $c_{j+1} = a_j \cdot b_1 = a \cdot b_1$, ..., $c_{j+m} = a_j \cdot b_m = a \cdot b_m$.

Combinando as três observações anteriores com o fato da adição de polinômios corresponder a adicionar os coeficientes das potências de x de mesmo expoente em ambos os polinômios, obtemos mais uma propriedade, que envolve as duas operações.

Propriedade da adição e multiplicação:

Sejam $f(x) = \sum_{j=0}^{n} a_j x^j$, $g(x) = \sum_{j=0}^{n} b_j x^j$ e $h(x) = \sum_{j=0}^{m} c_j x^j$.

(AM) Distributiva: $(f(x) + g(x)) \cdot h(x) = f(x) \cdot h(x) + g(x) \cdot h(x)$.

Lembre que no anel A a adição e a multiplicação têm a propriedade distributiva:
$a(b + c) = ab + ac$.

Com as propriedades acima da adição e multiplicação de polinômios em $A[x]$, obtivemos a seguinte proposição.

Proposição 1
Seja A um anel comutativo com unidade 1_A. Então, $A[x]$ é um anel comutativo com unidade.

Proposição 2
Se A é um domínio, então $A[x]$ é um domínio. Em particular, se K é um corpo, então $K[x]$ é um domínio.

Demonstração: Suponhamos que A seja um domínio e sejam $f(x), g(x) \in A[x]$ não-nulos. Digamos que grau$(f(x)) = m$, com coeficiente líder $a_m \neq 0_A$, e grau$(g(x)) = n$, com coeficiente líder $b_n \neq 0_A$. Então, o coeficiente líder de $f(x) \cdot g(x)$ é $c_{m+n} = a_m \cdot b_n \neq 0_A$. Logo, grau$(f(x) \cdot g(x)) = m + n$ e $f(x) \cdot g(x) \neq 0$. ■

Exemplo 6

São anéis de polinômios muito importantes: $\mathbb{Z}[x], \mathbb{Q}[x], \mathbb{R}[x]$ e $\mathbb{C}[x]$. Assim como $\mathbb{Z}_n[x]$, $n \geq 2$, e em particular $\mathbb{Z}_p[x]$, onde p é primo.

Agora podemos fazer exemplos da multiplicação de polinômios.

Exemplo 7

Consideremos os polinômios $f(x) = 4x^3 - 3x^2 + 4x + 5$, $g(x) = 2x^2 - 5x - 2$ e $h(x) = -4x^3 - 3x + 1$ em $\mathbb{Z}[x]$.

(a) Vamos calcular $f(x) \cdot g(x)$.

Usando a propriedade distributiva da multiplicação de polinômios, temos

$$\begin{aligned} f(x) \cdot g(x) &= (4x^3 - 3x^2 + 4x + 5) \cdot (2x^2 - 5x - 2) \\ &\overset{(1)}{=} 4x^3 \cdot (2x^2 - 5x - 2) + (-3x^2) \cdot (2x^2 - 5x - 2) + 4x \cdot (2x^2 - 5x - 2) + 5 \cdot (2x^2 - 5x - 2) \\ &\overset{(2)}{=} (8x^5 - 20x^4 - 8x^3) + (-6x^4 + 15x^3 + 6x^2) + (8x^3 - 20x^2 - 8x) + (10x^2 - 25x - 10) \\ &\overset{(3)}{=} 8x^5 + (-20 - 6)x^4 + (-8 + 15 + 8)x^3 + (6 - 20 + 10)x^2 + (-8 - 25)x - 10 \\ &\overset{(4)}{=} 8x^5 - 26x^4 + 15x^3 - 4x^2 - 33x - 10 \in \mathbb{Z}[x]. \end{aligned}$$

Observe que as igualdades acima foram obtidas:
(1) distribuindo as parcelas de $f(x)$ na multiplicação por $g(x)$;
(2) distribuindo cada multiplicação com respeito às parcelas de $g(x)$;
(3) usando a definição da adição de polinômios;
(4) fazendo a adição dos coeficientes das potências de x de mesmo expoente.

(b) Vamos calcular $h(x) \cdot g(x)$.

Construiremos uma tabela, escrevendo $h(x)$ na primeira linha e $g(x)$ na segunda, com as potências de x em ordem decrescente. Fazemos a multiplicação usando a propriedade distributiva e calculando a multiplicação dos termos do polinômio $g(x)$ por $h(x)$, em ordem crescente das potências de x e organizando na tabela os resultados parciais em ordem decrescente das potências de x. A última linha da tabela será a adição das multiplicações parciais.

			$-$	$4x^3$	$+$	$0x^2$	$-$	$3x$	$+$	1	
				$(\times)$		$2x^2$	$-$	$5x$	$-$	2	
				$8x^3$	$+$	$0x^2$	$+$	$6x$	$-$	2	$-2 \cdot (-4x^3 - 3x + 1)$
		$20x^4$	$+$	$0x^3$	$+$	$15x^2$	$-$	$5x$			$-5x \cdot (-4x^3 - 3x + 1)$
$-8x^5$	$+$	$0x^4$	$-$	$6x^3$	$+$	$2x^2$					$2x^2 \cdot (-4x^3 - 3x + 1)$
$-8x^5$	$+$	$20x^4$	$+$	$2x^3$	$+$	$17x^2$	$+$	x	$-$	2	adição das 3 parcelas

Temos $\text{grau}(h(x) \cdot g(x)) = 5 = 3 + 2 = \text{grau}(h(x)) + \text{grau}(g(x))$.

Exemplo 8

Sejam $f(x) = \overline{2}x + \overline{1}$ e $g(x) = \overline{2}x + \overline{3}$ em $\mathbb{Z}_4[x]$. Então,

$f(x) \cdot g(x) = (\overline{2}x + \overline{1})(\overline{2}x + \overline{3}) = \overline{4}x^2 + \overline{6}x + \overline{2}x + \overline{3} = \overline{3} \in \mathbb{Z}_4[x]$.

Observe que $f(x)^2 = \overline{1}$.

Exercícios

1. Sejam $f(x) = 2x^3 - 5x^2 + 1$, $g(x) = x^5 - x^4 + x^3 - 2x - 3$, $h(x) = 2x^3 - 2x^2 - x + 2$, $r(x) = -2x^3 + 3x^2 + 5x - 3$ e $s(x) = -x^2 + x - 3$ em $\mathbb{Z}[x]$. Efetue a operação e dê o grau dos resultados não identicamente nulos:
   (a) $f(x) + g(x)$ (b) $x^2 \cdot f(x) - g(x) + x \cdot h(x)$
   (c) $g(x) + (3 - 2x^2) \cdot h(x)$ (d) $g(x) + h(x) + r(x) + s(x)$
   (e) $h(x) + r(x)$ (f) $h(x) \cdot s(x) + r(x) \cdot s(x)$
   (g) $(2x - 1) \cdot r(x) - (3x + 2) \cdot s(x)$ (h) $(x^2 - 1) \cdot (x^2 + 1) - (s(x))^2$

2. Determine em $\mathbb{Z}[x]$:
   (a) $(x^4 - 3x^2 + 5)(2x + 3) + (x^2 + 3x)(4x^3 - 6x)$.
   (b) $9x^2(2x^2 + 3) + 4x(3x^3 - 2)$.

3. Considere o anel $\mathbb{Q}[x]$. Determine:
   (a) $(x^2 + 2)(x^2 - 2)$ (b) $(x - 2)^3$ (c) $(x - 1)^2(x + 1)^2$
   (d) $(x + 3)(x + 1)(x - 4)$ (e) $(x + 2)^4$ (f) $\left(\frac{1}{2}x - 4\right)^2$
   (g) $\left(\frac{1}{3}x + 3\right)^3$

4. Determine os números reais a, b, c e d para que as identidades de polinômios sejam verdadeiras em $\mathbb{R}[x]$:
   (a) $(a + 5)x^3 + (1 - b)x^2 + (2c - 1)x + (d + 2) = 0$.
   (b) $3ax^7 - 2bx^5 + 3cx^4 + (d + 3) = x^5 - x^4 + 3$.
   (c) $ax^2 + bx + c = (ax - d)^2$.
   (d) $(b + d)x^4 + (d + a)x^3 + (a - c)x^2 + (c + b)x = 4x^4 + 2x^2$.

5. Determine números reais a, b, c e d tais que
   $$f(x) + 2g(x) - 3h(x) = -3x^4 + 5x^3 - 3x^2 + x + 2,$$
   sabendo que $f(x) = ax^3 + 2x^2 - x + d$, $g(x) = x^3 + bx^2 - 2x - 4$ e $h(x) = x^4 + 2x^3 + dx^2 + cx + c$ estão em $\mathbb{R}[x]$.

6. Dado o polinômio $g(x) \in \mathbb{R}[x]$, determine, em cada item, o polinômio $f(x) \in \mathbb{R}[x]$, tendo a condição indicada:

Se $f(x)$ é um polinômio em $A[x]$, onde A é um anel comutativo com unidade e $n \geq 1$ é um número natural, então
$(f(x))^n = \underbrace{f(x) \cdot f(x) \cdots f(x)}_{n \text{ fatores}}$

Convencionamos não escrever o sinal da operação de multiplicação de polinômios. Assim,
$f(x)g(x) = f(x) \cdot g(x)$.

Lembre da fórmula do binômio de Newton em $\mathbb{Q}$
$(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$

(a) $f(x) + g(x) = 0$, $g(x) = x^2 - x + 3$.

(b) $2f(x)+3g(x) = 4x^5+x^3+x^2-x+1$, $g(x) = 2x^4-x^3-x^2+3x+5$.

(c) $3f(x)-2g(x)+5x-3 = 6x^3+5x^2-3x-2$, $g(x) = 5ax^3-bx^2+2x+c$.

7. Discuta, para $a \in \mathbb{R}$, o grau do polinômio $f(x) \in \mathbb{R}[x]$:

   (a) $f(x) = (a^2-1)^2x^3 + (a^2-3a+2)x + a + 3$

   (b) $f(x) = ax^2 + 2ax + 9$

   (c) $f(x) = (a^3-a)x^3 + a(a-1)x^2 + a^3 - 1$

8. Sejam $f(x) = \overline{3}x + \overline{1}$, $g(x) = \overline{2}x + \overline{5} \in \mathbb{Z}_6[x]$.

   (a) Determine $f(x) \cdot g(x)$.

   (b) Compare grau$(f(x) \cdot g(x))$ com grau$(f(x))$ + grau$(g(x))$.

9. Dê exemplo de um polinômio de grau 1 em $\mathbb{Z}_4[x]$ que tenha inverso em $\mathbb{Z}_4[x]$.

10. Dados os polinômios $f(x) = \overline{2}x^2 + \overline{3}x - \overline{1}$, $g(x) = x^3 + \overline{2}x^2 + \overline{4} \in \mathbb{Z}_5[x]$, determine:

    (a) $-f(x) + \overline{2}g(x)$.

    (b) $\overline{3}f(x)^2 \cdot g(x)$.

$a \in A$ é invertível se, e somente se, existe $b \in A$ tal que $a \cdot b = b \cdot a = 1_A$. Mais ainda, $A^* = \{a \in A$ tal que a é invertível $\}$.

11. Seja A um anel comutativo com unidade 1_A. Mostre que:

    (a) A é um subanel de $A[x]$.

    (b) $A[x]^* = A^*$, se A é um domínio.

    (c) Se A é um corpo, então $A[x]^* = A\backslash\{0\}$.

    (d) Dê exemplo de um anel A comutativo com unidade tal que $A^* \subsetneq A[x]^*$.

Polinômios sobre domínios

Vamos olhar com mais atenção para polinômios com coeficientes em domínios.

Sabemos que se A é um domínio, então $A[x]$ é um domínio, $A^* = A[x]^*$ e a função grau tem a propriedade de

$$\text{grau}(f(x)g(x)) = \text{grau}(f(x)) + \text{grau}(g(x)),$$

para quaisquer $f(x), g(x)$ em $A[x]$ não-nulos.

Como conseqüência da propriedade acima temos:

Corolário 1
Seja A um domínio. Se $f(x), g(x) \in A[x]\backslash\{0\}$ e $g(x)$ divide $f(x)$, então $\text{grau}(g(x)) \leq \text{grau}(f(x))$.

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

$$\text{grau}(f(x)) = \text{grau}(g(x)h(x)) = \text{grau}(g(x)) + \text{grau}(h(x)) \geq \text{grau}(g(x)),$$

mostrando o resultado. ■

Quando A é um domínio, podemos fazer a divisão por polinômio em $A[x]$ cujo coeficiente líder é invertível em A e com resto controlado, chamada *divisão euclidiana*.

Teorema 1 (Divisão euclidiana)
Seja A um domínio. Sejam $f(x), g(x) \in A[x]$, com $g(x) \neq 0$ e coeficiente líder invertível em A. Então, existem $q(x)$ e $r(x)$ em $A[x]$, unicamente determinados, tais que

$$f(x) = q(x)g(x) + r(x),$$

onde $r(x) = 0$ ou $\text{grau}(r(x)) < \text{grau}(g(x))$.

Demonstração: Seja $g(x) = b_0 + b_1x + \cdots + b_mx^m$, $b_m \in A^*$, $m = \text{grau}(g(x))$. Primeiramente, vamos mostrar a existência.

(Existência) Se $f(x) = 0$, então tome $q(x) = r(x) = 0$. Suponhamos que $f(x) \neq 0$. Seja $n = \text{grau}(f(x))$ e escreva $f(x) = a_0 + a_1x + \cdots + a_nx^n$, com $a_n \neq 0$.

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

Podemos supor $n \geq m$. A demonstração é por indução sobre $n = \text{grau}(f(x))$.

Se $n = 0$, então $0 = n \geq m = \text{grau}(g(x))$, logo $m = 0$, $f(x) = a_0 \neq 0$, $g(x) = b_0 \in A^*$. Assim, $f(x) = a_0 b_0^{-1} g(x)$, com $q(x) = a_0 b_0^{-1}$ e $r(x) = 0$.

Suponhamos o resultado válido para polinômios com grau menor do que $n = \text{grau}(f(x))$. Vamos mostrar que vale para $f(x)$.

O polinômio $a_n\, b_m^{-1}\, x^{n-m}\, g(x)$ tem grau n e coeficiente líder a_n.

Seja $f_1(x)$ o polinômio definido por $f_1(x) = f(x) - a_n b_m^{-1} x^{n-m} g(x)$.

Observe que $\text{grau}(f_1(x)) < \text{grau}(f(x))$. Por hipótese de indução, existem $q_1(x)$ e $r_1(x)$ em $A[x]$ tais que

$$f_1(x) = q_1(x)g(x) + r_1(x),$$

com $r_1(x) = 0$ ou $\text{grau}(r_1(x)) < \text{grau}(g(x))$. Logo,

Em (1) substituímos a expressão de $f_1(x)$ e em (2) usamos a comutatividade da adição (A2) e a distributividade (AM) em $A[x]$.

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

Tomamos $q(x) = q_1(x) + a_n b_m^{-1} x^{m-n}$ e $r(x) = r_1(x)$.

(Unicidade) Sejam $q_1(x), r_1(x), q_2(x), r_2(x)$ tais que

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

$$(\star\star) \quad \begin{cases} r_1(x) = 0 \text{ ou } \text{grau}(r_1(x)) < \text{grau}(g(x)) \text{ e} \\ r_2(x) = 0 \text{ ou } \text{grau}(r_2(x)) < \text{grau}(g(x)). \end{cases}$$

De $(\star)$ segue que $(q_1(x) - q_2(x))g(x) = r_2(x) - r_1(x)$.

Se $q_1(x) \neq q_2(x)$, então $q_1(x) - q_2(x) \neq 0$, logo $r_2(x) - r_1(x) \neq 0$ e, do Corolário 1, obtemos

$$\text{grau}(\underbrace{g(x)}_{\text{divisor}}) \leq \text{grau}(r_2(x) - r_1(x)) \overset{(\star\star)}{<} \text{grau}(g(x)),$$

uma contradição.

Portanto, $q_1(x) = q_2(x)$, logo $r_1(x) = r_2(x)$. ■

Definição 5 (Quociente e resto)
Sejam $f(x), g(x), q(x)$ e $r(x)$ como no Teorema anterior. Chamamos $f(x)$ de *dividendo*, $g(x)$ de *divisor*, $q(x)$ de *quociente* e $r(x)$ de *resto*.

Você deve ter observado que a determinação do monômio de maior grau do quociente só depende dos monômios de maior grau do dividendo e do divisor. Na divisão de polinômios devemos prestar atenção aos graus do dividendo, do divisor e do resto. Agora vamos armar a divisão.

Vejamos como determinar o quociente $q(x)$ e o resto $r(x)$ da divisão euclidiana do polinômio $f(x)$ por $g(x) \neq 0$. Elaboramos uma tabela, ilustrando os cálculos passo a passo. Na tabela armamos a divisão para calcular o quociente e o resto, resultados da divisão euclidiana. Os seguintes exemplos consistem de *armar e efetuar*, conforme o modelo.

$$\begin{array}{r|l} f(x) & g(x) \\ \hline \vdots & q(x) \\ \hline r(x) & \end{array}$$

Exemplo 9

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

(1) Temos $\text{grau}(f(x)) = 1 < 2 = \text{grau}(g(x))$. Nada a fazer.

(2) O quociente é $q(x) = 0$ e o resto é $r(x) = f(x) = 4x + 3$.

$$\begin{array}{rcr|l} 4x & + & 3 & x^2 + 3x + 1 \\ \hline & - & 0 & 0 \\ \hline 4x & + & 3 & \end{array}$$

$\mathbb{Z}^\star = \{-1, 1\}$.

Exemplo 10

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

(1) O monômio de maior grau de $f(x)$ é $2x^2$ e o monômio de maior grau de $g(x)$ é x^2. O quociente da divisão de $2x^2$ por x^2 é $q_1(x) = 2$.

(2) Fazemos o cálculo:

$r_1(x) = f(x) - q_1(x)g(x) = (2x^2 + 4x + 3) - 2x^2 - 6x - 2 = -2x + 1$.

$$\begin{array}{rcrcr|l} 2x^2 & + & 4x & + & 3 & x^2 + 3x + 1 \\ \hline - \ 2x^2 & - & 6x & - & 2 & 2 \\ \hline & - & 2x & + & 1 & \end{array}$$

Sempre que $n = r + m$, com $n, m, r \in \mathbb{N}$, temos $n \geq m$, $x^n = x^r \cdot x^m$ é equivalente a x^m divide x^n.

(3) Como $1 = \text{grau}(r_1(x)) < \text{grau}(g(x)) = 2$, não podemos continuar a divisão, paramos os cálculos.

(4) Obtemos $q(x) = q_1(x) = 2$ e $r(x) = r_1(x) = -2x + 1$.

Exemplo 11

Faça a divisão euclidiana de $f(x) = 3x^4+5x^3+x^2+2x-3$ por $g(x) = x^2+3x+1$ em $\mathbb{Z}[x]$.

(1) O monômio de maior grau de $f(x)$ é $3x^4$ e o monômio de maior grau de $g(x)$ é x^2. O quociente da divisão de $3x^4$ por x^2 é $q_1(x) = 3x^2$.

(2) Fazemos o cálculo:

$r_1(x) = f(x) - q_1(x)g(x) = (3x^4 + 5x^3 + x^2 + 2x - 3) - 3x^4 - 9x^3 - 3x^2 = -4x^3 - 2x^2 + 2x - 3$.

$$\begin{array}{rcrcrcrcr|l}
 & 3x^4 & + & 5x^3 & + & x^2 & + & 2x & - & 3 & x^2 + 3x + 1 \\
\cline{10-10}
- & 3x^4 & - & 9x^3 & - & 3x^2 & & & & & 3x^2 \\
\cline{1-8}
 & & - & 4x^3 & - & 2x^2 & + & 2x & - & 3 &
\end{array}$$

(3) Como $3 = \text{grau}(r_1(x)) > \text{grau}(g(x)) = 2$ devemos continuar, dividindo $r_1(x)$ por $g(x)$, pois $r_1(x)$ não é o resto da divisão euclidiana.

(4) O monômio de maior grau de $r_1(x)$ é $-4x^3$ e o monômio de maior grau de $g(x)$ é x^2. O quociente da divisão de $-4x^3$ por x^2 é $q_2(x) = -4x$.

(5) Fazemos o cálculo:

$r_2(x) = r_1(x) - q_2(x)g(x) = (-4x^3 - 2x^2 + 2x - 3) + 4x^3 + 12x^2 + 4x = 10x^2 + 6x - 3$.

$$\begin{array}{rcrcrcrcr|l}
 & 3x^4 & + & 5x^3 & + & x^2 & + & 2x & - & 3 & x^2 + 3x + 1 \\
\cline{10-10}
- & 3x^4 & - & 9x^3 & - & 3x^2 & & & & & 3x^2 - 4x \\
\cline{1-8}
 & & - & 4x^3 & - & 2x^2 & + & 2x & - & 3 & \\
 & & & 4x^3 & + & 12x^2 & + & 4x & & & \\
\cline{3-8}
 & & & & & 10x^2 & + & 6x & - & 3 &
\end{array}$$

(6) Como $2 = \text{grau}(r_2(x)) = \text{grau}(g(x)) = 2$, podemos continuar, calculando a divisão de $r_2(x)$ por $g(x)$, pois $r_2(x)$ não é o resto da divisão euclidiana.

(7) O monômio de maior grau de $r_2(x)$ é $10x^2$ e o monômio de maior grau de $g(x)$ é x^2. O quociente da divisão de $10x^2$ por x^2 é $q_3(x) = 10$.

(8) Fazemos o cálculo:

$r_3(x) = r_2(x) - q_3(x)g(x) = (10x^2 + 6x - 3) - 10x^2 - 30x - 10 = -24x - 13$.

$$\begin{array}{rcrcrcrcr|l}
 & 3x^4 & + & 5x^3 & + & x^2 & + & 2x & - & 3 & x^2 + 3x + 1 \\
\cline{10-10}
- & 3x^4 & - & 9x^3 & - & 3x^2 & & & & & 3x^2 - 4x + 10 \\
\cline{1-8}
 & & - & 4x^3 & - & 2x^2 & + & 2x & - & 3 & \\
 & & & 4x^3 & + & 12x^2 & + & 4x & & & \\
\cline{3-8}
 & & & & & 10x^2 & + & 6x & - & 3 & \\
 & & & & - & 10x^2 & - & 30x & - & 10 & \\
\cline{5-8}
 & & & & & & - & 24x & - & 13 &
\end{array}$$

(9) Como $1 = \text{grau}(r_3(x)) < \text{grau}(g(x)) = 2$, terminamos o algoritmo, pois $r_3(x)$ é o resto da divisão euclidiana.

(10) Obtemos
$q(x) = 3x^2 - 4x + 10 = q_1(x) + q_2(x) + q_3(x)$ e $r(x) = r_3(x) = -24x - 13$.

Exemplo 12
Vamos fazer a divisão euclidiana em $\mathbb{Z}_3[x]$ de $x^3 + x^2 + \overline{2}$ por $x^2 + \overline{2}x + \overline{1}$.

$$\begin{array}{rcrcrcr|l} x^3 & + & x^2 & + & \overline{0}x & + & \overline{2} & x^2 + \overline{2}x + \overline{1} \\ \cline{8-8} \overline{2}x^3 & + & x^2 & + & \overline{2}x & & & x + \overline{2} \\ \cline{1-5} & & \overline{2}x^2 & + & \overline{2}x & + & \overline{2} & \\ & & x^2 & + & \overline{2}x & + & \overline{1} & \\ \cline{3-7} & & & & x & & & \end{array}$$

$\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$.
Temos $-\overline{1} = \overline{2}$ e $-\overline{2} = \overline{1}$.

Logo, o quociente é $x + \overline{2}$ e o resto é x.

Observação: Sejam A um anel comutativo com unidade e $\beta \in A$. A avaliação de $f(x) = a_0 + a_1x + \cdots + a_nx^n \in A[x]$ em β é definida por

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

Definição 6 (Raiz)
Sejam A um anel comutativo com unidade e $\beta \in A$. Dizemos que β é uma raiz de $f(x)$ se, e somente se, $f(\beta) = 0$.

Exemplo 13
$\overline{2} \in \mathbb{Z}_6$ é uma raiz de $f(x) = x^2 + x \in \mathbb{Z}_6[x]$, pois $f(\overline{2}) = (\overline{2})^2 + \overline{2} = \overline{0}$.
Verifique que os elementos de $\mathbb{Z}_6$ $\overline{5}$, $\overline{3}$ e $\overline{0}$ também são raízes de $f(x)$.

Proposição 3
Seja A um domínio e seja $f(x) \in A[x]\backslash\{0\}$. Então, $\beta \in A$ é uma raiz de $f(x)$ se, e somente se, $x - \beta$ divide $f(x)$.

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

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

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

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

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

Reciprocamente, suponhamos que $x - \beta$ divida $f(x)$. Então, existe $q(x) \in A[x]$ tal que $f(x) = q(x)(x - \beta)$. Logo, $f(\beta) = q(\beta)(\beta - \beta) = q(\beta) \cdot 0 = 0$. ■

Proposição 4

Seja A um domínio e seja $f(x) \in A[x]\backslash\{0\}$. Se $f(x)$ tem grau n, então $f(x)$ tem no máximo n raízes em A.

No Exemplo 13, o polinômio de grau 2 tinha 4 raízes no anel dos coeficientes. Nesse caso, $\mathbb{Z}_6$ não é um domínio.

Demonstração: A demonstração é por indução sobre $n = \text{grau}(f(x))$.

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

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

Se $f(x)$ não tem raízes em A, nada há a demonstrar. Digamos que $f(x)$ tenha uma raiz $\beta \in A$. Pela Proposição anterior, $x - \beta$ divide $f(x)$ em $A[x]$, logo existe $q(x) \in A[x]$ tal que $f(x) = q(x)(x-\beta)$, com $\text{grau}(q(x)) = n$. Por hipótese de indução, $q(x)$ tem no máximo n raízes em A. Observe que

$$\begin{aligned} \alpha \in A \text{ é raiz de } f(x) &\iff 0 = f(\alpha) = q(\alpha)(\alpha - \beta) \\ &\overset{A \text{ domínio}}{\iff} q(\alpha) = 0 \text{ ou } \alpha - \beta = 0 \\ &\iff \alpha \text{ é raiz de } q(x) \text{ ou } \alpha = \beta. \end{aligned}$$

Logo, $f(x)$ tem no máximo $n + 1$ raízes em A. ■

Corolário 2

Se $f(x) \in K[x]$, $n = \text{grau}(f(x)) \geq 1$ e K é um corpo, então $f(x)$ tem no máximo n raízes em K.

Definição 7 (Corpo algebricamente fechado)

Um corpo K é um *corpo algebricamente fechado* se, e somente se, todo polinômio não-constante em $K[x]$ tem pelo menos uma raiz em K.

Exemplo 14

(1) $\mathbb{Q}$ e $\mathbb{R}$ não são algebricamente fechados. O polinômio $x^2+1 \in \mathbb{Q}[x] \subsetneq \mathbb{R}[x]$ tem grau 2 e não tem raízes em $\mathbb{R}$, logo não tem raízes em $\mathbb{Q}$.

(2) $\mathbb{C}$ é um corpo algebricamente fechado. Esse fato não será demonstrado aqui, mas será utilizado.

A importância dos corpos algebricamente fechados será entendida na próxima proposição.

Proposição 5 (Propriedade dos corpos algebricamente fechados)

Sejam K um corpo algebricamente fechado e $f(x) \in K[x]$ um polinômio não-constante. Se $\text{grau}(f(x)) = n \geq 1$, então existem $\beta_1, \ldots, \beta_n \in K$, não necessariamente distintos, e $a \in K\backslash\{0\}$ tais que

Observamos que a é o coeficiente líder de $f(x)$.

$$f(x) = a(x - \beta_1) \cdot \ldots \cdot (x - \beta_n).$$

Demonstração: A demonstração é por indução sobre $n = \text{grau}(f(x))$. Se $\text{grau}(f(x)) = 1$, então $f(x) = ax + b$, com $a, b \in K$ e $a \neq 0$, logo $f(x) = a(x + a^{-1}b)$ e $\beta_1 = -a^{-1}b$. Suponhamos o resultado válido para n , onde $n \geq 1$, e seja $f(x)$ em $K[x]$ com $\text{grau}(f(x)) = n + 1$. Por hipótese, $f(x)$ tem uma raiz $\beta \in K$. Pela Proposição 3, $f(x) = q(x)(x - \beta)$, para algum $q(x) \in K[x]$ e $\text{grau}(q(x)) = n$. Por hipótese de indução, existem $a, \beta_1, \ldots, \beta_n \in K$, com $a \neq 0$ tais que

$$q(x) = a(x - \beta_1) \cdot \ldots \cdot (x - \beta_n).$$

Logo,

$$f(x) = a(x - \beta_1) \cdot \ldots \cdot (x - \beta_n)(x - \beta).$$

Tomando $\beta_{n+1} = \beta$, obtemos o resultado. ■

Proposição 6
Todo corpo algebricamente fechado é infinito.

Demonstração: Seja K um corpo algebricamente fechado e suponhamos, por absurdo, que K seja finito. Então,

$$K = \{a_1 = 0_K, a_2 = 1_K, \ldots, a_n\}, \text{ onde } n \geq 2.$$

Seja $f(x) = (x - a_1) \cdot \ldots \cdot (x - a_n) + 1_K$. Então, $f(a_j) = 1_K \neq 0_K$, para todo $j = 1, \ldots, n$. Portanto, esse polinômio não-constante não tem raízes em K, contradizendo a hipótese de K ser algebricamente fechado. ■

Exemplo 15
$\mathbb{Z}_p$, com p natural primo, não é algebricamente fechado.

O seguinte Teorema não pode ser demonstrado nesse contexto, mas é muito importante.

Teorema 2
Para todo corpo K existe um corpo $\overline{K}$, tal que $K \subset \overline{K}$ e $\overline{K}$ é algebricamente fechado.

Moral da história:
Se $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in K[x]$, com $a_n \neq 0$ e $n \geq 1$, então em $\overline{K}[x]$ temos $f(x) = a_n(x - \beta_1) \cdot \ldots \cdot (x - \beta_n)$.

$\beta_1, \ldots, \beta_n \in \overline{K}$ não são, necessariamente, distintos.

Corolário 3
Se $f(x) \in K[x]$ é um polinômio de grau $n \geq 1$, então $f(x)$ tem no máximo n raízes em qualquer corpo L tal que $K \subset L$.

Observação: Se A é um subanel de $\mathbb{C}$, então $A[x] \subset \mathbb{C}[x]$ e o polinômio $f(x) \in A[x]$, com grau$(f(x)) = n \geq 1$, tem exatamente n raízes em $\mathbb{C}$ e

$$f(x) = a(x - \beta_1) \cdot \ldots \cdot (x - \beta_n),$$

$\beta_1, \ldots, \beta_n \in \mathbb{C}$ não são, necessariamente, distintos.

onde $a \in A$ e $\beta_1, \cdots, \beta_n \in \mathbb{C}$.

Em particular, esse resultado é válido nos anéis $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$ e $\mathbb{C}[x]$.

Exercícios

1. Calcule a soma e produto dos polinômios $f(x)$ e $g(x)$:
   (a) $f(x) = \overline{2}x^3 + \overline{4}x^2 + \overline{3}x + \overline{3}$ e $g(x) = \overline{3}x^4 + \overline{2}x + \overline{4}$ em $\mathbb{Z}_5[x]$.
   (b) $f(x) = \overline{2}x^3 + \overline{4}x^2 + \overline{3}x + \overline{3}$ e $g(x) = \overline{3}x^4 + \overline{2}x + \overline{4}$ em $\mathbb{Z}_7[x]$.
2. Use o método dos coeficientes a determinar para:
   (a) Escrever $x^4 + 4 \in \mathbb{Z}[x]$ como o produto de dois polinômios do segundo grau com coeficientes inteiros.
   (b) Determinar $a, b \in \mathbb{Z}_7$ de modo que $x^4 + \overline{4}x^3 + ax^2 - \overline{4}x + b \in \mathbb{Z}_7[x]$ seja o quadrado de um polinômio mônico em $\mathbb{Z}_7[x]$.
   (c) Determinar a de modo que $x^4 - ax^3 + 8x^2 - 8x + a \in \mathbb{Z}[x]$ seja o quadrado de um polinômio mônico em $\mathbb{Z}[x]$.
3. Calcule todas as raízes em $\mathbb{Z}_5$ do polinômio $f(x) = x^5 + \overline{3}x^3 + x^2 + \overline{2}x$ de $\mathbb{Z}_5[x]$.
4. Mostre que o polinômio $f(x) = x^2 - \overline{1} \in \mathbb{Z}_{15}[x]$ tem 4 raízes no anel $\mathbb{Z}_{15}$.
5. Sejam A um domínio, $\beta \in A$ e $f(x) \in A[x]$. Mostre que o resto da divisão euclidiana de $f(x)$ por $x - \beta$ em $A[x]$ é $f(\beta)$.
6. Determine o resto da divisão euclidiana de $f(x)$ por $x - \beta$:
   (a) $f(x) = x^6 - 1$, $x + 2 \in \mathbb{Z}[x]$,

(b) $f(x) = x^{10} + \overline{3}$, $x + \overline{5} \in \mathbb{Z}_7[x]$.

7. Sejam K um corpo, $p(x) \in K[x]$ e $a, b \in K$ com $a \neq b$. Mostre que o resto $r(x)$ da divisão de $p(x)$ por $(x-a)(x-b)$ é

$$r(x) = \frac{p(a) - p(b)}{a - b}x + \frac{ap(b) - bp(a)}{a - b}.$$

8. Determine o quociente $q(x)$ e o resto $r(x)$ da divisão euclidiana de $f(x)$ por $g(x)$:

(a) $f(x) = x^3 + x - 1$ e $g(x) = x^2 + 1$ em $\mathbb{R}[x]$.

(b) $f(x) = x^5 - 1$ e $g(x) = x - 1$ em $\mathbb{R}[x]$.

(c) $f(x) = x^3 - 3$ e $g(x) = x - \sqrt[3]{2}$ em $\mathbb{R}[x]$.

(d) $f(x) = x^3 + \overline{2}x^2 + x + \overline{3}$ e $g(x) = x^2 + \overline{4}x + \overline{3}$ em $\mathbb{Z}_5[x]$.

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

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

Atenção: se D é um domínio e o coeficiente líder do divisor $g(x)$ é um elemento de D^*, então a divisão euclidiana vale em $D[x]$.

$D^* = \{a \in D; a \text{ é invertível } \}$

POLINÔMIOS SOBRE DOMÍNIOS E CORPOS

Polinômios sobre corpos

Começamos relembrando o conceito de ideal em anéis comutativos com unidade.

Definição 8 (Ideal)
Seja A um anel comutativo com unidade. Um subconjunto I de A é um *ideal* de A se, e somente se,

(i) $0_A \in I$;
(ii) se $a, b \in I$, então $a + b \in I$;
(iii) se $a \in A$ e $b \in I$, então $a \cdot b \in I$.

Exemplo 16
Seja A um anel comutativo com unidade. São exemplos de ideais:

(1) $I = \{0_A\}$ e $I = A$, chamados de *ideais triviais*.

(2) Fixe $a \in A$. O conjunto

$$I(a) = \{a \cdot \lambda \,;\, \lambda \in A\}$$

dos elementos de A que são múltiplos de a é um ideal de A, chamado de *ideal principal gerado por* a.

(3) Fixe $a, b \in A$. O conjunto

$$I(a, b) = \{a \cdot \lambda + b \cdot \delta \,;\, \lambda, \delta \in A\}$$

é um ideal de A, chamado de *ideal gerado por* a e b.

Definição 9 (Domínio Principal)
Seja A um domínio. A é um *domínio principal* se, e somente se, todo ideal de A é principal.

Exemplo 17
$\mathbb{Z}$ é um domínio principal.

Os ideais de $\mathbb{Z}$ são da forma $I(n) = n\mathbb{Z}$, para algum $n \geq 0$.

A demonstração usa a divisão euclidiana e o Princípio da Boa Ordenação (todo subconjunto de $\mathbb{Z}$ limitado inferiormente tem menor elemento).

Exemplo 18
$\mathbb{Z}[x]$, o domínio dos polinômios com coeficientes em $\mathbb{Z}$, não é principal.

De fato, consideremos o ideal $I = I(2, x)$. Suponhamos, por absurdo, que I seja principal. Então, existe $p(x) \in \mathbb{Z}[x]$ tal que $I = I(p(x))$. Como $2, x \in I$, então existem $f(x)$ e $g(x)$ em $\mathbb{Z}[x]$ tais que $2 = p(x)f(x)$ e $x = p(x)g(x)$.

Calculando o grau nas duas igualdades, concluímos que
$\text{grau}(f(x)) = \text{grau}(p(x)) = 0$, $1 = \text{grau}(p(x)) + \text{grau}(g(x))$ e $\text{grau}(g(x)) = 1$.
Logo, $p(x) = a \neq 0$, $f(x) = b \neq 0$, $a, b \in \mathbb{Z}$ e $ab = 2$, além de $g(x) = cx$, $x = a \cdot cx$ dando que $ac = 1$. Logo, $a = 1$ ou $a = -1$. Então, em qualquer dos casos, $I(p(x)) = \mathbb{Z}[x]$. Como $1 \in \mathbb{Z}[x] = I(p(x)) = I(2, x)$, então existem $s(x), r(x) \in \mathbb{Z}[x]$ tais que

$$1 = 2s(x) + xr(x).$$

$s(x) = s_0 + s_1 x + \cdots + s_n x^n$, com $s_j \in \mathbb{Z}$.

Avaliando em $x = 0$, obtemos $1 = 2s(0) = 2s_0$, com $s_0 \in \mathbb{Z}$, contradizendo o fato de 2 não ser invertível em $\mathbb{Z}$. Portanto, $\mathbb{Z}[x]$ não é domínio principal.

O resultado a seguir é muito importante! Teremos agora muitos exemplos de domínios principais.

Reveja a demonstração de que $\mathbb{Z}$ é um domínio principal.

Teorema 3
Seja K um corpo. $K[x]$ é um domínio principal.

Demonstração: Vamos mostrar que todo ideal de $K[x]$ é principal. Se $I = \{0\}$, então é claro que $I = I(0)$ é principal. Seja $I \neq \{0\}$ um ideal de $K[x]$. Seja

$$S = \{\text{grau}(f(x)) \ ; \ f(x) \neq 0 \text{ e } f(x) \in I\}.$$

Então, S é um subconjunto não-vazio de $\mathbb{N}$. Pelo princípio da Boa Ordenação, S tem menor elemento, digamos n_0. Seja $p(x) \in I$, $p(x) \neq 0$, com $\text{grau}(p(x)) = n_0$.

Afirmamos que $I = I(p(x)) = \{\ p(x)g(x) \ ; \ g(x) \in K[x]\ \}$.

De fato, como $p(x) \in I$ e I é um ideal de $K[x]$, então para qualquer $g(x) \in K[x]$ temos que $p(x)g(x) \in I$. Logo, $I(p(x)) \subset I$.

Consideremos agora $f(x) \in I$. Pela divisão euclidiana de $f(x)$ por $p(x)$, existem $q(x), r(x) \in K[x]$ tais que

$$f(x) = p(x)q(x) + r(x),$$

onde $r(x) = 0$ ou $\text{grau}(r(x)) < \text{grau}(p(x)) = n_0$.

Logo, $r(x) = \underbrace{f(x)}_{\in I} - \underbrace{\underbrace{p(x)}_{\in I}\, q(x)}_{\in I} \in I$.

Portanto, a segunda possibilidade não ocorre, temos $r(x) = 0$, $f(x) = p(x)q(x) \in I(p(x))$ e $I \subset I(p(x))$ ■.

Observação:

(1) Na demonstração acima temos que o polinômio gerador de um ideal não-nulo de $K[x]$ é um polinômio não-nulo de menor grau que tem a propriedade de estar no ideal.

(2) Os elementos invertíveis de $K[x]$ são os elementos invertíveis de K, isto é, $K[x]^* = K^* = K\backslash\{0\}$.

(3) Sejam A um domínio e $a \in A$ não-nulo. Então, $I(a) = I(ua)$, para qualquer u invertível em A.

Verifique.

(4) Seja $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in K[x]$, onde K é um corpo e $a_n \neq 0$. Então,

$$\begin{aligned} p(x) &= a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \\ &= a_n \underbrace{(x^n + a_n{}^{-1}a_{n-1}x^{n-1} + \cdots + a_n{}^{-1}a_1 x + a_n{}^{-1}a_0)}_{g(x)} \end{aligned}$$

Das observações (2) e (3), temos que $I(p(x)) = I(ap(x))$, para qualquer $a \in K$, com $a \neq 0$. Em particular, tomando $a = a_n{}^{-1}$, obtemos

$$I(p(x)) = I(g(x)), \text{ onde } g(x) \text{ é mônico.}$$

Corolário 4

Se I é um ideal não-nulo de $K[x]$, então existe um único gerador mônico de I, a saber, o polinômio mônico de menor grau que está em I.

Exemplo 19

Seja $I = \{f(x) \in \mathbb{R}[x] \,;\, f(\sqrt{2}) = 0\}$. I é um ideal de $\mathbb{R}[x]$, pois

(i) $0(\sqrt{2}) = 0$.

(ii) Sejam $f(x) = \sum_{j=0}^{n} a_j x^j$, $g(x) = \sum_{j=0}^{n} b_j x^j \in I$. Então,

$$h(x) = f(x) + g(x) = \sum_{j=0}^{n} (a_j + b_j)x^j \text{ e}$$

$$\begin{aligned} h(\sqrt{2}) &= \sum_{j=0}^{n} (a_j + b_j)(\sqrt{2})^j \\ &\overset{(1)}{=} \sum_{j=0}^{n} \left(a_j(\sqrt{2})^j + b_j(\sqrt{2})^j\right) \\ &\overset{(2)}{=} \sum_{j=0}^{n} a_j(\sqrt{2})^j + \sum_{j=0}^{n} b_j(\sqrt{2})^j \\ &\overset{(3)}{=} f(\sqrt{2}) + g(\sqrt{2}) \\ &\overset{(4)}{=} 0 + 0 = 0. \end{aligned}$$

Em (1) usamos a propriedade distributiva da adição e multiplicação de números reais; em (2), as propriedades comutativa e associativa da adição de números reais; em (3), a definição de avaliação e, em (4) o fato de $f(x), g(x) \in I$.

Logo, $h(x) = f(x) + g(x) \in I$.

(iii) Sejam $f(x) = \sum_{j=0}^{m} a_j x^j \in \mathbb{R}[x]$ e $g(x) = \sum_{k=0}^{n} b_k x^k \in I$. Então,

$$h(x) = f(x)g(x) = \sum_{j=0}^{m+n} c_j x^j, \text{ onde } c_j = \sum_{\lambda+\mu=j} a_\lambda b_\mu \text{ e}$$

$$\begin{aligned} h(\sqrt{2}) &= \sum_{j=0}^{m+n} c_j (\sqrt{2})^j \\ &= \sum_{j=0}^{m+n} \left(\sum_{\lambda+\mu=j} a_\lambda b_\mu \right) (\sqrt{2})^j. \end{aligned}$$

Calculando $f(\sqrt{2})g(\sqrt{2})$ temos

$$\begin{aligned} f(\sqrt{2})g(\sqrt{2}) &= \left(\sum_{\lambda=0}^{m} a_\lambda (\sqrt{2})^\lambda \right) \left(\sum_{\mu=0}^{n} b_\mu (\sqrt{2})^\mu \right) \\ &\overset{(1)}{=} \sum_{\lambda=0}^{m} \left(\sum_{\mu=0}^{n} \left(a_\lambda (\sqrt{2})^\lambda b_\mu (\sqrt{2})^\mu \right) \right) \\ &\overset{(2)}{=} \sum_{\lambda=0}^{m} \left(\sum_{\mu=0}^{n} \left(a_\lambda b_\mu (\sqrt{2})^{\lambda+\mu} \right) \right) \\ &\overset{(3)}{=} \sum_{j=0}^{m+n} \left(\sum_{\lambda+\mu=j} a_\lambda b_\mu \right) (\sqrt{2})^j. \end{aligned}$$

Em (1) usamos a distributividade da adição e multiplicação de números reais; em (2) usamos a comutatividade da multiplicação em $\mathbb{R}$; em (3), a comutatividade e a associatividade da adição em $\mathbb{R}$ e definimos $j = \lambda + \mu$.

Comparando os resultados vemos que $h(\sqrt{2}) = f(\sqrt{2})g(\sqrt{2}) = f(\sqrt{2}) \cdot 0 = 0$. Logo, $h(x) \in I$.

O polinômio mônico $p(x) \in \mathbb{R}[x]$ de menor grau que está em I é $x - \sqrt{2}$. Logo, $I = I(x - \sqrt{2})$.

Exemplo 20

Agora você deve mostrar que $I = \{f(x) \in \mathbb{Q}[x] \ ; \ f(\sqrt{2}) = 0\}$ é um ideal de $\mathbb{Q}[x]$. Os cálculos são análogos ao anterior, observando que para todo $g(x) \in \mathbb{Q}[x]$, como $\sqrt{2} \in \mathbb{R}$ e $\mathbb{Q}$ é um subcorpo de $\mathbb{R}$, então $g(\sqrt{2}) \in \mathbb{R}$.

Nesse caso, $I = I(x^2 - 2)$. Justifique!

Definição 10 (Máximo divisor comum)

Seja A um domínio. Sejam $a_1, \ldots, a_n \in A$. Um elemento $d \in A \backslash \{0\}$ é chamado um máximo divisor comum de $a_1, \ldots, a_n$ se, e somente se, tem as seguintes propriedades:

Sejam $d, u \in A$ com u invertível. d é um mdc se, e somente se, ud é um mdc.

(i) d é divisor comum de $a_1, \ldots, a_n$, isto é, d divide a_1, ..., d divide a_n;
(ii) se $c \in A\backslash\{0\}$ é um divisor comum de $a_1, \ldots, a_n$, então c divide d.

Em domínios principais temos a existência de máximos divisores comuns. A seguir a versão no domínio principal $K[x]$.

Teorema 4 (Existência de mdc)
Seja K um corpo. Sejam $f_1(x), \ldots, f_n(x) \in K[x]$ nem todos nulos e seja $I = I(f_1(x), \ldots, f_n(x))$. Então, existe $d(x)$ em $K[x]$ tal que $I = I(d(x))$ e $d(x)$ tem as propriedades:
(i) existem $q_1(x), \ldots, q_n(x) \in K[x]$ tais que

$$d(x) = q_1(x)f_1(x) + \cdots + q_n(x)f_n(x).$$

(ii) $d(x)$ é um divisor comum de $f_1(x), \ldots, f_n(x)$;
(iii) se $c(x)$ é um divisor comum de $f_1(x)$, ..., $f_n(x)$, então $c(x)$ divide $d(x)$.

As propriedades (ii) e (iii) dizem que $d(x)$ é um mdc de $f_1(x), \ldots, f_n(x)$.

Demonstração:
(i) Pelo Teorema 3, existe $d(x) \in K[x]$, tal que

$$I(d(x)) = I = K[x]f_1(x) + \cdots + K[x]f_n(x),$$

então existem $q_1(x), \ldots, q_n(x) \in K[x]$ tais que

$$d(x) = q_1(x)f_1(x) + \cdots + q_n(x)f_n(x).$$

(ii) Como $f_1(x), \ldots, f_n(x) \in I = I(d(x))$, então existem $g_1(x), \ldots, g_n(x)$ em $K[x]$ tais que $f_1(x) = g_1(x)d(x)$, ..., $f_n(x) = g_n(x)d(x)$ e $d(x) \neq 0$, pois $I \neq \{0\}$. Logo, $d(x) \mid f_1(x)$, ..., $d(x) \mid f_n(x)$.

Para algum $j = 1, \ldots, n$, temos $f_j(x) \neq 0$, logo $I \neq \{0\}$.

(iii) Seja $c(x)$ um divisor comum de $f_1(x)$, ..., $f_n(x)$. Então, existem $\ell_1(x)$, ..., $\ell_n(x)$ em $K[x]$ tais que $f_j(x) = \ell_j(x)c(x)$, para cada $j = 1, \ldots, n$ e

$$\begin{aligned} d(x) &\overset{(1)}{=} q_1(x)f_1(x) + \cdots + q_n(x)f_n(x) \\ &\overset{(2)}{=} q_1(x)\big(\ell_1(x)c(x)\big) + \cdots + q_n(x)\big(\ell_n(x)c(x)\big) \\ &\overset{(3)}{=} \big(q_1(x)\ell_1(x)\big)c(x) + \cdots + \big(q_n(x)\ell_n(x)\big)c(x) \\ &\overset{(4)}{=} \big(q_1(x)\ell_1(x) + \cdots + q_n(x)\ell_n(x)\big)c(x). \end{aligned}$$

Em (1) usamos o item (i); em (2), $f_j(x) = \ell_j(x)c(x)$, para $j = 1, \ldots, n$; em (3), a associatividade da multiplicação em $K[x]$; em (4), a distributividade da adição e multiplicação em $K[x]$.

Logo, $c(x)$ divide $d(x)$. ■

Observação: $d(x)$ é um máximo divisor comum de $f_1(x)$, ..., $f_n(x)$ se, e somente se, $ad(x)$, com $a \in K$ e $a \neq 0$ é um mdc. Portanto, existe um único polinômio mônico (coeficiente líder igual a 1_K) que é um máximo divisor comum de $f_1(x)$, $\dots f_n(x)$. Denotaremos o máximo divisor comum mônico por $\text{mdc}\big(f_1(x), \dots, f_n(x)\big)$.

Sejam $f(x), g(x) \in K[x]$. Se $f(x) = 0$ e $g(x) \neq 0$, então $g(x)$ é um máximo divisor comum de $f(x)$ e $g(x)$. Tomando o coeficiente líder de $g(x)$, digamos a, então $a^{-1}g(x)$ é mônico e $\text{mdc}\big(f(x), g(x)\big) = \text{mdc}\big(0, g(x)\big) = a^{-1}g(x)$.

Definição 11 (Primos entre si)
Os polinômios $f_1(x), \dots, f_n(x)$ são ditos *primos entre si* se, e somente se, $\text{mdc}\big(f_1(x), \dots, f_n(x)\big) = 1$.

Exemplo 21
Os polinômios $x - 1$ e $x - 3$ em $\mathbb{R}[x]$ são primos entre si.
$2 = (x-1) - (x-3) \Longrightarrow 1 = \frac{1}{2}(x-1) - \frac{1}{2}(x-3) \Longrightarrow 1 = \text{mdc}(x-1, x-3)$.

A divisão euclidiana em $K[x]$, feita sucessivamente, permite determinar um máximo divisor comum para dois polinômios não-nulos.

Usaremos as seguintes propriedades de ideais:

- $I(a, 0) = I(a)$, para todo $a \in A$.

- a substituição de um dos geradores do ideal por ele menos qualquer múltiplo de outro gerador não altera o ideal, a saber,

$$I(a, b) = I(b, a - bc), \text{ para todo } c \in A,$$

Sejam $f(x), g(x) \in K[x]$ não-nulos, com $\text{grau}(f(x)) \geq \text{grau}(g(x))$. Pela divisão euclidiana de $f(x)$ por $g(x)$, existem polinômios $q(x), r(x) \in K[x]$ tais que

$$f(x) = q(x)g(x) + r(x),$$

onde $r(x) = 0$ ou $\text{grau}(r(x)) < \text{grau}(g(x))$.

Definimos $r_{-1}(x) = f(x)$, $r_0(x) = g(x)$, $q_0(x) = q(x)$ e $r_1(x) = r(x)$.

Temos que $I(f(x), g(x)) = I(r_0(x), f(x) - r_0(x)q_0(x)) = I(r_0(x), r_1(x))$.

Se $r_1(x) = 0$, então $r_0(x) = g(x)$ é um mdc de $f(x)$ e $g(x)$, pois $I(f(x), g(x)) = I(r_0(x), 0) = I(r_0(x))$.

Se $r_1(x) \neq 0$, temos $\text{grau}(r_1(x)) < \text{grau}(r_0(x))$ e fazemos a divisão euclidiana de $r_0(x)$ por $r_1(x)$, obtendo $q_1(x)$ e $r_2(x)$ tais que

$$r_0(x) = q_1(x)r_1(x) + r_2(x),$$

onde $r_2(x) = 0$ ou $\text{grau}(r_2(x)) < \text{grau}(r_1(x))$.

Nesse caso, $I(f(x), g(x)) = I(r_0(x), r_1(x)) = I(r_1(x), r_2(x))$.

Se $r_2(x) = 0$, terminamos, pois $I(r_1(x), r_2(x)) = I(r_1(x), 0) = I(r_1(x))$.

Se $r_2(x) \neq 0$, fazemos a divisão euclidiana de $r_1(x)$ por $r_2(x)$, obtendo quociente $q_2(x)$ e resto $r_3(x)$ tais que

$$r_1(x) = q_2(x)r_2(x) + r_3(x),$$

onde $r_3(x) = 0$ ou $\text{grau}(r_3(x)) < \text{grau}(r_2(x))$.

Continuamos esse processo, até que para algum $n \geq 0$ temos $r_n(x) \neq 0$, mas $r_{n+1}(x) = 0$. Então, $r_n(x)$ é um máximo divisor comum de $f(x)$ e $g(x)$.

De fato, se $r_j(x) \neq 0$ para todo $j \geq 0$, então

$$\text{grau}(r_0(x)) > \text{grau}(r_1(x)) > \cdots > \text{grau}(r_j(x)) > \cdots \geq 0,$$

é uma seqüência de inteiros positivos limitada inferiormente sem menor elemento, contradizendo o Princípio da Boa Ordenação.

Portanto, existe um $n \geq 0$ tal que $r_n(x) \neq 0$ com $r_{n+1}(x) = 0$.

Nesse caso,

$$\begin{aligned} I(f(x), g(x)) &= I(r_0(x), r_1(x)) = \cdots \\ &= I(r_n(x), r_{n+1}(x)) \\ &= I(r_n(x), 0) \\ &= I(r_n(x)), \end{aligned}$$

mostrando que $r_n(x)$ é um máximo divisor comum de $f(x)$ e $g(x)$.

Cuidado: $r_n(x) \in K[x]$ pode não ser um polinômio mônico.

Algoritmo euclidiano

Sejam $f(x), g(x) \in K[x]\backslash\{0\}$ com $\text{grau}(f(x)) \geq \text{grau}(g(x))$.

(1) Faça $r_{-1}(x) = f(x)$, $r_0(x) = g(x)$. Faça $j = 0$.

(2) Faça a divisão de $r_{j-1}(x)$ por $r_j(x)$, determinando $q_j(x)$ e $r_{j+1}(x)$ tais que $r_{j-1}(x) = q_j(x)r_j(x) + r_{j+1}(x)$.

(3) Se $r_{j+1}(x) = 0$, então $r_j(x)$ é um mdc. Vá para (5)

(4) Se $r_{j+1}(x) \neq 0$, faça $j = j + 1$ e vá para (2).

(5) Faça um mdc de $f(x)$ e $g(x)$ igual a $r_j(x)$. Pare.

Podemos guardar, organizadamente, os cálculos do algoritmo euclidiano na tabela

	$q_0(x)$	$q_1(x)$		$q_{n-2}(x)$	$q_{n-1}(x)$	$q_n(x)$
$f(x)$	$g(x)$	$r_1(x)$	$\cdots$	$r_{n-2}(x)$	$r_{n-1}(x)$	$r_n(x)$
$r_1(x)$	$r_2(x)$	$r_3(x)$		$\underbrace{r_n(x)}_{\text{um mdc}}$	$r_{n+1}(x)= 0$	

Exemplo 22

Sejam $f(x) = 2x^3+4x^2+2x$ e $g(x) = x^2+3x+2$ em $\mathbb{Q}[x]$. Vamos determinar o seu mdc. Temos $3 = \text{grau}(f(x)) > \text{grau}(g(x)) = 2$.

Fazendo as divisões euclidianas e transportando para a tabela, obtemos:

	$2x - 2$	$\frac{1}{4}x + \frac{1}{2}$	
$2x^3 + 4x^2 + 2x$	$x^2 + 3x + 2$	$4x + 4$	
$4x + 4$	0		

$4x + 4$ é um mdc de $f(x)$ e $g(x)$. Logo, $\text{mdc}(f(x), g(x)) = x + 1$.

Exemplo 23

Sejam $f(x) = x^3-x^2-x-2$ e $g(x) = x^3-3x-2$ em $\mathbb{Q}[x]$. Vamos determinar o seu mdc. Nesse caso, $\text{grau}(f(x)) = \text{grau}(g(x)) = 3$.

Fazendo as divisões euclidianas e transportando para a tabela, obtemos:

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

Nesse caso, $\text{mdc}(f(x), g(x)) = x - 2$.

Exemplo 24

Sejam $f(x) = x^5 + x^4 - x - 1$ e $g(x) = x^3 - 2x^2 - x + 2$ em $\mathbb{Q}[x]$. Vamos determinar o seu mdc. Nesse caso, $5 = \text{grau}(f(x)) > \text{grau}(g(x)) = 3$.

Fazendo as divisões euclidianas e transportando para a tabela, obtemos:

	$x^2 + 3x + 7$	$\frac{1}{15}x - \frac{2}{15}$	
$x^5 + x^4 - x - 1$	$x^3 - 2x^2 - x + 2$	$15x^2 - 15$	
$15x^2 - 15$	0		

$15x^2 - 15 = 15(x^2 - 1)$ é um mdc. Logo, $\text{mdc}(f(x), g(x)) = x^2 - 1$.

Exemplo 25

Podemos escrever um mdc de $f(x)$ e $g(x)$ em $K[x]$ como uma soma de um múltiplo de $f(x)$ e de um múltiplo de $g(x)$, a partir do algoritmo euclidiano.

Voltamos ao Exemplo 23, onde $f(x), g(x) \in \mathbb{Q}[x]$.

	1	$-x - 2$	$-x$	
$f(x) = x^3 - x^2 - x - 2$	$g(x) = x^3 - 3x - 2$	$-x^2 + 2x$	$x - 2$	
$-x^2 + 2x$	$x - 2$	0		
(1)	(2)			

Escrevemos as igualdades obtidas em cada passo do algoritmo, destacando os polinômios $f(x)$ e $g(x)$ dados, além dos restos não-nulos encontrados.

$(1) \quad f(x) = 1 \cdot g(x) + \underbrace{(-x^2 + 2x)}$

$(2) \quad g(x) = (-x^2 + 2x)(-x - 2) + \underbrace{(x - 2)}_{\text{um mdc}}.$

Na última igualdade temos um mdc. Destacamos esse polinômio e substituímos, de trás para frente, apenas os valores dos restos obtidos.

$$\begin{aligned} x - 2 &\overset{(2)}{=} g(x) - \underbrace{(-x^2 + 2x)}(-x - 2) \\ &\overset{(1)}{=} g(x) - \big(f(x) - g(x)\big)(-x - 2) \\ &= (2 + x)f(x) + (-x - 1)g(x) \end{aligned}$$

Como $K[x]$ é um domínio principal, vale a fatoração única de elementos não-nulos e não-invertíveis em produto de elementos irredutíveis.

Vamos relembrar esses conceitos.

Definição 12 (Elemento irredutível)
Seja A um domínio. Seja $a \in A\backslash\{0\}$ um elemento não-invertível.

Os divisores de a irredutível são invertíveis ou $u \cdot a$, onde u é invertível.

a é dito *irredutível* se, e somente se,

se $a = b \cdot c$, com $b, c \in A$, então b ou c é invertível.

Caso contrário, a é dito *redutível*, isto é,

a é dito *redutível* se, e somente se,

existem b, c em A não-invertíveis tais que $a = b \cdot c$.

É bom dividir um produto por um primo: se um primo divide um produto ele tem que dividir um dos fatores.

a é dito *primo* se, e somente se,

se $b, c \in A$ e $a \mid b \cdot c$, então $a \mid b$ ou $a \mid c$.

Antes dos exemplos uma propriedade muito importante.

Proposição 7
Sejam A um domínio e $a \in A$. Se a é um elemento primo, então a é irredutível.

Demonstração: Sejam a primo e $b, c \in A$ tais que $a = b \cdot c$. Vamos mostrar que b ou c é invertível em A.

Como a divide $a = b \cdot c$ e a é primo, então a divide b ou a divide c. Suponhamos que a divida b. Então, $b = a \cdot d$, para algum $d \in A$ e logo,

$$a = b \cdot c = (a \cdot d) \cdot c = a \cdot (d \cdot c).$$

Como A é um domínio e $a \neq 0$, pela lei do cancelamento, temos $1_A = d \cdot c$, logo c é invertível. ■

Agora exemplos de elementos irredutíveis.

Exemplo 26
Em $\mathbb{Z}$ temos $\mathbb{Z}^* = \{1, -1\}$. Todo $p \in \mathcal{P} = \{2, 3, 5, 7, 11, 13, \ldots\}$ é irredutível, pois $p = 1 \cdot p$ ou $p = (-1) \cdot (-p)$ são as fatorações possíveis.

Os irredutíveis de $\mathbb{Z}$ são $\mathcal{P} \cup (-\mathcal{P})$.

Exemplo 27
Se A é um domínio, então $x - a$, onde $a \in A$, é irredutível em $A[x]$.

De fato, escrevendo $x - a = f(x)g(x)$, com $f(x), g(x) \in A[x]$ temos que ambos os fatores são não-nulos e $1 = \text{grau}(x-a) = \text{grau}(f(x)) + \text{grau}(g(x))$. Logo, $\text{grau}(f(x)) = 0$ e $\text{grau}(g(x)) = 1$ ou $\text{grau}(f(x)) = 1$ e $\text{grau}(g(x)) = 0$. Suponhamos válido o primeiro caso. Então, $f(x) = a \neq 0$, $g(x) = bx + c$, com $b \neq 0$, e $a \cdot b = 1_A$. Assim, $f(x) = a$ é invertível em A, logo é invertível em $A[x]$.

Temos $A^* = A[x]^*$.

Exemplo 28

Em $\mathbb{Z}[x]$ temos $\mathbb{Z}[x]^* = \mathbb{Z}^* = \{1, -1\}$.

Os polinômios do tipo $x - a$, onde $a \in \mathbb{Z}$ são irredutíveis.

$2x + 3$ é irredutível, entretanto $6x + 9 = 3(2x + 3)$ não é irredutível.

Cuidado! Há polinômios de grau 1 que não são irredutíveis em $A[x]$, quando o domínio A não é um corpo.

Exemplo 29

Seja K um corpo qualquer. Temos $K[x]^* = K^*$.

Os polinômios $x - \alpha$, com $\alpha \in K$, são irredutíveis em $K[x]$.

Os polinômios $ax + b$, onde $a, b \in K$ e $a \neq 0$, também são irredutíveis.

De fato, escrevendo $ax + b = f(x)g(x)$, com $f(x), g(x) \in K[x]$ temos que ambos os fatores são não-nulos e $1 = \text{grau}(ax+b) = \text{grau}(f(x)) + \text{grau}(g(x))$. Logo, $\text{grau}(f(x)) = 0$ e $\text{grau}(g(x)) = 1$ ou $\text{grau}(f(x)) = 1$ e $\text{grau}(g(x)) = 0$. Em ambos os casos $f(x) = c \neq 0$ ou $g(x) = d \neq 0$. Logo, $f(x)$ ou $g(x)$ é invertível em $K[x]$.

Traduzindo o conceito de irredutível em $K[x]$:

(1) Todo polinômio $f(x) \in K[x]$ com $\text{grau}(f(x)) = 1$ é irredutível.

(2) $f(x) \in K[x]$, com $\text{grau}(f(x)) \geq 2$, é irredutível em $K[x]$ se, e somente se,

se $f(x) = g(x)h(x)$, com $g(x), h(x) \in K[x]$, então $g(x) = a \in K\backslash\{0\}$ ou $h(x) = b \in K\backslash\{0\}$.

Exemplo 30

Se K é um corpo algebricamente fechado, então os polinômios de grau 1 são os únicos polinômios irredutíveis de $K[x]$.

Verifique!

Proposição 8

Sejam A um domínio e $a \in A$. As seguintes condições são equivalentes:

(i) a é irredutível;

(ii) para todo invertível $u \in A$, $u \cdot a$ é irredutível;

(iii) existe um invertível $u \in A$, tal que $u \cdot a$ é irredutível.

Demonstração:

((i) $\Longrightarrow$ (ii)) Seja u invertível em A e escreva $ua = b \cdot c$. Então, $a = (u^{-1} \cdot b) \cdot c$. Como a é irredutível $u^{-1} \cdot b$ é invertível ou c é invertível. Se $u^{-1} \cdot b = v$ é invertível, então $b = u \cdot v$ é invertível. Logo, b ou c é invertível.

((ii) $\Longrightarrow$ (iii)) É óbvio.

((iii) $\Longrightarrow$ (i)) Seja u invertível em A tal que ua seja irredutível. Todo divisor de a é um divisor de ua e logo só pode ser um invertível ou $v(ua) = (vu)a$, com v invertível. Assim, a é irredutível. ■

vu é invertível.

Definição 13 (Associado)
Seja A um domínio. Sejam $a, b \in A$. Dizemos que b é *associado* de a se, e somente se, existe $u \in A$ invertível tal que $b = u \cdot a$.

A relação $b \sim a$ se, e somente se, b é associado de a é uma relação de equivalência em A (Verifique).

Exemplo 31
Em $\mathbb{Z}$ temos $\mathbb{Z}^* = \{1, -1\}$.

O único associado de 0 é 0.

Os associados de $a \neq 0$ são a e $-a$

Exemplo 32
Em $K[x]$ temos $K[x]^* = K^*$.

Os associados de $f(x) \neq 0$ são $af(x)$, onde $a \in K^* = K\backslash\{0\}$.

Traduzindo os conceitos de irredutível e associado em $K[x]$:

se $f(x) \in K[x]$, com grau$(f(x)) \geq 1$, é irredutível em $K[x]$, existe um polinômio mônico irredutível associado a $f(x)$, a saber, $g(x) = b^{-1}f(x)$, onde b é o coeficiente líder de $f(x)$.

Exemplo 33
Se K é um corpo algebricamente fechado os únicos polinômios mônicos irredutíveis em $K[x]$ são $x - \alpha$, onde $\alpha \in K$.

Em particular, os únicos polinômios mônicos irredutíveis em $\mathbb{C}[x]$ são $x - \alpha$, onde $\alpha \in \mathbb{C}$.

Qual a importância dos elementos irredutíveis?

Proposição 9
Seja A um domínio principal. Se $a \in A$ é irredutível, então a é um elemento primo.

Demonstração: Seja a irredutível em A e suponhamos que a divida $b \cdot c$ e $a \nmid b$. Vamos mostrar que a divide c.

Seja I o ideal de A gerado por a e b, isto é, $I = I(a, b)$. Como $a \in I(a, b) = I$ e $a \neq 0$, então $I \neq \{0\}$. Como A é um domínio principal, então existe $d \in A$ tal que $I = I(d)$ e $d \neq 0$. Como $a, b \in I = I(d)$, então $d \mid a$ e $d \mid b$. Os divisores de a são invertíveis ou associados de a. Logo, $d = u$ invertível em A ou $d = v \cdot a$, com v invertível em A. Pelo fato de $a \nmid b$, concluímos que a única possibilidade é $d = u$. Assim, $I = I(d) = I(u) = A$. Logo, $1_A \in A = I(a, b)$. Portanto, existem $\alpha, \beta \in A$ tais que $1_A = \alpha \cdot a + \beta \cdot b$ e

$$c = 1_A \cdot c = (\alpha \cdot a + \beta \cdot b) \cdot c = \underbrace{\alpha \cdot a \cdot c}_{a \text{ divide}} + \underbrace{\beta \cdot \underbrace{b \cdot c}_{a \text{ divide}}}_{a \text{ divide}} .$$

Das propriedades da divisibilidade segue que a divide c. ■

Corolário 5
Sejam A um domínio principal e $a \in A$. O elemento a é irredutível se, e somente se, a é primo.

Teorema 5 (Fatoração única)
Seja K um corpo e seja $f(x) \in K[x]$ com grau$(f(x)) \geq 1$. Então, existem polinômios mônicos irredutíveis $p_1(x)$, ..., $p_s(x)$ distintos; naturais $n_1 \geq 1$, ..., $n_s \geq 1$ e $a \in K^*$ tais que

$$f(x) = a p_1(x)^{n_1} \cdot \ldots \cdot p_s(x)^{n_s}.$$

Note que a é o coeficiente líder de $f(x)$.

Essa expressão é única, a menos da ordem dos fatores.

Demonstração: Vamos mostrar que existem polinômios mônicos irredutíveis, não necessariamente distintos, $p_1(x)$, ..., $p_m(x)$ tais que

$$f(x) = a p_1(x) \cdot \ldots \cdot p_m(x) \text{ e}$$

essa expressão é única a menos da ordem dos fatores. Obtemos a expressão do enunciado, supondo que os fatores distintos são $p_1(x)$, ..., $p_s(x)$, com $s \leq m$ (após uma reenumeração, caso necessário), trocando a ordem dos fatores e associando os fatores iguais.
(Existência) A demonstração é por indução sobre $n = \text{grau}(f(x))$.

Se grau$(f(x)) = 1$, então $f(x) = ax + b = a(x + a^{-1}b)$, com $a, b \in K$ e $a \neq 0$.

Suponhamos que grau$(f(x)) = n \geq 2$ e o teorema válido para polinômios em $K[x]$ não-constantes com grau menor do que n. Vamos mostrar que vale para $f(x)$. Seja $f(x) = a_n x^n + \cdots + a_1 x + a_0$. Se $f(x)$ é irredutível, então $f(x) = a_n \underbrace{(x^n + \cdots + a_n^{-1}a_1 x + a_n^{-1}a_0)}_{p_1(x) \text{ mônico}}$, e $p_1(x)$ é irredutível pela Proposição 8. Portanto, podemos supor que $f(x)$ seja redutível. Então, existem $g(x)$ e $h(x)$ em $K[x]$ não-constantes tais que

$$f(x) = g(x)h(x), \text{ com } 1 \leq \text{grau}(g(x)), \text{grau}(h(x)) < n = \text{grau}(f(x)).$$

Por hipótese de indução,

$g(x) = bp_1(x) \cdot \ldots \cdot p_r(x)$, $b \in K^*$ e $p_1(x), \ldots, p_r(x)$ mônicos e irredutíveis.

$h(x) = cp_{r+1}(x) \cdot \ldots \cdot p_{r+\ell}(x)$, $c \in K^*$ e $p_{r+1}(x), \ldots, p_{r+\ell}(x)$ mônicos e irredutíveis.

Logo,

$$\begin{aligned} f(x) &= b \cdot p_1(x) \cdot \ldots \cdot p_r(x) \cdot c \cdot p_{r+1}(x) \cdot \ldots \cdot p_{r+\ell}(x) \\ &= a \cdot p_1(x) \cdot \ldots \cdot p_r(x) \cdot p_{r+1}(x) \cdot \ldots \cdot p_{r+\ell}(x), \end{aligned}$$

onde $a = b \cdot c \in K^*$ e $p_1(x), \ldots, p_{r+\ell}(x)$ são mônicos irredutíveis.

(Unicidade) Suponhamos que

$$f(x) = a \cdot p_1(x) \cdots p_m(x) = b \cdot q_1(x) \cdots q_r(x), \qquad (\star)$$

com $a, b \in K^*$ e $p_1(x), \ldots, p_m(x), q_1(x), \ldots, q_r(x)$ mônicos e irredutíveis.

Como a =coeficiente líder de $f(x) = b$, cancelando em $(\star)$ obtemos

$$p_1(x) \cdots p_m(x) = q_1(x) \cdots q_r(x).$$

Como $p_1(x)$ divide a esquerda, temos que $p_1(x)$ divide $q_1(x) \cdots q_r(x)$ e $p_1(x)$ é primo, então $p_1(x)$ divide $q_j(x)$ para algum $j = 1, \ldots, r$. Pela Proposição 8, $q_j(x) = up_1(x)$ para algum $u \in K^*$. Comparando os coeficientes líderes, obtemos $u = 1_K$ e $q_j(x) = p_1(x)$. Reenumerando os polinômios $q_1(x), \ldots, q_r(x)$ se necessário, podemos supor $p_1(x) = q_1(x)$

Faremos indução sobre m. Se $m = 1$, então $r = 1$. Se $m > 1$, cancelamos $p_1(x)$, obtendo

$$p_2(x) \cdots p_m(x) = q_2(x) \cdots q_r(x)$$

e, por hipótese de indução, $m - 1 = r - 1$, que é equivalente a $m = r$, e cada $p_j(x)$ é igual a $q_j(x)$. ■

Usando a fatoração única em $K[x]$ temos expressões para o mdc e o mmc de polinômios não-nulos.

Lembramos o conceito de mmc.

Definição 14 (Menor múltiplo comum)
Seja A um domínio. Sejam $a_1, \ldots, a_n$ elementos não-nulos. Um elemento $m \in A$ é dito um *menor múltiplo comum* de $a_1, \ldots, a_n$ se, e somente se,

(i) $m \in A$ é um múltiplo comum de $a_1, \ldots, a_n$;

(ii) se $c \in A$ é um múltiplo de $a_1, \ldots, a_n$, então c é múltiplo de m.

Em geral, m é um mmc de $a_1, \ldots, a_n$ se, e somente se, um é um mmc de $a_1, \ldots, a_n$, para todo u invertível em A.

Exemplo 34

Em $\mathbb{Z}$ vimos que: m é um mmc dos inteiros não-nulos $a_1, \ldots, a_n$ se, e somente se, $-m$ também é um mmc.

Em $\mathbb{Z}$ denotamos por $\text{mmc}(a_1, \ldots, a_n)$ o único mmc que é positivo. Assim, $\text{mmc}(2^2 \cdot 3^3 \cdot 5, -2 \cdot 3^4 \cdot 5^2 \cdot 7) = 2^2 \cdot 3^4 \cdot 5^2 \cdot 7$.

Exemplo 35

Sejam $a_1(x), \ldots, a_n(x)$ polinômios não-nulos em $K[x]$.

$m(x)$ é um mmc de $a_1(x), \ldots, a_n(x)$ se, e somente se, $a \cdot m(x)$ é um mmc de $a_1(x), \ldots, a_n(x)$, para todo $a \in K^*$.

Denotaremos por $\text{mmc}\big(a_1(x), \ldots, a_n(x)\big)$ o único mmc mônico.

Observação: Sejam $f(x)$, $g(x)$ em $K[x]$ polinômios não-nulos. Vamos determinar o mdc e o mmc, usando a fatoração única.

Fazemos a fatoração de $f(x)$ e de $g(x)$ em produto de potências de polinômios mônicos irredutíveis em $K[x]$.

Sejam $p_1(x), \ldots, p_s(x)$ os irredutíveis que ocorrem na fatoração de $f(x)$ ou de $g(x)$. Então,

$f(x) = a \cdot p_1(x)^{m_1} \cdots p_s(x)^{m_s}$, com $m_1 \geq 0, \ldots, m_s \geq 0$.

$g(x) = b \cdot p_1(x)^{n_1} \cdots p_s(x)^{n_s}$, com $n_1 \geq 0, \ldots, n_s \geq 0$.

Definindo $\gamma_j = \min\{m_j, n_j\}$ e $\delta_j = \max\{m_j, n_j\}$, obtemos que

$$\text{mdc}\big(f(x), g(x)\big) = p_1(x)^{\gamma_1} \cdots p_s(x)^{\gamma_s}$$

e

$$\text{mmc}\big(f(x), g(x)\big) = p_1(x)^{\delta_1} \cdots p_s(x)^{\delta_s}.$$

Exemplo 36

Os polinômios $x-1$, x^2+1, x^2-2 e $x-3$ são irredutíveis em $\mathbb{Q}[x]$. Verifique.

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

$\text{mdc}_{\mathbb{Q}[x]}\big(f(x), g(x)\big) = (x-1)(x^2+1)^2(x^2-2)(x-3)^0 = (x-1)(x^2+1)^2(x^2-2)$ e

$\text{mmc}_{\mathbb{Q}[x]}\big(f(x), g(x)\big) = (x-1)^2(x^2+1)^3(x^2-2)^2(x-3)^2$.

Exemplo 37

Qual o máximo divisor comum e qual o menor múltiplo comum dos polinômios $f(x) = (x^4-4)(x^2+2)$ e $g(x) = 2(x^4-4x^2+4)(x+\sqrt{2})$ em $\mathbb{R}[x]$?

Primeiramente, fatoramos $f(x)$ e $g(x)$ em produto de mônicos irredutíveis em $\mathbb{R}[x]$.

Os polinômios x^2+2, $x-\sqrt{2}$ e $x+\sqrt{2}$ são irredutíveis em $\mathbb{R}[x]$.

$f(x) = (x^2-2)(x^2+2)(x^2+2) = (x-\sqrt{2})(x+\sqrt{2})(x^2+2)^2$ e

$g(x) = 2(x^2-2)^2(x+\sqrt{2}) = 2(x-\sqrt{2})^2(x+\sqrt{2})^3$

$\text{mdc}_{\mathbb{R}[x]}\big(f(x),g(x)\big) = (x-\sqrt{2})(x+\sqrt{2})(x^2+2)^0 = (x-\sqrt{2})(x+\sqrt{2})$

$\text{mmc}_{\mathbb{R}[x]}\big(f(x),g(x)\big) = (x-\sqrt{2})^2(x+\sqrt{2})^3(x^2+2)^2$.

O problema fundamental é determinar quais são os polinômios mônicos irredutíveis em $K[x]$.

A resposta depende do corpo K.

Nas próximas seções vamos estudar esse problema, primeiramente, em $\mathbb{R}[x]$ e depois em $\mathbb{Q}[x]$.

Encerramos lembrando o conceito de ideal primo.

Definição 15 (Ideal primo)
Seja A um domínio. Um ideal $P \subsetneq A$ é dito um *ideal primo* se, e somente se, $a, b \in A$ e $a \cdot b \in P$, então $a \in P$ ou $b \in P$.

Exemplo 38
Em $\mathbb{Z}$ os ideais primos são $\{0\}$ ou $I(p)$, para algum p primo.

Exemplo 39
Em $K[x]$ um ideal $P \neq \{0\}$ é primo se, e somente se, $P = I(p(x))$, para algum polinômio mônico irredutível.

De fato, em qualquer domínio $I = \{0\}$ é um ideal primo.

Consideremos P um ideal primo não-nulo em $K[x]$. Então, existe um único polinômio mônico $p(x) \in K[x]\backslash K$ tal que $P = I(p(x))$, pois $P \subsetneq K[x]$ e todo ideal de $K[x]$ é principal. Afirmamos que $p(x)$ é irredutível.

De fato, suponhamos que $p(x) = f(x)\cdot g(x)$. Então, $f(x)\cdot g(x) = p(x) \in P$ e P é um ideal primo implica que $f(x) \in P$ ou $g(x) \in P$. Logo, $f(x)$ é múltiplo de $p(x)$ ou $g(x)$ é múltiplo de $p(x)$. No primeiro caso, existe $h(x)$ tal que $f(x) = p(x)\cdot h(x)$. Logo,

$$p(x) = f(x)\cdot g(x) = (p(x)\cdot h(x))\cdot g(x).$$

Cancelando $p(x)$, obtemos $1 = h(x)\cdot g(x)$. Logo, $g(x)$ é invertível, mostrando que $p(x)$ é irredutível.

Reciprocamente, suponhamos que $P = I(p(x))$, onde $p(x)$ é mônico irredutível. Vamos mostrar que P é um ideal primo. Sejam $f(x), g(x)$ em $K[x]$

tais que $f(x) \cdot g(x) \in P$. Então, $p(x)$ divide $f(x) \cdot g(x)$. Como $p(x)$ é um elemento primo, temos $p(x)$ divide $f(x)$ ou $p(x)$ divide $g(x)$. Logo, $f(x) \in P$ ou $g(x) \in P$.

Exemplo 40
$I = \{f(x) \in \mathbb{Q}[x] \ ; \ f(\sqrt{3}) = 0\}$ é um ideal de $\mathbb{Q}[x]$ e $I = I(x^2 - 3)$, pois $x^2 - 3$ é o polinômio mônico em $\mathbb{Q}[x]$ de menor grau com a propriedade de estar em I.

Como $x^2 - 3$ é irredutível em $\mathbb{Q}[x]$, temos que I é um ideal primo de $\mathbb{Q}[x]$.

Seja $f(x) \in K[x]$ com $\text{grau}(f(x)) \in \{2, 3\}$. $f(x)$ é irredutível em $K[x]$ se, e somente se, $f(x)$ não tem raiz em K.

Exemplo 41
Seja I o ideal de $\mathbb{R}[x]$ gerado por $x^2 - 3$. Então, $I = I(x^2 - 3) \subsetneq \mathbb{R}[x]$ não é um ideal primo em $\mathbb{R}[x]$, pois $x^2 - 3 = (x - \sqrt{3})(x + \sqrt{3})$ não é irredutível em $\mathbb{R}[x]$.

Exemplo 42
$I = \{f(x) \in \mathbb{R}[x] \ ; \ f(\sqrt{3}) = 0\}$ é um ideal de $\mathbb{R}[x]$, $I = I(x - \sqrt{3}) \subsetneq \mathbb{R}[x]$ e esse ideal é primo.

Encerramos essa seção com o conceito de multiplicidade de uma raiz.

Definição 16 (Multiplicidade)
Sejam K e L corpos, com $K \subset L$, $f(x) \in K[x]$ com $\text{grau}(f(x)) \geq 1$ e $\beta \in L$ uma raiz de $f(x)$. Dizemos que β é uma raiz de $f(x)$ de *multiplicidade* m se, e somente se, em $L[x]$, $(x - \beta)^m$ divide $f(x)$ e $(x - \beta)^{m+1}$ não divide $f(x)$. Quando $m = 1$ dizemos que β é uma *raiz simples* de $f(x)$ e quando $m \geq 2$ dizemos que β é uma *raiz múltipla* de $f(x)$.

$m = 2$ a raiz é dupla, $m = 3$ a raiz é tripla, ...

Contamos as raízes de um polinômio com as suas multiplicidades, isto é, se β tem multiplicidade m contamos como m raízes, a saber, $\beta_1 = \beta, \ldots, \beta_m = \beta$.

Exemplo 43
Seja $f(x) = (x^2 - 2x + 1)(x^4 - 1) \in \mathbb{Q}[x]$. Então, $f(x)$ se escreve em $\mathbb{Q}[x]$ como $f(x) = (x - 1)^2(x^2 - 1)(x^2 + 1) = (x + 1)(x - 1)^3(x^2 + 1)$. Portanto, $\beta = 1 \in \mathbb{Q}$ é uma raiz de multiplicidade 3 e $\beta = -1 \in \mathbb{Q}$ é uma raiz simples de $f(x)$.

Exemplo 44
Seja $f(x) = (x^2 - 2x + 1)(x^4 - 1) \in \mathbb{Q}[x] \subset \mathbb{C}[x]$. Então, em $\mathbb{C}[x]$ temos que $f(x) = (x - 1)^2(x^2 - 1)(x^2 + 1) = (x + 1)(x - 1)^3(x + i)(x - i)$ e agora $f(x)$ tem mais duas raízes simples em $\mathbb{C}$, além das duas raízes já mencionadas.

$\mathbb{Q} \subset \mathbb{C}$.

Observação: Seja K um subcorpo de L. Note que $\beta \in L$ é uma raiz de $f(x) \in K[x]$ de multiplicidade m se, e somente se, existe $q(x) \in L[x]$, tal que em $L[x]$

$$f(x) = (x-\beta)^m q(x), \text{ com } q(\beta) \neq 0.$$

Vejamos no exemplo a seguir como determinar a multiplicidade de uma raiz de um polinômio.

Exemplo 45
Seja $f(x) = x^7 - x^6 + x^5 - x^4 - x^3 + x^2 - x + 1 \in \mathbb{Q}[x]$. Verificamos que $f(1) = 0$. Vamos determinar a multiplicidade da raiz $\beta = 1$. Primeiramente, $x-1$ divide $f(x)$ em $\mathbb{Q}[x]$. Fazemos a divisão e obtemos:

$$f(x) = (x-1)(x^6 + x^4 - x^2 - 1).$$

Substituindo $\beta = 1$ em $g(x) = x^6+x^4-x^2-1$, obtemos $g(1) = 0$. Logo, $x-1$ divide $g(x)$ em $\mathbb{Q}[x]$. Escrevemos $g(x) = (x-1)(x^5+x^4+2x^3+2x^2+x+1)$. Logo,

$$f(x) = (x-1)^2(x^5 + x^4 + 2x^3 + 2x^2 + x + 1).$$

O polinômio $q(x) = x^5 + x^4 + 2x^3 + 2x^2 + x + 1$ é tal que $q(1) \neq 0$. Logo, $\beta = 1$ tem multiplicidade 2 em $f(x)$.

Verifique que $f(x)$ só tem mais uma raiz em $\mathbb{Q}$ e a sua fatoração em mônicos irredutíveis é

$$\begin{cases} f(x) = (x-1)^2(x+1)(x^2+1)^2, \text{ em } \mathbb{Q}[x] \\ f(x) = (x-1)^2(x+1)(x-i)^2(x+i)^2, \text{ em } \mathbb{C}[x]. \end{cases}$$

Em $\mathbb{C}$, $f(x)$ tem mais duas raízes, ambas com multiplicidade 2.

Exercícios

1. Calcule o $\text{mdc}(f(x), g(x))$ dos seguintes polinômios em $\mathbb{Q}[x]$:

   (a) $f(x) = x^3 - 6x^2 + x + 4$ e $g(x) = x^5 - 6x + 1$.

   (b) $f(x) = x^2 + 1$ e $g(x) = x^6 + x^3 + x + 1$.

2. Determine quais dos conjuntos $I \subset \mathbb{Q}[x]$ são ideais de $\mathbb{Q}[x]$ e, no caso afirmativo, calcule $p(x) \in I$ mônico tal que $I = p(x)\mathbb{Q}[x]$:

(a) $I = \{f(x) \in \mathbb{Q}[x] \; ; \; f(1) = f(7) = 0\}$

(b) $I = \{f(x) \in \mathbb{Q}[x] \; ; \; f(2) = 0 \text{ e } f(5) \neq 0\}$

(c) $I = \{f(x) \in \mathbb{Q}[x] \; ; \; f(\sqrt{2}) = 0\}$

(d) $I = \{f(x) \in \mathbb{Q}[x] \; ; \; f(4) = 0 \text{ e } f(0) = f(1)\}$

3. No Exercício anterior, mostre que o ideal do item (a) não é primo e o do item (c) é primo.

4. (a) Mostre que $I = \{f(x) \in \mathbb{R}[x] \; ; \; f(\sqrt{2}) = 0\}$ é um ideal primo de $\mathbb{R}[x]$ e dê o polinômio mônico de menor grau em I.

   (b) Mostre que $I = \{f(x) \in \mathbb{R}[x] \; ; \; f(\sqrt{2}) = f(-\sqrt{2}) = 0\}$ é um ideal de $\mathbb{R}[x]$, não é ideal primo e dê o polinômio mônico de menor grau em I.

5. Sejam D um domínio e $a \in D$, $a \neq 0$.

   (a) Mostre que $x - a$ divide $x^n - a^n$ em $D[x]$.

   (b) Quais as condições para que $x + a$ divida $x^n + a^n$ em $D[x]$?

   (c) Quais as condições para que $x + a$ divida $x^n - a^n$ em $D[x]$?

6. Sem efetuar a divisão, mostre que:

   (a) $x^2 + 1$ divide $2x^6 + 2x^5 + x^4 + 2x^3 + x^2 + 2$ em $\mathbb{Z}[x]$.

   (b) $x^2 + x + 1$ divide $x^6 + 4x^5 + 3x^4 + 2x^3 + x + 1$ em $\mathbb{Z}[x]$.

   (c) $x^4 + x^3 + x^2 + x + 1$ divide $x^{444} + x^{333} + x^{222} + x^{111} + 1$ em $\mathbb{Z}[x]$.

   (d) Para $n \geq 1$, $(x+1)^{2n} - x^{2n} - 2x - 1$ é divisível por $x(x+1)(2x+1)$ em $\mathbb{Q}[x]$.

7. Sejam $p_1(x), \ldots, p_s(x)$ em $K[x]$, onde K é um corpo. Sejam, respectivamente, $r_1(x), \ldots, r_s(x)$ os restos da divisão desses polinômios por $t(x) \neq 0$. Sejam $a_1, \ldots, a_s \in K$. Mostre que o resto da divisão de $p(x) = \sum_{j=1}^{s} a_j p_j(x)$ por $t(x)$ é o polinômio $r(x) = \sum_{j=1}^{s} a_j r_j(x)$.

8. Determine o mdc dos polinômios em $\mathbb{Q}[x]$:

   (a) $x^5 + 4x^3 + 3x^2 + x + 1$ e $x^3 + 2x^2 + x + 1$.

   (b) $x^5 + 10x^4 + 40x^3 + 80x^2 + 80x + 32$ e $x^3 + 6x^2 + 12x + 8$.

   (c) $x^4 + x^3 + 2x^2 + x + 1$ e $x^4 + 3x^3 + 5x^2 + 3x + 4$.

(d) $x^3 - x^2 - x - 2$ e $x^3 - 3x - 2$.

9. Seja K um subcorpo de F. Sejam $f(x)$ e $g(x)$ em $K[x]$ e $\beta \in F$.

   Mostre que β é raiz comum de $f(x)$ e $g(x)$ se, e somente se, β é raiz de $\text{mdc}(f(x), g(x))$.

10. Ache as raízes comuns em $\mathbb{C}$ dos pares de polinômios do Exercício 8.

11. Seja K um corpo.

    (a) Mostre que todo polinômio de grau 1 é irredutível em $K[x]$.

    (b) Sejam $a, b \in K$ com $a \neq b$. Mostre que para todos $n, m \geq 1$ os polinômios $(x-a)^n$ e $(x-b)^m$ são primos entre si.

    (c) Mostre que se K é algebricamente fechado, então os únicos polinômios irredutíveis em $K[x]$ são os polinômios de grau 1.

12. Sejam K um corpo e $f(x) \in K[x]$.

    (a) Seja $\text{grau}(f(x)) > 1$. Mostre que se $f(x)$ tem uma raiz em K, então $f(x)$ é redutível em $K[x]$.

    Dê um exemplo mostrando que não vale a recíproca.

    (b) Seja $f(x)$ de grau 2 ou 3. Mostre que $f(x)$ é redutível em $K[x]$ se, e somente se, tem raiz em K.

    Vale esse resultado para polinômio de grau maior do que 3 ?

    (c) Dê exemplos de um corpo K e um polinômio $f(x) \in K[x]$ com $\text{grau}(f(x)) = 4$, tal que $f(x)$ não é irredutível em $K[x]$ e $f(x)$ não tem raízes em K. Conclua que não vale a recíproca do item (a) e o item (b) é falso para polinômio de grau maior do que 3.

13. Determine todos os polinômios mônicos irredutíveis de grau menor ou igual a 4 em $\mathbb{Z}_2[x]$.

14. Determine todos os polinômios mônicos irredutíveis de grau menor ou igual a 3 em $\mathbb{Z}_3[x]$.

15. Decomponha os seguintes polinômios como produto de polinômios mônicos irredutíveis em $\mathbb{Z}_3[x]$:

    (a) $f(x) = x^2 + x + \overline{1}$ (b) $f(x) = x^3 + x + \overline{2}$

    (c) $f(x) = \overline{2}x^3 + \overline{2}x^2 + x + \overline{1}$ (d) $f(x) = x^4 + x^3 + x + \overline{1}$

Fatoração em $\mathbb{C}[x]$ e $\mathbb{R}[x]$

Na França, o Teorema Fundamental da Álgebra é conhecido como Teorema de D'Alembert, pois ele dispendeu muito tempo e esforço tentando demonstrá-lo.

Como conseqüência do corpo dos números complexos ser algebricamente fechado, temos o Teorema Fundamental da Álgebra, demonstrado por Gauss e conhecido hoje na França como Teorema de D'Alembert.

Teorema 6 (Teorema Fundamental da Álgebra)
Todo polinômio $f(x)$ de grau $n \geq 1$ com coeficientes complexos se escreve de modo único, a menos da ordem dos fatores, como:

$$f(x) = a(x-\beta_1)^{r_1} \cdots (x-\beta_t)^{r_t}, \text{ onde } r_1 + \cdots + r_t = n,$$

com $a, \beta_1, \ldots, \beta_t \in \mathbb{C}$, $a \neq 0$ e $\beta_j \neq \beta_k$, se $j \neq k$.

Em linguagem matemática, a expressão *a menos de* é largamente utilizada. Exprime a idéia de: salvo ou excetuada.

As raízes distintas de $f(x)$ são $\beta_1, \ldots \beta_t$, e o natural r_j, $j = 1, \ldots, t$ é a multiplicidade da raiz β_j.

Como grau$(f(x)) = r_1 + \cdots + r_t$, segue que todo polinômio $f(x)$ de grau $n \geq 1$ com coeficientes complexos tem exatamente n raízes em $\mathbb{C}$, contadas com as suas multiplicidades.

Note que a é o coeficiente líder de $f(x)$.

Curiosidades sobre a vida e trabalhos de Jean le Rond D'Alembert:

era filho ilegítimo de uma aristocrata e foi por ela abandonado nos degraus da Igreja St. Jean Le Rond (daí a origem de seu nome), mas seu pai conseguiu que uma família humilde o acolhesse, deu apoio à sua educação e deixou, com a sua morte em 1726, dinheiro suficiente para a sua instrução.

D'Alembert e Euler trocaram correspondência sobre tópicos de interesse mútuo, entre 1750 e 1760, e D'Alembert publicava seus trabalhos na Academia de Berlim. Foi convidado para a presidência da Academia e recusou, em respeito a Euler. De 1761 a 1780, época em que esteve estremecido com Euler, publicou seus trabalhos em 8 volumes como *Opuscules Mathématiques*.

Nosso objetivo é obter a decomposição de $f(x) \in \mathbb{R}[x]$ em produto de fatores mônicos irredutíveis em $\mathbb{R}[x]$, a partir da sua fatoração em $\mathbb{C}[x]$.

Vamos aprender algumas propriedades de polinômios com coeficientes complexos.

Definição 17 (Polinômio conjugado)
Seja $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$. O *polinômio conjugado* de $f(x)$ é

$$\overline{f}(x) = \overline{a_n} x^n + \cdots + \overline{a_1} x + \overline{a_0},$$

onde $\overline{a_j}$ é o conjugado de a_j, $j = 0, \ldots, n$.

Proposição 10 (Propriedades da conjugação)
Sejam $f(x), g(x), h(x) \in \mathbb{C}[x]$. Valem as seguintes propriedades:
(i) se $f(x) = g(x) + h(x)$, então $\overline{f}(x) = \overline{g}(x) + \overline{h}(x)$;
(ii) se $f(x) = g(x) \cdot h(x)$, então $\overline{f}(x) = \overline{g}(x) \cdot \overline{h}(x)$;
(iii) $\overline{f}(x) = f(x)$ se, e somente se, $f(x) \in \mathbb{R}[x]$;
(iv) se $\beta \in \mathbb{C}$, então $\overline{f}(\overline{\beta}) = \overline{f(\beta)}$.

Demonstração:

(i) Sejam $f(x) = \sum_{j=0}^{n} a_j x^j$, $g(x) = \sum_{j=0}^{n} b_j x^j$ e $h(x) = \sum_{j=0}^{n} c_j x^j$ em $\mathbb{C}[x]$, com $f(x) = g(x)+h(x)$. Da definição de adição de polinômios, temos $a_j = b_j + c_j$, para $j = 0, \ldots, n$. Logo, $\overline{a_j} = \overline{b_j + c_j} = \overline{b_j} + \overline{c_j}$. Da definição de conjugado, segue que $\overline{f}(x) = \sum_{j=0}^{n} \overline{a_j} x^j$, $\overline{g}(x) = \sum_{j=0}^{n} \overline{b_j} x^j$ e $\overline{h}(x) = \sum_{j=0}^{n} \overline{c_j} x^j$. Usando a definição da adição em $\mathbb{C}[x]$, temos $\overline{g}(x) + \overline{h}(x) = \overline{f}(x)$.

(ii) Sejam $f(x) = \sum_{j=0}^{s} a_j x^j$, $g(x) = \sum_{j=0}^{n} b_j x^j$ e $h(x) = \sum_{j=0}^{m} c_j x^j$ em $\mathbb{C}[x]$, com $f(x) = g(x) \cdot h(x)$. Da definição de multiplicação de polinômios, temos $a_j = \sum_{\lambda+\mu=j} b_\lambda c_\mu$, para $j = 0, \ldots, s$. Logo, $\overline{a_j} = \overline{\sum_{\lambda+\mu=j} b_\lambda c_\mu} = \sum_{\lambda+\mu=j} \overline{b_\lambda}\overline{c_\mu}$, para $j = 0, \ldots, s$. Da definição de conjugado, segue que $\overline{f}(x) = \sum_{j=0}^{s} \overline{a_j} x^j$, $\overline{g}(x) = \sum_{j=0}^{n} \overline{b_j} x^j$ e $\overline{h}(x) = \sum_{j=0}^{m} \overline{c_j} x^j$. Usando a definição da multiplicação em $\mathbb{C}[x]$, temos $\overline{g}(x) \cdot \overline{h}(x) = \overline{f}(x)$.

(iii) Seja $f(x) = \sum_{j=0}^{n} a_j x^j$. Então, $\overline{f}(x) = \sum_{j=0}^{n} \overline{a_j} x^j$. Assim,

$$\begin{aligned} f(x) = \overline{f}(x) &\iff a_j = \overline{a_j}, \text{ para todo } j = 0, \ldots, n \\ &\iff a_j \in \mathbb{R}, \text{ para todo } j = 0, \ldots, n \\ &\iff f(x) \in \mathbb{R}[x]. \end{aligned}$$

(iv) Seja $f(x) = \sum_{j=0}^{n} a_j x^j$. Então, $\overline{f}(x) = \sum_{j=0}^{n} \overline{a_j} x^j$. Seja $\beta \in \mathbb{C}$, assim

$$\begin{aligned} \overline{f}(\overline{\beta}) &= \sum_{j=0}^{n} \overline{a_j}\overline{\beta}^j \\ &= \overline{\sum_{j=0}^{n} a_j \beta^j} \\ &= \overline{f(\beta)} \qquad \blacksquare \end{aligned}$$

Usamos na segunda igualdade que o produto dos conjugados é o conjugado do produto; na terceira, que a soma dos conjugados é o conjugado da soma e na última, a definição de avaliação de $f(x)$ em β.

Corolário 6

Seja $\beta \in \mathbb{C}$ uma raiz de $f(x) \in \mathbb{C}[x]$ de multiplicidade m. Então, $\overline{\beta}$ é uma raiz de $\overline{f}(x)$ com multiplicidade m.

Demonstração: Seja $\beta \in \mathbb{C}$ uma raiz de $f(x) \in \mathbb{C}[x]$ de multiplicidade m. Então, $f(x) = (x-\beta)^m q(x)$ com $q(\beta) \neq 0$. De (ii) na Proposição anterior, segue que $\overline{f}(x) = (x-\overline{\beta})^m \overline{q}(x)$ e de (iv), $\overline{q}(\overline{\beta}) = \overline{q(\beta)} \neq \overline{0} = 0$, mostrando que $\overline{\beta}$ é raiz de $\overline{f}(x)$ de multiplicidade m.

Proposição 11

Seja $f(x) \in \mathbb{R}[x]$. Se $\beta \in \mathbb{C}$ é uma raiz de $f(x)$ com multiplicidade m, então $\overline{\beta}$ também é raiz de $f(x)$ de multiplicidade m.

Demonstração: Se $f(x) \in \mathbb{R}[x]$, temos em $\mathbb{C}[x]$

$$f(x) = (x-\beta)^m q(x), \text{ com } q(\beta) \neq 0.$$

Então, $f(x) = \overline{f}(x) = (x-\overline{\beta})^m \overline{q}(x)$ com $\overline{q}(\overline{\beta}) = \overline{q(\beta)} \neq \overline{0} = 0$, mostrando que $\overline{\beta}$ também é raiz de $f(x)$ de multiplicidade m. ■

Corolário 7

As raízes complexas não-reais de $f(x) \in \mathbb{R}[x]$ ocorrem aos pares. Todo polinômio de grau ímpar em $\mathbb{R}[x]$ tem pelo menos uma raiz real.

Demonstração: Seja $f(x) \in \mathbb{R}[x]$ e seja $\beta \in \mathbb{C}$, $\beta \notin \mathbb{R}$, tal que $f(\beta) = 0$. Então, $\beta \neq \overline{\beta}$ e $f(\beta) = 0$ se, e somente se, $f(\overline{\beta}) = 0$, ambas com a mesma multiplicidade. Portanto, se o polinômio tem grau ímpar, tem de ter pelo menos uma raiz real. ■

Proposição 12

Os polinômios mônicos irredutíveis em $\mathbb{R}[x]$ são da forma $x-a$, $a \in \mathbb{R}$, ou x^2+bx+c, com $b^2-4c < 0$. Todo polinômio $f(x) \in \mathbb{R}[x]$, com $\text{grau}(f(x)) > 2$, é redutível em $\mathbb{R}[x]$.

Demonstração: Já sabemos que os polinômios $x-a$, onde $a \in K$, são irredutíveis em qualquer corpo K.

Um polinômio de grau 2 com coeficientes em qualquer corpo K é irredutível em $K[x]$ se, e somente se, não tem raízes em K.

Seja $f(x) = x^2 + bx + c \in \mathbb{R}[x]$. Existe $\beta \in \mathbb{C}$ uma raiz de $f(x)$.

$f(x)$ é irredutível em $\mathbb{R}[x]$	se, e somente se,	$\beta \in \mathbb{C}$ e $\beta \notin \mathbb{R}$
	se, e somente se,	$\beta \neq \overline{\beta}$ são as raízes de $f(x)$
	se, e somente se,	$\Delta = b^2 - 4c < 0$.

Nesse caso, $x^2 + bx + c = (x-\beta)(x-\overline{\beta}) = x^2 - (\beta+\overline{\beta})x + \beta\overline{\beta}$ e

Jean Le Rond D'Alembert 1717 - 1783, França.

D'Alembert tinha instrução nas áreas de Direito, Medicina, Ciência e Matemática. Com apenas 24 anos, foi eleito para a *Académie de Sciences* da França. Entre 1751 e 1772, colaborou com Diderot na edição da primeira enciclopédia: *Encyclopédie raisonné des sciences, des arts et des métiers*, onde publicou diversos trabalhos de Matemática. Em 1744, publicou *Traité de l'equilibre et du mouvement des fluides* e, em 1747, seu trabalho em vibração de cordas, onde aparece pela primeira vez a equação da onda. Deu importantes contribuições à Matemática: foi o primeiro a entender a importância das funções e da teoria dos limites; a definir a derivada como o limite de um quociente de incrementos; e pioneiro no estudo de equações diferenciais parciais.

$$\begin{aligned}\Delta &= (\beta+\overline{\beta})^2-4\beta\overline{\beta}\\ &= \beta^2+2\beta\overline{\beta}+\overline{\beta}^2-4\beta\overline{\beta}\\ &= \beta^2-2\beta\overline{\beta}+\overline{\beta}^2\\ &= (\beta-\overline{\beta})^2\\ &= (2\,\mathrm{Im}(\beta)i)^2\\ &= -4\big(\mathrm{Im}(\beta)\big)^2<0.\end{aligned}$$

Seja $\beta\in\mathbb{C}$.
$\beta\notin\mathbb{R}\iff \mathrm{Im}(\beta)\neq 0$.

Para demonstrar a última afirmação seja $f(x)\in\mathbb{R}[x]$ tal que $\mathrm{grau}(f(x))>2$. Então, existe $\beta\in\mathbb{C}$ uma raiz de $f(x)$. Temos dois casos a considerar:

Caso 1: Se $\beta\in\mathbb{R}$, então $x-\beta$ divide $f(x)$ em $\mathbb{R}[x]$. Logo, $f(x)=(x-\beta)q(x)$, com $q(x)\in\mathbb{R}[x]$, e $f(x)$ é redutível em $\mathbb{R}[x]$.

Caso 2: Se $\beta\in\mathbb{C}$ e $\beta\notin\mathbb{R}$, então $\beta\neq\overline{\beta}$ e $\overline{\beta}$ também é raiz de $f(x)$. Logo, $(x-\beta)(x-\overline{\beta})$ divide $f(x)$ em $\mathbb{C}[x]$. Entretanto,

$$\begin{aligned}(x-\beta)(x-\overline{\beta}) &= x^2-(\beta+\overline{\beta})x+\beta\overline{\beta}\\ &= x^2-2\,\mathrm{Re}(\beta)x+\mid\beta\mid^2\in\mathbb{R}[x],\end{aligned}$$

logo $(x-\beta)(x-\overline{\beta})$ divide $f(x)$ em $\mathbb{R}[x]$. ■

Quer saber mais sobre Gauss?

A habilidade de Gauss com a Matemática foi percebida por seu professor quando ele tinha sete anos. Ao ser perguntado qual a soma dos números naturais de 1 a 100, Gauss imediatamente respondeu: são 50 pares de números somando 101!

Gauss publicou, dois anos após a obtenção do seu doutorado, um dos clássicos da literatura matemática, *Disquisitiones Arithmeticae* e contribuiu em diversas áreas: Geometria Diferencial (no estudo das superfícies com suas idéias sobre curvatura e seu interesse sobre as geodésicas); Teoria dos Números; Análise Matemática (apresentou critérios de convergência de séries) e Astronomia.

Por que o *Disquisitiones Arithmeticae* é um dos clássicos da literatura matemática?
Nessa obra aparecem: os conceitos de congruência de inteiros e classe de restos; uma demonstração do Teorema Fundamental da Aritmética e números da forma

$\mathbb{Z}[i]=\{\,a+bi\mid a,b\in\mathbb{Z}\,\}$,

hoje conhecidos como os inteiros de Gauss.

Agora, estamos prontos para apresentar o Teorema Fundamental da Álgebra, ou o Teorema de D'Alembert, demonstrado por Gauss de quatro maneiras diferentes.

Vejamos algumas conseqüências do Teorema 6.

Estamos interessados nos polinômios com coeficientes reais. Vamos enunciar o Teorema Fundamental da Álgebra para os polinômios com coeficientes reais.

Teorema 7 (Teorema Fundamental da Álgebra em $\mathbb{R}[x]$)
Todo polinômio $f(x)$ de grau $n\geq 1$ com coeficientes reais se escreve de modo único, a menos da ordem dos fatores, como:

$$\boxed{f(x)=a(x-\beta_1)^{r_1}\cdots(x-\beta_t)^{r_t}(x^2+b_1x+c_1)^{n_1}\cdots(x^2+b_sx+c_s)^{n_s},}$$

onde $a\in\mathbb{R}$, $a\neq 0$, é o coeficiente líder de $f(x)$; $\beta_1,\ldots,\beta_t$ são as raízes reais distintas de $f(x)$; $x^2+b_1x+c_1,\ldots,x^2+b_sx+c_s$ são polinômios distintos com coeficientes reais tais que ${b_j}^2-4c_j<0$, para todo $j=1,\ldots,s$, e $r_1+\cdots+r_t+2n_1+\cdots+2n_s=n$.

Exemplo 46

Vamos determinar a decomposição de $f(x) = 3x^8 - 3$ em produto de potências de fatores mônicos irredutíveis em $\mathbb{R}[x]$.

Lembrando do produto notável $a^2 - b^2 = (a - b)(a + b)$, temos

$$x^8 - 1 = (x^4 - 1)(x^4 + 1),\ x^4 - 1 = (x^2 - 1)(x^2 + 1)$$

e

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

Combinando essas decomposições, obtemos:

$$f(x) = 3(x^8 - 1) = 3(x - 1)(x + 1)(x^2 + 1)(x^4 + 1).$$

Agora devemos fatorar $x^4 + 1$ (Veja a observação na margem).

Não esqueça:

Se $f(x) \in \mathbb{R}[x]$ e seu grau é maior ou igual a 2, então $f(x)$ é divisível por algum polinômio do tipo $x - a$ ou $x^2 + bx + c$ com $b^2 - 4c < 0$.

As raízes $\beta \in \mathbb{C}$ desse polinômio são as raízes complexas quartas de -1, pois $\beta^4 + 1 = 0$ se, e somente se, $\beta^4 = -1$. Vamos determiná-las. O argumento de -1 é π. Assim, as raízes complexas quartas de -1 têm argumentos $\phi_k = \frac{\pi + 2\pi k}{4} = \frac{\pi(2k+1)}{4}$, $k = 0, 1, 2, 3$ e módulo $\rho = \sqrt[4]{|-1|} = \sqrt[4]{1} = 1$. Logo,

$$\begin{aligned}
\phi_0 = \tfrac{\pi}{4} &\implies z_0 = \cos\tfrac{\pi}{4} + i\,\mathrm{sen}\,\tfrac{\pi}{4} = \tfrac{\sqrt{2}}{2} + \tfrac{\sqrt{2}}{2}i \\
\phi_1 = \tfrac{3\pi}{4} &\implies z_1 = \cos\tfrac{3\pi}{4} + i\,\mathrm{sen}\,\tfrac{3\pi}{4} = -\tfrac{\sqrt{2}}{2} + \tfrac{\sqrt{2}}{2}i \\
\phi_2 = \tfrac{5\pi}{4} &\implies z_2 = \cos\tfrac{5\pi}{4} + i\,\mathrm{sen}\,\tfrac{5\pi}{4} = -\tfrac{\sqrt{2}}{2} - \tfrac{\sqrt{2}}{2}i \\
\phi_3 = \tfrac{7\pi}{4} &\implies z_3 = \cos\tfrac{7\pi}{4} + i\,\mathrm{sen}\,\tfrac{7\pi}{4} = \tfrac{\sqrt{2}}{2} - \tfrac{\sqrt{2}}{2}i, \text{ então}
\end{aligned}$$

$$x^4 + 1 = (x - z_0)(x - z_1)(x - z_2)(x - z_3) \text{ em } \mathbb{C}[x].$$

Note que $\overline{z_0} = z_3$ e $\overline{z_1} = z_2$. Portanto, z_0 e z_3 são raízes do polinômio $(x - z_0)(x - \overline{z_0}) = x^2 - \sqrt{2}x + 1$ e z_1 e z_2 são raízes do polinômio $(x - z_1)(x - \overline{z_1}) = x^2 + \sqrt{2}x + 1$. Logo,

$$x^4 + 1 = (x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1) \quad \text{em } \mathbb{R}[x].$$

Como $x^2 + 1 = (x - i)(x + i)$ em $\mathbb{C}[x]$, então

$$3x^8 - 3 = 3(x - 1)(x + 1)(x - i)(x + i)(x - z_0)(x - z_1)(x - z_2)(x - z_3),$$

em $\mathbb{C}[x]$ e

$$3x^8 - 3 = 3(x - 1)(x + 1)(x^2 + 1)(x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1), \text{ em } \mathbb{R}[x].$$

Obtemos a fatoração em irredutíveis mônicos em $\mathbb{R}[x]$ a partir da fatoração em irredutíveis mônicos em $\mathbb{C}[x]$.

Exemplo 47

Seja $f(x) = x^4 - 2 \in \mathbb{R}[x]$.

Observamos que só há dois números reais cuja quarta potência é 2: $\sqrt[4]{2}$ e $-\sqrt[4]{2}$. Esses números reais são raízes de $f(x)$, o que é equivalente a $(x - \sqrt[4]{2})(x + \sqrt[4]{2})$ dividir $f(x)$. Fazendo a divisão, obtemos:

$$f(x) = x^4 - 2 = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x^2 + \sqrt{2}).$$

Entretanto, no conjunto dos números complexos há quatro números cuja quarta potência é 2: $-\sqrt[4]{2}$, $\sqrt[4]{2}$, $-\sqrt[4]{2}i$ e $\sqrt[4]{2}i$, que são as raízes complexas

Trace o círculo de raio $\sqrt[4]{2}$ e visualize as raízes complexas quartas de 2.

quartas de 2.

Para determiná-los, tomamos os argumentos $\phi_k = \frac{2\pi\cdot k}{4}, k = 0,1,2,3$, obtendo

$$\phi_0 = 0, \quad \phi_1 = \frac{\pi}{2}, \quad \phi_2 = \pi \quad \text{e} \quad \phi_3 = \frac{3\pi}{2}.$$

Lembre que ...
Geometricamente, as raízes complexas n–ésimas de um número real $r > 0$ dividem o círculo de raio $\sqrt[n]{r}$ em n partes iguais.

Escrevendo o módulo $\rho = \sqrt[4]{2}$ das raízes complexas quartas de 2, temos as quatro raízes complexas quartas de 2 dadas por:

$$z_0 = \sqrt[4]{2}, \quad z_1 = \sqrt[4]{2}i, \quad z_2 = -\sqrt[4]{2} \quad \text{e} \quad z_3 = -\sqrt[4]{2}i.$$

Os números complexos conjugados $\sqrt[4]{2}i$ e $-\sqrt[4]{2}i$ são as raízes em $\mathbb{C}$ do polinômio do $2^{\underline{o}}$ grau $x^2 + \sqrt{2}$ com coeficientes reais.

Em $\mathbb{C}$ a equação $x^4 - 2 = 0$ tem quatro soluções, enquanto em $\mathbb{R}$ há apenas duas soluções.

Exemplo 48

Seja $f(x) = -2x^9 + 32x^6 - 128x^3 \in \mathbb{R}[x]$. Quais são as raízes de $f(x)$?

Colocando -2 em evidência, temos $f(x) = -2(x^9 - 16x^6 + 64x^3)$ e vemos que $f(x)$ é divisível por x^3. Portanto,

$$f(x) = -2x^3(x^6 - 16x^3 + 64).$$

O número $a = 0$ é uma raiz de $f(x)$ com multiplicidade 3. As outras raízes de $f(x)$, forçosamente, são raízes de $x^6 - 16x^3 + 64$, pois

$$f(\alpha) = -2\alpha^3(\alpha^6 - 16\alpha^3 + 64) = 0 \iff \alpha^3 = 0 \text{ ou } \alpha^6 - 16\alpha^3 + 64 = 0$$
$$\iff \alpha = 0 \text{ ou } \alpha^6 - 16\alpha^3 + 64 = 0\,.$$

Não esqueça que:
Se $a, b \in \mathbb{R}$, então $a \cdot b = 0 \iff a = 0$ ou $b = 0$.
Se $z, w \in \mathbb{C}$, então $z \cdot w = 0 \iff z = 0$ ou $w = 0$.

Lembre dos produtos notáveis:
$(a+b)^2 = a^2 + 2ab + b^2$,
$(a-b)^2 = a^2 - 2ab + b^2$.
$a^2 - b^2 = (a-b)(a+b)$.

Para continuar a pesquisa das raízes de $f(x)$, devemos buscar agora as raízes do fator $x^6 - 16x^3 + 64$. Observando as potências de x e os coeficientes, lembramos de um produto notável e escrevemos

$$x^6 - 16x^3 + 64 = (x^3 - 8)^2.$$

Portanto, as raízes de $x^6 - 16x^3 + 64$ são as raízes de $(x^3 - 8)^2$. Assim, basta determinar as raízes de $x^3 - 8$, sem esquecer que a multiplicidade delas no polinômio $x^6 - 16x^3 + 64$ é 2.

O polinômio $x^3 - 8$ tem três raízes em $\mathbb{C}$, as raízes complexas cúbicas de 8. Apenas uma delas é um número real e as outras duas são números complexos não-reais. Para determiná-las, calculamos o módulo $\rho = \sqrt[3]{8} = 2$ e os argumentos $\phi_k = \frac{2\pi k}{3}$, com $k = 0,1,2$. Obtemos, $\phi_0 = 0$, $\phi_1 = \frac{2\pi}{3}$ e $\phi_2 = \frac{4\pi}{3}$.

Assim, $z_0 = 2$, $z_1 = 2(\cos\frac{2\pi}{3} + i\,\text{sen}\,\frac{2\pi}{3}) = 2(-\frac{1}{2} + i\frac{\sqrt{3}}{2}) = -1 + \sqrt{3}i$ e $z_2 = 2(\cos\frac{4\pi}{3} + i\,\text{sen}\,\frac{4\pi}{3}) = 2(-\frac{1}{2} - i\frac{\sqrt{3}}{2}) = -1 - \sqrt{3}i$.

Note que

$$z_2 = \overline{z}_1\,,\ z_1 + z_2 = z_1 + \overline{z}_1 = -2 \quad \text{e} \quad z_1 \cdot z_2 = z_1 \cdot \overline{z}_1 = |z_1|^2 = 4\,.$$

Logo, z_1 e z_2 são raízes do polinômio do $2^{\underline{o}}$ grau $x^2+2x+4 \in \mathbb{R}[x]$.

Lembre que:
$(x-a)(x-b) = x^2-(a+b)x+ab$.

Fazendo a divisão euclidiana de x^3-8 por $x-2$, temos

$$x^3-8=(x-2)(x^2+2x+4) \quad \text{e} \quad (x^3-8)^2=(x-2)^2(x^2+2x+4)^2.$$

Portanto,

$$-2x^9+32x^6-128x^3=-2x^3(x^3-8)^2=-2x^3(x-2)^2(x^2+2x+4)^2.$$

Esse polinômio de grau 9 tem duas raízes reais: a raiz 0 com multiplicidade 3 e a raiz 2 com multiplicidade 2. No conjunto dos números complexos temos, além dessas, as raízes $-1+\sqrt{3}i$ e $-1-\sqrt{3}i$, ambas com multiplicidade 2, porque $(x^2+2x+4)^2$ divide $f(x)$, mas $(x^2+2x+4)^3$ não divide $f(x)$. Contando as raízes com as suas multiplicidades, temos $3+2+2+2=9=\text{grau}(f(x))$ raízes complexas.

Exemplo 49

O polinômio $f(x)=x^n-a \in \mathbb{C}[x]$ é fácil de ser decomposto em produto de fatores lineares em $\mathbb{C}[x]$. Basta conhecer uma de suas raízes para determinar todas elas.

Seja $\beta \in \mathbb{C}$ uma raiz de $f(x)$. Tomando $\omega=\cos\frac{2\pi}{n}+i\,\text{sen}\,\frac{2\pi}{n}$, raiz primitiva n-ésima da unidade, temos que ω^j, com $j=0,1,\ldots,n-1$, são as n raízes complexas da unidade. Assim,

$$\left(\beta\omega^j\right)^n=\beta^n\omega^{jn}=a\left(\omega^n\right)^j=a\cdot 1^j=a.$$

$f(\beta)=\beta^n-a=0 \iff \beta^n=a$.

Logo, $\beta, \beta\omega, \ldots, \beta\omega^{n-1}$ são as n raízes complexas de x^n-a e em $\mathbb{C}[x]$ temos

$$x^n-a=\prod_{j=0}^{n-1}(x-\beta\omega^j)=(x-\beta)(x-\beta\omega)\cdot\ldots\cdot(x-\beta\omega^{n-1}).$$

Exemplo 50

Vamos fatorar $f(x)=x^6-2$ em $\mathbb{C}[x]$ e em $\mathbb{R}[x]$.

$\sqrt[6]{2}$ é uma raiz real de $f(x)$. As raízes complexas de $f(x)$ são $\sqrt[6]{2}\omega^j$, com $j=0,1,\ldots,5$, onde $\omega=\cos\frac{2\pi}{6}+i\,\text{sen}\,\frac{2\pi}{6}=\cos\frac{\pi}{3}+i\,\text{sen}\,\frac{\pi}{3}$ é uma raiz primitiva 6-ésima da unidade. Como ω está na forma polar, determinamos suas potências facilmente. Temos que

$$\omega^j=\cos\tfrac{\pi j}{3}+i\,\text{sen}\,\tfrac{\pi j}{3},\ j=0,\ldots 5,$$

Visualize no círculo trigonométrico, fazendo a divisão em 6 partes iguais, no sentido positivo das rotações, a partir de $A=(1,0)$.

cujos valores são

$$\begin{array}{lll} \omega^0=1 & \omega=\frac{1}{2}+i\frac{\sqrt{3}}{2} & \omega^2=-\frac{1}{2}+i\frac{\sqrt{3}}{2} \\ \omega^3=-1 & \omega^4=-\frac{1}{2}-i\frac{\sqrt{3}}{2} & \omega^5=\frac{1}{2}-i\frac{\sqrt{3}}{2} \end{array}$$

As raízes complexas de $f(x)$ são

$$\begin{array}{lll} \beta_0 = \sqrt[6]{2} & \beta_1 = \sqrt[6]{2}\left(\frac{1}{2} + i\frac{\sqrt{3}}{2}\right) & \beta_2 = \sqrt[6]{2}\left(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\right) \\ \beta_3 = -\sqrt[6]{2} & \beta_4 = \sqrt[6]{2}\left(-\frac{1}{2} - i\frac{\sqrt{3}}{2}\right) & \beta_5 = \sqrt[6]{2}\left(\frac{1}{2} - i\frac{\sqrt{3}}{2}\right). \end{array}$$

Então,

$$x^6 - 2 = (x - \beta_0)(x - \beta_1)(x - \beta_2)(x - \beta_3)(x - \beta_4)(x - \beta_5), \text{ em } \mathbb{C}[x].$$

Seja $c = \sqrt[6]{2}$. Observando que $\overline{\beta_1} = \overline{c\omega} = c\omega^5 = \beta_5$, $\overline{\beta_2} = \overline{c\omega^2} = c\omega^4 = \beta_4$, obtemos os fatores irredutíveis mônicos em $\mathbb{R}[x]$ do segundo grau
$(x - c\omega)(x - c\omega^5) = x^2 - c(\omega + \omega^5)x + c^2 = x^2 - cx + c^2$ e
$(x - c\omega^2)(x - c\omega^4) = x^2 - c(\omega^2 + \omega^4)x + c^2 = x^2 + cx + c^2$.
Logo,

$$x^6 - 2 = (x - \sqrt[6]{2})(x + \sqrt[6]{2})(x^2 - \sqrt[6]{2}x + \sqrt[3]{2})(x^2 + \sqrt[6]{2}x + \sqrt[3]{2}), \text{ em } \mathbb{R}[x].$$

Exemplo 51
Vamos determinar a fatoração em polinômios mônicos e irredutíveis em $\mathbb{R}[x]$ e em $\mathbb{C}[x]$ de $f(x) = x^4 + 16$.

As raízes complexas de $f(x)$ são as raízes quartas de -16. Escrevendo -16 na forma polar, obtemos $-16 = 16(\cos\pi + i\,\mathrm{sen}\,\pi)$, com $r = 16$ e $\arg(-16) = \pi$. Portanto, as raízes complexas de $f(x)$ têm $\rho = \sqrt[4]{r} = \sqrt[4]{16} = 2$ e argumento $\phi_k = \frac{\pi + 2\pi k}{4} = \frac{(2k+1)\pi}{4}$, para $k = 0, 1, 2, 3$. Assim, as raízes complexas de $f(x)$ são $\beta_k = 2\left(\cos\frac{(2k+1)\pi}{4} + i\,\mathrm{sen}\,\frac{(2k+1)\pi}{4}\right)$, com $k = 0, 1, 2, 3$. Temos
$\beta_0 = 2\left(\cos\frac{\pi}{4} + i\,\mathrm{sen}\,\frac{\pi}{4}\right) = \sqrt{2} + i\sqrt{2}$
$\beta_1 = 2\left(\cos\frac{3\pi}{4} + i\,\mathrm{sen}\,\frac{3\pi}{4}\right) = -\sqrt{2} + i\sqrt{2}$
$\beta_2 = 2\left(\cos\frac{5\pi}{4} + i\,\mathrm{sen}\,\frac{5\pi}{4}\right) = -\sqrt{2} - i\sqrt{2}$ e
$\beta_3 = 2\left(\cos\frac{7\pi}{4} + i\,\mathrm{sen}\,\frac{7\pi}{4}\right) = \sqrt{2} - i\sqrt{2}$.
Logo, a fatoração em produto de polinômios mônicos irredutíveis em $\mathbb{C}[x]$ é

$$x^4 + 16 = (x - \beta_0)(x - \beta_1)(x - \beta_2)(x - \beta_3).$$

Como $\beta_3 = \overline{\beta_0}$, $\beta_2 = \overline{\beta_1}$ temos

$$(x - \beta_0)(x - \overline{\beta_0}) = x^2 - 2\sqrt{2}x + 4 \text{ e } (x - \beta_1)(x - \overline{\beta_1}) = x^2 + 2\sqrt{2}x + 4.$$

Portanto, a fatoração em produto de polinômios mônicos irredutíveis em $\mathbb{R}[x]$ é

$$x^4 + 16 = (x^2 - 2\sqrt{2}x + 4)(x^2 + 2\sqrt{2}x + 4).$$

Observação: A estratégia para decompor polinômios $f(x)$ em $\mathbb{R}[x]$ é obter as raízes complexas não-reais β, caso existam, e combiná-las com a sua conjugada $\overline{\beta}$, de modo a determinar os divisores de $f(x)$ do tipo $x^2 + bx + c$ com $b^2 - 4c < 0$.

Exercícios

1. Faça o que se pede:

   (a) Determine o polinômio $f(x)$ de grau 3 com coeficientes reais e coeficiente líder 2, tal que -1 e $1 + i$ são raízes de $f(x)$.

   (b) Determine o polinômio $g(x)$ de grau 4 com coeficientes reais e coeficiente líder -1, tal que i e $3 - 4i$ são raízes de $f(x)$.

   (c) Determine a decomposição do polinômio $f(x)$ do item (a) em produto de potências de fatores mônicos irredutíveis em $\mathbb{R}[x]$ e em $\mathbb{C}[x]$.

   (d) Determine a decomposição do polinômio $g(x)$ do item (b) em produto de potências de fatores mônicos irredutíveis em $\mathbb{R}[x]$ e em $\mathbb{C}[x]$.

2. Decomponha em produto de polinômios mônicos irredutíveis em $\mathbb{C}[x]$ e em $\mathbb{R}[x]$:

   (a) $x^4 - 4$

   (b) $x^4 + 4$

   (c) $x^8 + 16$

   (d) $x^8 - 16$

3. Fatore em $\mathbb{R}[x]$ os seguintes polinômios:

   (a) $x^4 + 4x^2 + 3$,

   (b) $x^4 + 4x^2 + 4$,

   (c) $x^4 - x^2 + 1$,

   (d) $x^4 + px^2 + q$, com $p, q \in \mathbb{R}$.

4. $1+i$ é uma raiz múltipla de $f(x) = x^6-3x^5+5x^4-4x^3+4x^2-4x+4$. Determine a sua multiplicidade, as outras raízes complexas de $f(x)$ e dê a decomposição de $f(x)$ em produto de potências de polinômios mônicos irredutíveis em $\mathbb{R}[x]$.

5. Mostre que se $n \geq 1$, então

   (a) $x^{2n}-1 = (x-1)(x+1)\prod_{k=1}^{n-1}\left(x^2-2x\cos\left(\frac{k\pi}{n}\right)+1\right)$ em $\mathbb{R}[x]$.

   (b) $x^{2n+1}-1 = (x-1)\prod_{k=1}^{n}\left(x^2-2x\cos\left(\frac{2k\pi}{2n+1}\right)+1\right)$ em $\mathbb{R}[x]$.

6. Fatore em $\mathbb{R}[x]$ os seguintes polinômios:

   (a) $x^{24}-1$,

   (b) $x^{12}-1$,

   (c) $x^{13}-1$.

Polinômios em $\mathbb{Z}[x]$ e em $\mathbb{Q}[x]$

Os domínios de fatoração única têm a seguinte propriedade: o elemento a é primo se, e somente se, a é irredutível. Portanto, em domínios de fatoração única quando um irredutível divide um produto tem que dividir um dos fatores. Temos o seguinte Teorema, que não será demonstrado aqui.

Teorema 8
Se A é um domínio de fatoração única, então $A[x]$ é um domínio de fatoração única.

Como conseqüência desse Teorema temos que: $\mathbb{Z}[x]$, $\mathbb{Z}[x,y] = \mathbb{Z}[x][y]$ e $K[x,y] = K[x][y]$, onde K é um corpo, são domínios de fatoração única.

Vamos estudar com mais cuidado a fatoração em irredutíveis em $\mathbb{Z}[x]$ e em $\mathbb{Q}[x]$.

Seja $f(x) \in \mathbb{Q}[x]$ um polinômio não-constante. Então,

$f(x) = \frac{a_0}{b_0} + \frac{a_1}{b_1}x + \cdots + \frac{a_n}{b_n}x^n$, onde $a_j, b_j \in \mathbb{Z}$, $b_j \neq 0$, para todo $j = 0, \ldots, n$, $a_n \neq 0$ e $n \geq 1$.

Sabemos que

$$f(x) \text{ é irredutível em } \mathbb{Q}[x] \iff a \cdot f(x) \text{ é irredutível em } \mathbb{Q}[x], \text{ para todo } a \in \mathbb{Q},\ a \neq 0.$$

Em particular, tomando $m = \text{mmc}(b_0, \ldots, b_n)$ temos:

$$f(x) \text{ é irredutível em } \mathbb{Q}[x] \iff m \cdot f(x) \in \mathbb{Z}[x] \text{ é irredutível em } \mathbb{Q}[x].$$

Observe que $\text{grau}(m \cdot f(x)) = \text{grau}(f(x))$.

Lema 1 (Lema de Gauss)
Seja $f(x) \in \mathbb{Z}[x]$, com $\text{grau}(f(x)) \geq 1$, tal que $f(x)$ é irredutível em $\mathbb{Z}[x]$. Então, $f(x)$ é irredutível em $\mathbb{Q}[x]$.

Demonstração: Suponhamos, por absurdo, que $f(x)$ seja irredutível em $\mathbb{Z}[x]$, mas $f(x) = g(x) \cdot h(x)$, onde $1 \leq \text{grau}(g(x)), \text{grau}(h(x)) < \text{grau}(f(x))$ e $g(x), h(x) \in \mathbb{Q}[x]$.

Existe $m > 0$ tal que

$$m \cdot f(x) = g_1(x) \cdot h_1(x), \qquad (1)$$

com $g_1(x), h_1(x) \in \mathbb{Z}[x]$, $\text{grau}(g_1(x)) = \text{grau}(g(x))$ e $\text{grau}(h_1(x)) = \text{grau}(h(x))$. Assim,

$g_1(x) = a_0 + a_1x + \cdots + a_rx^r$, com $a_j \in \mathbb{Z}$, para todo $j = 0, \ldots, r$ e $a_r \neq 0$;

$h_1(x) = b_0 + b_1x + \cdots + b_sx^s$, com $b_j \in \mathbb{Z}$, para todo $j = 0, \ldots, s$ e $b_s \neq 0$.

Seja agora p um natural primo tal que p divide m. Vamos mostrar que $p \mid a_j$, para todo $j = 0, \ldots, r$, ou $p \mid b_j$, para todo $j = 0, \ldots, s$.

De fato, suponhamos, por absurdo, que existam $i \in \{0, \ldots, r\}$ e $j \in \{0, \ldots, s\}$ tais que $p \nmid a_i$ e $p \nmid b_j$. Consideremos i e j os menores possíveis com essa propriedade. Como $p \mid m$, então p divide todos os coeficientes de $g_1(x)h_1(x)$ e, em particular, p divide c_{i+j}, o coeficiente de x^{i+j} em $g_1(x)h_1(x)$. Temos

$$c_{i+j} = a_0b_{i+j} + a_1b_{i+j-1} + \cdots + a_{i-1}b_{j+1} + \underbrace{a_ib_j}_{\star} + a_{i+1}b_{j-1} + \cdots + a_{i+j}b_0, \text{ com}$$

$p \mid a_0, \ldots, p \mid a_{i-1}$ e $p \mid b_0, \ldots, p \mid b_{j-1}$.

p dividindo c_{i+j}, p dividindo cada parcela à esquerda de $\star$ e p dividindo cada parcela à direita de $\star$, contradizendo o fato de que p não divide a_ib_j.

Suponhamos, sem perda de generalidade, que p divide a_i, para todo $i = 0, \ldots, r$. Então, $g_1(x) = p \cdot g_2(x)$, com $g_2(x) \in \mathbb{Z}[x]$ e $m = p \cdot m_1$ com $m_1 > 0$ e $m_1 \in \mathbb{Z}$. Substituindo em (1), obtemos

$$p \cdot m_1 \cdot f(x) = p \cdot g_2(x)h_1(x).$$

Cancelando p, temos $m_1 \cdot f(x) = g_2(x)h_1(x)$. Continuamos o processo com cada fator primo positivo de m_1 (que é em número finito). Ao final, obtemos $f(x) = g^*(x)h^*(x)$, com $1 \leq \text{grau}(g^*(x)), \text{grau}(h^*(x)) < \text{grau}(f(x))$ e $g^*(x), h^*(x) \in \mathbb{Z}[x]$, contradizendo o fato de $f(x)$ ser irredutível em $\mathbb{Z}[x]$. ■

$\text{grau}(g^*(x)) = \text{grau}(g(x))$
$\text{grau}(h^*(x)) = \text{grau}(h(x))$

Observação: Seja $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]\backslash\mathbb{Z}$ tal que $\text{mdc}(a_0, \ldots, a_n) = 1$. Segue do Lema de Gauss que para mostrar a irredutibilidade de $f(x)$ em $\mathbb{Q}[x]$ basta mostrar que $f(x)$ é irredutível em $\mathbb{Z}[x]$.

Isto é muito útil para resolver problemas.

Como conseqüência do Lema de Gauss temos o seguinte critério de irredutibilidade em $\mathbb{Q}[x]$.

Teorema 9 (Critério de Eisenstein)
Seja $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$. Suponhamos que existe p primo tal que $p \nmid a_n$, $p \mid a_0$, ..., $p \mid a_{n-1}$ e $p^2 \nmid a_0$. Então, $f(x)$ é irredutível em $\mathbb{Q}[x]$.

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

Suponhamos, por absurdo, que $f(x) = g(x)h(x)$, com $g(x), h(x) \in \mathbb{Z}[x]$ e $1 \leq \text{grau}(g(x)), \text{grau}(h(x)) < n = \text{grau}(f(x))$. Sejam

$g(x) = b_0 + b_1x + \cdots + b_rx^r$, com $b_j \in \mathbb{Z}$, para todo $j = 0, \ldots, r$, e

$h(x) = c_0 + c_1x + \cdots + c_sx^s$, com $c_j \in \mathbb{Z}$, para todo $j = 0, \ldots, s$.

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

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

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

Como $a_n = b_r \cdot c_s$ e $p \nmid a_n$, então $p \nmid b_r$. Seja ℓ o menor natural $1 \leq \ell \leq r$ tal que $p \nmid b_\ell$. Então, $p \mid b_0$, $\ldots$, $p \mid b_{\ell-1}$ e

$$a_\ell = \underbrace{b_0c_\ell + \cdots + b_{\ell-1}c_1}_{p \text{ divide}} + \underbrace{b_\ell c_0}_{p \text{ não divide}}\,.$$

Logo, $p \nmid a_\ell$ e, por hipótese, $\ell = n = \text{grau}(f(x)) > r$, uma contradição. ■

Exemplo 52

$f(x) = x^5 + 4x + 2 \in \mathbb{Z}[x]$ é irredutível em $\mathbb{Q}[x]$.

Temos $a_5 = 1$ $a_4 = a_3 = a_2 = 0$, $a_1 = 4$ e $a_0 = 2$. Valem as hipóteses do Teorema anterior para o primo $p = 2$: $2 \mid a_0$, $2 \mid a_1$, $2 \mid a_2$, $2 \mid a_3$, $2 \mid a_4$, $2 \nmid a_5$ e $4 \nmid a_0$.

Exemplo 53

Há polinômios irredutíveis em $\mathbb{Q}[x]$ de grau n, para todo $n \geq 1$.

A saber, $f(x) = x^n - p$, onde p é um natural primo, é irredutível em $\mathbb{Q}[x]$, para todo $n \geq 1$.

De fato, o caso $n = 1$ é trivial. Para $n \geq 2$, aplicamos o critério de Eisenstein, com o primo p. Nesse caso, $a_0 = p$, $a_1 = \cdots = a_{n-1} = 0$ e $a_n = 1$.

Exemplo 54

$f(x) = 5x^4 - 24x^3 + 3x^2 + 12x - 6$ é irredutível em $\mathbb{Q}[x]$.

Nesse caso, $a_4 = 5$, $a_3 = -24$, $a_2 = 3$, $a_1 = 12$ e $a_0 = -6$. Aplique o critério de Eisenstein com o primo $p = 3$.

Exemplo 55

O polinômio $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$, onde p é primo, é irredutível em $\mathbb{Q}[x]$.

De fato, $f(x) = \dfrac{x^p - 1}{x - 1}$ e

As raízes em $\mathbb{C}$ de $f(x)$ são as raízes p-ésimas da unidade diferentes de 1.

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

Usamos a fórmula do binômio de Newton.

Como p divide $\binom{p}{j}$, para $1 \leq j \leq p-1$ e $\binom{p}{p-1} = p$, podemos aplicar o critério de Eisenstein ao polinômio $f(x+1)$ com o primo p. Assim, $f(x+1)$ é irredutível em $\mathbb{Q}[x]$, seguindo que $f(x)$ é irredutível em $\mathbb{Q}[x]$.

Fez o Exercício 8?

Sabemos que a existência de fator de grau 1 na fatoração de um polinômio $f(x)$ em $K[x]$ é equivalente à existência em K de uma de raiz de $f(x)$. O seguinte resultado é muito importante.

Proposição 13

Seja $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]\backslash\mathbb{Z}$. Seja $\beta \in \mathbb{Q}$, $\beta \neq 0$, uma raiz de $f(x)$. Escrevendo $\beta = \frac{r}{s}$, com $r, s \in \mathbb{Z}\backslash\{0\}$, então $r \mid a_0$ e $s \mid a_n$.

Demonstração: Podemos supor que $\text{mdc}(r, s) = 1$. Temos

$$0 = f\left(\frac{r}{s}\right) = a_0 + a_1 \cdot \frac{r}{s} + \cdots + a_{n-1}\frac{r^{n-1}}{s^{n-1}} + a_n\frac{r^n}{s^n}.$$

Multiplicando essa igualdade por s^n, obtemos:

$$0 = \underbrace{a_0 \cdot s^n + a_1 \cdot r \cdot s^{n-1} + \cdots + a_{n-1} \cdot r^{n-1} \cdot s}_{b} + a_n \cdot r^n.$$

Como $s \mid 0$ e $s \mid b$, então $s \mid a_n \cdot r^n$, mas $\text{mdc}(r, s) = 1$, logo $s \mid a_n$.

Analogamente, definindo $a = a_1 \cdot r \cdot s^{n-1} + \cdots + a_{n-1} \cdot r^{n-1} \cdot s + a_n \cdot r^n$ temos $0 = a_0 \cdot s^n + a$. Como $r \mid 0$ e $r \mid a$, então $r \mid a_0 \cdot s^n$, mas $\text{mdc}(r, s) = 1$, logo $r \mid a_0$. ■

Exemplo 56

Seja $f(x) = 4x^3 + 11x^2 + 45x - 12 \in \mathbb{Z}[x]$.

0 não é raiz de $f(x)$, pois $f(0) = -12$.

Se $\beta = \frac{r}{s} \neq 0$ é uma raiz de $f(x)$ e $s > 0$, então $r \mid -12$ e $s \mid 4$, logo $r \in \{\pm1, \pm2, \pm3, \pm4, \pm6, \pm12\}$ e $s \in \{1, 2, 4\}$.

Portanto, as possíveis raízes racionais de $f(x)$ são tais que

$$\beta \in \left\{\pm1, \pm2, \pm3, \pm4, \pm6, \pm12, \pm\tfrac{1}{2}, \pm\tfrac{3}{2}, \pm\tfrac{1}{4}, \pm\tfrac{3}{4}\right\}.$$

Como $f(0) = -12$ e $f(1) = 48$, com os nossos conhecimentos de Cálculo, sabemos que $f(x)$ tem uma raiz real no intervalo $(0, 1)$. Se esta raiz for racional, então tem que ser $\frac{1}{4}$, $\frac{1}{2}$ ou $\frac{3}{4}$. Por avaliação, verificamos que $f\left(\frac{1}{4}\right) = 0$. Assim, $x - \frac{1}{4}$ divide $f(x)$ em $\mathbb{Q}[x]$. Fazendo a divisão em $\mathbb{Q}[x]$, obtemos:

$$\begin{aligned} f(x) &= \left(x-\tfrac{1}{4}\right)(4x^2+12x+48) \text{ em } \mathbb{Q}[x] \\ &= (4x-1)(x^2+3x+12), \text{ com ambos irredutíveis em } \mathbb{Q}[x]. \end{aligned}$$

Observamos que $f(x) = (4x-1)(x^2+3x+12)$ é uma fatoração em polinômios irredutíveis em $\mathbb{Z}[x]$.

Para apresentarmos mais um critério de irredutibilidade em $\mathbb{Q}[x]$, vamos introduzir um novo conceito.

Lema 2

Seja p um primo fixo. A função φ é um homomorfismo sobrejetor de anéis, onde

$$\begin{aligned} \varphi : \mathbb{Z}[x] &\longrightarrow \mathbb{Z}_p[x] \\ f(x) &\longmapsto \overline{f}(x), \end{aligned}$$

onde $f(x) = a_0 + a_1x + \cdots + a_nx^n$ e $\overline{f}(x) = \overline{a_0} + \overline{a_1}x + \cdots + \overline{a_n}x^n \in \mathbb{Z}_p[x]$, com $\overline{a_j} = a_j \mod p$.

Demonstração: Sejam

$f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$, $\overline{f}(x) = \overline{a_0} + \overline{a_1}x + \cdots + \overline{a_n}x^n \in \mathbb{Z}_p[x]$ e

$g(x) = b_0 + b_1x + \cdots + b_mx^m \in \mathbb{Z}[x]$, $\overline{g}(x) = \overline{b_0} + \overline{b_1}x + \cdots + \overline{b_m}x^m \in \mathbb{Z}_p[x]$

Então,

$$f(x) + g(x) = \sum_{j=0}^{\max\{m,n\}} (a_j + b_j)x^j \qquad (\star)$$

$$\begin{aligned} \varphi(f(x)+g(x)) &\overset{(1)}{=} \sum_{j=0}^{\max\{m,n\}} \overline{(a_j+b_j)}x^j \\ &\overset{(2)}{=} \sum_{j=0}^{\max\{m,n\}} (\overline{a_j}+\overline{b_j})x^j \\ &\overset{(3)}{=} \overline{f}(x) + \overline{g}(x) \\ &\overset{(4)}{=} \varphi(f(x)) + \varphi(g(x)) \end{aligned}$$

Em (1) usamos $(\star)$ e a definição de φ; em (2), a soma módulo p; em (3), as definições de $\overline{f}(x)$ e $\overline{g}(x)$ e a soma em $\mathbb{Z}_p[x]$; e em (4), a definição de φ.

$$f(x)\cdot g(x) = \sum_{j=0}^{m+n} \left(\sum_{\lambda+\mu=j} a_\lambda \cdot b_\mu \right) x^j \qquad (\star\star)$$

$$\begin{aligned}
\varphi(f(x)\cdot g(x)) &\overset{(1)}{=} \sum_{j=0}^{m+n}\overline{\left(\sum_{\lambda+\mu=j} a_\lambda\cdot b_\mu\right)}x^j\\
&\overset{(2)}{=} \sum_{j=0}^{m+n}\left(\sum_{\lambda+\mu=j}\overline{a_\lambda\cdot b_\mu}\right)x^j\\
&\overset{(3)}{=} \sum_{j=0}^{m+n}\left(\sum_{\lambda+\mu=j}\overline{a_\lambda}\cdot\overline{b_\mu}\right)x^j\\
&\overset{(4)}{=} \overline{f}(x)\cdot\overline{g}(x)\\
&\overset{(5)}{=} \varphi(f(x))\cdot\varphi(g(x)).
\end{aligned}$$

Em (1) usamos $(\star\star)$ e a definição de φ; em (2), a soma módulo p; em (3), o produto módulo p; em (4), as definições de $\overline{f}(x)$ e $\overline{g}(x)$ e a multiplicação em $\mathbb{Z}_p[x]$; e em (5), a definição de φ.

É claro que φ é sobrejetora. ■

Proposição 14

Seja $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]\backslash\mathbb{Z}$. Seja p um primo tal que $a_n \not\equiv 0 \mod p$. Se $\overline{f}(x) = \overline{a_0} + \overline{a_1}x + \cdots + \overline{a_n}x^n \in \mathbb{Z}_p[x]$ é irredutível em $\mathbb{Z}_p[x]$, então $f(x)$ é irredutível em $\mathbb{Q}[x]$.

Demonstração: Suponhamos que $f(x)$ seja redutível em $\mathbb{Q}[x]$. Pelo Lema de Gauss, existem polinômios $g(x)$ e $h(x) \in \mathbb{Z}[x]$ tais que $f(x) = g(x)\cdot h(x)$ e $1 \leq \text{grau}(g(x)), \text{grau}(h(x)) < \text{grau}(f(x))$. Escrevemos

$g(x) = b_0 + b_1x + \cdots + b_rx^r$, com $b_j \in \mathbb{Z}$, para $j = 0, \ldots, r$ e

$h(x) = c_0 + c_1x + \cdots + c_sx^s$, com $c_j \in \mathbb{Z}$, para $j = 0, \ldots, s$.

Passando módulo p, pelo Lema anterior, obtemos $\overline{f}(x) = \overline{g}(x)\overline{h}(x)$ em $\mathbb{Z}_p[x]$, onde

$\overline{g}(x) = \overline{b_0} + \overline{b_1}x + \cdots + \overline{b_r}x^r$ e $\overline{h}(x) = \overline{c_0} + \overline{c_1}x + \cdots + \overline{c_s}x^s$.

Logo, $\overline{b_r}\cdot\overline{c_s} = \overline{a_n} \neq \overline{0}$. Como $\mathbb{Z}_p$ é um corpo, então $\overline{b_r} \neq \overline{0}$ e $\overline{c_s} \neq \overline{0}$, logo $\text{grau}(\overline{g}(x)) = \text{grau}(g(x)) \geq 1$ e $\text{grau}(\overline{h}(x)) = \text{grau}(h(x)) \geq 1$ e $\overline{f}(x)$ é redutível em $\mathbb{Z}_p[x]$. ■

Exercícios

1. Determine, caso existam, todas as raízes racionais de $f(x)$ e dê a sua decomposição em produto de potências de fatores mônicos irredutíveis em $\mathbb{R}[x]$:

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

   (b) $f(x) = 2x^6 + 5x^5 + x^4 + 10x^3 - 4x^2 + 5x - 3$.

2. Seja $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$. Mostre que se $\alpha \in \mathbb{Q}$ é uma raiz de $f(x)$, então $\alpha \in \mathbb{Z}$.

3. (a) Mostre que $\beta = \sqrt{2} + \sqrt{3}$ é raiz de $x^4 - 10x^2 + 1$ e prove que β é irracional.

   (b) Mostre que $\sqrt{5} + \sqrt{7}$ é irracional.

   (c) Mostre que $\sqrt[3]{2} - \sqrt{3}$ é irracional.

4. Ache as raízes racionais dos seguintes polinômios:

   (a) $x^4 - x^3 - x^2 + 19x - 42$

   (b) $x^3 - 9x^2 + 22x - 24$

   (c) $2x^3 - x^2 + 1$

   (d) $10x^3 + 19x^2 - 30x + 9$

   (e) $6x^5 + x^4 - 14x^3 + 4x^2 + 5x - 2$

5. Determine todas as raízes reais e complexas não-reais, suas multiplicidades e dê a decomposição do polinômio em produto de potências de fatores mônicos irredutíveis em $\mathbb{C}[x]$ e em $\mathbb{R}[x]$:

   (a) $-x^5 + 5x^4 - 3x^3 - 15x^2 + 18x$.

   (b) $x^4 - x^3 - 5x^2 - x - 6$.

   (c) $x^5 + x^4 + 5x^2 - x - 6$.

   (d) $x^4 + 4x^3 - 7x^2 - 36x - 18$.

   (e) $x^4 - 3x^3 + 5x^2 - x - 10$.

   (f) $x^5 - 3x^4 - 3x^3 + 9x^2 - 10x + 30$.

   (g) $x^5 - 9x^4 + 31x^3 - 49x^2 + 36x - 10$.

   (h) $-x^3 + 28x + 48$.

   (i) $x^4 - 5x^3 + 3x^2 + 15x - 18$.

6. Decomponha o polinômio $x^4 - 5x^2 + 6$ em produto de polinômios mônicos irredutíveis em $\mathbb{Q}[x]$, $\mathbb{Q}(\sqrt{2})[x]$ e $\mathbb{R}[x]$.

7. Mostre que os polinômios são irredutíveis em $\mathbb{Q}[x]$:

   (a) $x^4 + 1$

   (b) $x^5 + x^2 + 1$

Seja $f(x) = a_0 + a_1x + \cdots + a_nx^n$ em $\mathbb{Z}[x] \setminus \mathbb{Z}$ com $\text{mdc}(a_0, \ldots, a_n) = 1$. Para mostrar que $f(x)$ é irredutível em $\mathbb{Q}[x]$, pelo Lema de Gauss, basta mostrar que $f(x)$ é irredutível em $\mathbb{Z}[x]$.

8. Sejam K um corpo e $a \in K$.

   (a) Mostre que a função

   $$\begin{array}{rcl} \varphi : K[x] & \longrightarrow & K[x] \\ f(x) & \longmapsto & f(x+a) \end{array}$$

   é um isomorfismo de anéis comutativos com unidade.

   (b) Mostre que $f(x)$ é irredutível em $K[x]$ se, e somente se, $f(x+a)$ é irredutível em $K[x]$.

9. Determine quais dos seguintes polinômios são irredutíveis em $\mathbb{Q}[x]$:

   (a) $2x^2 - 3x + 1$

   (b) $x^2 - 2$

   (c) $x^2 + x + 1$

   (d) $4x^3 + 3x^2 + 3x - 1$

   (e) $x^3 + 5x^2 + 4x + 1$

   (f) $x^4 + 6x^2 + 8x - 2$

   (g) $x^3 - x + 1$

   (h) $x^3 + 2x + 10$

   (i) $x^3 - 2x^2 + x + 15$

   (j) $x^4 - x + 1$

   (k) $x^7 + 22x^3 + 11x^2 - 44x + 33$

   (l) $x^3 - 7x^2 + 3x + 3$

10. Determine todos os polinômios mônicos irredutíveis de $\mathbb{Z}_2[x]$ de graus 1, 2, 3 e 4.

11. Mostre que $x^5 + x^2 + 1$ é irredutível em $\mathbb{Z}_2[x]$.

12. Determine todos os polinômios mônicos irredutíveis de $\mathbb{Z}_3[x]$ de graus 1, 2 e 3.

13. Mostre que $x^4 + x + 2$ é irredutível em $\mathbb{Z}_3[x]$.

Resolução por radicais

Vamos mostrar que as equações de graus 2, 3 e 4 com coeficientes complexos têm as suas raízes expressas por radicais de funções algébricas racionais dos seus coeficientes.

A equação do 2º grau em $\mathbb{C}[x]$

Vamos resolver por radicais a equação $x^2 + \alpha x + \beta = 0$, onde $\alpha, \beta \in \mathbb{C}$. Para isto, consideramos, primeiramente, um caso particular.

Seja $x^2 = \alpha$, onde $\alpha \in \mathbb{C}$ e $\alpha \neq 0$. Sabemos resolver em $\mathbb{C}$ esta equação, usando a forma polar do número complexo α, que inclui o caso $\alpha = a \in \mathbb{R}$. Vamos dar uma outra solução, obtida diretamente da expressão de $\alpha = a+bi$, onde $a, b \in \mathbb{R}$.

Consideremos $\alpha = a + bi$, onde $b \neq 0$. Vamos determinar um número complexo $c + di$ tal que $a + bi = (c + di)^2 = c^2 - d^2 + 2cdi$.

Pela igualdade de números complexos, temos que

$$\begin{cases} a = c^2 - d^2 \\ b = 2cd \end{cases} \implies \begin{cases} a^2 = (c^2 - d^2)^2 \\ b^2 = 4c^2d^2 \end{cases}$$
$$\implies a^2 + b^2 = c^4 + d^4 + 2c^2d^2 = (c^2 + d^2)^2$$

Portanto, $c^2 + d^2 = \sqrt{a^2 + b^2}$. Como $c^2 - d^2 = a$, somando e subtraindo essas equações, obtemos, respectivamente,

$$c^2 = \frac{\sqrt{a^2 + b^2} + a}{2} \quad \text{e} \quad d^2 = \frac{\sqrt{a^2 + b^2} - a}{2}.$$

Logo,

$$|\, c \,| = \sqrt{\frac{\sqrt{a^2 + b^2} + a}{2}} \quad \text{e} \quad |\, d \,| = \sqrt{\frac{\sqrt{a^2 + b^2} - a}{2}}. \qquad (\star)$$

Como $b \neq 0$ e $b = 2cd$, devemos escolher os números reais c e d, com a propriedade $(\star)$, de modo que o sinal do seu produto seja o mesmo sinal de b. Assim, quando $b > 0$, tomamos $c > 0$ e $d > 0$, ou $c < 0$ e $d < 0$; quando $b < 0$, tomamos $c > 0$ e $d < 0$, ou $c < 0$ e $d > 0$. Dessa maneira temos exatamente dois números complexos da forma $c + di$ cujo quadrado é $\alpha = a + bi$. ■

Exemplo 57

Vamos resolver a equação $x^2 = -i$.

Nesse caso, $a = 0$ e $b = -1$. Temos $a^2 + b^2 = 1$ e, pelas equações $(\star)$,

$$|\,c\,| = \sqrt{\frac{\sqrt{1}+0}{2}} = \frac{1}{\sqrt{2}} \quad \text{e} \quad |\,d\,| = \sqrt{\frac{\sqrt{1}+0}{2}} = \frac{1}{\sqrt{2}}.$$

Como $b < 0$, as soluções da equação são $\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}i$ e $-\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i$.

Exemplo 58

Vamos resolver a equação $x^2 = 1 + i$.

Nesse caso, $a = 1$ e $b = 1$. Temos $a^2 + b^2 = 2$ e, pelas equações $(\star)$,

$$|\,c\,| = \sqrt{\frac{\sqrt{2}+1}{2}} \quad \text{e} \quad |\,d\,| = \sqrt{\frac{\sqrt{2}-1}{2}}.$$

Como $b > 0$, as soluções da equação são

$$\sqrt{\frac{\sqrt{2}+1}{2}} + i\sqrt{\frac{\sqrt{2}-1}{2}} \text{ e } -\sqrt{\frac{\sqrt{2}+1}{2}} - i\sqrt{\frac{\sqrt{2}-1}{2}}.$$

Agora podemos resolver por radicais a equação $x^2 + \alpha x + \beta = 0$, onde $\alpha, \beta \in \mathbb{C}$. Temos:

$$\begin{aligned} x^2 + \alpha x + \beta &= \left(x + \frac{\alpha}{2}\right)^2 - \frac{\alpha^2}{4} + \beta \\ &= \left(x + \frac{\alpha}{2}\right)^2 - \frac{\alpha^2 - 4\beta}{4}. \end{aligned}$$

Seja $\Delta = \alpha^2 - 4\beta \in \mathbb{C}$. Pelas considerações anteriores, existem δ e $-\delta$ em $\mathbb{C}$, tais que $\delta^2 = \Delta$. Escrevendo $\delta = \sqrt{\Delta}$, temos $-\delta = -\sqrt{\Delta}$ e a equação proposta $\left(x + \frac{\alpha}{2}\right)^2 - \frac{\alpha^2 - 4\beta}{4} = 0$ é equivalente a $x + \frac{\alpha}{2} = \pm\frac{\sqrt{\Delta}}{2}$.

As soluções da equação proposta são

$$x_1 = \frac{-\alpha + \sqrt{\alpha^2 - 4\beta}}{2} \quad \text{e} \quad x_2 = \frac{-\alpha - \sqrt{\alpha^2 - 4\beta}}{2},$$

onde $\sqrt{\alpha^2 - 4\beta}$ é uma das raízes de $x^2 = \alpha^2 - 4\beta$.

Exemplo 59

Vamos resolver a equação $x^2 + 2ix + (-2 - i) = 0$.

Nesse caso, $\Delta = (2i)^2 - 4(-2 - i) = 4 + 4i$. Devemos determinar números complexos cujo quadrado é $4 + 4i$. Temos $a = 4$, $b = 4$ e $a^2 + b^2 = 32$. Pelas fórmulas $(\star)$, temos

$$|\,c\,| = \sqrt{\frac{\sqrt{32}+4}{2}} = \sqrt{\frac{4\sqrt{2}+4}{2}} = \sqrt{2\sqrt{2}+2}$$

e

$$|\,d\,| = \sqrt{\frac{\sqrt{32}-4}{2}} = \sqrt{\frac{4\sqrt{2}-4}{2}} = \sqrt{2\sqrt{2}-2}.$$

Tomamos $\sqrt{\Delta} = \sqrt{2\sqrt{2}+2} + i\sqrt{2\sqrt{2}-2}$.

As soluções da equação proposta são

$$x_1 = \frac{-2i+\sqrt{\Delta}}{2} \text{ e } x_2 = \frac{-2i-\sqrt{\Delta}}{2}.$$

A equação do 3º grau em $\mathbb{C}[x]$

Consideremos a equação

$$x^3 + a_2x^2 + a_1x + a_0 = 0, \text{ com } a_j \in \mathbb{C}. \qquad (1)$$

Substituindo x por $y + b$, temos:

$$\begin{aligned} 0 &= (y+b)^3 + a_2(y+b)^2 + a_1(y+b) + a_0 \\ &= y^3 + (3b+a_2)y^2 + (3b^2+2a_2b+a_1)y + (b^3+a_2b^2+a_1b+a_0) \end{aligned}$$

Tomando $b = -\frac{a_2}{3}$, temos

$$x^3 + a_2x^2 + a_1x + a_0 = y^3 + py + q,$$

$$\text{onde } \begin{cases} x = y - \frac{a_2}{3} \\ p = \frac{3{a_2}^2}{9} - \frac{2{a_2}^2}{3} + a_1 = a_1 - \frac{{a_2}^2}{3}, \\ q = \frac{2{a_2}^3}{27} - \frac{a_1a_2}{3} + a_0. \end{cases}$$

Determinar as raízes de (1) é equivalente a determinar as raízes de

$$y^3 + py + q = 0. \qquad (2)$$

e somar $-\frac{a_2}{3}$.

Consideremos $y = u+v$, onde u e v são variáveis que vamos relacionar.

Substituindo na equação (2), obtemos:

$$\begin{aligned} 0 &= (u+v)^3 + p(u+v) + q \\ &= u^3 + 3u^2v + 3uv^2 + v^3 + p(u+v) + q \\ &= (u^3+v^3+q) + 3uv(u+v) + p(u+v) \\ &= (u^3+v^3+q) + (u+v)(3uv+p) \end{aligned}$$

Logo,

$$(u^3+v^3+q)+(u+v)(3uv+p)=0. \qquad (3)$$

Cada solução (u,v) do sistema (4),

$$(4)\quad \begin{cases} u^3+v^3+q=0 \\ 3uv+p=0 \end{cases}$$

nos dá uma solução (u,v) de (3) e uma solução $y=u+v$ de (2).

Como (4) é equivalente a (5),

$$(5)\quad \begin{cases} u^3+v^3=-q \\ uv=-\frac{p}{3} \end{cases}, \qquad \text{então} \qquad \begin{cases} u^3+v^3=-q \\ u^3v^3=-\frac{p^3}{27}. \end{cases}$$

Logo, u^3 e v^3 são raízes em $\mathbb{C}$ da equação

$$z^2+qz-\tfrac{p^3}{27}=0. \qquad (6)$$

Seja $\Delta=q^2+\frac{4p^3}{27}$. Então, $z=\frac{-q\pm\sqrt{q^2+\frac{4p^3}{27}}}{2}=-\frac{q}{2}\pm\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}$, onde $\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}$ é uma das raízes quadradas complexas de $\frac{q^2}{4}+\frac{p^3}{27}$.

As raízes de (6) são $z_1=-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}$ e $z_2=-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}$.

Escrevemos $u^3=z_1 \quad$ e $\quad v^3=z_2$.

Reveja na Seção 4, no Exemplo 49, a solução da equação $x^n-a=0$, onde $a\in\mathbb{C}$.

Escolha uma das raízes cúbicas de z_1 e escreva-a com $\sqrt[3]{z_1}$. As soluções de $u^3=z_1$ são

$$u_1=\sqrt[3]{z_1},\ u_2=\omega\sqrt[3]{z_1} \text{ e } u_3=\omega^2\sqrt[3]{z_1},$$

onde $\omega=\cos\frac{2\pi}{3}+i\,\mathrm{sen}\,\frac{2\pi}{3}$ é uma raiz primitiva cúbica da unidade.

Lembre que $uv=-\frac{p}{3}$.

Seja agora $\sqrt[3]{z_2}$ a raiz cúbica de z_2, tal que $\sqrt[3]{z_1}\cdot\sqrt[3]{z_2}=-\frac{p}{3}$.

As soluções de (5) são

$$\begin{array}{ll} u_1=\sqrt[3]{z_1} & v_1=\sqrt[3]{z_2} \\ u_2=\omega\sqrt[3]{z_1} & v_2=\omega^2\sqrt[3]{z_2} \\ u_3=\omega^2\sqrt[3]{z_1} & v_3=\omega\sqrt[3]{z_2} \end{array}$$

$u_j v_j=-\frac{p}{3}$, com $j=1,\ 2\ ,3$.

As soluções de (2) são

$$y_1=u_1+v_1=\sqrt[3]{-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}+\sqrt[3]{-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}$$

$$y_2=u_2+v_2=\omega\sqrt[3]{-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}+\omega^2\sqrt{-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}$$

$$y_3=u_3+v_3=\omega^2\sqrt[3]{-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}+\omega\sqrt{-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}},$$

conhecidas como Fórmulas de Cardan.

As fórmulas que resolvem a equação (1) são obtidas das Fórmulas de Cardan fazendo $x = y - \frac{a_2}{3}$.

Observação: Os cálculos acima são válidos em corpos K algebricamente fechados, desde que $\mathrm{car}(K) \neq 2$ e $\mathrm{car}(K) \neq 3$.

Exemplo 60

Não decore as fórmulas, entenda o procedimento. Depois da translação, caso necessário, só precisamos das fórmulas (5) e (6), para determinar as raízes.

Vamos resolver a equação $y^3 + 3y + 4 = 0$.

Nesse caso, $p = 3$, $q = 4$ e temos as equações

$$(5)\ \begin{cases} u^3 + v^3 = -q = -4 \\ uv = \frac{-p}{3} = -1 \end{cases} \Longrightarrow \begin{cases} u^3 + v^3 = -4 \\ u^3 v^3 = -1 \end{cases}$$

Devemos resolver a equação $z^2 + 4z - 1 = 0$. (6)

Como $\Delta = 16 - 4 \cdot (-1) = 20$, temos

$$z_1 = \tfrac{-4+\sqrt{20}}{2} = -2 + \sqrt{5} \text{ e } z_2 = \tfrac{-4-\sqrt{20}}{2} = -2 - \sqrt{5}.$$

As soluções de $u^3 = z_1$ são $u_1 = \sqrt[3]{-2+\sqrt{5}} \in \mathbb{R}$, $u_2 = u_1\omega$ e $u_3 = u_1\omega^2$, onde $\omega = \cos\frac{2\pi}{3} + i\,\mathrm{sen}\,\frac{2\pi}{3} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ e $\omega^2 = \cos\frac{4\pi}{3} + i\,\mathrm{sen}\,\frac{4\pi}{3} = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$.

Como $u_j v_j = -1$, as soluções de $v^3 = z_2$ são $v_1 = \sqrt[3]{-2-\sqrt{5}} \in \mathbb{R}$, $v_2 = v_1\omega^2$ e $v_3 = v_1\omega$.

As equações $u^3 = z_1$ e $v^3 = z_2$, com $z_1, z_2 \in \mathbb{R}$, têm uma única solução real. Como $u_1 \in \mathbb{R}$ e $u_1 v_1 = -1$, então $v_1 \in \mathbb{R}$.

As raízes da equação dada são:

$$\begin{aligned}
y_1 &= u_1 + v_1 = \sqrt[3]{-2+\sqrt{5}} + \sqrt[3]{-2-\sqrt{5}} \\
&= \sqrt[3]{-2+\sqrt{5}} - \sqrt[3]{2+\sqrt{5}} \in \mathbb{R} \\
y_2 &= u_2 + v_2 = u_1\omega + v_1\omega^2 = u_1\left(-\tfrac{1}{2} + i\tfrac{\sqrt{3}}{2}\right) + v_1\left(-\tfrac{1}{2} - i\tfrac{\sqrt{3}}{2}\right) \\
&= -\tfrac{1}{2}(u_1 + v_1) + i\tfrac{\sqrt{3}}{2}(u_1 - v_1) \\
&= -\tfrac{1}{2}\left(\sqrt[3]{-2+\sqrt{5}} - \sqrt[3]{2+\sqrt{5}}\right) + i\tfrac{\sqrt{3}}{2}\left(\sqrt[3]{-2+\sqrt{5}} + \sqrt[3]{2+\sqrt{5}}\right) \\
y_3 &= u_3 + v_3 = u_1\omega^2 + v_1\omega = u_1\left(-\tfrac{1}{2} - i\tfrac{\sqrt{3}}{2}\right) + v_1\left(-\tfrac{1}{2} + i\tfrac{\sqrt{3}}{2}\right) \\
&= -\tfrac{1}{2}(u_1 + v_1) - i\tfrac{\sqrt{3}}{2}(u_1 - v_1) \\
&= -\tfrac{1}{2}\left(\sqrt[3]{-2+\sqrt{5}} - \sqrt[3]{2+\sqrt{5}}\right) - i\tfrac{\sqrt{3}}{2}\left(\sqrt[3]{-2+\sqrt{5}} + \sqrt[3]{2+\sqrt{5}}\right)
\end{aligned}$$

As raízes estão escritas de uma maneira complicada.

É facil verificar que -1 é uma raiz de $y^3 + 3y + 4$. Fazendo a divisão do polinômio $y^3 + 3y + 4$ por $y + 1$, obtemos $y^3 + 3y + 4 = (y + 1)(y^2 - y + 4)$. As raízes de $y^2 - y + 4$ são $\frac{1 \pm \sqrt{-15}}{2} = \frac{1 \pm i\sqrt{15}}{2}$.

Logo, as raízes da equação dada são

$$-1,\ \tfrac{1+i\sqrt{15}}{2} = \tfrac{1}{2} + i\tfrac{\sqrt{3}}{2}\sqrt{5} \text{ e } \tfrac{1-i\sqrt{15}}{2} = \tfrac{1}{2} - i\tfrac{\sqrt{3}}{2}\sqrt{5}.$$

Comparando com as raízes obtidas pelas fórmulas de Cardan, temos as seguintes relações muito interessantes:

$$\sqrt[3]{-2+\sqrt{5}}-\sqrt[3]{2+\sqrt{5}}=-1 \text{ e } \sqrt[3]{-2+\sqrt{5}}+\sqrt[3]{2+\sqrt{5}}=\sqrt{5}.$$

Somando essas igualdades e subtraindo a primeira igualdade da segunda, obtemos:

$$2\left(\sqrt[3]{-2+\sqrt{5}}\right)=-1+\sqrt{5} \text{ e } 2\left(\sqrt[3]{2+\sqrt{5}}\right)=1+\sqrt{5}.$$

Concluímos que $\sqrt[3]{-2+\sqrt{5}}=\frac{-1+\sqrt{5}}{2}$ e $\sqrt[3]{2+\sqrt{5}}=\frac{1+\sqrt{5}}{2}$.

A equação do 4º grau em $\mathbb{C}[x]$

Sabemos resolver por radicais as equações de graus 2 e 3. A resolução da equação do 4º grau pelo método de Ferrari consiste em resolver uma equação do 3º grau e duas equações do 2º grau.

Consideremos $x^4+a_3x^3+a_2x^2+a_1x+a_0=0$, com $a_j\in\mathbb{C}$.

Escrevemos $x^4+a_3x^3=-a_2x^2-a_1x-a_0$.

Completando o quadrado à esquerda, temos

$$\left(x^2+\tfrac{a_3}{2}x\right)^2=(x^4+a_3x^3)+\tfrac{{a_3}^2}{4}x^2.$$

Logo,

$$\left(x^2+\tfrac{a_3}{2}x\right)^2=\left(\tfrac{{a_3}^2}{4}-a_2\right)x^2-a_1x-a_0. \qquad (\star)$$

Se o membro à direita da igualdade acima for um quadrado perfeito, então teremos que resolver duas equações do 2º grau. Precisamos transformar o lado direito num quadrado, sem alterar o quadrado do lado esquerdo. Para isto, introduzimos no lado esquerdo uma nova variável y a ser determinada de modo que o lado direito seja um quadrado.

$$\begin{aligned}\left(x^2+\tfrac{a_3}{2}x+y\right)^2 &= \left(x^2+\tfrac{a_3}{2}x\right)^2+y^2+2\left(x^2+\tfrac{a_3}{2}x\right)y\\ &= \left(\tfrac{{a_3}^2}{4}-a_2\right)x^2-a_1x-a_0+y^2+2\left(x^2+\tfrac{a_3}{2}x\right)y\\ &= \left(2y+\tfrac{{a_3}^2}{4}-a_2\right)x^2+(a_3y-a_1)x+(y^2-a_0)\end{aligned}$$

Na segunda igualdade, usamos a relação em $(\star)$.

Logo,

$$\left(x^2+\tfrac{a_3}{2}x+y\right)^2=\left(2y+\tfrac{{a_3}^2}{4}-a_2\right)x^2+(a_3y-a_1)x+(y^2-a_0)\ . \qquad (\star\star)$$

Vamos determinar y de modo que o lado direito de $(\star\star)$ seja um quadrado. Basta fazermos o discriminante Δ do polinômio em x do lado direito igual a zero. Temos

$$\begin{aligned}\Delta &= (a_3y - a_1)^2 - 4\left(2y + \tfrac{{a_3}^2}{4} - a_2\right)(y^2 - a_0)\\ &= {a_3}^2y^2 - 2a_1a_3y + {a_1}^2 + (-8y - {a_3}^2 + 4a_2)y^2 + a_0(8y + {a_3}^2 - 4a_2)\\ &= -8y^3 + 4a_2y^2 + (-2a_1a_3 + 8a_0)y + ({a_1}^2 + a_0{a_3}^2 - 4a_0a_2)\end{aligned}$$

Escolhemos $y \in \mathbb{C}$ como uma raiz da equação

$$-8y^3 + 4a_2y^2 + (-2a_1a_3 + 8a_0)y + ({a_1}^2 + a_0{a_3}^2 - 4a_0a_2) = 0. \qquad (\star\star\star)$$

Substituindo esse valor em $(\star\star)$, temos que

$$\left(x^2 + \tfrac{a_3}{2}x + y\right)^2 = (\alpha x + \beta)^2,$$

com α e β convenientes. Portanto,

$$x^2 + \tfrac{a_3}{2}x + y = \alpha x + \beta \text{ ou } x^2 + \tfrac{a_3}{2}x + y = -(\alpha x + \beta)$$

A resolução da equação do $4^{\underline{o}}$ grau recai na resolução de uma equação do $3^{\underline{o}}$ e das duas equações acima do $2^{\underline{o}}$ grau.

Atenção: precisamos apenas de uma das raízes da equação do $3^{\underline{o}}$ grau.

Exemplo 61

Vamos resolver a equação $x^4 - 2x^3 + 4x^2 - 2x + 3 = 0$. A fórmula $(\star\star\star)$ não é para ser memorizada. Seguimos o raciocínio utilizado na demonstração, com o polinômio dado.

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

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

$$\begin{aligned}(x^2 - x + y)^2 &= (-3x^2 + 2x - 3) + 2(x^2 - x)y + y^2\\ &= (-3 + 2y)x^2 + (2 - 2y)x + (y^2 - 3) \qquad (*)\end{aligned}$$

$$\begin{aligned}\Delta &= (2 - 2y)^2 - 4(-3 + 2y)(y^2 - 3)\\ &= 4 - 8y + 4y^2 + (12 - 8y)(y^2 - 3)\\ &= 4 - 8y + 4y^2 + 12y^2 - 36 - 8y^3 + 24y\\ &= -8y^3 + 16y^2 + 16y - 32\end{aligned}$$

Portanto, $-8y^3 + 16y^2 + 16y - 32 = 0$ é equivalente a $y^3 - 2y^2 - 2y + 4 = 0$.

Vemos, facilmente, que $y = 2$ é uma raiz da equação do $3^{\underline{o}}$ grau.

Substituindo $y = 2$ em $(*)$, obtemos:

$(x^2 - x + 2)^2 = (-3 + 4)x^2 + (2 - 4)x + (4 - 3) = x^2 - 2x + 1 = (x - 1)^2$.

Portanto,

$x^2 - x + 2 = x - 1$ ou $x^2 - x + 2 = -(x - 1)$

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

$x = \frac{2 \pm \sqrt{4-12}}{2} = 1 \pm \sqrt{2}i$ ou $x = \pm i$

As raízes da equação dada são $1 + \sqrt{2}i$, $1 - \sqrt{2}i$, i e $-i$.

Exemplo 62

Vamos resolver $x^4 - 12x^2 + 24x - 5 = 0$.

$x^4 = 12x^2 - 24x + 5$

$(x^2)^2 = 12x^2 - 24x + 5$

$$\begin{aligned}(x^2 + y)^2 &= (12x^2 - 24x + 5) + 2x^2y + y^2 \\ &= (12 + 2y)x^2 - 24x + (y^2 + 5) \qquad (*)\end{aligned}$$

$$\begin{aligned}\Delta &= (24)^2 - 4(12 + 2y)(y^2 + 5) \\ &= (24)^2 - 48y^2 - 240 - 8y^3 - 40y \\ &= -8(y^3 + 6y^2 + 5y - 72 + 30)\end{aligned}$$

Portanto, $y^3 + 6y^2 + 5y - 42 = 0$.

Vemos que $y = 2$ é uma raiz da equação acima.

Substituindo esse valor em $(*)$, obtemos:

$(x^2 + 2)^2 = 16x^2 - 24x + 9 = (4x - 3)^2$

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

$x^2 - 4x + 5 = 0$ ou $x^2 + 4x - 1 = 0$

$x = \frac{4 \pm \sqrt{16-20}}{2} = 2 \pm i$ ou $x = \frac{-4 \pm \sqrt{16+4}}{2} = -2 \pm \sqrt{5}$

As raízes da equação dada são $2 + i$, $2 - i$, $-2 + \sqrt{5}$ e $-2 - \sqrt{5}$.

Exercícios

1. Determine em $\mathbb{C}$ as soluções das equações:
   (a) $z^2 = 5 - 12i$.
   (b) $z^2 = 8 + 6i$

2. Resolva em $\mathbb{C}$ as equações:
   (a) $x^3 - 6x^2 + 21x - 18 = 0$.
   (b) $x^3 - 9x - 12 = 0$.
   (c) $x^3 + 12x - 30 = 0$.
   (d) $x^3 - 9x^2 - 9x - 15 = 0$.

3. Mostre que as raízes em $\mathbb{C}$ da equação $x^3 - 3x + 1 = 0$ são $2\cos\frac{2\pi}{9}$, $2\cos\frac{4\pi}{9}$ e $2\cos\frac{8\pi}{9}$.

4. Mostre que

   (a) $\sqrt[3]{7+\sqrt{50}} + \sqrt[3]{7-\sqrt{50}} = 2$.

   (b) $\sqrt[3]{\sqrt{108}+10} - \sqrt[3]{\sqrt{108}-10} = 2$.

   (c) $\sqrt[3]{\sqrt{243}+\sqrt{242}} - \sqrt[3]{\sqrt{243}-\sqrt{242}} = 2\sqrt{2}$

5. Resolva em $\mathbb{C}$ usando o método de Ferrari:

   (a) $x^4 - 15x^2 - 12x - 2 = 0$.

   (b) $x^4 + 2x^2 - 4x + 8$.

   (c) $x^4 - 2x^3 + 5x^2 - 2x + 4 = 0$.

   (d) $x^4 + 2x^3 + x^2 + 4x - 2 = 0$.