Teorema. [Factorização única em $C[x]$]

Todo o polinómio $r(\boldsymbol{x}) \in C[x]$ de grau positivo pode ser escrito na forma

$$r(\boldsymbol{x}) = cp_1(\boldsymbol{x})^{n_1}p_2(\boldsymbol{x})^{n_2}\cdots p_t(\boldsymbol{x})^{n_t} \tag{1}$$

onde $c \in C \setminus \{0\}$, $p_1(\boldsymbol{x}), p_2(\boldsymbol{x}), \ldots, p_t(\boldsymbol{x})$ são polimónios mónicos irredutíveis em $C[x]$, todos distintos, e $n_1, n_2, \ldots, n_t \in \mathbb{N}$.

E mais: esta factorização é única a menos da ordem pela qual se escrevem os factores.

Demonstração. Comecemos por demonstrar a existência da factorização, por indução sobre $n = gr(r(\boldsymbol{x}))$.

O caso $n = 1$ é evidente: $r(\boldsymbol{x})$ sendo de grau 1 é irredutível. Seja c o coeficiente do termo de grau 1. Então $r(\boldsymbol{x}) = c(c^{-1}r(\boldsymbol{x}))$, onde $c^{-1}r(\boldsymbol{x})$ é um polinómio mónico irredutível.

Suponhamos, por hipótese de indução, que o resultado é válido para todos os polinómios não constantes de grau $< n$. Seja $r(\boldsymbol{x})$ um polinómio de grau n. Se $r(\boldsymbol{x})$ é irredutível nada há a provar (basta considerar a factorização canónica como no caso $n = 1$). Se $r(\boldsymbol{x})$ é redutível então $r(\boldsymbol{x}) = r_1(\boldsymbol{x})r_2(\boldsymbol{x})$, onde $1 \leq gr(r_1(\boldsymbol{x})) < n$ e $1 \leq gr(r_2(\boldsymbol{x})) < n$. Por hipótese de indução, $r_1(\boldsymbol{x})$ e $r_2(\boldsymbol{x})$ podem ser factorizados na forma (1), logo $r(\boldsymbol{x})$ também.

Quanto à unicidade da factorização, sejam

$$cp_1(\boldsymbol{x})^{n_1}p_2(\boldsymbol{x})^{n_2}\cdots p_t(\boldsymbol{x})^{n_t} = dq_1(\boldsymbol{x})^{m_1}q_2(\boldsymbol{x})^{m_2}\cdots q_k(\boldsymbol{x})^{m_k}$$

duas factorizações canónicas de $r(\boldsymbol{x})$. No polinómio da esquerda, c é o coeficiente do termo de maior grau, enquanto que no da direita esse coeficiente é d. Portanto $c = d$. Daqui segue imediatamente que

$$p_1(\boldsymbol{x})^{n_1}p_2(\boldsymbol{x})^{n_2}\cdots p_t(\boldsymbol{x})^{n_t} = q_1(\boldsymbol{x})^{m_1}q_2(\boldsymbol{x})^{m_2}\cdots q_k(\boldsymbol{x})^{m_k}. \tag{2}$$

Então $p_1(\boldsymbol{x}) \mid q_1(\boldsymbol{x})^{m_1}q_2(\boldsymbol{x})^{m_2}\cdots q_k(\boldsymbol{x})^{m_k}$ donde, pela Proposição 2 da aula anterior, $p_1(\boldsymbol{x}) \mid q_i(\boldsymbol{x})$ para algum $i \in \{1, 2, \ldots, k\}$. Como $q_i(\boldsymbol{x})$ é irredutível, então $q_i(\boldsymbol{x}) = ap_1(\boldsymbol{x})$ o que implica $a = 1$ (pois quer $q_i(\boldsymbol{x})$ quer $p_1(\boldsymbol{x})$ são mónicos), ou seja $q_i(\boldsymbol{x}) = p_1(\boldsymbol{x})$. Então (2) equivale a

$$p_1(\boldsymbol{x})^{n_1-m_i} = p_2(\boldsymbol{x})^{-n_2}\ldots p_t(\boldsymbol{x})^{-n_t}q_1(\boldsymbol{x})^{m_1}\ldots q_{i-1}(\boldsymbol{x})^{m_{i-1}}q_{i+1}(\boldsymbol{x})^{m_{i+1}}\ldots q_k(\boldsymbol{x})^{m_k},$$

o que implica $n_1 = m_i$ (senão, $p_1(\boldsymbol{x}) = q_i(\boldsymbol{x})$ dividiria algum $p_j(\boldsymbol{x})$, $j \neq 1$, ou algum $q_j(\boldsymbol{x})$, $j \neq i$, o que é manifestamente impossível pois $p_1(\boldsymbol{x})$ é diferente de qualquer

outro dos polinómios $p_j(\boldsymbol{x})$ e $q_i(\boldsymbol{x})$ é diferente de qualquer outro dos polinómios $q_j(\boldsymbol{x})$).

Cancelando $q_i(\boldsymbol{x})$ e $p_1(\boldsymbol{x})$ em (2) obtemos

$$p_2(\boldsymbol{x})^{n_2}\cdots p_t(\boldsymbol{x})^{n_t} = q_1(\boldsymbol{x})^{m_1}q_2(\boldsymbol{x})^{m_2}\cdots q_{i-1}(\boldsymbol{x})^{m_{i-1}}q_{i+1}(\boldsymbol{x})^{m_{i+1}}\cdots q_k(\boldsymbol{x})^{m_k}.$$

Repetindo o raciocínio, chegaremos à conclusão que $p_2(\boldsymbol{x}) = q_j(\boldsymbol{x})$ para algum $j \in \{1, 2, \ldots, i-1, i+1, \ldots, n\}$ e $n_2 = m_j$. Continuando assim, após um número finito de passos, temos provada a unicidade da factorização (1), a menos da ordem pela qual se escrevem os factores. ∎

Apêndice 1: apontamentos para estudo complementar

[O Teorema da Factorização Única é tão importante que é natural averiguar se se pode generalizar a outros anéis. Por outro lado, o estudo que acabámos de fazer dos anéis polinomiais $C[x]$ exibe tantas semelhanças com o anel $\mathbb{Z}$ dos inteiros que é bem possível que não sejam mera coincidência, e sejam sim casos particulares de resultados válidos num contexto muito mais geral.]

Como sabemos, um inteiro $p \neq 0$ não invertível é primo se $p|ab$ implica $p = a$ ou $p = b$. É claro que podemos adaptar esta definição a $C[x]$ e, mais geralmente, a $D[x]$. Do mesmo modo, podemos adaptar a definição de polinómio irredutível ao domínio dos inteiros:

DOMÍNIO	$\mathbb{Z}$	$C[x]$
unidades	$\mathcal{U}_{\mathbb{Z}} = \{-1, 1\}$	$\mathcal{U}_{C[x]} = \{p(\boldsymbol{x}) \in C[x] : gr(p(\boldsymbol{x})) = 0\}$
primo	$p \neq 0$, $p \notin \mathcal{U}_{\mathbb{Z}}$ $p\|ab \Rightarrow p\|a$ ou $p\|b$	$p(\boldsymbol{x}) \neq 0$, $p(\boldsymbol{x}) \notin \mathcal{U}_{C[x]}$ $p(\boldsymbol{x})\|a(\boldsymbol{x})b(\boldsymbol{x}) \Rightarrow p(\boldsymbol{x})\|a(\boldsymbol{x})$ ou $p(\boldsymbol{x})\|b(\boldsymbol{x})$
irredutível	$p \neq 0$, $p \notin \mathcal{U}_{\mathbb{Z}}$ $p = ab \Rightarrow a \in \mathcal{U}_{\mathbb{Z}}$ ou $b \in \mathcal{U}_{\mathbb{Z}}$ isto é $p = ab \Rightarrow a = 1$ ou $a = -1$ ou $b = 1$ ou $b = -1$	$p(\boldsymbol{x}) \neq 0$, $p(\boldsymbol{x}) \notin \mathcal{U}_{C[x]}$ $p(\boldsymbol{x}) = a(\boldsymbol{x})b(\boldsymbol{x}) \Rightarrow a(\boldsymbol{x}) \in \mathcal{U}_{C[x]}$ ou $b(\boldsymbol{x}) \in \mathcal{U}_{C[x]}$ isto é $p(\boldsymbol{x}) = a(\boldsymbol{x})b(\boldsymbol{x}) \Rightarrow gr(a(\boldsymbol{x})) = 0$ ou $gr(b(\boldsymbol{x})) = 0$

DOMÍNIO	$D[x]$
unidades	$\mathcal{U}_{D[x]} = \{p(\boldsymbol{x}) \in D[x] : p(\boldsymbol{x}) = c \in \mathcal{U}_D\}$
primo	$p(\boldsymbol{x}) \neq 0,\ p(\boldsymbol{x}) \notin \mathcal{U}_{D[x]}$ $p(\boldsymbol{x})\|a(\boldsymbol{x})b(\boldsymbol{x}) \Rightarrow p(\boldsymbol{x})\|a(\boldsymbol{x})$ ou $p(\boldsymbol{x})\|b(\boldsymbol{x})$
irredutível	$p(\boldsymbol{x}) \neq 0,\ p(\boldsymbol{x}) \notin \mathcal{U}_{D[x]}$ $p(\boldsymbol{x}) = a(\boldsymbol{x})b(\boldsymbol{x}) \Rightarrow a(\boldsymbol{x}) \in \mathcal{U}_{D[x]}$ ou $b(\boldsymbol{x}) \in \mathcal{U}_{D[x]}$ isto é $p(\boldsymbol{x}) = a(\boldsymbol{x})b(\boldsymbol{x}) \Rightarrow a(\boldsymbol{x}) = c \in \mathcal{U}_D$ ou $b(\boldsymbol{x}) = d \in \mathcal{U}_D$

É claro que podemos estender estas duas noções a um domínio de integridade D qualquer:

- $p \in D$ é *primo* se $p \neq 0$, $p \notin \mathcal{U}_D$ e $p|ab \Rightarrow p|a$ ou $p|b$;
- $p \in D$ é *irredutível* se $p \neq 0$, $p \notin \mathcal{U}_D$ e $p = ab \Rightarrow a \in \mathcal{U}_D$ ou $b \in \mathcal{U}_D$.

Portanto, os elementos irredutíveis são os que apenas admitem factorizações triviais e um elemento $p \neq 0$ é primo se e só se o respectivo ideal principal (p) é primo. É fácil verificar que nos anéis $\mathbb{Z}$ e $C[x]$ os elementos primos no sentido da definição acima são exactamente os elementos irredutíveis, e é apenas por razões históricas que usamos o termo "primo" em $\mathbb{Z}$ e o termo "irredutível" em $C[x]$. Não é esse o caso em todos os domínios de integridade, mas é possível identificar extensas classes de domínios onde estas duas noções são equivalentes, e onde é possível estabelecer uma generalização apropriada do Teorema Fundamental da Aritmética e do Teorema da Factorização Única em $C[x]$.

No caso geral, a única implicação que é válida é a seguinte:

$$\text{primo} \ \Rightarrow \ \text{irredutível}.$$

De facto, se $p \in D$ é primo e $p = ab$, então $p|a$ ou $p|b$. Se, por exemplo, $p|a$, então existe $x \in D$ tal que $a = px$. Concluímos então que $p = ab = pxb$, e como $p \neq 0$, $1 = xb$, ou seja, b é invertível. De igual forma, se $p|b$ concluímos que a é invertível.

A implicação recíproca é, em geral, falsa. Por exemplo, no domínio dos inteiros pares, 18 é irredutível mas não é primo, uma vez que $18|(6 \times 6)$ mas $18 \nmid 6$ (note que neste caso não há factorização única: $36 = 6 \times 6 = 2 \times 18$). Outro exemplo: no domínio

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\},$$

$9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5})$, donde $3|(2 + \sqrt{-5})(2 - \sqrt{-5})$. No entanto, 3, que é irredutível, não divide $2 + \sqrt{-5}$ nem $2 - \sqrt{-5}$, pelo que não é primo (note que também neste exemplo não há factorizações únicas).

No entanto, a demonstração, na Proposição 2 da Aula 9, de que todo o polinómio irredutível em $C[x]$ é primo pode imediatamente ser adaptada a qualquer domínio de ideais principais D. Portanto:

Proposição. *Num domínio de ideais principais, um elemento é irredutível se e só se é primo.* ∎

Um elemento a de um domínio de integridade D diz-se *associado* de b (e escreve-se $a \sim b$) se $a|b$ e $b|a$. Um domínio D diz-se um *domínio de factorização única* (abreviadamente, d.f.u.) se as seguintes duas condições são satisfeitas:

- Para cada $d \in D$ ($d \neq 0$, $d \notin \mathcal{U}$), existem elementos irredutíveis $p_1, p_2, \ldots, p_n$ tais que $d = p_1 p_2 \cdots p_n$.
- Se $p_1, p_2, \ldots, p_n$ e $q_1, q_2, \ldots, q_m$ são irredutíveis, e $p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$, então $n = m$ e existe uma permutação $\pi \in S_n$ tal que $p_i \sim q_{\pi(i)}$.

Por outras palavras, num domínio de factorização única, todo o elemento não-nulo e não invertível possui uma factorização num produto de elementos irredutíveis, e esta factorização é única a menos da ordem dos factores e da multiplicação de cada factor por uma unidade convenientemente escolhida. Por exemplo, em $\mathbb{Z}$, $1 \times 5 = 5 \times 1 = (-1) \times (-5) = (-5) \times (-1)$ são as únicas factorizações do primo 5 e $1 \times (-5) = (-5) \times 1 = (-1) \times 5 = 5 \times (-1)$ são as únicas factorizações do primo -5. Pelo Teorema Fundamental da Aritmética, $\mathbb{Z}$ é um domínio de factorização única. Pelo Teorema da Factorização Única em $C[x]$, $C[x]$ é um domínio de factorização única. Outro exemplo de domínio de factorização única é o anel dos *inteiros de Gauss*,

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

Mais exemplos: $D[x]$ é um d.f.u. sempre que D o é. Em particular, $\mathbb{Z}[x]$ é um d.f.u., assim como $D[x][y]$.

Pode ainda provar-se o seguinte:

Teorema. *Todo o domínio de ideais principais é um domínio de factorização única.*

O recíproco é falso, como o exemplo $\mathbb{Z}[x]$ mostra.

Observe-se que a factorização indicada na definição de d.f.u. pode equivalentemente ser expressa em potências de elementos irredutíveis, mas neste caso pode ser necessário incluir uma unidade u na factorização, que passa a ser da forma

$$d = up_1^{m_1} \cdots p_n^{m_n},$$

como enunciámos no teorema da factorização única em $C[x]$.

Mais pormenores:
[R. L. Fernandes e M. Ricou, Introdução à Álgebra, IST Press, 2004]
[M. Sobral, Álgebra, Universidade Aberta, 1996]

Apêndice 2: critérios de irredutibilidade (para as aulas práticas)

Como vimos, em $\mathbb{C}[x]$ e $\mathbb{R}[x]$ sabemos quais são os polinómios irredutíveis:

(1) Em $\mathbb{C}[x]$ os polinómios irredutíveis são os polinómios de grau 1.

[Pelo Teorema Fundamental da Álgebra, que assegura que qualquer polinómio não constante de coeficientes em $\mathbb{C}$ tem pelo menos uma raiz complexa]

(2) Em $\mathbb{R}[x]$ os polinómios irredutíveis são os de grau 1 e os de grau 2 com binómio discriminante negativo ($a\boldsymbol{x}^2 + b\boldsymbol{x} + c$ tal que $b^2 - 4ac < 0$).

[Também pelo Teorema Fundamental da Álgebra]

A situação é diferente em $\mathbb{Q}[x]$:

(3) Em $\mathbb{Q}[x]$ a identificação dos irredutíveis é mais difícil. Neste caso apenas conhecemos condições suficientes de irredutibilidade mas não podemos indicar explicitamente os polinómios irredutíveis como fizemos nos dois casos anteriores.

Em primeiro lugar vejamos que todo o polinómio de coeficientes inteiros que seja irredutível em $\mathbb{Z}[x]$ também o é em $\mathbb{Q}[x]$ (contudo, o recíproco é falso: $2x$ é irredutível em $\mathbb{Q}[x]$ mas é redutível em $\mathbb{Z}[x]$ — pois quer 2 quer x não são unidades de $\mathbb{Z}[x]$):

Lema. [Lema de Gauss]
Se um polinómio $p(\boldsymbol{x}) \in \mathbb{Z}[x]$ se pode escrever como produto de dois polinómios $a(\boldsymbol{x})$ e $b(\boldsymbol{x})$ de $\mathbb{Q}[x]$, com graus inferiores ao de $p(\boldsymbol{x})$, então existem $a_1(\boldsymbol{x})$ e $b_1(\boldsymbol{x})$ em $\mathbb{Z}[x]$ tais que $p(\boldsymbol{x}) = a_1(\boldsymbol{x})b_1(\boldsymbol{x})$, sendo $a_1(\boldsymbol{x})$ associado de $a(\boldsymbol{x})$ e $b_1(\boldsymbol{x})$ associado de $b(\boldsymbol{x})$.

Deste lema conclui-se que

> *um polinómio de coeficientes inteiros é irredutível em $\mathbb{Q}[x]$ se e só se não pode decompor-se num produto de polinómios de grau ≥ 1 em $\mathbb{Z}[x]$.*

É claro que a todo o polinómio de coeficientes racionais se pode associar um polinómio de coeficientes inteiros: basta multiplicá-lo pelo mínimo múltiplo comum dos denominadores dos coeficientes.

Também é simples calcular as raízes racionais (logo os factores lineares) de polinómios de coeficientes inteiros:

Proposição. *Se o número racional $\dfrac{c}{d}$ é raiz do polinómio de coeficientes inteiros*

$$a_0 + a_1\boldsymbol{x} + a_2\boldsymbol{x}^2 + \cdots + a_n\boldsymbol{x}^n, \text{ com } n \geq 1,$$

então c divide a_0 e d divide a_n.

(Este resultado é muito útil. Por exemplo, se quisermos saber *se o polinómio $2\boldsymbol{x}^7 + 1 \in \mathbb{Z}_3[x]$ tem raízes no corpo $\mathbb{Z}_3$*, como $\mathbb{Z}_3$ tem apenas três elementos, é possível calcular o valor da respectiva função polinomial em cada um deles, concluindo-se que 1 é a única raiz do polinómio. No entanto, se substituirmos $\mathbb{Z}_3$ por $\mathbb{Q}$, já não é possível calcular o valor da função polinomial em todos os elementos de $\mathbb{Q}$. Contudo, a proposição acima reduz o nosso campo de procura a um conjunto finito. Os elementos de $\mathbb{Q}$ que podem ser raízes do polinómio são 1, -1, 1/2 e -1/2. É fácil ver que *estes números não são raízes do polinómio.* Portanto ele não tem raízes racionais.)

Deste modo, determinar os factores lineares, quando existam, de um polinómio de coeficientes inteiros é simples. O problema é mais complicado para factores de

ordem superior. O critério seguinte dá-nos uma condição suficiente de irredutibilidade em $\mathbb{Q}[x]$:

Teorema. [Critério de Eisenstein]
Seja $a(\boldsymbol{x}) = a_0 + a_1\boldsymbol{x} + \cdots + a_n\boldsymbol{x}^n$ *um polinómio de coeficientes inteiros. Se existe um inteiro primo* p *tal que*

(1) $p|a_i$ *para* $i = 0, 1, \ldots, n-1$,

(2) $p \nmid a_n$,

(3) $p^2 \nmid a_0$,

então $a(\boldsymbol{x})$ *é irredutível em* $\mathbb{Q}[x]$.

Utilizando este critério, podemos concluir que são irredutíveis sobre $\mathbb{Q}$, por exemplo, os polinómios

$$\frac{1}{2}\boldsymbol{x}^4 - 2\boldsymbol{x}^2 + 1 = \frac{1}{2}(\boldsymbol{x}^4 - 4\boldsymbol{x}^2 + 2),$$

$$\boldsymbol{x}^7 + 11\boldsymbol{x}^4 - 22\boldsymbol{x} + 11,$$

$$\boldsymbol{x}^5 + 9\boldsymbol{x}^3 + 27\boldsymbol{x}^2 + 3$$

e muitos outros. Mas nada podemos concluir sobre, por exemplo, $\boldsymbol{x}^5 - 3\boldsymbol{x}^2 + 6\boldsymbol{x} + 5$. Como proceder neste caso?

É fácil concluir que o polinómio não tem factores lineares. Suponhamos então que

$$\boldsymbol{x}^5 - 3\boldsymbol{x}^2 + 6\boldsymbol{x} + 5 = (a_1\boldsymbol{x}^2 + b_1\boldsymbol{x} + c_1)(a_2\boldsymbol{x}^3 + b_2\boldsymbol{x}^2 + c_2\boldsymbol{x} + d_2)$$

é uma factorização desse polinómio em $\mathbb{Z}[x]$. Verifica-se com relativa facilidade que o sistema

$$\begin{cases} a_1a_2 = 1 \\ a_1b_2 + b_1a_2 = 0 \\ a_1c_2 + b_1b_2 + c_1a_2 = 0 \\ a_1d_2 + b_1c_2 + c_1b_2 = -3 \\ b_1d_2 + c_1c_2 = 6 \\ c_1d_2 = 5 \end{cases}$$

não tem soluções inteiras. Logo, o polinómio é irredutível em $\mathbb{Q}[x]$.

Este tipo de problemas pode resolver-se de modo mais rápido com a ajuda de outros critérios.

Dado um homomorfismo de anéis $\phi : A \to B$, é evidente que existe um homomorfismo $\overline{\phi} : A[x] \to B[x]$ tal que $\overline{\phi}_{|A} = \phi$, definido por

$$\overline{\phi}\Big(\sum_{i=0}^{n} a_i \boldsymbol{x}_i\Big) = \sum_{i=0}^{n} \phi(a_i)\boldsymbol{x}^i.$$

Teorema. *Sejam A um corpo, B um domínio de integridade, $\phi : A \to B$ um homomorfismo e $a(\boldsymbol{x}) \in A[x]$. Se $\overline{\phi}(a(\boldsymbol{x}))$ tem o mesmo grau de $a(\boldsymbol{x})$ e é irredutível em $B[x]$, então $a(\boldsymbol{x})$ é irredutível em $A[x]$.*

No caso mais geral de A ser um domínio de integridade, este resultado ainda é válido para polinómios mónicos:

Teorema. *Sejam A e B domínios de integridade, $\phi : A \to B$ um homomorfismo e $a(\boldsymbol{x}) \in A[x]$ mónico. Se $\overline{\phi}(a(\boldsymbol{x}))$ tem o mesmo grau de $a(\boldsymbol{x})$ e é irredutível em $B[x]$, então $a(\boldsymbol{x})$ é irredutível em $A[x]$.*

Exemplo: Consideremos o polinómio $a(\boldsymbol{x}) = \boldsymbol{x}^5 - 3\boldsymbol{x}^2 + 6\boldsymbol{x} + 5$ e o homomorfismo $\phi : \mathbb{Z} \to \mathbb{Z}_2$ que a cada inteiro faz corresponder o resto da sua divisão por 2. A imagem de $a(\boldsymbol{x})$ pelo homomorfismo $\overline{\phi} : \mathbb{Z}[x] \to \mathbb{Z}_2[x]$ é $\overline{\phi}(a(\boldsymbol{x})) = \boldsymbol{x}^5 + \boldsymbol{x}^2 + 1$. Como é fácil verificar, este polinómio não tem nenhuma raiz em $\mathbb{Z}_2$, pelo que $\overline{\phi}(a(\boldsymbol{x}))$ não tem factores lineares em $\mathbb{Z}_2[x]$. Suponhamos que

$$\boldsymbol{x}^5 + \boldsymbol{x}^2 + 1 = (a_1\boldsymbol{x}^2 + b_1\boldsymbol{x} + c_1)(a_2\boldsymbol{x}^3 + b_2\boldsymbol{x}^2 + c_2\boldsymbol{x} + d_2)$$

é uma factorização desse polinómio em $\mathbb{Z}_2[x]$. Verifica-se facilmente que o sistema

$$\begin{cases} a_1a_2 = 1 \\ a_1b_2 + b_1a_2 = 0 \\ a_1c_2 + b_1b_2 + c_1a_2 = 0 \\ a_1d_2 + b_1c_2 + c_1b_2 = 1 \\ b_1d_2 + c_1c_2 = 0 \\ c_1d_2 = 1 \end{cases}$$

não tem solução em $\mathbb{Z}_2$. Então $\overline{\phi}(a(\boldsymbol{x}))$ é irredutível em $\mathbb{Z}_2[x]$ e, consequentemente, pelo Teorema e pelo Lema de Gauss, $a(\boldsymbol{x})$ é irredutível em $\mathbb{Q}[x]$.

Se considerarmos o homomorfismo $\phi : \mathbb{Z} \to \mathbb{Z}_5$, que a cada inteiro faz corresponder o seu resto na divisão por 5, vem $\overline{\phi}(a(\boldsymbol{x})) = \boldsymbol{x}^5 + 2\boldsymbol{x}^2 + \boldsymbol{x}$, que não é

irredutível em $\mathbb{Z}_5[x]$, pelo que neste caso já não podemos usar o teorema acima. Deste teorema podemos concluir que um polinómio $a(\boldsymbol{x})$ de coeficientes inteiros é irredutível sobre $\mathbb{Q}$ sempre que exista um homomorfismo $\phi : \mathbb{Z} \to B$ nas condições do teorema e $a(\boldsymbol{x})$ seja irredutível em $B[x]$. Em particular, se considerarmos, para algum primo p, o homomorfismo $\phi : \mathbb{Z} \to \mathbb{Z}_p$, que a cada inteiro faz corresponder o seu resto na divisão por p, temos:

Corolário. *Se $\overline{\phi}(a(\boldsymbol{x}))$ é irredutível em $\mathbb{Z}_p[x]$ e p não divide o coeficiente de maior grau de $a(\boldsymbol{x}) \in \mathbb{Z}[x]$, então $a(\boldsymbol{x})$ é um polinómio irredutível em $\mathbb{Q}[x]$.*

Apêndice 3: uma aplicação
Como encontrar números irracionais

O conjunto dos números reais é constituído pelos racionais e pelos irracionais. É bem conhecido que o conjunto dos números racionais é um conjunto enumerável. De facto existe uma relação um-um, ou seja, uma bijecção, entre o conjunto dos números racionais e o conjunto dos números naturais. Isto já não é verdade para o conjunto dos números irracionais: este conjunto tem cardinal estritamente superior ao de $\mathbb{N}$.

Que números irracionais conhece? Geralmente ocorrem-nos os exemplos $\sqrt{2}$, π (que coincide com a razão entre o perímetro e o diâmetro de qualquer circunferência), o número de Neper e e poucos mais. De facto, nem sempre é fácil demonstrar a irracionalidade de um número por métodos elementares. No que se segue vamos utilizar algumas propriedades dos domínios de factorização única $\mathbb{Z}$ e $\mathbb{Z}[x]$ para demonstrar a irracionalidade de muitos números reais.

Números irracionais

Começamos por recordar a demostração da irracionalidade de $\sqrt{2}$ atribuída a Pitágoras. Ela tem como base o seguinte: para todo o inteiro n, se n^2 é par então n é par. Suponhamos que existem inteiros p e q tais que

$$\sqrt{2} = \frac{p}{q},$$

e que p e q não são ambos pares (não há perda de generalidade nesta assumpção: se fossem ambos pares, dividiríamos por 2 ambos os membros da fracção, o número de vezes necessário até estarmos na situação pretendida). Então $p^2 = 2q^2$, pelo

que p^2 é par e, consequentemente, p também. Portanto, $p = 2k$ para algum inteiro k. Mas então, voltando atrás, obtemos $4k^2 = 2q^2$, donde $2k^2 = q^2$, e q^2 é par. Portanto q é também par, chegando-se assim a uma conclusão absurda.

Esta era a demonstração, referida por Aristóteles como sendo dos Pitagóricos, usada pelos Gregos para provar que

> *Num triângulo rectângulo isósceles a razão entre a hipotenusa e qualquer um dos catetos não é um número racional* $\frac{p}{q}$.

Esta é uma das primeiras demonstrações de que há memória na história da matemática. Constitui o primeiro exemplo conhecido de demonstração por *redução ao absurdo*. Os comprimentos da hipotenusa e dos catetos deste tipo de triângulo são o que Euclides designa no Livro X dos *Elementos* por grandezas que não são *comensuráveis* num sentido óbvio: duas grandezas da mesma espécie A e B dizem-se *comensuráveis* se existe uma grandeza da mesma espécie C e inteiros p e q tais que A=pC e B=qC. Ora isso não sucede neste caso: não é possível arranjar uma unidade de comprimento que "caiba" um número inteiro de vezes simultaneamente na hipotenusa e num dos catetos.

Sabe-se que Teodoro de Cirene provou a irracionalidade de $\sqrt{n}$ para

$$n = 3, 5, 6, 7, 8, 10, 11, 12, 13, 14, 15, 17,$$

isto é, para todo o inteiro até 17 que não é quadrado perfeito, mas não chegaram até nós essas provas.

Estas descobertas foram, ao tempo, extremamente inquietantes, como se pode ver pela lenda criada a esse respeito,

> *"... e o divulgador da descoberta dos irracionais, um certo Hippase de Métaponte, foi engolido pelas vagas",*

interpretada por Proclus da seguinte forma:

> *"Os autores da lenda quiseram falar através duma alegoria. Eles queriam dizer que tudo o que é irracional e privado de formas deve manter-se escondido. Que qualquer alma que queira penetrar nessa região secreta e deixá-la aberta, é arrastada pelo mar do futuro e afogada no incessante movimento das correntes."*

E mais uma citação:

"O mais insuportável na matemática são os números irracionais. A sua introdução na aritmética é um verdadeiro escândalo. Ao lado da noção de inteiro que é a noção mais clara do mundo, ao lado das proposições mais puras, belas e perfeitas, eis que aparece todo o cortejo de transcendentes e de infinito.

É no número real que estão condensadas as dificuldades das ideias de limite, de convergência e de continuidade. Se queremos escrever $\sqrt{2}+\sqrt{3}$ *não o podemos evitar e é inútil indignar-mo-nos: a ideia de infinito está na necessidade das coisas; tê-la-emos reduzido à sua forma mais simples dizendo que depois de um inteiro há sempre outro, mas não podemos libertar-nos desta realidade."*

[J. Dhombres, *Nombre, Mesure et Continu. Épistémologie et Histoire*, l'IREM de Nantes]

$\sqrt[n]{a}$ é quase sempre irracional

Porquê Teodoro de Cirene parou em $\sqrt{17}$?

Como é que ele provou a irracionalidade desses números?

É um mistério! É claro que Cirene podia muito bem ter adaptado a demonstração de Pitágoras aos outros casos. Por exemplo, no caso da $\sqrt{3}$:

Se

$$\sqrt{3}=\frac{p}{q},$$

onde, sem perda de generalidade, p e q não são ambos divisíveis por 3, então

$$p^2=3q^2 \Rightarrow 3|p^2 \Rightarrow 3|p,$$

isto é, $p=3k$, para algum inteiro k. Assim, $9k^2=3q^2$, ou seja, $3k^2=q^2$, donde se conclui que 3 divide q, o que contradiz a hipótese.

De forma análoga se demonstra a irracionalidade de qualquer raiz quadrada de um número primo.

Também para outros inteiros positivos, que não sejam quadrados perfeitos, tais como $\sqrt{6}$, basta supor que

$$\sqrt{6}=\frac{p}{q},$$

sendo p e q primos entre si, para chegar facilmente a uma contradição.

Mais irracionais

Recordemos a proposição da página 6. Trata-se de um resultado útil em muitas questões. Por exemplo:

O polinómio $2\boldsymbol{x}^7 + 1 \in \mathbb{Z}_3[x]$ *tem raízes no corpo* $\mathbb{Z}_3$*?*

Claro que sim: como $\mathbb{Z}_3$ tem apenas três elementos, é possível calcular o valor da função polinomial associada ao polinómio em cada um deles, concluindo-se que 1 é raiz do polinómio. E se substituirmos $\mathbb{Z}_3$ por $\mathbb{Q}$ no problema referido? Neste caso não é possível calcular o valor da função polinomial associada em todos os elementos de $\mathbb{Q}$. Mas a proposição reduz o nosso campo de procura a um conjunto finito. Os elementos de $\mathbb{Q}$ que podem ser raízes do polinómio são 1, -1, 1/2 e -1/2. É fácil ver que nenhum destes números é raiz do polinómio. Portanto, não tem raízes racionais.

Em particular, se o polinómio for mónico, temos:

Corolário. *As raízes reais de qualquer polinómio mónico de coeficientes inteiros*

$$a_0 + a_1\boldsymbol{x} + a_2\boldsymbol{x}^2 + \cdots + \boldsymbol{x}^n \quad (n \geq 1)$$

são números inteiros ou irracionais. ∎

Então, como $\sqrt{2}$ é raiz de $\boldsymbol{x}^2-2$, $\sqrt{3}$ é raiz de $\boldsymbol{x}^2-3$, $\sqrt{6}$ é raiz de $\boldsymbol{x}^2-6$ e, de uma forma geral, para qualquer inteiro positivo a, $\sqrt{a}$ é raiz de $\boldsymbol{x}^2 - a$, um polinómio cujas raízes reais só podem ser inteiras ou irracionais, $\sqrt{a}$ é necessariamente um inteiro (o que quer dizer que a é um quadrado perfeito) ou um irracional.

Também para $\sqrt[3]{a}$, com a inteiro, dois casos podem ocorrer:

(1) a é um cubo perfeito, ou

(2) a raiz cúbica real de a é irracional.

Assim, a raiz cúbica real de a é irracional para $a = 2, 3, 4, 5, 6, 7, 9, 10, \ldots$

De modo geral, para quaisquer inteiros a e n superiores à unidade, como $\sqrt[n]{a}$ é raiz de $\boldsymbol{x}^n - a$, então $\sqrt[n]{a}$ é um inteiro ou um irracional. Por exemplo, $\sqrt[5]{245}$ e $\sqrt[6]{16000}$ são irracionais.

Números trigonométricos irracionais

Todos sabemos que $\cos 60°$, $\sin 30°$ e $\tan 45°$ são números racionais: $1/2$, $1/2$ e 1, respectivamente. O que já não é tão conhecido é que

> *Se θ é um ângulo cuja medida em graus é um número racional entre $0°$ e $90°$, então $\cos\theta$, $\sin\theta$ e $\tan\theta$ são números irracionais com excepção de $\cos 60°$, $\sin 30°$ e $\tan 45°$.*

Para provar esta afirmação necessitamos da identidade

$$2\cos n\theta = (2\cos\theta)^n + a_{n-1}(2\cos\theta)^{n-1} + \cdots + a_1(2\cos\theta) + a_0, \tag{3}$$

com $n \geq 1$ e $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Z}$, que é válida para todo o inteiro positivo n, como facilmente se pode demonstrar por indução sobre n.

Se θ é o número racional c/d, para $n = 360\,d$ vem $\cos n\theta = \cos(360c) = 1$, o que significa, por (3), que $2\cos\theta$ é raiz do polinómio de coeficientes inteiros

$$-2 + a_0 + a_1\boldsymbol{x} + \cdots + a_{n-1}\boldsymbol{x}^{n-1} + \boldsymbol{x}^n.$$

Logo, $2\cos\theta$, sendo raiz real de um polinómio mónico de coeficientes inteiros, é um inteiro ou um irracional.

- Como $0 < \cos\theta < 1$, $2\cos\theta \in \mathbb{Z}$ implica $\cos\theta = 1/2$, logo $\theta = 60°$. Portanto, o único cosseno que é inteiro é o de $60°$.

- Como $\sin\theta = \cos(90° - \theta)$, o único seno que é inteiro é o de θ tal que $90° - \theta = 60°$, ou seja, $\theta = 30°$.

- Da igualdade
$$\cos 2\theta = \frac{1 - \tan^2\theta}{1 + \tan^2\theta}$$
conclui-se que, se $\tan\theta$ é racional, $\cos 2\theta$ também o é. Mas, para 2θ entre $0°$ e $180°$, $\cos 2\theta$ é racional para 2θ igual a $60°$, $90°$ ou $120°$, ou seja, para θ igual a $30°$, $45°$ ou $60°$. Como $\tan 30° = \sqrt{3}/3$ e $\tan 60° = \sqrt{3}$ são irracionais, resta apenas $\tan 45°$, que, sendo igual a 1, é racional.

Irracionais da forma $\log_m n$

Se m e n são números naturais, $\log_m n \in \mathbb{Q}$ se e só se m e n têm os mesmos factores primos e a razão das potências dos mesmos primos nas factorizações de m e n são iguais.

Encontrar números desta forma que sejam irracionais é muito fácil:

$$\log_{10} 2,\ \log_{10} 6,\ \log_{20} 4, \ldots$$

Já é preciso pensar um pouco para indicar um racional deste tipo: para $\log_m 12$ ser racional, m pode tomar os valores $2^2 \times 3$, $2^4 \times 3^2$ e, mais geralmente, qualquer número da forma $2^{2k} \times 3^k$ ($k \in \mathbb{N}$). Além disso, só estes valores de m é que dão origem a racionais. Este resultado aparece no artigo [*Another shoal of irrationals*, Mathematical Gazette 70 (1986) 218-219] de T. Crilly. O artigo termina com a seguinte frase:

> *"Such a stringent condition may reinforce our belief that almost all real numbers are irrational!"*

3. Teoria de Galois

Motivação

O desenvolvimento da Álgebra está intimamente ligado à resolução de equações polinomiais de coeficientes reais (ou complexos). Uma *equação polinomial* é uma equação do tipo

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0. \tag{4}$$

Ao primeiro membro chama-se, como vimos no capítulo anterior, um polinómio na indeterminada x.

Resolver a equação (4) é determinar as suas soluções (ou seja, as raízes do polinómio), isto é, os valores numéricos para x que transformam a equação numa identidade verdadeira.

A equação do primeiro grau, ou linear,

$$ax + b = 0 \quad (a \neq 0)$$

tem uma só solução, óbvia,

$$x = -\frac{b}{a}.$$

A solução de uma equação quadrática era já conhecida pelos matemáticos da Babilónia, que sabiam como "completar o quadrado", e foi popularizada no mundo ocidental durante o Renascimento, por traduções em latim do livro do

matemático islâmico Muhammad al-Khowarizmi[1], *Al-jabr wa'l muqābalah*[2], publicado na primeira metade do século IX. Todos sabemos hoje que a equação do segundo grau

$$ax^2 + bx + c = 0 \quad (a \neq 0)$$

tem soluções dadas pela fórmula

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

Será possível encontrar uma fórmula semelhante para resolver equações do terceiro grau

$$ax^3 + bx^2 + cx + d = 0 \quad (a \neq 0)?$$

E de grau superior?

Vejamos em primeiro lugar o que significa "fórmula semelhante". O que se pretende saber é se existe um processo geral para calcular as raízes de equações de grau superior a dois, a partir dos coeficientes, aplicando as operações racionais (adição, subtracção, multiplicação e divisão) e a extracção de raízes, um número finito de vezes. Soluções obtidas desta forma chamam-se *soluções por radicais*.

Em segundo lugar, observemos que na procura das raízes de um polinómio

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

é evidente que podemos, sem perda de generalidade, supor $a_n = 1$. Além disso, basta considerar o caso $a_{n-1} = 0$. Com efeito, supondo já $a_n = 1$, a mudança de variável

$$x = y - \frac{a_{n-1}}{n} \tag{5}$$

transforma o polinómio dado num polinómio em y em que o coeficiente de y^{n-1} é zero, sendo as raízes do primeiro polinómio facilmente calculáveis a partir das raízes deste novo polinómio `[confirme]`.

No século XVI, matemáticos italianos descobriram uma fórmula para resolver as equações do terceiro e quarto graus (vale a pena referir que a descoberta destas fórmulas e a luta pela prioridade da sua descoberta tem uma história bastante curiosa e divertida). Geronimo Cardano (1501-1576), também conhecido por Cardan, inclui no seu livro *Ars Magna*, publicado em 1545, fórmulas para a resolução

[1] Nome que deu origem às palavras *algarismo* — para designar cada um dos dígitos de numeração árabe — e *algoritmo* — o termo moderno que designa um procedimento sistemático para resolver problemas matemáticos.

[2] A partir de al-Khowarizmi, o termo *al-jabr* tornou-se sinónimo de resolver equações (*álgebra*).

de equações do terceiro e quarto graus, atribuídas pelo autor, respectivamente, a Nicolo Tartaglia (1500-1565) e Ludovico Ferrari (1522-1565).

A "fórmula de Cardan", como é hoje conhecida, para resolver a equação cúbica da forma

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

escrita em linguagem actual, é a seguinte:

$$y = \sqrt[3]{\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}.$$

Usando (5), o caso geral de uma equação do terceiro grau

$$x^3 + bx^2 + cx + d = 0$$

pode ser reduzido a este caso pela translação $x = y - b/3$. A verificação, por substituição, de que a fórmula de Cardan fornece uma solução da equação deverá dar uma ideia do grau de dificuldade envolvido neste tipo de problema.

A equação do quarto grau pode também ser reduzida à solução de uma cúbica. Com efeito, podemos sempre supor, eventualmente após uma translação (5), que a quártica é da forma

$$x^4 + ax^2 + bx + c = 0.$$

Completando o quadrado, obtemos

$$x^4 + ax^2 + bx + c = 0 \Leftrightarrow (x^2 + a)^2 = ax^2 - bx - c + a^2.$$

O truque consiste em observar que então, para qualquer y, temos

$$\begin{aligned} (x^2 + a + y)^2 &= ax^2 - bx - c + a^2 + 2y(x^2 + a) + y^2 \\ &= (a + 2y)x^2 - bx + (a^2 - c + 2ay + y^2). \end{aligned} \tag{6}$$

Como esta última equação é quadrática em x, podemos escolher y de forma a que seja um quadrado perfeito. Isto consegue-se precisamente, impondo que o discriminante $b^2 - 4(a + 2y)(a^2 - c + 2ay + y^2)$ seja zero, o que dá uma equação cúbica em y,

$$-8y^3 - 20ay^2 + (-16a^2 + 8c)y + (b^2 - 4a^3 + 4ac) = 0,$$

que pode ser resolvida com recurso à fórmula de Cardan. Para este valor de y, o membro direito de (6) fica igual ao quadrado perfeito

$$\left(x - \frac{b}{2(a + 2y)}\right)^2,$$

de forma que, extraindo as raízes em ambos os membros de (6), obtemos uma equação quadrática que pode ser resolvida.

Nos três séculos que se seguiram, muitos esforços foram feitos para obter uma fórmula resolvente para a equação quíntica. No princípio do século XIX, Niels Henrik Abel (1802-1829), na sequência de trabalhos de matemáticos eminentes como Joseph Lagrange (1736-1813) e Paolo Ruffini (1765-1833), provou que existem equações do quinto grau cujas soluções não podem ser obtidas por radicais. Este facto levantou de imediato um novo problema: dada uma equação desse grau como reconhecer se ela é ou não resolúvel por radicais?

Foi Évariste Galois (1811-1832) quem obteve uma condição necessária e suficiente para a resolubilidade por radicais de uma equação polinomial de qualquer grau e mostrou a impossibilidade de resolução da equação algébrica geral de grau maior ou igual a cinco. Este matemático, com uma vida breve e aventurosa, é considerado o criador da Álgebra tal como ela é entendida nos nossos dias e o seu trabalho teve consequências muito para além do problema original da resolução de equações algébricas por radicais. Galois associou a cada equação um grupo, hoje chamado *grupo de Galois*; as propriedades desse grupo revelam a resolubilidade por radicais da equação. O feito de Galois é tanto mais notável quanto a noção de grupo era ainda incipiente nessa altura.

Para ilustrarmos as ideias de Galois, consideremos a equação quártica com coeficientes racionais

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

Esta equação tem as raízes $r_k = e^{i\frac{2\pi k}{5}}$ $(k = 1, 2, 3, 4)$. Pensemos agora em todas as possíveis equações polinomiais, com coeficientes racionais, que são satisfeitas por estas raízes. Estas incluem, entre outras, as equações

$$\begin{aligned}
&r_1 + r_2 + r_3 + r_4 - 1 = 0,\\
&(r_1 + r_4)^2 + r_1 + r_4 - 1 = 0,\\
&r_1 r_4 = 1,\\
&(r_1)^5 - 1 = 0,\\
&(r_4)^5 - 1 = 0,\\
&\dots
\end{aligned}$$

A observação chave é a seguinte: se considerarmos todas as permutações de $\{r_1, r_2, r_3, r_4\}$ que transformam equações deste tipo ainda em equações deste tipo, obtemos o chamado *grupo de Galois* da equação. Por exemplo, a permutação (14)(23) transforma todas as equações listadas em cima em equações dessa lista.

Pode provar-se que, neste exemplo, $G = \{id, (1243), (14)(23), (1342)\}$. Galois descobriu que a estrutura deste grupo é a chave para a resolução desta equação (mas antes Galois teve de inventar o próprio conceito de grupo, inexistente até à data!).

Consideremos por exemplo o subgrupo $H = \{id, (14)(23)\}$. É simples verificar que as expressões polinomiais nas raízes, com coeficientes racionais, que são fixas pelos elementos de H são precisamente os polinómios em $y_1 = r_1 + r_4$ e $y_2 = r_2 + r_3$. Mas y_1 e y_2 são as soluções da equação quadrática

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

Assim, e supondo que não conhecíamos as expressões das soluções da equação original, poderíamos descobri-las resolvendo primeiro esta equação quadrática, obtendo

$$r_1 + r_4 = \frac{-1 + \sqrt{5}}{2}, \qquad r_2 + r_3 = \frac{-1 - \sqrt{5}}{2},$$

e de seguida a equação quadrática

$$(x - r_1)(x - r_4) = x^2 - (r_1 + r_4)x + r_1 r_4 = 0,$$

já que de facto esta equação tem como coeficientes expressões polinomiais em y_1 e y_2 (pois $r_1 r_4 = 1$).

Note-se que o grupo de Galois pode ser caracterizado como o *grupo de simetrias* da equação original: são as transformações que levam soluções (raízes) em soluções preservando a estrutura algébrica das soluções. Este é precisamente o ponto de partida na exposição moderna da Teoria de Galois: constrói-se o corpo[3] $\mathbb{Q}(r_1, \ldots, r_n)$ gerado pelas raízes da equação, e os elementos do grupo de Galois aparecem como automorfismos destes corpos. Nesta linguagem, a Teoria de Galois consiste em transformar questões sobre a estrutura destes corpos em questões sobre a estrutura do grupo de automorfismos associado.

[3] A noção de corpo só foi formalizada por Dedekind em 1879, mais de 50 anos depois da morte trágica de Galois.