J. SEBASTIÃO E SILVA

COMPÊNDIO DE MATEMÁTICA

1.º volume

2.º tomo

Curso Complementar
do Ensino Secundário

Edição GEP

LISBOA

COMPÊNDIO DE MATEMÁTICA

J. SEBASTIÃO E SILVA

COMPÊNDIO DE MATEMÁTICA

1.º VOLUME

(2.º TOMO)

CURSO COMPLEMENTAR
DO ENSINO SECUNDÁRIO

1 9 7 5

GABINETE DE ESTUDOS E PLANEAMENTO
DO
MINISTÉRIO DA EDUCAÇÃO E CULTURA

Av. Miguel Bombarda, 20 — Lisboa

CAPÍTULO V

OPERAÇÕES BINÁRIAS. GRUPÓIDES

1. **Expressões designatórias e operações.** Consideremos a expressão designatória $x - y$ no universo IN. Neste caso, o valor da expressão só existe quando os valores de x e y verificam a condição $x > y$. Diremos, por isso, que o *domínio de existência* da expressão $x - y$, no universo IN, é o conjunto de pares ordenados (relação binária):

$$D = \{ (x , y): \ x > y \ \wedge \ x , y \in \mathbb{N} \}$$

Assim, para cada par ordenado (x,y) pertencente a D, o valor de $x - y$ é um determinado elemento de IN; para cada par ordenado (x,y) não pertencente a D, *não existe valor de* $x - y$ no universo considerado. Exprime-se este facto dizendo que a referida expressão define uma *operação binária* (ou uma *função de duas variáveis*), cujo *domínio* é o conjunto D e cujos *resultados* (ou *valores*) pertencem a IN. Como se sabe, esta operação é chamada subtracção (em IN); podemos designá-la pelo sinal $-$.

Um outro exemplo em IN é-nos dado pela expressão designatória m.d.c. (x , y), abreviatura de

'máximo divisor comum de x *e* y'

Neste caso, a expressão define também uma *operação binária* (ou uma função de duas variáveis), cujo *domínio* é $\mathbb{N}^2$ e cujos *resultados* (ou *valores*) pertencem a $\mathbb{N}$.

Vejamos, agora, dois exemplos relativos à geometria de Euclides. Seja $\mathcal{E}$ o conjunto dos pontos (isto é, o espaço), $\mathcal{R}$ o conjunto das rectas e $\mathcal{P}$ o conjunto dos planos. Consideremos, então, as duas expressões designatórias:

'recta que passa por M *e* N'

'plano que passa por M *e é perpendicular a* r'

em que as letras M, N são variáveis em $\mathcal{E}$ e a letra r é uma variável em $\mathcal{R}$ (também se diz, por abuso de linguagem, que M, N designam dois *pontos variáveis* e r designa uma *recta variável*).

A primeira expressão só toma um valor determinado, quando $M \neq N$: o seu domínio de existência é, pois, o conjunto $\mathcal{D} = \{ (M, N);\ M \neq N \}$. Para cada par $(M,N) \in \mathcal{D}$ o valor da expressão é uma determinada recta, isto é, um elemento de $\mathcal{R}$. Diremos, assim, que a expressão define uma *operação binária* (ou uma *função de duas variáveis*), cujo *domínio* é $\mathcal{D}$ e cujos *resultados* (ou *valores*) pertencem a $\mathcal{R}$.

A segunda expressão toma um valor determinado, pertencente a $\mathcal{P}$, para todo o par (M,r), tal que $M \in \mathcal{E}$ e $r \in \mathcal{R}$. Diremos, assim, que tal expressão define uma *operação binária* (ou uma *função de duas variáveis*), cujo domínio é o conjunto $\mathcal{E} \times \mathcal{R}$ e cujos *resultados* (ou *valores*) pertencem a $\mathcal{P}$.

Muitos outros exemplos poderíamos apresentar de operações binárias (sobre valores lógicos, sobre conjuntos, sobre números, sobre funções, etc.).

Dum modo geral, chama-se *operação binária* (ou *função de duas variáveis*) toda a aplicação f dum conjunto D de pares ordenados num conjunto C qualquer. O conjunto D chama-se *domínio de* f. Assim, a cada par $(x,y) \in D$, a operação f faz corresponder um *e*

um só elemento de C, que pode ser designado por qualquer das notações

$$f(x,y) \quad , \quad x\,f\,y$$

e se chama *valor da função* f correspondente ao par (x,y) ou *resultado da operação* f efectuada sobre os elementos x, y dados.

O domínio duma operação binária f apresenta-se geralmente como subconjunto dum produto cartesiano $A \times B$ (ver exemplos anteriores). Em particular pode ser $A = B$; diz-se, então, que f é uma *operação sobre elementos de* A.

Em vez de expressões designatórias com 2 variáveis, podemos considerar expressões designatórias com 3 variáveis, com 4 variáveis, etc., que nos conduzem, de modo análogo, aos conceitos de *operação ternária* (ou *função de* 3 *variáveis*), de *operação quaternária* (ou *função de* 4 *variáveis*), etc. Por exemplo, no universo IR, a expressão designatória $\sqrt{x^2 + y^2 + 2xz}$ define uma *função de três variáveis* (ou uma *operação ternária*), cujo domínio é o subconjunto de $\mathbb{R}^3$

$$\{(x,y,z):\ x^2 + y^2 + 2xz \geqslant 0\}$$

Neste quadro, é natural chamar *funções de uma variável* (ou *operações unárias*) às aplicações, tais como foram definidas no capítulo anterior (1.º tomo).

Finalmente, há situações que conduzem naturalmente a falar de 'funções plurívocas' ou de 'operações plurívocas'. Tornemos, por exemplo, ao caso anterior da geometria euclidiana e consideremos a expressão

'plano que passa por M *e é paralelo a* r'

Tal expressão é *indeterminada* (ou *plurívoca*), para cada par (M,r), visto que, por um ponto M, passa uma infinidade de planos paralelos

a uma recta r. É, então, natural dizer que tal expressão representa uma *operação plurívoca*.

Outro exemplo: seja f uma função qualquer de uma variável e A um conjunto que contenha estritamente o domínio de f. Neste caso, a expressão

'extensão de f *a* A'

representa, como sabemos, uma *operação plurívoca*. Pelo contrário, a operação de restrição é *unívoca,* como vimos.

Esta terminologia impõe-se, portanto, na prática. Porém, como as operações mais frequentes e que mais interessam são unívocas, convém, uma vez por todas, convencionar que, *ao falar de 'operação' (ou 'função') fica subentendido que se trata de 'operação unívoca' (ou 'função unívoca').*

2. **Os conceitos de restrição e extensão para funções de mais de uma variável.** Estes conceitos podem ser definidos exactamente como no caso duma só variável. Bastará que nos limitemos a um exemplo. Consideremos, novamente, a expressão designatória $x - y$. Já vimos que, no universo $\mathbb{N}$, esta expressão define uma operação cujo domínio é o conjunto

$$D = \{ (x,y): \quad x > y \quad \wedge \quad x,y \in \mathbb{N} \}$$

e cujos resultados pertencem a $\mathbb{N}$. Porém, se passarmos ao universo $\mathbb{R}$, a mesma expressão define uma operação que é sempre possível neste universo; portanto, o domínio da operação é, agora, $\mathbb{R}^2$ e os seus resultados pertencem a $\mathbb{R}$. É claro que as duas operações (em $\mathbb{N}$ e em $\mathbb{R}$) são *distintas,* visto que não têm o mesmo domínio; *mas, quando aplicadas a qualquer par* (x,y) *do primeiro domínio,* D, *dão sempre o mesmo resultado.* Por conseguinte, a segunda é *uma extensão da primeira a* $\mathbb{R}^2$ e a primeira é

a restrição da segunda a D. (O que se pode dizer quanto à restrição da segunda a $\mathbb{N}^2$?)

Porém, na prática, não há, em regra, inconveniente em dar às duas operações o mesmo nome ('subtracção') e designá-las pelo mesmo símbolo ('−').

3. **Operações binárias de domínio finito.** Quando o domínio duma operação binária é finito, podemos sempre defini-la por meio duma tabela em que se indique o resultado da operação f para cada par (x,y) pertencente ao seu domínio. Neste caso, pode recorrer-se a *tabelas de duas entradas*. Seja, por exemplo, a operação f sobre os números 1, 2, 3, definida pela seguinte tabela:

x f y

x \ y	1	2	3
1			
2	1		
3	2	1	

Tem-se, neste caso, $2\,f\,1 = 2-1 = 1$, $3\,f\,1 = 3-1 = 2$, $3\,f\,2 = 3-2 = 1$. As casas em branco indicam que *não existe* resultado de operação para os pares correspondentes a essas casas. Trata-se, como se vê, duma restrição da subtracção.

Seja, agora, a operação φ definida pela tabela seguinte:

$\varphi\ (x, y)$

x \ y	Lisboa	Porto	Coimbra
Lisboa	0 km	321 km	204 km
Porto	321 km	0 km	117 km
Coimbra	204 km	117 km	0 km

Tem-se, por exemplo:

$$\varphi(\text{Porto, Coimbra}) = \varphi(\text{Coimbra, Porto}) = 117 \text{ km}$$

Também podíamos escrever:

$$\text{Porto } \varphi \text{ Coimbra} = 117 \text{ km}$$

Neste caso, o domínio da operação é o quadrado cartesiano do conjunto { Lisboa, Porto, Coimbra } e os resultados da operação (ou valores da função) são *distâncias*.

4. **Grupóides.** Designemos por A o conjunto

{ Lisboa, Porto, Coimbra }

e consideremos a operação θ definida pela tabela

$x\ \theta\ y$

x \ y	Lisboa	Porto	Coimbra
Lisboa	Lisboa	Coimbra	Porto
Porto	Coimbra	Porto	Lisboa
Coimbra	Porto	Lisboa	Coimbra

Como se vê, esta operação θ faz corresponder, a cada par ordenado de elementos de A, um (e só um) elemento do *mesmo conjunto* A: é, pois, uma aplicação de A^2 em A. Exprime-se este facto dizendo que *o conjunto* A *é um grupóide, relativamente à operação* θ.

Dum modo geral, diz-se que um conjunto A qualquer é um *grupóide relativamente a uma operação* θ, sse θ é uma aplicação de A^2 em A. Chama-se aqui *grupóide* precisamente ao par ordenado (A, θ) e *suporte do grupóide* ao conjunto A. Mas, muitas vezes, quando está subentendida a operação de que se trata, identifica-se o grupóide (A, θ) com o seu suporte A.

OUTROS EXEMPLOS:

1. Nos exemplos do número anterior, o conjunto $\{1, 2, 3\}$ não é um grupóide relativamente à operação f e o conjunto { Lisboa, Porto, Coimbra } não é um grupóide relativamente à operação φ. Porquê?

2. O conjunto $\mathbb{N}$ é um grupóide relativamente à adição e também relativamente à multiplicação; mas não relativamente à subtracção nem à divisão. Porquê? Chama-se *grupóide aditivo* $\mathbb{N}$ o grupóide $(\mathbb{N}, +)$ e *grupóide multiplicativo* $\mathbb{N}$ o grupóide $(\mathbb{N}, \times)$.

3. O conjunto Z (dos números inteiros relativos) é um grupóide relativamente à subtracção, mas não relativamente à divisão. Idem para o conjunto $\mathbb{R}$. Porquê?

Mais exemplos serão estudados no n.º 6.

5. **Conceito de subgrupóide.** Seja M_2 o conjunto dos números pares positivos (subconjunto de $\mathbb{N}$). *A soma de dois números pares é sempre um número par; isto é, simbolicamente:*

$$x, y \in M_2 \Rightarrow x + y \in M_2$$

Exprime-se este facto dizendo que o conjunto M_2 é *fechado para a adição*. Mas já a soma de dois números ímpares não é um número ímpar: o conjunto dos números ímpares (positivos) *não é fechado para a adição;* é, porém, *fechado para a multiplicação. (Porquê?)*

• Consideremos agora, dum modo geral, um grupóide (A, θ):

DEFINIÇÃO. *Diz-se que um subconjunto* C *de* A *é fechado para* θ, *sse esta operação, efectuada sobre qualquer par de elementos de* C, *dá sempre como resultado um elemento de* C, *isto é, sse a condição seguinte é verificada:*

$$x, y \in C \Rightarrow x \theta y \in C$$

É claro que isto equivale a dizer que o conjunto C é um grupóide relativamente à operação θ restringida a C^2. Diz-se então que o conjunto C, com esta operação, é um *subgrupóide* de (A, θ).

Assim, o conjunto M_2 forma um subgrupóide do grupóide aditivo IN (e também do grupóide multiplicativo IN), enquanto o conjunto $IN \setminus M_2$ forma um subgrupóide do grupóide multiplicativo IN, mas não do grupóide aditivo IN.

EXERCÍCIOS:

I. Determinar os subgrupóides do grupóide considerado no exemplo inicial do número anterior.

II. Determinar os subgrupóides do grupóide aditivo IN. Idem para *Z*.

6. **Grupóides comutativos e grupóides associativos (ou semigrupos).** Consideremos um grupóide (A, θ). Diz-se que a operação θ é *comutativa,* sse

$$x \theta y = y \theta x, \quad \forall \quad x, y \in A$$

Diz-se que a operação θ é *associativa*, sse

$$(x \theta y) \theta z = x \theta (y \theta z), \quad \forall x, y, z \in A$$

No primeiro caso também se diz que o *grupóide é comutativo*. No segundo caso também se diz que o *grupóide é associativo* ou que é um *semigrupo* (assim, o termo 'semigrupo' é sinónimo de 'grupóide associativo').

EXEMPLOS E EXERCÍCIOS:

I. O grupóide considerado no exemplo inicial do n.º 4 é comutativo, *mas não associativo*. Por exemplo:

$$(\text{Lisboa } \theta \text{ Porto}) \theta \text{ Coimbra} = \text{Coimbra } \theta \text{ Coimbra} = \text{Coimbra}$$

$$\text{Lisboa } \theta (\text{Porto } \theta \text{ Coimbra}) = \text{Lisboa } \theta \text{ Lisboa} = \text{Lisboa}$$

II. Seja $\mathcal{F}$ um conjunto qualquer de aplicações, fechado para a multiplicação (ou composição). Então, pelo que vimos no Cap. IV, n.os 10-17, $\mathcal{F}$ é um grupóide associativo (portanto um semigrupo), mas pode não ser comutativo. É o que sucede, por exemplo, se $\mathcal{F}$ é o conjunto das aplicações do conjunto $\{1, 2\}$ em si mesmo. Tem-se, com efeito:

$$\begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$$

Chama-se *semigrupo de aplicações* precisamente todo o conjunto de aplicações fechado para a multiplicação (ou composição).

III. Os grupóides $(\mathbb{N}, +)$ e $(\mathbb{N}, \cdot)$ são ambos semigrupos comutativos, mas já o grupóide $(Z, -)$ não é comutativo nem associativo.

IV. Seja $\mathscr{C}$ o conjunto de todos os subconjuntos de um conjunto U dado, isto é, $\mathscr{C} = \mathcal{P}(U)$. Verifique, se, para cada uma das operações $\cap$, $\cup$, $\setminus$, o conjunto $\mathscr{C}$ é: a) um grupóide; b) um semigrupo; c) um grupóide comutativo (1).

V. Problema análogo ao anterior, considerando o conjunto $\{V, F\}$ dos valores lógicos e as operações $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$.

VI. Seja μ a operação que faz corresponder a cada par (M, N) de pontos do espaço $\mathscr{E}$ o ponto médio do segmento $\overline{MN}$. Verificar se $(\mathscr{E}, \mu)$ é: a) um grupóide; b) um semigrupo; c) um grupóide comutativo.

Posto isto, facilmente se reconhecem os dois seguintes factos:

1.º Todo o subgrupóide dum grupóide comutativo também é comutativo.

2.º Todo o subgrupóide dum grupóide associativo também é associativo.

7. **Linguagem aditiva e linguagem multiplicativa.** Muitas vezes a operação dum grupóide chama-se *multiplicação* (grupóide multiplicativo) e muitas outras chama-se *adição* (grupóide aditivo). No primeiro caso, o resultado da operação aplicada a dois elementos a, b chama-se *produto de* a *por* b e representa-se por $a \times b$, $a \cdot b$ ou ab. No segundo caso, o resultado da operação aplicada a dois elementos, a, b chama-se *soma de a com b* e representa-se por

(1) Note-se que as operações lógicas sobre conjuntos têm o mesmo nome e são designadas pelos mesmos símbolos ('$\cap$', '$\cup$', etc.) qualquer que seja o universo U considerado, embora sejam na realidade *operações distintas,* quando se muda de universo. Mas não há, em geral, perigo de confusão nesta identidade de terminologia e notações.

a + b. Há depois, como veremos adiante, uma série de termos e de notações que se ligam a cada um destes casos.

Temos, assim, duas linguagens — a multiplicativa e a aditiva — que se usam até em alternativa com outras. Por exemplo, no caso dos conjuntos, a reunião $A \cup B$ também se chama soma (lógica) e se representa por $A + B$, enquanto a intersecção $A \cap B$ se chama produto (lógico) e se representa por AB (*mas não por* $A \times B$). Analogamente para as operações $\vee$, $\wedge$ sobre valores lógicos. Por sua vez, no caso das aplicações, a expressão 'produto de f por g' e a notação 'fg' usam-se em alternativa com a expressão 'f composta com g' e com a notação 'fog' (excepto quando haja possibilidade de confusão). É claro que se trata apenas de convenções de linguagem, mais ou menos arbitrárias; havemos de ver mais adiante que o produto de duas aplicações f, g, nesta acepção, também aparece algumas vezes com o nome de soma de f com g e representada por f + g.

8. **Operações iteradas. Propriedades comutativa e associativa generalizadas.** Consideremos um grupóide (A, θ). A operação binária θ dará origem a uma operação ternária, a uma operação quaternária, etc., se pusermos, por definição:

$$a_1 \theta a_2 \theta a_3 = (a_1 \theta a_2) \theta a_3,$$

$$a_1 \theta a_2 \theta a_3 \theta a_4 = (a_1 \theta a_2 \theta_1 a_3) \theta a_4$$

e assim sucessivamente, sendo a_1, a_2,... elementos quaisquer de A. Chama-se *operação* θ *iterada* à operação que deste modo se define, a partir de θ, para uma sequência qualquer $(a_1, a_2, \ldots a_n)$ de elementos de A (com $n > 1$). O resultado desta operação pode ser representado em geral pela notação

$$a_1 \theta a_2 \theta \ldots \theta a_n$$

ou ainda, quando n é variável, pela notação mais correcta

$$(1) \qquad \overset{n}{\underset{k=1}{\theta}} a_k$$

em que k é um índice mudo. Põe-se, ainda, por definição:

$$\overset{1}{\underset{k=1}{\theta}} a_k = a_1$$

Aliás, na indicação destas operações, não é necessário que o índice tome só valores inteiros, de 1 a n; basta que tome valores inteiros relativos. Por exemplo:

$$\overset{2}{\underset{k=0}{\theta}} a = a_0 \,\theta\, a_1 \,\theta\, a_2, \qquad \overset{6}{\underset{k=3}{\theta}} a_k = a_3 \,\theta\, a_4 \,\theta\, a_5 \,\theta\, a_6, \quad \text{etc.}$$

Já vimos, atrás, convenções deste tipo aplicadas às operações $\cap$ e $\cup$. No entanto, quando a operação se chama 'adição' é costume tomar para símbolo inicial a letra Σ (em vez do sinal +); e, quando a operação se chama 'multiplicação', é costume tomar para símbolo inicial a letra Π. Também já encontrámos estas convenções a propósito dos números naturais.

Posto isto, demonstram-se os dois seguintes teoremas importantes:

TEOREMA I. *Se a operação* θ *é associativa, a operação* θ *iterada tem a propriedade associativa generalizada, isto é: o valor duma expressão da forma* (1) *não muda, substituindo dois ou mais dados consecutivos pelo respectivo resultado da operação iterada.*

Simbolicamente, isto pode ser expresso pela fórmula

$$\overset{n}{\underset{k=1}{\theta}} a_k = \left(\overset{p}{\underset{k=1}{\theta}} a_k\right) \theta \left(\overset{n}{\underset{k=p+1}{\theta}} a_k\right), \quad \forall\, p: 1 \leqslant p < n$$

(Traduza nas linguagens aditiva e multiplicativa.)

TEOREMA II. *Se a operação* θ *é associativa e comutativa, a operação* θ *iterada tem a propriedade comutativa generalizada, isto é: o valor duma expressão da forma* (1) *não depende da ordem dos dados.*

Repare na extrema generalidade destes teoremas: o primeiro aplica-se a *todos os possíveis* grupóides associativos (semigrupos); o segundo aplica-se a *todos os possíveis* semigrupos comutativos.

Não vamos, agora, demonstrar estes teoremas. Limitar-nos-emos a dar uma ideia de como se demonstram, considerando dois casos particulares e usando a notação multiplicativa por ser a mais cómoda.

Suponhamos que a multiplicação é associativa e provemos que se tem:

$$a_1a_2a_3a_4a_5 = (a_1a_2a_3)\,(a_4a_5), \quad \forall\, a_1,a_2,a_3,a_4,a_5 \in A$$

Já sabemos que

$$a_1a_2a_3a_4a_5 = (a_1a_2a_3a_4)a_5 = ((a_1a_2a_3)a_4)a_5 \quad (\textit{Porquê?})$$

Ponhamos $a_1a_2a_3 = b$. Então, virá:

$$a_1a_2a_3a_4a_5 = (ba_4)a_5 = b(a_4a_5) \qquad (\textit{Porquê?})$$

Donde:

$$a_1a_2a_3a_4a_5 = (a_1a_2a_3)\,(a_4a_5)$$

Suponhamos, agora, que a multiplicação é associativa e comutativa, e provemos, por exemplo, que:

$$a_1a_2a_3a_4 = a_3a_1a_4a_2\,, \quad \forall\, a_1,a_2,a_3,a_4 \in A$$

Comecemos por levar o factor a_3 ao primeiro lugar. Temos:

$$a_1a_2a_3a_4 = a_1(a_2a_3)a_4 = a_1(a_3a_2)a_4 \quad (\textit{Porquê?})$$
$$= (a_1a_3)\,(a_2a_4) = a_3a_1a_2a_4 \quad (\textit{Porquê?})$$

É fácil, agora, terminar a demonstração:

$$a_3a_1a_2a_4 = (a_3a_1)\,(a_2a_4) = (a_3a_1)\,(a_4a_2) \quad (\textit{Porquê?})$$

Donde, finalmente: $a_1a_2a_3a_4 = a_3a_1a_4a_2$.

9. **Múltiplos e potências.** Consideremos um grupóide aditivo (A, +). Já definimos o significado da expressão $\sum_{k=1}^{n} a_k$, sendo n um número natural qualquer e $a_1,\ldots a_n$ elementos quaisquer de A. Pode acontecer em particular que $a_1 = a_2 = \ldots = a_n = a$; neste caso, o resultado da adição iterada chama-se *produto de* n *por* a, e representa-se por na. Será, pois, por definição:

$$na = \sum_{k=1}^{n} a_k, \text{ sendo } a_1 = \ldots = a_n = a \quad (\forall n \in \mathbb{N},\ a \in A)$$

Assim: $1 \cdot a = a$, $2a = a + a$, $3a = a + a + a$, etc.

Os elementos a, 2a,..., na,... chamam-se *múltiplos (naturais) de* a: 2a *o dobro de* a, 3a *o triplo de* a, etc.

Analogamente, num grupóide multiplicativo (A, ·), põe-se por definição:

$$a^n = \prod_{k=1}^{n} a_k, \text{ sendo } a_1 = \ldots = a_n = a \quad (\forall\, n \in \mathbb{N},\ a \in A)$$

Assim: $a^1 = a$, $a^2 = aa$, $a^3 = aaa$, etc.

Diz-se então que a^n é a *potência de expoente* n *de* a: a^2 *o quadrado de* a, a^3 *o cubo de* a, a^4 *a quarta potência de* a, etc.

Aplicando os dois teoremas anteriores, podemos agora estender as propriedades clássicas das potências de expoente natural, a *grupóides multiplicativos quaisquer,* nos seguintes termos:

TEOREMA I. **Se a multiplicação é associativa, tem-se:**

$$a^m a^n = a^{m+n} \quad (\forall\, m, n \in \mathbb{N},\ a \in A)$$

Vamos apresentar a demonstração sob forma intuitiva. Temos:

$$a^m a^n = \underbrace{(a...a)}_{m \text{ vezes}} \underbrace{(a...a)}_{n \text{ vezes}} \quad (\textit{Porquê?})$$

$$= \underbrace{aa...a}_{m+n \text{ vezes}} = a^{m+n} \quad (\textit{Porquê?})$$

TEOREMA II. *Se a multiplicação é associativa e comutativa, tem-se:*

$$a^n b^n = (ab)^n, \quad \forall\, n \in \mathbb{N},\ a, b \in A$$

Com efeito, temos:

$$a^n b^n = \underbrace{(aa...a)}_{n \text{ vezes}} \underbrace{(bb...b)}_{n \text{ vezes}}$$

$$= \underbrace{(ab)\ (ab)...(ab)}_{n \text{ vezes}} = (ab)^n \quad (\textit{Porquê?})$$

Notemos, agora, o seguinte facto muito importante:

Tudo o que for demonstrado para grupóides multiplicativos fica automaticamente demonstrado para grupóides com outra linguagem qualquer; bastará traduzir a linguagem multiplicativa na linguagem adoptada para o grupóide em questão.

Por exemplo, em linguagem aditiva, isto é, para um grupóide $(A,+)$, os teoremas I e II enunciam-se:

TEOREMA I'. *Se a adição é associativa, tem-se:*

$$ma + na = (m + n)a, \quad \forall m, n \in \mathbb{N},\ a \in A$$

TEOREMA II'. *Se a adição é associativa e comutativa, tem-se:*

$$na + nb = n(a + b) \quad , \quad \forall\, n \in \mathbb{N},\ a \in A$$

A passagem de 'ma + na' para '(m + n)a' é a operação algébrica a que, nos casos clássicos, se chama 'pôr o factor comum *a* em evidência'; e analogamente para a segunda fórmula. Aplicando a propriedade simétrica da relação =, as duas fórmulas anteriores também se podem escrever do seguinte modo:

$$(m + n)a = ma + na \quad \textit{(distributividade à esquerda)}$$

$$n(a + b) = na + nb \quad \textit{(distributividade à direita)}$$

Mais uma vez chamamos a atenção do aluno para a extrema generalidade destes teoremas: o primeiro aplica-se a *qualquer* semigrupo e o segundo a *qualquer* semigrupo comutativo, qualquer que seja a natureza dos elementos do conjunto A (funções, números ou quaisquer outras entidades que venham a ser consideradas). *A linguagem e as notações adoptadas são apenas pormenores acidentais, maneiras diferentes de exprimir os mesmos factos.*

Começamos a ver aqui em que consiste o chamado 'método abstracto (ou formal) da matemática moderna' e quais as suas vantagens. Um dos recursos fundamentais deste método é o conceito de *isomorfismo,* que vamos em seguida apresentar no caso dos grupóides.

10. **Isomorfismos entre grupóides.** Consideremos, por exemplo, no universo IN, a função $x \curvearrowright 2^x$ (chamada *função exponencial de base* 2). Trata-se duma aplicação de conjunto IN *sobre* o conjunto das potências naturais de 2. Designemos por P_2 esse conjunto e por f a referida aplicação. Teremos, assim: $f(x) \equiv 2^x$ (em IN) ou, em notação mais intuitiva:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \dots & n & \dots \\ 2 & 4 & 8 & 16 & 32 & \dots & 2^n & \dots \end{pmatrix}$$

Ora, segundo o teorema I do número anterior, tem-se:

$$2^{m+n} = 2^m \cdot 2^n \quad (\forall\, m, n \in \mathbb{N})$$

ou seja, atendendo a que $2^x = f(x)$ para todo o $x \in \mathbb{N}$:

$$(1) \qquad f(m+n) = f(m) \cdot f(n) \quad (\forall\, m, n \in \mathbb{N})$$

Assim, ao passar de $\mathbb{N}$ para P_2 por meio da aplicação f a adição *traduz-se* na multiplicação. Por exemplo, aos números 2 e 3 correspondem, respectivamente, os números 4 e 8; então à *soma* dos dois primeiros $(2 + 3 = 5)$ corresponderá o *produto* dos dois últimos $(4 \times 8 = 32)$, e assim por diante. Ora bem, este facto deveras curioso, expresso pela fórmula (1), também se pode indicar dizendo que a aplicação f *transforma a adição na multiplicação* ou que:

> f *é um isomorfismo do grupóide aditivo* $\mathbb{N}$ *sobre o grupóide multiplicativo* P_2

• Consideremos, agora, a aplicação inversa:

$$f^{-1} = \begin{pmatrix} 2 & 4 & 8 & 16 & 32 & \dots & 2^n & \dots \\ 1 & 2 & 3 & 4 & 5 & \dots & n & \dots \end{pmatrix}$$

A cada número x da primeira linha corresponde, assim, o número y tal que $x = 2^y$. Este número y é chamado *logaritmo de* x *na base* 2 e representa-se pela notação $\log_2 x$. Por exemplo, $\log_2 8 = 3$, $\log_2 128 = 7$, etc.

Assim, a função $x \curvearrowright \log_2 x$ é a inversa da primeira: chama-se *função logarítmica na base* 2.

Ora, se f transforma a adição em multiplicação, o que é de

prever para f^{-1}? Que transforme a multiplicação *em adição,* isto é, que:

$$f^{-1}(m \cdot n) = f^{-1}(m) + f^{-1}(n) \quad , \quad \text{ou seja:}$$

$$\log_2(m \cdot n) = \log_2 m + \log_2 n, \quad \forall\, m, n \in P_2$$

Este facto, consequência dum teorema geral que demonstraremos mais adiante, pode exprimir-se dizendo:

A função $\log_2$ *é um isomorfismo de* $(P_2, \cdot)$ *sobre* $(\mathbb{N}, +)$.

É claro que estas considerações se generalizam a qualquer número natural a, como base, em vez de 2. A função $x \mapsto a^x$ (chamada função exponencial de base a) é um *isomorfismo de* $(\mathbb{N}, +)$ *sobre* $(P_a, \cdot)$, onde P_a designa o conjunto das potências naturais de a. Dado um número $x \in P_a$, chama-se *logaritmo de* x *na base* a, e representa-se por $\log_a x$, o número y tal que $x = a^y$. Por exemplo:

$$\log_{10} 10000 = 4 \quad , \quad \log^5 125 = 3 \quad , \quad \text{etc.}$$

Deste modo, a função $\log_a$ (chamada *função logarítmica na base* a) é a inversa da primeira, isto é:

$$y = \log_a x \Leftrightarrow x = a^y \quad (\forall\, x \in P_a \quad , \quad y \in \mathbb{N})$$

ou ainda (cf. 12):

$$\log_a a^x = x, \forall\, x \in \mathbb{N} \quad ; \quad a^{\log_a x} = x, \forall\, x \in P_a$$

Ora, tal como no caso particular a = 2, teremos:

$$\log_a(m \cdot n) = \log_a m + \log_a n, \quad \forall\, m, n \in P_a$$

o que se exprime de modo análogo.

Vejamos, agora, um outro exemplo. Seja ainda *a* um número natural qualquer e consideremos a função $x \curvearrowright ax$ definida em IN. Esta função, que vamos designar por φ é uma aplicação biunívoca de IN sobre o conjunto dos múltiplos de *a*, que designaremos por M_a. Tem-se, agora, evidentemente:

$$\varphi(m + n) = \varphi(m) + \varphi(n) \quad , \quad \forall\, m, n \in \mathbb{N},$$

visto que é sempre: $a(m + n) = am + an$. Ora, indica-se este facto dizendo que φ *respeita a adição,* ou antes, que *transforma a adição do grupóide* IN *na adição do grupóide* M_a. E como, *além disso,* φ é aplicação *biunívoca de* IN *sobre* M_a, diz-se que

$$\varphi \textit{ é um isomorfismo de } (\mathbb{N},+) \textit{ sobre } (M_a,+)$$

Daqui resultará, pelo teorema que demonstraremos, que a função inversa, $x \curvearrowright \frac{1}{a}x$, é um isomorfismo de $(M_a,+)$ sobre $(\mathbb{N}, +)$.

(Depois de estudados estes exemplos e possivelmente os seguintes, tente definir, por si, o conceito geral de isomorfismo entre grupóides, e confira, depois, o resultado com a definição que vem no número seguinte.)

EXERCÍCIOS:

I. a) Prove que a aplicação $x \curvearrowright -x$ é um isomorfismo do grupóide aditivo Z sobre si mesmo (ou, como também se diz, um automorfismo deste grupóide) (1).

b) Designando por Z_2 o conjunto dos números pares relativos $(0, 2, -2, 4, -4, \ldots)$, determine os isomorfismos de $(Z, +)$ sobre $(Z_2, +)$.

---

(1) Não esquecer que há duas fases da demonstração: 1.º demonstrar que a aplicação é bijectiva; 2.º demonstrar que a aplicação respeita a adição. A definição geral de isomorfismo é dada no número seguinte.

II. Prove que as aplicações $x \mapsto x^3$, $x \mapsto x^{-1}$ e $x \mapsto \sqrt{x}$ são automorfismos do grupóide multiplicativo $\mathbb{R}^+$. Tente incluir numa só proposição geral estes três factos (designa-se por $\mathbb{Q}$ o conjunto dos números *racionais relativos*).

III. Seja $\mathcal{L}$ o conjunto $\{V, F\}$ dos valores lógicos. Prove que o operador $\sim$ (negação) é um isomorfismo de $(\mathcal{L}, \wedge)$ sobre $(\mathcal{L}, \vee)$ e de $(\mathcal{L}, \dot{\vee})$ sobre $(\mathcal{L}, \Leftrightarrow)$ (considerando $\Leftrightarrow$ como operação e não como relação binária).

IV. Designemos por 0, r, 2r, 3r, respectivamente, as amplitudes de ângulo nulo, de ângulo recto, de 2 rectos (180°) e de 3 rectos (270°). Definamos no conjunto $A = \{0, r, 2r, 3r\}$ uma operação binária chamada 'adição' e dada pela primeira das tabelas abaixo apresentadas.

A segunda é a tabela do grupóide multiplicativo constituído pelas potências naturais da aplicação

$$S = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

$x + y$

x \ y	0	r	2r	3r
0	0	r	2r	3r
r	r	2r	3r	0
2r	2r	3r	0	r
3r	3r	0	r	2r

$u \cdot v$

u \ v	I	S	S^2	S^3
I	I	S	S^2	S^3
S	S	S^2	S^3	I
S^2	S^2	S^3	I	S
S^3	S^3	I	S	S^2

É fácil ver que se tem $S^4 = I$, $S^5 = S$, $S^6 = S^2$, etc.
Ponhamos $B = \{I, S, S^2, S^3\}$.

Olhando para as duas tabelas anteriores rapidamente se reconhece a existência de um isomorfismo de (A, +) sobre (B, •), que é a aplicação:

$$f = \begin{pmatrix} 0 & r & 2r & 3r \\ I & S & S^2 & S^3 \end{pmatrix}$$

Com efeito, esta aplicação é *bijectiva* e tem-se:

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

Por exemplo:

$$f(r + 2r) = f(3r) = S^3 = S \cdot S^2 = f(r) \cdot f(2r)$$

Aliás, verifica-se muito facilmente (1), notando que se passa da primeira tabela para a segunda, aplicando f não só aos *dados*, como também aos *resultados* da operação +. *Deste modo,* f *é, por assim dizer, uma tradução do primeiro grupóide no segundo.* Posto isto:

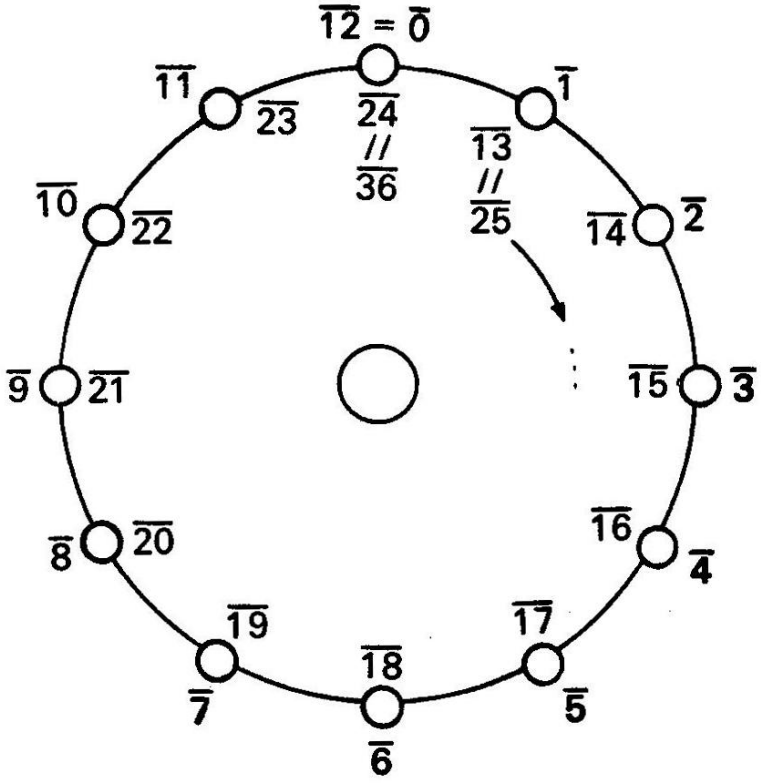
Verifique se existe algum outro isomorfismo de (A, +) *sobre* (B, •) *e se existe algum automorfismo de* (A, +) *diferente da identidade* (as duas questões estão interligadas).

V (BAILADO DAS HORAS). Designemos por H um conjunto de 12 elementos, que podem ser, por exemplo, 6 rapazes e 6 raparigas, digamos: Pedro, Helena, Júlio, Manuela, Rui, Luísa, David, Natércia, Eduardo, Beatriz, Álvaro, Urbana. Vamos supor estes elementos dispostos em círculo, à maneira das horas dum relógio, e designá-los, respectivamente, pelos seguintes símbolos(1):

$$\overline{1},\quad \overline{2},\quad \overline{3},\quad \overline{4},\quad \overline{5},\quad \overline{6},\quad \overline{7},\quad \overline{8},\quad \overline{9},\quad \overline{10},\quad \overline{11}\quad \overline{12}$$

---

(1) Estes símbolos podem ler-se 'um traço', 'dois traço', etc.



O elemento $\overline{12}$ (Urbana) também pode ser designado por qualquer dos símbolos $\overline{0}$, $\overline{24}$, $\overline{36}$, ...; isto é, em geral, pela notação $\overline{m}$, onde m é qualquer múltiplo de 12. Analogamente, o elemento $\overline{1}$ (Pedro) também pode ser designado por qualquer dos símbolos $\overline{13}$, $\overline{25}$, ...; isto é, em geral, pela notação $\overline{n}$, onde n é 1 *mais* um múltiplo de 12. E assim por diante. Deste modo, teremos, por exemplo:

$$\text{Rui} = \overline{5} = \overline{17} = \overline{29} = \ldots = \overline{5 + 12\,k} \quad , \quad \forall\ k \in \mathbb{N}_0,$$

isto é, as designações $\overline{5}$, $\overline{17}$, etc., são equivalentes.

Posto isto, vamos definir em H uma operação (chamada 'adição') mediante a fórmula:

(2) $$\overline{m} + \overline{n} = \overline{m + n}, \quad \forall\ \overline{m},\ \overline{n} \in H$$

x + y

x \ y	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{12}$
$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{12}$	$\overline{1}$
$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{12}$	$\overline{1}$	$\overline{2}$
$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{12}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{12}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{12}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{12}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{12}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{12}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$
$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{12}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$
$\overline{10}$	$\overline{11}$	$\overline{12}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$
$\overline{11}$	$\overline{12}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$
$\overline{12}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$	$\overline{12}$

Assim teremos, por exemplo:

$$\overline{3} + \overline{8} = \overline{11}, \quad \overline{5} + \overline{7} = \overline{12} = \overline{0}, \quad \overline{6} + \overline{9} = \overline{15} = \overline{3}, \ldots$$

É claro que, na fórmula (2), podemos sempre substituir m + n pelo *resto da divisão de* m + n *por* 12.

Desde logo se reconhece que a operação definida por (2) é sempre possível em H. *Vamos ver que também é unívoca.*

Com efeito, suponhamos que

$$\overline{m'} = \overline{m} \text{ e } \overline{n'} = \overline{n}, \text{ com } 0 \leqslant m < 12 \quad \text{e} \quad 0 \leqslant n < 12.$$

Então $m' = m + 12h$, $n' = n + 12k$, com $h, k \in \mathbb{N}_0$. Por conseguinte $m' + n' = (m + n) + 12(h + k)$ e como $h + k \in \mathbb{N}_0$, teremos:

$$\overline{m'} + \overline{n'} = \overline{m} + \overline{n}$$

A operação é pois unívoca, isto é, faz corresponder a cada par $(\overline{m}, \overline{n})$ de elementos de H um único elemento $\overline{m} + \overline{n}$ de H. Assim, fica provado que H *é um grupóide relativamente à operação definida.* Esta também pode ser dada pela tabela da página anterior.

Este grupóide sugere-nos a imagem de um baile de roda. Por exemplo, *adicionar* $\overline{1}$, $\overline{2}$, ... traduz-se por fazer *rodar* o conjunto H de 30°, 60°, ..., no sentido dos ponteiros dum relógio. Por isso, chamaremos pitorescamente *'Bailado das Horas'* ao grupóide aditivo H.

Usando a fórmula (1) não oferece dificuldade nenhuma provar que o *Bailado das Horas é um semigrupo comutativo.* Consideremos, agora, a transformação

$$S = \begin{pmatrix} \overline{1} & \overline{2} & \overline{3} & \overline{4} & \overline{5} & \overline{6} & \overline{7} & \overline{8} & \overline{9} & \overline{10} & \overline{11} & \overline{12} \\ \overline{2} & \overline{3} & \overline{4} & \overline{5} & \overline{6} & \overline{7} & \overline{8} & \overline{9} & \overline{10} & \overline{11} & \overline{12} & \overline{1} \end{pmatrix}$$

e as suas sucessivas potências S, S^2, S^3, ... É fácil ver que $S^{12} = I$, $S^{13} = S^1$, $S^{14} = S^2$, ... *O conjunto das potências de* S *reduz-se, pois, a 12 elementos.* Designemos este conjunto por H^*. Posto isto:

Designando por f *a aplicação* $\overline{n} \curvearrowright S_n$, *prove que* f *é:*

1) *uma aplicação biunívoca de* H *sobre* H^*;
2) *um isomorfismo do grupóide aditivo* H *sobre o grupóide multiplicativo* H^*.

Verifique se existe algum automorfismo de H *diferente da identidade e algum outro isomorfismo de* H *sobre* H^* *(problemas equivalentes).*

Para terminar este importante exemplo, recordemos que os símbolos $\overline{1}$, $\overline{2}$, ... foram interpretados como designações de 6 rapazes e 6 raparigas. Mas é claro que *temos a liberdade* de designar por

estes símbolos outros entes, por exemplo determinadas cidades portuguesas, determinados planetas, determinados ângulos (múltiplos de 30°), etc. Sendo assim, fica automaticamente definida uma aplicação do referido conjunto de rapazes e raparigas sobre conjunto dos novos entes e vê-se que essa aplicação é um isomorfismo para a adição definida com os referidos símbolos. *Neste caso, o que muda é unicamente a natureza dos elementos, isto é, a MATÉRIA; o que permanece é a estrutura lógica do grupóide, isto é, a FORMA.* Como teremos ocasião de ir observando, dois dos caracteres essenciais da matemática moderna são os seguintes:

1) *A matemática moderna tem um grau de liberdade muito superior ao da matemática clássica.*

2) *Os universos considerados em matemática moderna são geralmente definidos a menos de um isomorfismo: o que interessa é a FORMA (isto é, as propriedades lógicas das operações ou relações consideradas nesses universos) e não a MATÉRIA (isto é, a natureza dos entes que constituem o universo).*

11. **Teoremas sobre isomorfismos.** Vamos, agora, formular a definição geral de isomorfismo entre grupóides.

DEFINIÇÃO. *Chama-se isoformismo dum grupóide* (A, Θ) *sobre um grupóide* (B, Φ) *toda a aplicação biunívoca* f *de* A *sobre* B *tal que:*

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

Esta fórmula também se pode exprimir dizendo que f *transforma* Θ *em* Φ. Se, em particular, $\Theta = \Phi$, diremos que f *respeita* Θ.

Assim, f funciona como um *dicionário*, que traduz os factos relativos ao primeiro grupóide nos factos relativos ao segundo. Por exemplo, f transforma a operação Θ iterada na operação Φ iterada, isto é:

$$f(a_1 \Theta a_2 \Theta \ldots \Theta a_n) = f(a_1) \Phi f(a_2) \Phi \ldots \Phi f(a_n)$$

quaisquer que sejam $n \in \mathbb{N}$ e $a_1, \ldots a_n \in A$ (prove, por exemplo, com $n = 3$). Daqui resulta em particular o seguinte:

1) Se $\Theta = +$, $\Phi = \cdot$, o isomorfismo f traduz o *'produto por* n' em *'potência de expoente* n':

$$f(nx) = [f(x)]^n, \quad \forall x \in A, \quad n \in \mathbb{N} \quad (\textit{Prove}).$$

2) Se $\Theta = \cdot$, $\Phi = +$, o isomorfismo f traduz *'potência de expoente* n' em *'produto por* n' (escreva a respectiva fórmula e prove).

O que sucede de análogo quando $\Theta = +$, $\Phi = +$ ou $\Theta = \cdot$, $\Phi = \cdot$?

Interessa, agora, demonstrar duas propriedades importantes dos isomorfismos:

TEOREMA I. *A aplicação inversa dum isomorfismo ainda é um isomorfismo.* Mais precisamente: *Se* f *é um isomorfismo de* (A, Θ) *sobre* (B, Φ), *então* f^{-1} *é um isomorfismo de* (B, Φ) *sobre* (A, Θ)

Demonstração (1):

Suponhamos que f é isomorfismo do primeiro grupóide sobre o segundo (hipótese). Vamos provar que f^{-1} é um isomorfismo do segundo sobre o primeiro (tese).

Sejam u, v elementos *quaisquer* de B; então existem elementos x, y de A tais que

$$u = f(x), \quad v = f(y) \qquad (\textit{Porquê?})$$

Por outro lado

$$f(x \,\Theta\, y) = u \,\Phi\, v \qquad (\textit{Porquê?})$$

Donde:

$$x \,\Theta\, y = f^{-1}\,(u \,\Phi\, v) \qquad (\textit{Porquê?})$$

---

(1) Para tornar esta demonstração mais intuitiva, convém desenhar diagramas a representar A, B, x, y, u, v, etc.

E, como $x = f^{-1}(u)$, $y = f^{-1}(v)$, virá, trocando os dois membros da igualdade anterior:

$$f^{-1}(u \Phi v) = f^{-1}(u) \Theta f^{-1}(v)$$

Como u, v são *elementos quaisquer de* B, isto quer dizer que f^{-1} é um isomorfismo de (B, Φ) sobre (A, Θ).

TEOREMA II. *O produto de dois isomorfismos ainda é um isomorfismo.* Mais precisamente: *Se* f *é um isomorfismo de* (A, Θ) *sobre* (B, Φ) *e se* g *é um isomorfismo de* (B, Φ) *sobre* (C, ψ), *então* gf *é um isomorfismo de* (A, Θ) *sobre* (C, ψ).

Demonstração (1):

Suponhamos verificada a hipótese; vamos provar a tese. Sejam x, y *elementos quaisquer de* A. Então, virá:

$$f(x \Theta y) = f(x) \Phi f(y) \qquad (Porquê?)$$

Donde:

$$g[f(x \Theta y)] = [g(f(x)] \psi [g(f(y))] \qquad (Porquê?)$$

E, portanto:

$$(g f) (x \Theta y) = [(gf) (x)] \psi [(gf) (y)] \qquad (Porquê?)$$

Mas isto significa que gf é isomorfismo de (A, Φ) sobre (C, ψ).

Ambos estes teoremas são de uma extrema generalidade. Já atrás aplicámos o teorema I às funções logarítmicas.

---

(1) Conselho análogo ao que foi dado no início da demonstração anterior.

12. **Grupóides isomorfos.** Diz-se que um grupóide (A, Θ) é *isomorfo* a um grupóide (B, Φ) quando existe, *pelo menos*, um isomorfismo de (A, Θ) sobre (B, Φ). Por exemplo, o grupóide $(\mathbb{N}, +)$ é isomorfo ao grupóide $(P_2, \cdot)$, pois que existe o isomorfismo $n \mapsto 2^n$ do primeiro sobre o segundo. Analogamente, o grupóide $(Z, +)$ é isomorfo ao grupóide $(Z_2, +)$, onde Z_2 é o conjunto dos números pares relativos; com efeito, já vimos que as aplicações $x \mapsto 2x$ e $x \mapsto -2x$ são isomorfismos do primeiro sobre o segundo (bastava que existisse *um* isomorfismo).

Para indicar que o grupóide (A, Θ) é isomorfo ao grupóide (B, Φ), escreve-se:

$$(A,\Theta) \simeq (B,\Phi)$$

A relação assim definida entre grupóides é chamada *relação de isomorfia* (1). Será esta relação reflexiva, simétrica, transitiva? Será uma relação de equivalência? É fácil ver que sim:

1.º *Todo o grupóide é isomorfo a si mesmo.*

2.º $(A, \Theta) \simeq (B, \Phi) \Rightarrow (B, \Phi) \simeq (A, \Theta)$

3.º $(A, \Theta) \simeq (B, \Phi) \wedge (B, \Phi) \simeq (C, \psi) \Rightarrow (A, \Theta) \simeq (C, \psi)$

Tente provar estes três factos, aplicando os dois teoremas do número anterior e lembrando que I_A *é um automorfismo de todo o grupóide* (A, Θ). Em conclusão:

> *A isomorfia entre grupóides é uma relação de equivalência.*

(1) Não confundir 'isomorfia' com 'isomorfismo'. Os isomorfismos são determinadas *aplicações* entre grupóides. A isomorfia é *uma relação* entre grupóides, que consiste na possibilidade de definir, *pelo menos*, um isomorfismo entre os dois grupóides dados.

Assim, em vez de dizer que um grupóide é isomorfo a outro, poderá dizer-se que *os dois grupóides são isomorfos* (ver pág. 129, 1.º tomo).

Como já observámos no número anterior, um isomorfismo f entre dois grupóides funciona como um dicionário que *traduz* a linguagem do primeiro na linguagem do segundo, e vice-versa, visto que f^{-1} também é um isomorfismo do segundo no primeiro. Daqui resulta o seguinte facto muito importante:

PRINCÍPIO DE ISOMORFIA. *Se os grupóides* (A, Θ) *e* (B, Φ), *são isomorfos, todas as propriedades lógicas da operação* Θ *são verificadas pela operação* Φ *e reciprocamente.*

Chamamos *propriedades lógicas* (ou *formais*) dum ente qualquer as propriedades desse ente que se podem exprimir integralmente mediante conceitos da lógica. Por exemplo, o facto de duas rectas serem ou não concorrentes é uma propriedade lógica, mas já o facto de duas rectas serem perpendiculares *não é* uma propriedade lógica; por sua vez, o facto de a perpendicularidade ser uma *relação simétrica* é uma *propriedade lógica dessa relação.*

Analogamente as propriedades comutativa, associativa, etc., *relativas a operações, são propriedades lógicas (ou formais) dessas operações.*

O anterior PRINCÍPIO DE ISOMORFIA é um teorema que se pode demonstrar na sua máxima generalidade. Limitar-nos-emos a verificá-lo aqui em alguns casos particulares, para dar uma ideia do seu alcance. Suponhamos que (A, Θ) *é isomorfo a* (B, Φ) e que *a operação* Θ *é comutativa;* segundo o PRINCÍPIO DE ISOMORFIA, *a operação* Φ *também deve ser comutativa.* Vamos provar directamente este facto:

Designe f um isomorfismo de (A, Θ) sobre (B, Φ) (existe um pelo menos; porquê?). Sejam agora u, v dois elementos *quais-*

quer de B(1). Então existem $x, y \in A$ tais que $f(x) = u$, $f(y) = v$. (*Porquê?*) Ora

$$x \Theta y = y \Theta x \quad (\textit{Porquê?})$$

Logo $f(x \Theta y) = f(y \Theta x)$ e, portanto:

$$f(x) \Phi f(y) = f(y) \Phi f(x) \quad (\textit{Porquê?})$$

ou seja $u \Phi v = v \Phi u$. Isto prova que Φ é comutativa. (*Porquê?*)

Como exercício, prove o seguinte corolário do anterior princípio:

Se dois grupóides são isomorfos, e um deles é um semigrupo, o outro também é um semigrupo.

Prove agora o seguinte facto, deveras interessante:

O PRINCÍPIO DA DUALIDADE LÓGICA, quer para valores lógicos (Cap. I, n.º 13), quer para conjuntos (Cap. II, n.º 11), é um corolário do PRINCÍPIO DE ISOMORFIA.

O facto de duas operações Θ e Φ terem exactamente as mesmas propriedades formais, exprime-se dizendo que os grupóides (A, Θ) e (B, Φ) *têm a mesma estrutura*. Assim, o PRINCÍPIO DE ISOMORFIA podia enunciar-se do seguinte modo:

Se dois grupóides são isomorfos, têm a mesma estrutura.

O mais curioso é que a recíproca desta proposição também é verdadeira.

Se dois grupóides têm a mesma estrutura, são isomorfos.

---

(1) Convém desenhar um diagrama a representar A, B, u, v, etc.

Por conseguinte:

> *Dizer que dois grupóides são isomorfos equivale a dizer que têm a mesma estrutura.*

EXERCÍCIOS:

I. Seja $\mathscr{C} = \mathscr{P}(U)$, onde U é um universo qualquer. Prove que os grupóides $(\mathscr{C}, \cap)$ e $(\mathscr{C}, \cup)$ são isomorfos.

II. Seja $f = (x \curvearrowright x + 1)$ em $\mathbb{R}$. Prove que o grupóide multiplicativo das potências $f, f^2, \ldots, f^n, \ldots$ de expoente natural de f é isomorfo a $\mathbb{N}$ (chamando multiplicação à composição de funções).

III. Prove que os grupóides aditivos $\mathbb{N}$ e $\mathbb{N}_0$ não são isomorfos, atendendo à seguinte propriedade válida em $\mathbb{N}$:

$$\forall\ a, b:\ a + b \neq a$$

IV. Prove que $(\mathbb{N}, +)$ não é isomorfo a $(\mathbb{N}, \cdot)$ atendendo à seguinte propriedade válida no primeiro:

$$a \neq b \Rightarrow \exists x\ :\ a + x = b \vee b + x = a$$

V. Prove que $(Z, +)$ não é isomorfo a $(\mathbb{N}_0, +)$.

13. **Elemento neutro dum grupóide.** Consideremos um grupóide (A, Θ) qualquer. Diz-se que um elemento *u* de A é *elemento neutro do grupóide* (ou *elemento neutro para a operação* Θ), sse verifica a condição

$$u \Theta a = a \Theta u = a\ ,\ \forall\ a \in A$$

Por exemplo, os grupóides $(\mathbb{N}_0,+)$ e $(\mathbb{N}_0,\cdot)$ têm como elementos neutros, respectivamente, os números 0 e 1; este é também elemento neutro de $(\mathbb{N},\cdot)$, mas já o grupóide $(\mathbb{N},+)$ *não tem* elemento neutro. Por sua vez, os grupóides $(\mathcal{L},\wedge)$ e $(\mathcal{L},\vee)$ têm por elementos neutros, respectivamente, os valores V e F. Também já vimos o que se passa no conjunto $\mathcal{P}(U)$ de todos os subconjuntos dum universo U: o universo é elemento neutro para a operação $\cap$, enquanto o conjunto vazio é elemento neutro para a operação $\cup$.

Daqui por diante, designaremos por $\mathcal{F}(U)$ o conjunto de *todas as aplicações dum conjunto* U *em si mesmo*. Já vimos que $\mathcal{F}(U)$ é um grupóide associativo relativamente à multiplicação (ou composição). Ora, é evidente que a identidade é elemento neutro deste grupóide (ver pág. 199, 1.º tomo).

$$I\ f = f\ \ I = f, \quad \forall\ f \in \mathcal{F}(U)$$

(É claro que neste caso I é a identidade em U, ou seja I_U.)

Quanto ao grupóide aditivo H, que baptizámos como 'BAILADO DAS HORAS' (exercício V do n.º 10) é fácil ver que também possui elemento neutro. (Qual é?)

Já observámos que $(\mathbb{N},+)$ não tem elemento neutro. Muitos outros exemplos se nos podem apresentar de grupóides sem elemento neutro (procure por si alguns). Mas, um facto se verifica nos exemplos anteriores: *é que, quando existe elemento neutro, num grupóide, existe um só*. Será sempre assim?

Suponhamos que *u* e *v* são elementos neutros dum grupóide (A,Θ). Então, será:

$$u\,\Theta\,v = u \quad (\textit{Porquê?}), \quad u\,\Theta\,v = v \quad (\textit{Porquê?})$$

donde $u = v$ (*Porquê?*) Assim, em conclusão:

Um grupóide não pode ter mais de um elemento neutro.

Nos grupóides aditivos o elemento neutro chama-se, geralmente, *elemento nulo* (ou zero). Representá-lo-emos, *em geral,* pelo símbolo (0 e, muitas vezes, por 0 (quando não importa confundir com o *número* 0).

Nos grupóides multiplicativos o elemento neutro chama-se, geralmente, *elemento unidade* (ou só unidade). Representá-lo-emos, *em geral,* pelo símbolo 1 e, muitas vezes, por 1 (quando não fizer mal confundir com o *número* 1).

14. Elementos opostos num grupóide com elemento neutro. Seja (A, Θ) um grupóide com elemento neutro, *u*. Dado um elemento *a* de A, diz-se que um elemento a' de A é *oposto de a* no grupóide, sse verifica a condição

(1) $$a \Theta a' = a' \Theta a = u$$

Por exemplo, no grupóide (*Z*,+) todo o elemento *a* tem oposto, que é –a. Por sua vez, no grupóide (IR, $\cdot$) todo o elemento a *diferente de zero* tem oposto que é 1/a (ou a^{-1}).

Da anterior definição, fórmula (1), deduz-se imediatamente que:

I. *Se* a *é oposto de* a', *também* a' *é oposto de* a.

Podemos, então, dizer que a e a' *são elementos opostos* do grupóide (ver pág. 129, 1.º tomo). Também é imediato que:

II. *O elemento neutro (quando existe) é oposto de si mesmo.*

Posto isto:

DEFINIÇÃO. *Num grupóide com elemento neutro, um elemento* a *diz-se regular, sse existe oposto de* a.

EXERCÍCIOS:

I. Determine os elementos regulares dos grupóides $(\mathbb{N},+)$, $(\mathbb{N}_0,+)$, $(\mathbb{N}, \cdot)$ e $(Z, \cdot)$.

II. Idem para os grupóides $(\mathcal{L}, \wedge)$ e $(\mathcal{L}, \vee)$.

III. Idem para os grupóides $(\mathcal{C}, \cap)$ e $(\mathcal{C}, \cup)$, sendo $\mathcal{C} = \mathcal{P}(U)$ e U qualquer conjunto.

Consideremos, novamente, o grupóide multiplicativo $\mathcal{F}(U)$, sendo U um conjunto qualquer. É evidente que toda a aplicação *biunívoca* f de U sobre si mesmo é *regular*, tendo por elemento oposto a aplicação inversa; com efeito (ver págs. 199-200, 1.º tomo):

$$f f^{-1} = f^{-1} f = I$$

Serão esses os únicos elementos regulares do grupóide? Aqui fica esta pergunta como exercício para os melhores alunos (1).

Nos exemplos anteriores verifica-se este facto: *todo o elemento regular tem um único oposto.*

Será sempre assim?

Seja (A, Θ) um grupóide com elemento neutro, u, e suponhamos que a', a* são elementos opostos dum dado elemento *a* no grupóide. Consideremos, agora, a expressão

$$a' \Theta a \Theta a^*$$

Por hipótese, temos $a' \Theta a = a \Theta a^* = u$. Assim, *se for verdade que*

$$(1) \qquad a' \Theta a \Theta a^* = (a' \Theta a) \Theta a^* = a' \Theta (a \Theta a^*),$$

---

(1) Observe que, se existe g tal que $fg = gf = I$, então $f(g(y)) = y$, $\forall\, y \in U$, o que mostra que f é sobrejectiva; por outro lado, tem-se $g(f(x)) = x$, $\forall\, x \in U$, e portanto $y = f(x) \Rightarrow x = g(y)$, $\forall\, x, y \in U$, o que mostra que f é *injectiva*.

virá: $a' \odot a \odot a^* = u \odot a^* = a' \odot u$ e, portanto:

$$a^* = a' \quad (\textit{Porquê?})$$

Ora, (1) será verdade *se* o grupóide for associativo. Assim, em conclusão:

TEOREMA 1. *Num grupóide associativo (semigrupo) um elemento nunca pode ter mais de um oposto.*

Nos grupóides aditivos o oposto dum elemento regular *a* chama-se, geralmente, *o simétrico de* a e representa-se por $-a$.

Como exercício, indique os elementos regulares do grupóide 'Bailado das Horas' *(n.º 10, exercício V), bem como os respectivos simétricos.*

Nos grupóides multiplicativos o oposto dum elemento regular *a* chama-se, geralmente, o *inverso de* a e representa-se por a^{-1} (ou $1/a$).

Teremos, pois, por definição:

$$\boxed{aa^{-1} = a^{-1}a = 1} \quad \text{e} \quad \boxed{a + (-a) = (-a) + a = 0},$$

e, portanto (propriedade I):

$$\boxed{(a^{-1})^{-1} = a} \quad \text{e} \quad \boxed{-(-a) = a},$$

para todo o elemento regular *a* dum grupóide, respectivamente multiplicativo ou aditivo.

Podemos, agora, generalizar o teorema do Cap. IV, n.º 13, em linguagem multiplicativa:

TEOREMA 2. *Num semigrupo multiplicativo, o produto de dois elementos* a, b *regulares é ainda um elemento regular e tem-se:*

$$(ab)^{-1} = b^{-1}a^{-1}$$

Demonstração:.

Sejam a,b elementos regulares dum semigrupo multiplicativo. Então existem a^{-1}, b^{-1} e, assim:

$$(ab)\,(b^{-1}a^{-1}) = a\,(bb^{-1})a^{-1} = aa^{-1} = \mathbf{1} \qquad (Porquê?)$$

$$(b^{-1}a^{-1})\,(ab) = b^{-1}(a^{-1}a)\,b = b^{-1}b = \mathbf{1} \qquad (Porquê?)$$

Logo, ab é regular e tem-se:

$$b^{-1}a^{-1} = (ab)^{-1} \qquad (Porquê?)$$

Traduza este teorema em linguagem aditiva.

15. Divisão em semigrupos multiplicativos. Acabámos de ver o interesse que a propriedade associativa pode ter no estudo de elementos regulares num grupóide. Para maior comodidade vamos referir-nos a um *semigrupo multiplicativo* A, *com elemento neutro,* **1**. Consideremos o seguinte problema:

Dados dois elementos a, b *de* A, *determinar um elemento* x *de* A *tal que*

$$(1) \qquad ax = b$$

No caso dos números, este problema tem solução, *se* a é regular. Vamos pois supor, no caso geral, que *a* é um elemento regular do semigrupo A. Então, *se existe um elemento* x *de* a *que verifica* (1), tem-se:

$$a^{-1}(ax) = a^{-1}b \quad (Porquê?)$$

Donde: $(a^{-1}a)x = a^{-1}b$ (*Porquê?*) Portanto:

$$(2) \qquad x = a^{-1}b \qquad (Porquê?)$$

Logo, (1) implica (2). Para ver que, reciprocamente, (2) implica (1), basta fazer a substituição de x por $a^{-1}b$ em (1). Ora tem-se, efectivamente:

$$a(a^{-1}b) = (aa^{-1})b = b \quad (Porquê?)$$

Por conseguinte:

TEOREMA 1. *Se* a *é elemento regular do semigrupo multiplicativo* A *e* b *um elemento qualquer de* A, *a equação* $ax = b$ *tem uma e uma só solução em* A, *que é dada por*

$$x = a^{-1}b$$

De modo análogo se prova que:

Na mesma hipótese, a equação $xa = b$ *tem uma única solução em* A *dada por*

$$x = ba^{-1}$$

DEFINIÇÃO. *Na referida hipótese,* ba^{-1} *e* $a^{-1}b$ *dizem-se respectivamente o quociente de* b *por* a *à direita e o quociente de* b *por* a *à esquerda.*

Por sua vez, as operações

$$(b,a) \curvearrowright ba^{-1} \quad , \quad (b,a) \curvearrowright a^{-1}b$$

são chamadas, respectivamente, *divisão à direita* e *divisão à esquerda* (operações inversas da multiplicação).

EXEMPLO. Seja $a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $b = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 2 \end{pmatrix}$

Então $a^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ e $ba^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 2 & 3 \end{pmatrix}$, $a^{-1}b = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 1 \end{pmatrix}$

Tem-se, neste caso, $a^{-1}b \neq ba^{-1}$. Porém:

TEOREMA 2. *Se* a *é regular e permutável com* b, *também* a^{-1} *é permutável com* b, *isto é,* $a^{-1}b = ba^{-1}$.

Demonstração:

Seja *a* regular e permutável com *b*. Então:

$$aba^{-1} = (ab)a^{-1} = (ba)a^{-1} = b(aa^{-1}) = b \qquad (Porquê?)$$

Portanto, $aba^{-1} = b$. Daqui, multiplicando à esquerda por a^{-1}, vem:

$$a^{-1}(aba^{-1}) = a^{-1}b$$

Donde:

$$ba^{-1} = a^{-1}b \qquad (Porquê?)$$

DEFINIÇÃO. *Se* b *é regular e permutável com* a, *o elemento* $ab^{-1}(= b^{-1}a)$ *chama-se quociente de* a *por* b *e representa-se por qualquer das notações:*

$$a/b, \quad \frac{a}{b} \quad \text{ou} \quad a : b$$

Portanto, em particular, se o semigrupo A é comutativo *a divisão à direita coincide com a divisão à esquerda* (a multiplicação tem, neste caso, uma única operação inversa).

Observe-se que, neste caso, *dividir um elemento por outro equivale a multiplicar o primeiro pelo inverso do segundo* (em qualquer ordem). Por exemplo, *dividir* o número 5 por $\sqrt{2}$ equivale a *multiplicar*

5 por $1/\sqrt{2}$; *dividir* 2/3 por 3/5 equivale a *multiplicar* 2/3 por 5/3 (Inverso de 3/5), etc.

TEOREMA 3. *Se* a, b, c, d *são permutáveis entre si e se* b, d *são regulares, tem-se:*

(1) $$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

Demonstração:

Suponhamos verificada a hipótese. Então, virá (justifique todas as passagens):

$$(ab^{-1})\,(cd^{-1}) = a\ (b^{-1}c)\,d^{-1} = a\,(cb^{-1})d^{-1}$$

$$= (ac)\,(b^{-1}d^{-1}) = (ac)\,(bd)^{-1}$$

Donde: (a/b) • (c/d) = (ac) / (bd), ou seja (1) (*Porquê?*)

COROLÁRIO 1. *Se* a, b, c *são permutáveis entre si e se* b, c *são regulares, tem-se:*

$$\frac{a}{b} = \frac{ac}{bc} \qquad (Porquê?)$$

COROLÁRIO 2. *Se* a, b, c, d *são premutáveis entre si e* b, c, d *são regulares, tem-se:*

$$\frac{a}{b} : \frac{c}{d} = \frac{ad}{bc}$$

ou seja, em notação uniforme:

$$(a/b) \,/\, (c/d) = (ad) \,/\, (bc)$$

Para a demonstração, basta aplicar o teorema 3 e a definição de quociente, notando que (teorema 2 do n.º 14):

$$(c/d)^{-1} = (cd^{-1})^{-1} = (d^{-1})^{-1}c^{-1} = dc^{-1} = d/c$$

Todos estes resultados se podem traduzir em linguagem aditiva, mas disso trataremos mais adiante.

EXERCÍCIOS:

I. Sendo $S = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 2 & 1 \end{pmatrix}$ e $T = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$, calcule os quocientes de S por T à direita e à esquerda.

II. Sendo $f(x) \equiv x^2$ e $g(x) \equiv 1/(x-1)$ calcule os quocientes de f por g à direita e à esquerda, chamando 'multiplicação' à composição de funções.

III. Sendo $\varphi(x) \equiv x^3$ e $\psi(x) \equiv x^5$, mostre que existe φ/ψ e calcule este quociente, chamando 'multiplicação' à composição de funções.

IV. Sendo $a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 2 \end{pmatrix}$ e $b = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 2 & 1 \end{pmatrix}$, determine todas as soluções da equação $ax = b$. Como se explica que esta equação tenha mais de uma solução?

16. *Potências de expoente nulo ou negativo.* Seja ainda A um semigrupo multiplicativo com elemento neutro. Da propriedade do produto de potências da mesma base (pág. 20) e dos resultados anteriores, deduz-se o seguinte:

COROLÁRIO. *Se* $m, n \in \mathbb{N}$ *e* $m > n$, *então:*

$$\frac{a^m}{a^n} = a^{m-n}, \textit{ para todo o elemento } a \textit{ regular de } A.$$

Demonstração:

Suponhamos verificada a hipótese. Então $a^m = a^{m-n} \cdot a^n$. (*Porquê?*) Logo $a^m/a^n = a^{m-n}$. (*Porquê?*)

Para que esta regra se possa estender ao caso $m \leqslant n$, é necessário generalizar o conceito de potência ao caso do expoente nulo ou negativo (inteiro). Assim, para que possa ser sempre $a^m/a^m = a^{m-m}$, deveremos admitir, *por definição,* $a^0 = 1$, visto que $a^m/a^m = 1$ e $m - m = 0$. Teremos, pois:

DEFINIÇÃO. $a^0 = 1$, *se* a *é regular em* A (1).

Posto isto, para que possa ser sempre $a^0/a^n = a^{0-n}$, como $a^0 = 1$ e $0 - n = -n$, deveremos admitir, *por definição,* $a^{-n} = 1/a^n$. Teremos, pois:

DEFINIÇÃO. *Para todo o* $n \in \mathbb{N}$,

$$a^{-n} = (a^n)^{-1} = \frac{1}{a^n}, \quad \textit{se a é regular em A.}$$

Assim, no caso em que *a* é um elemento regular de A, fica definido o conceito de potência a^n, *qualquer que seja* $n \in Z$ (positivo, negativo ou nulo). E é fácil verificar (como se fez no 4.º ano no caso em que *a* é um número $\neq 0$) que se mantêm as anteriores propriedades das potências, ao adoptar o novo conceito.

EXERCÍCIOS. — I. *Sendo* $f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, *calcule* f^{-2}, f^{-3} *e verifique que* $f^{-2} = f^4$, $f^{-3} = f^3 = f^0$.

II. *Sendo* $f = (x \curvearrowright x-1)$, *com* $x \in \mathbb{R}$, *calcule* f^2, f^0, f^{-1}, f^{-2} e prove que se tem $f^m = f^n$, sse $m = n$, $\forall$ $m, n \in Z$ (chamando 'multiplicação', neste caso, à composição de funções). Prove que o grupóide das aplicações f^n, com $n \in Z$ é isomorfo a *Z*.

---

(1) Note-se que não podemos escrever $0^0 = 1$ em *Z*.

NOTA. Quando f é função real, f^n também pode designar a função definida pela fórmula $f^n(x) \equiv [f(x)]^n$. Para evitar confusões, designa-se algumas vezes pela notação f^{on} a potência *n* do operador f no sentido anterior.

17. **Radiciação em semigrupos multiplicativos.** Continuamos a supor que A é um semigrupo multiplicativo, com elemento neutro **1**. Consideremos o seguinte problema:

Dados um elemento a *de* A *(qualquer) e um número* $n \in \mathbb{N}$, *achar um elemento* x *de* A *tal que*

$$x^n = a$$

EXEMPLOS — I. Seja $n = 2$, $a = 9$. Então o problema tem uma solução única em $\mathbb{N}$ ($x = 3$) e duas soluções em Z ($x_1 = 3$, $x_2 = -3$).

II. Seja $n = 2$, $a = 2$. Então o problema não tem solução nenhuma em $\mathbb{N}$, nem sequer em $\mathbb{Q}$ (conjunto dos números racionais). Mas tem uma solução única em $\mathbb{R}^+$, que é um *número irracional* representável por uma *dízima infinita não periódica,* e tem duas soluções simétricas em $\mathbb{R}$ (ver *Compêndio de Álgebra, 6.º ano,* Cap. I, n.os 16, 18, 25 e Apêndice 1) (1).

III. Seja $n = 2$, $a = -9$. Neste caso o problema não tem solução em $\mathbb{R}$. (*Porquê?*)

IV. Seja, agora, A o semigrupo das aplicações do conjunto $\{1, 2, 3, 4, 6\}$ em si mesmo. Tomemos então $n = 3$ e

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 1 & 2 & 3 \end{pmatrix}$$

(1) Refere-se o autor ao *Compêndio de Álgebra* aprovado ao tempo, podendo hoje ser consultados diversos livros que tratam do assunto (N. do E.).

Neste caso, é fácil observar que o problema tem 9 soluções, entre as quais:

$$x_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix}, \quad x_2 = a, \quad x_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

DEFINIÇÃO. *Qualquer solução* x *da equação* $x^n = a$ *(se existe pelo menos uma em* A*) é chamada raiz de índice* n *de* a. *Se existe uma única solução dessa equação em* A, *representá-la-emos por* $\sqrt[n]{a}$. *Neste caso a expressão* $\sqrt[n]{a}$ *chama-se radical (*a, *o radicando;* n *o índice da raiz) e a operação* $(n, a) \curvearrowright \sqrt[n]{a}$ *é chamada radiciação.*

Ter-se-á pois, por definição, neste último caso:

$$\sqrt[n]{a} = \iota\,(x^n = a) \quad \text{e portanto} \quad \left(\sqrt[n]{a}\right)^n = a$$

Verifica-se este caso se $A = \mathbb{R}^+$, quaisquer que sejam $a \in A$ e $n \in \mathbb{N}$ (ver *Compêndio de Álgebra, 6.º ano,* Cap. I, n.º 25; para a hipótese $A = \mathbb{R}$, ver Cap. III, n.º 1) (1).

18. **Potências de expoente fraccionário.** Seja ainda A um semigrupo multiplicativo com elemento neutro, **1**. Da propriedade relativa ao produto de potências da mesma base reduz-se o seguinte

COROLÁRIO: $(a^m)^n = a^{mn}$, $\forall\, a \in A$; $m, n \in \mathbb{N}$.

Demonstração:

Tem-se:

$$(a^m)^n = \overbrace{a^m \cdot \ldots \cdot a^m}^{\text{(n vezes)}} = \overbrace{a^{m+\ldots+m}}^{\text{(n vezes)}} = a^{mn}$$

Esta propriedade generaliza-se facilmente ao caso em que m,n são elementos quaisquer de *Z*.

Suponhamos agora verificada a seguinte

HIPÓTESE: *Quaisquer que sejam* $a \in A$ *e* $n \in \mathbb{N}$, *a equação* $x^n = a$ *tem uma solução única* em A.

---

(1) Ver nota da pág. 48.

Segundo a definição anterior essa solução é representada por $\sqrt[n]{a}$. A *hipótese verifica-se, por exemplo, quando* $A = \mathbb{R}^+$.

Posto isto, sejam m,n dois números naturais quaisquer e designemos por r o número racional m/n. Se *m* não é múltiplo de *n*, r é um número fraccionário. Que significado atribuir então ao símbolo a^r? O significado deve ser tal que se mantenham as anteriores propriedades das potências. Assim, em particular, deverá ser $(a^r)^n = a^{rn}$ e, como $r = m/n$, virá sucessivamente $rn = m$,

$$(a^r)^n = a^m \quad \text{e portanto} \quad a^r = \sqrt[n]{a^m} \quad (\textit{Porquê?})$$

Deveremos, pois, adoptar a seguinte

DEFINIÇÃO:

$$a^{\frac{m}{n}} = \sqrt[n]{a^m} \ , \ \forall\, a \in A \ ; \ m,n \in \mathbb{N}$$

É fácil ver, como se fez no 4.º ano (1), que o valor da potência de expoente m/n de *a* dado por esta definição é único, isto é, que:

$$\frac{m}{n} = \frac{m'}{n'} \Rightarrow a^{\frac{m}{n}} = a^{\frac{m'}{n'}}$$

Em particular, se m/n é inteiro, o valor obtido é a potência usual. Mais ainda, pode verificar-se que todas as anteriores propriedades das potências se mantêm, com a referida definição.

Finalmente, *se a é regular em* A, define-se potência de *expoente fraccionário negativo,* como se fez para o expoente inteiro negativo:

$$a^{-\frac{m}{n}} = \frac{1}{a^{m/n}} = \frac{1}{\sqrt[n]{a^m}} \ , \ \forall\ a \in A \ ; \ m,n \in \mathbb{N}$$

E mais uma vez se verifica que as propriedades das potências se mantêm com a nova definição.

---

(1) Corresponde ao actual 2.º ano do ensino secundário (N. do E.).

19. **Conceito de grupo; grupos de aplicações.** Chama-se *grupo* qualquer grupóide associativo (A, Θ), que tenha elemento neutro e em que *todo* o elemento *a* seja regular ([1]). Assim, por definição, todo o grupo será um semigrupo (grupóide associativo), mas nem todo o semigrupo será um grupo.

Por exemplo, Z é um grupo (comutativo) relativamente à adição, mas não é um grupo relativamente à multiplicação (embora seja um semigrupo multiplicativo). Por sua vez, $\mathbb{Q}^+$ (conjunto dos números racionais positivos) é um grupo relativamente à multiplicação, mas não relativamente à adição. (*Porquê?*) Finalmente $\mathbb{Q}$ (ou $\mathbb{R}$) é um grupo aditivo, mas não um grupo multiplicativo. (*Porquê?*)

Da definição e do teorema 1 do n.º 15 ([2]), resulta imediatamente o seguinte:

Se (A, Θ) *é um grupo, cada uma das equações*

$$a \Theta x = b, \quad y \Theta a = b,$$

tem uma solução única em A, *quaisquer que sejam* $a, b \in A$.

Exprime-se este facto dizendo que a operação Θ é *reversível.*

Posto isto, chama-se *grupo de aplicações* todo o grupóide $\mathcal{G}$ de aplicações biunívocas dum conjunto U *sobre* si mesmo que verifique as duas seguintes condições:

1) $I \in \mathcal{G}$;

2) se $f \in \mathcal{G}$, também $f^{-1} \in \mathcal{G}$.

Imediatamente se reconhece que, nesta hipótese, $\mathcal{G}$ é de facto um grupo, segundo a definição geral anterior.

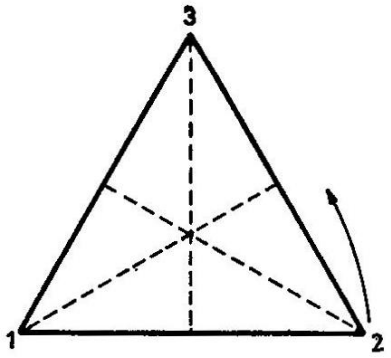
Em particular, será um grupo o conjunto de *todas* as aplicações biunívocas de U sobre si mesmo (*grupo simétrico* ou *grupo total* sobre U).

OUTROS EXEMPLOS E EXERCÍCIOS:

I. Verifique se o grupóide aditivo H (*Bailado das Horas*) é ou não um grupo.

([1]) Subentende-se que o conjunto A não é vazio.

([2]) Este teorema foi enunciado e demonstrado em linguagem multiplicativa, mas a sua tradução para um grupóide (A, Θ) qualquer não oferece dificuldade.



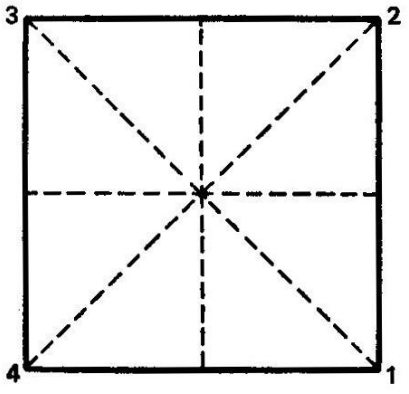
II. Consideremos um triângulo equilátero de vértices 1, 2, 3. Os deslocamentos do plano (1) que aplicam este triângulo sobre si mesmo são, como é fácil ver, as simetrias em relação às medianas do triângulo e as rotações de 120°, 240° e 360° em torno do centro. Estes deslocamentos são definidos pelas seguintes aplicações:

$$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\quad \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},\quad \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\quad \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},$$

$$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},\quad \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$$

que formam o *grupo simétrico* sobre $\{1, 2, 3\}$.

III. Consideremos um quadrado de vértices 1, 2, 3, 4. Os deslocamentos que aplicam este quadrado sobre si mesmo são dados pelas seguintes aplicações:



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

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

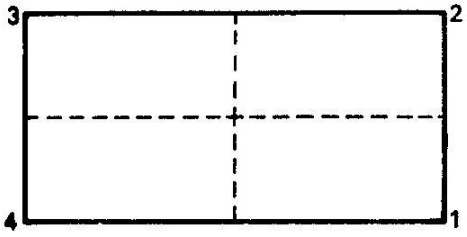
$$\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}\quad \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}\quad \begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}\quad \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}$$

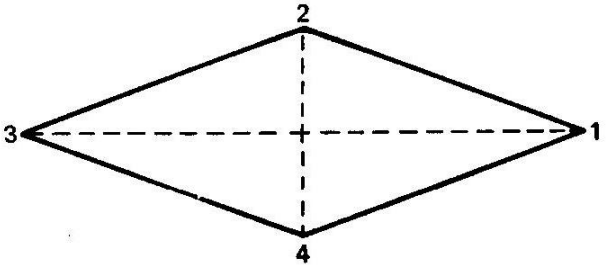
que formam um subgrupo do grupo simétrico sobre $\{1, 2, 3, 4\}$ (*grupo do quadrado*).

---

(1) Usamos aqui a palavra 'deslocamento' no sentido intuitivo usual.

IV*. Determine o *grupo do rectângulo* e o *grupo do losango* a seguir representados, definindo cada elemento do grupo por uma aplicação de {1, 2, 3, 4} (subgrupos do grupo do quadrado).

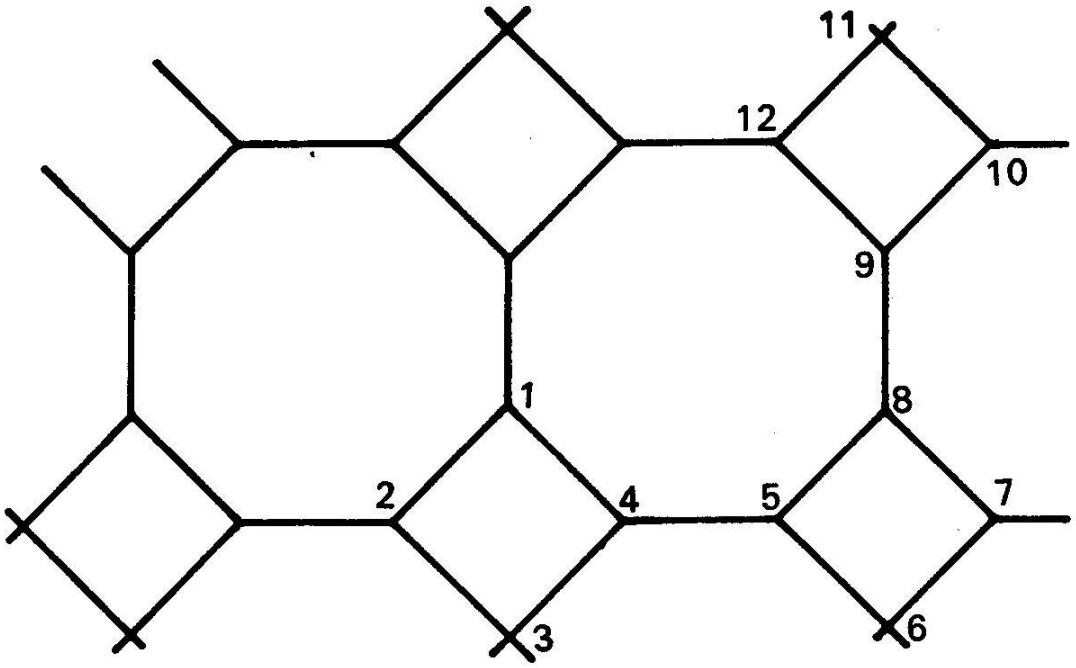




Mostre que estes dois grupos são isomorfos.

V*. Quantos elementos tem o *grupo do tetraedro regular?* E o *grupo do octaedro regular?*

VI*. Imagine um mosaico formado por octógonos e quadrados a cobrir todo o plano. Os deslocamentos do plano que não alteram este mosaico formam um *grupo infinito*. Indique alguns desses deslocamentos não incluídos no grupo do quadrado de vértices 1, 2, 3, 4.



VII*. **Demonstre que os automorfismos dum grupóide formam um grupo. Verifique que o grupo dos automorfismos do grupóide** (A, Θ) **considerado no exemplo inicial do n.º 4 é isomorfo ao grupo do triângulo equilátero.**

NOTA. A teoria dos grupos aplica-se em vários domínios da matemática e da física, e ainda em química, cristalografia, etc. Foi o grande matemático francês Evaristo Galois quem primeiro pôs em evidência a importância do conceito de grupo de transformações, ao estudar o problema da resolubilidade algébrica de equações (ver *Compêndio de Álgebra, 7.º ano,* NOTA HISTÓRICA do Cap. XXI)([1]).

20. **Quase-grupos; quadrados latinos***. Chama-se *quase-grupo todo o grupoide* (A, Θ) *cuja operação* Θ *é reversível, isto é, tal que cada uma das equações*

$$a \Theta x = b \quad , \quad y \Theta a = b$$

tem uma solução única em A, quaisquer que sejam a, $b \in A$ ([2]).

É óbvio que todo o grupo é um quase-grupo, mas a recíproca não é verdadeira. Por exemplo, facilmente se reconhece que o grupóide considerado no exemplo inicial do n.º 4 é um quase-grupo comutativo, mas não um grupo, pois não tem elemento neutro. Analogamente, se designarmos por Φ a operação que faz corresponder a cada par (a, b) de pontos do espaço ordinário E o ponto *c* tal que *b* é o ponto médio do segmento $\overline{ac}$, vê-se que (E, Φ) é um quase-grupo não comutativo. Tem-se, porém:

([1]) Ver nota da pág. 48.

([2]) Subentende-se que o conjunto A não é vazio.

TEOREMA. *Um quase-grupo é um grupo, sse for associativo.*

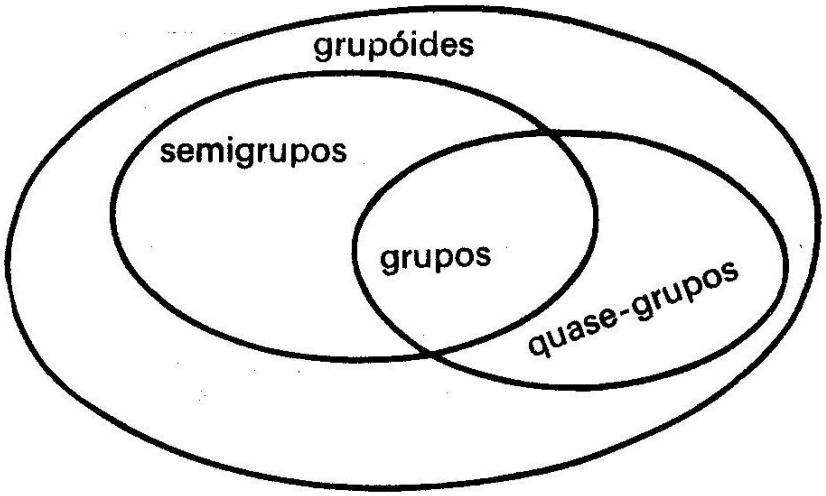
Demonstração:

Seja (A, Θ) um quase-grupo. Se (A, Θ) é um grupo, então é associativo (por definição de grupo). Suponhamos agora, reciprocamente, que (A, Θ) é associativo e seja *c* um elemento qualquer de A. Então existe um elemento u de A tal que $c \Theta u = c$. (Porquê?) Vamos provar que se tem $a \Theta u = a$, $\forall a \in A$. Com efeito, dado arbitrariamente $a \in A$, existe b tal que $b \Theta c = a$ (*porquê?*) e, assim:

$$a \Theta u = (b \Theta c) \Theta u = b \Theta (c \Theta u) = b \Theta c = a$$

Analogamente, se prova a existência de um elemento v de A tal que $v \Theta a = a$, $\forall a \in A$. Então, será $v \Theta u = u$, $v \Theta u = v$ e, portanto, $u = v$, o que prova a existência do elemento neutro em (A, Θ). Finalmente, para cada elemento *a* de A existe um elemento a' de A tal que $a \Theta a' = u$ e um elemento a^* tal que $a^* \Theta a = u$; e mais uma vez se prova (como no n.º 14) que $a' = a^*$. Logo, todo o elemento de A é regular e portanto (A, Θ) é um grupo q.e.d.

Verifica-se, pois, a seguinte hierarquia entre os conceitos de grupóide, semigrupo, quase-grupo e grupo:



Existem grupóides que não são semigrupos nem quase-grupos. Tal é, por exemplo, o grupóide ($\mathcal{L}$, $\Rightarrow$), que já vimos não ser comutativo

nem associativo e em que a equação $(x \Rightarrow V) = F$ não tem solução. Outro exemplo: seja $A = \mathbb{N}$ e designemos por P a operação $(a, b) \curvearrowright a^b$ (potenciação) isto é, ponhamos $a\ Pb = a^b$, $\forall\, a,\ b \in \mathbb{N}$; então $(\mathbb{N}, P)$ é um grupóide, mas facilmente se reconhece que P não é associativa, nem comutativa, nem reversível.

• Já sabemos que a operação dum grupóide finito (não excessivamente numeroso) pode ser dada por uma tabela de duas entradas (ver exemplos dos n.os 4 e 10). Consideremos, por exemplo, a operação φ definida pela tabela junta.

$x\ \varphi\ y$

x \ y	a	b	c	d
a	b	a	d	c
b	c	d	a	b
c	a	c	b	d
d	d	b	c	a

O conjunto $\{a, b, c, d\}$, munido da operação φ, é manifestamente um grupóide. Note-se, por outro lado, que as correspondências $y \curvearrowright a\varphi y$, $y \curvearrowright b\varphi y$, $y \curvearrowright c\varphi y$, $y \curvearrowright d\varphi y$ são, respectivamente, as aplicações

$$\begin{pmatrix} a & b & c & d \\ b & a & d & c \end{pmatrix}, \quad \begin{pmatrix} a & b & c & d \\ c & d & a & b \end{pmatrix}, \quad \begin{pmatrix} a & b & c & d \\ a & c & b & d \end{pmatrix}, \quad \begin{pmatrix} a & b & c & d \\ d & b & c & a \end{pmatrix}$$

todas biunívocas. Analogamente, as correspondências $x \curvearrowright x\varphi a$, $x \curvearrowright x\varphi b$, $x \curvearrowright x\varphi c$, $x \curvearrowright x\varphi d$ são as aplicações

$$\begin{pmatrix} a & b & c & d \\ b & c & a & d \end{pmatrix}, \quad \begin{pmatrix} a & b & c & d \\ a & d & c & b \end{pmatrix}, \quad \begin{pmatrix} a & b & c & d \\ d & a & b & c \end{pmatrix}, \quad \begin{pmatrix} a & b & c & d \\ c & b & d & a \end{pmatrix}$$

também todas biunívocas. Ora isto significa, por um lado, que, no quadro dos resultados da operação, *cada um dos elementos do conjunto figura uma única vez em cada linha e uma única vez em cada coluna*; e significa, por outro lado, que a operação é *reversível* e, portanto, o grupóide é um quase-grupo.

b	a	d	c
c	d	a	b
a	c	b	d
d	b	c	a

Chama-se *quadrado latino* todo o quadro, como o anterior, formado por símbolos dispostos num certo número de linhas e num igual número de colunas, de tal modo que cada um dos elementos designados por esses símbolos seja indicado uma única vez em cada linha e uma única vez em cada coluna.

Em todas as tabelas dos quase-grupos atrás referidos vemos quadrados latinos (os quadros dos resultados). *Será sempre assim? E a recíproca será também verdadeira?*

Aqui fica o seguinte problema para os melhores alunos:

Provar que o grupóide definido por uma tabela é um quase-grupo, se e só se o quadro dos resultados for um quadrado latino.

Sugestão: provar primeiro que, num grupóide (A, Θ) a operação Θ é reversível, sse são verificadas as duas condições: 1) para todo o $x_0 \in A$, a correspondência $y \curvearrowright x_0 \Theta y$ é uma aplicação biunívoca de A sobre A; 2) para todo o $y_0 \in A$, a correspondência $x \curvearrowright x \Theta y$ é uma aplicação biunívoca de A sobre A.

NOTA. A teoria dos quadrados latinos (e, portanto, a dos quase-grupos) é fundamental em métodos estatísticos, relativos ao planeamento de experiências científicas (no campo da biologia, da medicina, da agronomia, etc.). A teoria dos quase-grupos tem, ainda, outras aplicações.

21. **Módulos.** Chama-se *módulo* todo o grupo aditivo, em que a adição é comutativa. Por exemplo, são módulos os conjuntos Z, $(Q$ e IR (relativamente à adição usual), mas não os conjuntos IN, $(Q^+$ e IR^+ (estes são apenas *semimódulos*). Outro exemplo de módulo é o grupóide a que chamámos 'Bailado das Horas'.

Por tradução da linguagem multiplicativa em linguagem aditiva os teoremas e definições dos n.os 14, 15 e 16 fornecem vários teoremas e definições em módulos.

Assim, seja M um módulo. Então, dados dois elementos a,b quaisquer de M existe sempre um e um só elemento x de M tal que

$$a + x = x + a = b$$

e que é $x = b + (-a)$. Este elemento chama-se *diferença entre b e a* e representa-se por $b-a$; em particular $-a = (0 - a$. A operação $(b,a) \curvearrowright b-a$ chama-se subtracção (*b* o aditivo e *a* o subtractivo).

Assim, subtrair a um elemento outro elemento equivale a adicionar ao primeiro o simétrico do segundo. Por exemplo, subtrair a 5 o número 7 equivale a *adicionar* a 5 o número -7.

Por sua vez, do teorema 2 do n.º 14, vem:

$$-(a+b) = (-a) + (-b) = -a-b, \quad \forall\, a, b \in M.$$

Por outro lado, a noção de '*potência* a^n' dá lugar à noção de '*produto* na', para todo o $n \in Z$ e $a \in M$. Como '1' se traduz por '(0' e 'inverso' por 'simétrico', teremos:

$a^0 = 1$ traduz-se por $\boxed{0 \cdot a = (0}$ (DEFINIÇÃO)

$a^{-n} = (a^n)^{-1}$ traduz-se por $\boxed{(-n)a = -(na)}$ (DEFINIÇÃO)

Por sua vez as propriedades das potências

$$a^{m+n} = a^m \cdot a^n \quad , \quad (ab)^n = a^n b^n \quad , \quad (a^n)^m = a^{mn}$$

traduzem-se, respectivamente, nas seguintes:

1) $(m+n)a = ma + na$ *(distributividade à esquerda)*

2) $n(a+b) = na + nb$ *(distributividade à direita)*

3) $m(na) = (mn)a$ *(associatividade)*

sendo *m,n* elementos quaisquer de *Z* e *a,b* elementos quaisquer de M.

NOTA: Não esquecer que, na propriedade 2), intervém a comutatividade da adição (ver teorema II do n.º 9).

Em particular M pode ser o próprio módulo *Z*. Neste caso, as definições

$$0 \cdot a = 0, \quad (-n)a = -(na)$$

fornecem as regras usuais da multiplicação em *Z*. Por exemplo:

$$(-3) \times 5 = -(3 \times 5) = -15,$$

$$(-3) \times (-5) = -[3 \times (-5)] = -(-15) = 15, \text{ etc.}$$

Estas regras foram, pois, escolhidas de modo que se mantivessem as propriedades anteriores, em especial a distributividade.

22. **Potências de expoente irracional dum número positivo (estudo intuitivo).** A teoria dos números reais será feita com rigor num outro capítulo. Entretanto, convém introduzir mais algumas noções referentes a números reais, *de modo intuitivo,* como se tem feito em anos anteriores. Só mais tarde trataremos de as apresentar com rigor.

Em tudo o que se segue, vamos supor que a *é um número real* > 0 *(isto é,* $a \in \mathbb{R}^+$*) e diferente de* 1.

Posto isto, demonstra-se o seguinte teorema (1):

Se $r > s$, *tem-se* $a^r > a^s$ *ou* $a^r < a^s$, *conforme* $a > 1$ ou $a < 1$.

Mais sugestivamente, este facto pode ser assim enunciado:

Quando o expoente duma potência a^x *aumenta, a potência aumenta se* $a > 1$ *e diminui se* $a < 1$.

Estamos aqui a supor que x só toma valores racionais (positivos, negativos ou nulo), *pois que, até agora, só definimos 'potência de expoente racional'*. Pois bem, a noção de potência de expoente irracional de *a* deverá ser definida *de modo que a propriedade anterior continue a ser verdadeira.*

Consideremos, por exemplo, a expressão $10^{\sqrt{3}}$. Que significado atribuir-lhe?

O número $\sqrt{3}$ é irracional; mas nós sabemos achar tantos algaris-

---

(1) A demonstração, dispensável nesta fase intuitiva, poderá ser vista no *Compêndio de Álgebra, 7.º ano,* Cap. XII, n.º 2 — (Ver nota da pág. 48 — N. do E.)

mos decimais, quantos quisermos, da dízima infinita que representa este número. Assim, até à 5.ª ordem decimal, temos:

$$\sqrt{3} = 1{,}73205\ldots$$

Esta dízima fornece uma sucessão de valores aproximados *por defeito* e uma sucessão de valores aproximados *por excesso* do número irracional $\sqrt{3}$:

(1) 1,7; 1,73; 1,732; 1,7320; 1,73205; ...

(1') 1,8; 1,74; 1,733; 1,7321; 1,73206; ...

A cada uma destas sucessões vai corresponder uma sucessão de potências de 10 de *expoente racional:*

(2) $10^{1,7}$, $10^{1,73}$, $10^{1,732}$, $10^{1,7320}$, $10^{1,73205}$, ...

(2') $10^{1,8}$, $10^{1,74}$, $10^{1,733}$, $10^{1,7321}$, $10^{1,73206}$, ...

Como se trata de expoentes racionais, já conhecemos o significado destas expressões. Por exemplo (1):

$$10^{1,732} = 10^{\frac{1732}{1000}} = \sqrt[1000]{10^{1732}}$$

Ora, cada termo da sucessão (1) é inferior (ou igual) ao termo seguinte. Logo, em virtude da propriedade anterior, o mesmo acontece com a sucessão (2). Por sua vez, cada termo da sucessão (1') é superior (ou igual) ao termo seguinte e, portanto, o mesmo acontece com a sucessão (2').

---

(1) Sobre a maneira de calcular estas expressões, ver a NOTA no fim deste número.

Mas $\sqrt{3}$ é superior a *todos* os termos da sucessão (1) e inferior a *todos* os termos da sucessão (1'):

$$1{,}7 < 1{,}73 < 1{,}732 < \ldots < \sqrt{3} < \ldots < 1{,}733 < 1{,}74 < 1{,}8$$

Logo, para que continue a ser válida a referida propriedade, o valor de $10^{\sqrt{3}}$ *deverá ser um número superior a todos os termos da sucessão* (2) *e inferior a todos os termos da sucessão* (2'), *isto é:*

$$10^{1,7} < 10^{1,73} < \ldots < 10^{\sqrt{3}} < \ldots < 10^{1,74} < 10^{1,8}$$

Mas, prova-se que *existe um único número real* L nestas condições, isto é, compreendido entre as duas sucessões, porque a diferença entre os termos da segunda e os da primeira se pode tornar inferior a qualquer unidade decimal, isto é, inferior a 0,1, a 0,01, a 0,001, etc. Logo, $10^{\sqrt{3}}$ só pode ser esse número L. Tomaremos, pois:

$$10^{\sqrt{3}} = \mathrm{L} \quad \text{(por definição)}.$$

No seguinte quadro indicam-se os sucessivos valores de $10^{\sqrt{3}}$, por defeito e por excesso, correspondentes aos valores aproximados de $\sqrt{3}$ considerados:

x	10^x
1,7	50,119 ...
1,73	53,103 ...
1,732	53,951 ...
1,7320	53,951 ...
1,73205	53,957 ...

x	10^x
1,8	63,095 ...
1,74	54,955 ...
1,733	54,085 ...
1,7321	53,963 ...
1,73206	53,958 ...

Como se vê, tem-se $53{,}957 < 10^{\sqrt{3}} < 53{,}958$ e não sabemos ainda, ao certo, se o algarismo das milésimas, da dízima representativa

de $10^{\sqrt{3}}$, é 7 ou 8. Só ficamos, portanto, a conhecer essa dízima, por enquanto, até à ordem das centésimas:

$$10^{\sqrt{3}} = 53{,}95 \ldots$$

Se quiséssemos determinar outros algarismos dessa dízima, teríamos de tomar valores de x mais próximos de $\sqrt{3}$ e calcular os valores correspondentes de 10^x, com mais algarismos decimais.

Posto isto, as considerações que fizemos para a expressão $10^{\sqrt{3}}$ entendem-se, *mutatis mutandis,* para qualquer expressão da forma a^u em que *a* é um número positivo diferente de 1 e *u* um número irracional positivo. Se $a < 1$, a única diferença essencial está em que os valores aproximados da potência variam em sentido inverso dos valores do expoente, segundo a propriedade anterior.

Finalmente, se *u* é um número irracional negativo, o seu simétrico, $u' = u$, é um número positivo, e definiremos a potência a^u como se fez para o caso dos números racionais negativos:

$$a^u = a^{-u'} = \frac{1}{a^{u'}}$$

NOTA. O cálculo dos valores de a^x para valores racionais de x obriga a fazer extracções de raiz de índices cada vez maiores, o que se torna muito laborioso por processos elementares. Havemos de ver mais tarde que, para o cálculo de sucessivos valores aproximados, poderíamos limitar-nos a sucessivas extracções de raiz quadrada. Por outro lado, veremos também como o uso de tábuas de logaritmos permite obter rapidamente raízes de qualquer índice, porém com um grau do aproximação limitado pelo número de decimais de tábua utilizada.

23. **Função exponencial de base** a. Continuamos a supor que *a* é um número positivo diferente de 1. Com as definições anteriores, a função $x \curvearrowright a^x$ (*função exponencial de base* a) acabou por ser estendida ao conjunto $\mathbb{R}$ de *todos* os números reais. Recordemos que esta função, primeiro definida em $\mathbb{N}$, tinha sido estendida a $\mathbb{Z}$

(ver n.º 16) e depois a (Q (ver n.º 18). Por exemplo, com $a = 2$, tem-se em Z a função:

$$\begin{array}{ccccccccccccc} \ldots, & -n, & \ldots, & -3, & -2, & -1, & 0, & 1, & 2, & 3, & \ldots, & n, & \ldots \\ & \downarrow & & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & & \downarrow & \\ \ldots, & \frac{1}{2^n}, & \ldots, & \frac{1}{8}, & \frac{1}{4}, & \frac{1}{2}, & 1, & 2, & 4, & 8, & \ldots, & 2^n, & \ldots \end{array}$$

Passando depois a (Q, tem-se, por exemplo, no intervalo [2,3]:

$$\begin{array}{ccccccc} 2 & 2{,}1 & 2{,}2 & 2{,}3 & \ldots & 2{,}9 & 3 \\ \downarrow & \downarrow & \downarrow & \downarrow & & \downarrow & \downarrow \\ 4 & \sqrt[10]{2^{21}} & \sqrt[10]{2^{22}} & \sqrt[10]{2^{23}} & \ldots & \sqrt[10]{2^{29}} & 8 \end{array}$$

e, analogamente, para outros expoentes racionais. Finalmente, passa-se a $\mathbb{R}$, como foi indicado no número anterior. Então 2^x (ou mais geralmente a^x) passa a representar uma aplicação do *conjunto* $\mathbb{R}$ *no conjunto* $\mathbb{R}^+$, visto que, como se vê, os valores das potências de *a* são sempre números positivos.

Mais ainda, prova-se que todas as propriedades usuais das potências se mantêm com a definição de potência de expoente irracional. Assim, tem-se:

$$\left.\begin{array}{ll} \text{I.} & a^u \cdot a^v = a^{u+v} \\ \text{II.} & a^u \cdot b_u = (ab)^u \\ \text{III.} & (a^u)^v = a^{uv} \end{array}\right\} \quad \forall\ u, v \in \mathbb{R};\ a, b \in \mathbb{R}^+$$

Finalmente, prova-se que é mantida, efectivamente, a propriedade indicada no número anterior, que serviu de fundamento à definição de potência de expoente irracional. Essa propriedade pode, agora, enunciar-se do seguinte modo:

A função a^x *é crescente ou decrescente conforme* $a > 1$ *ou* $a < 1$.

É claro que também podemos definir a^x com $a = 1$. Mas, neste caso, tem-se $a^x = 1$, $\forall\, x \in \mathbb{R}$.

Quanto à representação gráfica destas funções, ver *Compêndio de Álgebra, 7.º ano,* pág. 238 (1).

24. **Função logarítmica na base** a. Continuamos a supor *a* positivo $\neq 1$. Já vimos que a expressão a^x representa uma aplicação de $\mathbb{R}$ *em* $\mathbb{R}^+$. Ora, essa aplicação é *bijectiva,* isto é, uma *aplicação biunívoca de* $\mathbb{R}$ *sobre* $\mathbb{R}^+$. É isto o que se afirma no seguinte

TEOREMA: *Para todo o número positivo* y, *existe um (e um só) número real* x, *tal que*

$$a_x = y \quad (\text{supondo } a > 0,\ a \neq 1)$$

O mesmo pode ser expresso simbolicamente como se segue:

$$\forall\, y \in \mathbb{R}^+,\ \exists^1\, x \in \mathbb{R} : a^x = y$$

Para dar uma ideia de como se pode demonstrar este teorema, suponhamos, por exemplo, $a = 10$, $y = 2$. Procura-se, pois, um número x tal que

(1) $$10^x = a$$

Comecemos por notar que

$$10^0 < 2 < 10^1$$

Então deverá ser $10^0 < 10_x < 10^1$, em virtude de (1), e portanto $0 < x < 1$. (*Porquê?*)

Experimentando, agora, os expoentes 0,1; 0,2; ... 0,9, vê-se que

$$10^{0,3} < 2 < 10^{0,4}$$

(1) Ver nota da pág. 48.

Para o reconhecer, basta elevar os três membros à 10.ª potência, o que dá

$$1000 < 2^{10} \ (= 1024) < 10\,000$$

Então, deverá ser $10^{0,3} < 10^{x} < 10^{0,4}$ e, portanto:

$$0,3 < x < 0,4$$

Experimentando, agora, os expoentes 0,31; 0,32, ... vê-se, de modo análogo, que $10^{0,30} < 2 < 10^{0,31}$ e, portanto:

$$0,30 < x < 0,31$$

Procedendo assim, sucessivamente, podemos determinar tantos algarismos, quantos quisermos, duma dízima infinita

$$0,30103\ldots ,$$

que representa um número real λ. Ora, segundo as considerações do n.º 23, atendendo a que a função exponencial de base 10 é crescente (n.º 24), a potência 10^{λ} deverá estar situada entre os termos das duas sucessões:

$$10^{0,3},\ 10^{0,30},\ 10^{0,301},\ 10^{0,3010},\ 10^{0,30103},\ \ldots$$

$$10^{0,4},\ 10^{0,31},\ 10^{0,302},\ 10^{0,3011},\ 10^{0,30104},\ \ldots$$

Mas, o número 2 também está situado entre as duas sucessões. *Como só pode haver um número nessa situação, terá de ser, portanto:*

$$10^{\lambda} = 2$$

Portanto, o número x procurado existe e *só pode ser:*

$$\lambda = 0,30103\ldots$$

O teorema torna lícita a seguinte

DEFINIÇÃO: *Chama-se logaritmo dum número positivo* y *na base* a *(positiva* $\neq 1$*) o número real* x *tal que*

$$a^x = y$$

Escreve-se, então: $x = \log_a y$, isto é, $\log_a y = \iota_x(a^x = y)$.

Em conclusão:

A expressão a^x *define uma aplicação biunívoca de* $\mathbb{R}$ *sobre* $\mathbb{R}^+$ *cuja inversa é a função* $\log_a$. Ter-se-á pois (n.º 12, pág. 199, 1.º tomo):

$$a^{\log_a x} = x, \ \forall\, x \in \mathbb{R}^+; \ \log_a a^x = x, \ \forall\, x \in \mathbb{R}$$

Por exemplo, tem-se:

$$\log_4 64 = 3, \quad \text{visto que } 4^3 = 64$$

$$\log_9 \frac{1}{3} = -0{,}5, \quad \text{visto que } 9^{-0,5} = \frac{1}{\sqrt{9}} = \frac{1}{3}$$

Nestes exemplos, o logaritmo é um número racional. *Porém, os casos mais frequentes e de maior interesse são aqueles em que o logaritmo é um número irracional.* Por exemplo, prova-se que $\log_{10} 2$ (atrás considerado) é um número irracional, e analogamente para o logaritmo na base 10 de qualquer outro número inteiro que não seja uma potência de expoente inteiro de 10.

Notemos, ainda, o seguinte facto: por ser sempre

$$a^0 = 1, \quad a^1 = a,$$

tem-se, em virtude da definição:

$$\boxed{\log_a 1 = 0; \quad \log_a a = 1}$$

isto é: *o logaritmo de* 1 *é zero e o logaritmo da base é* 1, *qualquer que seja a base.*

• Designemos, agora, por f a função exponencial de base *a*, isto é, ponhamos:

$$f(x) = a^x \text{ (em } \mathbb{R})$$

Então f é uma aplicação biunívoca de $\mathbb{R}$ sobre $\mathbb{R}^+$ e a propriedade $a^{u+v} = a^u a^v$ escreve-se:

$$f(u+v) = f(u) \cdot f(v), \quad \forall\, u, v \in \mathbb{R}.$$

Ora, estes factos exprimem-se dizendo (n.os 10 e 11):

A função exponencial $x \curvearrowright a^x$ *é um isomorfismo do grupo aditivo* $\mathbb{R}$ *sobre o grupo multiplicativo* $\mathbb{R}^+$.

Assim, esta função traduz toda a linguagem aditiva de $\mathbb{R}$ na linguagem multiplicativa de $\mathbb{R}^+$. Por sua vez, do teorema I do n.º 11 e do que precede, resulta imediatamente:

A função $\log_a$ *é um isomorfismo do grupo multiplicativo* $\mathbb{R}^+$ *no grupo aditivo* $\mathbb{R}$.

Assim, a função logarítmica traduz toda a linguagem multiplicativa de $\mathbb{R}^+$ na linguagem aditiva de $\mathbb{R}$:

$$\left.\begin{aligned} &\log_a (u \cdot v) = \log_a u + \log_a v \\ &\log_a \frac{u}{v} = \log_a u - \log_a v \\ &\log_a u^v = v \log_a u \\ &\ldots \end{aligned}\right\} \forall\, u, v \in \mathbb{R}^+$$

Para complementos e exercícios sobre a função logarítmica (excepto no que se refere a limites e continuidade), ver *Compêndio de Álgebra, 7.º ano,* Cap. XII, n.os 9 e seguintes (1).

Sobre logaritmos decimais, ver Cap. XXIII do mesmo *Compêndio.*

(1) Ver nota da pág. 48.

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 μ um número inteiro maior que 1. Daqui por diante, designaremos por A_μ um conjunto constituído por μ 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 μ 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_μ 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 μ, A_μ *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 $'\exists x,\ x \neq (0 \wedge x^2 = (0'$ 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

z	u	i	j
↓	↓	↓	↓
$(\overline{0},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{0},\overline{1})$	$(\overline{1},\overline{0})$

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_μ, 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* μ *seres distintos.* Em particular, podemos adoptar a seguinte interpretação: $\overline{0}$ é o conjunto dos múltiplos de μ, $\overline{1}$ é o conjunto dos inteiros que divididos por μ 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

$$(a_0 + b_0)x^n + (a_1 + b_1)x^{n-1} + \ldots + (a_n + b_n)$$

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, ..., n; k = 0, ..., 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):

$$\begin{array}{l|l} q_0 x^{n-1} + q_1 x^{n-2} + q_2 x^{n-3} + \ldots + q_{n-2} x + q_{n-1} & x - \alpha \\ \hline q_0 x^n + q_1 x^{n-1} + q_2 x^{n-2} + \ldots + q_{n-1} x & \\ - \alpha q_0 x^{n-1} - \alpha q_1 x^{n-2} - \ldots - \alpha q_{n-2} x - \alpha q_{n-1} & \\ \hline q_0 x^n + (q_1 - \alpha q_0) x^{n-1} + (q_2 - \alpha q_1) x^{n-2} + \ldots + (q_{n-1} - \alpha q_{n-2}) x - \alpha q_{n-1} & \end{array}$$

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 $q_0, q_1, \ldots, q_{n-1}$ 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
α		αq_0	αq_1	...	αq_{n-2}	αq_{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 α, 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* α.

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* α *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* μ *não é primo,* A_μ *não é um corpo* (por ter divisores de zero). Veremos mais tarde que a recíproca também é verdadeira e que portanto:

A_μ *é um corpo, sse* μ *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):

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

---

(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:

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

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* α. 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

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

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

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

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

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

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

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

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

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

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 Δ 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 Δ ter raiz quadrada. Mas, se $\Delta = 0$, existe uma raiz quadrada de Δ (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* Δ *tem raiz quadrada em* K *e se além disso* $\Delta \neq 0$. *A equação não terá solução em* K, *se* Δ *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** $\mathbb{R}$. Suponhamos agora em particular que o corpo K considerado é $\mathbb{R}$ e continuemos a designar por Δ o discriminante do polinómio do 2.º grau $ax^2 + bx + c$, isto é: $\Delta = b^2 - 4ac$, com $a, b, c \in \mathbb{R}$, $a \neq 0$. 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* Δ, 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 Δ 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.

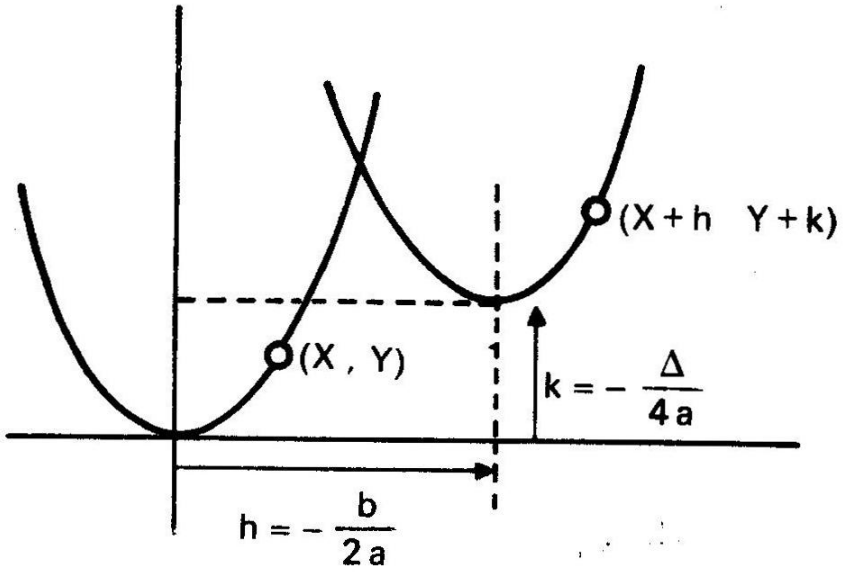
ou seja, pondo $b^2-4ac = \Delta$:

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

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 IR):

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

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

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 α *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 α 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 α 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 α é um número exterior ao intervalo das raízes, pode ainda interessar saber se α 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* α *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 (α,β) 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 (α, β) 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:

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

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:

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

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:

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

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:

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

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:

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

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

* * *

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 $\Delta \neq 0$:

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

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* α. *Uma* das raízes cúbicas de α, 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 $\mathbb{R}$, 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 α e β 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 α *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* α, *qualquer que seja a raiz cúbica de* α *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) $$a = a' \wedge b = b' \Rightarrow a + bi = a' + b'i$$

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

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 α, β *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 α é conjugado de si mesmo, sse α 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 complexos:

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

Como $\mathbb{C}$ é um corpo, existe o quociente de α por β, 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:

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

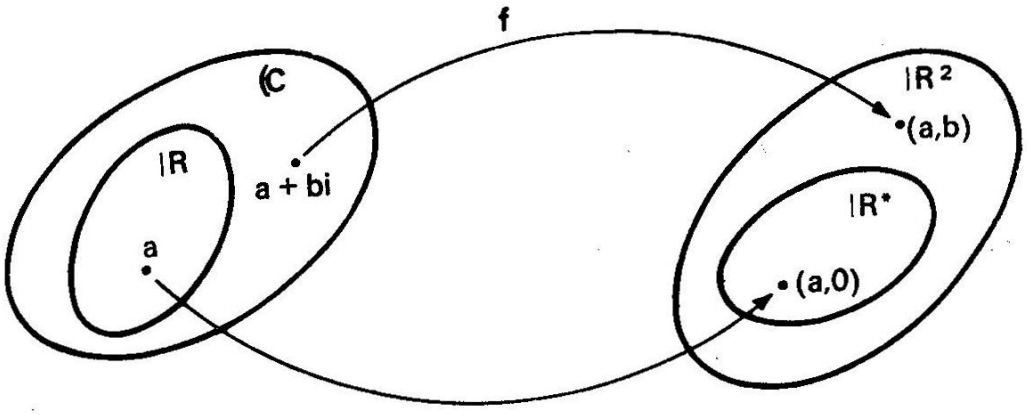
$$f[(a + bi) \cdot (c + di)] = f[(ac - bd) + (ad + bc)i]$$
$$= (ac - bd, ad + bc) = (a, b) \cdot (c, d) =$$
$$= f(a + bi) \cdot f(c + di)$$

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* $\mathbb{C}$ *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 ∈ $\mathbb{R}$:

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

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 $\mathbb{C}$ abstraíremos, em geral, da natureza dos seus elementos, para só atender às regras de cálculo que são válidas em $\mathbb{C}$.

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:

$$\left.\begin{aligned} (a, b) + (c, d) &= (a + c,\ b + d) \\ (a, b) \cdot (c, d) &= (ac,\ bd) \end{aligned}\right\} \quad \forall\, a, b, c, d \in \mathbb{R}$$

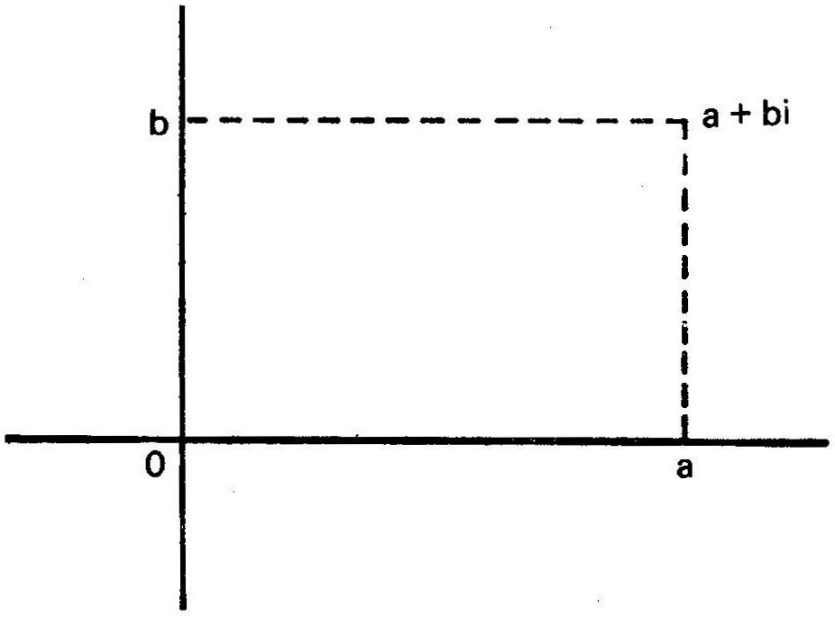
(1) Deste modo, os números imaginários têm existência tão real como os números reais, ao contrário do que podem sugerir as designações 'número real' e 'número imaginário'. Na verdade, estas designações foram introduzidas historicamente, porque, a princípio, se admitia, de certo modo, que só os números 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:

$$(3, 0) \cdot (0, 5) = (0, 0), \text{ sendo } (3, 0) \neq (0, 0) \text{ e } (0, 5) \neq (0, 0)$$

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 θ.

---

(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 Δ não tem raiz quadrada em $\mathbb{R}$. *Mas acabámos de ver que, neste caso, Δ 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* α *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:

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

Designemos a segunda por ε. Pode verificar-se directamente que ε^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 α, 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 α. *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 α, 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 α 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* θ *uma das raízes da equação* $x^3 = \overline{4}$ *em* K.

Uma das soluções do problema é constituída precisamente pelos polinómios em θ 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 μ 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:

$$a_p = (-1)^p a_o S_p, \text{ donde:}$$

$$(2) \qquad \boxed{S_p = (-1)^p \frac{a_p}{a_o}, \text{ para } p = 1, 2, \ldots, n}$$

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.*

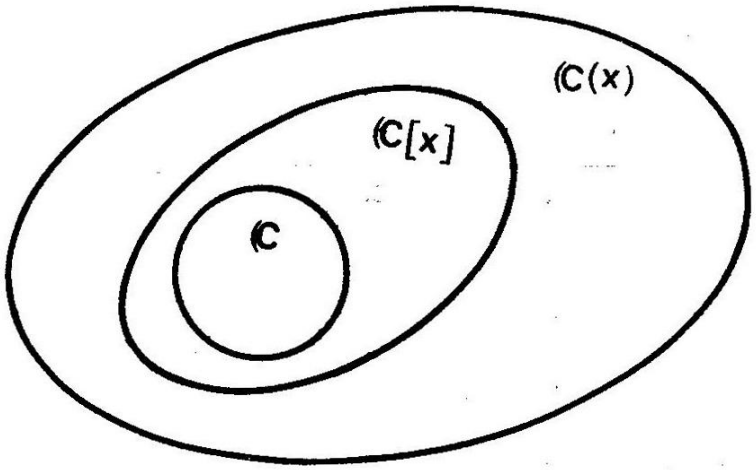
Podemos, com base neste teorema, identificar (C[x] ao referido anel das funções racionais inteiras, de modo que *ficará* (C[x] *a ser um subanel do corpo* (C(x). Como, por sua *vez*, o corpo (C é isomorfo ao subcorpo do anel (C[x] constituído pelos polinómios de grau zero, vemos que:

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) $$y = \frac{x+1}{x+2} \quad , \quad \text{sendo } \mathbb{C} \text{ o universo.}$$

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

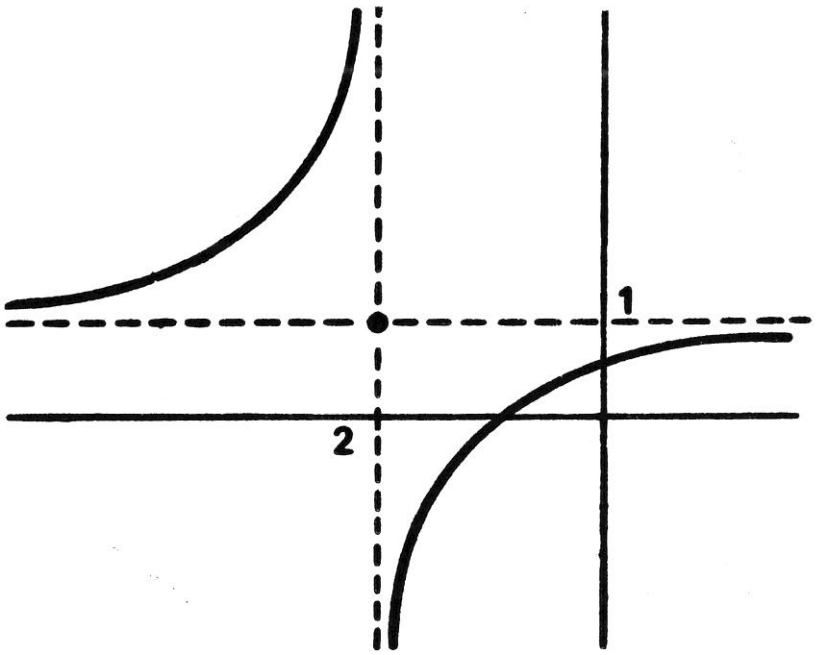
$$y - 1 = Y, \quad x + 2 = X$$

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 $(\mathcal{L}, +, \cdot)$ e $(\mathcal{C}, +, \cdot)$ 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:*

I) $a \cdot 0 = 0$, II) $a + 1 = 1$, $\forall a \in A$

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,*

$$\tilde{\tilde{a}} = a \quad , \quad \forall a \in A$$

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)

(1) $$x + y = 1 \wedge xy = 0$$

---

(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, $\cdot$) *e deste sobre aquele. Poderíamos também dizer que é um isomorfismo da álgebra de Boole* (A, +, $\cdot$) *sobre a álgebra de Boole* (A, $\cdot$, +) *(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: $a + x = 0 \Rightarrow a \cdot a + a \cdot x = 0$.)

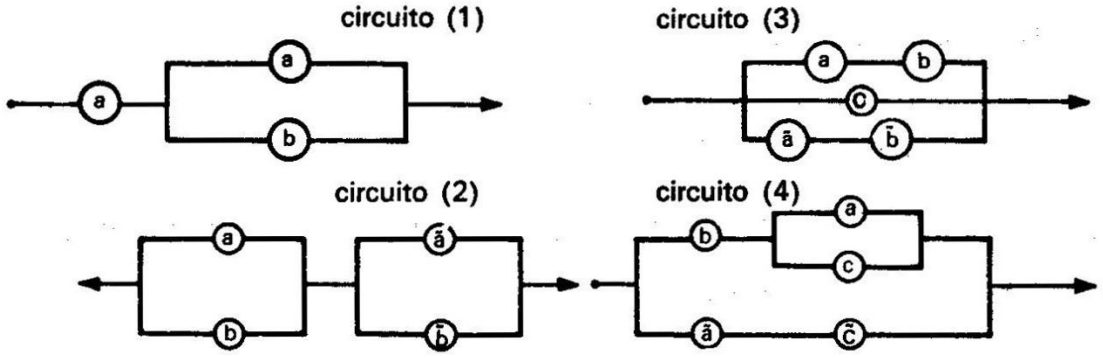
III. Prove que, em qualquer álgebra de Boole, $\tilde{a}$ nunca é $-a$ nem a^{-1}.

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 $\tilde{1} = 0$:

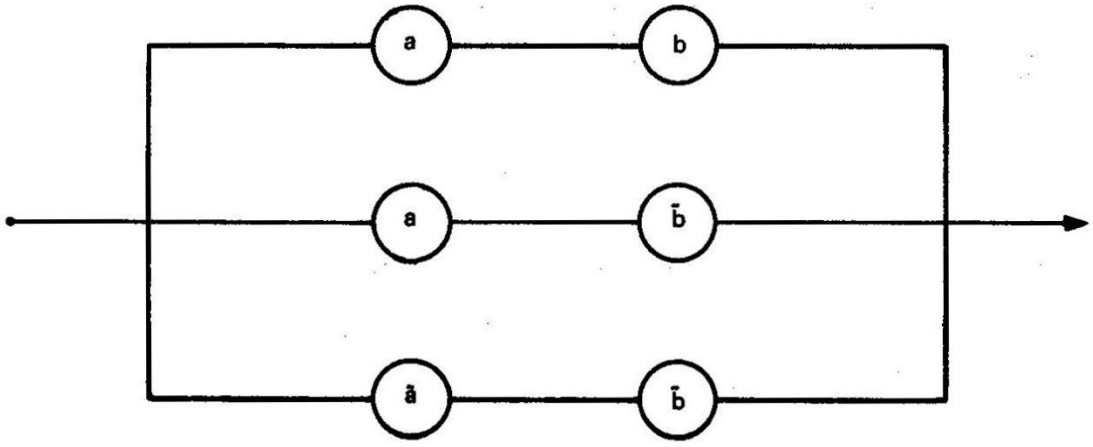


VI. Indicar um circuito para cada polinómio de Boole:

(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:

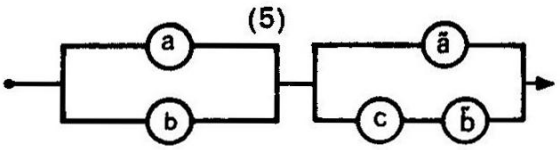
P = possibilidade de fumar nesta casa,
F = haver fósforos utilizáveis,
I = haver isqueiro utilizável,
C_1 = haver cigarros,
C_2 = haver charutos,
C_3 = haver cachimbo,
T = haver tabaco,
D = haver atmosfera deflagrante.

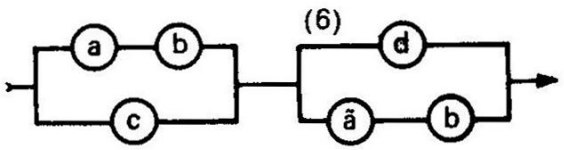
Trace o diagrama de um circuito que dê P como função das restantes variáveis, *utilizando, neste caso, circuitos elementares de conjunção, disjunção e negação, como os que foram considerados no Capítulo I.*

RESPOSTAS

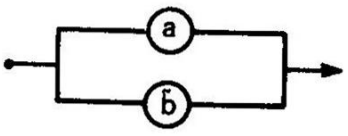
V. (3) $ab+\tilde{a}\,\tilde{b}+c$, (4) $b(a+c)+\tilde{a}\,\tilde{c}$

VI.





VII. $a\tilde{b}+a\tilde{b}+\tilde{a}\tilde{b} \equiv a+\tilde{b}$

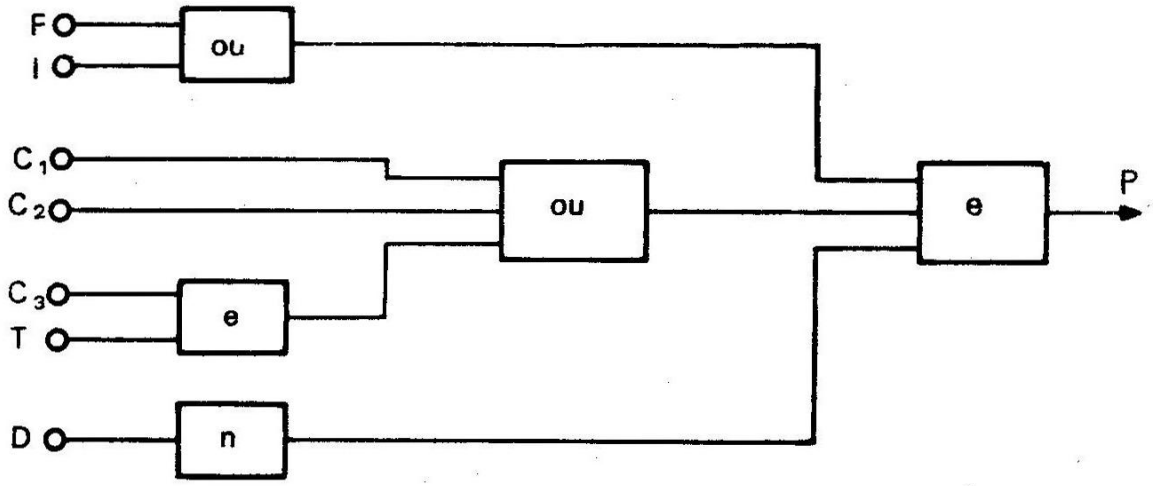


VIII. $P = ABC + ABD + \tilde{A}B\tilde{C} + CD + B\tilde{D}$

Note que $ABD+B\tilde{D}=AB+B\tilde{\tilde{D}}\supset ABC$, donde $P=AB+\tilde{A}B\tilde{C}+CD+B\tilde{\tilde{D}}$. Por outro lado $AB+\tilde{A}B\tilde{C}=AB+B\tilde{C}$, donde $P=AB+B\tilde{C}+CD+B\tilde{\tilde{D}}$. Ora $B\tilde{C}+CD=BD+CD$ e $BD+B\tilde{\tilde{D}}=B\supset AB$. 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. $P = (F + I) \cdot (C_1 + C_2 + C_3T) \cdot \tilde{\tilde{D}}$



CAPÍTULO VII

INTRODUÇÃO À ESTATÍSTICA E AO CÁLCULO DAS PROBABILIDADES

1. **Lógica de atributos e lógica de conjuntos.** Já vimos que toda a propriedade (ou atributo) num dado universo U define um conjunto, que é o *conjunto de todos os indivíduos que têm essa propriedade*. Por exemplo, seja U o conjunto dos portugueses existentes numa dada época e sejam *e, c, s, r, a, m, p, b*, respectivamente, os atributos *estudante, casado, solteiro, ruivo, algarvio, menor de* 25 *anos, poeta, com bigode*. Cada um destes atributos define, no universo U, um conjunto; designemos, respectivamente, por E, C, S, R, A, M, P, B os conjuntos assim definidos. Deste modo, E é o *conjunto dos estudantes portugueses,* C o *conjunto dos portugueses casados,* etc. na referida época (1).

Também vimos como as operações lógicas de *conjunção, disjunção* e *negação* sobre atributos se traduzem, respectivamente, nas

---

(1) Alguns destes conjuntos, como por exemplo R, não estão na realidade definidos. Tratando-se dum inquérito estatístico, relativo a indivíduos ruivos, haverá casos de dúvida, em que o autor do inquérito pode incluir um dado indivíduo no conjunto R ou no seu complementar, de modo *mais ou menos* arbitrário.

operações lógicas de *intersecção, reunião e complementação* sobre conjuntos. Trata-se, apenas, de duas linguagens ou pontos de vista equivalentes: o *ponto de vista da compreensão* (relativo a atributos) e o *ponto de vista da extensão* (relativo a conjuntos).

Assim, tornando ao exemplo anterior, sabemos que os referidos atributos se podem associar entre si de diferentes modos por meio das operações lógicas fundamentais, dando lugar a novos atributos. Por exemplo os atributos

$$e \wedge c \ , \ e \vee m \ , \ \sim s, \ e \wedge \sim s \ , \ e \wedge a \wedge m \ , \ p \vee b \ , \ \sim p \wedge \sim b,$$

que, em linguagem comum, se traduzem pelas expressões 'estudante casado', 'estudante ou menor de 25 anos', 'não solteiro', 'estudante não solteiro', 'estudante algarvio, menor de 25 anos', 'poeta ou com bigode', 'não poeta e sem bigode', definem respectivamente os conjuntos

$$E \cap C \ , \ E \cup M \ , \ \complement S \ , \ E \cap \complement S \ , \ E \cap A \cap M \ , \ P \cup B \ , \ \complement P \cap \complement B$$

que o aluno facilmente pode identificar (convém recorrer a diagramas de Venn).

Também vimos que a implicação entre atributos se traduz na inclusão entre conjuntos. Por exemplo, no universo considerado, o atributo c *implica* o atributo $\sim$s (não lhe sendo, contudo, equivalente); por isso, o conjunto C *está contido* no conjunto $\complement$S. Assim, a implicação $c \Rightarrow \sim s$ traduz-se na inclusão $C \subset \complement S$.

Por sua vez, a equivalência entre atributos traduz-se na *identidade* entre conjuntos. Por exemplo:

'$\sim(p \vee b) \Leftrightarrow \sim p \wedge \sim b$' traduz-se por '$\complement(P \cup B) = \complement P \cap \complement B$'

Finalmente, vimos que, deste modo, a um *atributo universal* corresponde o *universo* e a um *atributo impossível* corresponde o *conjunto vazio;* e que dois *atributos incompatíveis* definem dois *conjuntos disjuntos.* Por exemplo, o atributo $s \vee \sim s$ é universal (portanto $S \cup \complement S = U$), o atributo $c \wedge s$ é impossível (ou seja $C \cap S = \varnothing$), os atributos c, s são incompatíveis (ou seja, os conjuntos C e S são disjuntos), etc.

2. **Terminologia e notações.** Daqui por diante será cómodo chamar *'produto lógico'* quer à conjunção (de atributos) quer à intersecção (de conjuntos), *'soma lógica'* quer à disjunção (de atributos) quer à reunião (de conjuntos) e *'contrário'* quer à negação (de atributos) quer ao complementar (de conjuntos). Ao mesmo tempo, dados dois atributos α, β ou dois conjuntos A, B, designaremos por

$$\alpha\beta, \quad AB, \quad \alpha + \beta, \quad A + B, \quad \tilde{\alpha}, \quad \tilde{A}\ (^1)$$

respectivamente, os produtos lógicos de α por β e de A por B, as somas lógicas de α com β e de A com B, e os contrários de α e de A (o símbolo $\tilde{\alpha}$ pode ler-se 'não α' e a expressão $\alpha + \beta$ pode continuar a ler-se 'α ou β').

Tornando ao exemplo do número anterior será fácil, agora, reconhecer os significados das expressões

$$ec, \quad e + m, \quad \tilde{s}, \quad e\tilde{s}, \quad e\,a\,m, \quad p + b, \quad \tilde{p}\,\tilde{b}$$
$$EC, \quad E + M, \quad \tilde{S}, \quad E\tilde{S}, \quad E\,A\,M, \quad P + B, \quad \tilde{P}\tilde{B}$$

Se convencionarmos considerar como *idênticos* dois atributos quando são equivalentes, é manifesto que o conjunto dos atributos

---

(1) O autor representa, aqui, $\complement A$ por $\tilde{A}$ — (N. do E.).

definidos num dado universo U é uma álgebra de Boole isomorfa à álgebra dos subconjuntos de U. Designaremos, neste caso, por **1** o atributo universal e por (0 o atributo impossível.

3. **Frequência absoluta de um atributo numa população.** Em vez de 'universo' usa-se, muitas vezes, em estatística o termo 'população', com significado idêntico. Assim, um conjunto de pessoas, um conjunto de árvores, um conjunto de livros, um conjunto de lâmpadas eléctricas, etc., etc. podem ser tomados como *populações* (ou *universos*) em diversas situações.

DEFINIÇÃO. *Chama-se frequência absoluta dum atributo* α *numa população finita* U *o número de indivíduos que possuem o atributo* α *(ou seja o número de elementos do conjunto* A *definido por* α *em* U).

Assim, *frequência absoluta do atributo* é o mesmo que *cardinal do conjunto* A *correspondente* — número que convencionámos representar pela notação $\#$ A. Representaremos pela notação $\Phi(\alpha)$ a frequência absoluta de α. É claro que se tem:

$$0 \leqslant \Phi(\alpha) \leqslant \# \, U$$

Tornando ao exemplo do n.º 1 vemos que $\Phi(e)$ é a frequência absoluta do atributo *estudante* na população dos portugueses da referida época, isto é, *o número total de estudantes portugueses existentes nessa época.*

Atendendo às considerações dos dois números anteriores, bem como ao que foi estabelecido no Cap. III, n.º 2, (pág. 137, 1.º tomo), vemos que

Se dois atributos α, β *são incompatíveis, a frequência absoluta do atributo* $\alpha+\beta$ *é igual à soma das frequências absolutas dos atributos* α, β *na população considerada; isto é, em fórmula*

$$\Phi(\alpha + \beta) = \Phi(\alpha) + \Phi(\beta), \quad \textit{se} \quad \alpha, \beta \ \textit{são incompatíveis}$$

Com efeito, se α, β, são incompatíveis, os conjuntos A, B correspondentes são disjuntos e, então, a frequência absoluta de $\alpha + \beta$ (ou seja o número de elementos de $A + B$) é a soma das frequências absolutas de α e de β (ou seja a soma dos cardinais de A e B).

É claro que a propriedade anterior se estende a um número qualquer (finito) de atributos, incompatíveis entre si dois a dois.

Se os atributos α, β, não são necessariamente incompatíveis, tem-se a seguinte propriedade que resulta do estabelecido no Cap. III, n.º 12 (pág. 157, 1.º tomo):

$$\Phi(\alpha + \beta) = \Phi(\alpha) + \Phi(\beta) - \Phi(\alpha\,\beta)$$

Assim, tornando ao exemplo do número I, vê-se que

$$\Phi(e + s) = \Phi(e) + \Phi(s) - \Phi(e\,s)$$

isto é: a frequência absoluta do atributo *estudante ou solteiro,* no universo dos portugueses, é a soma das frequências absolutas do atributo *estudante* e do atributo *solteiro,* menos a frequência do atributo *estudante solteiro,* no referido universo.

No caso geral, de *n* atributos quaisquer $a_1,\ldots,a_n$, num universo U, tem-se um novo aspecto da FÓRMULA DE DANIEL DA SILVA (pág. 159, 1.º tomo), com atributos no lugar de conjuntos.

EXERCÍCIO. Sendo α um atributo qualquer numa população finita U, indique condições equivalentes às seguintes: 1) $\Phi(\alpha)=0$, 2) $\Phi(\alpha) = \#\, U$.

4. **Frequência relativa.** Chama-se *frequência relativa* dum atributo α numa população finita U ao quociente da frequência absoluta de α pelo número de elementos de U. Designaremos por $fr(\alpha)$ a frequência relativa de α. Então, se for $\nu = \Phi(\alpha)$ e $n = \#\, U$, será, por definição:

$$fr(\alpha) = \frac{\nu}{n}$$

Por exemplo, sabe-se que, numa cidade com 23 528 habitantes, 9 253 desses pertencem ao sexo masculino e os restantes 14 275 ao sexo feminino. Os dois últimos números são, pois, as frequências absolutas do sexo masculino e do sexo feminino na referida população. As frequências relativas dos mesmos atributos serão, *com aproximação até às centésimas:*

$$\frac{9\,253}{23\,528} \approx 0{,}39 \quad , \quad \frac{14\,275}{23\,528} \approx 0{,}61$$

Também podemos dizer, neste caso, que a frequência relativa do primeiro atributo é de 39 % e a do segundo é de 61%. Dum modo geral, se for ν a frequência absoluta dum atributo num universo finito U e n o cardinal de U, a *frequência relativa de α em percentagem,* neste universo, será:

$$fr(\alpha) = \frac{100\,\nu}{n}\ \%$$

Vejamos um outro exemplo. Num dado país, com 8 438 250 habitantes, 82 % dos habitantes têm cabelos castanhos ou pretos, 14 %

têm os cabelos louros e 4 % têm os cabelos ruivos. Serão, pois, 0,82, 0,14 e 0,04 as frequências relativas dos referidos atributos, *até às centésimas*. As respectivas frequências absolutas serão:

$$0{,}82 \times 8\,432\,250 \approx 6\,900\,000 \quad \text{(castanhos ou pretos)}$$

$$0{,}14 \times 8\,432\,250 \approx 1\,200\,000 \quad \text{(louros)}$$

$$0{,}04 \times 8\,432\,250 \approx 300\,000 \quad \text{(ruivos)}$$

Assim, da definição resulta que é sempre:

$$0 \leqslant \mathrm{fr}(\alpha) \leqslant 1,$$

tendo-se $\mathrm{fr}(\alpha) = 0$ *sse* α é impossível e $\mathrm{fr}(\alpha) = 1$ *sse* α é universal.

Do estabelecido no número anterior resulta o seguinte:

Se α e β são atributos incompatíveis, a frequência relativa de $\alpha+\beta$ é igual à soma das frequências relativas de α e β; isto é, em fórmula:

$$\mathrm{fr}(\alpha + \beta) = \mathrm{fr}(\alpha) + \mathrm{fr}(\beta), \text{ se } \alpha, \beta \text{ são incompatíveis.}$$

Com efeito, pondo $\# U = n$, vem (justifique):

$$\mathrm{fr}(\alpha+\beta) = \frac{\Phi(\alpha + \beta)}{n} = \frac{\Phi(\alpha) + \Phi(\beta)}{n} = \frac{\Phi(\alpha)}{n} + \frac{\Phi(\beta)}{n} = \mathrm{fr}(\alpha) + \mathrm{fr}(\beta)$$

Se α, β não são necessariamente incompatíveis, tem-se a fórmula mais geral (justifique):

$$\boxed{\mathrm{fr}(\alpha + \beta) = \mathrm{fr}(\alpha) + \mathrm{fr}(\beta) - \mathrm{fr}(\alpha\,\beta)}$$

No caso geral de n atributos quaisquer num universo finito, tem-se um novo aspecto da FÓRMULA DE DANIEL DA SILVA. Da propriedade anterior deduz-se o seguinte corolário:

A frequência relativa do atributo contrário de α *é* $1 - \mathrm{fr}(\alpha)$.

Em fórmula:

$$\mathrm{fr}(\tilde{\alpha}) = 1 - \mathrm{fr}(\alpha)$$

Vamos ilustrar as considerações anteriores com um exemplo usual. Suponhamos que num dado exame se apresentaram 189 alunos e que os resultados foram os que constam da seguinte tabela:

Tabela 1

Classificações	N.º de alunos	Classificações	N.º de alunos
0	0	11	45
1	0	12	28
2	0	13	17
3	0	14	9
4	2	15	12
5	1	16	7
6	5	17	5
7	11	18	2
8	7	19	1
9	0	20	0
10	37		

Assim, nesta prova, a frequência absoluta da classificação 3 foi 0; a frequência absoluta da classificação 10 foi 37, etc. As frequências

relativas das classificações, em percentagens, são as que constam da seguinte tabela:

Tabela 2

Classificações	Percentagem	Classificações	Percentagem
0	0,0	10	19,6
1	0,0	11	23,8
2	0,0	12	14,8
3	0,0	13	9,0
4	1,1	14	4,8
5	0,5	15	6,3
6	2,6	16	3,8
7	5,8	17	2,6
8	3,7	18	1,1
9	0,0	19	0,5
		20	0,0

Designemos por m, M, S, b, B, A, R, respectivamente, os atributos *mediocre, mau, suficiente, bom, muito bom, aprovado, reprovado*. Como habitualmente, chama-se 'suficiente' à soma lógica dos atributos correspondentes às classificações 10, 11, 12, 13, 'bom' à soma lógica dos atributos correspondentes a 14, 15, 16, 17, etc Por outro lado:

$$R = M + m, \quad A = S + b + B$$

Visto que as diferentes classificações são incompatíveis entre si, tem-se:

$$fr(S) = 0{,}196 + 0{,}238 + 0{,}148 + 0{,}090 = 0{,}672$$

$$fr(b) = 0{,}048 + 0{,}063 + 0{,}038 + 0{,}026 = 0{,}175$$

$$fr(B) = 0{,}011 + 0{,}005 = 0{,}016$$

Por sua vez, como os atributos S, b, B também são incompatíveis entre si, vem:

$$fr(A) = 0{,}672 + 0{,}175 + 0{,}016 = 0{,}863$$

Finalmente, como R é o *atributo contrário de* A, vem:

$$fr(R) = 1 - 0{,}863 = 0{,}137$$

5. **Frequência relativa do produto lógico. Primeiro exemplo de probabilidade.** Quando se pretende averiguar em que medida dois atributos ou dois fenómenos estão *ligados entre si,* numa dada população ou num dado tipo de experiências, o que há a fazer é um inquérito estatístico, de que vamos indicar os passos preliminares.

Suponhamos, por exemplo, que se trata de saber se, entre pessoas, a miopia está de qualquer modo associada com o facto de *ter olhos azuis.* O que desde logo ocorre é indagar, numa população tão numerosa e variada quanto possível, quais as percentagens de míopes:

1.º *entre os indivíduos com olhos azuis;*

2.º *na população total.*

Se estas duas percentagens são sensivelmente iguais, há razões para pensar que os atributos 'míope' e 'com olhos azuis' são *independentes;* se as duas percentagens se afastam consideravelmente uma da outra, seremos inclinados a admitir que os dois atributos estão *associados* ou *correlacionados*: em sentido *positivo,* se a primeira percentagem é maior que a segunda, em sentido *negativo* no caso oposto.

Analogamente se procederia para averiguar, por exemplo, se o *fumar* está ou não ligado com o *ter cancro dos pulmões,* se um

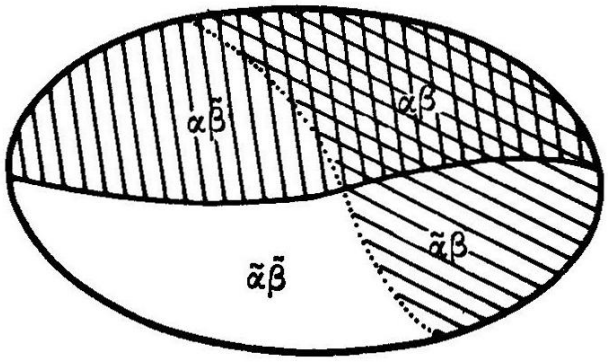
insecticida é ou não eficaz no tratamento de certas plantas, etc. Nestes exemplos, começa a desenhar-se a hipótese duma relação *causa-efeito* entre os fenómenos considerados.

As considerações precedentes podem ser teorizadas do seguinte modo: sejam α, β, dois atributos num universo finito U constituído por n indivíduos. Para indicar as frequências dos atributos $\alpha\beta$, $\alpha\tilde{\beta}$, etc. podemos fazer uso duma tabela de duas entradas do seguinte tipo (chamada *tabela de contingência*):

	β	β	Total
α	$\Phi(\alpha\beta)$	$\Phi(\alpha\tilde{\beta})$	$\Phi(\alpha)$
$\tilde{\alpha}$	$\Phi(\tilde{\alpha}\beta)$	$\Phi(\tilde{\alpha}\tilde{\beta})$	$\Phi(\tilde{\alpha})$
Total	$\Phi(\beta)$	$\Phi(\tilde{\beta})$	n

Por exemplo, se α e β são, respectivamente, os atributos 'míope' e 'com olhos azuis', então $\alpha\beta$ é o atributo 'míope com olhos azuis', $\Phi(\alpha\tilde{\beta})$ é *o número de indivíduos míopes com olhos não azuis (no universo* U), etc. Neste caso, a frequência relativa do atributo 'míope' entre indivíduos com olhos azuis será:

$$\frac{\Phi(\alpha\beta)}{\Phi(\beta)}, \quad \text{supondo} \quad \Phi(\beta) \neq 0$$



Chamar-lhe-emos *frequência relativa de* α *se* β (isto é, *frequência relativa de* α *na hipótese de* β *se verificar)* e representá-la-emos por $\mathrm{fr}(\alpha|\beta)$, quaisquer que sejam os atributos α e β. Será, pois, por definição:

$$\mathrm{fr}(\alpha|\beta) = \frac{\Phi(\alpha\beta)}{\Phi(\beta)} \tag{1}$$

Por sua vez, a frequência relativa do atributo α (no universo considerado) será:

$$\mathrm{fr}\,(\alpha) = \frac{\Phi(\alpha)}{n}$$

Ora, segundo as considerações precedentes, os atributos α e β serão chamados *independentes* (em U), sse

$$\mathrm{fr}(\alpha|\beta) = \mathrm{fr}(\alpha) \tag{2}$$

ou, o que é equivalente, sse

$$\frac{\Phi(\alpha\beta)}{\Phi(\beta)} = \frac{\Phi(\alpha)}{n}$$

o que pode escrever-se de maneira mais simétrica:

$$\Phi(\alpha\beta) = \frac{\Phi(\alpha) \cdot \Phi(\beta)}{n} \tag{3}$$

Assim, qualquer das fórmulas (2) e (3) exprime que *os atributos* α *e* β *são independentes.*

Dividindo ambos os membros de (3) por *n* vem:

$$\frac{\Phi(\alpha\beta)}{n} = \frac{\Phi(\alpha)}{n} \cdot \frac{\Phi(\beta)}{n}$$

ou seja:

$$fr(\alpha\,\beta) = fr(\alpha)\,.\,fr(\beta),$$

o que é uma nova forma de exprimir a independência dos atributos α e β. Assim, teremos:

(4) $\boxed{fr(\alpha\,\beta) = fr(\alpha) \cdot fr(\beta),\ \text{sse}\ \alpha\ \text{e}\ \beta\ \text{são independentes}}$

isto é: *a frequência relativa do produto lógico* $\alpha\beta$ *é o produto das frequências relativas de* α *e de* β, *sse estes atributos são independentes* (pela própria definição de 'atributos independentes').

Notemos, agora, que a fórmula (1) se pode escrever

$$\Phi(\alpha\beta) = \Phi(\beta) \cdot fr(\alpha|\beta)$$

ou seja, dividindo ambos os membros por n:

$$fr(\alpha\beta) = fr(\beta) \cdot fr(\alpha|\beta)$$

É claro que podemos trocar os papéis de α e de β:

(5) $\boxed{fr(\alpha\beta) = fr(\alpha) \cdot fr(\beta|\alpha)}$

isto é: quaisquer que sejam os atributos α e β, *a frequência relativa de* α β *é o produto de frequência relativa de* α *pela frequência relativa de* β *se* α (por definição de 'frequência relativa de β se α').

A fórmula (4) é, evidentemente, um caso particular de (5), pois que $fr(\beta|\alpha) = fr(\beta)$, sse α e β são independentes.

É claro que, na prática, só por coincidência se tem *exactamente* $fr(\beta|\alpha) = fr(\beta)$ ou, o que é equivalente:

$$\Phi(\alpha\beta) = \frac{\Phi(\alpha) \cdot \Phi(\beta)}{n}$$

O segundo membro desta igualdade representa-se por $\Phi_o(a\beta)$:

$$\Phi_o(\alpha\beta) = \frac{\Phi(\alpha) \cdot \Phi(\beta)}{n}$$

e chama-se *valor de independência ou valor esperado de* $\Phi(\alpha\beta)$ (isto é, *valor esperado na hipótese de* α *e* β *serem independentes*). Quase sempre o valor esperado é diferente do *valor observado* (ou *valor real*), $\Phi(\alpha\beta)$, e a diferença

$$\delta = \Phi(\alpha\beta) - \Phi_o(\alpha\beta)$$

é chamada *desvio* ou *discrepância* (entre o valor observado e o valor esperado).

Se o desvio δ é *relativamente pequeno* (ou *insignificante*), podemos atribuí-lo ao acaso e dizer que os atributos α e β são *independentes,* do ponto de vista da *estatística*. Se o desvio é *relativamente grande* (ou *significante*), já não é atribuível ao acaso e diremos que os atributos α e β estão *associados* (na população U).

Quanto ao significado das expressões 'relativamente pequeno', 'relativamente grande', 'acaso', etc., só mais tarde e progressivamente poderão ir sendo esclarecidos.

Note-se que, em particular, se pode ter

$$fr(\alpha|\beta) = 1 \quad \text{ou seja} \quad \Phi(\alpha\beta) = \Phi(\beta)$$

Por exemplo, se α e β são os atributos 'míope' e 'com olhos azuis' isto quereria dizer que o número de indivíduos *míopes com olhos azuis* é igual ao número de indivíduos *com olhos azuis* e que, por-

tanto, *todos os indivíduos com olhos azuis são míopes* (isto é, que o atributo β *implica* o atributo α). Dum modo geral tem-se, quaisquer que sejam os atributos α e β:

$$\boxed{\text{fr}(\alpha|\beta) = 1 \quad \text{sse} \quad \beta \Rightarrow \alpha}$$

(Demonstre, considerando conjuntos em vez de atributos e atendendo à propriedade característica dos conjuntos finitos considerada no Cap. III).

Diz-se que α e β estão *completamente associados* sse $\alpha \Rightarrow \beta$ ou $\beta \Rightarrow \alpha$, isto é sse $\text{fr}(\beta|\alpha) = 1 \vee \text{fr}(\alpha|\beta) = 1$.

· Um outro caso particular é aquele em que

$$\text{fr}(\alpha|\beta) = 0 \text{ ou seja } \Phi(\alpha\beta) = 0 \; [\text{supomos } \Phi(\beta) \neq 0]$$

Isto significa manifestamente, que α e β são incompatíveis ou, o que é equivalente, que $\alpha \Rightarrow \tilde{\beta}$ ou ainda que $\beta \Rightarrow \tilde{\alpha}$ (no exemplo concreto considerado: 'nenhum indivíduo míope tem olhos azuis' ou 'nenhum indivíduo com olhos azuis é míope').

Diz-se que α e β estão *completamente dissociados* sse são incompatíveis os atributos α e β ou os atributos $\tilde{\alpha}$ e $\tilde{\beta}$, isto é, sse $\Phi(\alpha\beta) = 0 \vee \Phi(\tilde{\alpha}\tilde{\beta}) = 0$.

Facilmente se reconhece que:

Os atributos α e $\tilde{\beta}$ estão completamente dissociados, sse os atributos α e β estão completamente associados.

É claro que neste enunciado os papéis de α e β podem ser trocados.

EXEMPLO. Imaginemos uma experiência destinada a avaliar em que medida a inoculação de certa vacina imuniza contra a cólera. Suponhamos que os resultados obtidos são os que constam da tabela 3.

Tabela 3

	Não atacados	Atacados	Total
Inoculados	276	3	279
Não inoculados	473	66	539
Total	749	69	818

Sejam α e β, respectivamente, os atributos 'inoculado' e 'não atacado'. Então:

$$(fr)\ (\beta|a) = \frac{\Phi(a\beta)}{\Phi(a)} = \frac{276}{279} \approx 0{,}99$$

$$fr\ (\beta) = \frac{\Phi(\beta)}{n} = \frac{749}{818} \approx 0{,}88$$

Neste caso, há uma diferença apreciável entre as duas frequências calculadas, indicativa de uma associação positiva entre os referidos atributos; e, como $fr(\beta|\alpha)$ se aproxima bastante de 1, ao contrário de $fr(\alpha|\beta)$ ($\approx 0{,}34$), vemos que a referida associação se dá no sentido $\alpha \Rightarrow \beta$.

São, também, elucidativas as seguintes indicações:

1) Percentagem de inoculados que foram atacados: 1 %

2) Percentagem de não inoculados que foram atacados: 12 %

Parece, pois, concluir-se daqui que, embora a referida vacina não imunize *em absoluto,* confere no entanto uma *imunidade relativa* bastante apreciável, contra a cólera.

Se várias outras experiências, em condições análogas, conduzirem a um resultado sensivelmente igual a este quanto a $fr(\alpha|\beta)$, seremos

levados a dizer, por indução, que a vacina imuniza em 99 % dos casos. Exprimiremos também este facto dizendo que a *probabilidade de ficar imunizado* é 99 % (ou 0,99) e que, portanto, a *probabilidade de não ficar imunizado é* 1 % (ou 0,01).

NOTA IMPORTANTE. A implicação $\alpha \Rightarrow \beta$ deduzida de vários inquéritos estatísticos, com uma certa probabilidade, nem sempre pode ser interpretada como relação de *causa-efeito*. Suponhamos, por exemplo, que a frequência relativa de indivíduos calvos nas duas primeiras filas dos teatros se aproxima de 1 mais do que nas restantes filas. É óbvio que tal observação nunca poderia ser interpretada deste modo:

O facto de uma pessoa se sentar numa das duas primeiras filas de um teatro pode produzir-lhe a calvície.

Um dos problemas da estatística será, pois, o de estabelecer critérios que permitam distinguir entre implicações de causalidade e outras que o não são.

5. Coeficiente de associação*. Sejam ainda α e β dois atributos definidos num universo finito U. Já vimos que se chama *desvio* (ou *discrepância*) à diferença

$$\delta = \Phi(\alpha\,\beta) - \frac{\Phi(\alpha) \cdot \Phi(\beta)}{n}$$

entre o *valor observado* e o *valor de independência* de $\Phi(\alpha\,\beta)$. Mais tarde estudaremos um teste estatístico que nos habilita em certos casos a decidir, com maior ou menor *segurança,* se tal desvio não é devido ao *acaso* (1).

---

(1) Aqui, 'segurança' significa 'probabilidade de não errar'. Por enquanto, temos de nos contentar com o significado intuitivo de tais expressões, que irá sendo progressivamente esclarecido.

Vamos, agora, substituir o desvio δ por um *desvio relativo,* que nos dá melhor ideia do grau de associação dos atributos α, β. Tal é, por exemplo, o número Q dado pela fórmula:

$$(1) \qquad Q = \frac{n\delta}{\Phi(\alpha\,\beta)\,\Phi(\tilde{\alpha}\,\tilde{\beta}) + \Phi(\alpha\,\tilde{\beta})\,\Phi\,(\tilde{\alpha}\,\beta)}$$

ou seja:

$$(2) \qquad Q = \frac{(n\Phi\alpha\,\beta) - \Phi(\alpha)\,\Phi\,(\beta)}{\Phi(\alpha\,\beta)\,\Phi\,(\tilde{\alpha}\,\tilde{\beta}) + \Phi(\alpha\,\tilde{\beta})\,\Phi\,(\tilde{\alpha}\,\beta)}$$

Este é chamado, precisamente, o *coeficiente de associação de* α *e* β. Notemos que se tem (justifique):

$$(\alpha + \tilde{\alpha})\,(\beta + \tilde{\beta}) = \alpha\,\beta + \tilde{\alpha}\,\beta + \alpha\,\tilde{\beta} + \tilde{\alpha}\,\tilde{\beta} = \mathbf{1}\ (^1)$$

Visto que as quatro parcelas são atributos incompatíveis entre si, daqui se deduz:

$$(3) \qquad \Phi(\alpha\,\beta) + \Phi(\tilde{\alpha}\,\beta) + \Phi(\alpha\,\tilde{\beta}) + \Phi(\tilde{\alpha}\,\tilde{\beta}) = n$$

Por outro lado:

$$\alpha = \alpha\,\beta + \alpha\,\tilde{\beta} \quad , \quad \beta = \alpha\,\beta + \tilde{\alpha}\,\beta \qquad \textit{(Porquê?)}$$

Donde:

$$(4) \qquad \Phi(\alpha) = \Phi(\alpha\,\beta) + \Phi\,(\alpha\,\tilde{\beta}), \quad \Phi\,(\beta) = \Phi(\alpha\,\beta) + \Phi(\tilde{\alpha}\,\beta)$$

---

(1) Lembremos que se designa por **1** o atributo universal e por (0 o atributo impossível (ver n.º 2).

Finalmente, substituindo em (2) as expressões de n, $\Phi(\alpha)$ e $\Phi(\beta)$ dadas por (3) e (4), e simplificando, vem:

$$(5) \qquad Q = \frac{\Phi(\alpha\,\beta)\,\Phi(\tilde{\alpha}\,\tilde{\beta}) - \Phi(\alpha\,\tilde{\beta})\,\Phi(\tilde{\alpha}\,\beta)}{\Phi(\alpha\,\beta)\,\Phi(\tilde{\alpha}\,\tilde{\beta}) + \Phi(\alpha\,\tilde{\beta})\,\Phi(\tilde{\alpha}\,\beta)}$$

É fácil ver que se tem sempre:

$$-1 \leqslant Q \leqslant 1$$

Posto isto, há a distinguir três casos notáveis:

1.º *Tem-se* $Q = 0$, *sse* α *e* β *são independentes.* Para o reconhecer, basta atender a (1) e lembrar que α e β são independentes, por definição, sse $\delta = 0$.

2.º *Tem-se* $Q = -1$, *sse* α *e* β *estão completamente dissociados.*

Com efeito, se α e β estão completamente dissociados, tem-se por definição

$$\Phi(\alpha\,\beta) = 0 \quad \vee \quad \Phi(\tilde{\alpha}\,\tilde{\beta}) = 0$$

o que implica $Q = -1$. Reciprocamente, é fácil ver que, se $Q = -1$, será necessariamente $\Phi(\alpha\,\beta)\ \Phi\ (\tilde{\alpha}\,\tilde{\beta}) = 0$ e, portanto:

$\Phi(\alpha\,\beta) = 0 \ \vee\ \Phi(\tilde{\alpha}\,\tilde{\beta}) = 0$. Basta lembrar que em IR:

$$\frac{x - y}{x + y} = -1 \Leftrightarrow x = 0, \text{ se } x + y \neq 0$$

3.º *Tem-se* $Q = 1$, *sse* α *e* β *estão completamente associados.*

Este caso reduz-se ao anterior, lembrando que α e β estão completamente associados, sse α e $\tilde{\beta}$ estão completamente dissociados.

Finalmente demonstraremos o seguinte

TEOREMA: *Se* (α, β) *é um par de atributos independentes, também* $(\tilde{\alpha}, \beta)$ $(\alpha, \tilde{\beta})$ *e* $(\tilde{\alpha}\tilde{\beta})$ *são pares de atributos independentes.*

Com efeito, como vimos, se α e β são independentes, tem-se $Q = 0$. Então, por exemplo, o coeficiente de associação de $\tilde{\alpha}$ e β será:

$$Q' = \frac{\Phi(\tilde{\alpha}\,\beta)\,\Phi(\alpha\,\tilde{\beta}) - \Phi(\tilde{\alpha}\tilde{\beta})\,\Phi(\alpha\,\beta)}{\Phi(\tilde{\alpha}\,\beta)\,\Phi(\alpha\,\tilde{\beta}) + \Phi(\tilde{\alpha}\tilde{\beta})\,\Phi(\alpha\,\beta)} = -\,Q = 0$$

e, portanto, $\tilde{\alpha}$ e β são independentes. Analogamente se procede nos restantes casos.

6. **Extensão dos conceitos do n.º 4 a mais de dois atributos.** Consideremos três atributos α, β, γ num universo finito U. Por exemplo, α, β, γ podem ser, respectivamente, os atributos 'fumador', 'alcoólico', 'com úlcera gástrica ou duodenal', num conjunto de pessoas. Visto que

$$\alpha\,\beta\,\gamma = (\alpha\,\beta)\,\gamma,$$

tem-se, aplicando a fórmula (5) do n.º 4:

$$\mathrm{fr}(\alpha\,\beta\,\gamma) = \mathrm{fr}(\alpha\ \beta) \cdot \mathrm{fr}(\gamma|\alpha\,\beta)$$

e, como $\mathrm{fr}(\alpha\,\beta) = \mathrm{fr}(\alpha) \cdot \mathrm{fr}(\beta \mid \alpha)$, vem, finalmente:

$$\boxed{\mathrm{fr}(\alpha\,\beta\,\gamma) = \mathrm{fr}(\alpha) \cdot \mathrm{fr}(\beta|\alpha) \cdot \mathrm{fr}(\gamma|\alpha\,\beta)}$$

É claro que nesta fórmula as letras α, β, γ podem ser permutadas de todos os modos possíveis, visto que α, β, γ são atributos *quaisquer.*

Em particular, *se for*

(1) $$\mathrm{fr}(\beta|\alpha) = \mathrm{fr}(\beta) \quad \text{e} \quad \mathrm{fr}(\gamma|\alpha\,\beta) = \mathrm{fr}(\gamma),$$

virá:

(2) $$\boxed{\mathrm{fr}(\alpha\,\beta\,\gamma) = \mathrm{fr}(\alpha) \cdot \mathrm{fr}(\beta) \cdot \mathrm{fr}(\gamma)}$$

DEFINIÇÃO. *Diz-se que três atributos* α, β, γ *são independentes (no universo U), sse verificam não só as condições (1), mas ainda as que se deduzem dessas, substituindo um ou mais dos atributos* α, β, γ *pelos seus contrários, como por exemplo* (1)*:*

$$\mathrm{fr}(\gamma|\tilde{\alpha}\,\beta) = \mathrm{fr}(\gamma), \quad \mathrm{fr}(\gamma|\tilde{\alpha}\,\tilde{\beta}) = \mathrm{fr}(\gamma), \text{ etc.}$$

Desde logo se vê que esta definição equivale à seguinte proposição:

Os atributos α, β, γ*, são independentes, sse, além da condição* (2)*, verificam as condições tais como*

$$\mathrm{fr}(\alpha\tilde{\beta}\gamma) = \mathrm{fr}(\alpha) \cdot \mathrm{fr}(\tilde{\beta}) \cdot \mathrm{fr}(\gamma),$$
$$\mathrm{fr}(\tilde{\alpha}\beta\tilde{\gamma}) = \mathrm{fr}(\tilde{\alpha}) \cdot \mathrm{fr}(\beta) \cdot \mathrm{fr}(\tilde{\gamma}), \text{ etc.}$$

que se deduzem de (2) *substituindo um ou mais dos atributos* α, β, γ *pelos respectivos contrários.*

Isto mostra imediatamente que *a relação ternária assim definida entre atributos é simétrica.*

---

(1) Parte das condições assim obtidas são consequência das restantes. Por exemplo, a equação $\mathrm{fr}(\beta|\alpha) = \mathrm{fr}(\beta)$ equivale a $\mathrm{fr}(\tilde{\beta}|\alpha) = \mathrm{fr}(\tilde{\beta})$, etc. (Ver teorema do número anterior).

Mas, notem-se os dois seguintes pontos importantes:

1) Os atributos α, β, γ podem ser *independentes dois a dois* (isto é, α independente de β, α independente de γ, e β independente de γ), sem serem os três independentes.

2) Ao contrário do que sucede no caso de dois atributos (ver teorema do número anterior), a fórmula (2) pode ser verificada sem que os atributos α, β, γ sejam independentes.

É preciso também não confundir 'atributos independentes' com 'atributos incompatíveis'.

É claro que estas considerações se podem generalizar imediatamente ao caso de um número finito n qualquer de atributos.

7. **A lógica em termos de acontecimentos.** Recordemos que, em alguns dos exemplos anteriores, os atributos considerados também se podem interpretar como *acontecimentos*. Assim, no exemplo final do número 4, os atributos 'inoculado' e atacado' correspondem, respectivamente, aos acontecimentos 'ser inoculado (com vacina)' e 'ser atacado (de cólera)'.

Não pretendemos aqui definir 'acontecimento', assim como não tentámos definir 'atributo' nem 'conjunto': trata-se de conceitos psicologicamente primitivos, gerados por indução ou intuição no nosso espírito. O que será possível e conveniente é esclarecer progressivamente a terminologia que lhes diz respeito.

Comecemos por notar que, em vez de 'acontecimento', se usam como significado semelhante os termos 'facto', 'fenómeno', 'eventualidade', etc.

Imaginemos uma prova ou experiência *que se possa repetir várias vezes em condições idênticas,* conduzindo, de cada vez, a um ou mais *resultados,* entre vários que são de prever. É a cada um desses resultados da prova que, em cálculo das probabilidades, se costuma dar o nome de *'acontecimento'*.

São inúmeros os exemplos que neste sentido se podem apresentar: desastre ou ausência de desastre numa viagem aérea, resultados dum exame ou duma prova desportiva, etc.

Mas convém registar o que há pouco foi observado: que muitas vezes os acontecimentos se traduzem por atributos (e vice-versa). Tal é, por exemplo, o caso dos resultados dum exame ou o caso análogo duma competição desportiva; assim, o acontecimento 'ficar reprovado' traduz-se pelo atributo 'reprovado'; o acontecimento 'vitória' traduz-se pelo atributo 'vencedor', relativamente a um dado clube; etc., etc.

Ainda aqui há portanto, de certo modo, uma questão de ponto de vista psicológico, semelhante à que se põe na distinção entre atributos e conjuntos. É, assim, de prever que a lógica de atributos se traduza numa lógica de acontecimentos. Com efeito, sejam α e β dois acontecimentos relativos a uma dada prova $\mathcal{P}$:

1) Chama-se *conjunção* (ou *produto lógico*) de α e β, e representa-se por $\alpha\beta$, o acontecimento que consiste na realização simultânea de α e de β.

2) Chama-se *disjunção* (ou *soma lógica*) de α e β e representa-se por $\alpha + \beta$, o acontecimento que consiste em se realizar *um, pelo menos,* dos acontecimentos α e β.

3) Chama-se *contrário de* α, e representa-se por $\tilde{\alpha}$, o acontecimento que consiste em não se realizar α.

4) Diz-se que α *implica* β, e escreve-se $\alpha \Rightarrow \beta$, sse β se realiza todas as vezes que se realiza α.

5) Dois acontecimentos α, β dizem-se *equivalentes* e escreve-se $\alpha \Rightarrow \beta$, sse $\alpha \Rightarrow \beta$ e $\beta \Rightarrow \alpha$.

6) Um acontecimento diz-se *certo,* sse sabemos, com certeza absoluta, que se realizará na prova $\mathcal{P}$, todas as vezes que esta for efectuada. Um acontecimento diz-se *impossível,* sse o seu contrário é certo.

7) Dois acontecimentos dizem-se *incompatíveis*, sse a sua conjunção é acontecimento impossível.

Por exemplo, no exame dum aluno é certo o acontecimento *aprovação* ou *reprovação* ou *desistência*, é impossível o acontecimento *aprovado com* 21 *valores* (em escolas portuguesas) e são incompatíveis os dois acontecimentos *aprovação* e *desistência*.

8. **Expressões proposicionais de acontecimentos; conceito de variável casual; passagem a conjuntos.** Tal como sucede com os atributos, os acontecimentos habitualmente considerados em estatística e em cálculo das probabilidades podem ser indicados por meio de expressões proposicionais com variáveis. Vejamos dois exemplos:

a) Imaginemos um saco que contenha várias bolas, umas brancas e outras pretas. Designando por U o universo das bolas contidas no saco, por B o conjunto das bolas brancas e por P o conjunto das bolas pretas, teremos duas expressões proposicionais:

$$x \in B \quad , \quad x \in P,$$

definidas em U. Os valores possíveis da variável x serão, pois, as bolas do conjunto U. Ora, o valor de x pode ser determinado extraindo *ao acaso* uma bola de U (no final discutiremos o significado da palavra 'acaso'). Nesta prova — extracção de uma bola — realiza-se então necessariamente um dos seguintes acontecimentos contrários: $x \in B$ (isto é: *sair bola branca*), $x \in P$ (isto é: *sair bola preta*). Vê-se, pois, como as referidas expressões proposicionais passam a indicar acontecimentos.

b) Seja x a classificação dum aluno numa prova $\mathcal{P}$ a realizar. Os resultados 'mau', 'medíocre', 'suficiente', 'bom', e 'muito bom'

são agora indicados, respectivamente, pelas expressões proposicionais seguintes:

$$0 \leqslant x < 6,\quad 6 \leqslant x < 10,\quad 10 \leqslant x < 14,\quad 14 \leqslant x < 18,\quad 18 \leqslant x < 20$$

O resultado 'aprovado', soma lógica de 'suficiente', 'bom' e 'muito bom', é indicado pela expressão $x \geqslant 10$.

Assim, em casos como estes, cada um dos acontecimentos a que pode dar lugar a prova $\mathcal{P}$ considerada aparece sob a forma de uma expressão proposicional com uma variável x, num determinado universo U. O valor da variável x (elemento de U) é, então, determinado em cada realização da prova $\mathcal{P}$ por um processo em que intervém mais ou menos o *acaso* e que, por isso, não permite prever qual será exactamente esse valor. Exprime-se este facto dizendo que x é uma *variável casual* (ou uma *variável aleatória*).

É claro que a conjunção de dois acontecimentos α e β será indicada pela conjunção das expressões proposicionais que indicam α e β, e analogamente para a disjunção, para a negação, etc.

Deste modo, a cada acontecimento α fica a corresponder um determinado conjunto A em U: o conjunto dos elementos que verificam a expressão indicativa de α. Aos dois acontecimentos α e β corresponde então um mesmo conjunto, sse $\alpha \Leftrightarrow \beta$.

Reciprocamente, a cada conjunto A em U corresponde o acontecimento indicado pela expressão $x \in A$.

Vemos assim que, tal como sucede com os atributos:

A lógica de acontecimentos é traduzida, segundo a referida correspondência, na lógica de conjuntos.

Notemos ainda que, tal como para atributos:

Se convencionarmos considerar como *idênticos* dois acontecimentos α e β quando são *equivalentes*, escrevendo então $\alpha = \beta$ em vez de $\alpha \Leftrightarrow \beta$, o conjunto dos acontecimentos relativos a uma dada prova $\mathcal{P}$ constitui uma álgebra de Boole isomorfa a uma álgebra

de conjuntos. Designaremos, então, por 1 o *acontecimento certo* e por (0 o *acontecimento impossível.*

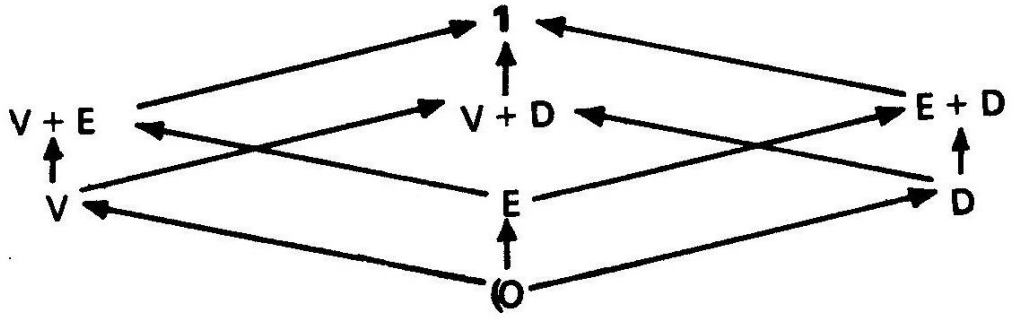
Por exemplo, consideremos as seguintes eventualidades relativas a um desafio de futebol entre duas equipas A e B:

$$V = \text{vitória de A}, \quad E = \text{empate}, \quad D = \text{derrota de A}$$

Então $V \cdot E = V \cdot D = E \cdot D = (0$. Por outro lado, tratando-se dum *desafio normal,* tem-se:

$$V + E + D = 1$$

Além destas, há ainda a considerar as seguintes eventualidades: V + E, V + D, E + D. Temos, assim, ao todo 8 hipóteses (que se podem considerar, por exemplo, em cada uma das provas indicadas num bilhete de TOTOBOLA). É evidente que o conjunto dessas oito hipóteses, com as operações de soma lógica e produto lógico, é uma álgebra de Boole, representada no seguinte esquema, em que usamos setas simples como símbolos de implicação:



É também fácil reconhecer que esta *álgebra de acontecimentos é isomorfa à álgebra dos subconjuntos do conjunto* { V, E, D }.

NOTA SOBRE O CONCEITO DE 'ACASO'. Numa primeira aproximação, poderíamos dizer que o termo 'acaso' significa 'ausência de causa' ou, pelo menos, 'ausência de causa conhecida', o que torna impossível a previsão de certos acontecimentos. Por exemplo, quando lançamos *ao acaso* uma moeda de um escudo ao ar ou quando tiramos *à sorte* uma bola de loto de um saco, somos incapazes de prever se sairá escudo ou face, ou qual o número da bola que vai aparecer. Diz-se, então, que se trata de acontecimentos *casuais (fortuitos, aleatórios* ou *eventuais),* isto é, de acontecimentos que não estão determinados *a priori,* e que, portanto, se podem verificar umas vezes e outras não.

Para certos autores, o *acaso* consistiria na acumulação de um grande número de pequenas causas desconhecidas, que actuam em diversos sentidos, tornando praticamente impossível a previsão do efeito global. Mas esta interpretação filia-se ainda no ponto de vista do *determinismo mecanicista,* que se admitiu no século passado e que é sintetizado pelas seguintes palavras de LAPLACE no seu *Essai philosophique sur les probabilités:*

'Um intelecto de tal modo vasto que conhecesse o estado e as posições relativas de todos os entes da natureza num dado instante, assim como todas as forças que os solicitam; intelecto que fosse, além disso, bastante poderoso para submeter todos esses dados à análise matemática — uma tal inteligência poderia abranger numa só fórmula o movimento dos maiores corpos e das mais ínfimas partículas do universo: então, nada ficaria incerto e tanto o passado como o futuro se tornariam presentes aos seus olhos' (1).

Ora, a ciência do século XX veio mostrar que esta posição é ilusória sob vários aspectos. É-se levado hoje a admitir que, na evolução do mundo físico, subsiste sempre algo de essencialmente imprevisível, isto é, um certo grau de incerteza radical, que não resulta apenas da nossa ignorância.

---

(1) O germe do determinismo mecanicista encontra-se já em DESCARTES, que dizia: *'Dai-me o espaço e o movimento, eu vos darei o mundo'.*

9. **Frequência dum acontecimento numa sequência de provas.** Comecemos por dois exemplos:

a) Numa série de 30 000 viagens efectuadas por uma dada companhia de aviação, houve desastres apenas em duas viagens. Diremos, então, que a *frequência absoluta* do acontecimento *desastre* nesta sequência de viagens foi 2 e que a *frequência relativa* do mesmo acontecimento nessa mesma sequência foi:

$$\frac{2}{30\,000} \approx 0{,}000067 \approx 7/100\,000$$

b) Numa série de competições, um dado clube desportivo teve 9 vitórias, 4 derrotas e 1 empate. Nesta sequência de provas as frequências relativas dos acontecimentos *vitória, derrota* e *empate* foram, respectivamente:

$$\frac{9}{14} \approx 0{,}64 = 64\,\%, \quad \frac{4}{14} \approx 0{,}29 = 29\,\%, \quad \frac{1}{14} \approx 0{,}07 = 7\,\%$$

Dum modo geral:

DEFINIÇÃO 1. *Chama-se frequência absoluta dum acontecimento* α *numa sequência de* n *provas* $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_n$, *consideradas como realizações de uma mesma prova-tipo* $\mathcal{P}$, *o número* ν *de vezes que* α *se verifica nessas provas. Chama-se frequência relativa de* α *na mesma sequência de provas o quociente* ν/n *da frequência absoluta pelo número total de provas da sequência.* Designaremos por $\Phi(\alpha)$ a frequência absoluta de α e por $\mathrm{fr}(\alpha)$ a frequência relativa de α na referida sequência.

Será, pois, por definição:

$$\mathrm{fr}(\alpha) = \frac{\Phi(\alpha)}{n} \tag{1}$$

Desta definição resultam imediatamente as propriedades:

I. *Tem-se sempre* $0 \leqslant \text{fr}(\alpha) \leqslant 1$

II. *Se* α *é certo, então* $\text{fr}(\alpha) = 1$ (*Porquê?*)

III. *Se* α *é impossível, então* $\text{fr}(\alpha) = 0$ (*Porquê?*)

Como no caso dos atributos, também se demonstra:

IV. *Se* α *e* β *são acontecimentos relativos à prova* $\mathcal{P}$, *então*

$$\text{fr}(\alpha+\beta) = \text{fr}(\alpha) + \text{fr}(\beta) - \text{fr}(\alpha\beta)$$

Por sua vez de IV e III deduz-se (justifique):

V. *Se* α *e* β *são incompatíveis, então*

$$\text{fr}(\alpha+\beta) = \text{fr}(\alpha) + \text{fr}(\beta)$$

Assim, no exemplo *b*) anterior, os acontecimentos *vitória* e *derrota* são incompatíveis e, portanto:

$$\text{fr}(V + D) = \text{fr}(V) + \text{fr}(D) = \frac{9}{14} + \frac{4}{14} = \frac{13}{14} \approx 93\,\%$$

Finalmente de II e V deduz-se:

VI. $$\text{fr}(\tilde{\alpha}) = 1 - \text{fr}(\alpha)$$

Com efeito tem-se, por definição, $\alpha + \tilde{\alpha} = 1$ e $\alpha\,\tilde{\alpha} = 0$, donde, aplicando II, $\text{fr}(\alpha + \tilde{\alpha}) = 1$ e, aplicando V,

$$\text{fr}(\alpha) + \text{fr}(\tilde{\alpha}) = 1 \quad \text{e portanto} \quad \text{fr}(\tilde{\alpha}) = 1 - \text{fr}(\alpha)$$

Tornando ao exemplo 2) anterior, temos $V + D = \tilde{E}$ e, portanto:

$$\text{fr}(V + D) = \text{fr}(\tilde{E}) = 1 - \text{fr}(E) = 1 - \frac{1}{14} = \frac{13}{14} \approx 93\,\%$$

Passemos, agora, ao caso do produto lógico:

DEFINIÇÃO 2. *Se* α *e* β *são acontecimentos relativos a uma prova* $\mathcal{P}$, *chama-se 'frequência relativa de* α *se* β', *numa sequência de realizações de* $\mathcal{P}$, *e representa-se por* $\mathrm{fr}(\alpha\,\beta)$, *o quociente* μ/ν *do numero* μ *de vezes que se realiza* $\alpha\beta$ *pelo número* ν *de vezes que se realiza* β Será, pois:

$$\mathrm{fr}(\alpha|\beta) = \frac{\Phi(\alpha\beta)}{\Phi(\beta)}$$

Dividindo ambos os termos desta fracção pelo número n de realizações de $\mathcal{P}$ e atendendo a (1), obtém-se:

$$\mathrm{fr}(\alpha|\beta) = \frac{\mathrm{fr}(\alpha\,\beta)}{\mathrm{fr}(\beta)}$$

ou seja: $\mathrm{fr}(\alpha\,\beta) = \mathrm{fr}(\beta) \cdot \mathrm{fr}(\alpha|\beta)$, ou ainda, invertendo os papéis de α e β:

$$\boxed{\mathrm{fr}(\alpha\,\beta) = \mathrm{fr}(\alpha)\ \ \mathrm{fr}(\beta|\alpha)}$$

Os acontecimentos α, β dizem-se *independentes da referida sequência de provas,* sse $\mathrm{fr}(\alpha|\beta) = \mathrm{fr}(\alpha)$, ou, o que é equivalente, $\mathrm{fr}(\beta|\alpha) = \mathrm{fr}(\beta)$, ou ainda

$$\Phi(\alpha\,\beta) = \frac{\Phi(\alpha)\ \Phi\ (\beta)}{n}$$

Suponhamos, por exemplo, que a prova $\mathcal{P}$ é *desafio de futebol dum clube* A *com um outro clube qualquer,* sendo α o acontecimento vitória de A e β o acontecimento *presença do jogador* X na equipa (concretize com casos do seu conhecimento). Neste exemplo, $\mathrm{fr}(\alpha|\beta)$ é a frequência relativa de vitórias do clube A nos desafios em

que entra X. Se $fr(\alpha|\beta) = fr(\alpha)$, diremos que, na sequência de jogos considerados, o acontecimento *vitória de* A foi independente do acontecimento *presença do jogador* X.

Um outro exemplo: suponhamos que $\mathcal{P}$ designa *viagem de automóvel,* sendo α o acontecimento *desastre* e β o acontecimento *chuva.* É então fácil interpretar o significado do símbolo $fr(\alpha|\beta)$.

Estes exemplos começam a sugerir a ideia de causalidade. Tal ideia está intimamente ligada ao processo de indução, a que já nos referimos no Cap. I, n.º 17, págs. 49-50, 1.º tomo, e ao conceito de probabilidade, de que trataremos seguidamente.

10. **Lógica indutiva; certeza absoluta e certeza prática.** Como vimos no número anterior, *se um acontecimento* α *é certo numa prova* $\mathcal{P}$, *então* $fr(\alpha) = 1$ *em qualquer sequência de realizações* de $\mathcal{P}$. Mas será a recíproca verdadeira, isto é: *se* $fr(\alpha) = 1$ numa sequência de provas, podemos daí concluir que α é acontecimento certo? Claro que não.

Consideremos um exemplo. Imaginemos um saco que contém 50 bolas, *todas brancas,* numeradas de 1 a 50 e seja $\mathcal{P}$ a seguinte prova: *tirar ao acaso uma bola do saco, tornando a colocá-la depois no saco.* Então o acontecimento *saída de bola branca* é certo (ao contrário dos acontecimentos *saída do n.º* 5, *saída de número par,* etc.) e, por isso, numa sequência qualquer de realizações de $\mathcal{P}$, a frequência relativa de *saída de bola branca* é necessariamente 1. Mas imaginemos, agora, a situação inversa: o saco contém bolas cuja cor ignoramos e alguém efectua a prova $\mathcal{P}$ um grande número de vezes. Suponhamos que a frequência relativa do acontecimento *saída de bola branca* é então 1 (isto é, que sai bola branca em todas as extracções, com reposição). Podemos nós daí concluir que tal acontecimento é certo, isto é, que se verificará *sempre,* em qualquer prova futura? Claro que não: só podemos ter a *certeza absoluta,* tirando todas as bolas do saco e examinando-as uma a uma.

Porém, se a frequência relativa desse acontecimento for 1 num grande número de provas, por exemplo 1000, começamos a *convencer-nos* de que o acontecimento é certo, e essa convicção aumentará com o número de provas, se a frequência relativa continuar a ser 1. Em vez de uma *certeza autêntica* (ou *certeza absoluta*) passamos a ter uma *certeza prática* (ou *certeza relativa*).

A maior parte das certezas em que nos baseamos no decorrer da nossa vida são *certezas práticas* e não *certezas absolutas*. Por exemplo, temos a certeza dos seguintes factos: *'O Sol nasce amanhã'*, *'Se largarmos um copo sem apoio, o copo cai'*, *'A água quando gela aumenta de volume'*, *'O gelo flutua na água líquida'*, etc. Mas trata-se aqui apenas de *certezas práticas,* resultantes de um enorme número de provas, em que a frequência relativa de tais acontecimentos tem sido sempre 1. Aliás, tais factos só são certos *em determinadas condições:* por exemplo, o Sol *não nasce amanhã* em certos pontos da Terra, um copo *não cai* se for largado no interior de uma nave espacial a grande altitude, etc.

Em contraste com as *certezas práticas das ciências experimentais,* encontramos *certezas absolutas na matemática,* tais como:

> *'O quadrado dum número ímpar é sempre um número ímpar'*
> *'Não existe nenhum número racional cujo quadrado seja 3'*
> *'Uma equação algébrica de grau* n *não pode ter mais de* n *raízes num corpo'*

e muitas outras mais.

Dum modo geral, sempre que a frequência relativa dum acontecimento é 1 numa sequência de provas *muito numerosa,* é-se levado a admitir que o acontecimento é *praticamente certo,* isto é, que se realizará em qualquer outra prova futura, efectuada em condições idênticas. Nisto consiste, essencialmente, a *indução* ou *raciocínio indutivo,* que se encontra na base de toda a ciência experimental. Porém, à luz da lógica dedutiva, não se trata propriamente dum raciocínio (como os das demonstrações matemáticas), mas antes de um *paralogismo,* visto que se está a concluir ilicitamente do particular

para o geral. Na verdade, as leis das ciências experimentais, em particular as *leis físicas,* têm todas carácter *contingente*: não se pode garantir que sejam infalíveis (ver Cap. I, n.º 17).

Vejamos mais alguns exemplos:

Suponhamos que, na Lotaria da Santa Casa da Misericórdia de Lisboa, nunca saiu a sorte grande no número 21212 (não vamos averiguar se isto é verdade ou não; interessa-nos apenas a hipótese, *que não é inverosímil*). Podemos nós daqui concluir que o acontecimento

$$\alpha = \textit{não sair a sorte grande no n.º 21212}$$

é certo, ou (o que é equivalente) que o acontecimento

$$\tilde{\alpha} = \textit{sair a sorte grande no n.º 21212}$$

é impossível?

Claro que não. Se o sistema de lotaria é correcto (e não deve haver dúvidas a esse respeito), há *tanta razão* para sair a sorte grande nesse número, como em qualquer dos outros em que tem saído. Por outras palavras: se o sistema é correcto, todos os números têm a *mesma probabilidade* de sair.

Portanto, o acontecimento $\tilde{\alpha}$, em rigor, é possível, embora possamos dizer que é *praticamente impossível* numa extracção isolada; no mesmo sentido em que podemos dizer:

'É praticamente impossível que, no próximo ano, o Tamisa suba até ao ponto de inundar a Abadia de Westminster'.

Recordemos, a propósito, a máxima popular:

A sorte grande sai sempre aos outros.

O significado disto é que *a sorte grande sai sempre num número diferente do nosso:* trata-se afinal de uma lei baseada na indução, exactamente como sucede com as leis da física. No entanto, há pessoas felizes que têm razão para não acreditar nesta lei...

Note-se que o grau de certeza prática pode, por vezes, equiparar-se ao da certeza matemática. Tal é, por exemplo, o que se observa com a proposição que tem servido de premissa a exemplos clássicos de silogismo:

'Todos os homens são mortais'

Trata-se aqui de uma *lei biológica qualitativa*. Mas se tentarmos precisá-la quantitativamente, afirmando por exemplo:

'Todos os homens morrem antes dos 1000 anos de idade'

já não sentiremos o mesmo grau de segurança. Conhecemos nós suficientemente o passado da espécie humana? E que sabemos nós sobre o seu futuro, quanto às possibilidades que vêm abrir os progressos da ciência, por exemplo as viagens espaciais?

O que pode dizer-se é que, nas condições actuais, é *extremamente improvável, praticamente impossível,* que um ser humano atinja a idade de 1000 anos.

Um outro exemplo análogo é o que se refere a alturas de pessoas: é praticamente impossível que um ser humano cresça até atingir a altura de 5 metros.

Porém, se formos baixando estes limites sucessivamente para 200 anos, 150 anos, etc. (no primeiro caso) ou para 3m, 2,50 m, etc. (no segundo caso), o grau de incerteza irá aumentando — e entraremos abertamente no campo das probabilidades (ver no fim do volume a *Tabela de Mortalidade*). É de salientar que o Cálculo das Probabilidades e a Estatística Matemática se têm desenvolvido principalmente no sector das ciências biológicas e das ciências sociais. Mas certo é também que, por um movimento de retrocesso, acabaram por invadir o campo das ciências físicas, principalmente no que se refere ao estudo do átomo. *A física deixou de ser determinista para se tornar probabilista.*

11. **Conceito quantitativo de probabilidade.** As considerações precedentes mostram como os atributos 'verdadeiro' e 'falso' aplicados a proposições se tornam insuficientes (1) quando, do rigor abstracto das teorias matemáticas, se passa à imprecisão inevitável dos *conhecimentos empíricos,* relativos ao mundo em que vivemos, e que são, por isso mesmo, *indispensáveis na vida prática.* Os conceitos de 'verdade' e 'falsidade' cedem, então, lugar ao conceito de 'probabilidade', complementar do de 'incerteza' (ou 'contingência'); um facto dir-se-á tanto mais *provável* quanto menos *incerto* (ou *contingente*) for.

O conceito de probabilidade, como todas as noções primitivas de fonte empírica, não é susceptível de definição lógica: gera-se no nosso espírito por um processo indutivo. Mais até: é inseparável do próprio raciocínio indutivo, como veremos.

Em muitos casos, a *probabilidade dum acontecimento* é algo que se pode *medir,* algo que se pode *exprimir por um número,* como se fosse uma grandeza mensurável – comprimento, velocidade, energia eléctrica ou qualquer outra. São esses, é claro, os casos que interessam no Cálculo das Probabilidades.

Vejamos um exemplo. Suponhamos que os alunos de uma turma foram encarregados da seguinte experiência: cada aluno lança 100 vezes uma moeda de um escudo ao ar e verifica quantas vezes sai *escudo* (em vez de *cara*). Suponhamos que todos acharam um número compreendido entre 35 e 65. Assim, se designarmos por α o acontecimento *sair escudo,* temos, em todas as referidas sequências:

$$(1) \qquad 0{,}35 < \mathrm{fr}(\alpha) < 0{,}65$$

Suponhamos que se chega à mesma conclusão em várias outras experiências efectuadas em idênticas condições. Então, pelo *raciocínio*

---

(1) Releia o n.º 9 do Cap. I (págs. 20-22, 1.º tomo).

indutivo, somos levados a prever que, em qualquer sequência futura de 100 lançamentos, a frequência relativa de α verifica a condição (1). Pois bem, exprimiremos este facto dizendo que a *probabilidade de* α é um número compreendido entre 0,35 e 0,65, ou ainda que a *probabilidade de* α *é aproximadamente* 0,5 *com erro inferior a* 0,15 (ou 50 % *com erro inferior a* 15 %).

Suponhamos agora que, em vez de 100 lançamentos se fazem *sequências de* 1000 *lançamentos* e que se obtém *sempre* o resultado

$$0{,}45 < \mathrm{fr}(\alpha) < 0{,}55$$

Então, com significado análogo ao anterior, diremos que a *probabilidade* de α é um número compreendido entre 0,45 e 0,55, e escreveremos:

$$0{,}45 < \mathrm{P}(\alpha) < 0{,}55$$

em que 'P(α)' é uma abreviatura de 'probabilidade de α'. Também diremos, neste caso, que a *probabilidade de* α *é aproximadamente* 0,5 *com erro inferior a* 0,05 (ou 50 % *a menos de* 5 %).

Passando a sequências de 10 000 lançamentos, é de esperar que se obtenha o resultado

$$0{,}485 < \mathrm{fr}(\alpha) < 0{,}515$$

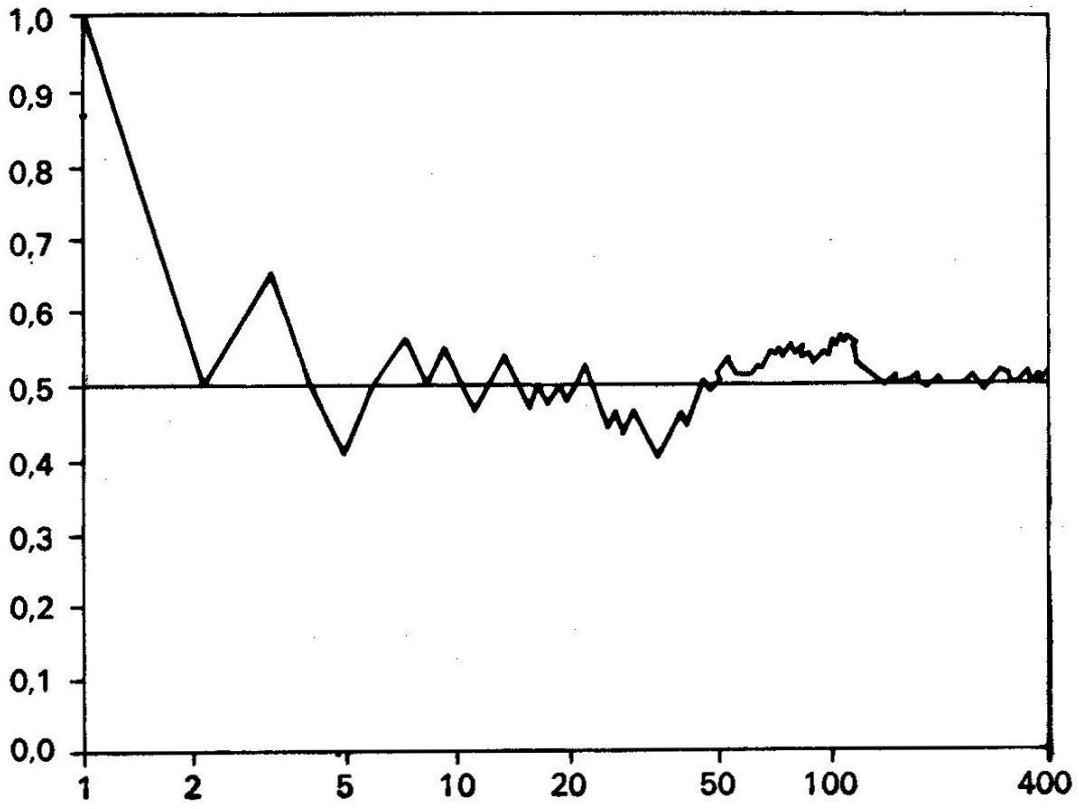
Então, escreveremos:

$$0{,}485 < \mathrm{P}(\alpha) < 0{,}515$$

e diremos que a *probabilidade de* α *é aproximadamente* 0,5 *a menos de* 0,015 (ou 50 % *a menos de* 1,5 %).

Assim, à medida que o número de lançamentos aumenta, a frequência relativa parece aproximar-se cada vez mais do número 0,5

que assumiremos como *valor aproximado* da probabilidade de α. Mas não tem sentido falar de *valor exacto* da probabilidade de α, do mesmo modo que não tem sentido falar de *medida exacta* duma grandeza física. Por exemplo, quando se diz que o comprimento de uma mesa é 1,65 m está-se a indicar um valor aproximado do comprimento da mesa, a menos de 1 cm; pode-se levar a aproximação até ao meio centímetro, até ao milímetro, etc., mas, abaixo de certo limite, já *não tem interesse* ou mesmo *não tem sentido* o grau de aproximação considerado.



Frequência relativa do acontecimento 'escudo' ao longo duma sequência de 400 lançamentos duma moeda ao ar. As frequências vão indicadas em escala logarítmica (isto é, as abcissas são logaritmos das frequências). (Exemplo dado por CRAMER em *Mathematical Methods of Statistics*.)

Em vez do lançamento de uma moeda ao ar, podíamos considerar outro tipo $\mathcal{P}$ de provas, por exemplo:

1) Lançar uma *punaise* (ou *attache*) ao ar e tomar nota da fre-

quência relativa do acontecimento *'cair de bico'*, que é contrário do acontecimento *'cair de cabeça'*. Ambas estas eventualidades vêm indicadas na figura seguinte:

2) Lançar um dado *ao acaso,* como é costume fazer-se, e tomar nota da frequência relativa de acontecimentos tais como 'sair o número 6', 'sair número par', 'sair número primo', etc.

Qualquer destas provas pode ser efectuada um grande número de vezes por uma equipa de alunos, utilizando *punaises* ou dados sensivelmente *iguais* em forma, dimensões e substância.

Em qualquer dos casos se deve verificar a chamada REGULARIDADE ESTATÍSTICA, isto é:

À medida que o número n *aumenta, a frequência relativa de cada acontecimento* α*, numa sequência de* n *provas, tende a ficar situada em intervalos*

$$[f_1,f'_1],\ [f_2,f'_2],\ \ldots,\ [f_n,f'_n],\ \ldots$$

cada vez mais pequenos, cada um deles contendo um seguinte. Nestas condições, os pontos médios

$$p_1 = \frac{f_1 + f'_1}{2}\ ,\ p_2 = \frac{f_2 + f'_2}{2},\ldots,\ p_n = \frac{f_n + f'_n}{2},\ldots$$

podem ser chamados 'valores aproximados da probabilidade do acontecimento α*' (com erro inferior a metade do comprimento do intervalo considerado).*

No exemplo da moeda, a probabilidade de sair escudo é aproximadamente 1/2, com erro bastante pequeno.

No exemplo da *attache,* a probabilidade do acontecimento

$$\alpha = \textit{cair de bico}$$

será *sensivelmente diferente* da probabilidade de

$$\tilde{\alpha} = \textit{cair de cabeça}$$

Essas probabilidades poderão ser determinadas com *suficiente aproximação,* por uma equipa de alunos, mas desde já é evidente que deverá ser:

$$P(\alpha) = 1 - P(\tilde{\alpha}) \text{ e, portanto, } P(\alpha) \neq \frac{1}{2} \qquad (\textit{Porquê?})$$

Quanto ao exemplo do dado, se designarmos por α_1, α_2, ..., α_6 os acontecimentos *'sair o n.º 1'*, *'sair o n.º 2'*, ..., *'sair o n.º 6'*, é de esperar que se tenha *aproximadamente*:

$$(1) \qquad P(\alpha_1) = P(\alpha_2) = \ldots = P(\alpha_6)$$

Mas, mesmo que o dado seja muito bem construído, aproximando-se bastante de um *cubo homogéneo,* nunca faz sentido afirmar *em absoluto* que as igualdades (1) são verdadeiras, do mesmo modo que não faz sentido afirmar *em absoluto* que duas réguas têm o mesmo comprimento.

Convenciona-se chamar *dado perfeito* a um dado que verifique a condição (1). Mas desde já vemos que se trata de uma noção abstracta: não existem *dados perfeitos,* do mesmo modo que não existem *gases perfeitos, água pura, pontos, rectas, cubos, esferas,* etc. Tais conceitos são apenas *esquemas,* isto é, modelos simplificados de entes concretos, idealizações que o nosso espírito elabora, tentando guiar-nos com maior ou menor êxito no mundo em que vivemos. Um desses esquemas é precisamente o conceito de probabilidade. *O que importa é saber aplicá-lo, de acordo com um conjunto*

adequado de regras (axiomas), que nos permita raciocinar logicamente sobre tal conceito. (No final do capítulo trataremos do *conceito qualitativo* de probabilidade.)

12. **Axiomatização do conceito de probabilidade.** Das considerações precedentes podemos tirar, como súmula, a seguinte norma prática:

Dizer que a *probabilidade de um acontecimento* α, relativo a uma prova $\mathcal{P}$, é um determinado número p, significa que, dado um número positivo ε, tão pequeno quanto se queira, existe sempre um número n bastante grande tal que, numa sequência de n ou mais realizações de $\mathcal{P}$, é *praticamente certo* que a frequência relativa de α estará compreendida entre $p - \varepsilon$ e $p + \varepsilon$.

Não se trata aqui propriamente duma definição. É preciso notar que, no conceito de 'certeza prática' já está implícito o de 'probabilidade': um acontecimento diz-se *praticamente certo,* quando a sua probabilidade é *aproximadamente* 1, com erro desprezível (1). No entanto, a regra anterior elucida bastante sobre o uso prático do termo 'probabilidade'. Uma vez que as probabilidades são *frequências relativas previstas,* é natural atribuir-lhes as mesmas propriedades formais que se aplicam a frequências relativas (ver n.º 9). Somos, assim, levados a admitir, como *axiomas,* as seguintes propriedades, sendo α e β dois acontecimentos relativos a uma prova $\mathcal{P}$:

AXIOMA 1. *A probabilidade de* α *— que se designa abreviadamente por* $P(\alpha)$ *— é sempre um número real não negativo, isto é:* $P(\alpha) \geqslant 0$.

---

(1) Analogamente, um acontecimento diz-se *praticamente impossível,* quando a sua probabilidade é aproximadamente 0, com erro desprezível. Por exemplo, é praticamente impossível que um macaco escreva à máquina a *Eneida* (exemplo do *macaco dactilógrafo,* de Emílio Borel).

AXIOMA 2. *A probabilidade do acontecimento certo é* 1, *isto é:* $P(\alpha) = 1$ *se* $\alpha = \mathbf{1}$.

AXIOMA 3. *Se* α *e* β *são acontecimentos incompatíveis, tem-se:*

$$P(\alpha + \beta) = P(\alpha) + P(\beta)$$

Destes axiomas (como premissas) deduzem-se, logicamente, vários *teoremas* (como conclusões), entre os quais os seguintes:

TEOREMA 1. *A probabilidade do acontecimento contrário de* α *é* $1 - P(\alpha)$, *isto é:*

$$P(\tilde{\alpha}) = 1 - P(\alpha)$$

Com efeito, como $\alpha\,\tilde{\alpha} = (0$ (*porquê?*) tem-se:

$$P(\alpha + \tilde{\alpha}) = P(\alpha) + (P\tilde{\alpha}) \qquad (Porquê?)$$

Por outro lado, como $\alpha + \tilde{\alpha} = \mathbf{1}$ (*porquê?*) tem-se:

$$P(\alpha) + P(\tilde{\alpha}) = 1 \quad (porquê?)$$

e, portanto, $P(\tilde{\alpha}) = 1 - P(\alpha)$.

COROLÁRIO 1. *Se* α *é acontecimento impossível, tem-se:*

$$P(\alpha) = 0 \quad (demonstre)$$

COROLÁRIO 2. *Qualquer que seja* α, *tem-se:*

$$P(\alpha) \leqslant 1 \quad (demonstre)$$

Portanto: $P(\alpha)$ é sempre um número real do intervalo $[0.1]$.

TEOREMA 2. *Se* $\alpha_1, \alpha_2, \ldots, \alpha_n$ *são* n *acontecimentos incompatíveis dois a dois (relativos à mesma prova* $\mathcal{P}$*) a probabilidade de que se realize um, pelo menos, dos acontecimentos* $\alpha_1, \alpha_2, \ldots, \alpha_n$ *é a soma das probabilidades destes acontecimentos, isto é:*

$$P\left(\sum_{i=1}^{n} \alpha_i\right) = \sum_{i=1}^{n} P(\alpha_i), \text{ se } \alpha_i \alpha_k = 0 \text{ para } i \neq k$$

Para demonstrar este teorema, basta aplicar, repetidamente, o axioma 2, observando que

$$\alpha_1 + \alpha_2 + \alpha_3 = (\alpha_1 + \alpha_2) + \alpha_3,$$

$$\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = (\alpha_1 + \alpha_2 + \alpha_3) + \alpha_4, \text{ etc.}$$

e que, se $\alpha_1, \alpha_2, \ldots, \alpha_n$ são incompatíveis dois a dois, também α_3 é incompatível com $\alpha_1 + \alpha_2$ (*prove*), α_4 com $\alpha_1 + \alpha_2 + \alpha_3$, etc.

TEOREMA 3. *Quaisquer que sejam os acontecimentos* α, β *relativos à prova* $\mathcal{P}$, *tem-se*:

$$P(\alpha + \beta) = P(\alpha) + P(\beta) - P(\alpha\beta)$$

Com efeito, tem-se (*prove*):

(1) $$\alpha = \alpha\tilde{\beta} + \alpha\beta \quad , \quad \beta = \tilde{\alpha}\beta + \alpha\beta$$

(2) $$\alpha + \beta = \alpha\tilde{\beta} + \tilde{\alpha}\beta + \alpha\beta$$

De (1) vem:

(3) $P(\alpha) = P(\alpha\tilde{\beta}) + P(\alpha\beta)$, $P(\beta) = P(\tilde{\alpha}\beta) + P(\alpha\beta)$ (*Porquê?*)

Por sua vez de (2) vem:

$$P(\alpha + \beta) = P(\alpha\tilde{\beta}) + P(\tilde{\alpha}\beta) + P(\alpha\beta) \qquad (\textit{Porquê?})$$

Donde, atendendo a (3):

$$P(\alpha+\beta) = P(\alpha) + P(\beta) - P(\alpha\,\beta)$$

Este teorema pode generalizar-se ao caso de *n* acontecimentos, obtendo-se a FÓRMULA DE DANIEL DA SILVA em termos de probabilidade.

13. **Exemplos de aplicação.** Vamos ver como as regras anteriores (axiomas e teoremas) podem ser aplicadas na prática. Os exemplos que vão seguir-se referem-se quase todos a *jogos de sorte,* também chamados *jogos de azar* (atribuindo aqui à palavra 'azar' o significado de 'acaso'). Na verdade, foram as reflexões de alguns matemáticos sobre jogos de azar que deram origem ao cálculo das probabilidades. Mais adiante trataremos de exemplos mais importantes.

EXEMPLO 1. Consideremos o caso do lançamento de um dado *ao acaso* e sejam α_1, α_2, ..., α_6 os acontecimentos *'sair o n.º* 1' *'sair o n.º* 2', ..., *'sair o número* 6'. Se o dado é *imperfeito,* isto é, se não se aproxima bastante de um cubo ou se é sensivelmente não homogéneo (por exemplo, mais denso nuns pontos que noutros), as probabilidades

$$P(\alpha_1),\ P(\alpha_2),\ \ldots,\ P(\alpha_6)$$

não são sensivelmente iguais, mas poderão ser determinadas *empiricamente* com maior ou menor aproximação. (*Como?*)

Seja porém como for, o acontecimento *'sair número primo menor que* 5' é, neste caso, $\alpha_2 + \alpha_3$ e, portanto, a sua probabilidade será:

$$P(\alpha_2+\alpha_3) = P(\alpha_2) + P(\alpha_3) \qquad (\textit{Porquê?})$$

Por sua vez, o acontecimento 'sair número par' é $\alpha_2+\alpha_4+\alpha_6$ e portanto, a sua probabilidade será:

$$P(\alpha_2 + \alpha_4 + \alpha_6) = P(\alpha_2) + P(\alpha_4) + P(\alpha_6) \quad (\textit{porquê?})$$

e analogamente em outros casos.

Suponhamos, agora, que o dado é perfeito. Então será por definição:

$$P(\alpha_1) = P(\alpha_2) = P(\alpha_3) = P(\alpha_4) = P(\alpha_5) = P(\alpha_6)$$

isto é, os casos possíveis $\alpha_1,\alpha_2,\ldots,\alpha_6$ são todos *igualmente prováveis*. Designemos por p o valor comum destas probabilidades. Visto que os acontecimentos $\alpha_1,\alpha_2,\ldots,\alpha_6$ são incompatíveis dois a dois e a sua soma lógica é 1 (*porquê?*), virá:

$$P(\alpha_1) + P(\alpha_2) + P(\alpha_3) + P(\alpha_4) + P(\alpha_5) + P(\alpha_6) = 6\ p = 1$$

e, portanto:

$$p = \frac{1}{6}$$

isto é, *a probabilidade de sair um determinado número, qualquer que ele seja, é* 1/6.

Posto isto, a probabilidade de *'sair número primo menor que* 5' será:

$$P(\alpha_2+\alpha_3) = P(\alpha_2) + P(\alpha_3) = \frac{1}{6} + \frac{1}{6} = \frac{2}{6} = \frac{1}{3};$$

a probabilidade de *sair número par será:*

$$P(\alpha_2+\alpha_4+\alpha_6) = P(\alpha_2) + P(\alpha_4) + P(\alpha_6) = \frac{3}{6} = \frac{1}{2}, \text{ etc.}$$

Estes exemplos conduzem-nos à seguinte regra prática, que durante muito tempo foi tomada como definição da probabilidade(1):

REGRA. *Quando os casos possíveis numa dada prova* $\mathcal{P}$ *são todos igualmente prováveis, a probabilidade de um acontecimento* α *relativo a* $\mathcal{P}$ *é igual ao quociente* ν/n *do número* ν *de casos favoráveis a* α *pelo número* n *de casos possíveis.*

Chama-se aqui 'casos possíveis' àqueles acontecimentos possíveis, de que todos os outros são somas lógicas, e 'casos favoráveis a um acontecimento α', precisamente, aos casos de que α é soma lógica. Pressupõe-se, além disso, que os *casos possíveis são em número finito.*

EXEMPLO 2. Imaginemos uma esfera de lotaria que contenha 20 bolas, numeradas de 1 a 20, das quais 8 são brancas, 7 vermelhas e 5 amarelas (2). Consideremos a prova $\mathcal{P}$ que consiste em *extrair uma bola da esfera ao acaso* e designemos por $\alpha_1, \alpha_2, \ldots, \alpha_{20}$ os acontecimentos 'sair o n.º 1', 'sair o n.º 2', ..., 'sair o n.º 20'. Serão estes, portanto, os *casos possíveis da prova* $\mathcal{P}$. Serão eles *equiprováveis*? Se as bolas são sensivelmente iguais em forma, dimensões e substância, e se além disso a *casualização* é bem feita (isto é, se as bolas são bem agitadas na esfera e se a extracção é feita automaticamente, sem escolha humana deliberada), é de admitir que sim, isto é, mostra a experiência que

$$P(\alpha_1) = P(\alpha_2) = \ldots = P(\alpha_{20}) \text{ (com grande aproximação).}$$

---

(1) Tal definição era inaceitável por conter um *círculo vicioso:* não se pode definir um conceito, utilizando esse mesmo conceito.

(2) Em vez de uma esfera da lotaria, podemos também considerar uma caixa com pequena abertura ou um saco, como os que se usam no jogo do loto. Dum modo geral, chama-se *urna*, em cálculo das probabilidades, um recipiente destinado a conter bolas, ou outros objectos, para fazer sorteios.

Nestas condições, podemos aplicar a regra prática anterior ao cálculo de probabilidades de vários acontecimentos:

a) *Probabilidade de que saia o n.º 10.* Número de casos possíveis: 20. Número de casos favoráveis: 1. Probabilidade pedida: 1/20.

b) *Probabilidade de que saia bola branca.* Como agora o número de casos favoráveis é 8, a probabilidade pedida será:

$$\frac{8}{20} = 0{,}4 = 40\,\%$$

c) *Probabilidade de que saia bola vermelha.* Obtém-se de modo análogo: $\frac{7}{20} = 0{,}35 = 35\,\%$.

d) *Probabilidade de sair bola amarela:* $\frac{5}{20} = 0{,}25$.

e) *Probabilidade de sair bola amarela ou vermelha.* Este acontecimento é soma lógica dos acontecimentos 'sair bola amarela' e 'sair bola vermelha', que são *incompatíveis entre si.* Logo, a probabilidade pedida é a soma das duas anteriores:

$$\frac{7}{20} + \frac{5}{20} = \frac{12}{20} = 0{,}6 = 60\,\%$$

O mesmo resultado se podia obter, notando que o acontecimento considerado é o contrário de 'sair bola branca'. Assim, a probabilidade pedida é:

$$1 - \frac{8}{20} = \frac{12}{20} = 0{,}6$$

f) *Probabilidade de sair bola preta:* 0 (*Porquê?*)

g) *Probabilidade de sair número inferior a cem:* 1 (*Porquê?*)

Se designarmos por B, V e A, respectivamente, os acontecimentos

'sair bola branca', *'sair bola vermelha'* e *'sair bola amarela'*, relativos à prova $\mathcal{P}$, teremos em resumo:

$$P(B) = 0{,}4, \quad P(V) = 0{,}35, \quad P(A) = 0{,}25$$

$$P(A + V) = 0{,}6, \quad P(B + V) = 0{,}75, \quad P(A + B + V) = 1$$

Muitas vezes, usa-se em cálculo das probabilidades o mesmo símbolo para designar um acontecimento e o conjunto correspondente. Por exemplo, o símbolo B pode designar indistintamente o acontecimento *'sair bola branca'* ou o *conjunto das bolas brancas* (existentes na esfera).

EXEMPLO 3. Consideremos, agora, duas esferas de lotaria, E_1 e E_2. Suponhamos que E_1 contém 20 bolas, nas condições do exemplo anterior, e que E_2 contém 10 bolas, numeradas de 1 a 10, sendo 7 brancas e 3 vermelhas (sensivelmente iguais em forma, volume e substância). Seja agora $\mathcal{P}$ a prova que consiste em extrair *ao acaso* uma bola de cada uma das esferas. É claro que os casos possíveis podem ser esquematicamente indicados pelos elementos do *produto cartesiano*,

$$\{1,2,...,20\} \times \{1,2,...,10\}$$

Por exemplo, o par ordenado (14,5) indica o caso que consiste em sair a bola 14 da esfera E_1 e a bola 5 da esfera E_2. Ora, o número de tais pares ordenados é $20 \times 10 = 200$. *Será, pois,* 200 *o número de casos possíveis.* Serão estes casos equiprováveis? É de admitir que sim, uma vez que as bolas sejam sensivelmente iguais, como se disse, e que a casualização seja bem feita; em particular as esferas E_1 e E_2 devem ser *independentes,* isto é, *a bola que sair de uma das esferas não depender de modo algum da bola que sair da outra esfera.*

Aceites estas premissas, podemos efectuar os seguintes cálculos:

a) *Probabilidade de que saia bola branca das duas esferas.*

Já sabemos que o número de casos possíveis é 20×10. O número de casos favoráveis será, manifestamente, o cardinal do produto cartesiano do conjunto das bolas brancas de E_1 (em número de 8) pelo conjunto das bolas brancas de E_2 (em número de 7). Será, pois, 8×7 o número de casos favoráveis e, assim, a probabilidade pedida é:

$$\frac{8 \times 7}{20 \times 10} = \frac{28}{100} = 0{,}28$$

b) *Probabilidade de que saia bola branca de* E_1 *e bola vermelha de* E_2. Obtém-se de modo análogo:

$$\frac{8 \times 3}{20 \times 10} = \frac{12}{100} = 0{,}20$$

c) *Probabilidade de sair bola amarela das duas esferas.*

d) *Probabilidade de sair de* E_1 *número duplo do que sair de* E_2. Resposta: 5 %.

e) *Probabilidade de não sair bola branca de nenhuma das esferas.*

f) *Probabilidade de sair bola branca de uma, pelo menos, das esferas.* (Sugestão: acontecimento contrário do anterior.)

g) *Probabilidade de sair bola branca de uma e uma só esfera.* (Sugestão: este acontecimento é soma lógica dos acontecimentos incompatíveis 'sair bola branca de E_1 e não sair bola branca de E_2', 'sair bola branca de E_2 e não sair bola branca de E_1'.)

EXEMPLO 4. Consideremos, novamente, uma esfera com a composição do exemplo 2 (20 bolas equiprováveis, sendo 8 brancas, 7 vermelhas e 5 amarelas). Designemos por $\mathcal{P}'$ a prova que consiste em duas extracções sucessivas, *repondo na esfera a bola que sai na*

1ª extracção; e por $\mathcal{P}''$ a prova que consiste em duas extracções sucessivas, *sem reposição*. Calculemos, então:

a) *Probabilidade de sair duas vezes bola branca na prova* $\mathcal{P}'$. Número de casos possíveis (equiprováveis): 20 × 20. Número de casos favoráveis: 8 × 8. Probabilidade pedida:

$$\frac{8 \times 8}{20 \times 20} = 0{,}4 \times 0{,}4 = 0{,}16$$

b) *Probabilidade de sair duas vezes bola branca na prova* $\mathcal{P}''$. Número de casos possíveis (equiprováveis): 20 × 19. Número de casos favoráveis: 8 × 7. Probabilidade pedida:

$$\frac{8 \times 7}{20 \times 19} = \frac{28}{190} \approx 0{,}19$$

c) *Probabilidade de sair primeiro bola branca e depois bola vermelha na prova* $\mathcal{P}'$

d) *Idem na prova* $\mathcal{P}''$

e) *Probabilidade de sair uma vez bola branca e outra vez bola vermelha, independentemente de ordem (prova* $\mathcal{P}'$ *e prova* $\mathcal{P}''$) (Sugestão soma lógica dos acontecimentos 'sair primeiro bola branca e depois bola evermelha sair primeiro bola vermelha e depois bola branca'.)

f) *Probabilidade de não sair vez nenhuma bola branca (prova* $\mathcal{P}'$ *e prova* $\mathcal{P}''$) (Sugestão acontecimento equivalente a 'sair duas vezes bola vermelha ou amarela')

g) *Probabilidade de sair alguma vez bola branca (prova* $\mathcal{P}'$ *e prova* $\mathcal{P}''$) (Acontecimento contrário do anterior.)

h) *Probabilidade de sairem duas bolas da mesma cor (prova* $\mathcal{P}'$ *e prova* $\mathcal{P}''$).

i) *Probabilidade de sairem duas bolas de cor diferente (prova* $\mathcal{P}'$ *e prova* $\mathcal{P}''$).

EXEMPLO 5. Tornemos ao caso de um dado perfeito. É agora fácil calcular as seguintes probabilidades:

a) *Probabilidade de que, em dois lances sucessivos, se obtenha uma vez um número par e outra vez um múltiplo de 3.*

b) *Probabilidade de que, em 3 lances sucessivos, não saiam os números 1 e 6.*

c) *Probabilidade de que, em 2 lances sucessivos, a soma dos números saídos seja menor que 5.*

EXEMPLO 6. Um cofre tem um segredo de 3 discos, com 24 letras cada um (ver pág. 163, 1.º tomo). *Calcular a probabilidade que um ladrão teria de descobrir o segredo, fazendo no máximo 100 tentativas.* Resposta: aproximadamente 0,007 ou seja 7 ‰.

EXEMPLO 7. *Calcular a probabilidade de, jogando uma vez no totobola com o equivalente a 9 600 apostas simples* (1), *se acertar nos 13 resultados, supondo que as apostas são feitas inteiramente ao acaso.* Resposta: aproximadamente 0,006, probabilidade ainda extremamente pequena (compare com o resultado anterior).

14. **Probabilidade do produto lógico.** Da axiomática do conceito de probabilidade (n.º 12), nada se pode deduzir quanto à probabilidade do produto lógico. Mas, por analogia com o que se fez para o conceito de frequência relativa, é natural introduzir a seguinte definição:

DEFINIÇÃO 1. *Sendo* α *e* β *dois acontecimentos relativos a uma dada prova, chama-se probabilidade de* α *se* β, *e representa-se por* $P(\alpha|\beta)$, *o quociente de* $P(\alpha\beta)$ *por* $P(\beta)$, *isto é:*

$$(1) \qquad P(\alpha|\beta) = \frac{P(\alpha\beta)}{P(\beta)}$$

(1) O que importa em 14 400$00 — (Valor calculado ao preço de cada aposta, ao tempo — N. do E.).

Por exemplo, seja α o acontecimento 'haver acidente numa viagem de automóvel em 100 km de estrada' e β o acontecimento 'ter chovido'. Então, supondo que podemos atribuir probabilidades aos acontecimentos α, β, $\alpha\beta$, o símbolo $P(\alpha|\beta)$ designa a probabilidade de *haver um tal acidente, após ter chovido.*

DEFINIÇÃO 2. *Diz-se que dois acontecimentos α, β são independentes, sse* $P(\alpha|\beta) = P(\alpha)$. *Caso contrário, α e β dizem-se dependentes ou associados.*

Notemos, agora, que (1) se pode escrever:

$$(P\alpha\beta) = P(\beta) \cdot P(\alpha|\beta)$$

ou ainda, trocando os papéis de α e de β:

(2) $$\boxed{P(\alpha\,\beta) = P(\alpha) \cdot P(\beta|\alpha)}$$

É evidente que esta fórmula apenas exprime a definição 1, sob uma forma diferente. Por outro lado, tem-se, atendendo à definição 2:

(3) $$\boxed{P(\alpha\beta) = P(\alpha)\ P(\beta),\ \text{sse}\ \alpha\ \text{e}\ \beta\ \text{são independentes}}$$

NOTA IMPORTANTE. O conceito de 'acontecimentos independentes' desempenha, em relação ao produto lógico, um papel análogo ao de 'acontecimentos incompatíveis', em relação à soma lógica. *Não confunda estes dois conceitos!*

Tratando-se de três acontecimentos α, β, γ relativos a uma prova $\mathcal{P}$ é fácil reconhecer qual o significado de símbolos tais como $\mathcal{P}(\alpha|\beta\gamma)$, $P(\gamma|\alpha\beta)$, etc. e ver que (cf. n.º 6, pág. 216):

(4) $$P(\alpha\,\beta\,\gamma) = P(\alpha) \cdot P(\beta|\alpha) \cdot P(\gamma|\alpha\,\beta)$$

Em particular, pode ter-se:

$$P(\alpha\,\beta\,\gamma) = P(\alpha) \cdot P(\beta) \cdot P(\gamma) \tag{5}$$

DEFINIÇÃO 3. *Diz-se que três acontecimentos* α, β, γ *são independentes, sse verificam as condições* $P(\beta) = P(\beta|\alpha)$, $P(\gamma) = P(\gamma|\alpha\,\beta)$ *e todas as que se deduzem destas, substituindo um ou mais dos acontecimentos* α, β, γ *pelos respectivos contrários.*

Em termos intuitivos poderíamos dizer:

'Três acontecimentos são *independentes,* sse a probabilidade de cada um deles é a mesma, quer se verifique ou não um só ou os dois outros acontecimentos'.

É evidente que a anterior definição equivale à seguinte proposição:

Três acontecimentos α, β, γ, *são independentes sse, além da condição* (5), *verificam todas as que desta se deduzem, substituindo um ou mais dos acontecimentos* α, β, γ, *pelos seus contrários.*

Isto mostra que a relação ternária definida é simétrica.
É porém de notar que, tal como no caso das frequências relativas:

1) Três acontecimentos α, β, γ podem ser independentes entre si dois a dois sem serem *os três* independentes (segundo a definição anterior).

2) Pode verificar-se a fórmula (5), sem que os acontecimentos α, β, γ sejam independentes.

15. **Probabilidade do produto cartesiano. Sistemas de lotaria.** Para melhor compreensão do que vai seguir-se, convém recordar algumas situações que surgem, em geometria aplicada, a propósito de produtos cartesianos. Viu-se que, por exemplo, no

universo IR, a condição $x \geqslant 2$, com *uma só* variável, pode ser identificada à condição *com duas variáveis*

$$x \geqslant 2 \wedge y \in \mathbb{R}$$

que é verificada por todos os pares ordenados (x, y) de números reais tais que: $x \geqslant 2$ e y é *qualquer*. Deste modo, a condição $x \geqslant 2$, que na recta representa geometricamente uma *semi-recta*, no plano passa a representar um *semiplano*. Analogamente, a condição $y \geqslant 1$, que na recta (ou mais precisamente no eixo dos y) representa uma semi-recta, pode ser identificada com a condição

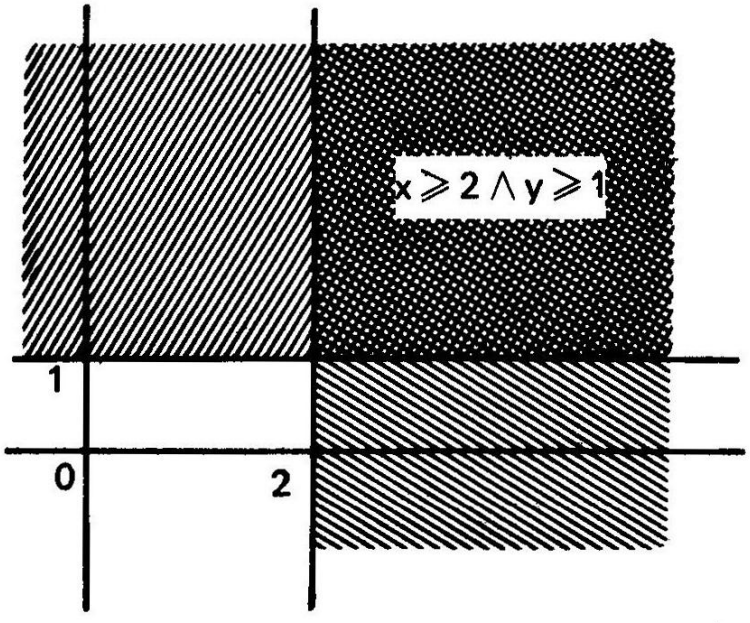
$$x \in \mathbb{R} \wedge y \geqslant 1,$$

e assim, no plano, passa a representar um semiplano.

Por sua vez, a condição

$$x \geqslant 2 \wedge y \geqslant 1$$

representa no plano um ângulo recto, que é a *intersecção* (ou produto *lógico*) dos semiplanos $x \geqslant 2$ e $y \geqslant 1$. Este produto lógico resulta



assim identificado ao *produto cartesiano* das semi-rectas representadas pelas condições $x \geqslant 2$ e $y \geqslant 1$, respectivamente no eixo dos x e no eixo dos y.

Consideremos, agora, duas esferas de lotaria, E_1 e E_2, nas condições indicadas no exemplo 3 do n.º 13. Designemos por $\mathcal{P}_1$ a prova que consiste em extrair ao acaso uma bola de E_1, por $\mathcal{P}_2$ a prova análoga para E_2 e por $\mathcal{P}'$ a prova que consiste em efectuar $\mathcal{P}_1$ e $\mathcal{P}_2$. Diremos, então, que $\mathcal{P}'$ é o produto cartesiano de $\mathcal{P}_1$ e $\mathcal{P}_2$ e escreveremos:

$$\mathcal{P}' = \mathcal{P}_1 \times \mathcal{P}_2$$

Sejam B_1, V_1 e A_1, respectivamente, os acontecimentos *sair bola branca, sair bola vermelha* e *sair bola amarela,* na prova $\mathcal{P}_1$. Sejam ainda B_2 e V_2 os acontecimentos sair *bola branca* e *sair bola vermelha,* na prova $\mathcal{P}_2$. Então, designaremos por $B_1 \times V_2$ (produto cartesiano de B_1 por V_2) o acontecimento sair bola branca de E_1 e bola vermelha de E_2. Análogos significados terão as expressões:

$$V_1 \times B_2,\ A_1 \times V_2,\ B_1 \times B_2,\ V_1 \times V_2,\ A_1 \times B_2$$

Notemos, agora, que o acontecimento B_1 relativo a $\mathcal{P}_1$ se pode identificar a um acontecimento B_1^* relativo a $\mathcal{P}_1 \times \mathcal{P}_2$: o acontecimento

Sair bola branca de E_1 *e bola qualquer de* E_2

De modo análogo, V_1, A_1, B_2, V_2 podem ser identificados a acontecimentos, respectivamente, V_1^*, A_1^*, B_1^* e V_2^*, relativos a $\mathcal{P}_1 \times \mathcal{P}_2$. Assim, podemos reduzir os *produtos cartesianos* a *produtos lógicos:*

$$B_1 \times V_2^* = B_1^* V_2^* \ , \quad V_1 \times B_2 = V_1^* B_2^* \ , \quad \text{etc.}$$

Posto isto, recordemos que, segundo as condições indicadas no exemplo 3 do n.º 13, os acontecimentos B_1 e V_2^* são independentes (o mesmo podendo dizer-se agora dos acontecimentos B_1 e V_2).

Será assim:

$$P(B_1 \times V_2) = P(B_1^*) \cdot P(V_2^*) = P(B_1) \cdot P(B_2)$$

E, como $P(B_1) = 4/10$, $P(V_2) = 3/10$, virá:

$$P(B_1) \cdot P(V_2) = \frac{4}{10} \cdot \frac{3}{10} = \frac{12}{100}$$

tal como tínhamos achado. Analogamente:

$$P(B_1 \times B_2) = P(B_1) \cdot P(B_2) = 0{,}4 \times 0{,}7 = 0{,}28$$

$$P(V_1 \times B_2) = 0{,}7 \times 0{,}7 = 0{,}49, \text{ etc.}$$

Dum modo geral, se α e β são acontecimentos relativos a duas provas distintas $\mathcal{P}_1$ e $\mathcal{P}_2$, representa-se por $\mathcal{P}_1 \times \mathcal{P}_2$ a prova que consiste em efectuar $\mathcal{P}_1$ e $\mathcal{P}_2$, e por $\alpha \times \beta$ (*produto cartesiano de* α *por* β) o acontecimento que consiste em *realizar-se* α *em* $\mathcal{P}_1$ *e* β *em* $\mathcal{P}_2$. Os acontecimentos α e β podem ser identificados a acontecimentos, respectivamente α^* e β^*, relativos a $\mathcal{P}_1 \times \mathcal{P}_2$, tal como foi indicado no exemplo anterior, permitindo reduzir o produto cartesiano a produto lógico

$$\alpha \times \beta = \alpha^* \beta^*$$

Os acontecimentos α e β dizem-se *independentes,* sse α^* e β^* o forem. Assim, virá:

(1) $\boxed{P(\alpha \times \beta) = P(\alpha) \cdot P(\beta), \text{ sse } \alpha \text{ e } \beta \text{ são independentes}}$

As provas $\mathcal{P}_1$ e $\mathcal{P}_2$ dizem-se *independentes,* sse todo o acontecimento relativo a $\mathcal{P}_1$ é independente de todo o acontecimento relativo a $\mathcal{P}_2$.

A regra (1) permite resolver mais simplesmente vários dos problemas que foram resolvidos no n.º 13 por contagem de casos possíveis e casos favoráveis (veja quais são esses problemas e resolva-os pelo novo processo).

Estas considerações podem estender-se de maneira óbvia ao caso de três provas, quatro provas, etc., tendo em conta o que foi estabelecido no número anterior.

Por exemplo, um dos modernos sistemas de lotaria mais em uso consiste em utilizar, por exemplo, 6 esferas em que se introduzem bolas cuja numeração pode ir de 0 a 9; uma das esferas é destinada a dar o algarismo das unidades, outra a dar o número das centenas, etc.

Em princípio, as extracções das diferentes esferas devem ser provas independentes, isto é, a probabilidade de saída de uma dada sequência de algarismos deve ser exactamente igual ao produto das probabilidades de saída de um algarismo de cada esfera. Além disso, os algarismos de cada esfera devem ter todos a mesma probabilidade de saída. Assim, por exemplo, num jogo com 300 000 bilhetes, a probabilidade de ser premiado um determinado número na primeira extracção deverá ser *exactamente* igual a

$$\frac{1}{3}\cdot\frac{1}{10}\cdot\frac{1}{10}\cdot\frac{1}{10}\cdot\frac{1}{10}\cdot\frac{1}{10}=\frac{1}{300\,000}$$

Já sabemos que não é possível, nem sequer faz sentido, falar de *exactidão absoluta*. O que se requer na prática é que seja impossível

detectar estatisticamente alguns números com maior probabilidade de saída, visto que esse facto poderia ser explorado ilicitamente por uma casa de jogo.

Assim, quando uma casa de jogo anuncia comercialmente que é contemplada com maior número de prémios, isso apenas deve significar que a referida casa vende um maior número de bilhetes, o que, evidentemente, aumenta a probabilidade de prémio. Qualquer outra interpretação equivaleria a admitir que essa casa está a usar ilicitamente o conhecimento de algum vício do sistema.

16. **Problema das provas repetidas; distribuição binomial.** Consideremos, por exemplo, o seguinte problema:

Determinar a probabilidade de que, em três lançamentos sucessivos dum dado perfeito, saia duas vezes (e só duas) o número 6.

Os três lançamentos sucessivos são três provas $\mathcal{P}_1$, $\mathcal{P}_2$, $\mathcal{P}_3$, que constituem realizações distintas de uma mesma prova-tipo $\mathcal{P}$ (lançamento do dado) A sequência dessas três provas constitui por sua vez, a prova

$$\mathcal{P}_1 \times \mathcal{P}_2 \times \mathcal{P}_3$$

Designemos por s_1, s_2, s_3, respectivamente, os acontecimentos *'sair o n.º 6 em* $\mathcal{P}_1$*'*, *'sair o n.º 6 em* $\mathcal{P}_2$*'*, *'sair o n.º 6 em* $\mathcal{P}_3$*'* Então o acontecimento *'sair o n.º 6 duas vezes (e duas só) em* $\mathcal{P}_1 \times \mathcal{P}_2 \times \mathcal{P}_3$*'* pode realizar-se de três maneiras distintas e incompatíveis:

(1) $$s_1 \times s_2 \times \tilde{s}_3, \quad s_1 \times \tilde{s}_2 \times s_3, \quad \tilde{s}_1 \times s_2 \times s_3$$

Ora, $P(s_1) = P(s_2) = P(s_3) = 1/6$ e, portanto,

$$P(\tilde{s}_1) = P(\tilde{s}_2) = P(\tilde{s}_3) = 1 - 1/6.$$

Por outro lado, é fácil reconhecer que os três acontecimentos s_1, s_2, s_3 são independentes (discutiremos este ponto mais adiante, no caso geral). Logo, os acontecimentos (1) têm todos probabilidade igual a

$$P(s_1 \times s_2 \times \tilde{s}_3) = P(s_1)\, P(s_2)\, P(\tilde{s}_3) = \left(\frac{1}{6}\right)^2 \frac{5}{6} = \frac{5}{216}$$

Mas o acontecimento cuja probabilidade se pede é a soma lógica dos referidos acontecimentos incompatíveis:

$$s_1 \times s_2 \times \tilde{s}_3 + s_1 \times \tilde{s}_3 \times s_3 + \tilde{s}_1 \times s_2 \times s_3$$

A probabilidade pedida será, pois, a soma de 3 números iguais a 5/216, ou seja:

$$3 \cdot \frac{5}{216} = \frac{5}{72} \approx 7\,\%$$

Consideremos, ainda, o problema análogo:

De uma urna que contém 10 bolas, das quais 3 são brancas e 7 pretas, tiram-se 4 bolas à sorte, sucessivamente, com reposição. Determinar a probabilidade de que seja 2 o número de bolas brancas saídas nas 4 extracções.

Designando por B_1, B_2, B_3, B_4 o acontecimento *saída de bola branca* nas sucessivas extracções, o acontecimento cuja probabilidade se pede será a soma lógica das seguintes hipóteses incompatíveis duas a duas:

$$B_1 \times B_2 \times \tilde{B}_3 \times \tilde{B}_4,\ B_1 \times \tilde{B}_2 \times B_3 \times \tilde{B}_4,\ B_1 \times \tilde{B}_2 \times \tilde{B}_3 \times B_4$$

$$\tilde{B}_1 \times B_2 \times B_3 \times \tilde{B}_4,\ \tilde{B}_1 \times B_2 \times \tilde{B}_3 \times B_4,\ \tilde{B}_1 \times \tilde{B}_2 \times B_3 \times B_4$$

Como interpretar o número destas hipóteses em cálculo combinatório? Pense por si uns momentos, antes de ver a resposta que vem a seguir.

É fácil reconhecer que estas hipóteses estão em correspondência biunívoca com as *combinações*

$$B_1B_2,\ B_1B_3,\ B_1B_4,\ B_2B_3,\ B_2B_4,\ B_3B_4,$$

dos acontecimentos B_1, B_2, B_3, B_4 tomados 2 a 2. O seu número é, pois:

$$\binom{4}{2} = \frac{4 \times 3}{1 \times 2} = 6$$

Por outro lado, os acontecimentos B_1, B_2, B_3, B_4 têm todos a probabilidade 3/10 e, portanto, os seus contrários têm a probabilidade 7/10. E, como se trata de acontecimentos independentes (1), segue-se que todas as referidas hipóteses têm a mesma probabilidade:

$$P(B_1 \times B_2 \times \tilde{B}_3 \times \tilde{B}_4) = \left(\frac{3}{01}\right)^2 \left(\frac{7}{10}\right)^2$$

Por conseguinte, a probabilidade pedida será a soma de 6 parcelas iguais a este número, ou seja:

$$\binom{4}{2} \cdot \left(\frac{3}{10}\right)^2 \left(\frac{7}{10}\right)^2 = 6 \times 21^2 \times 10^{-4} = 0{,}2646$$

Estes dois exemplos ajudam-nos a resolver o seguinte problema geral, muito importante:

PROBLEMA DAS PROVAS REPETIDAS. *Sendo* α *um acontecimento de probabilidade* p, *relativo a uma prova* $\mathcal{P}$, *determinar a probabilidade de que, em* n *realizações de* $\mathcal{P}$, *seja* x *o número de vezes que* α *se verifica.*

Como se vê, o que se pede afinal é a *probabilidade de que em* n *realizações de* $\mathcal{P}$, *a preferência absoluta de* α *seja um dado número inteiro* x $(0 \leqslant x \leqslant n)$.

---

(1) Este ponto será esclarecido a seguir, no caso geral.

Designemos por $\mathcal{P}_1$, $\mathcal{P}_2$, , $\mathcal{P}_n$ as n realizações de $\mathcal{P}$ e, dum modo geral, por α_k o acontecimento que consiste em *verificar-se* α *na prova* $\mathcal{P}_k$ (k=1, 2, ..., n) Então, o acontecimento

$$x\,\alpha = \textit{verificação de } \alpha \textit{ em } x \textit{ das } n \textit{ provas consideradas}$$

é a soma lógica de todos os acontecimentos que resultam de

$$\alpha_1 \times \alpha_2 \times \cdots \times \alpha_n,$$

deixando ficar x factores como estão e substituindo os n-x restantes pelos acontecimentos contrários. Um deles será o acontecimento

$$\alpha_1 \times a_2 \times \cdots \times \alpha_x \times \tilde{\alpha}_{x+1} \times \cdots \times \tilde{\alpha}_n,$$

que consiste em verificar-se α precisamente nas primeiras x provas da sequência.

Qual é o número de hipóteses assim obtidas? Pensando um momento, vê-se que é igual ao número de combinações dos acontecimentos $\alpha_1, \alpha_2, \ldots, \alpha_n$ tomados x a x, ou seja $\binom{n}{x}$. Ora

$$P(\alpha_k) = p, \quad P(\tilde{\alpha}_k) = 1 - p, \quad \text{para } k=1, 2, \ldots, n$$

Além disso, os acontecimentos $\alpha_1, \alpha_2, \ldots, \alpha_n$ são *independentes*. Com efeito, do próprio conceito de probabilidade (n.os 11 e 12) decorre naturalmente que a probabilidade de α se verificar em cada uma das provas $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_n$ (n realizações sucessivas de $\mathcal{P}$, em condições idênticas) é sempre a mesma, qualquer que seja o resultado das restantes provas (cf. n.os 14 e 15). Logo, as hipóteses consideradas têm todas a probabilidade

$$P(\alpha_1 \times \cdots \times \alpha_x \times \tilde{\alpha}_{x+1} \times \cdots \times \tilde{\alpha}_n) = p^x(1-p)^{n-x}$$

Ora, estas hipóteses são incompatíveis entre si duas a duas e o seu número é, como vimos $\binom{n}{x}$. Logo, a probabilidade pedida será:

$$P(x\alpha) = \binom{n}{x} p^x(1-p)^{n-x}$$

Assim o problema está resolvido.

Costuma simplificar-se a fórmula anterior escrevendo P(x) em vez de P(xα) e pondo 1−p=q:

(1) $$\boxed{P(x) = \binom{n}{x} p^x q^{n-x}}$$

Como se vê, x é uma variável casual (ver n.º 8), cujos valores possíveis são 0,1,...,n, e, a cada um destes valores, a fórmula (1) faz corresponder uma determinada probabilidade P(x). Exprime-se este facto dizendo que a fórmula (1) define *a distribuição de probabilidade da variável casual* x *considerada* (frequência absoluta de α em *n* realizações de P). Como, além disso, o segundo membro de (1) é precisamente o termo em p^x do desenvolvimento de $(p+q)^x$ segundo a *fórmula do binómio,* diz-se que a distribuição de probabilidade definida por (1) é a DISTRIBUIÇÃO BINOMIAL (também chamada *'distribuição de BERNOULLI'*).

Apresentam-se, na prática, muitas outras distribuições de probabilidade (1). Por exemplo, o número que sai no lançamento dum dado é uma variável casual x, cujos valores possíveis são 1, 2, 3, 4, 5, 6 e tal que

$$P(x) = \frac{1}{6}, \text{ sse o dado é perfeito.}$$

Se o dado é imperfeito a distribuição será outra.

---

(1) A par do conceito de 'distribuição de probabilidade' apresenta-se naturalmente o conceito de *'distribuição de frequência'*.

NOTA. A fórmula (1) pode ser demonstrada de maneira mais breve e mais rigorosa pelo *método de indução matemática,* que estudaremos mais tarde.

17. **Aplicações de distribuição binomial; exemplo da genética.** Diz-se que uma moeda é *equilibrada,* sse a probabilidade de aparecer escudo num lançamento da moeda ao ar é 1/2. Determinemos a probabilidade de que, em 10 lançamentos de uma moeda equilibrada, apareça x vezes escudo. Neste caso, basta aplicar a distribuição binomial com $p = 1/2$ e $q = 1 - 1/2 = 1/2$, o que dá:

$$P(x) = \binom{10}{x} \left(\frac{1}{2}\right)^x \left(\frac{1}{2}\right)^{10-x}$$

Por exemplo, se $x = 3$, vem:

$$P(3) = \binom{10}{3} \left(\frac{1}{2}\right)^3 \left(\frac{1}{2}\right)^7 = \frac{10 \cdot 9 \cdot 8}{3 \cdot 2 \cdot 1} \cdot \left(\frac{1}{2}\right)^{10} = \frac{15}{128} \approx 0{,}117$$

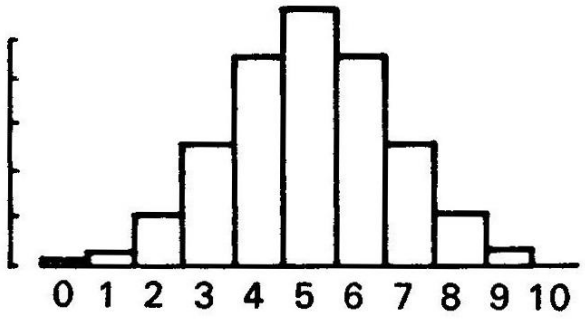
Os valores de P(x) para $x = 0, 1, \ldots, 10$, são dados pela tabela seguinte, com erro inferior a 0,001

Tabela

x	P(x)	x	P(x)
0	0,001	6	0,205
1	0,010	7	0,177
2	0,044	8	0,044
3	0,177	9	0,010
4	0,205	10	0,001
5	0,246		

Para ter uma imagem desta distribuição convém recorrer a um *gráfico de colunas* (ou *histograma*), que consiste neste caso em cons-

truir, para cada um dos valores de x considerados, um rectângulo de altura P(x) e de base 1, assente no eixo das abcissas, tendo esse valor de x por ponto médio. Convém, neste caso, adoptar uma unidade de comprimento bastante maior para as ordenadas do que para as abcissas.



Note-se que este histograma é simétrico (a distribuição *é simétrica*) e que P(x) atinge um valor máximo (= 0,246) para x = 5. É, portanto, 5 o *valor mais provável* da variável casual considerada, o que aliás era de esperar, visto que, sendo 1/2 a probabilidade de aparecer escudo, a frequência relativa mais provável deverá ser 50 % e, como o número de lançamentos é 10, a frequência absoluta mais provável é $0{,}5 \times 10 = 5$. Mas, note-se o seguinte facto curioso, aparentemente paradoxal:

É mais provável não se verificar o valor mais provável do que verificar-se este valor.

Com efeito, a probabilidade do valor mais provável é 0,246, enquanto a do acontecimento contrário é $1 - 0{,}246 = 0{,}754$. A explicação do *aparente paradoxo* é simples: o acontecimento contrário é a soma lógica dos acontecimentos que correspondem a *todos* os outros valores possíveis; embora menos prováveis, a soma das probabilidades destes é $0{,}754 \approx 75\,\%$.

Chama-se *moda* de uma distribuição de probabilidade de uma variável x (com um número finito de valores) todo o valor de x com

probabilidade máxima. A distribuição anterior tem uma única moda: o valor 5 (distribuição *unimodal*). Mas, se em vez de n = 10 tivéssemos tomado n = 11 (com p = 1/2), já encontraríamos duas modas: os valores 5 e 6 (distribuição *bimodal*). Há ainda distribuições *trimodais,* etc. A distribuição binomial só pode ser unimodal ou bimodal.

Tornando ao caso anterior (p = 1/2, n = 10), calculemos a probabilidade de que *x* satisfaça, por exemplo, à condição $3 \leqslant x \leqslant 7$, equivalente à soma lógica das condições x = 3, x = 4, x = 5, x = 6, x = 7. Será, pois:

$$P(3 \leqslant x \leqslant 7) = \sum_{k=3}^{7} \binom{10}{k} \left(\frac{1}{2}\right)^k \left(\frac{1}{2}\right)^k$$

$$\approx 2 \times 0{,}117 + 2 \times 0{,}205 + 0{,}246 \approx 0{,}89$$

Podemos também dizer que *é* 89 % *a probabilidade duma frequência relativa* f *do acontecimento 'aparecer escudo' tal que* $0{,}3 \leqslant f \leqslant 0{,}7$, *numa sequência de* 10 *provas.*

Passando a uma sequência de 100 provas, as frequências absolutas correspondentes às frequências relativas 0,3 e 0,7 são 0,3 × 100 = 30 e 0,7 × 100 = 70. Será, então:

$$P(30 \leqslant x \leqslant 70) = \sum_{k=30}^{70} \binom{100}{k} \left(\frac{1}{2}\right)^k \left(\frac{1}{2}\right)^k$$

Porém, os cálculos exigidos por esta fórmula são demasiado laboriosos, mesmo que se recorra ao *triângulo aritmético*. Por métodos que se estudam em matemática superior, é possível achar o valor aproximado 0,9994 para esta probabilidade, efectuando cálculos muito simples e utilizando uma tabela numérica (tabela da *distribuição normal* ou *distribuição de Gauss*) (1). Podemos, portanto, garantir com

(1) Em vez de 'distribuição binomial', 'distribuição normal', etc. também se diz 'lei binomial', 'lei normal', etc.

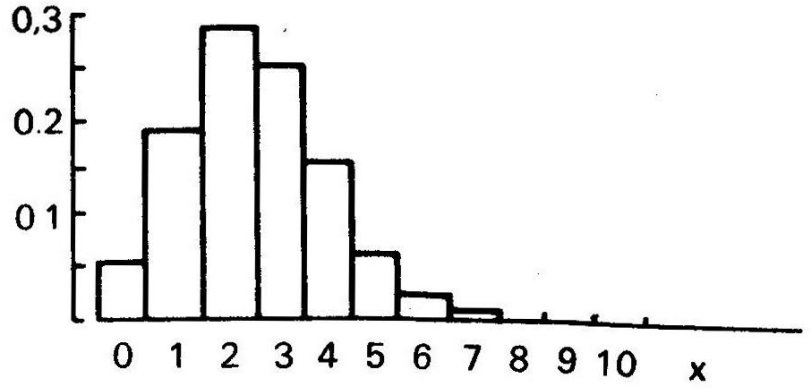
grande segurança (isto é, com pequeníssima probabilidade de errar) que, numa sequência de 100 provas, a frequência relativa do acontecimento considerado estará no intervalo fechado de extremos 0,3 e 0,7 (cf. considerações do n.º 9, pág. 224).

Assim, a distribuição binomial vem lançar nova luz sobre as relações entre o conceito de probabilidade e o conceito de frequência relativa.

Suponhamos, agora, $p = 1/4$ e $n = 10$. Neste caso, a distribuição binomial será, concretamente:

$$(1) \qquad P(x) = \binom{10}{x}\left(\frac{1}{4}\right)^x\left(\frac{3}{4}\right)^{10-x}$$

Na figura que a seguir se apresenta é dado o histograma desta distribuição, que já *não é simétrica*. Temos ainda aqui uma distribuição unimodal, sendo a *moda* o valor $x = 2$.



A distribuição binomial encontra importantes aplicações nos mais diversos domínios: na biologia, na psicologia, etc. Vamos apresentar um exemplo relativo à *genética,* ramo da biologia que estuda cientificamente os fenómenos da hereditariedade.

Segundo as experiências de MENDEL (1), relativas ao cruzamento de certas plantas *de flor genuinamente vermelha com outras*

(1) Monge austríaco (Silésia), fundador da Genética (1822-1884).

de flor genuinamente branca, verifica-se que, na primeira geração, todas as plantas dão flor vermelha *(carácter dominante),* ao passo que, na segunda geração (resultante dos cruzamentos entre híbridos da primeira geração), há a probabilidade 3/4 de aparecer uma planta de flor vermelha e a probabilidade 1/4 de aparecer uma planta de flor branca ('carácter recessivo') (1).

Assim, a probabilidade de, em 10 indivíduos da 2.ª geração, aparecerem x plantas de cor branca é dada pela fórmula (1).

Se, em vez de 10, consideramos 500 indivíduos, o *valor esperado* do número de indivíduos de flor branca (na 2.ª geração), será:

$$\frac{1}{4} \times 500 = 125$$

Mas o *valor observado* será geralmente diferente do valor esperado, sendo a diferença entre o primeiro e o segundo *(desvio* ou *discrepância)* devido ao *acaso.*

Por exemplo, a probabilidade de que, no conjunto dos referidos 500 indivíduos, o número de plantas de flor branca esteja compreendido entre 100 e 150, é dada pela expressão:

$$P\,(100 < x < 150) = \sum_{x=101}^{149} \binom{500}{x} \left(\frac{1}{4}\right)^x \left(\frac{3}{4}\right)^x$$

Todavia, tal como num dos exemplos anteriores, os cálculos exigidos por esta fórmula são impraticáveis. Utilizando o processo a que fizemos alusão (com o emprego duma *tabela da distribuição normal,* que não podemos aqui estudar), consegue-se facilmente obter o valor aproximado 0,003 para aquela probabilidade. É, portanto, quase certo que, no referido conjunto de 500 indivíduos, a frequência

---

(1) Recordemos que, em biologia, se usa o termo 'carácter' (plural 'caracres'), como sinónimo de 'atributo'.

relativa do atributo considerado esteja no intervalo aberto de extremos 0,2 e 0,3 ou mesmo numa vizinhança mais pequena de 0,25(1).

Para interpretar estes e outros resultados análogos de Mendel, o biologista americano T. H. MORGAN (1866-1945, Prémio Nobel 1933), introduziu a hipótese da existência de partículas materiais, chamadas *'genes'*, como factores de hereditariedade localizados nos cromossomas, conseguindo mesmo identificar a posição de alguns deles. Cada gene representa um carácter elementar: p. ex. 'flor vermelha' ou 'flor branca'. Todas as células de um indivíduo biológico (em particular, de cada um de nós, seres humanos) têm a mesma composição genética, sendo os genes de cada célula comparáveis às bolas de uma esfera de lotaria. Na verdade, como bolas de lotaria se comportam, em certa medida, essas minúsculas porções de matéria, no cruzamento de dois indivíduos, dando por vezes resultados imprevistos, ao entrarem na composição genética do novo ser: por exemplo, de pais com olhos castanhos pode nascer uma criança com olhos azuis, que recebe de um antepassado mais ou menos próximo o gene desse carácter, *segregado* na resultante genética dos progenitores.

18. **Casos extremos da distribuição binomial.** Como vimos, a distribuição binomial dá-nos a probabilidade de que, em n realizações duma prova $\mathcal{P}$, um acontecimento α de probabilidade p se verifique x vezes, sendo x um dado número inteiro tal que $0 \leqslant x \leqslant n$. Os dois casos extremos são, pois:

1) $x = n$ (o acontecimento α verifica-se nas n provas)

2) $x = 0$ (o acontecimento $\tilde{\alpha}$ verifica-se nas n provas)

---

(1) Chama-se *vizinhança* dum número real a qualquer intervalo com centro em *a*.

A probabilidade do primeiro caso é, evidentemente:

$$P(n) = p^n$$

A probabilidade do segundo caso é:

$$P(0) = q^n \quad (\text{com } q = 1-p)$$

Note-se, porém, que o contrário do acontecimento $x = 0$ não é o acontecimento $x = n$, mas sim o acontecimento que consiste em *α se verificar, pelo menos, uma vez nas* n *provas.*

A probabilidade desse acontecimento será, pois:

$$P(x \neq 0) = 1 - q^n = 1 - (1-p)^n = \sum_{x=1}^{n} (-1)^{x-1} \binom{n}{x} p^x$$

EXEMPLO 1. *Calcular a probabilidade de que, em* 6 *lances dum dado perfeito saia, pelo menos, uma vez o número* 1.

Neste caso $p = 1/6$, $n = 6$ e, portanto:

$$P(x \neq 0) = 1 - \left(\frac{5}{6}\right)^6 = \frac{31031}{46656} \approx 66\,\%$$

EXEMPLO 2. *Calcular a probabilidade de que, comprando ao todo mil bilhetes em mil lotarias sucessivas de* 100 000 *números, se tenha ao menos uma vez a sorte grande.*

Agora é $p = 10^{-5}$, $n = 1000$ e, portanto:

$$P(x \neq 0) = 1 - \left(1 - \frac{1}{10^5}\right)^{1000} = \frac{1000}{100\,000} - \binom{1000}{2} \frac{1}{100\,000^2} + \ldots$$

$$= 0{,}01 - 0{,}000\,0495 + \ldots \approx 0{,}00995$$

A probabilidade pedida é, pois, praticamente igual a 1 % (os termos omitidos no desenvolvimento são desprezíveis).

19. **Valor médio, esperança matemática. Jogos equitativos.** Tornemos ao exemplo da tabela n.º 1 da pág. 204. Suponhamos que se trata de achar a *média* das classificações dadas no exame em questão. Como se procede? É bem conhecido o processo:

Multiplica-se cada classificação pelo número de alunos que a obtiveram e divide-se o resultado pelo número total de alunos.

Dum modo geral, consideremos uma variável casual x que toma *m* valores reais

$$x_1,\ x_2,\ \ldots,\ x_m$$

respectivamente, com as *frequências absolutas*

$$\nu_1,\ \nu_2,\ \ldots,\ \nu_m$$

e seja $n = \nu_1+\nu_2+\ldots+\nu_m$. Chama-se *valor médio da variável* x (com esta distribuição de frequência) o número

$$\frac{\nu_1 x_1+\nu_2 x_2+\ldots+\nu_m x_m}{n}$$

que se representa por $M\{x\}$. É claro que, se pusermos

$$f_1 = \frac{\nu_1}{n}\ ,\quad f_2 = \frac{\nu_2}{n}\ ,\ \ldots,\ f_m = \frac{\nu_m}{n}$$

(frequências relativas de $x_1, x_2, \ldots, x_m$), virá:

$$M\{x\} = f_1x_1+f_2x_2+\ldots+f_mx_m = \sum_{k=1}^{m} f_kx_k \quad (\textit{Porquê?})$$

Em rigor, não deveríamos dizer *'valor médio da variável casual x'*, mas sim *'valor médio da sua distribuição de frequência (absoluta ou relativa)'*. Todavia, na prática, quando se fala de uma variável casual x, subentende-se geralmente que é dada uma distribuição de frequência ou de probabilidade dessa variável.

Como vimos, as probabilidades são *frequências relativas esperadas no futuro*. Haverá, portanto, um conceito correspondente ao de valor médio, quando passarmos de frequências a probabilidades.

DEFINIÇÃO. *Seja* x *uma variável casual que só pode tomar um número finito* r *de valores reais* $x_1,\ldots,x_r$, *com probabilidades respectivamente* $p_1,\ldots,p_r$. Chama-se *esperança matemática* (ou *valor esperado*) da variável x, e representa-se por $E\{x\}$, o número:

$$E\{x\} = p_1x_1+p_2x_2+\ldots+p_rx_r = \sum_{k=1}^{r} p_kx_k \ (^1)$$

Como exemplo, calculemos a esperança matemática duma variável x com distribuição binomial (ou, mais precisamente, a *esperança matemática da distribuição binomial)*. Por definição, é:

$$E\{x\} = \sum_{x=0}^{n} P(x) \cdot x,$$

com $P(x) = \binom{n}{x} p^x q^{n-x}$ e $q = 1 - p$. Será, pois:

$$E\{x\} = \sum_{x=0}^{n} x \cdot \frac{n!}{x!\ (n-x)!} p^x q^{n-x}$$

---

(1) Também se define 'esperança matemática' de uma variável casual com uma infinidade de valores possíveis, mas isso ultrapassa o carácter elementar desta introdução.

Visto o primeiro termo ser nulo (x=0), pode escrever-se:

$$E\{x\} = pn \cdot \sum_{x=0}^{n} \frac{(n-1)!}{(x-1)!(n-x)!} p^{x-1} q^{n-x}$$
$$= pn(p+q)^{n-1}$$

e, portanto:

$$E\{x\} = np$$

Por exemplo, sendo $p = 1/2$ e $n = 10$, a esperança matemática (ou valor esperado) da distribuição binomial é 5: exactamente igual à moda da distribuição (ver n.º 17). Mas, sendo $p=1/2$ e $n=11$, a distribuição binomial tem, como vimos, duas modas (5 e 6) e a sua esperança matemática é agora 5,5.

Muitas vezes, em vez de 'esperança matemática' ou 'valor esperado', também se diz 'valor médio', mesmo quando se trata de distribuições de probabilidade.

Posto isto, chama-se *esperança matemática dum jogador* à soma $p_1x_1+...+p_nx_n$ dos produtos p_kx_k das quantias x_k que ele pode ganhar num dado jogo, pelas respectivas probabilidades p_k de as ganhar. Um jogo diz-se *equitativo,* quando a entrada de cada jogador (isto é, a quantia com que entra no jogo) é igual à sua esperança matemática.

São habitualmente equitativos os jogos *puramente de sorte* (como, por exemplo, o loto) entre pessoas que se reúnem para jogar a dinheiro. Não é equitativo, em geral, por exemplo, o bridge a dinheiro, precisamente porque não é um jogo de sorte, mas antes de *perícia.*

Mas há, também, jogos de sorte que não podem ser equitativos: por exemplo a roleta, a lotaria, etc. No caso da roleta ou da lotaria, a entrada do jogador tem de ser superior à sua esperança matemática: o excesso destina-se a contribuir para as despesas e receitas da banca ou instituição emissora. *Simplesmente a entrada deve ser proporcional*

à esperança matemática, isto é, deve existir um número $k > 1$, *igual para todos os jogadores (constante de proporcionalidade), tal que, sendo* E' *a entrada de cada jogador e* E *a sua esperança matemática, se tenha sempre*:

$$E' = kE.$$

Podemos exprimir este facto, dizendo que o jogo é *equitativo entre o público,* o que equivale afinal a dizer, no caso da lotaria, que a *probabilidade de saída dos diferentes prémios é a mesma para todos os números da emissão.*

Por exemplo, na Santa Casa da Misericórdia de Lisboa, 60 % dos preços dos bilhetes de lotaria são destinados a prémios e os restantes 40 % a despesas e receitas da Instituição. Tem-se pois, neste caso:

$$0{,}6 \times E' = E \quad \text{ou seja} \quad E' = \frac{5}{3} E$$

Surge agora, naturalmente, a pergunta:

É o totobola um jogo equitativo para o público?

Claro que não.

O totobola não é um jogo puramente de sorte, mas sim um jogo de sorte e de perícia.

Na verdade, o facto de um jogador de totobola estar *bem informado* acerca das equipas que se defrontam aumenta a sua probabilidade de acertar, probabilidade que será muito maior, ainda, se o concorrente juntar a essa condição as seguintes: 1) ter uma apreciável *intuição* para prever os resultados dos desafios, intuição essa baseada na experiência; 2) dispor de *bastante dinheiro,* para poder, com uma aposta múltipla, cobrir uma zona de grande probabilidade (1).

---

(1) Esta última condição *por si só* é demasiado fraca e pode constituir uma tentação perigosa para pessoas ingénuas que desejam, à viva força, ser milionárias (ver pág. 246, ex. 7).

Os exemplos de pessoas que são únicas a acertar nos 13 resultados, com uma aposta dupla *feita ao acaso,* nada provam contra o anterior argumento; não só porque, em estatística, os casos individuais não contam, mas ainda por uma razão, aparentemente paradoxal, semelhante à que já foi indicada a propósito da distribuição binomial (cf. n.º 17):

Como o número dos peritos em totobola é extremamente reduzido em comparação com a massa total dos concorrentes, pode acabar por ser mais provável que acerte um concorrente não perito, principalmente se tivermos em conta a possibilidade de resultados que estejam fora de todas as previsões admissíveis.

Também não se pode inferir daqui que, quando os resultados estão ou parecem estar inteiramente fora das previsões admissíveis, só um *não perito* pode ser totalista. Entre os indivíduos a que podemos chamar 'peritos em totobola', há naturalmente uma grande diversidade de *graus de perícia* e serão, portanto, os *peritos-mores* (chamemos-lhes assim) os concorrentes com mais probabilidade de se *tornarem milionários do totobola.*

Como argumento final decisivo, a experiência parece confirmar as considerações de carácter apriorístico que acabamos de expor.

20. **Aplicação da teoria das probabilidades nos seguros.** Como vimos, foram os jogos de azar que deram origem ao cálculo das probabilidades, mas este acabou por ter numerosas aplicações importantes nos mais diversos domínios. Uma das mais antigas aplicações importantes do cálculo das probabilidades encontra-se na teoria matemática dos seguros. Esta é denominada *'cálculo actuarial'* e os especialistas neste ramo são chamados *'actuários'*.

O sistema dos seguros assemelha-se, em vários aspectos, ao das lotarias. Comecemos por um exemplo simples:

Um chefe de família vai fazer uma viagem de avião e, prevendo

a possibilidade de um acidente fatal, procura proteger a família, fazendo um seguro de 2000 contos. Para 24 horas de viagem esta importa em cerca de 160 escudos *(prémio do seguro)*. É claro que neste caso, o acidente (ou *sinistro*) desempenha o papel da *sorte* na lotaria e que, portanto, o prémio do seguro deve ser superior à respectiva *esperança matemática,* isto é, ao produto do capital segurado pela probabilidade p do referido acidente, a fim de contribuir para as despesas e lucros da companhia seguradora. No exemplo concreto considerado deverá ter-se, pois:

$$p \times 2\,000\,000\$00 < 160\$00$$

Donde:

$$p < \frac{160}{2\,000\,000} = \frac{1}{12\,500}$$

Aliás, a probabilidade p, cujo valor só grosseiramente poderá ser avaliado, deve ser muito inferior a este limite, talvez inferior a 1/100 000, o que deve tranquilizar as pessoas que viajam de avião...

Assim, este ramo de seguros funciona como um *jogo equitativo entre os segurados:* tudo se passa como se, em caso de acidente, *todos* os segurados contribuissem para o pagamento do capital devido à família do sinistrado, sendo essa contribuição *equitativa,* isto é, proporcional à importância que cada segurado estipula para emergência análoga.

Um exemplo semelhante, embora mais complexo, é o dos *seguros de vida.* O cálculo destes seguros é baseado em *tabelas de mortalidade,* construídas por métodos de estatística matemática a partir de dados empíricos respeitantes a populações muito numerosas, distribuídas por vastas regiões e por longos períodos. Essas tabelas fornecem *frequências relativas ajustadas* (isto é, submetidas a certas correcções teóricas), que podem ser assumidas como *probabilidades,*

num futuro não muito distante da época em que foram elaboradas tabelas.

As companhias portuguesas de seguros adoptam ainda, por lei, as tábuas francesas AF (abreviatura de 'assurés français') e RF (abreviatura de 'rentiers français'), que foram elaboradas no século passado.

No fim do volume apresenta-se um extracto da tábua AF. A tábua refere-se à evolução de uma população humana hipotética, que começa com um milhão de indivíduos, sem distinção de sexos. Na primeira coluna, indica-se o *número* x *de anos de idade* e, na segunda coluna, em correspondência por linhas, *o número de vivos com a idade* x, número este que vamos designar por v_x (os actuários usam, neste caso, o símbolo l_x, abreviatura do inglês 'number living at age x'). Por exemplo, consultando a tábua AF para x = 20, x = 50 e x = 102, encontra-se:

$$v_{20} = 824159 \quad , \quad v_{50} = 628727 \quad , \quad v_{102} = 3$$

Quer isto dizer, segundo a referida tábua, que, entre um milhão de indivíduos que nascem, 824159 atingem os 20 anos, 628727 atingem os 50, e só 3 atingem os 102 anos; por outras palavras, as probabilidades de atingir essas idades são, respectivamente:

$$\frac{v_{20}}{v_0} = 0{,}824159, \quad \frac{v_{50}}{v_0} = 0{,}628727, \quad \frac{v_{102}}{v_0} = 0{,}000003$$

A última é, como se vê, extremamente pequena, *em todo o caso superior à probabilidade de acertar nos* 13 *resultados do totobola, com uma aposta dupla puramente casual.*

Segundo a mesma tábua, nenhum dos indivíduos da população inicial de um milhão atinge os 104 anos. Não quer isto dizer que seja *impossível atingir* essa idade ou ainda outras superiores (citam-se casos, naturalmente *raríssimos,* de macróbios com 120 anos e mais).

A única conclusão a tirar daí é esta: *a probabilidade que tem um recém-nascido de ultrapassar os* 103 *anos é inferior a um milionésimo* (segundo a referida tábua).

É fácil reconhecer, agora, o seguinte:

A probabilidade que um indivíduo de idade x *tem de chegar a uma idade* $y \geqslant x$ *é* v_y/v_x.

Por exemplo, a probabilidade que um indivíduo de 20 anos tem de sobreviver até aos 50 (pelo menos) é:

$$\frac{v_{50}}{v_{20}} = \frac{628727}{824159} \approx 0{,}76$$

portanto, superior à probabilidade que tem um recém-nascido de chegar aos 50 ($\approx 0{,}63$).

Como exercício, calcule a probabilidade de que duas pessoas com idades x e x' atinjam ambas as idades y e y' respectivamente (com $y \geqslant x$ e $y' \geqslant x'$).

Um conceito intimamente relacionado com este assunto é o de *vida média* duma pessoa (após uma idade x). A questão pode pôr-se intuitivamente nestes termos:

Calcular o número médio de anos de vida que têm ainda à sua frente as pessoas de idade x.

Para obter este valor médio *em primeira aproximação,* admite-se uma hipótese simplificadora que, evidentemente, não é verificada na prática: *todas as pessoas vivem um número inteiro de anos, falecendo imediatamente após o último aniversário.* Nesta hipótese, o número de pessoas de idade x que sobrevivem só 1 ano é $v_{x+1}-v_{x+2}$; o número de pessoas de idade x que sobrevivem só 2 anos é $v_{x+2}-v_{x+3}$, e assim por diante. Nestas condições, a vida média após a idade x obtém-se dividindo por v_x (número total de indivíduos que atingiram a idade x) a soma dos produtos dos anos de sobrevivência pelos respectivos números de indivíduos. Assim,

se designarmos por ω o número máximo de anos de vida (103 na tabela AF) e por e_x a vida média após a idade x, teremos:

$$(1) \qquad e_x = \frac{(v_{x+1}-v_{x+2})+2(v_{x+2}-v_{x+3})+\ldots+(\omega-x)v_\omega}{v_x}$$

$$= \frac{v_{x+1}+v_{x+2}+\ldots+v_\omega}{v_x} = \frac{1}{v_x} \sum_{n=1}^{\omega-x} v_{x+n}$$

Para obter aproximações cada vez melhores da vida média após a idade x, deveríamos dispor de tábuas de mortalidade sucessivamente mais minuciosas, por exemplo por trimestres, por meses, por semanas, etc., que nos permitissem substituir a hipótese inicial por hipóteses cada vez mais próximas da realidade. Todavia, na prática, tem-se revelado suficiente uma segunda aproximação, que consiste em adicionar meio ano ao valor médio anterior. Esta segunda aproximação costuma ser designada pelo símbolo $\mathring{e}_x$. Tem-se, pois, por definição:

$$\mathring{e}_x = \frac{1}{2} + e_x$$

Em vez de 'vida média após a idade x', também se diz *'esperança de vida na idade* x' (donde a escolha da letra *e* nas anteriores notações). Porém, a primeira expressão é mais de origem *estatística,* referindo-se ao *passado,* e só enquanto se aplica ao futuro pode, com propriedade, ser substituída pela segunda, de carácter *probabilista.* Sob este aspecto, trata-se, na realidade, de uma esperança matemática, como vamos ver, relativamente a e_x.

Com efeito, de (1) resulta imediatamente que

$$e_x = 1 \cdot \frac{v_{x+1}-v_{x+2}}{v_x} + 2 \cdot \frac{v_{x+2}-v_{x+3}}{v_x} + \ldots + (\omega-x)\,\frac{v_\omega}{v_x}$$

Ora $(v_{x+1}-v_{x+2})/v_x$ é a *probabilidade* que tem um indivíduo de idade x de viver só mais 1 *ano,* $(v_{x+2}-v_{x+3})/v_x$ a *probabilidade* que tem um indivíduo de idade x de viver só mais 2 *anos,* e assim sucessivamente. Logo, a expressão anterior dá, efectivamente, segundo a definição do n.º 19, a esperança matemática da variável casual

$$n = \textit{número de anos de vida após a idade } x,$$

adoptando a hipótese simplificadora inicial.

Posto isto, suponhamos que uma pessoa de idade x pretende fazer um seguro de vida na importância de C escudos, que deverá ser entregue à pessoa ou às pessoas designadas pela primeira, após a sua morte. Suponhamos que esta decide pagar para esse fim um prémio anual de *c* escudos, enquanto viva. Se o sistema fosse equitativo e se os prémios não rendessem juro, o produto de *c* pela parte inteira da vida média dessa pessoa após a idade x deveria ser igual a C, isto é:

$$mc = C,$$

sendo *m* a parte inteira (ou característica) de $\mathring{e}_x$.

Mas, já sabemos que o sistema só pode ser equitativo em relação ao público entre si, visto que o prémio deve contribuir não só para a constituição do capital C, mas também para as despesas, riscos e receitas da companhia seguradora.

Por outro lado, os prémios devem ficar a render juros compostos, a favor do segurado, durante a vida deste, com determinada taxa r anual (geralmente 4 %).

Estas e outras circunstâncias vêm complicar o cálculo dos seguros de vida inteira (bem como de outras modalidades afins), com pormenores técnicos que ultrapassam o âmbito desta iniciação elementar.

21. **As variações da probabilidade no cálculo de seguros.** Como vimos nos n.os 11 e 12, a atribuição de uma probabilidade p a um acontecimento α assenta no método de indução e está, portanto, sujeita a todas as limitações próprias deste método, nomeadamente no espaço e no tempo: *não podemos extrapolar os resultados da experiência para além de certos limites.* Isto verifica-se com a própria física e até com a geometria. Por exemplo, o teorema segundo o qual a soma dos ângulos dum triângulo é igual a 180° é válida até às aproximações exigidas na prática, numa região do espaço que não exceda muito as dimensões da Terra; porém, a TEORIA DA RELATIVIDADE veio mostrar que, em domínios astronómicos mais extensos, a soma dos ângulos dum triângulo pode ser sensivelmente superior a 180°(1). Isto revela que os postulados da geometria euclidiana, e em especial o próprio POSTULADO DE EUCLIDES (2), deixam de dar resultados com aproximação razoável em tais domínios.

É, portanto, natural que a probabilidade dum acontecimento (ou melhor, de um tipo de acontecimentos) esteja sujeita a variações mais ou menos imprevisíveis. Por vezes, essas variações são tão rápidas, que nem sequer faz sentido falar de probabilidade, por *ausência de regularidade estatística,* mesmo em zonas ou períodos bastante limitados. Outras vezes as variações de probabilidade são bastante lentas, para que os números atribuídos como probabilidades aos acontecimentos possam ser aceites com relativa confiança; é o que sucede, por exemplo, com as probabilidades indicadas por tábuas de mortalidade não muito antigas, abstraindo, é claro, de períodos excepcionais de guerras, grandes epidemias, etc. e de regiões do Globo a que essas tábuas não se apliquem.

---

(1) Neste caso chamam-se *segmentos de recta* as trajectórias dos fotões no vazio.

(2) 'Dados um ponto e uma recta, existe sempre uma recta e uma só que passa pelo ponto dado e é paralela à recta dada'. Na geometria que melhor se adapta a domínios astronómicos, não existem rectas paralelas.

Já atrás foi mencionado que as companhias portuguesas de seguros ainda usam, por lei, as tábuas francesas AF e RF, elaboradas no século passado. *Essas tábuas fornecem probabilidades diferentes.* Como se explica esta discordância em tábuas do mesmo país e da mesma época? As razões são as seguintes:

A tábua AF ('assurés français') destina-se essencialmente a *seguros de vida* e a tábua RF ('rentiers français') a *rendas vitalícias.* É natural que tenham maior tendência para a segunda modalidade pessoas saudáveis que esperam ter uma longa vida e que se decidem a confiar capitais a companhias de seguros ou ao Estado, a fim de serem convertidos, com os respectivos juros, em *rendas vitalícias,* de carácter periódico (mensais, trimestrais, etc.) conforme o estipulado. Pelo contrário, é natural que tenham maior tendência para seguros de vida pessoas com preocupações de saúde. Ora, as tábuas foram organizadas não só utilizando os resultados de censos populacionais, mas também com base na experiência das próprias companhias *— e essa experiência parece confirmar as previsões anteriores, apesar de as companhias tomarem a precaução de sujeitar a inspecção médica as pessoas que pretendem fazer seguros de vida.* Assim se explica, portanto, que as tábuas RF dêem probabilidades de vida um pouco superiores às correspondentes da tábua AF.

Deve acrescentar-se, no entanto, que estão actualmente em estudo entre nós tábuas de mortalidade recentes, também de origem francesa, uma para cada sexo: tábua PM ('population masculine') e tábua PF ('population féminine'). Verifica-se que as pessoas do sexo feminino têm, para cada idade x, vida média geralmente superior às do sexo masculino para a mesma idade, o que está de acordo com certos factos que chamam a atenção: por exemplo, parece ser mais frequente a viuvez no sexo feminino do que no masculino.

No final do volume é apresentado um extracto da tábua PM. Comparando-a com a tábua AF observa-se um considerável acréscimo das vidas médias (ou esperanças de vida) para cada idade: assim, para a idade 0, a tábua AF dá como vida média 52,0187

anos enquanto a tábua PM dá 66,9551, *cerca de* 15 *anos mais;* para a idade 50, a tábua AF dá como vida média 19,6593 anos, enquanto a tábua PM dá 22,5495, *cerca de* 3 *anos mais,* etc. Estes acréscimos, que podem ser explicados pelos progressos da medicina e pelas condições mais higiénicas da vida moderna, são confirmados, ao que parece, pela própria experiência das companhias que continuam a adoptar as tábuas AF e RF: o ramo dos seguros de vida tem-se tornado mais lucrativo (aumentando a vida média, aumenta o número de prémios pagos pelos segurados na modalidade *vida inteira*); ao passo que as rendas vitalícias se tornam menos vantajosas (vivendo mais tempo, as pessoas recebem maior número de rendas).

Observa-se, no entanto, um facto estranho ao comparar as duas tábuas: no primeiro ano de vida a tábua PM dá um número de mortes (68620) quase duplo do que é dado pela tábua AF (36015). Este facto contradiz a afirmação corrente de que os progressos da medicina e da higiene, associados ao progresso social, têm diminuído enormemente a mortalidade infantil. Deve notar-se, porém, que a tábua AF não merece grande confiança relativamente às primeiras idades, quer pela insuficiência de dados estatísticos, quer pelos métodos de ajustamento utilizados. Convém assinalar entretanto que, logo na idade 1, a tábua PM apresenta um número de mortes (6706), que é cerca de 30 % do valor correspondente dado pela tábua AF e esta forte diminuição da mortalidade mantém-se em todos os anos de infância e da adolescência.

Finalmente deve dizer-se que foi elaborada, há poucos anos, uma tábua de mortalidade portuguesa.

22. **Interpretação estatística duma tábua de contingência. Teste do qui-quadrado com um grau de liberdade.** Imaginemos uma experiência destinada a averiguar da eficácia de um certo tratamento em determinada doença. Suponhamos que o expe-

rimentador dispõe de 300 animais atacados dessa doença e que decide submeter 100 destes ao referido tratamento, reservando os outros 200 para *contrôle* (ou *testemunho*). Suponhamos, além disso, que se obtiveram os resultados indicados na seguinte tabela (1):

TABELA DOS VALORES OBSERVADOS

	Sobreviventes	Mortos	Total
Não tratados	152	48	200
Tratados	88	12	100
TOTAL	240	60	300

Para averiguar *em que medida* estes resultados autorizam a admitir uma real influência do tratamento na doença (no sentido da cura ou no sentido do agravamento), adopta-se uma atitude mental semelhante ao método de demonstração por redução ao absurdo usado em matemática pura. Consiste essa atitude em admitir uma hipótese, chamada *hipótese nula* (ou *hipótese de independência*), que é exactamente a negação daquilo que se pretende estabelecer.

HIPÓTESE NULA. *O tratamento adoptado não influi na mortalidade da doença, nem num sentido nem no outro.*

Admitida esta hipótese, seria de esperar que os resultados obti-

(1) Exemplo dado por FINNEY na sua obra 'An introduction to statistical science on agriculture'.

dos fossem aqueles a que, no n.º 5, chamámos *valores de independência* (ou *valores esperados*) e que são os indicados na seguinte tabela:

TABELA DOS VALORES ESPERADOS (1)

	Sobreviventes	Mortos	Total
Não tratados	160	40	200
Tratados	80	20	100
TOTAL	240	60	300

Estes valores foram obtidos segundo a fórmula definidora de $\Phi^{o}(\alpha\,\beta)$ (ver pág. 210), que se aplica igualmente a $\Phi_{o}(\tilde{\alpha}\,\beta)$, $\Phi_{o}(\tilde{\alpha}\,\tilde{\beta})$, etc. Assim, tem-se:

$$160 = \frac{240 \times 200}{300}, \qquad 80 = \frac{240 \times 100}{300} = 240 - 160,$$

$$40 = \frac{60 \times 200}{300} = 200 - 160, \qquad 20 = \frac{60 \times 100}{300} = 100 - 80.$$

Quer dizer: segundo a hipótese nula, o número de sobreviventes não tratados deveria ser 160, a dos sobreviventes tratados 40, etc. Com efeito, só deste modo a percentagem dos sobreviventes entre os tratados seria igual à dos sobreviventes entre os não tratados, ou seja:

$$\frac{80}{100} = \frac{160}{200} = 80\,\%,$$

(1) Aqui 'valores esperados' é abreviatura de 'valores esperados *na hipótese da independência*'.

e, analogamente, a percentagem dos mortos entre os tratados seria igual à dos mortos entre os não tratados, ou seja:

$$\frac{20}{100} = \frac{40}{200} = 20\,\%$$

Porém, os valores observados não coincidem com os correspondentes valores esperados. As diferenças entre os primeiros e os segundos, chamados *desvios* (ou *discrepâncias*) são indicados na seguinte tabela:

TABELA DOS DESVIOS

	Sobreviventes	Mortos	Total
Não tratados	− 8	8	0
Tratados	8	− 8	0
TOTAL	0	0	0

É claro que, em tabelas de contingência deste tipo, basta conhecer um dos desvios para que os restantes fiquem determinados, uma vez que *as somas dos desvios, tanto por linhas como por colunas,* têm de ser zero. Exprime-se este facto dizendo que as tabelas deste tipo têm *um só grau de liberdade.*

Surge, agora, a pergunta:

Estão estes desvios em contradição com a hipótese nula?

Em rigor, isto é, em matemática pura baseada na lógica bivalente do 'sim ou não', a resposta só pode ser 'sim'. Não esqueçamos, porém, que não se trata agora de proposições matemáticas, mas de *factos empíricos,* necessariamente *contingentes.*

Por outras palavras:

O facto de o tratamento não influir na doença não obriga, de

modo nenhum, a uma rígida confirmação dos valores de independência, pois pode haver desvios não nulos *devidos ao acaso*; só se os desvios excederem, em valor absoluto, um *certo limite* é que haverá razão para *rejeitar a hipótese nula*. Tudo está, portanto, em avaliar aproximadamente esse limite, para além do qual deixará de ser admissível a hipótese nula.

* * *

A situação anterior é análoga à que se levanta a propósito de lançamentos sucessivos duma moeda ao ar. Supondo que a moeda é equilibrada, é de *esperar* que, por exemplo, numa sequência de 100 lançamentos, se apresente *escudo* 50 vezes, isto é, que a frequência relativa deste acontecimento seja 1/2. Mas, é possível (e até, como vimos, *muito mais provável*), que a frequência absoluta desse acontecimento em 100 provas seja diferente de 50; simplesmente, a frequência absoluta será tanto menos provável quanto mais se afastar do *valor esperado* (ou *esperança matemática*), que é, como vimos, 50. Aliás, a distribuição binomial (n.os 17 e 18) habilita-nos a calcular, neste caso, a probabilidade de que o desvio (diferença entre o valor esperado e o valor observado) tenha módulo inferior a um certo limite. Todavia, como vimos, os cálculos exigidos pela distribuição binomial para 100 provas são demasiado laboriosos, o que o obriga a um cálculo aproximado (tanto mais aproximado quanto maior é o número de provas), recorrendo à *distribuição normal,* que ainda não estamos em condições de estudar.

Tornando à experiência do exemplo inicial, podemos imaginar um tipo de provas semelhantes ao que consiste em atirar uma moeda ao ar, para ver em que medida os desvios verificados são atribuíveis unicamente ao acaso.

Tomem-se 300 bocados de cartão, sensivelmente iguais em forma, dimensões e substância, e distingam-se 100 desses cartões com a cor vermelha (representativos dos 100 animais tratados) e os 200 restantes com a cor branca (representativos dos animais não tratados).

Executa-se, depois, um *grande número de vezes seguidas* a prova $\mathcal{P}$ que consiste nas seguintes operações:

1.º *Fechar todos os cartões numa caixa bastante espaçosa.*

2.º *Agitar fortemente a caixa várias vezes.*

3.º *Tirar da caixa, ao acaso,* 60 *cartões (representativos dos animais mortos).*

4.º *Registar o número de cartões vermelhos existentes nessa amostra de* 60 *cartões.*

É claro que a prova $\mathcal{P}$ implica a reposição dos cartões retirados na prova anterior.

O número x de cartões vermelhos em cada amostra indica o *número de animais tratados mortos,* numa experiência hipotética, em que o desvio $x - 20$ entre x e o valor esperado 20 seja atribuível exclusivamente ao acaso (segundo a HIPÓTESE NULA). Uma vez conhecido este desvio, imediatamente se determinam os restantes, visto que as somas por linhas e por colunas são nulas, como vimos.

Ora, no caso em estudo, o módulo dos desvios verificados é 8. Portanto, o que está indicado é *determinar a frequência relativa com que, nas referidas provas casuais, se apresentam desvios cujo módulo é igual ou superior a* 8.

Quem tiver a paciência de efectuar um número muito grande de tais provas (pelo menos 1000) verificará que *só em cerca de* 2 % *das provas se apresentam desvios com módulo igual a* 8. Somos, assim, levados a concluir, por indução, que:

A probabilidade de desvios puramente casuais, com módulo igual ou superior a 8, *é aproximadamente* 2%;

ou ainda, o que é equivalente:

A probabilidade de desvios puramente casuais, com módulo inferior a 8, *é cerca de* 98 %.

Como esta probabilidade é muito próxima de 1, podemos tomar como *quase certo* que os desvios puramente casuais têm módulo inferior a 8. *Mas isto é contrário à hipótese nula.* Somos, portanto,

levados a *rejeitar a hipótese nula,* isto é, a concluir, com uma *boa margem de segurança,* que:

O tratamento influi realmente na evolução da doença, sendo o efeito benéfico, visto ser positivo o desvio correspondente a 'animais tratados sobreviventes'.

* * *

Releia, com muita atenção, todas as considerações anteriores acerca da experiência em estudo. *Analise-as com espírito crítico.* A argumentação usada é de tipo muito diferente do das demonstrações matemáticas, apesar da analogia com as demonstrações por redução ao absurdo. Para quem se habituou ao chamado 'rigor lógico da matemática', deixam uma certa insatisfação no espírito, não é verdade? Mas é tempo de se ir habituando também à ideia de que o rigor matemático se refere a um ideal platónico de perfeição absoluta, que jamais se encontra realizado neste mundo em que vivemos — *muito embora nos seja indispensável para interpretar, com êxito cada vez maior, esta mesma realidade, sempre mutável e imperfeita.* Já vimos que todas as leis experimentais sofrem do mesmo carácter contingente, que resulta do método indutivo. Mas são essas leis que marcam o progresso real do homem no conhecimento do mundo empírico.

Um dos inconvenientes do método anterior é o de obrigar a um enorme número de provas fastidiosas. Todavia esse inconveniente pode ser evitado, recorrendo precisamente ao *método dedutivo da matemática,* segundo os princípios do cálculo das probabilidades. Com efeito, não é difícil reconhecer que a probabilidade de, numa amostra casual de 60 cartões, aparecerem x cartões vermelhos é (1):

$$P(x) = \frac{\binom{100}{x}\binom{200}{60-x}}{\binom{300}{60}} \quad (\textit{distribuição hipergeométrica})$$

(1) A dedução desta fórmula pode ficar como exercício para os alunos mais interessados. É fácil determinar o número de casos possíveis e o número de casos favoráveis.

Esta fórmula permite, pelo menos teoricamente, calcular a probabilidade de um desvio $x-20$ com módulo igual ou superior a 8. Essa probabilidade, até à ordem das centésimas, é precisamente:

$$P(|x-20| \geqslant 8) = 0{,}0210 \approx 2\,\%$$

Simplesmente, tal como no caso da distribuição binomial, os cálculos exigidos pela utilização da fórmula (1) são impraticáveis. Mas, também como no caso da distribuição binomial, podemos rodear a dificuldade recorrendo a um cálculo aproximado que se baseia numa outra distribuição. Com efeito:

A probabilidade de que os *desvios casuais* não excedam, em valor absoluto, um certo limite pode ser calculada aproximadamente, recorrendo a uma lei de probabilidade chamada DISTRIBUIÇÃO DE PEARSON. Embora não estejamos ainda em condições de fazer o estudo teórico desta lei de probabilidade, *podemos, desde já, indicar como pode ser usada na prática, recorrendo a tabelas numéricas dessa distribuição*. Para isso, começa-se por calcular um *índice estatístico* da tabela de contingência, que se designa pelo símbolo χ^2 (lê-se 'qui-quadrado', visto 'χ' ser a letra grega chamada 'qui') e que é assim definida:

O χ^2 duma tabela de contingência é a soma dos números que se obtêm dividindo o quadrado de cada desvio pelo valor esperado correspondente. Assim, no exemplo anterior, o valor de χ^2 é:

$$\chi^2 = \frac{(-8)^2}{160} + \frac{8^2}{80} + \frac{8^2}{40} + \frac{(-8)^2}{20} = 6$$

Ora bem, demonstra-se em Estatística Matemática a seguinte proposição, cujo significado irá sendo compreendido posteriormente com exemplos práticos(1):

---

(1) Como estamos a seguir uma exposição de tipo prático, renunciamos a precisar o sentido exacto desta proposição.

O χ^2 duma tabela de contingência inteiramente casual segue aproximadamente a lei de Pearson, sendo a aproximação tanto maior quanto maior for o máximo valor esperado.

Por este facto, a lei de Pearson também é chamada *'distribuição do qui-quadrado'*. No final do volume encontra-se uma tábua desta distribuição, apresentada do seguinte modo:

A tábua tem duas entradas, uma para o *número de graus de liberdade* (n) *e a outra para a probabilidade* (P). Suponhamos, por exemplo, n = 1 (o caso que nos interessa por agora) e P = 0,02 ou P = 0,01. No cruzamento da linha 1 com as colunas 0,02 e 0,01 encontramos, respectivamente, os valores 5,41 e 6,64 do χ^2. Quer isto dizer o seguinte:

A probabilidade de um χ^2 igual ou superior a 5,41 *é* 0,02; *a probabilidade de um* X^2 *igual ou superior a* 6,64 *é* 0,01 *(supondo que os desvios se devem exclusivamente ao acaso)*. Simbolicamente:

$$P(\chi^2 \geqslant 5{,}41) = 2\,\%, \quad P(\chi^2 \geqslant 6{,}64) = 1\,\%$$

Analogamente se procede em qualquer outro caso. No exemplo anterior, o valor obtido do χ^2 é 6, portanto *compreendido entre* 5,41 e 6,64. Nestas condições, a probabilidade de um χ^2 *igual ou superior a* 6 *estará entre* 1 % *e* 2 %.

Mas é preciso não esquecer que o uso da distribuição de Pearson em casos como este envolve aproximações que só são aceitáveis quando os valores esperados são relativamente grandes. *Uma regra que costuma ser recomendada na prática é a de não utilizar a distribuição de Pearson quando algum dos valores esperados é inferior a* 5. Contudo, a aproximação pode ser melhorada consideravelmente, em qualquer caso, por um simples artifício chamado *'correcção de YATES'*, que consiste em diminuir 0,5 ao módulo de cada desvio. Assim, no caso em estudo, temos o *valor corrigido* (1):

$$\chi^2 = \frac{(-7{,}5)^2}{160} + \frac{7{,}5^2}{40} + \frac{7{,}5^2}{80} + \frac{(-7{,}5)^2}{20} = 5{,}27$$

(1) Por comodidade continuamos a designar por χ^2 o valor corrigido.

Ora, este valor aproxima-se muito mais do valor 5,41 correspondente a P = 0,02, que do valor 3,84 correspondente a P = 0,05. Assim se confirma o que já tinha sido indicado atrás como resultado de métodos muito mais laboriosos:

A probabilidade de, na referida experiência, haver desvios puramente casuais com módulo igual ou superior a 8, *é aproximadamente* 0,02.

* * *

Esta conclusão levou-nos a rejeitar a hipótese nula, mas aí está um outro motivo de insatisfação que nos deixa o método estatístico usado. Nós concluímos que é *quase impossível* haver desvios casuais com módulo igual ou superior a 8 (ou, o que é equivalente, que é *quase certo* os desvios casuais terem módulo inferior a 8). Mas o que se entende por 'quase certo' e por 'quase impossível'? Em matemática pura todo o conceito não primitivo é definido com rigor absoluto e de modo inteiramente *objectivo,* isto é, com um critério independente das pessoas e das circunstâncias. Agora, pelo contrário, é necessário usar critérios subjectivos, que dependem da intuição e do bom senso do experimentador, assim como da natureza da própria experiência e das circunstâncias que a rodeiam.

Em certas investigações biológicas é usual considerar já como *muito pequena* a probabilidade de 1 por 20 (0,05), embora muitas vezes se prefira considerar como *muito pequena* a de 1 por 50 (0,02) ou a de 1 por 100. Cada uma destas probabilidades é chamada *'nível de significância'*, no método estatístico descrito, o qual por sua vez é denominado *'teste de significância do* χ^2,' ou simplesmente *'teste do* χ^2'.

Convenciona-se chamar *'significante'* o nível de 5 % e *'altamente significante'* o nível de 1 %. Mas convém salientar que se trata aqui apenas de convenções cómodas de linguagem, adoptadas por estatísticos e experimentadores.

Aliás, não são estes os únicos níveis de significância adoptados na prática. Casos há em que o nível de 1 por 10 é já considerado como significante (especialmente em investigaçãos médicas em que o tratamento consiste numa ligeira alteração de regime, pouco dispendiosa e sem risco para o doente); e casos há em que, pelo contrário, se requer um nível de 1 por 1000 (quando se trate de alterações profundas ou muito dispendiosas).

Além disso, o teste do χ^2 não é senão um exemplo, entre muitos, dos *testes de significância* oferecidos pela estatística matemática.

Nas suas linhas gerais, um teste de significância compreende os seguintes passos:

1) *Formular a hipótese nula, que nega o facto experimental a estabelecer.*

2) *Escolher o nível de significância que pareça mais adequado à natureza da experiência e ao tipo de decisão a tomar.*

3) *Calcular a probabilidade de que os valores absolutos dos desvios puramente casuais sejam iguais ou superiores àqueles observados.*

4) *Se a probabilidade obtida em* 3) *é inferior ao nível de significância adoptado em* 2), *rejeitar a hipótese nula; caso contrário, deixar a conclusão em suspenso.*

* * *

Note-se que o papel da estatística matemática não se limita, de modo nenhum, à *interpretação de resultados experimentais:* os métodos estatísticos devem ser usados, primeiro que tudo, no *planeamento das experiências.* Não podemos aqui estudar este assunto de alto interesse. Limitar-nos-emos, por isso, a breves indicações sobre a natureza do problema, no caso particular do tratamento hipotético atrás considerado.

É claro que, quanto maior for o número total de casos individuais estudados, melhor informação fornecem os resultados obtidos; mas,

esse número é forçosamente limitado, especialmente por razões de ordem económica, *e, por isso, mais necessário se torna tirar o maior rendimento possível do material de que se dispõe.*

Suponhamos, por exemplo, que se tinham escolhido apenas 2 ou 3 animais para serem tratados entre os 300, reservando os restantes para *contrôle* (ou vice-versa); é manifesto mesmo *a priori* que os resultados não autorizariam um juízo seguro. Deve, portanto, haver uma proporção óptima para revelar a eficácia do tratamento, caso este tenha de facto efeito. Porém, essa proporção não é, como poderia parecer à primeira vista, a de 50 % para os dois grupos. Na tabela seguinte estão indicados os valores do χ^2 para diferentes proporções de animais tratados, entre os 300, na hipótese de a percentagem de mortos entre animais tratados ser a mesma que se observou na experiência imaginada (12 %).

N.º de animais tratados	para 12 % de mortalidade
25	1,2
50	2,8
100	5,3
125	6,1
150	6,5
175	6,6
200	6,3
250	4,0
275	2,0

Vê-se que o máximo valor do χ^2 é atingido na proporção de 175 tratados para 125 não tratados. Deve ser, portanto, essa a proporção ideal para a experiência.

Há, ainda, outros pormenores relativos à realização da experiência que precisam de ser observados, para que o teste de significância não resulte ilusório. É óbvio que, se os animais tratados tiverem uma

proveniência diferente da dos animais não tratados, as diferenças registadas podem não ser devidas ao tratamento nem ao acaso. Para atenuar o mais possível os factores estranhos ao tratamento, o que há a fazer é destacar os 300 animais duma população tão homogénea quanto possível, e entre esses escolher, *completamente ao acaso*, os 100 animais a serem tratados, dando a todos os 300 igual probabilidade de serem escolhidos. Esta operação, chamada *amostragem casual*, tem de ser efectuada por um processo objectivo, em que não intervenha qualquer factor pessoal de escolha. Um tal processo pode consistir no seguinte: *numerar os animais de* 1 *a* 300, *deitar numa caixa* 300 *cartões iguais, numerados de* 1 *a* 300, *e tirar* 100 *à sorte; os números saídos serão os dos animais a tratar.*

Nunca é de mais encarecer a importância da *amostragem casual*, neste e noutros tipos de experiências, como base duma investigação estatística bem orientada. Não podemos, contudo, indicar aqui os pormenores de técnica, a que tem por vezes de obedecer uma tal operação, que é hoje objecto de estudos desenvolvidos em estatística matemática.

NOTA SOBRE A TERMINOLOGIA. Entre as palavras 'teste', 'significância' e 'significante', atrás usadas, as duas primeiras são anglicismos. Por isso, alguns autores portugueses preferem a essas, respectivamente, as palavras 'prova', 'significação' e 'significativo'. A conveniência em adoptar as primeiras está em que, quando se trata de termos técnicos (como é aqui o caso), importa evitar qualquer confusão com acepções da linguagem comum.

23. **Teste do qui-quadrado com mais de um grau de liberdade.** Limitar-nos-emos a um exemplo ([1]). Trata-se de colheitas de cevada em 260 campos, feitas em 1942. No Inverno e na Primavera antecedentes, tinha-se avaliado em cada campo a frequência

---

([1]) Extraído da obra de FINNEY, já citada.

da larva dum coleóptero designado em inglês por 'wireworm' (variedade de insecto chamado em português 'alfinete'). Segundo determinado critério, classificou-se a infestação dos diferentes campos em 'baixa', 'moderada', 'alta', e 'muito alta'. Por sua vez, a qualidade das colheitas foi classificada em 'satisfatória' e 'não satisfatória'. Os resultados são os que constam da seguinte tabela:

Resultados das colheitas	Infestação				Total
	Baixa	Moderada	Alta	Muito alta	
Satisfatórios	94	62	31	15	202
Não satisfatórios	15	15	17	11	58
Total	109	77	48	26	260

Daqui se deduziu uma tabela dos valores esperados e uma outra dos desvios (tabelas que não reproduzimos). O valor do χ^2 será ainda, neste caso, *a soma dos números que se obtêm, dividindo o quadrado de cada desvio, pelo respectivo valor esperado*. Acha-se, então:

$$\chi^2 = \frac{9{,}3^2}{84{,}7} + \frac{2{,}2^2}{59{,}9} + \frac{(-6{,}3)^2}{37{,}3} + \frac{(-5{,}2)^2}{20{,}2} + \frac{(-9{,}3)^2}{24{,}3} + \frac{(-2{,}2)^2}{17{,}2} + \frac{6{,}3^2}{10{,}9} + \frac{5{,}2^2}{5{,}8} = 15{,}7$$

A hipótese nula formula-se, agora, do seguinte modo:

HIPÓTESE NULA. *A infestação não influi em nada na qualidade da colheita.*

Adoptemos o nível 1 % (altamente significante). Para utilizar o teste do χ^2 há que notar, agora, os seguintes factos:

1) A distribuição de Pearson não depende do número de casos

considerados, mas depende do *número de graus de liberdade* da tabela de contingência. Neste caso, trata-se de uma tabela 2 × 4 (isto é, com 2 linhas e 4 colunas). Como, na correspondente tabela de desvios, são nulas as somas dos desvios quer por linhas quer por colunas, é necessário e suficiente conhecer os desvios numa linha e em três colunas (portanto, ao todo, 3), para que os restantes desvios fiquem determinados. Exprime-se este facto dizendo que a tabela tem 3 *graus de liberdade*. Dum modo geral, uma tabela com *m* linhas e *n* colunas tem (m−1) (n−1) graus de liberdade.

2) O teste do χ^2 não deve aplicar-se quando algum dos valores esperados for *demasiado pequeno*.

3) A correcção de Yates é somente aplicável nas tábuas 2 × 2 (com 1 grau de liberdade).

Portanto, como nenhum dos valores esperados é demasiado pequeno e a tabela tem 3 graus de liberdade, podemos utilizar o anterior valor do χ^2 atrás obtido (15,7). Procurando na tábua da distribuição de Pearson o valor do χ^2 correspondente ao nível de probabilidade 0,01 e a 3 graus de liberdade, achamos 11,34. Ora, o χ^2 obtido é muito superior a este e aproxima-se até do que corresponde ao nível 0,001 (que é 16,27).

Podemos, pois, rejeitar a hipótese nula com nível altamente significante.

24. **Conceitos qualitativo e quantitativo de probabilidade.** Consideremos frases tais como:

'É provável que, já antes de Cristóvão Colombo, navegadores portugueses tenham chegado à América'.

'É provável que existam seres vivos em Marte', etc.

O primeiro juízo refere-se ao passado e o segundo ao presente; nenhum deles se baseia em frequências relativas observadas em sequências estatísticas. Trata-se, em ambos os casos, de um *conceito*

qualitativo de probabilidade — muito diverso do conceito quantitativo atrás considerado.

O conceito quantitativo de probabilidade é *objectivo,* isto é, depende só do *objecto* (facto considerado) e não do *sujeito* (pessoa que pensa e emite o juízo), visto que se baseia em dados estatísticos.

Pelo contrário, o conceito qualitativo de probabilidade é *subjectivo,* isto é, depende do sujeito que o aplica: constitui uma *opinião,* que pode variar de pessoa para pessoa e de época para época.

Em vez da expressão 'é provável' também se usam, neste caso, com significado idêntico expressões tais como *'é verosímil', 'é de crer', 'é crível', 'é admissível', 'é natural'* e ainda *'é possível'* (agora com significado diferente do que temos atribuído a esta última palavra).

Por vezes diz-se mesmo, falando na primeira pessoa gramatical: *'não me repugna admitir', 'não excluo a hipótese',* etc., o que põe mais em evidência o carácter subjectivo do conceito em questão.

Podemos chamar *credibilidade* à probabilidade no sentido qualitativo. Embora se trate de um conceito que parece estar fora da alçada da ciência, há cientistas que pensam diversamente. Mas trata-se, ainda aqui, de uma opinião pessoal discutível...

Porém, a delimitação entre os conceitos qualitativo e quantitativo de probabilidade não é tão nítida como possa parecer à primeira vista.

Consideremos a seguinte afirmação:

'Com os progressos da técnica, a probabilidade de acidente numa viagem aérea tem diminuído nos últimos 30 anos, relativamente a percursos iguais. É, portanto, *provável* que essa probabilidade continue a diminuir'.

Neste caso, a palavra 'provável' sublinhada poderia substituir-se por 'admissível'. Refere-se a um conceito de probabilidade situado entre o qualitativo e o quantitativo, porém mais próximo do segundo, visto que a conclusão se baseia em dados estatísticos *objectivos,* de acordo com o *método de indução.* Mediante uma análise estatística aprofundada, essa probabilidade talvez pudesse mesmo vir a ser definida quantitativamente.

Muitas vezes, a avaliação de uma probabilidade começa por uma *suspeita* ou *intuição*, de carácter mais ou menos subjectivo. Por exemplo, alguns cientistas começaram a ter a suspeita de que o fumar contribui para se ter cancro nos pulmões. Depois disso, numerosas investigações têm sido efectuadas sobre o assunto, com a aplicação de testes tais como o do χ^2 (que implicam já, eles próprios, o conceito de probabilidade). Há pouco tempo, uma revista americana de divulgação indicava o seguinte resultado:

'A probabilidade que tem um grande fumador de contrair cancro nas vias respiratórias é cerca de 1/8'.

Considera-se aqui como 'grande fumador', ao que parece, um indivíduo que fume pelo menos 40 cigarros por dia. Estas investigações têm sido fortemente dificultadas pelo facto de haver enormes interesses económicos em causa. No entanto, a ser válida a conclusão anterior, o comércio de tabacos deveria ser equiparado ao negócio de estupefacientes, para efeitos legais...

Atitude análoga se deveria, aliás, adoptar em relação a muitas das *drogas* que inundam os mercados e que só têm servido para fazer grandes fortunas à custa da bolsa e da saúde, física ou mental, das pessoas incautas. A propaganda comercial não conhece limites morais para fazer vingar os seus fins e, assim, todos os sofismas lhe podem servir.

Sabe-se, por exemplo, que Puccini, fumador excessivo, morreu com um cancro na garganta. Pois não faltará quem justifique este caso, alegando que, se Puccini não tivesse fumado tanto, talvez não tivesse produzido a *Bohème,* a *Madame Butterfly,* etc. — além de que já tinha 66 anos quando faleceu...

Quanto àqueles que argumentam com o facto de haver muitos casos de não fumadores que contraem o cancro, esses apenas revelam ausência de espírito científico, semelhante ao das pessoas ingénuas que concluem, a partir de exemplos, que tem maior probabilidade de ganhar no totobola quem não conhecer nada de futebol.

Um facto é certo: os métodos estatísticos têm sido uma arma poderosa na luta contra o cancro e outras doenças que afligem a humanidade, assim como no combate à superstição e ao charlatanismo.

Estes e outros exemplos não vêm senão confirmar um princípio que deve estar presente no espírito de todo o cientista:

Embora partindo de intuições de carácter mais ou menos subjectivo, a investigação científica, para conduzir a resultados seguros, tem de ser sempre submetida a critérios de lógica dedutiva ou indutiva, tanto quanto possível objectivos, desinteressados, alheios a toda a paixão humana.

FIM DO 1.º VOLUME

TÁBUAS DE MORTALIDADE

TÁBUA AF

Idade x	N.º de vivos v_x	Esperança de vida: $\mathring{e}_x$	Idade x	N.º de vivos v_x	Esperança de vida: $\mathring{e}_x$
0	1 000 000	52,0187	26	791 780	37,4315
1	963 985	52,9434	27	786 713	36,6693
2	937 488	53,4257	28	781 578	35,9070
3	917 939	53,5528	29	776 368	35,1446
4	903 486	53,4015	30	771 075	34,3824
5	892 765	53,0368	31	765 690	33,6207
6	884 754	52,5125	32	760 203	32,8597
7	878 676	51,8723	33	754 606	32,0997
8	873 932	51,1511	34	748 887	31,3411
9	870 056	50,3768	35	746 036	30,5839
10	866 684	49,8708	36	737 038	29,8287
11	863 529	48,7501	37	730 884	29,0757
12	860 371	47,9272	38	724 556	28,3253
13	857 043	47,1114	39	718 042	26,5777
14	853 426	46,3090	40	711 324	26,8334
15	849 446	45,5236	41	704 386	26,0928
16	845 069	44,7568	42	697 210	25,3562
17	840 298	44,0081	43	689 777	24,6241
18	835 173	43,2750	44	682 067	23,8967
19	829 762	42,5540	45	674 058	23,1748
20	824 159	41,8399	46	665 729	22,4584
21	818 171	41,1272	47	657 056	21,7483
22	812 809	40,4102	48	648 015	21,0477
23	807 271	39,6840	49	638 581	20,3483
24	801 926	38,9451	50	628 727	19,6593
25	796 786	38,1932	51	618 429	18,9784

TÁBUAS DE MORTALIDADE

TÁBUA AF

(Continuação)

Idade x	N.º de vivos v_x	Esperança de vida: $\mathring{e}_x$	Idade x	N.º de vivos v_x	Esperança de vida: $\mathring{e}_x$
52	607 659	18,3059	78	143 530	5,1134
53	596 389	17,6424	79	124 896	4,8016
54	584 594	16,9882	80	107 354	4,5046
55	572 246	16,3440	81	91 047	4,2218
56	559 322	15,7101	82	76 094	3,9531
57	545 797	15,0870	83	62 588	3 6983
58	531 649	14,4752	84	50 588	3,4570
59	516 861	13,8751	85	40 118	3,2287
60	501 417	13,2870	86	31 159	3,0132
61	485 307	12,7115	87	23 658	2,81012
62	468 525	12,1489	88	17 523	2,61893
63	451 075	11,5995	89	12 632	2,43936
64	432 964	11,0638	90	8 841	2,27095
65	414 214	10,5420	91	5 992	2,11316
66	394 851	10,0345	92	3 920	1,96566
67	374 918	9,5414	93	2 468	1,82804
68	354 468	9,0630	94	1 490	1,69984
69	333 567	8,5995	95	859	1,58062
70	312 299	8,1511	96	471	1,47000
71	290 735	7,7179	97	245	1,36754
72	269 062	7,3000	98	120	1,27286
73	247 333	6,8974	99	55	1,18555
74	225 714	6,5101	100	23	1,10410
75	204 359	6,1382	101	9	1,03130
76	183 430	5,7815	102	3	0,96307
77	163 096	5,4399	103	1	0,89864

TÁBUAS DE MORTALIDADE

TÁBUA PM

Idade x	N.º de vivos v_x	Esperança de vida: $\mathring{e}_x$	Idade x	N.º de vivos v_x	Esperança de vida: $\mathring{e}_x$
0	1 000 000	66,9551	30	879 672	39,4565
1	931 380	65,4829	31	877 007	38,5748
2	924 674	64,9541	32	874 244	37,6952
3	922 002	64,1409	33	871 377	36,8176
4	920 268	63,2608	34	868 388	35,9426
5	918 851	62,3576	35	865 262	35,0706
6	917 638	61,4394	36	862 000	34,2014
7	916 574	60,5101	37	858 578	33,3357
8	915 630	59,5720	38	854 980	32,4739
9	914 787	58,6264	39	851 201	31,6159
10	914 010	57,6758	40	847 218	30,7622
11	913 260	56,7228	41	843 007	29,9133
12	912 502	55,7695	42	838 556	29,0695
13	911 699	54,8182	43	833 843	28,2309
14	910 815	53,8709	44	828 840	27,3983
15	909 813	52,9297	45	823 527	26,5719
16	908 667	51,9958	46	817 870	25,7522
17	907 349	51,0706	47	811 842	24,9397
18	905 861	50,1537	48	805 412	24,1348
19	904 194	49,2452	49	798 550	23,3379
20	902 359	48,3443	50	791 219	22,5495
21	900 383	47,4493	51	783 386	21,7700
22	898 294	46,5585	52	775 012	20,9998
23	896 165	45,6680	53	766 053	20,2395
24	893 996	44,7775	54	756 462	19,4898
25	891 770	43,8881	55	746 197	18,7510
26	889 487	42,9994	56	735 213	18,0237
27	887 139	42,1119	57	723 464	17,3083
28	884 726	41,2254	58	710 905	16,6052
29	882 240	40,3402	59	697 483	15,8152

TÁBUAS DE MORTALIDADE

TÁBUA PM

(Continuação)

Idade x	N.º de vivos v_x	Esperança de vida: $\mathring{e}_x$	Idade x	N.º de vivos v_x	Esperança de vida: $\mathring{e}_x$
60	683 156	15,2384	85	89 057	3,5776
61	667 881	14,5755	86	71 598	3,3280
62	651 611	13,9270	87	56 353	3,0931
63	634 311	13,2932	88	43 331	2,8723
64	615 948	12,6746	89	32 476	2,6653
65	596 502	12,0715	90	23 665	2,4715
66	575 953	11,4843	91	16 720	2,2904
67	554 297	10,9135	92	11 420	2,1213
68	531 549	10,3591	93	7 514	1,9641
69	507 730	9,8216	94	4 746	1,8180
70	482 882	9,3013	95	2 866	1,6825
71	457 076	8,7982	96	1 648	1,5564
72	430 397	8,3126	97	897	1,4409
73	402 963	7,8445	98	460	1,3348
74	374 909	7,3941	99	221	1,2376
75	346 409	6,9613	100	99	1,1465
76	317 657	6,5461	101	41	1,0610
77	288 874	6,1485	102	16	0,9375
78	260 310	5,7683	103	5	0,9000
79	232 225	5,4055	104	2	0,5000
80	204 897	5,0597	105	0	
81	178 609	4,7308			
82	153 637	4,4185			
83	130 241	4,1224			
84	108 651	3,8422			

TÁBUA DE DISTRIBUIÇÃO DO χ^2 DE PEARSON

	PROBABILIDADE (P)										
n	0,90	0,80	0,70	0,50	0,30	0,20	0,10	0,05	0,02	0,01	0,001
1	0,016	0,064	0,15	0,46	1,07	1,64	2,71	3,84	5,41	6,64	10,83
2	0,21	0,45	0,71	1,39	2,41	3,22	4,61	5,99	7,82	9,21	13,82
3	0,58	1,01	1,42	2,37	3,67	4,64	6,25	7,82	9,84	11,34	16,27
4	1,06	1,65	2,20	3,36	4,88	5,99	7,78	9,49	11,77	13,28	18,47
5	1,61	2,34	3,00	4,35	6,06	7,29	9,24	11,07	13,39	15,09	20,52
6	2,20	3,07	3,83	5,35	7,23	8,56	10,65	12,59	15,03	16,81	22,46
7	2,83	3,82	4,67	6,35	8,38	9,80	12,02	14,07	16,62	18,48	24,32
8	3,49	4,59	5.53	7,34	9,52	11,03	13,36	15,51	18,17	20,09	26,13
9	4,17	5,38	6,39	8,34	10,66	12,24	14,68	16,92	19,68	21,67	27,88
10	4,87	6,18	7,27	9,34	11,78	13,44	15,99	18,31	21,16	23,21	29,59
12	6,30	7,81	9,03	11,34	14,01	15,81	18,55	21,03	24,05	26,22	32,91
14	7,79	9,47	10,82	13,34	16,22	18,15	21,06	23,69	26,87	29,14	36,12
16	9,31	11,15	12,62	15,34	18,42	20,47	23,54	26,30	29,63	32,00	39,25
18	10,87	12,86	14,44	17,34	20,60	22,76	25,99	28,87	32,35	34,81	42,31
20	12,44	14,58	16,27	19,34	22,78	25,04	28,41	31,41	35,02	37,57	45,32
22	14,04	16,31	18,10	21,34	24,94	27,30	30,81	33,92	37,66	40,29	48,27
24	15,66	18,06	19,94	23,34	27,10	29,55	33,20	36,42	40,27	42,98	51,18
26	17,29	19,82	21,79	25,34	29,25	31,80	35,56	38,89	42,86	45,64	54,05
28	18,94	21,59	23,65	27,34	31,39	34,03	37,92	41,34	45,42	48,28	56,89
30	20,60	23,36	25,51	29,34	33,53	36,25	40,26	43,77	47,96	50,89	59,70

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