Extensões de corpos

As sucessivas extensões do conceito de número, dos naturais para os inteiros, racionais, reais e, finalmente, complexos foram impostas pela necessidade de *resolver equações polinomiais* ou, o que é equivalente, de *determinar raízes de polinómios*.

Os números irracionais surgiram com a necessidade de resolver a equação polinomial $x^2 - 2 = 0$, imposta pelo Teorema de Pitágoras. É bem conhecido que $x^2 + 1 = 0$ não tem solução no corpo dos reais. Para resolver uma tal equação foi necessária a introdução do número "imaginário" $i = \sqrt{-1}$. Portanto, estes problemas foram resolvidos com a construção de sucessivas extensões do conceito de número.

Nos nossos dias todos estes números nos são familiares mas é claro que não foi sempre assim. Atribui-se ao matemático do século XIX Leopold Kronecker (1823-1891) a seguinte frase:

Deus criou os números inteiros e tudo o resto é obra do homem.

Na resolução da equação do segundo grau, é com a maior tranquilidade que trabalhamos com o caso em que o binómio discriminante $b^2 - 4ac$ é negativo. Os números complexos são-nos perfeitamente familiares o que não sucedia no século XVI. De facto foi Cardan quem primeiro introduziu números da forma $a + \sqrt{-b}$, com a e b inteiros positivos. No entanto, fê-lo com sérias reservas e um forte sentimento de culpa.

É curioso notar que foi a determinação das soluções da equações de terceiro grau que levou à construção dos números complexos. As equações de grau dois e binómio discriminante negativo eram simplesmente classificadas como insolúveis mas, para a equação de terceiro grau, o caso muda de figura pois soluções reais são obtidas passando por números complexos. Por exemplo, a equação $x^3 - 15x - 4 = 0$, pela regra de Cardan dá

$$x = \sqrt[3]{2 + \sqrt{-121}} + \sqrt[3]{2 - \sqrt{-121}}$$

e, consequentemente, é considerada sem solução. No entanto, ela tem três raízes reais: $4, -2+\sqrt{3}$ e $-2-\sqrt{3}$. Isto foi constatado por Bombelli, também matemático italiano do século XVI. Ele foi o primeiro a introduzir uma notação para o que hoje denotamos por i e $-i$ (a que ele chamou "più di meno" e "meno di meno")

e a trabalhar com esses símbolos utilizando as regras bem conhecidas $i \times i = -1$, $-i \times i = 1$, etc. Às sucessivas extensões do conceito de número, dos naturais para os inteiros, racionais e reais, algumas bem conturbadas, tornava-se inevitável juntar mais uma: os números complexos.

A invenção de novos números se, por um lado, foi inevitável - por exemplo para resolver equações de terceiro grau, como já foi referido - não foi um processo pacífico nem facilmente aceite pela comunidade matemática como o revelam nomes tais como "irracionais" ou "imaginários".

O estudo que fizemos sobre anéis e corpos dá-nos, como veremos, um processo sistemático de "inventar raízes de polinómios". Neste processo os polinómios irredutíveis desempenham um papel determinante.

Sendo C um corpo, $K \subseteq C$ é um *subcorpo* de C quando K é um subconjunto não-vazio de C tal que $(K, +)$ é um subgrupo de $(C, +)$ e $(K \setminus \{0\}, \cdot)$ é um subgrupo de $(C \setminus \{0\}, \cdot)$.

[Observe: $K \subseteq C$ é um subcorpo de C sse
(1) $0, 1 \in K$
(2) $a - b \in K$ para quaisquer $a, b \in K$
(3) $ab^{-1} \in K$ para quaisquer $a \in K$, $b \in K \setminus \{0\}$]

EXTENSÃO DE UM CORPO

Diz-se que um corpo C é uma *extensão* de um corpo K, se K é um subcorpo de C. A extensão é *própria* quando $C \neq K$.

Consideremos o corpo de Galois de ordem p (prima), $\mathbb{F}_p = (\mathbb{Z}_p, \oplus_p, \otimes_p)$. Qualquer subcorpo K de $\mathbb{F}_p$ contém a identidade 1 logo contém os elementos

$$1 + 1, 1 + 1 + 1, \ldots, -1, -1 - 1, \ldots$$

Portanto $\mathbb{F}_p \subseteq K$, pelo que $K = \mathbb{F}_p$. Isto mostra que $\mathbb{F}_p$ não contém subcorpos próprios (isto é, $\neq \mathbb{F}_p$). Diz-se que $\mathbb{F}_p$ é um *corpo primo*. Portanto, os corpos primos são, em certo sentido, os *menores* corpos que existem. Outro exemplo de corpo primo é o corpo dos racionais: sendo K um subcorpo de $\mathbb{Q}$, se $1 \in K$ então imediatamente $\mathbb{Z} \subseteq K$, donde qualquer $\frac{n}{m} = nm^{-1}$ $(n \in \mathbb{Z}, m \in \mathbb{Z} \setminus \{0\})$ também pertence a K, isto é, $K = \mathbb{Q}$. Por outro lado, $\mathbb{R}$ e $\mathbb{C}$ não são primos.

Aproveitaremos agora para mostrar que os corpos $\mathbb{F}_p$ e $\mathbb{Q}$ são, a menos de isomorfismo, os *únicos* corpos primos que existem.

É fácil verificar que a intersecção de qualquer família de subcorpos de um corpo C é ainda um subcorpo de C.

[Este facto decorre imediatamente do correspondente facto para grupos, provado em Álgebra I]

Em particular, a intersecção de todos os subcorpos de C é um subcorpo P de C.

SUBCORPO PRIMO

A este subcorpo P chama-se *subcorpo primo* de C. Evidentemente, trata-se de um corpo primo.

Teorema. *O subcorpo primo de um corpo C é isomorfo a $\mathbb{F}_p$ ou a $\mathbb{Q}$, consoante a característica de C seja p ou 0.*

Demonstração. Consideremos a aplicação $\phi : \mathbb{Z} \to C$ definida por $\phi(n) = n1_C$, onde 1_C designa a identidade do corpo C. É evidente que ϕ é um homomorfismo de anéis:

- $\phi(n+m) = (n+m)1_C = n1_C + m1_C = \phi(n) + \phi(m)$.
- $\phi(nm) = (nm)1_C = (n1_C)(m1_C) = \phi(n)\phi(m)$.

Consideremos o *núcleo* de ϕ:

$$Nuc\,\phi = \{n \in \mathbb{Z} \mid \phi(n) = 0\}.$$

[Em Álgebra I foi observado que $Nuc\,\phi$ é um subgrupo de $\mathbb{Z}$. Observe agora que $Nuc\,\phi$ é um ideal de $\mathbb{Z}$]

Pelo Teorema do Isomorfismo para anéis, $\phi(\mathbb{Z}) \cong \mathbb{Z}/Nuc\,\phi$.

[Este teorema é uma generalização imediata para anéis do Teorema do Isomorfismo para grupos, estudado em Álgebra I: *Se $\phi : A \to B$ é um homomorfismo de grupos (anéis), e N é o núcleo de ϕ, então os grupos (anéis) $\phi(A)$ e A/N são isomorfos.*]

Como qualquer subcorpo de C contém 1_C, também contém $\phi(\mathbb{Z})$. Logo $\phi(\mathbb{Z})$ está contido no subcorpo primo P de C. Por outro lado,

$$Nuc\,\phi = \{n \in \mathbb{Z} \mid n1_C = 0\} = \begin{cases} p\mathbb{Z} & \text{se } car(C) = p \\ \\ \{0\} & \text{se } car(C) = 0 \end{cases}$$

No primeiro caso, tem-se $\phi(\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}_p$. Como $\mathbb{Z}_p$ é um corpo, $\phi(\mathbb{Z})$ é um corpo, donde necessariamente coincide com P.

No segundo caso, tem-se $\phi(\mathbb{Z}) \cong \mathbb{Z}/\{0\} \cong \mathbb{Z}$, donde $\mathbb{Z} \cong \phi(\mathbb{Z}) \subset P$. Portanto P contém uma cópia isomorfa de $\mathbb{Z}$. Estendendo o homomorfismo $\phi : \mathbb{Z} \to \phi(\mathbb{Z})$ a $\mathbb{Q}$, definindo $\overline{\phi} : \mathbb{Q} \to P$ por $\overline{\phi}(\frac{n}{m}) = \phi(n)\phi(m)^{-1}$, obtemos um isomorfismo de anéis, o que mostra que, neste caso, $P \cong \mathbb{Q}$.

[Alternativamente, podia observar-se, como fizemos no início da aula para $\mathbb{Q}$, que um corpo P que contenha(uma cópia de) $\mathbb{Z}$, terá que conter necessariamente (uma cópia de) $\mathbb{Q}$, pois $n, m \in P \Rightarrow \frac{n}{m} = nm^{-1} \in P$]

■

Exemplos: $\mathbb{Q}$ é o subcorpo primo de $\mathbb{R}$ e $\mathbb{C}$. Da mesma forma, $\mathbb{Q}$ é também o subcorpo primo de $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.

Qualquer extensão C de um corpo K pode ser vista como um espaço vectorial sobre K, tomando para adição vectorial $\oplus$ a própria adição no corpo e para multiplicação escalar $*$ a multiplicação em C:

$$\text{Adição vectorial:} \quad a \oplus b := a + b, \ \forall a, b \in C$$

$$\text{Multiplicação escalar:} \quad \kappa * a := \kappa a, \ \forall \kappa \in K, \ \forall a \in C$$

[Exercício: Verifique]

Este resultado é fundamental para o desenvolvimento da teoria dos corpos, porque nos permite aplicar as ferramentas da álgebra linear.

GRAU DE UMA EXTENSÃO

Seja C uma extensão de K. O *grau* da extensão C sobre K, que denotaremos por $[C : K]$, é a dimensão do espaço vectorial C sobre K. A extensão C diz-se *finita* se $[C : K]$ for finita, e diz-se uma *extensão infinita*, caso contrário.
