J. SEBASTIÃO E SILVA

# COMPÊNDIO DE MATEMÁTICA

1.º volume

2.º tomo

Curso Complementar
do Ensino Secundário

Edição GEP

LISBOA

CAPÍTULO VI

# ANÉIS E CORPOS. NÚMEROS COMPLEXOS. ÁLGEBRAS DE BOOLE

1. **Conceito de anel.** No capítulo anterior apareceram-nos vários exemplos de conjuntos em que são consideradas, ao mesmo tempo, duas ou mais operações. Nesses casos, porém, as operações foram, em geral, estudadas *separadamente* e não nas suas possíveis *interligações*. No presente capítulo vamos atender, precisamente, a tais interligações, que, como é de esperar, geram muito maior riqueza de propriedades.

Para começar, um exemplo sugestivo será ainda o conjunto H considerado nas páginas 27-29. Nesse conjunto, definimos apenas uma *adição* e foi precisamente ao grupóide (H, +), aliás módulo, que chamámos BAILADO DAS HORAS. Mas, é claro que no mesmo conjunto podemos definir uma multiplicação por um processo inteiramente análogo:

$$(1) \qquad \overline{m} \,.\, \overline{n} = \overline{m \,.\, n} \quad , \quad \forall\, \overline{m}, \overline{n} \in H$$

Nesta fórmula, m,n são números inteiros absolutos quaisquer, mas, tal como no caso da adição, podemos sempre substituir m,n

e m • n pelos restos das divisões destes números por 12. Assim, por exemplo:

$$\overline{5} \cdot \overline{7} = \overline{5 \cdot 7} = \overline{35} = \overline{11}$$
$$\overline{5} \cdot \overline{12} = \overline{5} \cdot \overline{0} = \overline{5 \cdot 0} = \overline{0}$$
$$\overline{4} \cdot \overline{9} = \overline{4 \cdot 9} = \overline{36} = \overline{0}$$
$$\overline{13} \cdot \overline{7} = \overline{1} \cdot \overline{7} = \overline{1 \cdot 7} = \overline{7}$$

Tal como no caso da adição, é fácil provar que a operação assim definida é *sempre possível* e *unívoca,* quer dizer: (H, • ) é um grupóide. Esta multiplicação pode também ser definida pela seguinte tabela:

x • y

| x \ y | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ | $\overline{5}$ | $\overline{6}$ | $\overline{7}$ | $\overline{8}$ | $\overline{9}$ | $\overline{10}$ | $\overline{11}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ |
| $\overline{1}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ | $\overline{5}$ | $\overline{6}$ | $\overline{7}$ | $\overline{8}$ | $\overline{9}$ | $\overline{10}$ | $\overline{11}$ |
| $\overline{2}$ | $\overline{0}$ | $\overline{2}$ | $\overline{4}$ | $\overline{6}$ | $\overline{8}$ | $\overline{10}$ | $\overline{0}$ | $\overline{2}$ | $\overline{4}$ | $\overline{6}$ | $\overline{8}$ | $\overline{10}$ |
| $\overline{3}$ | $\overline{0}$ | $\overline{3}$ | $\overline{6}$ | $\overline{9}$ | $\overline{0}$ | $\overline{3}$ | $\overline{6}$ | $\overline{9}$ | $\overline{0}$ | $\overline{3}$ | $\overline{6}$ | $\overline{9}$ |
| $\overline{4}$ | $\overline{0}$ | $\overline{4}$ | $\overline{8}$ | $\overline{0}$ | 4 | $\overline{8}$ | $\overline{0}$ | $\overline{4}$ | $\overline{8}$ | $\overline{0}$ | $\overline{4}$ | $\overline{8}$ |
| $\overline{5}$ | $\overline{0}$ | $\overline{5}$ | $\overline{10}$ | $\overline{3}$ | $\overline{8}$ | $\overline{1}$ | $\overline{6}$ | $\overline{11}$ | $\overline{4}$ | $\overline{9}$ | $\overline{2}$ | $\overline{7}$ |
| $\overline{6}$ | $\overline{0}$ | $\overline{6}$ | $\overline{0}$ | $\overline{6}$ | $\overline{0}$ | $\overline{6}$ | $\overline{0}$ | $\overline{6}$ | $\overline{0}$ | $\overline{6}$ | $\overline{0}$ | $\overline{6}$ |
| $\overline{7}$ | $\overline{0}$ | 7 | $\overline{2}$ | $\overline{9}$ | $\overline{4}$ | $\overline{11}$ | $\overline{6}$ | $\overline{1}$ | $\overline{8}$ | $\overline{3}$ | $\overline{10}$ | $\overline{5}$ |
| $\overline{8}$ | $\overline{0}$ | $\overline{8}$ | $\overline{4}$ | $\overline{0}$ | $\overline{8}$ | $\overline{4}$ | $\overline{0}$ | $\overline{8}$ | $\overline{4}$ | $\overline{0}$ | $\overline{8}$ | $\overline{4}$ |
| $\overline{9}$ | $\overline{0}$ | $\overline{9}$ | $\overline{6}$ | $\overline{3}$ | $\overline{0}$ | $\overline{9}$ | $\overline{6}$ | $\overline{3}$ | $\overline{0}$ | $\overline{9}$ | $\overline{6}$ | $\overline{3}$ |
| $\overline{10}$ | $\overline{0}$ | $\overline{10}$ | $\overline{8}$ | $\overline{6}$ | $\overline{4}$ | $\overline{2}$ | $\overline{0}$ | $\overline{10}$ | $\overline{8}$ | $\overline{6}$ | $\overline{4}$ | $\overline{2}$ |
| $\overline{11}$ | $\overline{0}$ | $\overline{11}$ | $\overline{10}$ | $\overline{9}$ | $\overline{8}$ | $\overline{7}$ | $\overline{6}$ | $\overline{5}$ | $\overline{4}$ | $\overline{3}$ | $\overline{2}$ | $\overline{1}$ |

Ainda como no caso da adição, a fórmula (1) permite-nos facilmente reconhecer que a multiplicação definida é associativa e comutativa. Mas, vê-se logo que a multiplicação não é reversível (pág. 51). Em compensação a fórmula (1) da pág. 71 e a fórmula (2) da pág. 28 permitem mostrar que

$$(2) \qquad (a + b) \cdot c = ac + bc, \quad \forall\, a, b, c \in H$$

Com efeito, sejam $a = \overline{m}$, $b = \overline{n}$, $c = \overline{p}$, com $m, n, p \in \mathbb{N}_0$. Então $(a + b)c$ será igual

$$(\overline{m}+\overline{n})\,\overline{p} = \overline{m+n} \cdot \overline{p} = \overline{(m+n) \cdot p} = \overline{mp+np} = \overline{mp}+\overline{np}$$

Mas $\overline{mp}+\overline{np} = \overline{m} \cdot \overline{p} + \overline{n} \cdot \overline{p} = ac + bc$, o que prova (2).

Por sua vez, daqui e da comutatividade da multiplicação, deduz-se

$$(3) \qquad a(b+c) = ab + ac \quad , \quad \forall\, a, b, c \in H$$

Pois bem, exprimem-se os factos (2) e (3) dizendo que a *multiplicação em* H *é distributiva relativamente à adição* (1). Ora, esta é precisamente uma PROPRIEDADE DE INTERLIGAÇÃO (ou, como também se diz, uma PROPRIEDADE DE ENLACE), das duas operações consideradas. Em resumo, verificam-se os seguintes factos:

1.º $(H,+)$ *é um grupo comutativo (portanto, um módulo)*

2.º $(H, \cdot)$ *é um semigrupo comutativo*

3.º *A operação* $\cdot$ *é distributiva relativamente à operação* $+$

---

(1) A fórmula (2) também se exprime dizendo que a multiplicação é *distributiva à esquerda* e a fórmula (3), dizendo que a multiplicação é *distributiva à direita*. Mas esta distinção só tem interesse quando a multiplicação não é comutativa.

Ora, exprime-se a conjunção destes três factos, abreviadamente, dizendo que o terno ordenado (H, +, ·) *é um anel comutativo.* A este anel convencionaremos chamar o ANEL DAS HORAS (foi ao *módulo* (H, +) que convencionámos chamar o BAILADO DAS HORAS). Dum modo geral:

DEFINIÇÃO. *Chama-se anel todo o terno ordenado (A, +, ·), constituído por um conjunto A, com mais de um elemento, e por duas operações, normalmente chamadas adição* (+) *e multiplicação* ( · ), *tais que:*

1) (A,+) é um grupo comutativo (módulo).
2) (A, · ) é um semigrupo.
3) A multiplicação é distributiva relativamente à adição, isto é:

$$(a+b)c = ac+bc \quad , \quad a(b+c) = ab + ac \quad , \quad \forall\, a, b, c, \in A$$

Diremos simplesmente 'o anel A' em vez de 'o anel (A, +, · )', sempre que estiver subentendido quais são as operações do anel.

O anel diz-se *comutativo,* sse a multiplicação for comutativa (caso do anel H).

Visto que todo o anel é um grupo relativamente à adição, chamaremos *zero* (ou *elemento nulo*) do anel, ao elemento neutro da adição; representá-lo-emos pelo símbolo (0 ou simplesmente por 0, se não houver perigo de confusão (no anel H o zero é $\overline{12} = \overline{0}$).

Se existe no anel elemento neutro da multiplicação, este será chamado *elemento unidade;* representá-lo-emos pelo símbolo **1** ou simplesmente por 1, se não houver perigo de confusão (1). (O anel H tem elemento unidade? Qual é?)

Convém ainda observar que, sendo um anel A ao mesmo tempo um *módulo* e um *semigrupo multiplicativo,* estão já definidos os con-

---

(1) Muitos autores representam por *o* o elemento unidade (inicial da palavra alemã 'oinheit', que significa 'unidade').

ceitos de *'produto* n.a', com $n \in Z$ e $a \in A$, e de *'potência* $a^n$', com $n \in \mathbb{N}$ e $a \in A$. Por exemplo, no ANEL DAS HORAS tem-se:

$$\overline{5} \cdot \overline{7} = \overline{7} + \overline{7} + \overline{7} + \overline{7} + \overline{7} = \overline{11} = \overline{5} \cdot \overline{7},$$
$$(-\overline{5}) \cdot \overline{7} = -(\overline{5} \cdot \overline{7}) = -\overline{11} = \overline{1},$$
$$\overline{5}^4 = \overline{5} \cdot \overline{5} \cdot \overline{5} \cdot \overline{5} = \overline{1}, \text{ etc.}$$

Por sua vez, da definição de anel resulta:

TEOREMA. *Num anel* A *a multiplicação é distributiva relativamente à subtracção, isto é, tem-se:*

$$(a-b)c = ac - bc \quad , \quad a(b-c) = ac-ac, \ \forall\, a, b, c \in A$$

Com efeito, a−b é, por definição, o número x tal que a = b + x.

Ora:

$$(b+x)c = bc + xc \qquad (\textit{Porquê?})$$

Donde:

$$xc = (b+x)c - bc \qquad (\textit{Porquê?})$$

E, portanto, como $x = a - b$ e $b + x = a$,

$$(a-b)c = ac - bc$$

COROLÁRIO 1. *Se* A *é um anel, tem-se:*

$$(0 \cdot a = a \cdot (0 = (0, \quad \forall\, a \in A$$

Com efeito, como $a-a = (0$ (*Porquê?*) tem-se:

$$(0 \cdot a = (a-a)\, a = a^2 - a^2 = (0 \qquad (\textit{Porquê?})$$

Portanto $(0 \cdot a = (0$.

Analogamente se prova que $a \cdot (0 = (0$.

COROLÁRIO 2. *Num anel o zero não pode ser elemento unidade.*

Com efeito, seja A um anel. Então, segundo a definição, A tem *mais de um elemento;* portanto, existe em A, pelo menos, um elemento c que não é (0. Ora, segundo o corolário 1, tem-se $0 \cdot c = (0$ e, como $c \neq (0$, vem $(0 \cdot c \neq c$, donde resulta que (0 não pode ser elemento unidade.

EXERCÍCIOS:

I. Verifique quais dos seguintes conjuntos são anéis, relativamente às operações usuais de adição e multiplicação: $\mathbb{N}$, $\mathbb{N}_0$, $Z$, $(\mathbb{Q}$, $\mathbb{R}$, $(\mathbb{Q}^+$, $\mathbb{R}^+$, $Z_2$ (*conjunto dos números pares relativos)*. Quais desses anéis são comutativos? Quais têm elemento unidade?

II. Seja $\mu$ um número inteiro maior que 1. Daqui por diante, designaremos por $A_\mu$ um conjunto constituído por $\mu$ elementos de *natureza qualquer,* cada um dos quais será designado por um símbolo da forma $\overline{n}$, com $n \in \mathbb{N}_0$, sendo, além disso, adoptadas as seguintes convenções:

1) $\overline{n} = \overline{n'}$, sse n e n' divididos por $\mu$ dão restos iguais.

2) $\overline{m} + \overline{n} = \overline{m+n}$ , $\overline{m} \cdot \overline{n} = \overline{m \cdot n}$, $\forall\, m, n \in \mathbb{N}_0$.

É claro que, se $\mu = 12$, $A_\mu$ é precisamente o ANEL DAS HORAS, isto é: $H = A_{12}$. Se $\mu = 4$, as operações +, • são dadas pelas duas seguintes tabelas:

x + y

| x \ y | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ |
|---|---|---|---|---|
| $\overline{0}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ |
| $\overline{1}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{0}$ |
| $\overline{2}$ | $\overline{2}$ | $\overline{3}$ | $\overline{0}$ | $\overline{1}$ |
| $\overline{3}$ | $\overline{3}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ |

x • y

| x \ y | 0 | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ |
|---|---|---|---|---|
| $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ |
| $\overline{1}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ |
| $\overline{2}$ | $\overline{0}$ | $\overline{2}$ | $\overline{0}$ | $\overline{2}$ |
| $\overline{3}$ | $\overline{0}$ | $\overline{3}$ | $\overline{2}$ | $\overline{1}$ |

e facilmente se reconhece que $A_4$ também é um anel. Um exemplo bastante familiar é o anel $A_9$, a que chamaremos ANEL DOS 'NOVES FORA', porque intervém nas provas dos nove das operações. Por exemplo, tem-se:

$$\overline{5} + \overline{8} = \overline{13} = \overline{4} \quad , \quad \overline{5} \cdot \overline{7} = \overline{35} = \overline{8} \quad (\text{em } A_9)$$

Posto isto, prove o seguinte facto geral:

*Qualquer que seja* $\mu$, $A_\mu$ *é um anel comutativo com elemento unidade.*

III. Introduzamos no conjunto $Z^2$ (quadrado cartesiano de $Z$) uma adição e uma multiplicação, mediante as seguintes fórmulas: $(a, b) + (c, d) = (a+c, b+d)$, $(a, b)\ (c, d) = (ac, bd)$, $\forall\ a, b, c, d \in Z$. [*Por exemplo:* $(2,3) + (6, -5) = (8, -2)$, $(2, 3) \cdot (6, -5) = (12, -15)$.] Prove que $Z^2$ é um anel comutativo com elemento unidade relativamente a estas duas operações. Qual é aqui o zero e qual é o elemento unidade?

IV. Prove que o conjunto dos números da forma $a + b\sqrt{2}$, com $a, b \in Z$, é um anel comutativo com elemento unidade (relativamente às operações usuais). Sugestão: trata-se de provar que a soma, a diferença e o produto de dois números deste conjunto ainda pertencem ao conjunto.

V. Prove que num anel A se tem:

$$\left.\begin{array}{l}(a+b)\ (c+d) = ac + ad + bc + bd \\ (a-b)\ (a+b) = a^2 + ab - ba - b^2\end{array}\right\} \quad \forall\ a, b, c, d \in A$$

e que, *se o anel* A *é comutativo,* será sempre

$$(a+b)^2 = a^2 + 2ab + b,$$
$$(a+b)\ (a-b) = a^2 - b^2,$$
$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3, \text{ etc.}$$

NOTA. Mais adiante estudaremos um exemplo importante de anel não comutativo (*anel dos quaterniões de Hamilton*). No 7.º ano estudaremos anéis não comutativos que intervêm hoje constantemente nas aplicações da matemática à física, à engenharia, à estatística, etc. (*anéis de matrizes*).

VI. Determine no anel $A_4$ *todas* as soluções de cada uma das seguintes equações: $x + \overline{1} = \overline{0}$, $x + \overline{1} = \overline{2}$, $x + \overline{2} = \overline{3}$, $x + \overline{2} = \overline{1}$, $\overline{3}x = \overline{1}$, $\overline{3}x = \overline{2}$, $\overline{2}x = 1$, $\overline{2}x = \overline{2}$, $\overline{2} - x = \overline{3}$, $\overline{1} - \overline{2}x = \overline{2}$, $\overline{1} - \overline{2}x = \overline{3}$.

2. **Isomorfismos entre anéis.** Dados dois anéis A e A', chama-se *isomorfismo de* A *sobre* A' toda a aplicação biunívoca f de A sobre A' tal que

$$f(x+y) = f(x) + f(y), \quad f(x \cdot y) = f(x) \cdot f(y), \quad \forall\, x, y \in A,$$

isto é, que seja ao mesmo tempo um isomorfismo de (A, +) sobre (A', +) e de (A, •) sobre (A', •). Nesta hipótese, se A = A' diz-se que f é um *automorfismo* do anel.

Diz-se que A é *isomorfo* a A', sse existe, pelo menos, um isomorfismo de A sobre A'. Facilmente se reconhece que a *relação de isomorfia entre anéis* também é uma relação de equivalência e que o PRINCÍPIO DE ISOMORFIA (pág. 35) se estende a anéis.

Consideremos, por exemplo, o anel U constituído por um conjunto de 4 elementos, z, u, i, j, com as seguintes operações:

$x + y$

| x \ y | z | u | i | j |
|---|---|---|---|---|
| z | z | u | i | j |
| u | u | z | j | i |
| i | i | j | z | u |
| j | j | i | u | z |

(z = (0)

$x \cdot y$

| x \ y | z | u | i | j |
|---|---|---|---|---|
| z | z | z | z | z |
| u | z | u | i | j |
| i | z | i | i | z |
| j | z | j | z | j |

(u = 1)

É fácil ver que este anel não é isomorfo ao anel $A_4$: basta observar, por exemplo, que a propriedade '$\exists x,\ x \neq \overline{0} \wedge x^2 = \overline{0}$' se verifica em $A_4$ (tem-se $\overline{2}^2 = \overline{0}$), mas não se verifica em U. No entanto, o anel U é isomorfo ao anel constituído pelo conjunto $A_2 \times A_2$, com as operações assim definidas:

$$(a, b) + (c, d) = (a+c, b+d),\ (a, b) \cdot (c, d) = (ac, bd),\ \forall\ a, b, c, d \in A_2$$

[Por exemplo, $(\overline{0},\overline{1}) + (\overline{1},\overline{1}) = (\overline{1},\overline{0})$, $(\overline{1},\overline{0}) \cdot (\overline{0},\overline{1}) = (\overline{0},\overline{0})$, etc.].

Com efeito, a aplicação

$$\begin{array}{cccc} z & u & i & j \\ \downarrow & \downarrow & \downarrow & \downarrow \\ (\overline{0},\overline{0}) & (\overline{1},\overline{1}) & (\overline{0},\overline{1}) & (\overline{1},\overline{0}) \end{array}$$

é, como facilmente se reconhece, um isomorfismo do anel U sobre o anel $A_2^2$. *(Existe algum outro isomorfismo entre estes dois anéis? Existe algum automorfismo de U diferente da identidade?)*

NOTAS — I. Pode acontecer que a primeira operação dum anel não se chame adição ou que a segunda não se chame multiplicação. Neste caso, o conceito de isomorfismo entre anéis define-se de modo análogo ao que fizemos para grupóides em geral.

II. Os anéis $A_\mu$, introduzidos no n.º 1, ex. 2, são *definidos a menos de um isomorfismo,* visto que deixámos inteira liberdade quanto à interpretação dos símbolos $\overline{0}$, $\overline{1}$, ..., $\overline{\mu-1}$ (podem designar pessoas, livros, cidades, etc.), *contanto que representem* $\mu$ *seres distintos.* Em particular, podemos adoptar a seguinte interpretação: $\overline{0}$ é o conjunto dos múltiplos de $\mu$, $\overline{1}$ é o conjunto dos inteiros que divididos por $\mu$ dão resto $\overline{1}$, e assim por diante.

Já atrás observámos que em matemática o que interessa não é a MATÉRIA (isto é, a natureza dos entes considerados), mas sim a FORMA (isto é, as propriedades formais das operações e relações).

Este ponto de vista confere à matemática um extraordinário poder unificador e uma imensa elasticidade nas aplicações. Dizia HENRI POINCARÉ: *'A matemática é a arte de dar o mesmo nome a coisas distintas — distintas pelo conteúdo, mas idênticas pela forma'.*

Verifica-se um facto semelhante em biologia. Um indivíduo biológico, isto é, um ser vivo, é, pelo menos na sua parte observável, constituído por *matéria,* que muda de instante para instante; o que se mantém, e torna o indivíduo idêntico a si mesmo ao longo do tempo, é algo a que poderíamos chamar *estrutura* ou *forma* (em sentido lato).

Assim, vemos reaparecer em matemática moderna o *conceito aristotélico de forma.*

3. **Cálculo algébrico num anel comutativo; operações sobre polinómios.** Das propriedades características dum anel, e em especial da propriedade de interligação, resultam várias regras de cálculo algébrico, que já foram estudadas no 2.º ciclo no caso particular do anel IR.

Seja A um anel *comutativo.* Chama-se *polinómio em* x relativo ao anel A toda a expressão da forma

$$a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n,$$

em que:

1.º — a letra x é uma *variável* em A;

2.º — nos lugares de $a_o$, $a_1$, ..., $a_n$ figuram constantes, que designam elementos de A (chamados coeficientes do polinómio);

3.º — no lugar de *n* figura uma *constante,* que designa um número inteiro absoluto.

Se $n > 0$ e $a_0 \neq 0$, diz-se que *n* é o *grau do polinómio.* Se $n = 0$, o polinómio reduz-se a uma constante, $a_0$, e diz-se então

que o *grau do polinómio* é zero (1). As expressões $a_0x^n$, $a_0x^{n-1}$, ..., $a^n$ (*monómios*) são os *termos* do polinómio, respectivamente, de *graus* n, n−1, ..., 0.

Por exemplo, no anel $A_{12}$, a expressão

$$\overline{3}x^4 + \overline{5}x^3 + \overline{1}x + \overline{9}x + \overline{6} \tag{1}$$

é um polinómio em x de grau 4 (ou do 4.º grau), cujos coeficientes são: $a_0 = \overline{3}$, $a_1 = \overline{5}$, $a_2 = \overline{1}$, $a_3 = \overline{9}$, $a_4 = \overline{6}$.

Analogamente, em $\mathbb{R}$, a expressão

$$\frac{2}{3}x^5 + 0x^4 + (-1)x^3 + (-4)x^2 + 1x + (-\sqrt{2})$$

é um polinómio em x do 5.º grau, que se escreve abreviadamente

$$\frac{2}{3}x^5 - x^3 - 4x^2 + x - \sqrt{2},$$

visto esta expressão ser equivalente à anterior.

Por sua vez, em $\mathbb{R}$, as expressões

$$0, \quad 5, \quad -2, \quad \sqrt{5}, \quad \pi, \quad \text{etc.}$$

são *constantes,* portanto *polinómios de grau zero,* que também se podem escrever sob a forma de polinómios de *grau aparente superior a zero*; por exemplo:

$$2 = 0 \cdot x + 2 = 0 \cdot x^2 + 0 \cdot x + 2 \quad (\forall x \in \mathbb{R})$$

Vejamos agora como se apresentam, de modo natural, operações algébricas sobre polinómios.

a) *Adição e subtracção.* Consideremos, por exemplo, os dois seguintes polinómios em x no anel $A_9$:

$$\overline{3}x^4 + \overline{5}x^3 + \overline{7}x^2 + x + \overline{5} \quad , \quad \overline{8}x^3 + \overline{6}x^2 + \overline{5}$$

---

(1) Convenciona-se aqui que $x^0 = 1$ para todo o valor de x, mesmo que esse valor não tenha inverso.

Então é fácil ver que, se tem, qualquer que seja $x \in A_9$:

$$(\overline{3}x^4 + \overline{5}x^3 + \overline{7}x^2 + x + \overline{5}) + (\overline{8}x^3 + \overline{6}x^2 + \overline{5}) = \overline{3}x^4 + \overline{4}x^3 + \overline{4}x^2 + x + \overline{1}$$

*Justifique esta equivalência, indicando em pomenor todas as propriedades em que se baseia nas diferentes passagens.*

É então natural dizer que o polinómio $\overline{3}x^4 + \overline{4}x^2 + x + \overline{1}$ é a *soma* dos polinómios dados, relativos ao anel $A_9$. A *adição* dos polinómios pode efectuar-se segundo o esquema habitual:

$$\begin{array}{r} \overline{3}x^4 + \overline{5}x^3 + \overline{7}x^2 + x + \overline{5} \\ \overline{8}x^3 + \overline{6}x^2 + \overline{5} \\ \hline \overline{3}x^4 + \overline{4}x^3 + \overline{4}x^2 + x + \overline{1} \end{array}$$

Analogamente se reconhece que, para todo o $x \in A_9$:

$$(\overline{3}x^4 + \overline{5}x^3 + \overline{7}x^2 + x + \overline{5}) - (\overline{8}x^3 + \overline{6}x^2 + \overline{5}) = \overline{3}x^4 + \overline{6}x^3 + x^2 + x$$

*(Justifique.)*

• Consideremos, agora, dois polinómios quaisquer relativos a um anel comutativo A:

$$a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$$

$$b_0x^m + b_1x^{m-1} + \ldots + b_{m-1}x + b_m$$

Estes podem escrever-se abreviadamente:

$$\sum_{k=0}^{n} a_k x^{n-k} \quad \text{e} \quad \sum_{k=0}^{m} b_k x^{m-k}$$

*Sem diminuir a generalidade, podemos supor* $m = n$. Com efeito, se fosse por exemplo $m < n$, bastaria introduzir no segundo polinómio

o termo (0 $x^n$ e, eventualmente, outros termos nulos, para ficar com *grau aparente* igual ao do primeiro. Então, supondo já m = n, é natural chamar *soma dos polinómios dados* ao polinómio

$$(a_o + b_o)x^n + (a_1 + b_1)x^{n-1} + \ldots + (a_n + b_n)$$

ou seja, abreviadamente,

$$\sum_{k=0}^{n} (a_k + b_k)x^{n-k},$$

*visto que este polinómio é uma expressão formalmente equivalente à que se obtém ligando os dois primeiros com o sinal +.*

Analogamente se define 'diferença' entre dois polinómios.

b) *Multiplicação dos polinómios.* Consideremos os dois seguintes polinómios relativos ao Anel dos 'Nove Fora':

$$\overline{4}x^3 + \overline{7}x^2 + \overline{5}x + \overline{2} \quad , \quad \overline{3}x^2 + \overline{6}x + \overline{4}$$

É fácil ver que se tem, para todo o $x \in A_9$ (*justifique*)(1):

$$(\overline{4}x^3 + \overline{7}x^2 + \overline{5}x + \overline{2}) \cdot (\overline{3}x^2 + \overline{6}x + \overline{4}) = (\overline{4}x^3 + \overline{7}x^2 + \overline{5}x + \overline{2}) \cdot \overline{3}x^2 +$$
$$+ (\overline{4}x^3 + \overline{7}x^2 + \overline{5}x + \overline{2}) \cdot \overline{6}x + (\overline{4}x^3 + \overline{7}x^2 + \overline{5}x + \overline{2}) \cdot \overline{4} =$$
$$= (\overline{3}x^5 + \overline{3}x^4 + \overline{6}x^3 + \overline{6}x^2) + (\overline{6}x^4 + \overline{6}x^3 + \overline{3}x^2 + \overline{3}x) +$$
$$+ (\overline{7}x^3 + x^2 + \overline{2}x + \overline{8}) = \overline{3}x^5 + x^3 + x^2 + \overline{5}x + \overline{8}$$

Assim, é natural dizer que o último polinómio é o *produto dos*

(1) Um anel ainda mais cómodo para exemplificação é, evidentemente, o anel $A_{10}$.

*dois polinómios dados*. Para o cálculo deste produto pode usar-se o esquema habitual:

$$\begin{array}{r}
\overline{4}x^3 + \overline{7}x^2 + \overline{5}x + \overline{2} \\
\overline{3}x^2 + \overline{6}x + \overline{4} \\
\hline
\overline{7}x^3 + \ x^2 + \overline{2}x + \overline{8} \\
\overline{6}x^4 + \overline{6}x^3 + \overline{3}x^2 + \overline{3}x \\
\overline{3}x^5 + \overline{3}x^4 + \overline{6}x^3 + \overline{6}x^2 \\
\hline
\overline{3}x^5 + \overline{0}x^4 + \ x^3 + \ x^2 + \overline{5}x + \overline{8}
\end{array}$$

Consideremos agora, em geral, dois polinómios em x

$$(2) \qquad \sum_{j=0}^{n} a_j x^{n-j} , \qquad \sum_{k=0}^{m} b_k x^{m-k}$$

relativos a um anel comutativo A. É claro que se tem

$$a_j x^{n-j} \cdot b_k x^{m-k} = (a_j b_k)\, x^{m+n-(j+k)} , \quad \forall\, x \in A,$$

para $j = 0, \ldots, n$; $k = 0, \ldots, m$. (*Porquê?*) Ora, para que este produto seja de grau $m+n-p$ deve ser $j + k = p$. Portanto, a soma de todos os termos de grau $m + n - p$, assim obtidos, será:

$$(a_0 b_p + a_1 b_{p-1} + \ldots + a_j b_{p-j} + \ldots + a_p b_0)\, x^{m+n-p}$$

Deste modo, é natural chamar *produto dos polinómios* (2) ao polinómio

$$\sum_{p=0}^{m+n} (a_0 b_p + a_1 b_{p-1} + \ldots + a_p b_0) x^{m+n-p}$$

*visto que esta é uma expressão formalmente equivalente à que se obtém ligando os dois primeiros (escritos entre parênteses) pelo sinal de multiplicação.*

4. **Anéis de polinómios.** Seja A um anel *comutativo*. Diz-se que dois polinómios relativos a A são *idênticos* (ou que são o *mesmo* polinómio), sse têm iguais os coeficientes dos termos do mesmo grau. Por exemplo, no anel $A_9$, os polinómios

$$\overline{4}x^3 - x^2 + \overline{5} \quad , \quad \overline{13}x^3 + \overline{8}x^2 + \overline{9}x - \overline{4}$$

são idênticos, visto que $\overline{4} = \overline{13}$, $-\overline{1} = \overline{8}$, $\overline{0} = \overline{9}$, $\overline{5} = -\overline{4}$.

Para indicar que dois polinómios são idênticos, escreve-se entre ambos o sinal =, desde que não haja perigo de confusão (ver NOTA no fim deste número).

Designa-se por A[x] o conjunto de todos os polinómios em x relativos ao anel A. Segundo as definições anteriores, a cada par de polinómios pertencentes a A[x] fica a corresponder:

1) um determinado polinómio pertencente a A[x], chamado *soma* dos dois primeiros;

2) um determinado polinómio pertencente a A[x] chamado *produto* dos dois primeiros.

Assim, o conjunto A[x] passa a ser um *grupóide*, relativamente e a cada uma das operações definidas. Mais ainda:

É fácil ver que as propriedades características das operações do anel A se transmitem às operações introduzidas em A[x]: *assim, a adição de polinómios pertencentes a* A[x] *é associativa, comutativa e reversível, enquanto a multiplicação dos mesmos é associativa, comutativa e distributiva relativamente à adição.*

Podemos, pois, concluir:

> *O conjunto* A[x] *é um anel comutativo relativamente à adição e à multiplicação definidas.*

Note-se que, no anel A[x], o elemento nulo é o polinómio que se reduz à constante (0: chamar-lhe-emos, por isso mesmo, *polinómio nulo* ou *polinómio zero*.

EXERCÍCIO. Qual é o elemento unidade no anel $Z[x]$? O anel $Z_2[x]$ tem elemento unidade? A que condição deve satisfazer um anel A para que o anel A[x] tenha elemento unidade?

Até aqui temo-nos referido exclusivamente a polinómios em *x*, mas é óbvio que a variável pode ser qualquer outra, por exemplo u. O símbolo A[u] representará então o *anel dos polinómios* em u relativos a A. É evidente que os anéis A[x] e A[u] são distintos. Mas também é óbvio que se fizermos corresponder, a cada polinómio pertencente a A[x], o polinómio que se obtém substituindo no primeiro x por u, fica assim definida uma aplicação biunívoca de A[x] sobre A[u], *que é um isomorfismo entre os dois anéis*. Por conseguinte:

*Os anéis* A[x] *e* A[u] *são isomorfos.*

É ainda fácil ver que todas as considerações se estendem ao caso de polinómios com mais de uma variável.

NOTA. Segundo o anterior conceito de identidade entre polinómios, um polinómio não será propriamente uma expressão, mas antes uma certa classe de expressões equivalentes entre si. Por isso, se quisermos ser inteiramente rigorosos, devemos designar um polinómio, não por uma das expressões que o representam (1), mas sim por um outro símbolo: — por exemplo, pôr essa expressão escrita entre colchetes. Assim, poderíamos escrever, relativamente a $A_9$:

$$[\overline{4}x^3 - x^2 + \overline{5}] = [\overline{13}x^3 + \overline{8}x^2 + \overline{9}x - \overline{4}]$$

em vez de

$$\overline{4}x^3 - x^2 + \overline{5} = \overline{13}x^3 + \overline{8}x^2 + \overline{9}x - \overline{4}$$

Isto já evitaria equívocos, pois a última fórmula não é, na realidade, uma proposição mas, apenas, uma expressão proposicional. É só por

(1) Mesmo neste caso, a expressão deveria ser escrita entre aspas, segundo a convenção estabelecida (pág. 13, 1.º tomo).

*abuso cómodo de escrita* que se usa esta última fórmula como indicando identidade entre dois polinómios.

Entretanto é óbvio que

$$\overline{4}x^3 - x^2 + \overline{5} \equiv \overline{13}x^3 + \overline{8}x^2 + \overline{9}x - \overline{4}$$

*Dois polinómios idênticos são sempre representados por duas expressões equivalentes.*

Prova-se que a recíproca desta proposição também é verdadeira em $\mathbb{R}$: *dois polinómios equivalentes (em* $\mathbb{R}$*) são necessariamente idênticos.*

Mas não é verdadeira num anel finito. Por exemplo, em $A_5$ tem-se:

$$x^5 + x - \overline{1} \equiv \overline{2}x - \overline{1}$$

e, contudo, os dois polinómios $x^5 + x - \overline{1}$, $2x - 1$ não são idênticos.

Pelas razões expostas, muitos autores consideram as letras x, u, etc. num polinómio, não propriamente como *variáveis,* mas como *indeterminadas,* isto é, como símbolos designativos de entes que podem ser escolhidos arbitrariamente (tais como, por exemplo, os símbolos $\overline{1}$, $\overline{2}$, ..., $\overline{11}$ do anel $A_{12}$, que podemos interpretar de vários modos).

5. **Divisão por polinómios do tipo $x - \alpha$; raízes dum polinómio.** Consideremos um polinómio qualquer (relativo a um anel comutativo A):

$$(1) \qquad a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$$

que vamos designar abreviadamente por P(x). Consideremos, por outro lado, um polinómio, aliás binómio, do tipo $x-\alpha$ (com $\alpha \in A$); por exemplo, $x - 3$ e $x + 5$ são polinómios deste tipo (em $Z$), tendo-se

no primeiro caso $\alpha = 3$ e no segundo $\alpha = -5$ (1). Posto isto, procuremos determinar um polinómio

$$q_0 x^{n-1} + q_1 x^{n-2} + \ldots + q_{n-2} x + q_{n-1},$$

que designaremos abreviadamente por Q(x), tal que

(2) $\qquad P(x) = (x - \alpha) \cdot Q(x) + R$, sendo R uma constante.

*Suponhamos que um tal polinómio* Q(x) *existe*. Calculemos então o binómio produto de $x - \alpha$ por Q(x):

$$q_0 x^{n-1} + q_1 x^{n-2} + q_2 x^{n-3} + \ldots + q_{n-2} x + q_{n-1}$$

$$\begin{array}{l|l} & x - \alpha \\ \hline q_0 x^n + q_1 x^{n-1} & + \quad q_2 x^{n-2} + \ldots + q_{n-1} x \\ \quad - \alpha q_0 x^{n-1} & - \alpha q_1 x^{n-2} \quad + \ldots - \alpha q_{n-2} x \quad - \alpha q_{n-1} \\ \hline q_0 x^n + (q_1 - \alpha q_0) x^{n-1} & + (q_2 - \alpha q_1) x^{n-2} + \ldots + (q_{n-1} - \alpha q_{n-2}) x - \alpha q_{n-1} \end{array}$$

Ora, segundo (2), este polinómio produto somado com R deve dar o polinómio P(x), indicado em (1); isto é, deve ter-se (2):

$$q_0 = a_0 \ , \ q_1 - \alpha q_0 = a_1 \ , \ q_2 - \alpha q_1 = a_2, \ldots$$

$$q_{n-1} - \alpha q_{n-2} = a_{n-1} \ , \ R - \alpha q_{n-1} = a_n$$

Donde:

(3) $\qquad q_0 = a_0, \ q_1 = a_1 + \alpha q_0, \ q_2 = a_2 + \alpha q_1, \ldots,$

$$q_{n-1} = a_{n-1} + \alpha q_{n-2}, \quad R = a_n + \alpha q_{n-1}$$

---

(1) Adoptamos a forma $x - \alpha$ para tornar mais simples o enunciado da regra que vamos deduzir (REGRA DE RUFFINI).

(2) Segundo o conceito de identidade de polinómios, dado no número anterior.

Portanto, se Q(x) existe, os seus coeficientes são *necessariamente* dados pelas fórmulas (3). Reciprocamente, os cálculos efectuados mostram que, se determinarmos $q_0$, $q_1$, ..., $q_{n-1}$ e R, por meio destas fórmulas, a condição (2) é verificada. Por conseguinte:

*O problema proposto tem uma e uma só solução, que é dada pelas fórmulas* (3).

Diremos então que Q(x) e R são, respectivamente, o *quociente* e o *resto* da divisão de P(x) por $x - \alpha$ (mais tarde trataremos da divisão de polinómios em geral).

O cálculo dos coeficientes $q_k$ por meio das fórmulas (3) pode efectuar-se conforme o seguinte esquema prático, chamado REGRA DE RUFFINI:

| | $a_0$ | $a_1$ | $a_2$ | ... | $a_{n-1}$ | $a_n$ |
|---|---|---|---|---|---|---|
| $\alpha$ | | $\alpha q_0$ | $\alpha q_1$ | ... | $\alpha q_{n-2}$ | $\alpha q_{n-1}$ |
| | $a_0$ | $a_1 + \alpha q_0$ | $a_2 + \alpha q_1$ | ... | $a_{n-1} + \alpha q_{n-2}$ | $a_n + \alpha q_{n-1}$ |
| | $= q_0$ | $= q_1$ | $= q_2$ | ... | $= q_{n-1}$ | $= R$ |

Por exemplo, tratando-se de dividir

$$\overline{2}x^5 + \overline{8}x^4 + \overline{5}x^2 + \overline{7}x + \overline{2} \quad \text{por} \quad x + \overline{6},$$

relativamente ao anel $A_9$, será $\alpha = -\overline{6} = \overline{3}$ e tem-se o quadro:

| | $\overline{2}$ | $\overline{8}$ | $\overline{0}$ | $\overline{5}$ | $\overline{7}$ | $\overline{2}$ |
|---|---|---|---|---|---|---|
| $\overline{3}$ | | $\overline{6}$ | $\overline{6}$ | $\overline{0}$ | $\overline{6}$ | $\overline{3}$ |
| | $\overline{2}$ | $\overline{5}$ | $\overline{6}$ | $\overline{5}$ | $\overline{4}$ | $\overline{5}$ |

O quociente é, pois, $\overline{2}x^4 + \overline{5}x^3 + \overline{6}x^2 + \overline{5}x + \overline{4}$ e o resto é $\overline{5}$. (Para outros exemplos e complementos, ver *Compêndio de Álgebra, 6.º ano,* págs. 282-285) (1).

(1) Ver nota da pag. 48.

Vamos, agora, deduzir uma consequência importante do resultado obtido.

Já sabemos que, uma vez determinados Q(x) e R pelo processo indicado, os dois membros da fórmula (2) são formalmente equivalentes, isto é, *tomam o mesmo valor, qualquer que seja o valor atribuído a* x. Em particular, se dermos a x o valor $\alpha$, virá:

$$P(\alpha) = (\alpha - \alpha) \cdot Q(\alpha) + R = (0 \cdot Q(\alpha) + R = (0 + R = R$$

Em conclusão:

TEOREMA. *O resto da divisão dum polinómio* (x) *por* $x - \alpha$ *é igual a* $P(\alpha)$, *isto é, ao valor que* P(x) *toma substituindo* x *por* $\alpha$.

DEFINIÇÃO. *Chama-se raiz ou zero dum polinómio* P(x) *todo o valor* a *de* x *que anule o polinómio, isto é, tal que* P(a) = (0. *Nesta hipótese, também se diz que* a *é raiz ou solução da equação* P(x) = (0.

Por outro lado, diz-se que o polinómio P(x) é *divisível* por $x - \alpha$, sse o resto da divisão de P(x) por $x - \alpha$ é zero. Destas definições e do teorema anterior deduz-se imediatamente o seguinte

COROLÁRIO: *Para que um polinómio* P(x) *seja divisível por* $x - \alpha$ *é necessário e suficiente que* $\alpha$ *seja uma raiz desse polinómio.*

Por exemplo, o resto da divisão de $x^3 - 5x - 2$ por $x - 2$ é $2^3 - 5 \cdot 2 - 2 = 8 - 10 - 2 = -4$. O resto da divisão do mesmo polinómio por $x + 2$ será: $(-2)^3 - 5 \cdot (-2) - 2 = 0$. Logo $x^3 - 5x - 2$ é divisível por $x + 2$. Apliquemos a regra de RUFFINI:

| | | | | |
|---|---|---|---|---|
| | 1 | 0 | −5 | −2 |
| −2 | | −2 | 4 | 2 |
| | 1 | −2 | −1 | 0 |

Será, pois:

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

**6. Elementos regulares e divisores de zero num anel.** Já sabemos que num anel todo o elemento tem simétrico. (*Porquê?*) Mas já não podemos dizer que todo o elemento do anel tem inverso: o anel pode mesmo não ter elemento unidade. *Seja então* A *um anel qualquer com elemento unidade; nestas condições:*

DEFINIÇÃO 1. *Diz-se que um elemento* a *de* A *é regular sse* a *tem inverso em* A. *Caso contrário, diz-se que* a *é singular (em* A*).*

Dos corolários 1 e 2 do n.º 1 deduz-se que:

| *O zero é elemento singular de* A |
|---|

Com efeito, não existe nenhum elemento x de A tal que $(0 \cdot x = \mathbb{1}$, visto que $(0 \cdot x = (0, \forall x \in A$, e $(0 \neq \mathbb{1}$.

*Daqui por diante vamos, em geral, designar o zero dum anel pelo símbolo* 0, *simplesmente.* Já vimos que se tem

$$0 \cdot a = a \cdot 0 = 0, \quad \forall a \in A.$$

Esta propriedade pode enunciar-se do seguinte modo:

*Se um, pelo menos, dos factores dum produto num anel é nulo, o produto também é nulo.*

A propriedade recíproca seria a seguinte:

*Se um produto é nulo, um dos factores, pelo menos, é nulo.*

Será sempre assim em qualquer anel?

Esta propriedade, como se sabe, é verdadeira nos anéis *Z*, (Q, R. Por isso podemos escrever, quando se trata de um destes anéis:

$$a \cdot b = 0 \Leftrightarrow a = 0 \vee b = 0$$

*Mas existem anéis em que isto não se verifica:* por exemplo, no anel $A_{12}$ tem-se: $\overline{6} \cdot \overline{4} = \overline{24} = \overline{0}$, sem que seja $\overline{6} = \overline{0}$ ou $\overline{4} = \overline{0}$.

DEFINIÇÃO 2. *Diz-se que um elemento* a *dum anel* A *é divisor de zero, sse verifica as duas seguintes condições:*

*1)* $a \neq 0$;

*2) existe pelo menos um elemento* b *de* A *diferente de* 0 *tal que* $a \cdot b = 0 \vee b \cdot a = 0$.

Assim, os elementos $\overline{4}$ e $\overline{6}$ de $A_{12}$ são divisores de zero. (Determine os divisores de zero em $A_{12}$ e em outros anéis considerados nos exemplos do n.º 1).

TEOREMA 1. *Se* a *é elemento regular dum anel* A, *então* a *não é divisor de zero.*

Vamos fazer uma demonstração por redução ao absurdo. Suponhamos que *a* é ao mesmo tempo regular e divisor de zero em A. Quer isto dizer, por um lado, que *a* tem inverso em A e, por outro lado, que existe um elemento b de A *diferente de zero* tal que $ab = 0 \vee ba = 0$. Suponhamos, por exemplo, $ab = 0$; então:

$$a^{-1} \cdot (ab) = a^{-1} \cdot 0 \qquad \text{ou seja} \qquad (a^{-1}a)b = 0,$$

donde $1 \cdot b = 0$, isto é, $b = 0$, *o que é contra a hipótese. Analogamente* concluiremos se $ba = 0$.

Logo, se *a* é regular, não pode ser divisor de zero.

Segundo a *propriedade lógica da conversão* (pág. 45, 1.º tomo) o teorema I também pode enunciar-se do seguinte modo:

| *Se* a *é divisor de zero, então* a *é singular em* A |
|---|

Note-se que nos anéis $A_4$, $A_9$, etc. os únicos elementos singulares são precisamente o zero e os divisores de zero. Mas já, por exemplo, no anel *Z*, não existem divisores de zero e todos os elementos são singulares excepto 1 e −1.

TEOREMA 2. *Se* a, b, c *são elementos dum anel* A *e* c *não é zero nem divisor de zero, então:*

$$ac = bc \Rightarrow a = b \qquad e \qquad ca = cb \Rightarrow a = b$$

Com efeito, suponhamos verificada a hipótese e seja $ac = bc$. Então $ac - bc = 0$ e, portanto

$$(a - b)\, c = 0 \quad (\textit{Porquê?})$$

Ora, como *c* não é zero nem divisor de zero, tem de ser $a - b = 0$ (*porquê?*) e, portanto, $a = b$.

Analogamente, se prova que $ca = cb \Rightarrow a = b$.

7. **Conceito de corpo.** Vimos atrás que o zero dum anel é sempre elemento singular. Há muitos exemplos de anéis em que o único elemento singular é o zero. Quando isto acontece será sempre possível dividir um elemento *a* do anel, à direita ou à esquerda, por um elemento *b* do anel diferente de zero (pg. 42). Por isso, tais anéis são chamados *anéis de divisão*. Ora:

DEFINIÇÃO. *Chama-se corpo todo o anel comutativo com elemento unidade, em que todo o elemento diferente de zero é regular.*

Assim 'corpo' significa o mesmo que 'anel de divisão comutativo'. *Portanto, se* A *é um corpo, existe sempre em* A *o quociente.*

$$\frac{a}{b}, \textit{ com } a, b \in A, \textit{ desde que } b \neq 0\,(^1).$$

Por exemplo, o anel *Z* não é um corpo. (*Porquê?*) Mas já os anéis

(1) Quer isto dizer que os elementos dum corpo diferentes de zero formam um grupo multiplicativo.

(Q e IR são corpos comutativos, chamados respectivamente o *corpo racional* e o *corpo real.*

• Do teorema I e da definição 2, do número anterior, bem como da definição de corpo, deduz-se imediatamente o seguinte

COROLÁRIO 1: *Num corpo não existem divisores de zero* (1).

Segundo uma observação atrás feita, deduz-se deste corolário, por sua vez, o seguinte

COROLÁRIO 2: *Se* A *é um corpo, então:*

$$ab = 0 \Leftrightarrow a = 0 \vee b = 0 \quad (\forall\, a,\ b \in A)$$

Segundo a propriedade da conversão (pág. 45, I tomo) esta propriedade ainda pode apresentar-se sob a forma:

$$a \neq 0 \wedge b \neq 0 \Leftrightarrow ab \neq 0 \quad (\forall\, a,\ b \in A)$$

isto é: *num corpo, o produto de dois elementos diferentes de zero é sempre diferente de zero.*

• Por sua vez, do teorema 2 do número anterior deduz-se este

COROLÁRIO 3: *Se* a, b, c *pertencem a um corpo e se* $c \neq 0$:

$$ac = bc \Rightarrow a = b$$

Como além disso $a = b \Rightarrow ac = bc$ (pelo 1.º *princípio lógico de equivalência,* pg. 61, 1.º tomo), temos na mesma hipótese:

(1) $$ac = bc \Leftrightarrow a = b \quad (\text{se } c \neq 0)$$

---

(1) Chama-se 'domínio de integridade' todo o anel comutativo sem divisores de zero. Assim, todo o corpo é um domínio de integridade. Mas Z é um domínio de integridade sem ser um corpo.

## OUTROS EXEMPLOS E EXERCÍCIOS:

I. Consideremos o anel $A_5$. A adição e a multiplicação neste anel são dadas pelas seguintes tabelas:

$x + y$

| x \ y | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ |
|---|---|---|---|---|---|
| $\overline{0}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ |
| $\overline{1}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ | $\overline{0}$ |
| $\overline{2}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ | $\overline{0}$ | $\overline{1}$ |
| $\overline{3}$ | $\overline{3}$ | $\overline{4}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ |
| $\overline{4}$ | $\overline{4}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ |

$x \cdot y$

| x \ y | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ |
|---|---|---|---|---|---|
| $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ |
| $\overline{1}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ |
| $\overline{2}$ | $\overline{0}$ | $\overline{2}$ | $\overline{4}$ | $\overline{1}$ | $\overline{3}$ |
| $\overline{3}$ | $\overline{0}$ | $\overline{3}$ | $\overline{1}$ | $\overline{4}$ | $\overline{2}$ |
| $\overline{4}$ | $\overline{0}$ | $\overline{4}$ | $\overline{3}$ | $\overline{2}$ | $\overline{1}$ |

Note-se que neste anel (comutativo) todos os elementos não nulos têm inverso. Assim, $\overline{1}^{-1} = \overline{1}$, $\overline{2}^{-1} = \overline{3}$, $\overline{3}^{-1} = \overline{2}$, $\overline{4}^{-1} = \overline{4}$. *Logo, o anel* $A_5$ *é um corpo.*

II. Consideremos, agora, o anel $A_2$. Neste caso, temos as tabelas:

$x + y$

| x \ y | $\overline{0}$ | $\overline{1}$ |
|---|---|---|
| $\overline{0}$ | $\overline{0}$ | $\overline{1}$ |
| $\overline{1}$ | $\overline{1}$ | $\overline{0}$ |

$x \cdot y$

| x \ y | $\overline{0}$ | $\overline{1}$ |
|---|---|---|
| $\overline{0}$ | $\overline{0}$ | $\overline{0}$ |
| $\overline{1}$ | $\overline{0}$ | 1 |

e vê-se, imediatamente, que $A_2$ é um corpo. Note-se que este corpo *é isomorfo* a $(L, \dot{\vee}, \wedge)$. Com efeito, a aplicação $\begin{pmatrix} \overline{0} & \overline{1} \\ F & V \end{pmatrix}$ transforma + em $\dot{\vee}$ e $\cdot$ em $\wedge$ (ver n.º 2, NOTA I, e págs. 23-25, 1.º tomo).

III. Já vimos que os anéis $A_4$, $A_9$ e $A_{12}$ têm divisores de zero e, portanto, não são corpos. *Note que* 4, 9, 12 *não são primos.* Prove que é sempre assim, isto é: *se* $\mu$ *não é primo,* $A_\mu$ *não é um corpo* (por ter divisores de zero). Veremos mais tarde que a recíproca também é verdadeira e que portanto:

$A_\mu$ *é um corpo, sse* $\mu$ *é primo.*

IV. Prove que o conjunto dos números da forma $a + b\sqrt{2}$, com $a, b \in \mathbb{Q}$, é um corpo, relativamente às operações usuais.

NOTA. O conceito de corpo foi introduzido por Galois na sua teoria da resolubilidade algébrica. Em particular, os corpos finitos (isto é, com um número finito de elementos) são chamados CAMPOS DE GALOIS e intervêm na construção de *quadros latinos* (ver pág. 57). Assim, todo o corpo $A_p$, com p primo, é um campo de Galois; mas há outros campos de Galois não isomorfos a estes.

8. **Generalidades sobre equações relativas a corpos.** Nas considerações que vão seguir-se, supõe-se que K *é um corpo.*

Ligando pelo sinal = duas expressões designatórias com uma ou mais variáveis, relativas ao universo K, obtém-se uma expressão proposicional, que é uma *equação relativa a* K. As variáveis dizem-se agora *incógnitas;* chamam-se *soluções* (ou *raízes*) da equação os valores da incógnita (ou as sequências de valores das incógnitas) que verificam a equação. Esta diz-se *possível* (ou *resolúvel*) sse tem, pelo menos, uma solução. Duas equações são *equivalentes*, sse têm o mesmo conjunto de soluções. Dos princípios lógicos de equivalência (pág. 61, 1.º tomo) e das propriedades das operações em K, deduzem-se os habituais *princípios de equivalência,* para equações relativas a K:

PRINCÍPIO I. *Substituindo um dos membros duma equação por uma expressão equivalente, obtém-se uma equação equivalente à primeira.*

PRINCÍPIO II. *Quando um dos membros duma equação tem a forma de uma soma de duas ou mais expressões, obtém-se uma equação equivalente à primeira, passando para o outro membro uma dessas expressões multiplicada por* $-1$.

PRINCÍPIO III. *Multiplicando ambos os membros duma equação por um elemento de* K *diferente de zero obtém-se uma equação equivalente à primeira.*

O princípio I é um caso particular do 1.º princípio lógico de equivalência. O princípio II é uma consequência do 2.º princípio lógico de equivalência, atendendo a que se tem, *por definição de diferença* a−b *de dois elementos:*

$$\left.\begin{array}{l} a = b + c \Leftrightarrow a - b = c \\ a + b = c \Leftrightarrow a = c - b \end{array}\right\} \forall\, a, b, c, \in K$$

O princípio III resulta do 2.º princípio lógico de equivalência e da seguinte propriedade demonstrada no número anterior:

*Sendo* c *um elemento de* K *diferente de* 0, *então:*

$$a = b \Leftrightarrow ac = bc \quad , \quad \forall\, a, b \in K$$

No princípio III baseia-se a conhecida técnica chamada *'desembaraçar de denominadores'*. Do mesmo princípio se deduz o seguinte

COROLÁRIO: *Quando um dos membros duma equação é um produto em que um dos factores é uma constante diferente de zero, obtém-se uma equação equivalente à primeira, passando esse factor para o outro membro como divisor.*

A resolução de equações no corpo K assenta nestes princípios de equivalência e ainda no seguinte

PRINCÍPIO DE DECOMPOSIÇÃO: *Quando o primeiro membro duma equação tem a forma de um produto de duas ou mais expressões, e o segundo membro é zero, as raízes da equação são as raízes das equações em que se decompõe a primeira, igualando a zero cada um dos factores do 1.º membro (e só essas raízes).*

Este princípio resulta do 2.º princípio lógico de equivalência aplicado à propriedade expressa pelo corolário 2 do n.º 8:

$$ab = 0 \Leftrightarrow a = 0 \vee b = 0,$$

e que pode estender-se a produtos de mais de dois factores.

Por exemplo, no corpo IR, tem-se:

$$x\,(x-2)\,(x+3) = 0 \Leftrightarrow x = 0 \vee x - 2 = 0 \vee x + 3 = 0,$$

o que mostra que as soluções da primeira equação são 0,2 e −3.

Analogamente, em IR, tem-se:

$$x^2 - y^2 = 0 \Leftrightarrow x + y = 0 \vee x - y = 0$$

o que reduz a resolução de $x^2 - y^2 = 0$ às de $x+y=0$ e de $x-y=0$.

(Para outros exemplos e exercícios em IR, pode-se ver *Compêndio de Álgebra, 7.º ano,* Cap. XIII) (1).

DEFINIÇÃO. *Chama-se equação algébrica de grau* n *toda a equação que, pelos princípios de equivalência, se possa reduzir à forma dum polinómio de grau n igualado a zero:*

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

Em particular para n = 0, 1, 2, 3, 4, ..., têm-se equações das formas:

$$a_0 = 0 \quad , \quad a_0 x + a_1 = 0 \quad , \quad a_0 x^2 + a_1 x + a_2 = 0$$

$$a_0 x^3 + a_1 x^2 + a_2 x + a_3 = 0 \quad , \quad a_0 x^4 + a_1 x^3 + a_2 x^2 + a_3 x + a_4 = 0$$

---

(1) Ver nota da pág. 48.

que são, respectivamente, de grau 0, do 1.º grau, do 2.º grau (ou *quadráticas*), do 3.º grau (ou *cúbicas*), do 4.º grau (ou *quárticas*), etc.

O corolário do n.º 6, bem como a REGRA DE RUFFINI, permitem baixar o grau de uma equação algébrica (relativa a um corpo), sempre que se conheça uma raiz dessa equação. Por exemplo, vimos no n.º 5 que $-2$ é raiz do polinómio $x^3 - 5x - 2$ (em IR) e que

$$x^3-5x-2 \equiv (x+2)\ (x^2-2x-1)$$

Portanto, segundo o PRINCÍPIO DE DECOMPOSIÇÃO,

$$x^3-5x-2=0 \Leftrightarrow x+2=0 \vee x^2-2x-1=0.$$

Quer dizer: as raízes da equação $x^3 - 5x - 2 = 0$ são $-2$ e as raízes da equação $x^2-2x-1=0$; *resta, pois, apenas resolver esta última, que é de grau inferior ao da primeira.*

NOTAS. O princípio I é válido em qualquer universo. O princípio II é válido em qualquer módulo. O princípio III pode estender-se a qualquer anel A, do seguinte modo: *multiplicando ambos os membros duma equação, à direita ou à esquerda, por um elemento de* A *que não seja zero nem divisor de zero, obtém-se uma equação equivalente.* Finalmente, o princípio de decomposição será válido em qualquer anel sem divisores de zero; mas deixa de o ser num anel com divisores de zero. Por exemplo, no anel A (exemplo I do n.º 1), a equação $(x-\overline{1})\ (x+\overline{3})=0$ além da raiz 1, que verifica as equações $x-\overline{1}=0$ e $x+\overline{3}=0$, tem ainda, como é fácil ver, a raiz $\overline{3}$, que não verifica nenhuma destas duas equações.,

9. **Equações lineares com uma incógnita.** Seja ainda K um corpo. Chama-se *equação linear com uma incógnita* relativa a K toda a equação de grau 1 ou 0, isto é, toda a equação que, pelos princípios de equivalência, seja redutível à forma:

$$ax + b = 0$$

em que *a* e *b* sejam elementos conhecidos de K. É claro que, pelo princípio II, se tem:

$$ax + b = 0 \Leftrightarrow ax = -b$$

Posto isto, três casos se podem dar:

1.º *caso.* $a \neq 0$ (equação do 1.º grau). Então, pelo corolário do princípio III, vem:

$$ax = -b \Leftrightarrow x = -\frac{b}{a}$$

Portanto, neste caso, a equação $ax + b = 0$ é *possível e determinada,* isto é, *tem uma e uma só solução,* que é $-b/a$.

2.º *caso.* $a = 0 \wedge b \neq 0$. Então, como $ax = 0$, $\forall x \in K$, *não existe* nenhum elemento x de K tal que $ax = -b$. Portanto, neste caso a equação $ax + b = 0$ é *impossível.*

3.º *caso.* $a = 0 \wedge b = 0$. Então, a equação $ax + b = 0$ reduz-se a $0 \cdot x + 0 = 0$ e *qualquer elemento* x *de* K *a verifica.* Portanto, neste caso, a equação $ax + b = 0$ *é indeterminada* e reduz-se mesmo a uma *identidade.*

EXERCÍCIOS — I. Resolva em IR as seguintes equações (ver *Compêndio de Álgebra, 7.º ano,* Cap. XIII, n.º 8) (1):

a) $\frac{x+4}{x} = \frac{x+9}{x+3}$ b) $\frac{1}{2} + \frac{4}{5x-5} = \frac{x}{2x-6}$

c) $\frac{x-1}{2} = x - \frac{1}{2}\left(x + \frac{3}{2}\right)$ d) $\frac{1}{2}\left(x - \frac{1}{3}\right) = \frac{1}{3}\left(\frac{5x-1}{2} - x\right)$

(1) Ver nota da pág. 48.

II. Resolva no corpo $A_5$ as equações:

a) $\frac{x-\overline{1}}{\overline{3}} - \frac{x+\overline{2}}{\overline{2}} = 2x$; b) $\overline{2}x - \overline{1} = \overline{2} - \overline{3}x$; c) $\overline{3} - x = \overline{2}(\overline{2}x - \overline{1})$

RESPOSTAS — I. a) x=6; b) x=– 9/7; c) impossível; d) indeterminada. II. a) $x=\overline{4}$; b) impossível; c) indeterminada.

10. **Equações do 2.º grau com uma incógnita.** Continuamos a referir-nos a um corpo K qualquer. Segundo a definição do n.º 8, *equação do 2.º grau* (ou *equação quadrática*) é toda a equação que, pelos princípios de equivalência, se pode reduzir à forma

$$ax^2 + bx + c = 0$$

sendo a, b, c elementos conhecidos de K, com $a \neq 0$. Como se viu, qualquer raiz (ou solução) desta equação será também chamada raiz (ou zero) do polinómio $ax^2 + bx + c$.

TEOREMA. *Se um polinómio do 2.º grau,* $ax^2 + bx + c$, *tem pelo menos uma raiz* $x_1$ *no corpo* K, *esse polinómio pode decompor-se em factores lineares segundo a fórmula:*

(1) $$\boxed{ax^2 + bx + c = a(x - x_1)\ (x - x_2)}$$

*em que* $x_2$ *designa também uma raiz do polinómio (que pode ser diferente de* $x_1$ *ou igual a* $x_1$*). Então, a soma e o produto das raízes* $x_1$, $x_2$ *são dadas pelas fórmulas:*

(2) $$\boxed{x_1 + x_2 = -\frac{b}{a}\ ,\quad x_1 x_2 = \frac{c}{a}}$$

*Demonstração:*

Suponhamos que o polinómio tem, pelo menos, uma raiz, $x_1$; então é divisível por $x-x_1$. Apliquemos a regra de Ruffini:

| | $a$ | $b$ | $c$ |
|---|---|---|---|
| $x_1$ | | $ax_1$ | $ax_1^2 + bx_1$ |
| | $a$ | $ax_1+b$ | $ax_1^2+bx_1+c=0$ |

Teremos, pois:

$$ax^2 + bx + c = (x - x_1)\ [ax + (ax_1 + b)]$$
$$= a(x - x_1)\ [x + a^{-1}\ (ax_1 + b)]$$

Daqui, pondo

$$x_2 = -\frac{ax_1 + b}{a}$$

resulta, finalmente:

(3) $$ax^2 + bx + c = a(x-x_1)\ (x-x_2)$$

e é óbvio que $x_2$ é, também, uma raiz do polinómio.

Ora $(x-x_1)\ (x-x_2) = x^2-(x_1+x_2)\ x + x_1x_2$. Então de (3) vem

$$ax^2 + bx + c = ax^2 - a(x_1+x_2)x + ax_1x_2$$

donde, visto tratar-se de polinómios idênticos (1):

$$-a(x_1 + x_2) = b\ ,\ ax_1\ x_2 = c$$

---

(1) A fórmula (3) indica que o polinómio $ax^2 + bx + c$ é o produto dos polinómios a, $x-x_1$, $x-x_2$ segundo as considerações dos n.os 5 e 6.

ou seja:

$$x_1+x_2 = -\frac{b}{a}, \quad x_1x_2 = \frac{c}{a}$$

COROLÁRIO 1. *Uma equação do 2.º grau não pode ter mais de duas raízes distintas no corpo* K(1).

Com efeito, se uma equação $ax^2 + bx + c = 0$ (com $a \neq 0$) tem, pelo menos, uma raiz $x_1$ em K, essa equação é equivalente, em virtude do teorema, a uma equação da forma

$$a(x-x_1)\ (x-x_2) = 0$$

e, segundo o PRINCÍPIO DE DECOMPOSIÇÃO (pág. 97), esta só pode ter como raízes as das equações $x-x_1 = 0$ e $x-x_2 = 0$, ou sejam $x_1$ e $x_2$ (em particular pode ser $x_1 = x_2$).

EXEMPLOS — I. A equação $2x^2 + 2x - 12 = 0$ tem como raízes 2 e $-3$ em IR, como se pode verificar. Então, será:

$$2x^2 + 2x-12 = 2\,(x-2)\,(x+3)$$

e vê-se que a equação não pode ter nenhuma raiz diferente de 2 e de $-3$.

II. É fácil ver que $4x^2 - 4x + 1 = (2x-1)^2 = 4(x-1/2)^2$. Daqui resulta que o polinómio $4x^2 - 4x - 1$ tem uma única raiz em IR, que é 1/2.

---

(1) O corolário 1 estende-se a qualquer *domínio de integridade* (anel comutativo sem divisores de zero), mas deixa de ser válido num anel comutativo com divisores do zero. Por exemplo, no *Anel das Horas* o polinómio do 2.º grau $x^2-\overline{1}$ tem 4 raízes distintas, $\overline{1}$, $\overline{5}$, $\overline{7}$, $\overline{11}$, e admite duas decomposições distintas com factores lineares:

$$x^2 - \overline{1} = (x-\overline{1})\ (x+\overline{1}) = (x-\overline{5})\ (x-\overline{7}) \qquad (\textit{Porquê?})$$

III. A equação $x^2+4=0$ não tem nenhuma raiz em IR. (*Porquê?*)

*Assim, uma equação quadrática pode ter 2 raízes, 1 raiz única ou nenhuma raiz, num dado corpo* K.

Quando uma equação quadrática tem uma única raiz, também se diz que tem uma *raiz dupla* ou que tem *duas raízes iguais* (embora se trate de uma única raiz).

Quando uma equação quadrática tem duas raízes distintas, também se diz que estas são *raízes simples* (e não *duplas*, como no caso anterior).

Do teorema deduzem-se ainda os dois seguintes corolários:

COROLÁRIO 2. *Se um polinómio do 2.º grau,* $ax^2 + bx + c$, *tem, pelo menos, uma raiz em* K, *a outra raiz será simétrica da primeira, se e só se* $b = 0$.

Com efeito, se o polinómio tem, pelo menos, em K uma raiz $x_1$, então, segundo o teorema admite uma raiz $x_2$ tal que $x_1+x_2 = -b \cdot a^{-1}$. Ora, como $a^{-1} \neq 0$ (*porquê?*), tem-se $b \cdot a^{-1} = 0$, se e só se $b = 0$. (*Porquê?*) Logo, será $x_2 = -x_1$ sse $b = 0$.

COROLÁRIO 3. *Um polinómio do 2.º grau* $ax^2 + bx + c$, *tem uma raiz nula, sse* $c = 0$.

Com efeito, se o polinómio tem uma raiz $x_1 = 0$, então admite uma raiz $x_2$ tal que $x_1x_2 = c \cdot a^{-1} = 0$, donde $c = 0$. Reciprocamente, se $c = 0$, o polinómio reduz-se a $ax^2 + bx \equiv (ax+b)x$, donde se conclui que 0 é uma raiz do polinómio.

• Um polinómio $ax^2 + bx+c$ (com $a \neq 0$), pode mesmo ter *duas* raízes nulas (isto é, *a raiz* 0 *dupla*); isso acontece, sse $b = c = 0$, reduzindo-se então o polinómio ao termo $ax^2$.

• Notemos, por último, que *é sempre possível construir uma equação do 2.º grau com raízes* $x_1$ *e* $x_2$ *dadas arbitrariamente.* Com efeito, segundo o PRINCÍPIO DE DECOMPOSIÇÃO, a equação $(x-x_1)\ (x-x_2) = 0$ tem como raízes, precisamente $x_1$ e $x_2$. Como

$(x-x_1)\ (x-x_2) \equiv x-(x_1+x_2)x+x_1x_2$, a equação, na forma canónica, será:

$$x^2 - Sx + P = 0 \quad , \quad \text{com } S = x_1 + x_2,\ P = x_1x_2$$

(Ver exemplos I e II do *Compêndio de Álgebra, 7.º ano,* págs. 108-109) (1).

11. **Resolução e discussão das equações quadráticas.** Continuemos a supor que K é um corpo. Chama-se equação quadrática binómia toda a equação da forma

$$x^2 - \alpha = 0, \quad \text{com } \alpha \in K$$

Suponhamos que, para um dado $\alpha \in K$, a equação $x^2 - \alpha = 0$ (equivalente a $x^2 = \alpha$) tem pelo menos uma raiz $x_1$ em K. Então $x_1$ será uma *raiz quadrada de* $\alpha$. Além disso, segundo o corolário 2 do número anterior, a outra raiz da equação será $-x_1$. Portanto, se convencionarmos designar por $\sqrt{\alpha}$ *uma* dessas raízes, a outra deverá ser designada por $-\sqrt{\alpha}$.

Consideremos, por exemplo, o corpo $A_5$. A aplicação $x \curvearrowright x^2$ deste corpo em si mesmo será:

$$\begin{pmatrix} \overline{0} & \overline{1} & \overline{2} & \overline{3} & \overline{4} \\ \overline{0} & \overline{1} & \overline{4} & \overline{4} & \overline{1} \end{pmatrix}$$

Desde logo se vê que esta aplicação não é bijectiva.

Assim, a equação $x^2-\alpha = 0$ em $A_5$ terá:

2 raízes $(x_1 = \overline{1},\ x_2 = \overline{4} = -\overline{1})$, se $\alpha = \overline{1}$
2 raízes $(x_1 = \overline{2},\ x_2 = \overline{3} = -\overline{2})$, se $\alpha = \overline{4}$
0 raízes, se $\alpha = \overline{2}$ ou $\alpha = \overline{3}$

(1) Ver nota da pág. 48.

Para resolver uma equação quadrática qualquer em K

(1) $$ax^2 + bx + c = 0 \qquad (a \neq 0),$$

procura-se transformá-la numa equação binómia com uma outra incógnita. Ponhamos $x = y + h$, em que y é a nova incógnita e h um elemento a determinar. Então o 1.º membro de (1) transforma-se em

(2) $$a(y^2+2hy+h^2)+b(y+h)+c \equiv ay^2+(2ah+b)y+ah^2+bh+c$$

Assim, para obter uma equação binómia, deveremos fazer $2ah+b=0$, o que equivale a tomar

(3) $$h = -\frac{b}{2a}, \quad \textit{desde que seja } 2a \neq 0.$$

*Vamos, pois, supor daqui por diante que o corpo* K *verifica a seguinte condição:*

(4) $$a \neq 0 \Rightarrow 2a \neq 0, \quad \forall\, a \in K$$

Esta condição não se verifica em $A_2$, mas verifica-se em (Q, em IR e em muitos outros corpos, como veremos adiante.

Entrando com o valor (3) de h no 2.º membro de (2) obtemos:

$$ay^2 + \frac{b^2}{4a} - \frac{b^2}{2a} + c \equiv ay^2 - \frac{b\ -4ac}{4a}$$

Igualando a zero e multiplicando ambos os membros por $a^{-1}$, obtém-se a equação binómia

(5) $$y^2 - \frac{b^2-4ac}{4a^2} = 0$$

É agora, evidente que

$$\begin{cases} ax^2 + bx + c = 0 \\ x = y - \dfrac{b}{2a} \end{cases} \Leftrightarrow \begin{cases} y^2 = \dfrac{b^2-4ac}{4a^2} \\ y = x + \dfrac{b}{2a} \end{cases}$$

*Assim, a resolução de* (1) *é reduzida à resolução da equação binómia* (5), *chamada 'equação resolvente' da primeira.*

Como $4a^2 = (2a)^2$ é fácil ver que a equação (5) é resolúvel *sse* $b^2 - 4ac$ *tiver raiz quadrada.* Virá portanto, *nesta hipótese,* representando por $\sqrt{b^2-4ac}$ *uma* das raízes quadradas:

$$y^2 = \frac{b^2-4ac}{4a^2} \quad \Leftrightarrow \quad y = \pm \frac{\sqrt{b^2-4ac}}{2a}$$

e portanto, visto que $x = -\frac{b}{2a} + y$:

$$ax^2 + bx + c = 0 \quad \Leftrightarrow \quad x = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$$

Esta última fórmula, que é apenas um modo abreviado de escrever

$$(6) \qquad x = \frac{-b + \sqrt{b^2-4ac}}{2a} \quad \vee \quad x = \frac{-b - \sqrt{b^2-4ac}}{2a},$$

será a *fórmula resolvente da equação do* 2.º *grau,* na hipótese de existir raiz quadrada de $b^2-4ac$. Costuma-se chamar *discriminante da equação* e representar por $\Delta$ o valor desta expressão:

$$\Delta = b^2 - 4ac$$

Assim, se designarmos por $x_1$ e $x_2$, respectivamente, as raízes dadas por (6), será:

$$x_1 - x_2 = \frac{\sqrt{\Delta}}{a} = a^{-1}\sqrt{\Delta}$$

e, portanto:

$$x_1 = x_2 \Leftrightarrow a^{-1}\sqrt{\Delta} = 0 \Leftrightarrow \sqrt{\Delta} = 0 \Leftrightarrow \Delta = 0$$

Isto na hipótese de $\Delta$ ter raiz quadrada. Mas, se $\Delta = 0$, existe uma raiz quadrada de $\Delta$ (única) que é 0; então, e só então,

$$x_1 = x_2 = -\frac{b}{2a}$$

donde, atendendo ao teorema do número 11:

$$ax^2 + bx + c = a(x - x_1)^2$$

o que se exprime dizendo que, neste caso, a equação (1) tem uma raiz *dupla*.

Em conclusão:

TEOREMA. *A equação* (1) *tem uma raiz dupla, igual a* $-\frac{b}{2a}$, *se* $\Delta = 0$. *A equação terá duas raízes simples em* K, *dadas por* (6), *se* $\Delta$ *tem raiz quadrada em* K *e se além disso* $\Delta \neq 0$. *A equação não terá solução em* K, *se* $\Delta$ *não tiver raiz quadrada em* K. [Supõe-se que o corpo K verifica a condição (4)].

Em resumo, há a distinguir os seguintes casos:

$$\exists\, z \in K:\ z^2 = \Delta \Rightarrow \begin{cases} \Delta \neq 0 \Rightarrow \exists^2 \textit{ raízes simples de } (1) \textit{ em } K \\ \Delta = 0 \Rightarrow \exists^1 \textit{ raiz dupla de } (1) \textit{ em } K \end{cases}$$

$$\left(\sim \exists\, z \in K:\ z^2 = \Delta\right) \Rightarrow \left(\sim \exists \textit{ raiz de } (1) \textit{ em } K.\right)$$

EXERCÍCIOS—I. Discutir e resolver as seguintes equações em $A_7$:

$$\bar{2}x^2 + \bar{5}x + \bar{3} = 0, \quad \bar{4}x^2 + \bar{5}x + \bar{2} = 0, \quad x^2 + \bar{3}x + \bar{6} = 0,$$

começando por construir uma tabela dos quadrados e uma tabela dos inversos em $A_7$. Decompor em factores lineares os polinómios dados quando houver solução em $A_7$.

II. Resolva no corpo IR as equações:

a) $3x^2 + 9x + 4 = 0$; b) $t^2 - \sqrt{2} \cdot t + 4/9 = 0$; c) $\frac{z}{2} + \frac{2}{z} = z$;

d) $\frac{k}{k+1} + \frac{k+1}{k+2} = 1$; e) $9\alpha^2 + 6\alpha + 1 = 0$; f) $m^2 + m - 1 = 0$

Decomponha, em factores lineares, os polinómios dados em a), b), c). *Calcule, com aproximação até às milésimas, as raízes de* a), b), d), *utilizando uma tabela de quadrados.*

12. **Característica dum corpo.** As conclusões do número anterior foram, em parte, baseadas na premissa (4). Ora vamos ver que tal condição é equivalente à seguinte, bastante mais simples:

(1) $$2 \cdot \mathbf{1} \neq 0$$

Com efeito, tem-se:

$$2a = (2 \cdot \mathbf{1}) \cdot a, \quad \forall\, a \in K \qquad (\textit{Porquê?})$$

Portanto, se $2 \cdot \mathbf{1} \neq 0$, tem-se:

(2) $$a \neq 0 \Rightarrow 2a \neq 0, \quad \forall\, a \in K \qquad (\textit{Porquê?})$$

Reciprocamente, se esta última condição se verifica, tem-se, em particular, $2 \cdot \mathbf{1} \neq 0$. (*Porquê?*)

*Logo, as condições* (1) *e* (2) *são equivalentes* q.e.d.

DEFINIÇÃO 1. *Diz-se que um corpo K é de característica 0, sse verifica a condição* $n \cdot \mathbf{1} \neq 0$ *para todo o inteiro* $n > 1$.

Imediatamente se reconhece que (Q e IR são de característica 0.

Segundo esta definição, se K não é de característica 0, existe pelo menos um inteiro $n > 1$ tal que $n \cdot \mathbf{1} = 0$. Ora, consegue-se demonstrar: *os inteiros que verificam tal condição são necessariamente múltiplos dum número primo.* Por exemplo, suponhamos que se tem $6 \cdot \mathbf{1} = 0$ em K. Ora

$$6 \cdot \mathbf{1} = (2 \cdot \mathbf{1}) \cdot (3 \cdot \mathbf{1})$$

Logo, sendo este produto nulo, verifica-se a *disjunção exclusiva:*

$$2 \cdot \mathbf{1} = 0 \ \dot{\vee} \ 3 \cdot \mathbf{1} = 0 \qquad \textit{(Porquê?)}$$

Então os inteiros *n* tais que $n > 1 \wedge n \cdot \mathbf{1} = 0$ só poderão ser os múltiplos de *um* dos números primos 2, 3.

DEFINIÇÃO 2. *Sendo p um número primo, diz-se que o corpo K é de característica p, sse* $p \cdot \mathbf{1} = 0$ *em* K.

Em particular, o corpo $A_p$ (pág. 96) é de característica p. Mas existem corpos de característica p não isomorfos a este.

Por conseguinte, a premissa em que se basearam as conclusões do número anterior pode assim enunciar-se:

| *O corpo* K *não é de característica* 2 |
|---|

13. **Equações quadráticas no corpo** IR. Suponhamos agora em particular que o corpo K considerado é IR e continuemos a designar por $\Delta$ o discriminante do polinómio do 2.º grau $ax^2 + bx + c$, isto é: $\Delta = b^2 - 4ac$, com $a, b, c \in \mathrm{IR}$, $a \neq 0$. Já sabemos que, neste caso:

$$\exists z, \ z^2 = \Delta \Leftrightarrow \Delta \geqslant 0$$

Designa-se então por $\sqrt{\Delta}$ precisamente *a raiz quadrada não negativa de* $\Delta$, isto é:

$$\sqrt{\Delta} = \iota_x(x^2 = \Delta \wedge x \geqslant 0)$$

Por exemplo, $\sqrt{9} = 3$ (e não $\sqrt{9} = -3$), $\sqrt{3}$ = raiz quadrada de 3 positiva, etc. Por conseguinte, no corpo IR, teremos os 3 seguintes casos, quanto à equação do 2.º grau:

1.º $\Delta > 0$: *duas raízes simples* $\begin{cases} x_1 = \dfrac{-b+\sqrt{\Delta}}{2a} \\ x_2 = \dfrac{-b-\sqrt{\Delta}}{2a} \end{cases}$

2.º $\Delta = 0$: *uma raiz dupla* $\left(x_1 = x_2 = -\dfrac{b}{2a}\right)$

3.º $\Delta < 0$: *nenhuma raiz* (*em* IR).

• A existência da relação de grandeza designada pelo sinal $<$, no corpo IR, permite-nos ainda levar mais longe a discussão. Ponhamos:

$$S = -\frac{b}{a} \quad , \quad P = \frac{c}{a},$$

atendendo a que $-b/a$ e $c/a$ são, respectivamente, a *soma* e o *produto* das raízes $x_1$, $x_2$ da equação nos dois primeiros casos ($\Delta > 0$, $\Delta = 0$). Posto isto, vamos provar o seguinte:

(1) $$\boxed{P < 0 \Rightarrow \Delta > 0}$$

Com efeito, se $c/a < 0$, os números c, a têm *sinais contrários* e,

portanto, também $ac<0$, donde $b^2-4ac>0$ *(porquê?)* ou seja $\Delta>0$. Por outro lado:

(2) $$P>0 \wedge \Delta>0 \Rightarrow x_1 \text{ e } x_2 \textit{ têm o sinal de } S$$

Com efeito, se $P>0$ e $\Delta>0$, as raízes $x_1$, $x_2$ têm o mesmo sinal, visto que $x_1x_2 = P>0$, e esse sinal terá de ser o de S visto que $x_1 + x_2 = S$.

Assim, em resumo, no corpo $\mathbb{R}$, a discussão da equação quadrática pode ser feita do seguinte modo:

$P<0$: 2 *raízes com sinais contrários*

$P=0$: $x_1 = 0$, $x_2 = -\dfrac{b}{a}$

$P>0$ {
- $\Delta>0$: { $S>0$: 2 *raízes positivas*; $S<0$: 2 *raízes negativas* }
- $\Delta=0$: 1 *raiz dupla,* $x_1 = x_2 = -\dfrac{b}{2a}$
- $\Delta<0$: *nenhuma raiz em* $\mathbb{R}$
}

No primeiro caso ($P<0$) ainda podemos distinguir as hipóteses (1):

$P<0$ {
- $S=0$: 2 *raízes simétricas*
- $S>0$: *predomínio da raiz positiva*
- $S<0$: *predomínio da raiz negativa*
}

Para exemplos, ver *Compêndio de Álgebra, 7.º ano,* Cap. XVI pág. 118(2) (não foram ainda introduzidos os números imaginários: quando $\Delta<0$ diz-se que a equação não tem raízes em $\mathbb{R}$).

---

(1) Só a primeira destas hipóteses tem geralmente interesse prático.

(2) Ver nota da pág. 48.

NOTA. Algumas vezes a equação quadrática apresenta-se naturalmente sob a forma $ax^2 + 2mx + c = 0$. Neste caso, a fórmula resolvente toma o aspecto

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

e o discriminante $\Delta$ pode ser substituído pelo *discriminante simplificado* $\Delta' = m^2 - ac = 4\,\Delta$.

**14. Estudo das funções quadráticas em IR.** Chama-se *função quadrática (em* IR*) toda a função representável por um polinómio do 2.º grau; será, portanto, toda a função da forma*

(1) $\qquad x \curvearrowright ax^2+bx+c$, com $a,b,c \in \mathbb{R}$, $a \neq 0$.

Já sabemos (*Compêndio de Álgebra 6.º ano,* pág. 129) (1) que o gráfico duma função quadrática do tipo particular

$$x \curvearrowright ax^2$$

é uma parábola que tem por *vértice* a origem, por *eixo* de *simetria* o eixo das ordenadas e cuja *concavidade* está voltada para cima ou para baixo, conforme $a > 0$ ou $a < 0$.

Passando ao caso geral, recordemos que se tem:

$$ax^2+bx+c = a(x^2 + \frac{b}{a}x + \frac{c}{a})$$

$$x^2 + \frac{b}{a}x + \frac{c}{a} \equiv (x + \frac{b}{2a})^2 - \frac{b^2}{4a^2} + \frac{c}{a}$$

e, portanto

(2) $\qquad ax^2+bx+c \equiv a\ [(x+ \frac{b}{2a})^2 - \frac{b^2-4ac}{4a^2}]$

(1) Ver nota da pág. 48.

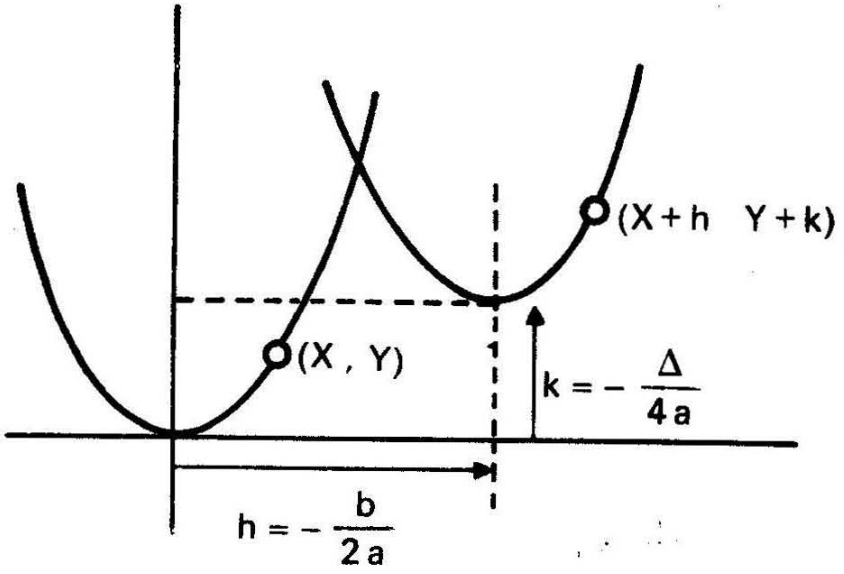
ou seja, pondo $b^2-4ac = \Delta$:

$$ax^2+bx+c \equiv a(x-h)^2 + k, \text{ com } \begin{cases} h = -\dfrac{b}{2a} \\ k = -\dfrac{\Delta}{4a} \end{cases}$$

Notemos agora que, se pusermos $X = x - h$, $Y = y - k$, teremos:

$$y = a(x-h)^2 + k \Leftrightarrow Y = a\,X^2$$

isto é: *se* $(X_0, Y_0)$ *for um par ordenado de números reais que verifica a segunda equação, então* $(X_0+h, Y_0+k)$ *será um par ordenado que verifica a primeira equação, e vice-versa.* Quer isto dizer o seguinte, em geometria analítica: *passa-se do gráfico da segunda equação para o gráfico da primeira por meio de uma translação* (somando *h* à abcissa e *k* à ordenada de cada ponto do 1.º gráfico).




Ora, atendendo ao que sabemos sobre o gráfico da função $x \mapsto ax^2$, segue-se que:

*O gráfico da função quadrática* (1) *é uma parábola de eixo vertical, com a concavidade voltada para cima ou para baixo, conforme* $a > 0$ *ou* $a < 0$.

Mais ainda, do estabelecido no número anterior conclui-se:

*A intersecção do gráfico de* (1) *com o eixo dos* x *tem dois pontos, um só ou nenhum, conforme* $\Delta > 0$, $\Delta = 0$ *ou* $\Delta < 0$.

EXERCÍCIOS: Dados os polinómios (em $\mathbb{R}$):

$$\frac{1}{2}x^2 - 2, -\frac{1}{2}t^2 + 2, \frac{1}{2}u^2 + 1, -\frac{1}{2}u^2 - 1,$$

$$\frac{1}{2}S^2 + S, -\frac{1}{2}m^2 + \frac{3}{2}m - 1, \frac{1}{2}v^2 - 3v + \frac{9}{2}, \frac{1}{2}e^2 - 3e + 5$$

determine, por cálculo, o número de pontos em que o gráfico de cada um deles intersecta o eixo das abcissas. Desenhe, em seguida, os respectivos gráficos.

Quanto ao sinal dos valores da função quadrática (1), vamos demonstrar três teoremas simples:

TEOREMA I. *Se* $\Delta > 0$, *o valor de* $ax^2+bx+c$ *tem sinal contrário ao de* a *ou o mesmo sinal de* a, *conforme o valor atribuído a* x *é interior ou exterior ao intervalo das raízes* (1).

*Demonstração:*

Suponhamos $\Delta > 0$. Então

$$ax^2+bx+c \equiv a(x-x_1)(x-x_2) \tag{3}$$

Como as raizes $x_1$, $x_2$ são diferentes, uma delas é menor que a outra, por exemplo $x_1 < x_2$. Então o intervalo das raízes é $[x_1, x_2]$. Suponhamos que se atribui a x um valor $\alpha$ *interior* a este intervalo, isto é, tal que

$$x_1 < \alpha < x_2$$

(1) Na demonstração se dirá o que significa *'intervalo das raízes'*, bem como *'interior'* e *'exterior'* a este intervalo.

Então $\alpha - x_1 > 0$, $\alpha - x_2 < 0$ e, portanto

$$(\alpha - x_1)\,(\alpha - x_2) < 0$$

Daqui se conclui, atendendo a (1), que o sinal de $ax^2 + bx + c$ é o contrário ao de a.

Suponhamos agora que $\alpha$ é exterior a $[x_1, x_2]$, isto é, que

$$\alpha < x_1 \vee \alpha > x_2$$

Então

$$(\alpha - x_1 < 0 \wedge \alpha - x_2 < 0) \vee (\alpha - x_2 > 0 \wedge \alpha - x_1 > 0)$$

e, portanto

$$(\alpha - x_1)\,(\alpha - x_2) > 0,$$

donde se conclui que $a\alpha^2 + b\alpha + c$ tem o mesmo sinal de a.

(O que acontece se $x = x_1$ ou $x = x_2$?)

TEOREMA II. *Se* $\Delta = 0$, *o valor de* $ax^2 + bx + c$ *tem o sinal de* a *para todo o valor de* x *diferente da raiz.*

*Demonstração:*

Suponhamos $\Delta = 0$. Então, o polinómio tem uma raiz dupla $x_1$ e, portanto

$$ax^2 + bx + c \equiv a(x - x_1)^2$$

Ora, para todo o valor $\alpha$ de x diferente de $x_1$ tem-se $\alpha - x_1 \neq 0$ e portanto $(\alpha - x_1)^2 > 0$, donde se conclui que $a\alpha^2 + b\alpha + c$ tem o sinal de a.

TEOREMA III. *Se* $\Delta < 0$, *o valor de* $ax^2+bx+c$ *tem o sinal de* a *para todo o valor de* x.

*Demonstração:*

Lembremos que, segundo (2),

$$(4) \qquad ax^2+bx+c \equiv a\left[(x+\frac{b}{2a})^2-\frac{\Delta}{4a^2}\right]$$

Suponhamos $\Delta < 0$. Então, como $4a^2 > 0$, tem-se $-\frac{\Delta}{4a^2} > 0$.

Como, além disso, $(x+\frac{b}{2a})^2 \geqslant 0$, $\forall x \in \mathbb{R}$, vem:

$$(x+\frac{b}{2a})^2-\frac{\Delta}{4a^2} > 0, \quad \forall x \in \mathbb{R}$$

Daqui e de (3) se conclui que $ax^2+bx+c$ tem o sinal de a qualquer que seja $x \in \mathbb{R}$.

*Para exemplificação da doutrina exposta, considere, novamente, os polinómios dos exercícios anteriores e determine, por cálculo, os intervalos de* $\mathbb{R}$ *nos quais a função definida em cada caso é positiva e aqueles em que a função é negativa. Confronte, em seguida, os resultados com os respectivos gráficos.*

No primeiro caso ($\Delta > 0$), supondo que $\alpha$ é um número exterior ao intervalo das raízes, pode ainda interessar saber se $\alpha$ é *maior* ou *menor* que as raízes, sem calcular estas. Para isso temos o seguinte COMPLEMENTO AO TEOREMA I:

*Se* $\Delta > 0$ *e* $a\alpha^2+b\alpha+c$ *tem o sinal de a, então* $\alpha$ *é maior que as raízes ou menor que as raízes conforme* $\alpha > S/2$ *ou* $\alpha < S/2$, *considerando* $S = -b/a$.

*Demonstração:*

Suponhamos que a hipótese se verifica e sejam $x_1, x_2$ as raízes com $x_1 < x_2$. Então $\alpha < x_1$ ou $\alpha > x_2$. Mas, se tivermos

$$\alpha > \frac{x_1+x_2}{2} = -\frac{b}{2a},$$

não poderá ser $\alpha < x_1$, porque então seria também $\alpha < x_2$ e, portanto, $2\alpha < x_1 + x_2$, ou seja $\alpha < (x_1 + x_2)/2$. Logo, se $\alpha > S/2$, será $\alpha > x_2$. Analogamente se prova que se $\alpha < S/2$, então $\alpha < x_1$.

EXERCÍCIOS:

I. Determine a posição dos números $-5$, 1, 6, em relação às raízes do polinómio $3x^2 - 5x - 16$.

II. Determine condições em t equivalentes às seguintes:

a) $\forall x: x^2 + 4x + t > 0$
b) $\forall x: (t+1)x^2 - 2tx + 5t + 6 < 0$ *(no universo* $\mathbb{R}$*)*

III. Determine condições em x equivalentes às seguintes:

a) $\exists y: y^2 + 4y + x \leqslant 0$
b) $\exists y: (x-1)y^2 - 2xy + 5x + 6 \geqslant 0$ *(em* $\mathbb{R}$*)*

15. **Sistemas de equações.** Seja novamente K um corpo qualquer. *Um sistema de equações relativas a* K será a conjunção de duas ou mais equações relativas a K (que se exprime usualmente por meio de uma chaveta colocada antes do conjunto das equações escritas em linhas sucessivas). Deste modo, uma *solução* (ou *raiz*) do sistema de equações será toda a sequência de valores das variáveis que verifique *todas* as equações dadas. O sistema será *possível* (ou *resolúvel*), sse tiver pelo menos uma solução; será *impossível* no caso contrário.

Dois sistemas de equações são *equivalentes*, sse tem o mesmo conjunto de soluções. Além dos princípios de equivalência que já indicámos para equações em geral (n.º 9), apresentam-se-nos agora dois novos princípios de equivalência, aplicáveis a sistemas de equações.

PRINCÍPIO DE SUBSTITUIÇÃO. *Quando, num sistema de equações, uma destas se apresente resolvida em relação a uma das incógnitas, o sistema é equivalente ao que resulta do primeiro, substituindo na outra equação (ou outras equações) essa incógnita pela sua expressão como função da outra incógnita (ou das outras incógnitas).*

Bastará fazer a demonstração no caso de um sistema de duas equações com duas incógnitas, porque a ideia é a mesma no caso geral. Consideremos um sistema de equações da forma

$$(1) \qquad \begin{cases} f(x, y) = 0 \\ y = \varphi(x) \end{cases}$$

que também se pode escrever:

$$f(x, y) = 0 \wedge y = \varphi(x)$$

Como se vê, a segunda equação supõe-se resolvida em relação a y, isto é, o 1.º membro reduz-se a y e o 2.º membro reduz-se a uma expressão *só* com a variável x. Posto isto, seja $(\alpha,\beta)$ uma solução do sistema, isto é, um par ordenado de elementos de K, tal que as proposições

$$f(\alpha, \beta) = 0 \quad e \quad \beta = \varphi(\alpha)$$

sejam ambas verdadeiras. Então, segundo o 1.º princípio lógico de equivalência (pág. 61, 1.º tomo), também a proposição

$$f(\alpha, \varphi(\alpha)) = 0$$

será verdadeira. Daqui se conclui que $(\alpha, \beta)$ também é solução do sistema de equações

$$(2) \qquad \begin{cases} f(x, \varphi(x)) = 0 \\ y = \varphi(x) \end{cases}$$

Analogamente se reconhece que toda a solução de (2) também é uma solução de (1).

NOTAS — I. Para comodidade de exposição, consideramos a primeira equação de (1) com segundo membro nulo. Mas já sabemos que, pela aplicação do 2.º princípio de equivalência de equações (pág. 97), é sempre possível reduzir uma equação a essa forma.

II. O princípio de substituição não se aplica só a equações em corpos: é válido em qualquer universo, isto é, constitui um *princípio lógico de equivalência.*

EXEMPLO. Seja o sistema

$$\begin{cases} 2x + y^2 = 3 \\ 3x - y = 2 \end{cases} \quad (\textit{no corpo } \mathbb{R})$$

Resolvendo a segunda equação em ordem a x, vem:

$$\begin{cases} 2x + y^2 = 3 \\ x = \dfrac{y+2}{3} \end{cases} \Leftrightarrow \begin{cases} 2 \cdot \dfrac{y+2}{3} + y^2 = 3 \\ x = \dfrac{y+2}{3} \end{cases} \Leftrightarrow \begin{cases} 3y^2 + 2y = 5 \\ x = \dfrac{y+2}{3} \end{cases}$$

Ora

$$3y^2 + 2y - 5 = 0 \Leftrightarrow y = \frac{-1 \pm \sqrt{16}}{3} \Leftrightarrow y = 1 \vee y = -\frac{5}{3}$$

Assim, o sistema dado é equivalente ao seguinte:

$$\begin{cases} y = 1 \vee y = -\dfrac{5}{3} \\ x = \dfrac{y+2}{3} \end{cases} \Leftrightarrow \begin{cases} y = 1 \\ x = \dfrac{1+2}{3} = 1 \end{cases} \vee \begin{cases} y = -\dfrac{5}{3} \\ x = \dfrac{-5/3 + 2}{3} = \dfrac{1}{9} \end{cases}$$

o que mostra que as soluções do sistema são (1, 1) e $(\frac{1}{9}, -\frac{5}{3})$, considerando x como a *primeira* incógnita e y como a *segunda* incógnita.

*Note que se aplicou aqui a distributividade da conjunção relativamente à disjunção, visto que um sistema de equações é uma conjunção de condições.*

PRINCÍPIO DA ADIÇÃO ORDENADA. *Todo o sistema de equações é equivalente ao que dele resulta substituindo uma qualquer das equações pela que se obtém adicionando ordenadamente os seus dois membros aos de outra equação qualquer do sistema.*

Este princípio é uma consequência do 2.º princípio lógico da equivalência, aplicado à seguinte equivalência formal:

$$a = b \wedge c = d \Leftrightarrow a + c = b + d \wedge c = d, \quad \forall\, a, b, c, d \in K,$$

que também se pode apresentar com o aspecto:

$$\begin{cases} a = b \\ c = d \end{cases} \Leftrightarrow \begin{cases} a + c = b + d \\ c = d \end{cases}, \quad \forall\, a, b, c, d \in K$$

Para demonstrar esta equivalência, notemos primeiro que, sendo a, b, c, d elementos quaisquer de K, se tem:

$$(a = b \wedge c = d) \Rightarrow (a + c = b + d,)$$

em virtude do primeiro princípio lógico de equivalência, atendendo a que a adição é *unívoca* em K. Como, além disso (pág. 45, 1.º tomo):

$$(a = b \wedge c = d) \Rightarrow (c = d)$$

virá (pág. 45, 1.º tomo):

$$(a = b \wedge c = d) \Rightarrow (a + c = b + d \wedge c = d)$$

A implicação inversa demonstra-se de modo análogo, notando que, pelo 1.º princípio lógico de equivalência,

$$(a + c = b + d \wedge c = d) \Rightarrow [(a+c) + (-c) = (b+d) + (-d)]$$

e que $(a+c) + (-c) = a$, $(b+d) + (-d) = b$ (*Porquê?*)

EXEMPLO. Seja, ainda, o sistema

$$\begin{cases} 2x + y^2 = 3 \\ 3x - y = 2 \end{cases}$$

Poderíamos eliminar a incógnita x na 1.ª equação por adição ordenada, *se os coeficientes de* x *fossem simétricos*. Mas isso consegue-se multiplicando os dois membros da 1.ª equação por 3 e os da segunda por −2. Em virtude do PRINCÍPIO III (pág. 97), as equações obtidas são, respectivamente, equivalentes às primeiras e, portanto

$$\begin{cases} 2x + y^2 = 3 \\ 3x - y = 2 \end{cases} \Leftrightarrow \begin{cases} 6x + 3y^2 = 9 \\ -6x + 2y = -4 \end{cases}$$

donde, por adição ordenada no segundo sistema:

$$\begin{cases} 2x + y^2 = 3 \\ 3x - y = 2 \end{cases} \Leftrightarrow \begin{cases} 3y^2 + 2y = 5 \\ 3x - y = 2 \end{cases}$$

Assim, eliminámos x na 1.ª equação pelo MÉTODO DE REDUÇÃO. Podemos, agora, terminar a resolução do sistema como anteriormente. A vantagem deste método patenteia-se, especialmente, no estudo geral dos sistemas de equações lineares, como veremos no número seguinte.

NOTA. Imediatamente se reconhece que o princípio da adição ordenadc é válido não só para corpos, como para módulos em geral.

16. **Sistemas de equações lineares.** Vamos limitar-nos ao càso de duas equações com duas incógnitas, porque, na sua essência, as ideias são análogas no caso geral.

Chama-se *sistema de duas equações lineares com duas incógnitas* (relativas a um corpo K), todo o sistema que, pelos princípios de equivalência, se possa reduzir à forma:

$$(1) \qquad \begin{cases} ax + by = c \\ a'x + b'y = c' \end{cases}$$

em que as letras x,y são variáveis (ou *incógnitas*) em K e a, b, c, a', b', c' são elementos conhecidos de K.

*Comecemos por supor que um, pelo menos, dos coeficientes das incógnitas é diferente de zero.* Seja, por exemplo, $a \neq 0$ (em qualquer dos outros casos possíveis as considerações são inteiramente análogas). Vamos ver que, neste caso, é possível eliminar x na 2.ª equação, *se porventura ainda aí figurar essa incógnita*. Com efeito, sendo $a \neq 0 \wedge a' \neq 0$, tem-se pelo PRINCÍPIO III (pág. 97):

$$(2) \qquad \begin{cases} ax + by = c \\ a'x + b'y = c' \end{cases} \Leftrightarrow \begin{cases} -aa'x - a'by = -a'c \\ aa'x + ab'y = ac' \end{cases}$$

donde, pelo PRINCÍPIO DA ADIÇÃO ORDENADA:

$$(3) \qquad \begin{cases} ax + by = c \\ a'x + b'y = c' \end{cases} \Leftrightarrow \begin{cases} ax + by = c \\ (ab'-a'b)y = ac'-a'c \end{cases}$$

Notemos, agora, que esta equivalência é válida *mesmo quando* $a \neq 0 \wedge a' = 0$, visto que, neste caso, a 2.ª equação do primeiro sistema se reduz à fórmula $b'y = c'$, enquanto a 2.ª equação do segundo sistema assume a forma $ab'y = ac'$, sendo, portanto, equivalente à anterior. (*Porquê?*) Posto isto:

HIPÓTESE 1. Suponhamos que se tem

$$ab' - a'b \neq 0$$

Então, virá:

$$\begin{cases} ax + by = c \\ a'x + b'y = c \end{cases} \Leftrightarrow \begin{cases} ax + by = c \\ y = \dfrac{ac' - a'c}{ab' - a'b} \end{cases} \quad (Porquê?)$$

Ora, pelo PRINCIPIO DE SUBSTITUIÇÃO:

$$\begin{cases} ax + by = c \\ y = \dfrac{ac' - a'c}{ab' - a'b} \end{cases} \Leftrightarrow \begin{cases} ax + b\,\dfrac{ac' - a'c}{ab' - a'b} = c \\ y = \dfrac{ac' - a'c}{ab' - a'b} \end{cases}$$

E, como a 1.ª equação do segundo sistema é equivalente a

$$ax = \frac{ab'c - a'bc - abc' + a'bc}{ab' - a'b} \Leftrightarrow ax = \frac{a(b'c - bc')}{ab' - a'b}$$

virá, finalmente, lembrando que $a \neq 0$:

$$(4) \qquad \begin{cases} ax + by = c \\ a'x + b'y = c' \end{cases} \Leftrightarrow \begin{cases} x = \dfrac{b'c - bc'}{ab' - a'b} \\ y = \dfrac{ac' - a'c}{ab' - a'b} \end{cases}$$

As duas últimas fórmulas dão-nos, pois, a solução (única) do sistema proposto, no caso em que $a \neq 0 \wedge ab' - a'b \neq 0$.

Aliás, como o coeficiente *a*, nestas fórmulas, desempenha um papel inteiramente análogo ao dos outros coeficientes das incógnitas, bastará supor $ab' - a'b \neq 0$, pois esta condição, por si só, implica que um, pelo menos, dos coeficientes a, b, a', b'(e mesmo dois) é diferente de zero, isto é:

$$(ab' - a'b \neq 0) \Rightarrow [(a \neq 0 \wedge b' \neq 0) \vee (a' \neq 0 \wedge b \neq 0)] \ (Porquê?)$$

Assim, em conclusão:

TEOREMA. *Se* $ab' - a'b \neq 0$ *o sistema* (1) *é possível e determinado, sendo a sua solução dada em* (4).

EXERCÍCIOS. Resolver os sistemas

a) $\begin{cases} \overline{2}x + \overline{3}y = \overline{4} \\ \overline{3}x + y = \overline{2} \end{cases}$, b) $\begin{cases} \dfrac{u}{9} + \dfrac{v}{7} = \dfrac{73}{63} \\ \dfrac{u}{12} - \dfrac{v}{8} = -\dfrac{7}{24} \end{cases}$

respectivamente, nos corpos $A_5$ e IR.

Passemos, agora, a uma segunda hipótese:

HIPÓTESE 2. Suponhamos que $ab' - a'b = 0$, sendo um, pelo menos, dos coeficientes das incógnitas diferente de zero.

Então, sendo por exemplo $a \neq 0$, tem-se, atendendo a (2) e (3):

$$\begin{cases} ax + by = c \\ a'x + b'y = c' \end{cases} \Leftrightarrow \begin{cases} ax + by = c \\ 0 \cdot x + 0 \cdot y = ac' - a'c \end{cases}$$

Quer isto dizer que, ao eliminar a incógnita x na 2.ª equação, se eliminou simultaneamente a incógnita y. Então, dois casos se podem verificar:

1) $ac' - a'c \neq 0$. Neste caso, a última equação é manifestamente impossível e, portanto, o sistema também o é. (*Porquê?*)

2) $ac' - a'c = 0$. Então *qualquer* par ordenado (x,y) de elementos de K verifica a última equação; esta é, pois, uma condição universal e, portanto:

$$\begin{cases} ax + by = c \\ a'x + b'y = c' \end{cases} \Leftrightarrow ax + by = c \quad (Porquê?)$$

Deste modo, as soluções do sistema proposto *são* as soluções da equação $ax + by = c$ que se podem obter resolvendo a equação em ordem a x (continuando a supor $a \neq 0$):

$$x = \frac{c - by}{a}$$

e atribuindo, depois, diferentes valores a y e calculando os valores correspondentes de x dados por esta fórmula.

EXEMPLOS E EXERCÍCIOS:

I. Seja o sistema:

$$\begin{cases} \overline{3}x + \overline{2}y = \overline{4} \\ \overline{4}x + y = \overline{3} \end{cases}, \qquad \text{no corpo } A_5$$

Multiplicando ambos os membros da 2.ª equação por $-\frac{\overline{3}}{\overline{4}} = \overline{3}$, obtém-se o sistema equivalente:

$$\begin{cases} \overline{3}x + \overline{2}y = \overline{4} \\ \overline{2}x + \overline{3}y = \overline{4} \end{cases} \Leftrightarrow \begin{cases} \overline{3}x + 2y = \overline{4} \\ 0x + 0y = \overline{3} \end{cases}$$

donde se conclui que o sistema dado é impossível.

II. Seja, agora, o sistema:

$$\begin{cases} \overline{3}x + \overline{2}y = \overline{4} \\ \overline{4}x + y = \overline{2} \end{cases}, \qquad \text{no corpo } A_5$$

Vê-se, então, que este sistema é equivalente a:

$$\begin{cases} \overline{3}x + \overline{2}y = \overline{4} \\ \overline{2}x + \overline{3}y = \overline{1} \end{cases} \Leftrightarrow \begin{cases} \overline{3}x + \overline{2}y = \overline{4} \\ 0x + 0y = 0 \end{cases}$$

e, portanto, equivalente à equação:

$$\overline{3}x + \overline{2}y = \overline{4} \Leftrightarrow y = \frac{\overline{4} + \overline{2}x}{\overline{2}} = x + \overline{2}$$

Atribuindo a x os valores $\overline{0},\overline{1},\overline{2},\overline{3},\overline{4}$, obtemos para y, respectivamento, os valores $\overline{2},\overline{3},\overline{4},\overline{0},\overline{1}$. As soluções do sistema proposto serão, pois:

$$(\overline{0},\overline{2}),\quad (\overline{1},\overline{3})\quad (\overline{2},\overline{4}),\quad (\overline{3},\overline{0})\quad (\overline{4},\overline{1})$$

III. Resolva os sistemas (em IR):

a)
$$\begin{cases} \dfrac{2x-1}{2} + \dfrac{y}{3} = x - \dfrac{1-2y}{6} \\ 2x + y = 1 - y \end{cases}$$

b)
$$\begin{cases} \dfrac{3-h}{2} + k - \dfrac{5}{4} = \dfrac{1 - 2h + 4k}{4} \\ 2h + h = 1 - h \end{cases}$$

Respostas: a) é impossível; b) é simplesmente indeterminado, equivalente à equação $3h + k = 1$; as suas soluções, *em número infinito,* podem obter-se, por exemplo, atribuindo valores reais arbitrários a h e calculando os valores correspondentes de $k = 1 - 3h$.

Resta-nos analisar uma terceira hipótese:

HIPÓTESE 3. Os coeficientes das incógnitas são todos nulos.

Neste caso, o sistema (1) reduz-se à forma

$$\begin{cases} 0x + 0y = c \\ 0x + 0y = c' \end{cases}$$

e é fácil ver que:

1) *será impossível se* $c \neq 0 \vee c' \neq 0$;

2) *admite como solução qualquer par ordenado de elementos*

*de* k *se* c = c' = 0 (diz-se, então, que o sistema é *duplamente indeterminado*).

EXERCÍCIO. Estudar os sistemas:

a) $\begin{cases} \dfrac{x}{3} + \dfrac{x}{2} + 1 = \dfrac{2x + 3y}{6} ; \\ \dfrac{2x - 5y}{10} + 2 = \dfrac{x}{5} - \dfrac{y}{2} + 2 \end{cases}$ b) $\begin{cases} \dfrac{r}{3} + \dfrac{s}{2} + 1 = \dfrac{2r + 3s}{6} + 1 \\ \dfrac{2r - 5s}{10} + 2 = \dfrac{r}{5} - \dfrac{s}{2} + 2 \end{cases}$

* * *

CASO DOS SISTEMAS COM MAIS DE UMA EQUAÇÃO OU MAIS DE UMA INCÓGNITA. As considerações anteriores estendem-se, facilmente, ao caso de sistemas de equações lineares com mais de 2 equações ou mais de 2 incógnitas. Seja, por exemplo, o sistema:

$$\begin{cases} \overline{3}x + \overline{2}y + \overline{4}z = \overline{1} \\ x + \overline{2}y + \overline{4}z = \overline{0} \\ \overline{2}x + \overline{4}y + \overline{3}z = \overline{5} \end{cases}, \quad \text{no corpo } A_7$$

Multiplicando ambos os membros da 2.ª equação por $-\overline{3} = \overline{4}$ e os da 3.ª por $-\overline{3}/\overline{2} = -\overline{5} = \overline{2}$; adicionando, em seguida, ordenadamente os dois membros da 1.ª aos da 2.ª e aos da 3.ª, vem sucessivamente:

$$\begin{cases} \overline{3}x + \overline{2}y + \overline{4}z = \overline{1} \\ \overline{4}x + y + \overline{2}z = \overline{0} \\ \overline{4}x + y + \overline{6}z = \overline{3} \end{cases} \Leftrightarrow \begin{cases} \overline{3}x + \overline{2}y + \overline{4}z = \overline{1} \\ \overline{3}y + \overline{6}z = \overline{1} \\ \overline{3}y + \overline{3}z = \overline{4} \end{cases}$$

Ora

$$\begin{cases} \overline{3}y + \overline{6}z = \overline{1} \\ \overline{3}y + \overline{3}z = \overline{4} \end{cases} \Leftrightarrow \begin{cases} \overline{3}y + \overline{6}z = \overline{1} \\ \overline{3}z = \overline{4} \end{cases}$$

e, como $\overline{3}z = \overline{4} \Leftrightarrow z = \overline{6}$, vem, substituindo na equação anterior:

$$\overline{3}y + \overline{6} \cdot \overline{6} = \overline{1} \Leftrightarrow \overline{3}y = \overline{0} \Leftrightarrow y = \overline{0}$$

e, finalmente, por substituição na 1.ª equação do sistema dado:

$$\overline{3}x + \overline{4} \cdot \overline{6} = \overline{1} \Leftrightarrow \overline{3}x + \overline{3} = \overline{1} \Leftrightarrow \overline{3}x = \overline{5} \Leftrightarrow x = \overline{4}$$

O sistema terá, pois, uma *única solução:*

$$x = \overline{4} \wedge y = \overline{0} \wedge z = \overline{6}$$

EXERCÍCIO. Resolver os seguintes sistemas em IR:

$$\begin{cases} 3x - 2y + z = 1 \\ 2x + 5y - 3z = 2 \\ 5x + 3y - 2z = 3 \end{cases} \quad , \quad \begin{cases} 3x - 2y + z = 1 \\ 2x + 5y - 3z = 2 \\ 5x + 3y - 2z = 1 \end{cases}$$

17. **Determinantes de 2.ª ordem e sua aplicação.** Seja ainda K um corpo qualquer. Escreve-se por definição:

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc \quad , \quad \forall\, a, b, c, d \in K$$

Chama-se *determinante de* 2.ª *ordem* à função de 4 variáveis assim definida. Também se dá esse nome ao símbolo do 1.º membro ou a qualquer outro que dele se obtenha substituindo as variáveis a, b, c, d por constantes ou por outras variáveis, dependentes ou independentes.

Como se viu no número anterior, a resolução e a discussão dos sistemas da forma

$$(1) \qquad \begin{cases} ax + by = c \\ a'x + b'y = c' \end{cases}$$

têm, como ponto de partida, a expressão ab' – a'b, que, segundo a definição anterior, se pode agora escrever

$$\begin{vmatrix} a & b \\ a' & b' \end{vmatrix}$$

Ao valor desta expressão (ou à própria expressão) chamaremos *determinante do sistema* (1). Segundo o que foi demonstrado:

> O sistema é possível e determinado, sse o seu determinante for diferente de zero.

Nesta hipótese, vimos que a solução (única) é dada pelas fórmulas:

$$x = \frac{b'c - bc'}{ab' - a'b} \quad , \quad y = \frac{ac' - a'c}{ab' - a'b} \, ,$$

que, com a notação de determinante, assumem agora o aspecto:

$$x = \frac{\begin{vmatrix} c & b \\ c' & b' \end{vmatrix}}{\begin{vmatrix} a & b \\ a' & b' \end{vmatrix}} \quad , \quad y = \frac{\begin{vmatrix} a & c \\ a' & c' \end{vmatrix}}{\begin{vmatrix} a & b \\ a' & b' \end{vmatrix}}$$

Traduzindo isto por palavras, obtemos a seguinte regra:

REGRA DE CRAMER. *Os valores de* x *e de* y *que verificam o sistema são dados por duas fracções, que têm por denominador comum o determinante do sistema e cujos numeradores são os determinantes que se deduzem deste, substituindo respectivamente os coeficientes de* x *e de* y *pelos segundos membros das respectivas equações.*

Chama-se *matriz completa do sistema* (1) ao quadro

$$\begin{bmatrix} a & b & c \\ a' & b' & c' \end{bmatrix}$$

constituído pelos coeficientes das incógnitas e pelos segundos membros das duas equações, tal como está indicado. Esta matriz fornece três determinantes de 2.ª ordem:

$$D = \begin{vmatrix} a & b \\ a' & b' \end{vmatrix}, \quad D' = \begin{vmatrix} a & c \\ a' & c' \end{vmatrix}, \quad D'' = \begin{vmatrix} b & c \\ b' & c' \end{vmatrix}$$

Como vimos, o sistema tem uma única solução, sse $\Delta \neq 0$:

$$x = -\frac{D''}{D} \quad , \quad y = \frac{D'}{D}$$

*Seja agora* $D = 0$ *e suponhamos que um dos coeficientes das incógnitas é diferente de zero: seja, por exemplo,* $a \neq 0 \vee a' \neq 0$.

Então, como vimos no número anterior, a discussão incide sobre o valor da expressão $ac' - a'c$, valor que podemos agora designar pelo símbolo:

$$\begin{vmatrix} a & c \\ a' & c' \end{vmatrix} \text{ ou seja } D'$$

e duas hipóteses se podem verificar:

1) $D' \neq 0$: *sistema impossível*

2) $D' = 0$: *sistema simplesmente indeterminado (equivalente à 1.ª ou à 2.ª equação, conforme* $a \neq 0$ *ou* $a' \neq 0$).

Se $b \neq 0 \vee b' \neq 0$, as conclusões são análogas, substituindo D' por D".

Assim, a discussão pode resumir-se no seguinte quadro:

$D \neq 0$: *sistema possível e determinado*

$$D = 0 \begin{cases} a \neq 0 \vee a' \neq 0 \begin{cases} D' \neq 0: \textit{ sistema impossível} \\ D' = 0: \textit{ simplesmente indeterminado} \end{cases} \\ b \neq 0 \vee b' \neq 0 \quad \textit{conclusões análogas com D" em vez de D'} \\ a = a' = b = b' = 0: \begin{cases} c \neq 0 \vee c' \neq 0: \textit{ sistema impossível} \\ c = c' = 0: \textit{ duplamente indeterminado} \end{cases} \end{cases}$$

(Para exemplos, bastará passar ao número seguinte).

18. **Interpretação geométrica dos resultados anteriores em $\mathbb{R}^2$; paralelismo e coincidência de rectas.** Para este estudo, ver *Geometria Analítica Plana,* Cap. III, § 2 (pág. 63-71) (1), utilizando o conceito de determinante. Supõe-se feito o estudo dos §§ 1, 2, definindo *'declive duma recta'*, não a partir da inclinação, mas directamente, como se faz no n.º 25 do mesmo compêndio.

19. **Equações paramétricas.** Consideremos a equação

$$(t-1)x = t + 1 \qquad \text{(no corpo } \mathbb{R})$$

Sem mais explicações, trata-se duma *equação com duas incógnitas,* x e t. As suas *soluções* são os pares ordenados (t,x) de números reais, tais como

$$(3,2),\quad (5,3/2),\quad (0,-1),\quad (-1,0),\quad \text{etc.}$$

que convertem a equação numa proposição verdadeira.

(1) Ver nota da pág. 48.

Mas, a mesma fórmula pode traduzir este *outro* problema, embora no fundo equivalente ao primeiro:

*Determinar uma função* f *tal que, substituindo* x *por* f(t), *a equação dada se transforma numa identidade (isto é, numa equação em* t *universal).*

Nestas condições, existe uma solução do problema, que é a função $t \curvearrowright x$ dada pela fórmula:

$$x = \frac{t+1}{t-1}$$

e cujo domínio é $D_f = \{ t \in \mathbb{R}: t \neq 1 \}$

*'Resolver a equação em relação a* x' *ou 'exprimir* x *como função de* t' são, neste caso, expressões equivalentes que significam *'determinar uma função* f *que verifique a condição enunciada'.*

Note-se que se têm:

$$(t-1)x = t+1 \Leftrightarrow x = \frac{t+1}{t-1}$$

e, por isso, dizemos que a referida função *resolve completamente o problema.*

Consideremos, agora, a equação

$$y^2 - 4x^2 = 0 \qquad (\text{em } \mathbb{R})$$

e o seguinte problema: *resolver esta equação em ordem a* y.

Neste caso, tem-se:

$$y^2 - 4x^2 = 0 \Leftrightarrow y = 2x \vee y = -2x$$

e, por isso, diremos que as funções $x \curvearrowright 2x$, $x \curvearrowright -2x$ *resolvem completamente o problema*. Mas, tem-se igualmente:

$$y^2 - 4x^2 = 0 \Leftrightarrow y = 2|x| \vee y = -2|x|$$

e, por isso, diremos que também as funções $x \curvearrowright 2|x|$, $x \curvearrowright -2|x|$ *resolvem completamente o problema* (ou ainda, que formam um *conjunto completo de soluções do problema)*.

Note-se que

$$y^2-4x^2 \equiv (y-2x)\,(y+2x) \equiv (y-2|x|)\quad(y+2|x|)$$

Dum modo geral, chama-se *equação paramétrica com uma incógnita* uma equação com mais de uma variável, uma das quais é denominada *incógnita*, sendo a restante ou as restantes variáveis chamadas parâmetros. Se for x a incógnita e houver um só parâmetro t, chama-se *solução da equação paramétrica* toda a função f tal que, substituindo x por f(t), a equação se converte numa identidade. Diz-se então que um conjunto de funções $f_1, f_2, \ldots f_n$ é um *conjunto completo* de soluções da equação paramétrica, sse esta for equivalente à condição

$$x = f_1(t) \vee x = f_2(t) \vee \ldots \vee x = f_n(t)$$

Analogamente, para mais de um parâmetro e para *equações ou sistemas de equações paramétricas com mais de uma incógnita.*

Por exemplo, a *equação geral do 2.º grau em* x

$$ax^2 + bx + c = 0$$

com a, b, c *variáveis* num corpo K e $a \neq 0$, é uma equação para-

métrica, em que a incógnita é *x* e os parâmetros são, a, b, c. Então as fórmulas

$$x = \frac{-b + \sqrt{b^2-4ac}}{2a} \quad , \quad x = \frac{-b - \sqrt{b^2-4ac}}{2a}$$

fornecem um sistema completo de soluções da equação paramétrica.

Analogamente, o sistema geral de *duas equações lineares com duas incógnitas* x,y:

$$\begin{cases} ax + by = c \\ a'x + b'y = c' \end{cases}$$

e com a,a', b,b', c,c' *variáveis* em K, é um sistema de equações paramétricas, que, no caso $ab'-a'b \neq 0$, é *resolvido completamente* pelo sistema de fórmulas

$$x = \frac{b'c - bc'}{ab' - a'b} \quad \wedge \quad y = \frac{ac' - a'c}{ab' - a'b},$$

mas que, no caso $ab'-a'b = ac'-a'c = 0 \wedge a \neq 0$ é equivalente à 1.ª equação paramétrica, etc.

Note-se que, na prática, uma equação ou um sistema de equações paramétricas é geralmente a tradução em linguagem simbólica, dum *problema concreto com dados variáveis, que vem a ser os parâmetros* (ver *Compêndio de Álgebra, 7.º ano,* pág. 71) (1).

Para discussão ou resolução de equações paramétricas, podem ver-se alguns exercícios do *Compêndio de Álgebra, VII ano,* Capítulos XIV, XV e XVI (1), mas *sem abusar,* pois que, como se dirá adiante, este assunto interessa principalmente quando relacionado com problemas concretos.

20. **Resolução e discussão de problemas concretos por meio de equações.** Para este assunto, ver *Compêndio de Álgebra, 7.º ano,* Cap. XXI, págs. 196-209 (1). Este assunto, como, dum modo

(1) Ver nota da pág. 48.

geral tudo o que se refere a aplicações concretas da matemática, é da máxima importância, quer formativa, quer informativa, É principalmente a propósito de problemas concretos — e não em abstracto — que interessa fazer a discussão de equações ou sistemas de equações.

21. **Equações do 3.º grau.** Seja ainda K um corpo qualquer. Como sabemos, chama-se *equação do* 3.º *grau* (ou *equação cúbica*) toda a equação que, pelos princípios de equivalência, possa ser reduzida à forma

$$ax^3 + bx^2 + cx + d = 0 \tag{1}$$

em que a, b, c, d são elementos dados de K, com $a \neq 0$.

• *Uma equação cúbica não pode ter mais de* 3 *raízes distintas.*

Com efeito, se uma equação da forma (1), com $a \neq 0$, tem *pelo menos* três raízes distintas $x_1, x_2, x_3$, o seu primeiro membro é divisível por $x - x_1$, isto é, existe um polinómio $ax^2 + b'x + c'$ tal que

$$ax^3 + bx^2 + cx + d \equiv (x - x_1)\ (ax^2 + b'x + c')$$

Então, como $x_2$ e $x_3$ não anulam o primeiro factor do 2.º membro ($x_2 \neq x_1 \wedge x_3 \neq x_1$), anulam necessariamente o segundo factor e portanto $ax^2 + b'x + c' = a(x - x_2)\ (x - x_3)$.

Assim:

$$ax^3 + bx^2 + cx + d \equiv a(x - x_1)\ (x - x_2)\ (x - x_3)$$

e, como $a \neq 0$, *não existe nenhum* x *em* K, *diferente de* $x_1$, *de* $x_2$ *e de* $x_3$, que anule este produto e, portanto, o primeiro membro.

• *Equação cúbica binómia* (relativa a K) será toda a equação da forma

$$x^3 - \alpha = 0 \text{ ou ainda } x^3 = \alpha, \text{ com } \alpha \in K$$

Toda a raiz de tal equação (se existe pelo menos uma) será chamada *raiz cúbica de* $\alpha$. *Uma* das raízes cúbicas de $\alpha$, que porventura existam, será designada pelo símbolo $\sqrt[3]{\alpha}$.

Seja por exemplo $K = A_5$. Então

$$(x \curvearrowright x^3) = \begin{pmatrix} \overline{0} & \overline{1} & \overline{2} & \overline{3} & \overline{4} \\ \overline{0} & \overline{1} & \overline{3} & \overline{2} & \overline{4} \end{pmatrix}$$

Assim, cada elemento do corpo $A_5$ tem uma e uma só raiz cúbica (em $A_5$):

$$\sqrt[3]{\overline{0}} = \overline{0}, \quad \sqrt[3]{\overline{1}} = \overline{1}, \quad \sqrt[3]{\overline{2}} = \overline{3}, \quad \sqrt[3]{\overline{3}} = \overline{2}, \quad \sqrt[3]{\overline{4}} = \overline{4}$$

Seja agora $K = A_7$. Então

$$(x \curvearrowright x^3) = \begin{pmatrix} \overline{0} & \overline{1} & \overline{2} & \overline{3} & \overline{4} & \overline{5} & \overline{6} \\ \overline{0} & \overline{1} & \overline{1} & \overline{6} & \overline{1} & \overline{6} & \overline{6} \end{pmatrix}$$

Assim, cada um dos elementos $\overline{1}$, $\overline{6}$, de $A_7$ tem $\overline{3}$ raízes cúbicas, o elemento $\overline{0}$ tem uma só raiz cúbica e os elementos $\overline{2}$, $\overline{3}$, $\overline{4}$, $\overline{5}$, não têm nenhuma raiz cúbica (em $A_7$).

Por sua vez em IR, como é sabido, cada elemento tem uma e só uma raiz cúbica.

Dada uma equação cúbica qualquer, é natural procurar reduzir a sua resolução à de equações binómias (*resolução algébrica ou resolução por meio de radicais*). Em primeiro lugar, procuremos,

como na equação do 2.º grau, determinar um elemento h tal que, substituindo x por y + h se obtenha uma equação cúbica em y:

$$(2) \qquad a(y+h)^3 + b(y+h)^2 + c(y+h) + d = 0$$

em que o coeficiente de $y^2$ seja nulo. Ora, feitos os cálculos necessários, vê-se que o termo em $y^2$, para cada valor de h, é $(3ah + b)y^2$. *Suponhamos que o corpo* K *não é de característica* 3. Então

$$3ah + b = 0 \Leftrightarrow h = -\frac{b}{3a}$$

Portanto, atribuindo este valor a *h* em (2) e multiplicando ambos os membros da equação (2) por $a^{-1}$, obtém-se uma equação em que o coeficiente de $y^3$ é 1 e o coeficiente de $y^2$ é 0. Podemos, pois, reduzir o nosso estudo a equações da forma

$$(3) \qquad x^3 + px + q = 0 \quad , \quad \text{com } p, q \in K$$

Para tentar resolver uma tal equação, ponhamos

$$(4) \qquad x = u + v$$

e procuremos determinar u,v de modo que se verifique a equação (3). Esta assume então a forma

$$u^3 + v^3 + 3u^2v + 3uv^2 + p(u+v) + q = 0$$

ou seja

$$u^3 + v^3 + + (3uv + p)\ (u + v) + q = 0$$

e vê-se que será verificada, *se*

$$(5) \qquad u^3 + v^3 = -q \ \wedge \ uv = -\frac{p}{3}$$

Procuremos, então, determinar dois elementos $\alpha$ e $\beta$ de K tais que

$$(6) \qquad \alpha + \beta = -q \ \wedge \ \alpha\beta = -\left(\frac{p}{3}\right)^3$$

Tais elementos, se existem, serão as raízes da equação

$$(z - \alpha)\ (z - \beta) = 0 \ \Leftrightarrow \ z^2 + qz - \frac{p^3}{27} = 0,$$

dadas pela fórmula resolvente usual, *se o corpo* K *não é de característica* 2. Suponhamos verificada mais esta hipótese e tomemos:

$$(7) \qquad \alpha = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$$

*Suponhamos, agora, que existe pelo menos uma raiz cúbica de* $\alpha$ *e designemo-la por* $\sqrt[3]{\alpha}$. Então, como $\alpha\beta = -\frac{p^3}{27}$ e $\alpha + \beta = -q$ virá:

$$\beta = -\frac{p^3}{27\alpha} \ \text{ e } \ \left(\sqrt[3]{\alpha}\right)^3 + \left(-\frac{p}{3\sqrt[3]{\alpha}}\right)^3 = -q$$

Por conseguinte, *se* tomarmos

$$u = \sqrt[3]{\alpha} \ \wedge \ v = -\frac{p}{3\sqrt[3]{\alpha}}$$

a condição (4) é verificada e assim, pondo $x = u + v$, também a equação (2) será verificada. Em conclusão:

TEOREMA. *Se* K *tem característica diferente de* 2 *e de* 3, *a fórmula*

$$(8) \qquad \boxed{x = \sqrt[3]{\alpha} - \frac{p}{3\sqrt[3]{\alpha}}, \ \text{com} \ \alpha = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

*dá uma solução da equação* (2) *em* K, *desde que exista pelo menos uma raiz quadrada de* $\frac{q^2}{4} + \frac{p^3}{27}$ *e uma raiz cúbica de* $\alpha$, *qualquer que seja a raiz cúbica de* $\alpha$ *designada pelo símbolo* $\sqrt[3]{\alpha}$.

A fórmula (8), sob uma forma um pouco diferente, é chamada FORMULA DE TARTAGLIA, embora tenha sido SCIPIONE DEL FERRO, ao que parece, quem primeiro teve a ideia que conduz a esta fórmula, no princípio do século XVI (ver *Compêndio de Álgebra, 7.º ano*, Nota Histórica do Cap. XXI) (1).

EXEMPLOS — I. Seja a equação

$$x^3 + 6x - 2 = 0, \quad \text{em } \mathbb{R}.$$

Então $p = 6$, $q = -2$, donde, $q/2 = -1$, $p/3 = 2$ e portanto

$$\alpha = 1 + \sqrt{1 + 8} = 4$$

Assim, uma solução será o número irracional

$$x = \sqrt[3]{4} - \frac{2}{\sqrt[3]{4}}$$

(Prove que este número é $> 0$ e verifique directamente que é uma raiz da equação). Aplicando a regra de Ruffini, elimina-se esta raiz obtendo-se a equação

$$x^2 + \left(\sqrt[3]{4} - \frac{2}{\sqrt[3]{4}}\right)x + \left(\sqrt[3]{4} - \frac{2}{\sqrt[3]{4}}\right)^2 + 6 = 0$$

Como o discriminante desta equação é negativo (*prove*), conclui-se que a equação cúbica dada tem só aquela raiz em $\mathbb{R}$. Calcule-a com aproximação até às milésimas, utilizando uma tabela de cubos.

---

(1) Ver nota da pag. 48.

II. Seja, agora, a equação $x^3 - 15x - 4 = 0$, em $\mathbb{R}$. Neste caso:

$$\frac{q^2}{4} + \frac{p^3}{27} = \left(-\frac{4}{2}\right)^2 + \left(-\frac{15}{3}\right)^3 = (-2)^2 + (-5)^3 = -121$$

*Ora,* $-121$ *não tem raiz quadrada em* $\mathbb{R}$. Logo, a fórmula de Tartaglia, restringida ao corpo $\mathbb{R}$, não fornece nenhuma raiz da equação neste corpo. *E, contudo, esta equação tem* 3 *raízes reais, que são* $4$, $2+\sqrt{5}$, $2-\sqrt{5}$, *como se pode verificar directamente.*

NOTA MUITO IMPORTANTE. Alargando o corpo $\mathbb{R}$, com a introdução dos *números imaginários,* a fórmula de Tartaglia passa a fornecer as três raízes reais da equação, como veremos adiante.

III. Seja a equação

$$x^3 + \overline{2}x + 2 = 0 \text{ no corpo } A_5$$

Então

$$-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3} = -\overline{1} + \sqrt{\overline{1} + \overline{4}^3} = \overline{4}$$

Ora, como vimos atrás, $\overline{4}$ tem a raiz cúbica $\overline{4}$ (única) em $A_5$. Logo, a fórmula de Tartaglia fornece *uma* raiz da equação, que é

$$x = \overline{4} - \frac{\overline{2}}{3 \cdot \overline{4}} = \overline{3}$$

Contudo, esta equação tem uma outra raiz em $A_5$, que é $\overline{1}$. Aliás, pode verificar-se que

$$x^3 + \overline{2}x + \overline{2} \equiv (x - \overline{1})^2 (x - \overline{3})$$

**(Diz-se, então, que $\overline{1}$ é uma *raiz dupla* e $\overline{3}$ uma *raiz simples* da equação.)**

*No entanto, como veremos adiante, a fórmula de Tartaglia fornece também a raiz* $\overline{1}$, *desde que se alargue de modo conveniente o corpo* $A_5$.

22. **Criação do corpo complexo.** No exemplo II do número anterior surgiu-nos uma situação paradoxal: a equação proposta tem 3 raízes reais e, contudo, a fórmula de Tartaglia não fornece nenhuma raiz (no exemplo III observámos uma situação semelhante em $A_5$). Por isso, a fórmula de Tartaglia foi a princípio considerada ilusória, destituída de real interesse (1). Porém, BOMBELLI, professor em Bolonha depois de Tartaglia, preferiu adoptar uma atitude construtiva, que se traduziu num *golpe audacioso de imaginação criadora:* não hesitou em considerar os radicais do tipo $\sqrt{-A}$, com $A > 0$, como representativos de números de nova espécie (a que ele chamava 'quantidades silvestres' e a que chamamos hoje 'imaginários') e em combiná-los, por adição, com os números reais. *Assim surgiram os números complexos, isto é, números da forma* $a + b\sqrt{-1}$, *com* $a, b \in \mathbb{R}$, *cuja teoria é esboçada no livro 'Álgebra' de Bombelli (*1752*).* O objectivo imediato desta teoria era dar validade à fórmula de Tartaglia, em qualquer caso, quando aplicada a *números.* Ora, esse objectivo não só foi atingido, como também foi largamente ultrapassado: a teoria dos números complexos acabou por ter enorme importância em matemática e encontra hoje constantes aplicações na física e na engenharia, nomeadamente em electrotecnia.

Assim, podemos dizer que a teoria dos números complexos é

---

(1) Era essa, por exemplo, a opinião de Pedro Nunes, que também não admitia a existência dos números negativos, porque não havia no seu tempo uma teoria rigorosa dos números relativos (ou números reais). Porém, a rejeição dos números negativos tornava extremamente complicado o estudo da álgebra e, em especial, a teoria da equação do 2.º grau.

um *subproduto,* de altíssimo valor, da teoria algébrica da equação do 3.º grau.

Vamos agora ver como a teoria dos números complexos pode ser estabelecida com rigor. O problema que se põe pode ser enunciado, com precisão, nos seguintes termos:

PROBLEMA. *Construir um corpo* (C *que verifique as* 3 *seguintes condições:*

1) (C *contém* |R, *e as operações de adição e multiplicação em* (C *são extensões das operações homónimas em* |R.

2) *A equação* $x^2 + 1 = 0$ *admite, pelo menos, uma solução em* (C.

3) *Todo o elemento de* (C *pode ser representado sob a forma* $a + bi$, *em que* a, b *são números reais, e* i *é uma das soluções da equação* $x^2 = -1$ *(a outra será* $-i$).

A condição 1) também se exprime dizendo:

'(C é uma *extensão do corpo* |R'

ou '|R é um *subcorpo* de (C'.

Para resolver este problema vamos seguir o MÉTODO DO PROBLEMA RESOLVIDO, que consiste em começar por supor que o problema admite, pelo menos, uma solução e em deduzir dessa hipótese consequências que acabem por indicar o caminho para construir efectivamente uma solução.

*Suponhamos, pois, que existe um corpo* (C *que verifica as condições do problema.* Chamar-lhe-emos *'corpo complexo'* e, aos seus elementos, *'números complexos'*. Portanto, segundo a condição 3), cada número complexo será da forma $a + bi$, com $a, b \in |R$ e $i^2 = -1$; o número *a* será chamado *'parte real'* e o número b *'coeficiente da parte imaginária'* (ou *'coeficiente de* i') do número $a + bi$. Por exemplo:

$$2 + 3i, \quad 1 - \frac{2}{3}i, \quad -1 + \sqrt{2}\,i, \quad 5, \quad -7i$$

serão números complexos, que têm como partes reais respectivamente 2, 1, −1, 5, 0, e como coeficientes das partes imaginárias respectivamente 3, −2/3, $\sqrt{2}$, 0, −7.

*Posto isto, vejamos como se opera com números complexos.*

a) IGUALDADE (1). Consideremos dois números complexos:

$$a + bi \quad , \quad a' + b'i, \text{ com } a, b, a', b' \in \mathbb{R}.$$

Se for $a = a'$ e $b = b'$, tem-se $a + bi = a' + b'i$, em virtude do 1.º *princípio lógico de equivalência* e atendendo a que a adição e a multiplicação são unívocas em $\mathbb{C}$.

Assim:

$$(1) \qquad a = a' \wedge b = b' \Rightarrow a + bi = a' + b'i$$

Suponhamos agora, reciprocamente, que

$$a + bi = a' + b'i$$

Daqui, atendendo a que $\mathbb{C}$ é um corpo, deduz-se:

$$(a + bi) - (a' + b'i) = 0$$

ou seja:

$$(2) \qquad (a - a') + (b - b')i = 0 \qquad (\textit{Porquê?})$$

Então, se fosse $b \neq b'$, seria $b - b' \neq 0$, donde:

$$i = \frac{a - a'}{b' - b} \quad \text{e, portanto} \quad \left(\frac{a - a'}{b' - b}\right)^2 = -1$$

---

(1) A palavra igualdade é aqui usada na acepção de 'identidade lógica'.

Ora isto é impossível, visto que $\frac{a - a'}{b' - b}$ seria, então, um número *real* e não existe nenhum número real cujo quadrado seja $-1$. Terá de ser pois $b = b'$. Então de (2) vem:

$$a - a' = 0 \quad \text{ou} \quad a = a'$$

Assim, $a + bi = a' + b'i \Rightarrow a = a' \wedge b = b'$ e portanto, atendendo a (1),

(3) $$\boxed{a + bi = a' + b'i \Leftrightarrow a = a' \wedge b = b'}$$

isto é: *dois números complexos são iguais, sse têm respectivamente iguais as partes reais e os coeficientes de* i.

Em particular, se $b' = 0$, tem-se $a' + b'i = a'$ e assim

$$a + bi = a' \Leftrightarrow a = a' \wedge b = 0, \quad \forall\, a, b, a' \in \mathbb{R},$$

isto é: *um número complexo* $a + bi$ *só é um número real se* $b = 0$. Portanto, se $b \neq 0$, o número $a + bi$ não é real: diz-se então que é *imaginário*. Assim, os números imaginários são os elementos de $\mathbb{C} \setminus \mathbb{R}$. Em particular, os números da forma bi, com $b \in \mathbb{R}$, tais como i, $-3i$, $\sqrt{3}\,i$, etc., chamam-se *imaginários puros.*

b) ADIÇÃO E MULTIPLICAÇÃO. Consideremos dois números complexos:

$$\alpha = a + bi, \quad \beta = c + di \quad (\text{com } a, b, c, d \in \mathbb{R}).$$

Atendendo a que $\mathbb{C}$ é um corpo, tem-se por um lado:

$$\alpha + \beta = (a + bi) + (c + di) = (a + c) + (bi + di)$$

Portanto:

$$(4) \qquad \boxed{(a + bi) + (c + di) = (a + c) + (b + d)\,i}$$

Por outro lado:

$$\alpha\,\beta = (a + bi) \cdot (c + di) = ac + (ad + bc)i + bdi^2,$$

donde, lembrando que $i^2 = -1$:

$$(5) \qquad \boxed{(a + bi) \cdot (c + di) = (ac - bd) + (ad + bc)i}$$

*Assim, a soma e o produto de dois números complexos* $\alpha$, $\beta$ *são calculados segundo as fórmulas* (4) e (5).

Por exemplo:

$$(1 + 2i) + (3 + 5i) = 4 + 7i$$

$$(1 + 2i)\,(3 + 5i) = (1 \times 3 - 2 \times 5) + (1 \times 5 + 2 \times 3)i = -7 + 11i$$

c) SUBTRACÇÃO. Sendo um corpo, (C é em particular um módulo e facilmente se reconhece que a diferença entre dois números complexos a + bi, c + di, é dada pela fórmula

$$\boxed{(a + bi) - (c + di) = (a - c) + (b - d)i}$$

Exemplos:

$$(8 + 5i) - (3 + 7i) = 5 + (-2)i = 5 - 2i$$

$$3 - (1 + i) = 2 - i, \quad (\sqrt{5} - \frac{2}{3}i) - (\sqrt{5} - 2i) = \frac{4}{3}i, \text{ etc.}$$

d) NÚMEROS CONJUGADOS. Chama-se *conjugado* dum número complexo $a + bi$ (com $a, b \in \mathbb{R}$) o número $a - bi$. Por exemplo, o conjugado de $3 + 5i$ é $3 - 5i$, o conjugado de $-1 - i$ é $-1 + i$, o conjugado de $3i$ é $-3i$, o conjugado de $-5$ é $-5$, etc. Desde logo se reconhece que:

I. *Todo o número complexo é conjugado do seu conjugado.*

II. *Um número complexo $\alpha$ é conjugado de si mesmo, sse $\alpha$ é real.*

III. *A soma e o produto de dois números complexos conjugados são sempre números reais.* Mais precisamente:

$$\left.\begin{array}{l}(a + bi) + (a - bi) = 2a \\ (a + bi)(a - bi) = a^2 + b^2\end{array}\right\} \quad \forall\, a, b \in \mathbb{R}$$

Por exemplo: $(1 + \sqrt{3}\,i)(1 - \sqrt{3}\,i) = 1 + (\sqrt{3})^2 = 4$

e) DIVISÃO. Consideremos dois números compiexos:

$$\alpha = a + bi \quad , \quad \beta = c + di \quad (\text{com } a, b, c, d \in \mathbb{R})$$

Como (C é um corpo, existe o quociente de $\alpha$ por $\beta$, sse $\beta \neq 0$ Ora, segundo o critério de igualdade, $c + di = 0$ sse $c = 0 \wedge d = 0$ e portanto, pela propriedade da conversão:

$$c + di \neq 0 \Leftrightarrow c \neq 0 \vee d \neq 0.$$

Assim, se $c + di \neq 0$, também $c - di \neq 0$ e, portanto (pg. 45):

$$\frac{a + bi}{c + di} = \frac{(a + bi)(c - di)}{(c + di)(c - di)} = \frac{(ac + bd) + (bc - ad)i}{c^2 + d^2}$$

$$= (c^2 + d^2)^{-1}\,[(ac + bd) + (bc - ad)i]$$

Portanto, supondo $c + di \neq 0$, tem-se:

$$\frac{a + bi}{c + di} = \frac{ac + bd}{c^2 + d^2} + \frac{bc - ad}{c^2 + d^2}\, i$$

Exemplos:

$$\frac{3 + 2i}{2 - 5i} = \frac{(3 + 2i)(2 + 5i)}{(2 - 5i)(2 + 5i)} = \frac{-4 + 19i}{29} = -\frac{4}{29} + \frac{19}{29}\, i$$

$$\frac{\sqrt{5} - i}{i\sqrt{5}} = \frac{(\sqrt{5} - i)(-i\sqrt{5})}{(i\sqrt{5})(-i\sqrt{5})} = -\frac{\sqrt{5}}{5} - i$$

f) EXISTÊNCIA DO CORPO COMPLEXO. Acabámos de ver como se opera sobre elementos dum corpo (C, que verifique as condições 1), 2), 3) do problema posto inicialmente. Mas todas as nossas conclusões se baseiam sobre uma premissa ainda não provada: *a de que existe (pelo menos) um corpo que verifica tais condições.* Ora, as próprias conclusões sugerem a maneira de construir uma solução:

*Designemos por* (C *o conjunto de todos os polinómios em* i, *de coeficientes reais e de grau não superior a* 1, *portanto da forma* a + bi, *sendo* a, b *números reais quaisquer. É óbvio que tal conjunto existe* (ver n.os 5 e 6). *Simplesmente, em vez de definir a multiplicação como se faz usualmente para polinómios, adoptemos a definição dada pela fórmula* (5), *que resulta de juntar a condição* $i^2 = -1$ *à regra usual. Quanto à adição, adoptemos a definição usual, que é dada pela fórmula* (4). *Então é fácil ver que, com tais definições de adição e multiplicação, o conjunto* (C *é efectivamente um corpo que verifica as condições do problema* (1).

(1) Neste caso, é preferível chamar 'indeterminada' em vez de 'variável' o símbolo i (ver pág. 87).

Porém, surge agora outra pergunta:

*O problema tem uma única solução?*

Vamos ver que não. Consideremos, por exemplo, o conjunto $\mathbb{R}^2$, que é constituído, como sabemos, por todos os pares ordenados (a, b) de números reais, e adoptemos em $\mathbb{R}^2$ as definições de adição e de multiplicação dadas pelas seguintes fórmulas:

$$(6)\quad \begin{cases} (a, b) + (c, d) = (a + c,\ b + d) \\ \\ (a, b) \cdot (c, d) = (ac - bd,\ ad + bc) \end{cases} \qquad (\forall\ a, b, c, d \in \mathbb{R})$$

Não oferece dificuldade verificar que, com estas definições, $\mathbb{R}^2$ é um corpo [prove, por exemplo, que (0, 0) é o elemento nulo, que (1, 0) é o elemento unidade, que a multiplicação é distributiva, e que todo o elemento não nulo de $\mathbb{R}^2$ é regular]. Mais ainda: *vamos provar que este corpo é isomorfo a qualquer corpo* (C *que verifique as condições do problema*. Seja f a aplicação

$$x + iy \curvearrowright (x, y) \quad , \quad \text{com } x, y \in \mathbb{R}$$

Facilmente se reconhece que f é uma aplicação *biunívoca* de (C sobre $\mathbb{R}^2$ (*prove*). Além disso, f *respeita a adição e a multiplicação*; com efeito, quaisquer que sejam $a, b, c, d \in \mathbb{R}$, tem-se:

$$f\,[(a + bi) + (c + di)] = f[(a + c) + (b + d)i] = (a + c, b + d)$$
$$= (a, b) + (c, d) = f(a + bi) + f(c + di)$$

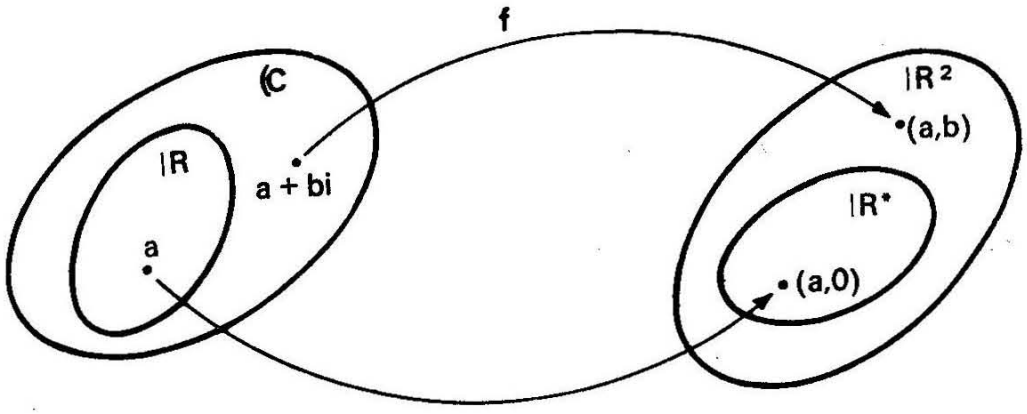
$$f[(a + bi) \cdot (c + di)] = f[(ac - bd) + (ad + bc)i]$$
$$= (ac - bd, ad + bc) = (a, b) \cdot (c, d) =$$
$$= f(a + bi) \cdot f(c + di)$$

***Por conseguinte,*** f *é um isomorfismo entre os corpos* (C *e* $\mathbb{R}^2$.

Em particular, f transforma cada número real *a* no elemento (a, 0) de $\mathbb{R}^2$. Portanto:

*A restrição de* f *ao subcorpo* $\mathbb{R}$ *de* (C *é um isomorfismo de* $\mathbb{R}$ *sobre um subcorpo* $\mathbb{R}^*$ *de* $\mathbb{R}^2$.

Esta situação é descrita pelo diagrama seguinte:




Deste modo, os corpos $\mathbb{R}^*$ e $\mathbb{R}$ têm a *mesma estrutura* e podemos, portanto, considerá-los como sendo o mesmo corpo (a menos de um isomorfismo) *identificando* cada elemento (a, 0) de $\mathbb{R}^*$ com o elemento a de $\mathbb{R}$. Feito isto, já podemos afirmar que $\mathbb{R}^2$ verifica a condição 1).

Por outro lado, f faz corresponder a i o elemento (0, 1) de $\mathbb{R}^2$ e, deste modo, como era de esperar, $\mathbb{R}^2$ verifica também a condição 2):

$$(0,1)^2 = (0,1) \cdot (0,1) = (-1,0) \text{ ou seja } (0,1)^2 = -1$$

visto que já identificámos (−1,0) com −1.

Finalmente tem-se, quaisquer que sejam a, b $\in \mathbb{R}$:

$$(a,b) = (a,0) + (0,b) = (a,0) + (b,0)\,(0,1)$$

ou seja (a, b) = a + bi, visto que identificámos (a, 0) com a, (b, 0) com *b* e (0, 1) com *i*. Assim, $\mathbb{R}^2$ verifica também a condição 3).

Em conclusão: *o conjunto* $\mathbb{R}^2$, *com todas as convenções adoptadas, é também uma solução do problema.*

Havemos ainda de encontrar mais tarde outras soluções do problema; na verdade, este admite uma infinidade de soluções. Simplesmente, o raciocínio anterior mostra o seguinte:

*Todas as soluções do problema são isomorfas ao corpo* $\mathbb{R}^2$ *considerado e, portanto, isomorfas entre si.*

Por outras palavras: *o corpo complexo existe e é determinado a menos de um isomorfismo* (1).

> Assim, o que interessa no corpo complexo não é propriamente o MATERIAL com que o construímos, isto é, a natureza dos entes a que convencionámos chamar 'números complexos', mas sim a sua ESTRUTURA, isto é, o conjunto de propriedades formais que caracterizam esse corpo.

Em conformidade, daqui por diante, ao tratar do corpo (C abstraíremos, em geral, da natureza dos seus elementos, para só atender às regras de cálculo que são válidas em (C.

Para ver até que ponto a natureza dos elementos é aqui secundária, basta observar que, no mesmo conjunto $\mathbb{R}^2$, poderíamos definir a adição e a multiplicação por meio das fórmulas:

$$\left.\begin{aligned} (a, b) + (c, d) &= (a + c,\ b + d) \\ (a, b) \cdot (c, d) &= (ac,\ bd) \end{aligned}\right\} \quad \forall\, a, b, c, d \in \mathbb{R}$$

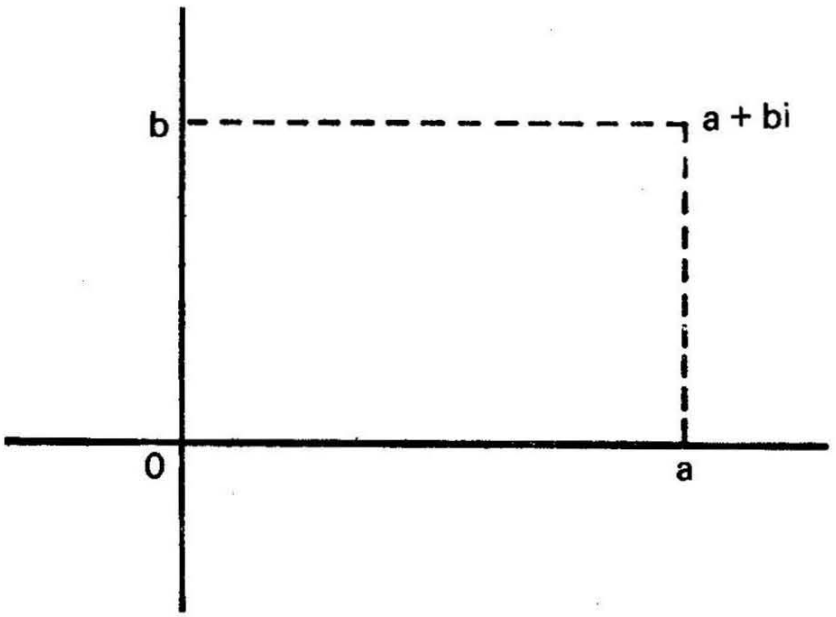
(1) Deste modo, os números imaginários têm existência tão real como os números reais, ao contrário do que podem sugerir as designações 'número real' e 'número imaginário'. Na verdade, estas designações foram introduzidas historicamente, porque, a princípio, se admitia, de certo modo, que só os números reais existiam efectivamente.

É fácil ver que, com estas definições, $\mathbb{R}^2$ passa a ser um anel comutativo, mas não um corpo, pois tem *divisores de zero*; por exemplo:

$(3, 0) \cdot (0, 5) = (0, 0)$, sendo $(3, 0) \neq (0, 0)$ e $(0, 5) \neq (0, 0)$

Portanto, a estrutura deste anel já não é a do corpo complexo, apesar de os seus elementos serem exactamente os mesmos que no caso anterior. *Mas só nesse caso — isto é, adoptando as definições* (6) *e identificando cada par* (a, 0) *ao número real* a — *é lícito chamar 'números complexos' aos elementos de* $\mathbb{R}^2$.

23. **Representação geométrica dos números complexos.** Já vimos como uma das possíveis concretizações do corpo $\mathbb{C}$ pode ser dada pelo conjunto $\mathbb{R}^2$. Por outro lado, já é sabido como se estabelece uma correspondência biunívoca entre os elementos de $\mathbb{R}^2$ e os pontos do plano cartesiano. Assim, resulta automaticamente definida uma correspondência biunívoca entre os números complexos e os pontos do plano cartesiano: a cada número complexo a + bi, que podemos identificar com o par ordenado (a, b) de números reais, corresponderá o ponto do plano que tem por abcissa e por ordenada respectivamente *a* e *b* (parte real e coeficiente da parte imaginária do número a + bi). Tal ponto será chamado a *imagem geométrica* (ou o *afixo*) de a + bi.



(Como exercício, represente geometricamente os números $3 + 5i$, $-2 + \frac{3}{2}i$, $3-5i$, $-3$, $\sqrt{2}$, $i$, $-3i$).

Veremos no 7.º ano como os números complexos podem também representar *operadores sobre vectores do plano*. É essa, aliás, a interpretação dos números complexos mais usada nas aplicações à física, à electrotecnia, etc. (Para já, pode-se ver *Compêndio de Álgebra, 6.º ano,* págs. 87-91) (1).

EXERCÍCIOS — Além dos que são propostos no referido *Compêndio,* interessa resolver os três seguintes:

I. Prove que os números $1, -\frac{1}{2} + i\frac{\sqrt{3}}{2}, -\frac{1}{2} - i\frac{\sqrt{3}}{2}$ formam um grupo multiplicativo isomorfo ao grupo das potências de

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

II. Prove que os números $1$, $i$, $-1$, $-i$ são raízes de índice 4 de 1 e formam um grupo multiplicativo isomorfo ao grupo das potências de $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$

III. Prove que as potências de expoente inteiro de $\frac{\sqrt{3}}{2} + \frac{1}{2}i$ formam um grupo multiplicativo isomorfo ao módulo H *(Bailado das Horas)* e que todas são raízes de índice 12 de 1. (Sugestão: pondo $\frac{\sqrt{3}}{2} + \frac{1}{2}i = \theta$, comece por verificar que $\theta^3 = i$ e que portanto $\theta^4 = i\theta$, $\theta^5 = i\theta^2$, etc.). Represente graficamente as referidas potências de $\theta$.

---

(1) Ver nota da pág. 48.

24. **Equações quadráticas e equações cúbicas no corpo complexo.** É fácil ver que:

*Todo o número negativo tem duas (e só duas) raízes quadradas que são números imaginários puros, simétricos entre si.*

Com efeito, seja $-a$ um número negativo. Então $a$ é um número positivo e, por isso, tem uma (e uma só) raiz quadrada positiva, que se designa por $\sqrt{a}$. Nestas condições, $i\sqrt{a}$ e $-i\sqrt{a}$ são imaginários puros e tem-se

$$(i\sqrt{a})^2 = i^2 \cdot (\sqrt{a})^2 = -a, \qquad (-i\sqrt{a})^2 = (-i)^2 \cdot (\sqrt{a})^2 = -a,$$

o que mostra que tanto $i\sqrt{a}$ como $-i\sqrt{a}$ são raízes quadradas de $-a$; e já sabemos que, *num corpo, um elemento não pode ter mais de duas raízes quadradas* (pág. 104).

É a primeira destas raízes quadradas de $-a$ que convencionaremos designar pelo símbolo $\sqrt{-a}$:

$$\sqrt{-a} = i\sqrt{a} \quad (a > 0)$$

Por exemplo, as raízes quadradas de $-1$ são $i$ e $-i$; as raízes quadradas de $-9$ são $3i$ e $-3i$; as raízes quadradas de $-3$ são $i\sqrt{3}$ e $-i\sqrt{3}$, etc.; e escreveremos:

$$\sqrt{-1} = i, \ \sqrt{-4} = 2i, \ \sqrt{-3} = \sqrt{3}\, i = i\sqrt{3}, \text{ etc.}$$

· Posto isto, consideremos uma equação quadrática

$$(1) \qquad ax^2 + bx + c = 0$$

de coeficientes a, b, c *reais* ($a \neq 0$). Já vimos que uma tal equação só tem raízes reais, sse o seu discriminante, $\Delta = b^2 - 4ac$, for $\geqslant 0$. Se $\Delta < 0$, a equação não tem raízes reais, porque $\Delta$ não tem raiz quadrada em $\mathbb{R}$. *Mas acabámos de ver que, neste caso, $\Delta$ tem duas*

*raízes quadradas em* (C, *que são números imaginários puros.* Assim, a equação (1) passa a ter, neste caso, duas raízes em (C,

$$x_1 = \frac{-b + \sqrt{\Delta}}{2a}, \quad x_2 = \frac{-b - \sqrt{\Delta}}{2a},$$

que são números imaginários, visto que $\sqrt{\Delta}$ é um imaginário puro e *a, b* são números reais.

Seja, por exemplo, a equação

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

Aplicando a fórmula resolvente simplificada, tem-se

$$x = 1 \pm \sqrt{1-5} = 1 \pm \sqrt{-4} = 1 \pm 2i$$

A equação tem, pois, duas raízes imaginárias conjugadas, $1 + 2i$ e $1 - 2i$. Em resumo:

TEOREMA. *Uma equação quadrática de coeficientes reais tem duas reais distintas, uma raiz real dupla ou duas raízes imaginárias conjugadas, conforme o seu discriminante é maior que zero, igual a zero ou menor que zero.*

Suponhamos, agora, que os coeficientes da equação (1) não são todos reais. Continuará a ser resolúvel em (C? A resposta é afirmativa. Com efeito, demonstra-se em matemática superior o seguinte teorema, conhecido por 'TEOREMA DE D'ALEMBERT':

*Toda a equação algébrica de grau* $n > 1$, *cujos coeficientes são números complexos, tem pelo menos uma raiz em* (C *(qualquer que seja* $n > 1$).

No sétimo ano demonstraremos este teorema no caso particular das *equações binómias:*

$$\forall\, n \in \mathbb{N}, \quad \forall\, \alpha \in (C, \quad \exists\, z \in (C: \quad z^n = \alpha$$

Mais precisamente, provaremos que *qualquer que seja* $n \in \mathbb{N}$ *um número complexo* $\alpha$ *diferente de zero tem* n *(e só* n*) raízes de índice* n *distintas;* e veremos como se determinam essas raízes (o número 0 continua a ter em $\mathbb{C}$ uma única raiz de índice *n* que é 0) (1).

Por exemplo, o número 1, que tem uma única raiz cúbica $\mathbb{R}$ (que é 1), passa a ter 3 raízes cúbicas em $\mathbb{C}$. Com efeito, $z^3-1$ é divisível por $z-1$; o quociente pode ser achado pela regra de RUFFINI:

| | 1 | 0 | 0 | −1 |
|---|---|---|---|---|
| 1 | | 1 | 1 | 1 |
| | 1 | 1 | 1 | 0 |

Será, pois, $z^3-1 \equiv (z-1)\ (z^2+z+1)$ e assim:

$$z^3 - 1 = 0 \Leftrightarrow (z-1)\ (z^2+z+1) = 0$$

Ora a equação $z^2+z+1=0$ tem duas raízes imaginárias que já sabemos achar: $-\frac{1}{2}+i\frac{\sqrt{3}}{2}$, $-\frac{1}{2}-i\frac{\sqrt{3}}{2}$. Portanto, as raízes cúbicas de 1 (ou sejam as raízes da equação $z^3-1=0$) no corpo $\mathbb{C}$ são:

$$1,\ -\frac{1}{2}+i\frac{\sqrt{3}}{2},\ -\frac{1}{2}-i\frac{\sqrt{3}}{2}$$

Designemos a segunda por $\varepsilon$. Pode verificar-se directamente que $\varepsilon^2$ dá a terceira raiz e que $\varepsilon^3=1$ (*faça os cálculos*). Assim, se

---

(1) Se $n=2$, o cálculo pode fazer-se muito facilmente aplicando a teoria da equação do 2.º grau (ver *Compêndio de Álgebra, 7.º ano,* Cap. XVI, n.º 14, págs. 129-131). — (Ver nota da pág. 48 — N. do E.).

representarmos por $\sqrt[3]{\alpha}$ *uma* das raízes cúbicas de um número complexo $\alpha$, as outras serão $\varepsilon\sqrt[3]{\alpha}$ e $\varepsilon^2\sqrt[3]{\alpha}$, visto que

$$(\varepsilon\sqrt[3]{\alpha})^3 = \varepsilon^3(\sqrt[3]{\alpha})^3 = 1 \cdot \alpha = \alpha$$
$$(\varepsilon^2\sqrt[3]{\alpha})^3 = \varepsilon^6(\sqrt[3]{\alpha})^3 = 1 \cdot \alpha = \alpha$$

Consideremos, agora, uma equação cúbica da forma

$$x^3 + px + q = 0, \tag{2}$$

sendo p, q números complexos *quaisquer*. Pelo que vimos atrás (n.º 22), a fórmula de Tartaglia

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

fornece, pelo menos, uma raiz da equação (2), desde que exista, pelo menos, uma raiz quadrada de $q^2/4 + p^3/27$ e, pelo menos, uma raiz cúbica de $\alpha$. *Ora, já sabemos que esta condição se verifica sempre em* (C. Logo, a fórmula de Tartaglia fornece, pelo menos, uma solução em (C. Mais ainda: *fornece as três soluções*. Com efeito, designando por $\sqrt[3]{\alpha}$ uma das raízes cúbicas de $\alpha$, as outras serão, como vimos, $\varepsilon\sqrt[3]{\alpha}$ e $\varepsilon^2\sqrt[3]{\alpha}$, e as três acabam por dar todas as soluções de (2), que não pode ter mais de 3 raízes distintas.

Tornemos ao exemplo da equação $x^3 - 15x - 4$ (ex. II do n.º 22). Neste caso, podemos agora tomar

$$\alpha = 2 + \sqrt{-121} = 2 + 11\,i$$

Ora, uma das raízes cúbicas de $\alpha$ é $2 + i$, como se pode ver:

$$(2 + i)^3 = (2 + i)^2(2 + i) = (3 + 4i)(2 + i) = 2 + 11\,i$$

Então, a fórmula de Tartaglia dá:

$$x = 2 + i + \frac{5}{2+i} = (2+i) + (2-i) = 4$$

Outra raiz cúbica de a será:

$$(2+i)\left(-\frac{1}{2} + \frac{i\sqrt{3}}{2}\right) = \left(-1 - \frac{\sqrt{3}}{2}\right) + i\left(\sqrt{3} - \frac{1}{2}\right)$$

e a fórmula de Tartaglia dá agora:

$$x = \left(-1 - \frac{\sqrt{3}}{2}\right) + i\left(\sqrt{3} - \frac{1}{2}\right) + \left(-1 - \frac{\sqrt{3}}{2}\right) - i\left(\sqrt{3} - \frac{1}{2}\right) = -2 - \sqrt{3}$$

A terceira raiz é obtida de modo análogo:

$$x = \left(-1 + \frac{\sqrt{3}}{2}\right) - i\left(\sqrt{3} + \frac{1}{2}\right) + \left(-1 + \frac{\sqrt{3}}{2}\right) + i\left(\sqrt{3} + \frac{1}{2}\right) = -2 + \sqrt{3}$$

Assim, observamos este facto extremamente curioso:

*Embora as três raízes da equação proposta sejam reais, é necessário sair do corpo real para que a fórmula de Tartaglia forneça as três raízes. Porém, a intervenção dos números imaginários aqui é puramente intermediária: a fórmula fornece cada uma das raízes como soma de dois números conjugados, e assim as duas partes imaginárias acabam por desaparecer. Tal fenómeno repete-se todas as vezes que as três raízes são reais — e é este precisamente o caso (chamado 'caso irredutível') em que a intervenção dos números imaginários é necessária para obter soluções reais.*

*Situações análogas se observam em vários domínios da matemática, pura ou aplicada: o caminho mais curto para obter soluções reais passa, muitas vezes, pelo campo imaginário.* Nesses casos a teoria dos números complexos funciona como *formalismo auxiliar,* isto é,

como *artifício engenhoso de cálculo,* para obter resultados, que de outro modo seria difícil ou muito trabalhoso encontrar (1).

Mas casos há em que a intervenção dos números imaginários não é apenas um meio, um processo de cálculo: *muitas vezes os resultados finais dos problemas são números imaginários susceptíveis de interpretação concreta (geralmente como operadores sobre vectores do plano).*

25. **Imaginários de Galois*.** Consideremos, novamente, a equação:

(1) $$x^3 + \overline{2}x + \overline{2} = 0 \quad \text{no corpo } A_5.$$

Como vimos (n.º 22, ex. 3) tem-se, neste caso:

$$\alpha = -\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3} = \overline{4}$$

Mas, como $\overline{4}$ tem apenas uma raiz cúbica em $A_5$, que é $\overline{4}$, a fórmula de Tartaglia dá apenas uma raiz da equação:

$$= \overline{4}x - \frac{\overline{2}}{3 \times \overline{4}} = \overline{4} - \overline{1} = \overline{3}$$

A fórmula não dá a outra raiz ($\overline{1}$, dupla), por que a equação

---

(1) Numa espécie de calão, os investigadores matemáticos costumam chamar 'truques' a tais artifícios. Mas, aqui, a palavra 'truque' não tem de modo nenhum sentido pejorativo. Pelo contrário, grandes progressos da ciência se devem a tais truques.

binómia $z^3-\overline{4}=0$ admite apenas uma raiz em $A_5$, que é $\overline{4}$. Eliminemos essa raiz pela regra de Ruffini:

| | $\overline{1}$ | 0 | 0 | $-\overline{4}$ |
|---|---|---|---|---|
| | | $\overline{4}$ | $\overline{1}$ | $\overline{4}$ |
| $\overline{4}$ | $\overline{1}$ | $\overline{4}$ | $\overline{1}$ | $\overline{0}$ |

Então, virá: $z^3-\overline{4} \equiv (z-\overline{4})\ (z^2+\overline{4}z+\overline{1})$. A origem do fenómeno está no facto de a equação $z^2+\overline{4}z+\overline{1}$ não ter solução em $A_5$. Com efeito, o seu discriminante

$$\Delta = \overline{4}^2-\overline{4} = \overline{2}$$

não tem raiz quadrada em $A_5$. *Mas também os números negativos não tinham raiz quadrada e nós conseguimos que passassem a tê-la, ampliando o corpo real com a adjunção de números imaginários.* Porque não proceder de modo análogo agora? A situação é muito semelhante. Pretende-se construir um corpo K que verifique as seguintes condições:

1) K *é uma extensão do corpo* $A_5$.

2) *A equação* $x^2 = \overline{2}$ *tem, pelo menos, uma solução em* $A_5$.

3) *Todo o elemento de* K *é da forma* a + bj, *em que* a, b *são elementos quaisquer de* $A_5$ *e* j *é uma das raízes da equação* $x^2 = \overline{2}$.

Uma solução do problema é constituída, precisamente, por todos os polinómios lineares em j

$$a + bj$$

de coeficientes a, b em $A_5$, com a definição usual de adição e com a definição de multiplicação dada pela seguinte fórmula:

$$\begin{aligned}(a+bj)\ (c+dj) &= ac + (ad + bc)j + bdj^2 \\ &= (ac + 2bd) + (ad + bc)j,\end{aligned}$$

que resulta de juntar a condição $j^2 = 2$ à definição usual. *Qualquer outra solução do problema é isomorfa a esta.*

Uma outra solução será dada pelo conjunto $A_5^2$, com as seguintes definições:

$$(a, b) + (c, d) = (a+c,\ b+d)$$

$$(c, b) \cdot (c, d) = (ac + 2bd,\ ad + bc)$$

identificando-se $(\overline{1},0)$ a $\overline{1}$ e $(0, \overline{1})$ a j.

Como j passa então a ser uma raiz quadrada de $\overline{2}$ em K (sendo a outra $-j$) podemos designar j por $\sqrt{\overline{2}}$. O novo corpo, K, poderá ser designado por $A_5(j)$ ou por $A_5(\sqrt{\overline{2}})$.

É fácil ver agora que a equação

$$z^2 + \overline{4}z + \overline{1} = 0$$

admite, neste corpo, as duas soluções

$$z_1 = \overline{3} + \overline{3}j \quad , \quad z_2 = \overline{3} - \overline{3}j$$

que são portanto, juntamente com $\overline{4}$, as raízes cúbicas de $\overline{4}$ em $A_5(j)$

Ora, utilizando estas três raízes cúbicas de $\overline{4}$, a fórmula de. Tartaglia já fornece as raízes $\overline{3}$ e $\overline{1}$ da equação (1), existentes em $A_5$, como se pode verificar.

Vejamos outro exemplo. A equação

$$x^3 - \overline{4} = 0$$

não tem solução nenhuma em $A_7$, como se pode verificar. Mas nós podemos construir um corpo K tal que:

1) K *é uma extensão do corpo* $A_7$.

2) *A equação* $x^3 = \overline{4}$ *tem, pelo menos, uma solução em* K.

3) *Cada elemento de* K *é da forma* $a + b\theta + c\theta^2$, *sendo* a, b, c

*elementos arbitrários de* $A_7$ *e* $\theta$ *uma das raízes da equação* $x^3 = \overline{4}$ *em* K.

Uma das soluções do problema é constituída precisamente pelos polinómios em $\theta$ de grau $\leqslant 2$:

$$a + b\theta + c\theta^2 \quad , \quad \text{com } a, b, c \in A_7$$

com a definição usual de adição e com a definição de multiplicação dada pela fórmula:

$$(a + b\theta + c\theta^2) \cdot (a' + b'\theta + c'\theta^2) = aa' + (ab' + a'b)\theta +$$
$$+ (ac' + a'c + bb')\theta^2 + (bc' + b'c)\theta^3 + cc'\theta^4 =$$
$$= (aa' + 4bc' + 4b'c) + (ab' + a'b + 4cc')\theta + (ac' + a'c + bb')\theta^2$$

que resulta de juntar a condição $\theta^3 = \overline{4}$ à definição usual de produto de polinómios.

Uma outra solução será constituída pelo conjunto $A_7^3$ com as definições:

$$(a,b,c) + (a',b',c') = (a + a', b + b', c + c')$$
$$(a,b,c) \cdot (a',b',c') = (aa'+4bc'+4b'c, ab'+a'b+4cc', ac'+a'c+bb')$$

*Mas todas as soluções serão isomorfas entre si.*

Os elementos com os quais são ampliados os corpos $A_p$, por processos análogos aos anteriormente indicados, chamam-se *imaginários de Galois*. Por processos semelhantes a estes é sempre possível ampliar um corpo K de modo que uma dada equação impossível em K passe a ter solução no novo corpo; este poderá ser sempre constituído por uma potência cartesiana de K, com definições adequadas de soma e de produto. É claro que, se K for finito, qualquer potência $K^n$, com $n \in \mathbb{N}$, será também um conjunto finito e, assim, o novo corpo será também finito *(campo de Galois)*.

## 26. Produtos de factores lineares; fórmula do binómio.

Consideremos *n* expressões

$$x+x_1, x+x_2, \ldots, x+x_n,$$

em que $x, x_1, \ldots, x_n$ são variáveis num *anel comutativo* A. É fácil ver que se tem:

$$(x+x_1)\ (x+x_2) = x^2 + (x_1 + x_2)\, x + x_1 x_2$$

Para desenvolver o produto $(x+x_1)\ (x+x_2)\ (x+x_3)$, bastará multiplicar o resultado anterior por $x+x_3$:

$$\begin{array}{r} x^2 + (x_1 + x_2)x + x_1x_2 \\ x + x_3 \\ \hline x^3 + (x_1 + x_2)x^2 + (x_1x_2)x \\ \qquad\qquad x_3x^2 + (x_1x_3 + x_2x_3)\, x + x_1x_2x_3 \\ \hline x^3 + (x_1 + x_2 + x_3)\, x^2 + (x_1x_2 + x_1x_3 + x_2x_3)\, x + x_1x_2x_3 \end{array}$$

Assim:

$$(x + x_1)\ (x + x_2)\ (x + x_3) = x^3 + S_1x^2 + S_2x + S_3$$

em que $S_1 = x_1 + x_2 + x_3$, $S_2 = x_1x_2 + x_1x_3 + x_2x_3$, $S_3 = x_1x_2x_3$

Analogamente, se obtém:

$$(x+x_1)\ (x+x_2)\ (x+x_3)\ (x+x_4) = x^4+S_1x^3+S_2x^2+S_3x+S_4$$

em que

$$S_1 = x_1+x_2+x_3+x_4$$
$$S_2 = x_1x_2+x_1x_3+x_1x_4+x_2x_3+x_2x_4+x_1x_4$$
$$S_3 = x_1x_2x_3+x_1x_2x_4+x_1x_3x_4+x_2x_3x_4$$
$$S_4 = x_1x_2x_3x_4$$

Somos, assim, levados a admitir, *por indução*, que se tem, para qualquer $n \in \mathbb{N}$:

$$(1) \quad (x+x_1)\ (x+x_2)\ldots(x+x_n)=x^n+S_1x^{n-1}+S_2x^{n-2}+\ldots+S_{n-1}x+S_n$$

em que $S_1$ é a soma das variáveis $x_1,x_2,\ldots,x_n$, $S_2$ a soma de todos os produtos distintos destas variáveis *duas a duas*, $S_3$ a soma de todos os produtos distintos destas variáveis *três a três*, e assim por diante, até $S_n$ que é $x_1x_2\ldots x_n$. A fórmula (1) escreve-se abreviadamente

$$(1') \qquad \prod_{k=1}^{n}(x+x_k) \quad = \quad \sum_{p=o}^{n} S_p x^{n-p}$$

onde $S_p$ é a soma dos produtos distintos das varáveis $x_1,x_2,\ldots x_n$ tomadas p a p (se $p=2,3,\ldots,n-1$); em particular

$$S_o=1, \quad S_1=\sum_{k=1}^{n} x_k \ , \quad S_n=\prod_{k=1}^{n} x_k$$

A fórmula (1) ou (1') pode ser demonstrada pelo MÉTODO DE INDUÇÃO MATEMÁTICA, de que trataremos no 7.º ano.

Visto que estes cálculos são referidos a um anel *comutativo* A, é fácil ver que *existe uma correspondência biunívoca entre os produtotos das variáveis* $x_1,x_2,\ldots,x_n$ *tomadas* p *a* p *e as combinações das mesmas variáveis* p *a* p. (*Porquê?*) Logo o número desses produtos é $\binom{n}{p}$.

Suponhamos, agora, que cada uma das variáveis é substituída por uma única variável *a* (no anel A). Então:

1) Cada um dos produtos dessas variáveis p a p tranforma-se em $a^p$.

2) $S_p$ transforma-se em $\binom{n}{p}a^p$.

3) $\prod_{k=1}^{n}(x+x_k)$ transforma-se em $(x+a)^n$.

É fácil ver que as conclusões 2) e 3) são válidas para todo o $p=0,1,\ldots,n$, e todo o $n \in \mathbb{N}$. Por conseguinte, de (1) vem

(2) $\quad (x+a)^n = x^n + nx^{n-1} + \binom{n}{2} a^2 x^{n-2} + \ldots + na^{n-1}x + a^n$

ou seja, em notação mais rigorosa, correspondente a (1'):

(2') $$\boxed{(x+a)^n = \sum_{k=o}^{n} \binom{n}{p} a^p x^{n-p}, \quad \forall\, n \in \mathbb{N}}$$

É claro que esta fórmula (habitualmente chamada FÓRMULA DO BINÓMIO ou FÓRMULA DE NEWTON) traduz uma *equivalência formal* entre os dois membros.

Das fórmulas (1) ou (1') é fácil deduzir, atendendo à regra dos sinais:

(3) $(x-x_1)(x-x_2)\ldots(x-x_n) = x^n - S_1 x^{n-1} + S_2 x^{n-2} - \ldots + (-1)^n S_n$,

ou seja, em notação mais precisa:

(3') $$\prod_{k=1}^{n} (x-x_k) = \sum_{p=o}^{n} (-1)^p S_p x^{n-p}$$

onde o símbolo $S_p$ mantém o significado anterior.

Daqui, por sua vez, deduz-se:

(4) $(x-a)^n = x^n - nax^{n-1} + \ldots + (-1)^p \binom{n}{p} a^p x^{n-p} \ldots + (-1)^n a^n$, ou, mais precisamente:

$$(x-a)_n = \sum_{p=o}^{n} (-1)^p \binom{n}{p} a^p x^{n-p}$$

Para exemplos e exercícios sobre a fórmula do binómio, ver *Compêndio de Álgebra, 7.º ano* (1).

---

(1) Ver nota da pág. 48.

27. **Decomposição dum polinómio em factores lineares; relações entre as raízes e os coeficientes do polinómio.** Consideremos um polinómio de grau $n > 0$:

$$a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n$$

Designemos este polinómio por $P(x)$ e suponhamos que $a_0$, $a_1,\ldots a_n$ *são números complexos quaisquer* (reais ou imaginários, com $a_0 \neq 0$). Segundo o teorema de D'Alembert (n.º 25) este polinómio tem, pelo menos, uma raiz em (C. Seja $x_1$ uma tal raiz; então $P(x)$ é divisível por $x-x_1$, isto é, existe um polinómio $P_1(x)$ de grau $n-1$, tal que

$$P(x)=(x-x_1)P_1(x)$$

Ora, se $n-1>0$, o polinómio $P_1(x)$ tem, pelo menos, uma raiz $x_2$ em (C *(porquê?)* e, portanto, existe um polinómio $P_2(x)$ de grau $n-2$ tal que

$$P_1(x) = (x-x_2)P_2(x), \text{ donde}$$
$$P(x)=(x-x_1)\,(x-x_2)P_2(x)$$

Raciocinando deste modo, sucessivamente, chega-se à conclusão de que existem números complexos, $x_1,x_2,\ldots,x_n$ tais que

$$P(x)=(x-x_1)\,(x-x_2)\ldots(x-x_n)P_n(x),$$

onde $P_n(x)$ é um polinómio de grau $n-n=0$. Mas, segundo a regra de Ruffini, o *coeficiente do primeiro termo dos sucessivos polinómios* $P_1(x),P_2(x),\ldots,P_n(x)$ *será sempre* $a_0$. *(Porquê?)* Logo, sendo $P_n(x)$ de grau 0, este polinómio reduz-se à constante $a_0$ e assim

(1) $$a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n = a_0(x-x_1)(x-x_2)\ldots(x-x_n)$$

ou seja, mais precisamente:

$$(1') \qquad \boxed{\sum_{p=0}^{n} a_p x^{n-p} = a_0 \prod_{k=1}^{n} (x - x_k)}$$

Assim, o teorema de D'Alembert conduz ao seguinte

TEOREMA: *Todo o polinómio de coeficientes no corpo* (C *admite uma decomposição em factores lineares, do tipo* (1) [*ou* (1')], *sendo* $a_0, x_1, x_2, \ldots, x_n$ *números complexos.*

É claro que, segundo o PRINCÍPIO DE DECOMPOSIÇÃO, $x_1, x_2, \ldots, x_n$ são as únicas raízes que o polinómio pode ter em (C. Alguma dessas raízes pode aparecer repetida na decomposição: chama-se *ordem de multiplicidade de uma raiz* o número $\mu$ de vezes que essa raiz figura na decomposição; a raiz diz-se *simples* se $\mu=1$, e *múltipla* se $\mu > 1$ (*dupla* se $\mu = 2$, *tripla* se $\mu = 3, \ldots$).

Notemos agora que, aplicando a fórmula (3') do número anterior, se deduz de (1'):

$$\sum_{p=o}^{n} a_p x^{n-p} = \sum_{p=o}^{n} (-1)^p a_o S_p x^{n-p}$$

Mais precisamente: *os dois membros desta igualdade representam o mesmo polinómio.* Portanto:

$a_p = (-1)^p a_o S_p$, donde:

$$(2) \qquad \boxed{S_p = (-1)^p \frac{a_p}{a_o}, \text{ para } p=1,2,\ldots,n}$$

*São estas as fórmulas que relacionam as raízes de polinómio* P(x) *com os seus coeficientes.* Em particular:

$$S_1 = x_1 + x_2 + \ldots + x_n = -\frac{a_1}{a_0}$$

$$S_n = x_1 x_2 \ldots x_n = (-1)^n \frac{a_n}{a_0}$$

Já tínhamos encontrado estas fórmulas no caso particular n=2 (equação do 2.º grau).

EXEMPLOS:

I. Seja o polinómio $3x^4-3x^2-6$. Para achar as suas raízes podemos recorrer a um truque muito simples que consiste em pôr $x^2=y$. Então o polinómio dado transforma-se no polinómio do 2.º grau $3y^2-3y-6$, cujas raízes são $y_1=2$, $y_2=-1$. Assim, é fácil ver que as raízes do polinómio dado são as raízes quadradas de 2 e de −1:

$$x_1 = \sqrt{2}, \quad x_2 = -\sqrt{2}, \quad x_3 = i, \quad x_4 = -i$$

Portanto:

(1) $$3x^4-3x^2-6 = 3(x-\sqrt{2})\,(x+\sqrt{2})\,(x-i)\,(x+i)$$

Diremos que os números $\sqrt{2}$, $-\sqrt{2}$, i, −i, são todos *raízes simples* do polinómio dado, porque cada um deles figura uma única vez na decomposição (1).

É fácil ver que neste $S_1=0$, $S_2=-1$, $S_3=0$, $S_4=-2$.

II Seja o polinómio $4x^4-8x^2+4$. Por um truque análogo ao anterior, este transforma-se no polinómio $4y^2-8y+4$, que admite a raiz dupla 1, isto é: $4y^2-8y+4=4(y-1)^2$. Então é fácil ver que

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

Diremos que 1 e −1 são *raízes duplas* do polinómio dado, porque cada uma delas figura duas vezes na decomposição. Neste caso, tem-se:

$$S_1 = S_3 = 0, \quad S_2 = -2, \quad S_4 = 1$$

III. Seja o polinómio $x^4-3x^3+3x^2-x$. É fácil ver que

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

Diremos, então, que 0 é uma raiz simples e 1 uma *raiz tripla* do polinómio: a primeira figura uma só vez e a segunda figura 3 vezes na decomposição. Neste caso, temos $S_1=3$, $S_2=3$, $S_3=1$, $S_4=0$.

28. **Princípios das identidades; factorização dum polinómio num corpo qualquer.** Consideremos, agora, um corpo K qualquer.

TEOREMA. *Um polinómio de grau* n *superior a zero não pode ter mais de* n *raízes diferentes em* K.

*Demonstração:*

Seja P(x) um polinómio relativo a K, de grau $n > 0$, e suponhamos que P(x) tem, pelo menos, *n* raízes diferentes, $x_1,\ldots,x_n$, em K. Então existe um polinómio $P_1(x)$ relativo a K, de grau n−1, tal que

$$P(x) = (x-x_1)P_1(x) \qquad \textit{(Porquê?)}$$

Ora, supondo $n > 1$, tem-se $P(x_2)=(x_2-x_1)P_1(x_2)=0$ (*porquê?*) e como $x_2 \neq x_1$, por hipótese, segue-se que $P_1(x_2) = 0$. (*Porquê?*) Logo, existe um polinómio $P_2(x)$ relativo a K, de grau n−2, tal que

$$P_1(x) = (x-x_2)P_2(x) \qquad \textit{(Porquê?)}$$

Raciocinando assim, sucessivamente, conclui-se, como no número anterior, que

$$P(x) = a_0(x-x_1)\,(x-x_2)\ldots(x-x_n),$$

em que $a_0$ é o coeficiente do termo de grau *n* em P(x).

Seja, agora, *c* um elemento de K diferente dos elementos $x_1,\ldots,x_n$. Então, como $a_0 \neq 0$ (*porquê?*) tem-se:

$$P(x) = a_0(c-x_1)\,(c-x_2)\ldots(c-x_n) \neq 0 \quad (\textit{Porquê?})$$

Por conseguinte, P(x) não pode ter em K mais do que *n* raízes distintas, $x_1, x_2, \ldots, x_n$

Daqui se deduz como corolário o seguinte

PRINCÍPIO DAS IDENTIDADES: *Se dois polinómios em* x, *relativos a* K, *de grau não superior a* m, *tomam o mesmo valor para mais de* m *valores da variável* x *em* K, *esses polinómios são idênticos (e, portanto, equivalentes).*

*Demonstração:*

Se A(x) e B(x) são dois polinómios de grau não superior a *m*, podemos escrevê-los sob a forma

$$A(x) = a_0x^m + a_1x^{m-1} + \ldots + a_{m-1}x + a_m.$$
$$B(x) = b_0x^m + b_1x^{m-1} + \ldots + b_{m-1}x + b_m.$$

sem ser necessariamente $a_0 \neq 0$, $b_0 \neq 0$. Suponhamos que estes polinómios tomam o mesmos valor para mais de *m* valores de x em K. Então, o polinómio

$$P(x) = (a_0 - b_0)x^m + (a_1 - b_1)x^{m-1} + \ldots + (a_m - b_m)$$

tem grau não superior a *m* e anula-se para mais de m valores de x em K. Ora, segundo o teorema, isto é impossível *se o grau do polinómio* P(x) *fosse* $>0$. Logo, o grau de P(x) é zero, isto é:

$$a_0 - b_0 = 0,\ a_1 - b_1 = 0,\ \ldots,\ a_{m-1} - b_{m-1} = 0,$$

e, sendo assim, também terá de ser $a_m - b_m = 0$, de contrário P(x) não se anularia para nenhum valor de x. Portanto $a_0 = b_0$, $a_1 = b_1$, ..., $a_m = b_m$, o que significa precisamente que os polinómios A(x) e B(x) são idênticos.

COROLÁRIO. *Se o corpo* K *é infinito, dois polinómios relativos a* K *que sejam equivalentes são necessariamente idênticos.*

Com efeito, sejam A(x) e B(x) dois polinómios relativos a K e suponhamos que K tem uma infinidade de elementos (por exemplo K=ℚ, K=ℝ ou K=ℂ). Então, se A(x) e B(x) são equivalentes, tomam o mesmo valor para uma infinidade de valores diferentes de x em K (*porquê?*) e, portanto, para um número de valores superior aos seus graus. Logo, segundo o PRINCÍPIO DAS IDENTIDADES, são idênticos.

*Note-se que este corolário não é válido se* K *é finito.* Por exemplo, em $A_5$ os polinómios

$$x^5 + \overline{2}x^3 - \overline{1} \quad \text{e} \quad \overline{2}x^3 + x - 1$$

são equivalentes (como se pode verificar) e, contudo, não são idênticos.

*Note-se, ainda, que os teoremas agora demonstrados são independentes do teorema de D'Alembert (que diz respeito só ao corpo* ℂ).

• Diz-se que um polinómio A(x) relativo a K é *completamente resolúvel em* K, quando admite uma decomposição em factores lineares em K, isto é, uma decomposição do tipo

$$P(x) = a_0 (x - x_1)(x - x_2) \ldots (x - x_n),$$

em que $a_0$ é o coeficiente do termo de grau *n* de P(x) e $x_1, x_2, \ldots, x_n$ são elementos de K, raízes de P(x). Nesta hipótese, pode acontecer, em particular, que alguma destas raízes apareça repetida (*raiz múltipla*), mas em qualquer caso é fácil reconhecer que o polinómio não admite

outras raízes em K. Também se prova que o número de vezes que cada raiz aparece numa tal decomposição (chamado *ordem de multiplicidade* da raiz) é determinado, isto é, não depende do modo como se chega à decomposição. Uma raiz diz-se *simples* se a sua ordem de multiplicidade é 1.

Finalmente, prova-se em matemática superior o seguinte teorema:

*Qualquer que seja o corpo* K, *é possível construir, para cada polinómio* P(x) *de coeficientes em* K, *um corpo* K,' *extensão de* K, *tal que* P(x) *seja completamente resolúvel em* K'. *Os corpos mínimos que verificam esta condição são todos isomorfos entre si.*

29. **Resolubilidade algébrica e resolução numérica de equações algébricas.** Vimos, atrás, que existem fórmulas resolventes para equações quadráticas e equações cúbicas, as quais permitem calcular todas as raízes da equação por meio de um certo número de operações — subtracções, multiplicações, divisões e *extracções de raiz* — efectuadas a partir dos coeficientes da equação (em corpos de característica diferente de 2 e de 3, em que a equação seja completamente resolúvel). Exprime-se este facto dizendo que *a equação geral do* 2.º *grau e a equação geral do* 3.º *grau são resolúveis algebricamente* (ou *resolúveis por meio de radicais*); e prova-se que *a equação geral do* 4.º *grau também é resolúvel algebricamente* (nos referidos corpos).

Em princípios do século passado, o matemático norueguês NIELS ABEL demonstrou que a equação geral do 5.º grau não é resolúvel algebricamente. Há, no entanto, tipos particulares de equações algébricas, mesmo de grau superior ao quinto, que são resolúveis algebricamente como, por exemplo, os seguintes:

(1) $ax^{2p} + bx^{p} + c = 0$

(2) $ax^{3p} + bx^{2p} + cx^{p} + d = 0$

(3) $ax^{4p} + bx^{3p} + cx^{2p} + dx^{p} + e = 0$

Com efeito, pondo $x^p = y$, a primeira reduz-se à equação do 2.º grau $ay^2+by+c=0$ e facilmente se reconhece que as suas soluções são dadas pela fórmula

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

Já no número anterior vimos exemplos de equações deste tipo, com p=2:

$ax^4+bx^2+c=0$ (chamam-se *equações biquadradas*)

Para as equações dos tipos (3) e (4) as considerações são análogas.

Surge, assim, o problema:

*Saber se um dado tipo de equações algébricas é ou não resolúvel por meio de radicais e achar a correspondente fórmula de resolução algébrica no caso afirmativo.*

A resolução deste problema encontra-se na difícil *teoria da resolubilidade algébrica de* GALOIS, a que já temos feito referência. São subprodutos importantíssimos desta teoria os conceitos de grupo e de corpo, que têm numerosas aplicações em vários ramos da matemática e da física.

Na prática, quando é dada uma equação algébrica de grau superior ao segundo, cujos coeficientes sejam números, prefere-se geralmente recorrer a certos métodos de aproximações excessivas que permitem calcular as raízes com o grau de aproximação que se desejar. Esses métodos são quase sempre muito trabalhosos quando não se dispõe de boas máquinas de calcular. Porém, um computador electrónico potente permite efectuar, com grande rapidez, os cálculos exigidos por esses métodos: por exemplo, as raízes duma equação do 6.º grau poderão ser então calculadas em média num minuto, com 12 algarismos exactos (partes reais e coeficientes de i no caso das raízes imaginárias).

Tais métodos, que se estudam em matemática superior, são chamados *métodos de resolução numérica* e fazem parte dum ramo da matemática moderna que tem tomado grande incremento com o uso dos computadores electrónicos: a ANÁLISE NUMÉRICA.

30. **Exemplo de um anel não comutativo (a álgebra dos quaterniões).** A álgebra dos quaterniões é um primeiro exemplo histórico de anel não comutativo, introduzido pelo grande matemático e físico irlandês HAMILTON, do século passado, que aplicou essa estrutura em várias questões de mecânica e de electromagnetismo. Consideremos o seguinte problema:

*Construir um anel* $\mathbb{H}$ *que verifique as seguintes condições:*

1) $\mathbb{H}$ *contém* $\mathbb{R}$, *e a adição e a multiplicação em* $\mathbb{H}$ *são extensões das operações homónimas em* $\mathbb{R}$.

2) *Existem três elementos* i, j, k *de* $\mathbb{H}$ *tais que:*

$$i^2=j^2=k^2=-1$$

$$ij=k,\ jk=i,\ ki=j$$

$$ji=-k,\ kj=-i,\ ik=-j$$

3) *Todo o elemento de* $\mathbb{H}$ *é da forma*

$$a+bi+cj+dk,\ \text{com}\ a,b,c,d \in \mathbb{R}$$

4) $a+bi+cj+dk=0 \Rightarrow a=b=c=d=0,\ \forall a,b,c,d, \in \mathbb{R}$.

Mais uma vez podemos seguir o MÉTODO DO PROBLEMA RESOLVIDO: suponhamos que existe um anel $\mathbb{H}$ nas referidas con-

dições. Então é fácil ver que, sendo a,b,c,d números reais quaisquer, se tem:

$$a+bi+cj+dk = a'+b'i+c'j+d'k, \text{ sse } a=a' \wedge b=b' \wedge c=c' \wedge d=d',$$

$$(a+bi+cj+dk)+(a'+b'i+c'j+d'k) = (a+a')+(b+b')i+(c+c')j+(d+d')k,$$

$$\begin{aligned}(a+bi+cj+dk)\ (a'+b'i+c'j+d'k) &= (aa'-bb'-cc'-dd') + \\ &+ (ab'+a'b+cd'-c'd)i + \\ &+ (ac'+a'c+b'd-bd')j + \\ &+ (ad'+a'd+bc'-b'c)k.\end{aligned}$$

Estes resultados indicam-nos uma solução para o problema, que pode ser constituída pelo conjunto $\mathbb{R}^4$ com as operações de adição e multiplicação assim definidas:

$$\begin{aligned}(a,b,c,d) + (a',b',c',d') &= (a+a', b+b', c+c', d+d') \\ (a,b,c,d) \cdot (a',b',c',d') &= (aa'-bb'-cc'-dd', ab'+a'b+cd'-c'd, \\ &\quad ac'+a'c+b'd-bd', ad'+a'd+bc'-b'c).\end{aligned}$$

Pode verificar-se que, com estas definições, $\mathbb{R}^4$ é realmente um anel que verifica as condições do problema, uma vez que se identifique cada número real *a* ao quaterno (a,0,0,0,) e se ponha, por exemplo, i=(0,1,0,0,), j=(0,0,1,0), k=(0,0,0,1). Podemos, pois, tomar $\mathbb{H}=\mathbb{R}^4$ com as referidas definições. Como os elementos de $\mathbb{R}^4$ são quaternos de números reais, os elementos de $\mathbb{H}$ receberam a designação de *quaterniões* (de *Hamilton*). Por sua vez, o anel $\mathbb{H}$ é chamado *álgebra dos quaterniões.*

*Para ver que este anel não é comutativo, basta notar que se tem, por exemplo,* $ij=k$, $ji=-k$, *e, portanto,* $ij \neq ji$; *de contrário seria* $k=0$, *o que não é verdade. Porquê?*

Por outro lado, como

$$(a+bi+cj+dk)\ (a-bi-cj-dk) = a^2+b^2+c^2+d^2,$$

vê-se que todo o quaternião a+bi+cj+dk diferente de zero é regular, sendo, então:

$$(a+bi+cj+dk)^{-1} = \frac{a-bi-cj-dk}{a^2+b^2+c^2+d^2}$$

Por conseguinte, IH é um anel de divisão (pág. 93). *Só lhe falta ser comutativo para ser um corpo* (1).

Finalmente, é fácil verificar que:

*A álgebra dos quaterniões contém três subcorpos isomorfos ao corpo* (C *constituídos, respectivamente, pelos quaterniões das formas:*

$$a+bi,\quad a+bj,\quad a+ck\quad ,\quad \text{com } a,b \in \mathbb{R}$$

Podemos, pois, identificar (C a um destes corpos, por exemplo ao primeiro, e dizer assim que *o anel* IH *contém* (C *como subcorpo.*

Vamos ver que existe uma infinidade de corpos não isomorfos entre si, que contêm (C como subcorpo.

31. **Corpos de funções racionais.** Para fixar ideias, vamos limitar o nosso estudo ao caso de funções racionais relativas ao corpo (C. Mas, as considerações que vão seguir-se continuam a ser válidas, substituindo (C por um corpo infinito qualquer (por exemplo (Q ou IR).

Comecemos por considerar a expressão

$$\frac{x-2}{x^2-4}$$

sendo x uma variável em (C. Essa fracção define uma função no con-

---

(1) Alguns autores chamam 'corpos' aos anéis de divisão e 'corpos comutativos' aos anéis de divisão comutativos (portanto aos corpos segundo a nossa terminologia).

junto dos números complexos que não anulam o denominador. Ora, as raízes de $x^2-4$ são 2 e $-2$, e uma destas — o número 2 — também anula o numerador. Assim, ambos os termos da fracção são divisíveis por $x-2$ e, portanto, virá:

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

*para todo o* $x \neq 2$ *e todo o* $x \neq -2$. (*Porquê?*)

Quer isto dizer que as duas fracções

$$\frac{x-2}{x^2-4} \quad \text{e} \quad \frac{1}{x+2}$$

são equivalentes no conjunto dos valores complexos de x diferentes de 2 e de $-2$. Nenhuma delas é definida para $x = -2$. *Porém, a segunda toma o valor* 1/4 *para* $x=2$, *enquanto a primeira não é aí definida.* Com efeito, a substituição de x por 2 nessa fracção conduz à expressão 0/0, a que chamaremos *'símbolo de indeterminação'*, visto que qualquer número x verifica a condição $0 \cdot x = 0$.

Vejamos um outro exemplo. Seja a expressão

$$\text{(1)} \qquad \frac{x^3-3x^2+4}{x^3-5x^2+8x-4}$$

Ambos os termos desta fracção se anulam para $x = 2$ e, portanto, ambos são divisíveis por $x-2$. Dividindo os dois termos por $x-2$ segundo a regra de Ruffini, obtém-se a fracção

$$\frac{x^2-x-2}{x^2-3x+2}$$

que é equivalente à primeira *no conjunto dos valores de* x *que não anulam o denominador da primeira. Porquê?* Mas os dois termos

da nova fracção ainda se anulam para $x = 2$; dividindo-os por $x-2$, obtém-se finalmente a fracção

$$\frac{x+1}{x-1} \tag{2}$$

O denominador desta tem como única raiz o número 1, que já não anula o numerador. Portanto, o domínio de existência desta expressão é o conjunto dos valores de x diferentes de 1. Para $x = 2$, a expressão (2) toma o valor 3, enquanto a expressão (1) assume a indeterminação 0/0. *No entanto, as duas expressões são equivalentes no conjunto dos valores de* x *diferentes de* 1 *e de* 2.

Vejamos um terceiro exemplo. Os dois termos da fracção

$$\frac{5x+15}{x^3+5x^2+3x-9} \tag{3}$$

anulam-se para $x = -3$. Dividindo-os por $x + 3$, obtém-se a fracção

$$\frac{5}{x^2+2x-3} \tag{4}$$

cujos termos já não se anulam simultaneamente para $x = -3$. No entanto, tal como a primeira, esta fracção continua a não ser definida para $x = -3$. Com efeito, substituindo x por $-3$, esta conduz à expressão 5/0 que não tem significado em (C, pois não existe nenhum número x tal que $0 \cdot x = 5$. As expressões do tipo a/0, em que a é um número $\neq 0$, são chamados *símbolos de impossibilidade* (visto que a divisão por 0 neste caso é impossível); veremos mais tarde como estes símbolos podem ser interpretados na teoria dos limites. Assim, em conclusão, vemos que as expressões (3) e (4) têm o mesmo domínio de existência, constituído pelos números diferentes de $-3$ e de 1, e são aí equivalentes, *definindo, portanto, a mesma função.*

Note-se que as três fracções a que chegámos

$$\frac{1}{x+1} \quad , \quad \frac{x+1}{x-1} \quad , \quad \frac{5}{x^2+2x-3}$$

já não podem simplificar-se mais, visto que os termos não têm raízes comuns: diremos, por isso, que são *irredutíveis*. Pois bem:

DEFINIÇÃO. *Chama-se função racional (relativa a* (C*) toda a função que possa ser representada por uma fracção do tipo*

$$\frac{a_0x^m + a_1x^{m-1} + \ldots + a_{m-1}x + a_m}{b_0x^n + b_1x^{n-1} + \ldots + b_{n-1}x + b_n}$$

*cujos termos sejam polinómios de coeficiente em* (C *sem raízes comuns (fracção irredutível)* (1).

É fácil reconhecer que, sendo $\frac{A(x)}{B(x)}$ $\frac{C(x)}{D(x)}$ duas fracções deste tipo, se tem, para todo o valor de x que não anule nenhum denominador:

I. $$\frac{A(x)}{B(x)} \pm \frac{C(x)}{D(x)} = \frac{A(x)D(x) \pm B(x)C(x)}{B(x)D(x)}$$

II. $$\frac{A(x)}{B(x)} \cdot \frac{C(x)}{D(x)} = \frac{A(x) \cdot C(x)}{B(x) \cdot D(x)}$$

III. $$\frac{A(x)}{B(x)} \,/\, \frac{C(x)}{D(x)} = \frac{A(x) \cdot D(x)}{B(x) \cdot C(x)} \quad [\text{com } C(x) \neq 0].$$

Pode acontecer, em particular, que os dois termos de alguma fracção do segundo membro tenham raízes comuns (*fracção redutível*). Porém, aplicando sucessivamente a regra de Ruffini tal como foi

---

(1) Está, portanto, automaticamente excluído o caso em que o denominador se reduz ao polinómio zero.

indicado nos exemplos anteriores, chega-se sempre a uma fracção irredutível.

Designaremos por (C(x) o *conjunto de todas as funções racionais de uma variável relativas* a (C. As considerações anteriores conduzem facilmente à seguinte conclusão:

TEOREMA. *O conjunto* (C(x) *constitui um corpo, relativamente às operações de adição e de multiplicação definidas pelas fórmulas* I *e* II, *supondo que os segundos membros são substituídos pelas fracções irredutíveis correspondentes, se acaso não forem já irredutíveis.*

Notemos, agora, que entre as fracções $A(x)/B(x)$, cujos termos são polinómios em x (de coeficientes em (C), figuram aquelas em que o polinómio denominador $B(x)$ se reduz a uma constante $k \neq 0$. Nesse caso, supondo $A(x) = \sum_0^n a_p x^{n-p}$, tem-se, evidentemente:

$$\frac{A(x)}{B(x)} \equiv \frac{a_0}{k} x^n + \frac{a_1}{k} x^{n-1} + \ldots + \frac{a_{n-1}}{k} x + \frac{a_n}{k}$$

e, portanto, a função definida pela fracção reduz-se a uma *função racional inteira,* pois que pode ser definida por um polinómio.

Assim, entre as funções racionais figuram as funções racionais inteiras, também chamadas *funções polinomiais.* As funções racionais que não são inteiras dizem-se *fraccionárias.*

Mas, segundo o corolário do PRINCÍPIO DAS IDENTIDADES, dois polinómios em x relativos a (C são idênticos, sse são equivalentes (isto é, sse definem a *mesma* função). *Portanto, existe uma correspondência biunívoca entre tais polinómios e as funções que eles representam.* Por outro lado, *a soma e o produto de dois polinómios* foram definidos de modo a representarem, precisamente, *a soma e o produto das funções definidas por esses polinómios.* Assim, em conclusão:

TEOREMA. *O anel* (C[x] *dos polinómios relativos a* (C *é isomorfo ao subanel do corpo* (C(x), *constituído pelas funções racionais inteiras.*

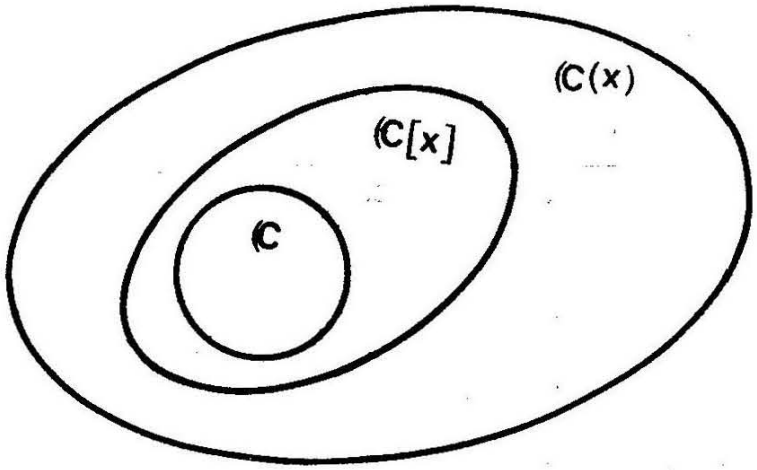
Podemos, com base neste teorema, identificar (C[x] ao referido anel das funções racionais inteiras, de modo que *ficará* (C[x] *a ser um subanel do corpo* (C(x). Como, por sua *vez*, o corpo (C é isomorfo ao subcorpo do anel (C[x] constituído pelos polinómios de grau zero, vemos que:

COROLÁRIO. *O corpo* (C(x) *pode ser considerado como uma extensão do corpo complexo.*

Temos, assim, duas sucessivas extensões de (C:

$$(C \subset (C[x] \subset (C(x)$$

sendo a primeira extensão o anel (C[x] dos polinómios e a segunda o corpo (C(x) das funções racionais.




Note-se que, em vez de funções racionais de uma só variável, podíamos considerar funções racionais de duas variáveis, três variáveis, etc., como, por exemplo, as que são representadas pelas expressões:

$$\frac{3}{x-y}\ ,\quad \frac{xy+xz+yz}{x^2+y^2+z^2}\ ,\quad \text{etc.}$$

Podemos, assim, definir uma infinidade de corpos, (C(x,y), (C(x,y,z), etc., *que são extensões de* (C *não isomorfas entre si.*

NOTA. Mesmo que dois polinómios A(x) e B(x) tenham raízes comuns, podemos falar da *função racional representada pela fracção* A(x)/B(x), como sendo a função definida pela fracção irredutível correspondente, desde que B(x) não seja o polinómio zero.

32. **Funções homográficas.** Consideremos a função $x \curvearrowright y$ em que:

(1) $$y = \frac{x+1}{x+2} \quad , \quad \text{sendo } (C \text{ o universo.}$$

Trata-se, como é fácil ver, de uma função racional fraccionária, que tem por domínio $\{ x : x \neq -2 \}$. Vamos limitar o seu estudo ao universo $\mathbb{R}$ (função real de variável real), com o fim de obter o seu gráfico. É fácil ver que

$$\frac{x+1}{x+2} = 1 - \frac{1}{x+2} \quad , \quad x \neq -2$$

e, portanto,

$$y = \frac{x+1}{x+2} \Leftrightarrow y - 1 = -\frac{1}{x+2}$$

Então, feita a substituição

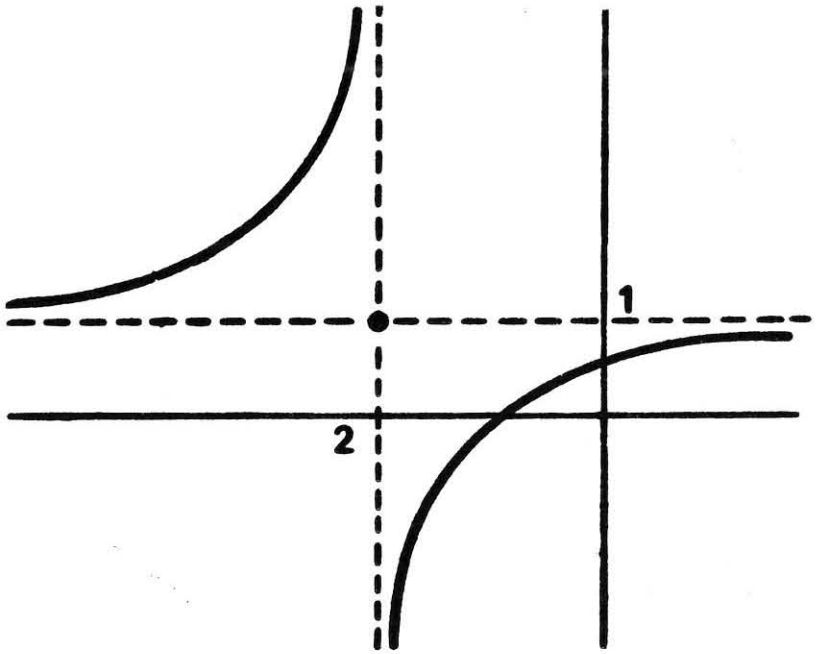
$$y - 1 = Y, \quad x + 2 = X$$

ou seja

$$y = Y + 1 \quad , \quad x = X - 2,$$

vê-se que se passa do gráfico da equação $Y = -1/X$ para o gráfico da equação (1), mediante uma translação que leva a origem para o ponto $(-2, 1)$. Ora, já sabemos que o gráfico da função $-1/X$ é uma hipérbole equilátera que tem por assímptotas os eixos coordenados.

Portanto, o gráfico da função dada é uma hipérbole equilátera que tem por assímptotas as rectas $x = -2$ e $y = 1$.




DEFINIÇÃO. *Chama-se função homográfica toda a função* $x \curvearrowright y$ *tal que*

$$y = \frac{ax + b}{cx + d} \tag{2}$$

*sendo* a, b, c, d *números complexos tais que* $ad - bc \neq 0$.

Dois casos há a distinguir nesta definição:

1.º *caso.* $c = 0$. Então, terá de ser $d \neq 0$; de contrário seria $ad - bc = 0$. Portanto:

$$\frac{ax + b}{cx + d} \equiv \frac{ax + b}{d} \equiv \frac{a}{d}\, x + \frac{b}{d}$$

Trata-se pois, neste caso, de *uma função linear,* cujo gráfico é uma recta, quando $a, b, c, d \in \mathbb{R}$ e x, y são variáveis reais.

2.º *caso.* $c \neq 0$. Então o denominador tem uma raiz, $x = -d/c$, e esta não anula o numerador, de contrário seria $-\frac{ad}{c} + b = 0$, o

que, multiplicando por $-c$, daria $ad - bc = 0$. Logo, a função não se reduz, neste caso, a uma função linear: é uma função fraccionária, a que chamaremos *'função homográfica não degenerada'*. É fácil verificar que se tem, neste caso:

$$\frac{ax+b}{cx+d} \equiv \frac{a}{c} - \frac{ad-bc}{cx+d}$$

e, portanto:

$$y = \frac{ax+b}{cx+d} \Leftrightarrow y - \frac{a}{c} = \frac{bc-ad}{cx+d}$$

Suponhamos, agora, que $a, b, c, d, \in \mathbb{R}$ e que $x, y$ são variáveis reais. As considerações anteriores mostram que, pondo:

$$\frac{a}{c} = k, \quad -\frac{d}{c} = h, \quad \frac{bc-ad}{c} = m,$$

$$y - k = Y, \quad x - h = X,$$

se passa do gráfico de $Y = m/X$ para o gráfico de (2) mediante uma translação, que leva a origem para o ponto $(h, k)$. Por conseguinte:

> *O gráfico da função homográfica não degenerada definida por* (2), *no caso real, é uma hipérbole equilátera que tem por assímptotas as rectas* $x = -\frac{d}{c}$ *e* $y = \frac{a}{c}$.

**33. Álgebras de Boole.** Consideremos o conjunto $\mathcal{L}$ dos valores lógicos V, F, com as operações de conjunção e disjunção. Já sabemos que a disjunção $a \vee b$ também se chama *soma lógica de* a *com* b e se representa por $a + b$; e que a conjunção $a \wedge b$ também se chama *produto lógico de* a *por* b e se representa por $a \cdot b$

ou ab. Porém, o termo ordenado $(\mathscr{L}, +, \cdot)$ não é um anel, porque o par ordenado $(\mathscr{L}, +)$ não é um grupo. (*Porquê?*) (1)

Consideremos, agora, o conjunto $\mathscr{C}$ de todos os subconjuntos dum universo U, com as operações de reunião e de intersecção. A reunião $A \cup B$ também se chama *soma lógica de* A *com* B e se representa por $A + B$; e a intersecção $A \cap B$ também se chama *produto lógico de* A *por* B e se representa por $A \cdot B$ ou AB. Mas o terno ordenado $(\mathscr{C}, +, \cdot)$ não é um anel porque o par ordenado $(\mathscr{C}, +)$ não é um grupo. (*Porquê?*)

No entanto, vimos que, tanto num caso como no outro, as operações consideradas têm um conjunto importante de propriedades.

DEFINIÇÃO. *Chama-se álgebra de Boole todo o terno ordenado constituído por um conjunto* A, *com mais de um elemento, e por duas operações, que podem chamar-se adição* (+) *e multiplicação* ( $\cdot$ ), *tais que:*

1) $(A, +)$ e $(A, \cdot)$ são *semigrupos comutativos,* com *elementos neutros,* respectivamente 0 e 1:

$$a + 0 = a, \quad a \cdot 1 = a, \quad \forall a \in A$$

2) A operação $\cdot$ é *distributiva em relação à operação* +, e vice-versa, isto é:

$$\left.\begin{array}{l} a \cdot (b+c) = (a \cdot b) + (a \cdot c) \\ a + (b \cdot c) = (a+b) \cdot (a+c) \end{array}\right\} \quad \forall a, b, c \in A$$

[Quando não haja perigo de confusão, a *primeira* destas fórmulas pode ser escrita, como no caso dos anéis, omitindo os parênteses do segundo membro: $a \cdot (b+c) = a \cdot b + a \cdot c$].

---

(1) Recordemos que o par $(\mathscr{L}, \cdot)$ também não é um grupo.

3) Para todo o elemento *a* de A, existe um e um só elemento x de A, tal que

$$a+x = 1 \wedge ax = 0 \ (^1)$$

Chamaremos *complementar de* a (ou *contrário de* a) e representaremos por ã (ler 'não *a*' ou '*a* til') o elemento x cuja existência e unicidade são postuladas em 3). Será, pois, por definição:

$$\tilde{a} = \iota_x \ (a+x = 1 \wedge ax = 0)$$

e, portanto:

$$a + \tilde{a} = 1 \wedge a \cdot \tilde{a} = 0, \quad \forall a \in A$$

Veremos nos exercícios que ã nunca é $-a$ nem $a^{-1}$.

Desde logo se reconhece que $(\mathscr{L}, +, \cdot)$ e $(\mathscr{C}, +, \cdot)$ são álgebras de Boole.

Daqui por diante, designaremos por A uma *álgebra de Boole qualquer.*

Notemos, desde já, que as condições 1), 2) e 3) da definição anterior (chamadas 'axiomas' ou 'postulados' da teoria das álgebras de Boole) são *simétricas relativamente às operações* + e ·, isto é, *convertem-se em proposições equivalentes quando se substitui* + *por* ·, *e vice-versa.* Daqui resulta o seguinte

PRINCÍPIO DE DUALIDADE: *Todo o teorema relativo a álgebras de Boole, enunciado em termos de adição* (+) *e/ou multiplicação* (·), *continua a ser verdadeiro, trocando entre si estas operações (e, portanto, os respectivos elementos neutros,* 0 *e* 1).

TEOREMA 1 (Propriedade da Idempotência). Tem-se:

I) $a + a = a$, II) $a \cdot a = a$, $\forall a \in A$

---

(1) Transcreva esta condição 3) em símbolos de lógica matemática.

*Demonstração. Provemos II):*

Visto que A é uma álgebra de Boole, tem-se (justifique as sucessivas passagens):

$$a = a \cdot 1 = a \cdot (a + \tilde{a}) = aa + a\tilde{a} = aa + 0 = aa,$$

donde: $a \cdot a = a$, $\forall\, a \in A$. Daqui, por sua vez, deduz-se I), aplicando o PRINCÍPIO DE DUALIDADE.

TEOREMA 2. *O elemento neutro da adição é elemento absorvente da multiplicação, e vice-versa, isto é, tem-se:*

$$\text{I)}\ \ a \cdot 0 = 0, \qquad \text{II)}\ \ a + 1 = 1, \qquad \forall\, a \in A$$

*Demonstração. Provemos I):*

Qualquer que seja $a \in A$, tem-se (prove as sucessivas passagens):

$$0 = a\,\tilde{a},\ \text{donde}\ a \cdot 0 = a(a\,\tilde{a}) = (aa)\,\tilde{a} = a\,\tilde{a} = 0$$

e, portanto, $a \cdot 0 = 0$, $\forall\, a \in A$. Daqui se deduz II), aplicando o PRINCÍPIO DE DUALIDADE.

TEOREMA 3. *O símbolo* $\sim$ *designa uma aplicação biunívoca* $a \curvearrowright \tilde{a}$ *do conjunto* A *sobre si mesmo, cuja inversa é a própria aplicação, isto é,*

$$\tilde{\tilde{a}} = a\ , \quad \forall\, a \in A$$

*Demonstração:*

Segundo a condição 3) da definição de 'álgebra de Boole', a cada elemento x de A corresponde *um e um só* elemento y de A tal que (1)

$$\text{(1)} \qquad x + y = 1 \wedge xy = 0$$

---

(1) É claro que estamos aqui aplicando ao axioma 3) o PRINCÍPIO DE SUBSTITUIÇÃO DE VARIÁVEIS APARENTES (pág. 71, 1.º tomo).

escrevendo-se, então: $y = \tilde{x}$. Fica, portanto, assim definida uma aplicação $x \curvearrowright y$ do conjunto A *em si mesmo*. Mas, pela mesma razão, a cada elemento y de A, corresponde *um e um só* elemento x de A tal que

$$y + x = 1 \wedge yx = 0,$$

o que equivale a (1) (*porquê?*), sendo $x = \tilde{y}$.

Em resumo:

$$x + y = 1 \wedge yx = 0 \Leftrightarrow y = \tilde{x} \Leftrightarrow x = \tilde{y}, \quad \forall x, y \in A$$

Ora, isto significa que a correspondência $x \curvearrowright \tilde{x}$ é uma aplicação biunívoca de A sobre si mesmo e que a inversa é a mesma aplicação, isto é: $\tilde{\tilde{x}} = x$, $\forall x \in A$.

DEFINIÇÃO. *Chama-se involução dum conjunto* M *toda a aplicação biunívoca* f *de* M *sobre si mesmo, tal que* $f^{-1} = f$, *isto é, tal que* $f^2 = I$.

Assim, o teorema 3 pode exprimir-se dizendo:

TEOREMA 3a. *O símbolo* $\sim$ *designa uma involução de* A.

Na definição deste operador, segundo a fórmula

$$a + \tilde{a} = 1 \wedge a\,\tilde{a} = 0,$$

vê-se imediatamente, atendendo à comutatividade da conjunção, que a troca de + com · e de 1 com 0 conduz a uma definição equivalente. Assim, concluímos:

PRINCÍPIO DE DUALIDADE (2.ª FORMA). *Todo o teorema relativo a uma álgebra de Boole* A, *em termos de adição* (+), *multiplicação* (·) *e/ou complementação* ($\sim$), *continua a ser verdadeiro, trocando entre si as duas primeiras operações (e, portanto, os respectivos elementos neutros) e mantendo a terceira operação.*

Por outro lado:

TEOREMA 4 (1.as Leis de De Morgan). Tem-se:

I) $\widetilde{a+b} = \tilde{a} \cdot \tilde{b}$ , II) $\widetilde{a \cdot b} = \tilde{a} + \tilde{b}$ , $\forall a, b \in A$

*Demonstração. Provemos I):*

Tem-se primeiro (justifique):

$$(a+b)(\tilde{a}\tilde{b}) = a(\tilde{a}\tilde{b}) + b(\tilde{a}\tilde{b}) = (a\tilde{a})\tilde{b} + (b\tilde{b})\tilde{a} = 0 \cdot \tilde{b} + 0 \cdot \tilde{a} = 0+0=0$$

Tem-se, por outro lado (justifique) (1):

$$(a+b) + (\tilde{a} \cdot \tilde{b}) = [(a+b) + \tilde{a}] \cdot [(a+b) + \tilde{b}] = [(a+\tilde{a})+b] \cdot [a+(b+\tilde{b})]$$
$$= (1+b)(a+1) = 1 \cdot 1 = 1$$

Por conseguinte:

$$(a+b) + (\tilde{a}\tilde{b}) = 1 \wedge (a+b) \cdot (\tilde{a}\tilde{b}) = 0 \quad , \quad \forall a, b \in A,$$

o que significa que $\tilde{a}\,b = \widetilde{a+b}$, $\forall a, b \in A$.

Daqui, por sua vez, deduz-se $\tilde{a} + b = \widetilde{a\,b}$, $\forall a, b \in A$, aplicando o PRINCÍPIO DE DUALIDADE (2.ª FORMA).

ESCÓLIO. *A conjunção dos teoremas* 3 *e* 4 *pode enunciar-se dizendo que o operador* $\sim$ *é, ao mesmo tempo, um isomorfismo do semigrupo* (A, +) *sobre o semigrupo* (A, •) *e deste sobre aquele. Poderíamos também dizer que é um isomorfismo da álgebra de Boole* (A, +, •) *sobre a álgebra de Boole* (A, •, +) *(chamado 'anti-automorfismo' destas álgebras de Boole).*

---

(1) É claro que estamos aqui aplicando ao axioma 3) o PRINCÍPIO DE SUBSTITUIÇÃO DE VARIÁVEIS APARENTES (pág. 71, 1.º tomo).

NOTA. Muitas vezes as duas operações binárias de uma álgebra de Boole são designadas pelos símoblos $\wedge$ e $\vee$ (ou vice-versa) e o complementar dum elemento *a* também é designado por uma das notações $\sim a$, $a'$, $\bar{a}$ ou $a^c$. Todavia, em várias aplicações das álgebras de Boole, nomeadamente a circuitos eléctricos, as notações aditiva e multiplicativa são as mais cómodas.

Já no capítulo I vimos como a teoria das álgebras de Boole se aplica a circuitos eléctricos. Neste caso, trata-se normalmente duma álgebra de Boole com dois elementos, que são precisamente 0 (elemento neutro da adição) e 1 (elemento neutro da multilpicação), sendo o primeiro interpretado como *ausência de corrente* e o segundo como *passagem de corrente*.

Os problemas que geralmente se põem nestas aplicações das álgebras de Boole são *problemas de minimização de circuitos,* de que já falámos no Cap. I, pág. 29, 1.º tomo. Tais problemas surgem não só a propósito de computadores, mas ainda em vários outros tipos de projectos de engenharia electrotécnica (p. ex. a propósito de instalações de ascensores, de redes telefónicas ou de distribuição de energia eléctrica, etc.). Há hoje técnicos — chamados 'TÉCNICOS DE AUTOMAÇÃO' — que se especializam precisamente neste género de problemas.

Uma das mais curiosas aplicações da álgebra de Boole está na possibilidade de reduzir raciocínios dedutivos a cálculos algébricos, executáveis por meio de máquinas. Está assim finalmente realizada, nas suas devidas proporções, uma ideia concebida, há três séculos, pelo grande matemático e filósofo Leibnitz.

Como vimos, o protótipo do silogismo aristotélico é baseado na propriedade transitiva da relação de inclusão entre conjuntos:

$$A \subset B \wedge B \subset C \Rightarrow A \subset C$$

Ora, a relação de inclusão pode ser definida em termos de 'produto lógico' ou de 'soma lógica'. Por exemplo, tem-se *(prove)*:

$$(1) \qquad A \subset B \Leftrightarrow AB = A \ , \ A \subset B \Leftrightarrow A\tilde{B} = 0$$

Utilizando a segunda fórmula, a propriedade transitiva da indução assume o aspecto

$$A\,\tilde{B} = 0 \wedge B\,\tilde{C} = 0 \Rightarrow A\,\tilde{C} = 0,$$

propriedade esta que pode ser deduzida dos axiomas das álgebras de Boole (1). *Ora, como se vê, a conclusão* $A\tilde{C} = 0$ *deduz-se das premissas* $A\tilde{B} = 0$, $B\tilde{C} = 0$, *multiplicando estas equações ordenadamente, o que dá*

$$A\,\tilde{B} \cdot B\,\tilde{C} = 0,$$

*e suprimindo em seguida os factores complementares* $\tilde{B}$ *e* B. *É claro que esta regra prática se pode estender a qualquer número de premissas, e inclui, como casos particulares, os tipos clássicos de silogismos da lógica aristotélica.*

Vamos dar um exemplo recreativo apresentado pelo matemático e escritor inglês LEWIS CARROL, do século passado, autor da obra célebre 'Alice no País das Maravilhas' e dum livro sobre Lógica Simbólica (2). Consideremos os seguintes conjuntos:

R = { homens que vão a uma recepção }
P = { homens que se penteiam bem }
A = { homens que cuidam do seu aspecto }
D = { homens desmazelados }
F = { fumadores de ópio }
L = { homens que usam luvas brancas }
S = { homens que são senhores de si }

---

(1) É mais fácil deduzi-la, provando primeiro que $A\tilde{B} = 0 \Leftrightarrow AB = A$ e, em seguida que $AB = A \wedge BC = B \Rightarrow AC = A$.

(2) LEWIS CARROL (pseudónimo de 'DODGSON') ensinou na Universidade de Oxford. Teve um excepcional talento em combinar a ciência com o sentido do humor.

Posto isto, L. CARROL apresenta as seguintes premissas:

1. *Nenhum homem vai a uma recepção sem se pentear bem:* $R\tilde{P} = 0$ (isto é, 'ir a uma recepção *e* não se pentear bem é impossível' ou 'ir a uma recepção implica pentear-se bem').

2. *Nenhum homem desmazelado cuida do seu aspecto:* $D\,A = 0$.

3. *Os fumadores de ópio não são senhores de si:* $F\,S = 0$.

4. *Todo o homem que se penteia bem cuida do seu aspecto:* $P\,\tilde{A} = 0$.

5. *Nenhum homem usa luvas brancas, a não ser quando vai a uma recepção:* $L\,\tilde{R} = 0$.

6. *Quando um homem não é senhor de si, torna-se desmazelado:* $\tilde{S}\,\tilde{D} = 0$.

Multiplicando os primeiros membros das equações 3, 6, 2, 4, 1, 5, tem-se a expressão:

$$F\,S \cdot \tilde{S}\,\tilde{D} \cdot D\,A \cdot \tilde{A}\,P \cdot \tilde{P}\,R \cdot \tilde{R}\,L$$

Eliminando em seguida dois a dois os termos complementares, segundo a regra prática anterior , obtém-se:

CONCLUSÃO: $F\,L = 0$ *(Nenhum fumador de ópio usa luvas brancas).*

EXERCÍCIOS:

I. Prove que se tem $\tilde{0} = 1$, $\tilde{1} = 0$ e $0 \neq 1$, em qualquer álgebra de Boole.

II. Prove que, em qualquer álgebra de Boole, o único elemento com simétrico é 0 e o único elemento com inverso é 1. (Sugestão: $a + x = 0 \Rightarrow a \cdot a + a \cdot x = 0$.)

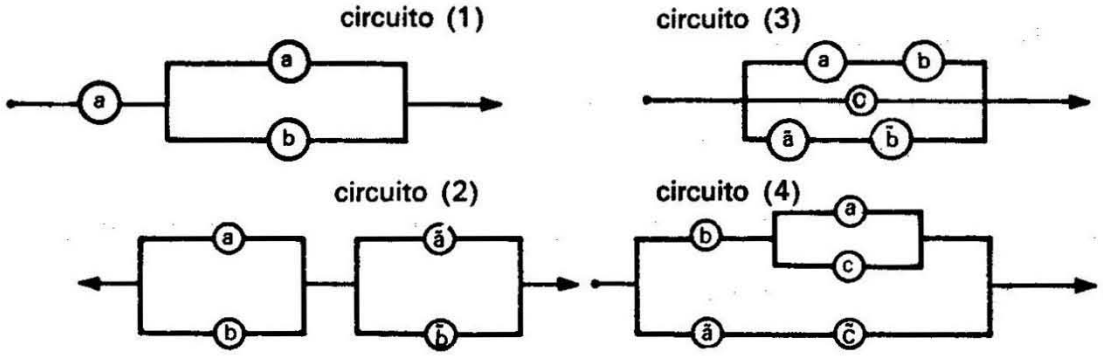
III. Prove que, em qualquer álgebra de Boole, ã nunca é $-a$ nem $a^{-1}$.

IV. Prove que, sendo A uma álgebra de Boole, se tem:

$$ab = a \Leftrightarrow a + b = b \Leftrightarrow a\tilde{b} = 0 \quad , \quad \forall\, a, b \in A$$

(Escreve-se, neste caso, por definição: $a \subset b$).

V. Determine polinómios de Boole para cada um dos seguintes circuitos, em que os círculos indicam comutadores e cada uma das variáveis *a*, *b*, *c* pode tomar o valor 0 (abrir o comutador) ou o valor 1 (fechar o comutador), tendo-se $\tilde{0} = 1$ e $\tilde{1} = 0$:

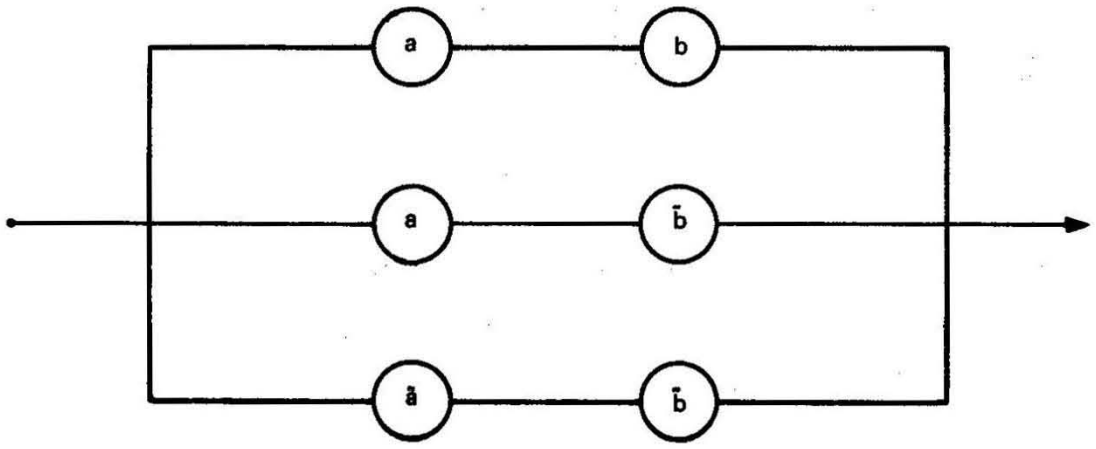



VI. Indicar um circuito para cada polinómio de Boole:

(1) $a + bc$ (3) $(a+b)(c+d)$ (5) $(a+b)(\tilde{a}+\tilde{b}c)$

(2) $a(b+c)$ (4) $ab + cd$ (6) $(ab+c)(d+\tilde{a}b)$

VII. Dado o circuito indicado no diagrama junto, indique um circuito mais simples que lhe seja equivalente.



VIII. As instruções relativas a certa apólice de seguros precisam que esta só pode ser passada a pessoas que satisfaçam uma, pelo menos, das seguintes condições: *a*) possuir a apólice n.º 19, e ser casado e do sexo masculino; b) possuir a apólice n.º 14, e ser casado e menor de 25 anos; c) não possuir a apólice n.º 19, e ser do sexo feminino; d) ser do sexo masculino e menor de 25 anos; e) ser casado e não menor de 25 anos. Pondo:

P = possibilidade de ter a apólice em questão;
A = ter a apólice n.º 19;
B = ser casado;
C = ser do sexo masculino;
D = ser menor de 25 anos,

exprima P como função booleana de A, B, C, D e indique um circuito *mínimo* que dê essa função.

IX. Sejam M o conjunto dos mamíferos, L o conjunto dos animais alados, A o conjunto das aves, P o conjunto dos animais com penas e B o conjunto dos bípedes. Tire conclusões das seguintes premissas:

1. Nenhum mamífero alado tem penas.
2. Todos os animais com penas são alados.
3. Todo o bípede é ave ou mamífero.
4. Nenhum mamífero é ave.

X. Transcreva, simbolicamente, a seguinte frase:

*'Para poder fumar nesta casa é necessário e suficiente que se verifiquem as três seguintes condições:* 1) *haver fósforos ou isqueiro utilizáveis;* 2) *haver cigarros ou charutos ou então cachimbo e tabaco;* 3) *não haver atmosfera deflagrante',*

usando as seguintes notações:

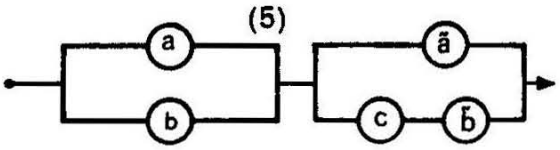
P = possibilidade de fumar nesta casa,
F = haver fósforos utilizáveis,
I = haver isqueiro utilizável,
$C_1$ = haver cigarros,
$C_2$ = haver charutos,
$C_3$ = haver cachimbo,
T = haver tabaco,
D = haver atmosfera deflagrante.

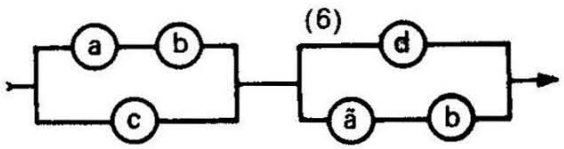
Trace o diagrama de um circuito que dê P como função das restantes variáveis, *utilizando, neste caso, circuitos elementares de conjunção, disjunção e negação, como os que foram considerados no Capítulo I.*

## RESPOSTAS

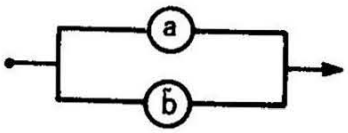
V. (3) $ab+\tilde{a}\,\tilde{b}+c$, (4) $b(a+c)+\tilde{a}\,\tilde{c}$

VI.




VII. $a\tilde{b}+a\tilde{b}+\tilde{a}\tilde{b} \equiv a+\tilde{b}$

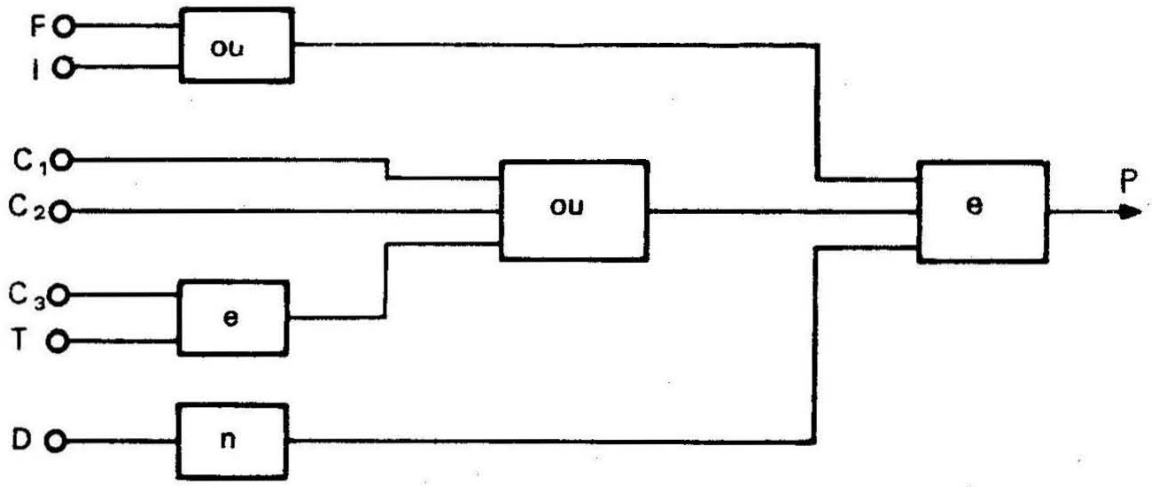



VIII. $P = ABC + ABD + \tilde{A}B\tilde{C} + CD + B\tilde{D}$

Note que $ABD+B\tilde{D}=AB+B\tilde{\tilde{D}}\supset ABC$, donde $P=AB+\tilde{A}B\tilde{C}+CD+B\tilde{D}$. Por outro lado $AB+\tilde{A}B\tilde{C}=AB+B\tilde{C}$, donde $P=AB+B\tilde{C}+CD+B\tilde{D}$. Ora $B\tilde{C}+CD=BD+CD$ e $BD+B\tilde{D}=B\supset AB$. Portanto $P=B+CD$.

IX. $MP=0$ (Nenhum mamífero tem penas), $(BP)M=0$ (Nenhum bípede com penas é mamífero), $(BP)\tilde{A}=0$ (Todo o bípede com penas é ave), etc.

X. $P = (F + I) \cdot (C_1 + C_2 + C_3T) \cdot \tilde{\tilde{D}}$



# Índice

*Págs.*

Composto e impresso na
*Tipografia Guerra — Viseu*
e concluiu-se
em Março de 1975

GABINETE DE ESTUDOS E PLANEAMENTO
DO MINISTÉRIO DA EDUCAÇÃO E CULTURA