J. SEBASTIÃO E SILVA

COMPÊNDIO DE MATEMÁTICA

1.º volume

2.º tomo

Curso Complementar
do Ensino Secundário

Edição GEP

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 $\mathbb{R}$, 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

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

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:

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

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

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 $x \curvearrowright a^x$ (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 (IN, +).

(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, ...), 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 $x \curvearrowright x^3$, $x \curvearrowright x^{-1}$ e $x \curvearrowright \sqrt{x}$ 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 $\mathscr{L}$ o conjunto $\{V, F\}$ dos valores lógicos. Prove que o operador $\sim$ (negação) é um isomorfismo de $(\mathscr{L}, \wedge)$ sobre $(\mathscr{L}, \vee)$ e de $(\mathscr{L}, \dot{\vee})$ sobre $(\mathscr{L}, \Leftrightarrow)$ (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 $(B, \cdot)$, 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:

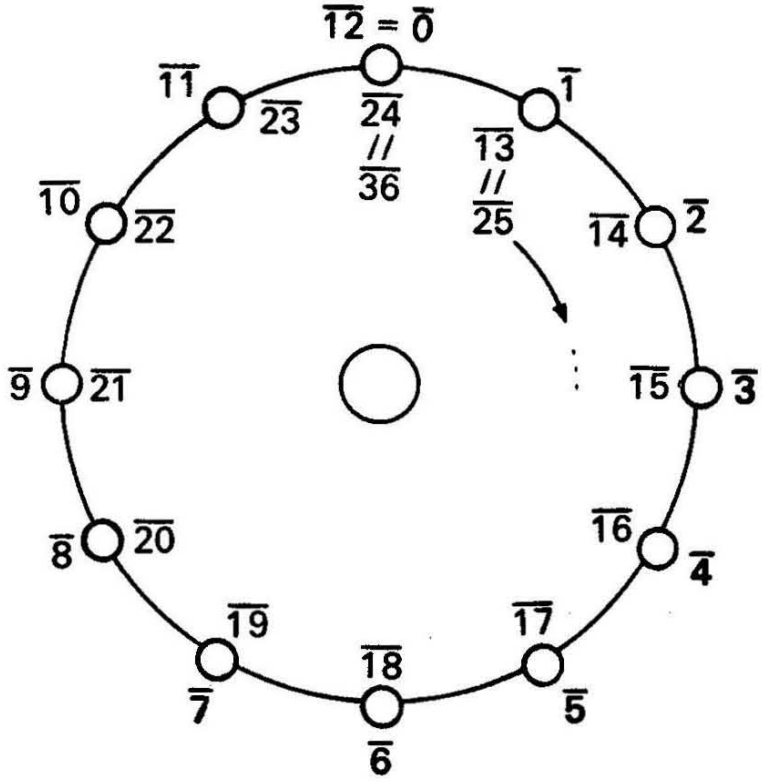
Verifique se existe algum outro isomorfismo de $(A, +)$ *sobre* $(B, \cdot)$ *e se existe algum automorfismo de* $(A, +)$ *diferente da identidade* (as duas questões estão interligadas).

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 $S, S^2, S^3, \ldots$ 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, ..., f^n,... 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

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

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:

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

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

Logo, ab é regular e tem-se:

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

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:

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

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.

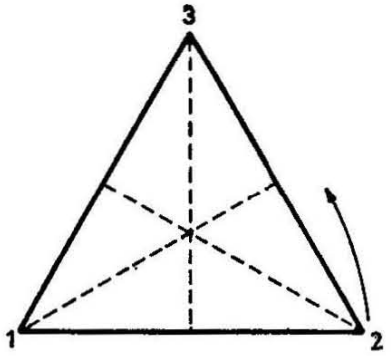
Em particular, será um grupo o conjunto de *todas* as aplicações biunívocas de U sobre si mesmo (*grupo simétrico* ou *grupo total* sobre U).

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.



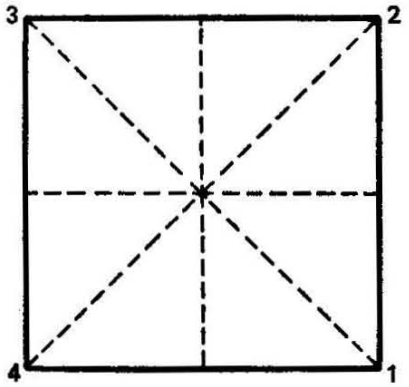
II. Consideremos um triângulo equilátero de vértices 1, 2, 3. Os deslocamentos do plano (1) que aplicam este triângulo sobre si mesmo são, como é fácil ver, as simetrias em relação às medianas do triângulo e as rotações de 120°, 240° e 360° em torno do centro. Estes deslocamentos são definidos pelas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



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

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

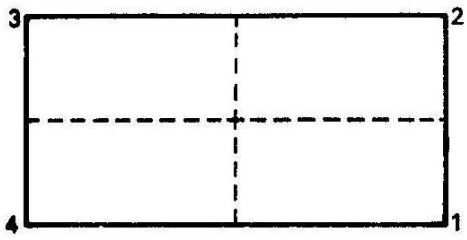
$$\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}\quad \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}\quad \begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}\quad \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}$$

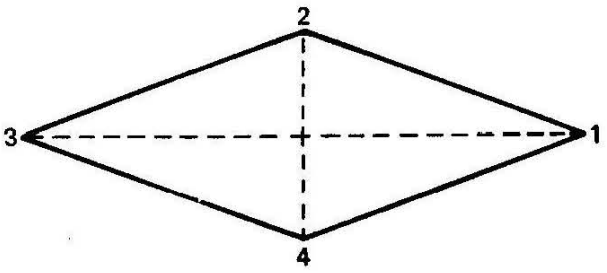
que formam um subgrupo do grupo simétrico sobre $\{1, 2, 3, 4\}$ (*grupo do quadrado*).

---

(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).

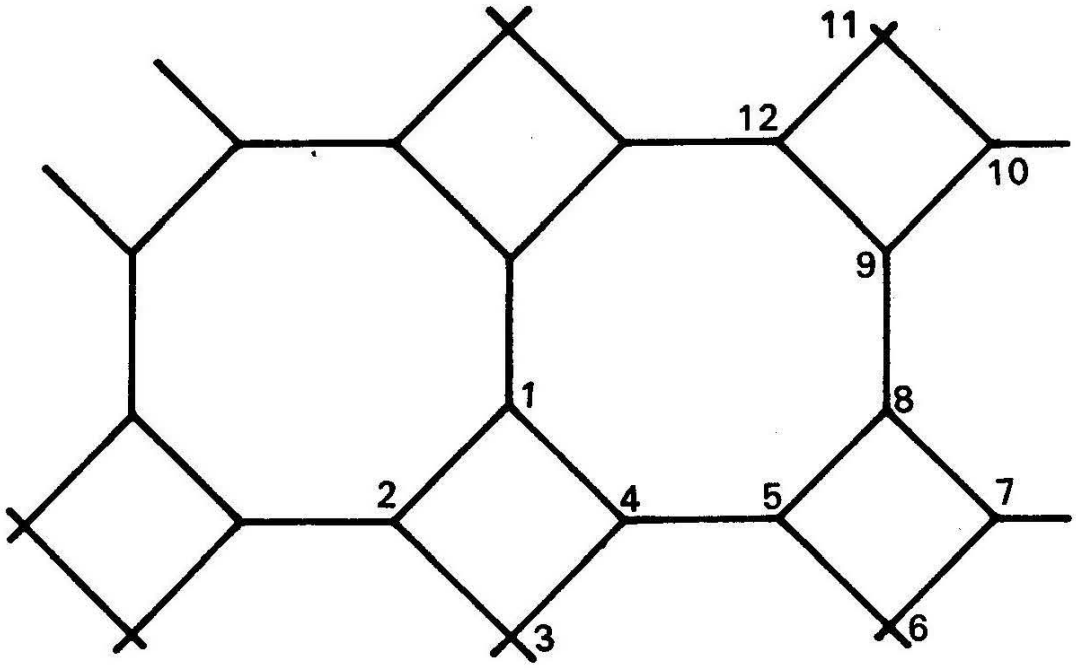




Mostre que estes dois grupos são isomorfos.

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.*

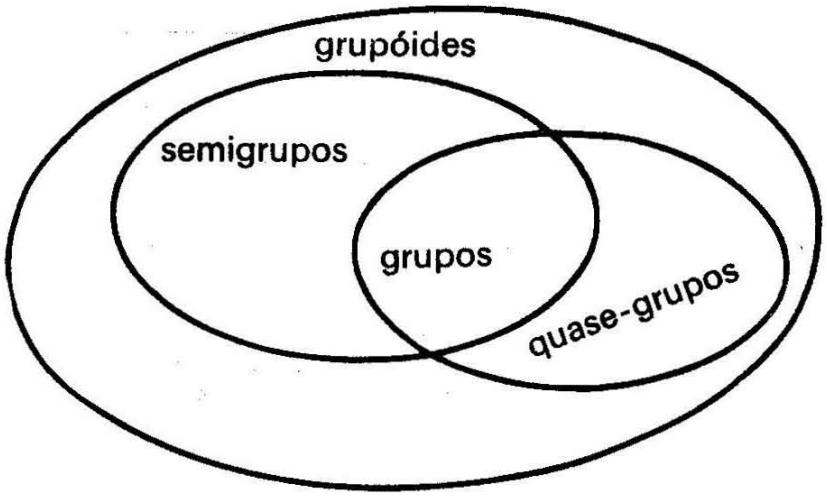
Demonstração:

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 $y \mapsto x_0 \Theta y$ é uma aplicação biunívoca de A sobre A; 2) para todo o $y_0 \in A$, a correspondência $x \mapsto x \Theta y$ 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, $\mathbb{Q}$ e $\mathbb{R}$ (relativamente à adição usual), mas não os conjuntos $\mathbb{N}$, $\mathbb{Q}^+$ e $\mathbb{R}^+$ (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 $(b,a) \mapsto b-a$ 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:

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

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 *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]:

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

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.

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