Elementos de

ANÁLISE MATEMÁTICA

por

A. Almeida Costa

&

A. J. Antunes Monteiro

Volume I

Capítulo I

Conjuntos. Números naturais

§ 1 – Generalidades de Teoria dos Conjuntos

***

1. Notações, definições e primeiras propriedades – Um conjunto $\mathcal{L}$, ou colecção de certos elementos $a, b, c, \ldots, x, y, \ldots$, será representado por um símbolo que põe em evidência todos êstes elementos: $\mathcal{L} = \{a, b, c, \ldots, x, y, \ldots\}$. Diz-se, então, que o elemento x, por exemplo, pertence a $\mathcal{L}$ e representa-se êste facto escrevendo $x \in \mathcal{L}$. Muitas vezes caracterizam-se os elementos de $\mathcal{L}$ por uma propriedade comum Π, caso em que se utiliza a representação $\mathcal{L} = \{x \mid \Pi\}$ para o conjunto. O símbolo Π figura aqui como abreviatura de propriedade, que deve ser claramente indicada.

Para mostrar que A é uma parte de $\mathcal{L}$, emprega-se a notação $A \subseteq \mathcal{L}$. Mesmo que A seja uma parte de uma parte B, de $\mathcal{L}$, escreve-se ainda $A \subseteq B$. Pode acontecer, de resto, que A seja uma parte imprópria de B, isto é que se tenha $A = B$. Quando se põe $A \subseteq B$ não se exclui o caso $A = B$; mas, se isto não acontece, pode escrever-se simplesmente $A \subset B$, dizendo-se que A é uma parte própria de B. Uma parte de $\mathcal{L}$ diz-se um subconjunto de $\mathcal{L}$. Considera-se também o conjunto vazio, repre-

tendo por ϕ, como uma parte de qualquer conjunto. ϕ não contém nenhum elemento.

Com $B \supseteq A$, significa-se o mesmo que $A \subseteq B$. Diz-se, então, que B contém A ou que A está contido em B. Analogamente, $B \supset A$ significa $A \subset B$.

A intersecção D de duas partes A e B, de $\mathcal{L}$, é o subconjunto composto dos elementos de $\mathcal{L}$ que pertencem a A e a B. Escreve-se

$$D = A \cap B = \{ x \in \mathcal{L} \mid x \in A, x \in B \}.$$

A reunião U de duas partes A e B, de $\mathcal{L}$, é o subconjunto formado pelos elementos de $\mathcal{L}$ pertencentes pelo menos a uma das partes. Escreve-se

$$U = A \cup B = \{ x \in \mathcal{L} \mid x \in A \text{ ou } x \in B \}.$$

A e B dizem-se subconjuntos disjuntos, se a sua intersecção é o conjunto vazio. Não há, então, elementos comuns a A e a B.

A e B dizem-se complementares em $\mathcal{L}$, se B contém exactamente os elementos de $\mathcal{L}$ que não pertencem a A. A diferença $A - B$ é o subconjunto composto pelos elementos de A que não estão em B. Quando A e B são complementares em $\mathcal{L}$, tem-se $B = \mathcal{L} - A$.

Tendo em conta as definições acabadas de dar, estabelecem-se de modo simples as igualdades e inclusões seguintes:

I) $A \subseteq A$ (reflexividade de $\subseteq$);

II) se $A \subseteq B$ e $B \subseteq A$, então $A = B$ (anti-simetria de $\subseteq$);

III) se $A \subseteq B$ e $B \subseteq C$, então $A \subseteq C$ (transitividade de $\subseteq$);

IV) se $A \subseteq B$, tem-se $A \cap B = A$, $A \cup B = B$, qualquer destas igualdades equivalendo à inclusão;

V) em particular, de $A \subseteq A$, tira-se $A \cap A = A$, $A \cup A = A$ (idempotência de $\cap$ e de $\cup$);

VI) é sempre $A \cap (\mathcal{L} - A) = \phi$ e $A \cup (\mathcal{L} - A) = \mathcal{L}$;

VII) supondo $A \cap B = \phi$, conclui-se $B \subseteq \mathcal{L} - A$ e reciprocamente;

VIII) supondo $A \cup B = \mathcal{L}$, conclui-se $B \supseteq \mathcal{L} - A$ e reciprocamente;

IX) $A \cap B = B \cap A$, $A \cup B = B \cup A$ (comutatividade de $\cap$ e de $\cup$);

X) $(A \cup B) \cup C = A \cup (B \cup C)$ e $(A \cap B) \cap C = A \cap (B \cap C)$ (associatividade de $\cup$ e de $\cap$);

XI) $\mathcal{L} - (A \cup B) = (\mathcal{L} - A) \cap (\mathcal{L} - B)$;

XII) $\mathcal{L} - (A \cap B) = (\mathcal{L} - A) \cup (\mathcal{L} - B)$;

XIII) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (distributividade de $\cap$);

XIV) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (distributividade de $\cup$);

As demonstrações reduzem-se a um processo comum; se se trata de uma igualdade, mostra-se que um elemento do 1º membro pertence

ao segundo e reciprocamente; tratando-se de uma inclusão, [illegible] só tem de verificar-se que um elemento do 1º membro pertence ao segundo.

*

Observação:- Faremos as convenções seguintes: um sinal cortado por um traço oblíquo significa a "negação" do que afirma o sinal (∉ significa "não pertencente a"; ⊄ significa "não contido em", etc.); o sinal ∀, designado por quantificador universal, significará "qualquer que seja" ou "para todo"; e o sinal ∃, designado por quantificador existencial, significará "existe pelo menos um".

*

A título de exemplo, justifiquemos XI), designada por primeira lei de De Morgan. Tomemos $a \in \mathcal{L} - (A \cup B)$, portanto $a \in \mathcal{L}$, $a \notin A \cup B$. Terá $a \notin A$, $a \notin B$, e, assim $a \in \mathcal{L} - A$, $a \in \mathcal{L} - B$, donde se conclui $a \in (\mathcal{L} - A) \cap (\mathcal{L} - B)$. Reciprocamente, se $a \in (\mathcal{L} - A) \cap (\mathcal{L} - B)$, ter-se-á $a \in \mathcal{L} - A$, $a \in \mathcal{L} - B$, portanto $a \notin A$, $a \notin B$, $a \notin A \cup B$, ou seja $a \in \mathcal{L} - (A \cup B)$.

*

Exercícios:- I') Mostrar que se tem $\mathcal{L} - (\mathcal{L} - A) = A$ [propriedade de involução da "operação $\mathcal{L} - $"] e que valem as leis de absorção $A \cap (A \cup B) = A$, $A \cup (A \cap B) = A$.

II') Verificar que $B \subseteq C$ e $B \cap C = \phi$ implicam $B = \phi$; e que $A \cap (\mathcal{L} - T) = A - T$.

III') Demonstrar XII), XIII) e XIV). [A relação XII) é chamada a segunda lei de De Morgan].

IV') Verificar a igualdade $E \cup F = [E - (E \cap F)] \cup [F - (E \cap F)] \cup (E \cap F)$.

***

2. Dualidade - As igualdades e as inclusões que se podem estabelecer entre partes dum conjunto satisfazem a uma regra de dualidade, que pode ser enunciada do modo seguinte: Se se dá a uma parte A dum conjunto $\mathcal{L}$ uma expressão onde figuram outras partes $X, Y, Z, \ldots$ do mesmo conjunto, sujeitas, além das "operações binárias" $\cap$ e $\cup$ e à "operação unária" $\mathcal{L} - $, que consiste em pôr a ser de X a $\mathcal{L} - X$, obtem-se $\mathcal{L} - A$ substituindo na expressão de A as partes $X, Y, Z, \ldots$ pelas partes complementares e trocando entre si os sinais $\cap$ e $\cup$; mas se se trata duma inclusão $A \supseteq B$, onde B está expresso em $X, Y, Z, \ldots$, então o processo indicado leva a $\mathcal{L} - A \subseteq B'$, onde B' é o transformado de B pelo processo indicado (portanto, $B' = \mathcal{L} - B$).

O emprêgo da regra da dualidade nos dois membros de uma igualdade $A = B$, ou de uma inclusão $A \supseteq B$, supondo, é claro, que os dois membros se encontram expressos em $X, Y, Z, \ldots$, leva a uma igualdade ou a uma inclusão dual da precedente (o sentido da inclusão fica invertido), quando

por fim se substituem de novo $X, Y, Z, \ldots$ pelos seus complementares. Os subconjuntos $X, Y, Z, \ldots$ são suportos arbitrários.

*

Exemplos: I) Quaisquer que sejam X e Y, tem-se $X \supseteq X \cap Y$. A regra de dualidade aplicada aos dois membros leva a $\mathcal{L}-X \subseteq (\mathcal{L}-X) \cup (\mathcal{L}-Y)$, e a inclusão daquela de que se partiu é $X \subseteq X \cup Y$.

II) Tome-se a igualdade XIII) do número anterior. A aplicação da regra da dualidade a ambos os membros leva a $(\mathcal{L}-A) \cap [(\mathcal{L}-B) \cup (\mathcal{L}-C)] = [(\mathcal{L}-A) \cap (\mathcal{L}-B)] \cup [(\mathcal{L}-A) \cap (\mathcal{L}-C)]$. A substituição de A, B, C pelos seus complementares dá $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, de forte que XIII) e XIV) são duais.

*

Suponhamos agora que $X, Y, Z, \ldots$ não são arbitrários, mas que as igualdades ou inclusões que eles verificam se realizam mediante condições impostas a $X, Y, Z, \ldots$. Então, a regra de dualidade enuncia-se assim: se se contiverem partes $X', Y', Z', \ldots$, de $\mathcal{L}$, verificando condições duais daquelas que são verificadas por $X, Y, Z, \ldots$, as igualdades ou inclusões que $X, Y, Z, \ldots$ verificam transformam-se em igualdades ou inclusões verificadas por $X', Y', Z', \ldots$, mediante a substituição de X por X', de Y por Y', etc. e de $\cap$ e $\cup$.

*

Observação: - Pode verificar-se que $X', Y', Z', \ldots$ são necessàriamente os complementares de $X, Y, Z, \ldots$

*

Exemplos: - I') A igualdade $X \cap Y = X$ é válida, se fôr $Y \supseteq X$. Então, a igualdade $(\mathcal{L}-X) \cup (\mathcal{L}-Y) = \mathcal{L}-X$ é válida, se fôr $\mathcal{L}-Y \in \mathcal{L}-X$.

II') Supondo $X \cup Y = \mathcal{L}$, tem-se, qualquer que seja Z, $Z \cap (X \cup Y) = Z$. Então, supondo $(\mathcal{L}-X) \cap (\mathcal{L}-Y) = \phi$, tem-se, qualquer que seja Z, $(\mathcal{L}-Z) \cup [(\mathcal{L}-X) \cap (\mathcal{L}-Y)] = \mathcal{L}-Z$.

***

3. Correspondências. Relações. Aplicações - Tomados dois conjuntos $\mathcal{O}_1$ e $\mathcal{L}_2$, diz-se produto cartesiano dêsses conjuntos e representa-se por $\mathcal{O}_1 \times \mathcal{L}_2$ o conjunto

$$\mathcal{O}_1 \times \mathcal{L}_2 = \{(x, y) \mid x \in \mathcal{O}_1, y \in \mathcal{L}_2\}.$$

Uma correspondência φ, de $\mathcal{O}_1$ para $\mathcal{L}_2$, é um subconjunto de $\mathcal{O}_1 \times \mathcal{L}_2$. Representa-se por φ^{-1} e diz-se correspondência inversa de φ a correspondência de $\mathcal{L}_2$ para $\mathcal{O}_1$ assim definida:

$$\varphi^{-1} = \{(y, x) \mid (x, y) \in \varphi\}.$$

Se ψ fôr uma correspondência de $\mathcal{L}$ para $\mathcal{D}$, define-se um produto $\varphi \circ \psi$, escrevendo

$$\varphi \circ \psi = \{(x, z) \mid \exists y,\ (x, y) \in \varphi;\ (y, z) \in \psi\}. \qquad (1)$$

O produto será vazio, se não existir y, como acontece se fôr $\mathcal{L}_2 \cap \mathcal{L}_1 = \phi$.

* Exercício:- Demonstrar as igualdades seguintes:

i) $\varphi \circ (\psi \circ \theta) = (\varphi \circ \psi) \circ \theta$; ii) $(\varphi \circ \psi)^{-1} = \psi^{-1} \circ \varphi^{-1}$; iii) $(\varphi^{-1})^{-1} = \varphi$.

*

Uma correspondência de $\mathcal{U}$ para $\mathcal{U}$ diz-se uma relação sobre $\mathcal{U}$.

Seja α uma relação sobre $\mathcal{U}$. Em vez de se escrever $(x,y) \in \alpha$, é também usual escrever $x \alpha y$ com o mesmo significado. α diz-se reflexiva, se for $x \alpha x$, $\forall x \in \mathcal{U}$; diz-se simétrica, se se tiver $y \alpha x$, sempre que se tenha $x \alpha y$; e diz-se transitiva, se as hipóteses $x \alpha y$, $y \alpha z$ arrastarem $x \alpha z$. Dá-se o nome de relação diagonal sobre $\mathcal{U}$ à relação

$$\Delta_{\mathcal{U}} = \{(x,x) \mid x \in \mathcal{U}\}.$$

Tomados dois conjuntos $\mathcal{L} = \{a, b, c, \dots\}$ e $\mathcal{D} = \{a', b', c', \dots\}$, suponhamos que, por um certo processo, se faz corresponder a cada elemento $a \in \mathcal{L}$, duma maneira unívoca, um elemento $a' \in \mathcal{D}$. Diz-se, então, que, pelo referido processo, se define uma aplicação (ou função) f, de $\mathcal{L}$ em $\mathcal{D}$. O elemento a' diz-se imagem de a, sendo habitual escrever $a' = f(a)$, ou também $a' = af$. Pode haver elementos de $\mathcal{D}$ que não sejam obtidos como imagens de elementos de $\mathcal{L}$. Quando todos os elementos de $\mathcal{D}$ forem imagens, diz-se que f é uma aplicação sobrejectiva (ou uma sobrejecção) de $\mathcal{L}$ sobre $\mathcal{D}$. $\mathcal{L}$ toma o nome de domínio de f e $\mathcal{D}$ diz-se contradomínio de f.

Se tomarmos $A \subseteq \mathcal{L}$, escreve-se $A' = f(A) \subseteq \mathcal{D}$, para significar o subconjunto de $\mathcal{D}$ constituído por todas as imagens dos elementos de A.

Em particular, a imagem do subconjunto vazio de $\mathcal{L}$ é o subconjunto vazio de $\mathcal{D}$.

É muito importante o caso duma aplicação biunívoca de $\mathcal{L}$ sobre $\mathcal{D}$. Significa-se com isto, não apenas que todos os elementos de $\mathcal{D}$ são obtidos como imagens, mas ainda que cada a' é imagem dum único elemento a. Esta última afirmação também se traduz dizendo que, supondo $a \neq b$, é $a' \neq b' = f(b)$, ou que $a' = b'$ arrasta $a = b$. Uma aplicação biunívoca de $\mathcal{L}$ sobre $\mathcal{D}$ diz-se uma bijecção. Entre as bijecções dum conjunto sobre si, que designaremos por permutações do conjunto, destacaremos a permutação identidade I, que aplica cada elemento em si mesmo.

Sempre que dois conjuntos se podem aplicar um sobre o outro de modo biunívoco, diz-se que os conjuntos têm a mesma potência ou que têm o mesmo número cardinal (são equicardinais).

*

Em termos de correspondências, uma função f determina uma correspondência de $\mathcal{L}$ para $\mathcal{D}$. Identificaremos f com esta correspondência. Inversamente, uma correspondência φ, de $\mathcal{L}$ para $\mathcal{D}$, será uma função, se e só se tiverem lugar as inclusões

$$\varphi \circ \varphi^{-1} \supseteq \Delta_{\mathcal{L}}, \qquad \varphi^{-1} \circ \varphi \subseteq \Delta_{\mathcal{D}}. \tag{2}$$

A primeira destas inclusões garante que todo o $a \in \mathcal{L}$ tem imagem $a' \in \mathcal{D}$, pois $(a,a) \in \varphi \circ \varphi^{-1}$, o que implica que $\exists\, x'$ tal que $(a,x') \in \varphi$, $(x',a) \in \varphi^{-1}$. Tem-se então $a' = x'$. A segunda inclusão mostra

que há uma só imagem de a, visto que $(a,b')\in\varphi$, $(a,c')\in\varphi$, com $b'\neq c'$, teria-se $(b',a)\in\varphi^{-1}$, $(a,c')\in\varphi$, e, portanto, ter-se-ia o absurdo $(b',c')\in A_{\mathcal{D}}$.

*

Exercício:- O produto de duas funções é uma função. [Nota: Tenham-se em conta o exercício anterior e as inclusões (2)].

*

Regressemos a $a'=af$. Podemos dizer que a é um objecto, original de a'. Pondo $f^{-1}=\{(a'_1,a),(b'_1,b),\dots\}$, é claro que f^{-1} tem o sentido que atribuímos à correspondência inversa de f. Não se trata, porém, de uma aplicação de $\mathcal{D}$ em $\mathcal{L}$, pois pode haver elementos de $\mathcal{D}$ sem original em $\mathcal{L}$, assim como pode $a'=af$ ter vários originais.

No que vai seguir-se, utilizaremos a convenção seguinte: supondo $D\subseteq\mathcal{D}$, o símbolo $f^{-1}(D)$ representará a totalidade dos originais dos elementos de D. Diremos $f^{-1}(D)$ imagem completa inversa de D.

Quando f é uma aplicação biunívoca de $\mathcal{L}$ sobre $\mathcal{D}$, f^{-1} é igualmente uma aplicação biunívoca de $\mathcal{D}$ sobre $\mathcal{L}$. Neste caso, f^{-1} é a aplicação inversa de f.

*

Exercício:- Demonstrar as seguintes igualdades e inclusões:

$$f(A\cup B)=f(A)\cup f(B),\qquad f^{-1}(A'\cup B')=f^{-1}(A')\cup f^{-1}(B'),$$
$$f(A\cap B)\subseteq f(A)\cap f(B),\qquad f^{-1}(A'\cap B')=f^{-1}(A')\cap f^{-1}(B'),$$
$$f(\mathcal{L}-A)\supseteq\mathcal{D}-f(A),\qquad f^{-1}(\mathcal{D}-A')=\mathcal{L}-f^{-1}(A').$$

[Nota: A inclusão $f(\mathcal{L}-A)\supseteq\mathcal{D}-f(A)$ implica que f seja sobrejectiva. Com esta mesma hipótese, também se tem $f(f^{-1}(A'))=A'$, enquanto que é sempre $f^{-1}(f(A))\supseteq A$].

*

Observações:- I) Consideremos um produto $f\circ g$ de duas aplicações. De acôrdo com a definição dada pela igualdade (1) para o produto $\varphi\circ\psi$ de duas correspondências, é natural escrever $x(fg)$, $(x\in\mathcal{R})$, para se obterem as imagens em $\mathcal{D}$ dos elementos x. Todavia também se poderá escrever $(fg)(x)$, $(y\in\mathcal{L})$, mas entendendo então que se efectuou primeiramente a aplicação g, depois a aplicação f. Interessando-nos principalmente o caso em que o produto não é vazio, notemos que isto acontece, tratando-se de $x(fg)$, quando g é uma aplicação $\mathcal{L}\to\mathcal{D}$; e, tratando-se de $(fg)y$ quando f é uma aplicação $\mathcal{L}\to\mathcal{R}$.

II) No caso de uma permutação θ dum conjunto, tem-se $\theta\circ\theta^{-1}=\theta^{-1}\circ\theta=I$.

III) Se φ é uma aplicação de $\mathcal{L}$ em $\mathcal{D}$, diz-se muitas vezes que $\varphi(A)$, $(A\in\mathcal{L})$ é a restrição a A da aplicação φ. Utilizando um argumento ξ, de tal modo que, escrevendo $\varphi(\xi)$, em vez de φ, se significa que o referido argumento percorre o domínio $\mathcal{L}$, então, em lugar de $\varphi(A)$, pode designar-se por $\varphi_A(\xi)$ a restrição em causa. Por sua vez, $\varphi(\xi)$ diz-se extensão de $\varphi_A(\xi)$.

4. Conjuntos ordenados- Um conjunto $L \subseteq M$ diz-se parcialmente ordenado, quando nele se distingue uma relação ρ com as propriedades seguintes: i) $\forall a \in M$, tem-se $a \rho a$; ii) a propriedade anti-simétrica é válida, isto é, se se tem $a \rho b$ e $b \rho a$, então $a = b$; iii) se se tem $a \rho b$ e $b \rho c$, então $a \rho c$. Em geral, tratando-se dum conjunto parcialmente ordenado, escreve-se $a \preceq b$, em vez de $a \rho b$.

Um conjunto O diz-se ordenado, totalmente ordenado ou uma cadeia, quando nele se distingue uma relação ρ com as propriedades seguintes: j) dados a e b, com $a \neq b$, realiza-se uma e uma só das hipóteses $a \rho b$ ou $b \rho a$ (dicotomia); jj) se $a \rho b$ e $b \rho c$, então $a \rho c$. Em geral, tratando-se dum conjunto ordenado, escreve-se $a < b$, em vez de $a \rho b$. Deverá observar-se que nunca se tem $a \rho a$.

Voltemos aos conjuntos parcialmente ordenados. Quando se tem $a \preceq b$, com $a \neq b$, pode escrever-se $a < b$. Se $M_0 \subseteq M$ é uma parte de M, diz-se que $v \in M$ é um majorante de M_0, se, para cada $a_0 \in M_0$, se tem $a_0 \preceq v$. O elemento $t \in M$ é um minorante de M_0, se se tem $t \preceq a_0$, para cada $a_0 \in M_0$. Evidentemente, M_0 é um conjunto parcialmente ordenado para a mesma relação de ordem $\preceq$. Um elemento $m \in M$ é chamado maximal, se não existe $x \in M$ tal que $m < x$. Um elemento $m_0 \in M$ é minimal, se não existe $x \in M$ tal que $x < m_0$. Se existe, entre os majorantes de M_0, um majorante v_0 tal que qualquer outro majorante v verifica a condição $v_0 \preceq v$, diz-se v_0 limite superior ou supremo de M_0. O limite inferior ou ínfimo de M_0, se existe, é um minorante t_0 tal que qualquer outro minorante t verifica a condição $t \preceq t_0$. Os limites superior e inferior de M_0 podem ou não pertencer a M_0.

Também num conjunto ordenado podem introduzir-se as noções de majorante, minorante, limite superior e limite inferior. Por exemplo, tomando $O_0 \subseteq O$, $v \in O$ será um majorante de O_0, se se tem $a_0 < v$, $\forall a_0 \in O_0$ tal que $a \neq v$; e um majorante v_0 de O_0 será o limite superior de O_0, se se tem $v_0 < v$, para todo o majorante $v \neq v_0$.

Um conjunto ordenado $O = b$ é bem ordenado, se cada subconjunto não vazio $A \subseteq b$ contém um primeiro elemento, isto é, um elemento a_0 que "precede" todos os elementos de A: $a_0 < a$, $\forall a \in A$ tal que $a \neq a_0$. Um conjunto bem ordenado designa-se também por ordinal. [Não se exclui a possibilidade de o vazio poder ser considerado um conjunto parcialmente ordenado, um conjunto ordenado ou um ordinal].

*

Exemplos: - i) Os subconjuntos dum conjunto L formam um conjunto par-

cialmente ordenado para a relação de inclusão. Supondo $A \subseteq \mathcal{L}$, $B \subseteq \mathcal{L}$, vê-se que $A \cap B$ é o limite inferior e $A \cup B$ o limite superior dos dois subconjuntos.

II) Um conjunto $\mathcal{L} = \{a, b, c, d, e, f, g\}$ no qual se supõe $a < b < c < d < e < f < g$ é ordenado e bem ordenado. No subconjunto $A = \{a, b, f\}$, $\underline{a}$ é o primeiro elemento e o limite inferior de $\underline{A}$; $\underline{f}$ é o seu limite superior.

*

O conjunto ordenado das relações:- Introduzimos no n.º 3 o conceito de relação. Se $\underline{\alpha}$ e $\underline{\beta}$ são duas relações sobre $\mathcal{U}$, define-se a intersecção $\alpha \wedge \beta$ destas relações pondo

$$x(\alpha \wedge \beta)y, \text{ se e só se } x \alpha y \text{ e } x \beta y.$$

A união $\alpha \vee \beta$ é definida pondo

$$x(\alpha \vee \beta)y, \text{ se e só se } x \alpha y \text{ ou } x \beta y.$$

O produto $\alpha\beta$, ou $\alpha\beta$, de duas relações, de harmonia com (1), n.º 3, é definido pondo

$$x(\alpha\beta)y, \text{ se existe } z \in \mathcal{U} \text{ tal que } x \alpha z, z \beta y.$$

Sempre que $x \alpha y$ implicar $x \beta y$, diremos que $\underline{\alpha}$ implica $\underline{\beta}$ e escrevemos $\alpha \subseteq \beta$. Com êste símbolo $\subseteq$ define-se uma relação de ordem parcial, cujos elementos são as relações sobre um conjunto. Verifica-se então:

i) que $\alpha \wedge \beta = \beta \wedge \alpha$ é ínfimo de $\{\alpha, \beta\}$;

ii) que $\alpha \vee \beta = \beta \vee \alpha$ é supremo de $\{\alpha, \beta\}$;

iii) que é válida a propriedade associativa: $(\alpha\beta)\gamma = \alpha(\beta\gamma)$;

iv) que, de $\alpha \subseteq \gamma$, $\beta \subseteq \delta$, se deduz $\alpha\beta \subseteq \gamma\delta$;

v) que $(\alpha \wedge \beta)\gamma \subseteq \alpha\gamma \wedge \beta\gamma$, (propriedade semidistributiva à direita);

vi) que $(\alpha \vee \beta)\gamma = \alpha\gamma \vee \beta\gamma$, (propriedade distributiva à direita);

vii) que, sendo $\underline{\alpha}$ reflexiva, então $\beta \subseteq \alpha\beta$, $\beta \subseteq \beta\alpha$;

viii) que, sendo $\underline{\alpha}$ reflexiva e transitiva, é $\alpha\alpha = \alpha$.

Demonstremos v) e vii), deixando ao cuidado do leitor as demonstrações das outras asserções. Quanto a v): da hipótese $x(\alpha \wedge \beta)\gamma)y$, pretendemos deduzir $x(\alpha\gamma)y$, $x(\beta\gamma)y$. Ora, $\exists z$ tal que $x(\alpha \wedge \beta)z$, $z \gamma y$; por conseguência, $x \alpha z$, $x \beta z$, $z \gamma y$, o que leva a $x(\alpha\gamma)y$, $x(\beta\gamma)y$. Quanto a vii): de $x \beta y$, pois que $x \alpha x$, $x \beta y$, tira-se $x(\alpha\beta)y$; analogamente, de $x \beta y$, $y \alpha y$, tira-se $x(\beta\alpha)y$.

*

Observação:- Também se introduz sobre um conjunto a relação vazia, segundo a qual não existem dois elementos em relação, e a relação um, segundo a qual dois elementos quaisquer estão sempre em relação. A relação vazia precede qualquer relação e por isso se diz elemento zero do respectivo conjunto parcialmente ordenado; e a relação um "segue" qualquer outra relação e por isso se diz elemento um do respectivo conjunto parcialmente ordenado.

***

5. Relações de equivalência - Uma relação ρ, sobre $\mathcal{L}$, que seja reflexiva, simétrica e transitiva toma o nome de relação de equivalência. Os elementos em relação dizem-se equivalentes.

*

Exemplos: -I) Dado $\mathcal{L}$, ponha-se $x\rho y$, se e só se $x \in \mathcal{L}$, $y \in \mathcal{L}$. ρ é relação de equivalência.

II) Consideremos um conjunto de bolas de côres diferentes. Define-se uma relação de equivalência, tomando como equivalentes as bolas da mesma côr.

III) Tome-se uma aplicação $\mathcal{U} \xrightarrow{f} b$. Define-se sobre $\mathcal{U}$ uma relação de equivalência, tomando como equivalentes os elementos de $\mathcal{U}$ que tenham a mesma imagem em b.

*

Exercícios: -I') Verificar que uma relação ρ é uma relação de equivalência, se e só se satisfizer as condições seguintes:

i) $\rho \supseteq \Delta_{\mathcal{U}}$; ii) $\rho^{-1} = \rho$; iii) $\rho \circ \rho = \rho$.

II') O exemplo III), acima, mostra que sendo f uma aplicação, $f \circ f^{-1}$ é uma relação de equivalência. Diz-se que esta relação é o núcleo de f.

*

Sobre um conjunto $\mathcal{L} \neq \phi$, tome-se uma relação de equivalência ρ. Se for $a \in \mathcal{L}$, representaremos por $\mathcal{C}_a$ o conjunto dos elementos equivalentes a a. $\mathcal{C}_a$ não é vazio, visto que $a\rho a$, portanto $a \in \mathcal{C}_a$. Se se dá uma segunda classe de equivalência $\mathcal{C}_b$, a existência dum elemento $d \in \mathcal{C}_a \cap \mathcal{C}_b$ implica $\mathcal{C}_a = \mathcal{C}_b$. De facto, sendo $a\rho d$ e $b\rho d$, vamos vê, por exemplo, que qualquer $f \in \mathcal{C}_a$ é um elemento de $\mathcal{C}_b$. De $a\rho d$, $a\rho f$, conclui-se $d\rho a$, $a\rho f$, por

tanto $d\rho f$. Então, de $b\rho d$, $d\rho f$, deduz-se $b\rho f$, o que leva a $f \in \mathcal{C}_b$.

Podemos dizer: um elemento do conjunto $\mathcal{L}$ pertence necessàriamente a uma classe; e duas classes diferentes são disjuntas.

O conjunto das diferentes classes representa-se por $\mathcal{L}/\rho$ e diz-se o conjunto cociente de $\mathcal{L}$ por ρ. Associando a cada $a \in \mathcal{L}$ a classe $\mathcal{C}_a$ obtemos a aplicação canónica ou aplicação natural $\mathcal{L} \longrightarrow \mathcal{L}/\rho$. Trata-se de uma aplicação sobrejectiva.

*

Exercícios: -II') Dada a aplicação $\mathcal{U} \xrightarrow{f} b$, verificar que ela admite a factorização $f = \varepsilon \tau j$, onde $\mathcal{U} \xrightarrow{\varepsilon} \mathcal{U}/\rho$ é uma sobrejecção, $\mathcal{U}/\rho \xrightarrow{\tau} \mathcal{U}f$ é uma bijecção e $\mathcal{U}f \xrightarrow{j} b$ é uma injecção.

II") Dissémos que uma relação de equivalência sobre $\mathcal{U}$ divide $\mathcal{U}$ em classes disjuntas, ou seja: determina uma partição de $\mathcal{U}$. Reciprocamente, uma partição de $\mathcal{U}$ define uma relação de equivalência única levando à dada partição.

*

Relação de equivalência cociente: Partamos dum conjunto cociente $\mathcal{L}/\rho$. Se τ é uma segunda relação de equivalência sobre $\mathcal{L}$, suponhamos $\rho \subseteq \tau$. Se for $\mathcal{L}/\rho = \{\mathcal{C}_a, \mathcal{C}_b, \ldots\}$, $\mathcal{L}/\tau = \{\mathcal{C}'_g, \mathcal{C}'_h, \ldots\}$, vê-se que $\mathcal{C}_a \subseteq \mathcal{C}'_g$, se $a \in \mathcal{C}'_g$. Cada classe $\mathcal{C}'_f$ compõe-se exactamente de classes $\mathcal{C}_a$. Obtêm-se as desses

C'_f, a partir das classes C_ε, introduzindo sobre Σ/ρ uma relação de equivalência, para a qual os elementos equivalentes (classes) são os que estão contidos numa mesma classe C'_f. Esta relação de equivalência diz-se relação de equivalência cociente e representa-se por τ/ρ. Há uma bijecção θ das classes de Σ/τ, que são formadas por elementos de Σ, sobre as classes de $(\Sigma/\rho)/(\tau/\rho)$:

$$(\Sigma/\rho)/(\tau/\rho) \xrightarrow{\theta} \Sigma/\tau.$$

*

Exemplo:- Seja Σ um conjunto de bolas brancas, amarelas, vermelhas e negras. ρ designará a relação de equivalência que considera equivalentes as bolas da mesma côr. ρ implica a relação τ, na qual são equivalentes as bolas negras, depois as vermelhas, e, em terceiro lugar, as bolas brancas e amarelas. A relação τ/ρ leva das classes que são definidas pela relação ρ a um conjunto que tem menos um elemento. Em Σ/ρ são equivalentes - τ/ρ - as classes compostas só de bolas integras, ou só de bolas vermelhas; enquanto que são equivalentes as classes de bolas brancas e de bolas amarelas.

*

Exercício:- Sabendo que $\rho \leq \sigma_1$, $\rho \leq \sigma_2$, mostrar que se tem $(\sigma_1 \wedge \sigma_2)/\rho = \sigma_1/\rho \wedge \sigma_2/\rho$.

§ 2 - Números naturais. Cardinais

***

1. Postulados e operações - Diz-se $\mathcal{N} = \mathbb{N}$ um conjunto de números naturais, se em $\mathbb{N}$ se supõem realizados os axiomas de Peano: I) existe um número natural chamado um e representado por 1; II) cada número natural a tem um "sucessor" a', que é também um número natural; III) o número 1 não é um sucessor dum número natural; IV) os sucessores a' e b', supondo $a \neq b$, são números naturais distintos; V) é válido o seguinte princípio de indução completa: se um subconjunto $\mathbb{N}_0 \subseteq \mathbb{N}$ contém 1 e, com cada $a \in \mathbb{N}_0$, contém a', então é $\mathbb{N}_0 = \mathbb{N}$.

O princípio de indução completa demonstra imediatamente que todo o número natural $\neq 1$ é sucessor de um elemento. Basta, com efeito, considerar o subconjunto $\mathbb{N}_0$ formado por 1 e pelos números naturais que são sucessores de números naturais.

No n.º 2, § anterior, falámos já de exemplos de operações. Aqui vamos limitar-nos às operações binárias. Introduzir uma tal operação num conjunto $\mathcal{A}$ é dar um processo pelo qual se deduz, de modo unívoco, de um par ordenado (a, b) de elementos de $\mathcal{A}$, um elemento $c \in \mathcal{A}$. Esta operação designa-se frequentemente por soma e escreve-se $a+b=c$, ou por

produto e escreve-se, então, $a.b=c$, ou, mais simplesmente ainda $ab=c$.

*

Soma:- No conjunto dos números naturais, define-se uma soma pelas duas igualdades seguintes: $a+1=a'$, $a+b'=(a+b)'$. A soma encontra-se efectivamente definida, porque sabemos "adicionar" 1 a um elemento qualquer a, e, sabendo adicionar b a a também sabemos adicionar b' a a. A soma goza das propriedades seguintes:

I') é associativa: $(a+b)+c=a+(b+c)$;

II') é comutativa: $a+b=b+a$;

III') de $a+b=a+c$, deduz-se $b=c$ (lei do corte).

*

Exercício:- Da definição de soma e do princípio de indução completa, deduzir a propriedade associativa.

*

A partir da propriedade associativa e tendo em conta o princípio de indução completa, vamos demonstrar a propriedade comutativa. Começemos por supôr $a=1$. Então $1+1=1+1=1'$; e, se $1+b=b+1=b'$, tem-se também $1+b'=1+(b+1)=(1+b)+1=(b+1)+1=b'+1$. Admitido por fim que $a+b=b+a$, vamos vêr que $a'+b=b+a'$. Ora $a'+b=(1+a)+b=1+(a+b)=1+(b+a)=(1+b)+a=(b+1)+a=b+(1+a)=b+a'$.

*

Exercício:- Tendo em conta o princípio da indução completa, o postulado IV e as propriedades já conhecidas da soma, demonstrar a lei do corte.

*

Produto:- Define-se um produto em $\mathbb{N}$ pelas igualdades seguintes: $a.1=a$, $a.b'=ab+a$. O produto goza das propriedades seguintes:

I") é distributivo à direita: $(a+b)d=ad+bd$;

II") é comutativo: $ab=ba$;

III") é associativo: $ab.d=a.bd$;

IV") de $ad=bd$, deduz-se $a=b$ (lei do corte).

Demonstremos I"). Logo $d=1$, tem-se $(a+b).1=a+b=a.1+b.1$. Se, agora, a igualdade I") é válida com $d=c$, vamos ver que é válida com $d=c'$. Com efeito, resulta da definição de produto e da hipótese $(a+b)c'=(a+b)c+(a+b)$, que é $(a+b)c'=(ac+bc)+(a+b)=(ac+a)+(bc+b)=ac'+bc'$.

*

Exercício:- Demonstrar II"), a distributividade à esquerda e a associatividade.

*

Vamos justificar IV"). Supondo $1d=bd$, conclui-se $b=1$, visto que não pode ter-se $b=b_0+1$. Admitindo em seguida que $ad=bd$ implica $b=a$, vamos verificar que $a'd=fd$ implica $f=a'$. De facto, tem-se $ad+d=fd$, portanto não pode ser $f=1$. Então, com $f=f_0+1$, obtemos $ad+d=f_0d+d$, $ad=f_0d$, $a=f_0$, $a'=f$.

2. Ordenação dos números naturais - A operação de soma permite introduzir uma ordenação nos números naturais, de modo a obter uma cadeia. Para isso, poremos $a<b$, sempre que exista c tal que $a+c=b$. Desta definição resulta imediatamente que não pode ter-se ao mesmo tempo $a<b$ e $b<a$. Com efeito, se se tivesse $b=a+c$, $a=b+d$, ter-se-ia também $b=b+(d+c)=b+k$, com $d+c=k$. Então, $b+1=b+b+(k+1)$, $1=k+1$, o que é absurdo. Importa porém demonstrar que, tomados a e b ou é $a<b$ ou $b<a$. De facto, tomemos a e consideremos o conjunto $\mathcal{N}_0$ dos números naturais, nas condições seguintes: pertencem a $\mathcal{N}_0$ o número a, os números que precedem a (também chamados menores do que a) e os números que têm precedidos por a (também chamados maiores do que a). O número 1 pertence a $\mathcal{N}_0$, pois que ou se tem $a=1$, ou, de contrário $a=a_0'=a_0+1=1+a_0$, o que implica $1<a$. E, se um número b pertence a $\mathcal{N}_0$, o mesmo sucede a b', pela razão seguinte: se $b=a$, $b'=a+1$ e $a<b'$; se $b\neq a$, tem-se, por exemplo, $b<a$, isto é $a=b+b_0$; neste caso, ou $b_0=1$ e $b'=a$, ou $b_0=k+1$ e $a=b+(k+1)=(b+1)+k$, o que dá $b'<a$. Quanto à hipótese $a<b$, ela dá imediatamente $a<b'$. Vê-se assim que $\mathcal{N}_0=\mathcal{N}$, por conseguinte $\mathcal{N}$ é um conjunto ordenado, visto que a transitividade do sinal $<$ é evidente. Na ordenação de que se trata, o número 1 precede todo o número natural $\neq 1$.

*

Exercício: - Verificar que o sinal $<$ goza das propriedades seguintes: i) de $a<b$, conclui-se $a+c<b+c$; ii) de $a<b$, conclui-se $ac<bc$; iii) não existe b tal que $a<b<a+1$.

*

A validade de iii) permite dar à noção abstracta de "sucessor" o sentido habitual: não existe b tal que $a<b<a'$, ou ainda não existe um número natural "entre" a e a'. Tendo em conta o princípio da indução completa, podemos afirmar que

$$\mathcal{N}=\{1,\ 1',\ (1')',\ ((1')')',\ \ldots\} \qquad (1)$$

*

Teorema 1 (da boa ordenação): - Todo o conjunto não vazio de números naturais tem primeiro elemento. Seja $\mathcal{N}_0$ o conjunto em questão. Se $1\in\mathcal{N}_0$, 1 é o seu primeiro elemento. Supondo $1\notin\mathcal{N}_0$, vamos considerar o conjunto B dos números naturais que precedem todos os números de $\mathcal{N}_0$. O conjunto B não é vazio, visto que $1\in B$; também não é igual a $\mathcal{N}$, pois que os elementos de $\mathcal{N}_0$ não pertencem a B. $\exists\, t\in B$ tal que $t'\notin B$. Por conseguinte, existe $v_0\in\mathcal{N}_0$ tal que $t<v_0$, sem que se tenha $t'<v_0$. Ora, ou $t'=v_0$ ou $t'=v_0+k$. Esta última hipótese não pode verificar-se, pois não é possível ter-se $t<v_0<t'$. Terá $t'=v_0=t+1$. Para qualquer outro $v\in\mathcal{N}_0$, temos $v=t+n$. Ou é $n=1$ e $v=v_0$, ou é $n=x+1$, o

que dá $v = (t+1) + x = v_0 + x$, $v_0 < v$. O número v_0 é o primeiro elemento de $\mathfrak{N}_0$.

* O segundo princípio de indução completa:- O princípio de indução completa pode ser substituido, por vezes com vantagem, pelo enunciado seguinte, que constitui o segundo princípio de indução completa: Um conjunto $\mathfrak{N}_0$ de números naturais que, quando contém os números naturais que precedem n, também contém n, é igual ao conjunto de todos os números naturais. Com efeito, $\mathfrak{N}_0$ não é vazio, porque estando o conjunto vazio contido em qualquer conjunto, $\mathfrak{N}_0$ contém o conjunto dos números naturais que precedem 1, portanto $1 \in \mathfrak{N}_0$. Em seguida designemos por $\mathfrak{N}_1$ o conjunto dos números naturais que não pertencem a $\mathfrak{N}_0$. Se este conjunto fôr vazio, a afirmação está demonstrada. Se não fôsse vazio, existiria, conforme o teorema da boa ordenação, um elemento mínimo n_1. Todos os números naturais precedendo n_1 pertenceriam a $\mathfrak{N}_0$ e seria $n_1 \in \mathfrak{N}_0$, o que dá uma contradição. $\mathfrak{N}_1$ é de facto vazio.

* Em lugar da representação (1) dos números naturais, utilizaremos esta outra:

$$\mathfrak{N} = \{1, 2, 3, 4, \dots, n, \dots\}. \qquad (2)$$

***

3 Cardinais- No conjunto (2) do número anterior, chamaremos S_n uma secção de $\mathfrak{N}$, se fôr um subconjunto exactamente composto de n e dos números naturais que precedem n. Tomadas duas secções S_m e S_n, se fôr $m < n$, será S_m uma parte própria de S_n. Um conjunto A diz-se finito e de número cardinal n, se A e S_n tiverem a mesma potência (fôrem equipotentes).

Utilizemos o símbolo $\sim$ para significar "equipotente a". Lê-se êste

* Exercício:- Supondo $\mathfrak{X} \subseteq A$, $\mathfrak{Y} \subseteq B$, $\mathfrak{X}$ e $\mathfrak{Y}$ equipotentes e $A - \mathfrak{X} = B - \mathfrak{Y}$, mostrar que os conjuntos A e B são equipotentes.

* Teorema 1:- Seja $A \sim S_{n+1}$; então, $\forall x \in A$, tem-se $A - \{x\} \sim S_n$. Se φ é a bijecção de A sobre S_{n+1}, tem-se $\varphi(A) = S_{n+1} = \varphi(A - \{x\}) \cup \varphi(x)$. Daqui se tira $S_{n+1} - \{\varphi(x)\} = \varphi(A - \{x\})$, de sorte que $A - \{x\} \sim S_{n+1} - \{\varphi(x)\}$. No caso de ser $\varphi(x) = n+1$, o teorema é logo evidente. Não sendo assim, tem-se $S_{n+1} - \{\varphi(x)\} - \{n+1\} = (S_{n+1} - \{\varphi(x), n+1\}) = S_n - \{\varphi(x)\}$. Conforme o exercício anterior, conclui-se $S_{n+1} - \{\varphi(x)\} \sim S_n$, ou seja $A - \{x\} \sim S_n$, como se deseja.

* Corolário 1:- Todo o subconjunto próprio A, de S_n, não pode ser equipotente a S_n. Se $n = 1$, a afirmação é evidente. Admitindo o corolário para S_n, vamos demonstrá-lo para S_{n+1}. Se se tivesse $A \subset S_{n+1}$, $A \sim S_{n+1}$, teríamos também $A - \{x\} \sim S_n$, $\forall x \in A$. No caso de ser $n+1 \in A$, pondo $x = n+1$ estaríamos em contradição com a hipótese; se $n+1 \notin A$, tem-se $A \subset S_n$, $A - \{x\} \subset S_n$, $A - \{x\} \sim S_n$, igualmente uma contradição.

* Corolário 2:- Todo o subconjunto próprio A dum conjunto finito $\mathcal{L}$ não pode ser equipotente a $\mathcal{L}$. Partamos de $A \subset \mathcal{L} \sim S_n$ e designemos por φ a bijecção $\mathcal{L} \to S_n$. Ter-se-á $\mathcal{L} \sim S_n$, $\varphi(A) \subset S_n$ e $A \sim \varphi(A)$. Portanto, não pode ter-se $A \sim \mathcal{L}$, visto que isto arrastaria $\varphi(A) \sim A \sim \mathcal{L} \sim S_n$, isto é $\varphi(A) \sim S_n$.

* Observação:- Um conjunto finito não pode ser equipotente a duas secções S_m e S_n distintas. Se é equipotente a S_m diz-se que tem m elementos.

* Exercícios:- I) Se $\mathcal{L}$ e $\mathcal{L}'$ são dois conjuntos, respectivamente com m e n elementos, o conjunto $\mathcal{L} \cup \mathcal{L}'$ tem $m+n$ elementos.

II') O conjunto reunião de m conjuntos distintos, cada um deles com n elementos, contém mn elementos.

* Exemplo dum conjunto não finito:- Consideremos o conjunto $\mathcal{N}$ dos números naturais. Uma aplicação biunívoca de $\mathcal{N}$ sobre $\mathcal{N}_0 = \{2, 3, 4, \dots\}$ é, por exemplo, a seguinte: $n \to \varphi(n) = n'$, $(n \in \mathcal{N})$. Resulta daqui que $\mathcal{N}$ não é um conjunto finito. Diz-se conjunto infinito todo o conjunto que não é finito. $\mathcal{N}$ é, assim, um conjunto infinito.

* Os conjuntos que têm o mesmo número cardinal de $\mathcal{N}$ ou de uma secção S_n dizem-se numeráveis. É hábito empregar o símbolo $\aleph_0$ para representar o número cardinal de $\mathcal{N}$.

***

4. O problema da tricotomia - Dados dois conjuntos finitos quaisquer $\mathfrak{A}$ e $\mathfrak{b}$, equipotentes, respectivamente de S_m e de S_n, o número cardinal de $\mathfrak{A}$ é inferior ao de $\mathfrak{b}$, se se tem $m < n$. Para dois conjuntos finitos $\mathfrak{A}$ e $\mathfrak{b}$, o problema da tricotomia tem uma solução positiva: 1) ou o cardinal de $\mathfrak{A}$ é inferior ao de $\mathfrak{b}$; 2) ou $\mathfrak{A}$ e $\mathfrak{b}$ têm o mesmo número cardinal; 3) ou, ainda, o cardinal de $\mathfrak{A}$ é superior ao de $\mathfrak{b}$ (caso em que $m > n$). O problema da tricotomia também se põe para conjuntos quaisquer e tem igualmente uma solução positiva. É de uma tal solução que agora vamos começar a ocupar-nos.

* Teorema 1 (Schroeder-Bernstein):- Se $\mathfrak{A}$ e $\mathfrak{b}$ são dois conjuntos tais que $\mathfrak{A}$ é equipotente a $\mathfrak{b}_0 \subseteq \mathfrak{b}$ e $\mathfrak{b}$ é equipotente a $\mathfrak{A}_0 \subseteq \mathfrak{A}$, então $\mathfrak{A}$ e $\mathfrak{b}$ são equipotentes. A bijecção $\mathfrak{b} \to \mathfrak{A}_0$ leva a $\mathfrak{A}_1 \subseteq \mathfrak{A}_0$ tal que $\mathfrak{b}_0 \sim \mathfrak{A}_1$. Então, ter-se-á $\mathfrak{A} \sim \mathfrak{b}_0 \sim \mathfrak{A}_1$, portanto $\mathfrak{A} \sim \mathfrak{A}_1$. O lema a seguir mostra que, de $\mathfrak{A} \sim \mathfrak{A}_1$, se deduz $\mathfrak{A} \sim \mathfrak{A}_0$, pelo que $\mathfrak{A} \sim \mathfrak{b}$, como se desejava.

* Lema 1:- Se $\mathfrak{A}$ é equipotente a uma das suas partes $\mathfrak{A}_1$, $\mathfrak{A}$ é equipotente a toda a parte $\mathfrak{A}_0$ compreendida entre $\mathfrak{A}$ e $\mathfrak{A}_1$. Ponhamos $\mathfrak{A}_1 = A$, $\mathfrak{A}_0 - \mathfrak{A}_1 = B$, $\mathfrak{A} - \mathfrak{A}_0 = C$, de sorte que $A \sim \mathfrak{A}_1$, $\mathfrak{A}_0 = A \cup B$, $\mathfrak{A} = A \cup B \cup C$. O nosso objectivo é demonstrar que $A \cup B \cup C \sim A \cup B$, e $A \cup B \cup C \sim A$. Se

a equipotência $A \cup B \cup C \sim A$ é definida pela bijecção φ, ponhamos $\varphi(A) = A_1$, $\varphi(B) = B_1$, $\varphi(C) = C_1$, de sorte que $A = A_1 \cup B_1 \cup C_1$. Observemos que A_1, B e C são disjuntos e que o mesmo acontece a A_1, B_1 e C_1. De resto, B_1 e C_1 são também disjuntos de B e C. De $A_1 \cup B_1 \cup C_1 \sim A_1$, deduz-se, como acima, $\varphi(A_1) = A_2$, $\varphi(B_1) = B_2$, $\varphi(C_1) = C_2$, com $A_1 = A_2 \cup B_2 \cup C_2$. Os conjuntos A_2, B_2 e C_2 são disjuntos dois a dois e B_2 e C_2 são disjuntos de B_1 e C_1, assim como de B e C. Prosseguindo, obtem-se

$$\mathcal{U} = (B \cup C) \cup A = (B \cup C) \cup (B_1 \cup C_1) \cup A_1 = (B \cup C) \cup (B_1 \cup C_1) \cup (B_2 \cup C_2) \cup A_2 = \dots = (B \cup C) \cup (B_1 \cup C_1) \cup (B_2 \cup C_2) \cup \dots \cup \left[\bigcap A_i\right] =$$

$$= (C \cup C_1 \cup C_2 \cup \dots) \cup \left[(B \cup B_1 \cup B_2 \cup \dots) \cup \left(\bigcap A_i\right)\right],$$

como vamos verificar. Tomemos $x \in \mathcal{U}$. Pode ter-se $x \in B \cup C$, mas, se não é assim, tem-se $x \in A$. Então, ou $x \in B_1 \cup C_1$, ou $x \in A_1$. Nesta última hipótese, ou $x \in B_2 \cup C_2$ ou $x \in A_2$. Com êste raciocínio, ou bem se chega a $x \in B_j \cup C_j$, ou, qualquer que seja j, nunca se tem $x \in B_j \cup C_j$. Então x pertence a todos os A_j, isto é, $x \in \bigcap A_j$. Vê-se assim que

$$\mathcal{U}_0 = A \cup B = B \cup (B_1 \cup C_1) \cup A_1 = \dots = (C_1 \cup C_2 \cup \dots) \cup \left[B \cup B_1 \cup B_2 \cup \dots \cup \left(\bigcap A_i\right)\right]$$

Por construção, tem-se $C \sim C_1 \sim C_2 \sim C_3 \sim \dots$, de sorte que, a partir de φ, pode obter-se uma bijecção ψ, de $\mathcal{U}$ sobre $\mathcal{U}_0$, pondo $\psi(C) = \varphi(C) = C_1$, $\psi(C_1) = \varphi(C_1) = C_2$, etc., ou seja: obtem-se ψ pondo $\psi(x) = \varphi(x)$ para todo o $x \in C, C_1, \dots$ e pondo $\psi(x) = x$, tanto para $x \in B, B_1, \dots$ como para $x \in \bigcap A_i$.

Feito isto, tomemos dois conjuntos infinitos $\mathcal{L}$ e $\mathcal{D}$. Se $\mathcal{L}$ tem o mesmo número cardinal que uma parte própria de $\mathcal{D}$, sem que $\mathcal{D}$ tenha o mesmo número cardinal que uma parte própria de $\mathcal{L}$, diz-se que a potência de $\mathcal{D}$ é *superior* à de $\mathcal{L}$ e que a potência de $\mathcal{L}$ é *inferior* à de $\mathcal{D}$.

A solução positiva do problema da tricotomia implica que não possa encontrar-se a situação seguinte: dados $\mathcal{L}$ e $\mathcal{D}$ nenhum deles é equivalente a uma parte do outro. Esta questão será completamente esclarecida mais adiante.

No que se refere pròpriamente à existência de infinidades distintas, vamos demonstrar o seguinte

* **Teorema 2 (Cantor):** — *A totalidade $\mathcal{P}(\mathcal{L})$ dos subconjuntos de $\mathcal{L}$ constitui um conjunto cujo número cardinal é superior ao de $\mathcal{L}$.* Tomemos $\mathcal{L}$ e façamos corresponder a cada $c \in \mathcal{L}$ o subconjunto $\{c\} \in \mathcal{P}(\mathcal{L})$. Obtem-se uma correspondência biunívoca entre $\mathcal{L}$ e uma parte de $\mathcal{P}(\mathcal{L})$. Portanto, o número cardinal de $\mathcal{P}(\mathcal{L})$ se não é igual ao de $\mathcal{L}$ ser-lhe-á superior. Para se vêr que é esta última hipótese que se realiza, consideremos um conjunto $A \in \mathcal{P}(\mathcal{L})$. Define-se uma aplicação de $\mathcal{L}$ no conjunto $\{1,2\}$, pondo $\varphi(c) = 1$, se $c \in A$ e $\varphi(c) = 2$, se $c \notin A$. Em particular, se $A = \mathcal{L}$, não existe um elemento de $\mathcal{L}$ do qual 2 seja imagem, e, se $A = \phi$, não existe elemento de $\mathcal{L}$ tendo 1 por imagem. Por êste processo, estabelece-se uma correspondência biunívoca entre os elementos de $\mathcal{P}(\mathcal{L})$ e as aplicações φ, de $\mathcal{L}$ em $\{1,2\}$. Suponhamos agora que o número cardinal de $\mathcal{L}$ poderia ser igual ao de $\mathcal{P}(\mathcal{L})$.

Haveria uma aplicação bijectiva $c \leftrightarrow \varphi_c$ dos elementos de $\mathcal{L}$ sobre as aplicações φ. Seja agora a aplicação $\bar{\varphi}$, assim definida: dado $c \in \mathcal{L}$, toma-se φ_c, portanto um certo subconjunto $C \in \mathcal{P}(\mathcal{L})$; se $c \in C$, escreve-se $\bar{\varphi}(c) = 2$, de contrário, se $c \notin C$, põe-se $\bar{\varphi}(c) = 1$. A função $\bar{\varphi}$ em questão corresponde a um certo $d \in \mathcal{L}$ e determina um certo $D \in \mathcal{P}(\mathcal{L})$. Será $\bar{\varphi} = \varphi_d$. Mas, se $d \in D$, tem-se $\varphi_d(d) = 1$, enquanto que $\bar{\varphi}(d) = 2$, pois se opõe a $\varphi_d = \bar{\varphi}$; se $d \notin D$, é $\varphi_d(d) = 2$, enquanto que $\bar{\varphi}(d) = 1$, pois, do mesmo modo se opõe a $\varphi_d = \bar{\varphi}$. O absurdo encontrado deve-se ao facto de havermos admitido que $\mathcal{L}$ e $\mathcal{P}(\mathcal{L})$ tinham o mesmo cardinal.

*

Emprega-se habitualmente o símbolo $2^{\mathcal{L}}$, ou também o símbolo 2^{γ}, onde γ é o cardinal de $\mathcal{L}$, para significar o número cardinal de $\mathcal{P}(\mathcal{L})$.

*

Exemplos: - Quando $\mathcal{L} = \phi$, $\mathcal{P}(\mathcal{L})$ contém um elemento, a saber, o conjunto vazio. Tem-se $2^{\phi} = 1$. Se $\mathcal{L} = \{1\}$, é $\mathcal{P}(\mathcal{L}) = \{\phi, \{1\}\}$, pelo que $2^1 = 2$. Se $\mathcal{L} = \{1, 2\}$, é $\mathcal{P}(\mathcal{L}) = \{\phi, \{1\}, \{2\}, \{1, 2\}\}$, o que dá $2^2 = 4$. Duma modo geral, $2^{\aleph_n} = 2^n = 2 \times 2 \times \cdots \times 2$ (n vezes), pelo que $n < 2^n$.

*

Exercícios: - I) Mostrar que não existe um conjunto onde todos os conjuntos possam ser injectados.

II) Construir uma família $\mathcal{P} \neq \mathcal{P}(\mathbb{N})$, de subconjuntos infinitos de $\mathbb{N}$, com número cardinal superior ao de $\mathbb{N}$. [Nota: O leitor pode deixar para mais tarde (§ 2, nº 6) a resolução deste exercício.

*

Observação: Neste número, a propósito da demonstração do teorema de Schroeder-Bernstein, empregámos o símbolo $\bigcap A_j$, em que o índice j pode percorrer uma infinidade de números. É claro que não há qualquer dificuldade de interpretação.

*

A hipótese do contínuo: - Diz-se que se faz a hipótese do contínuo, quando se afirma que nenhum número cardinal existe entre $\aleph_0$ e $2^{\aleph_0}$; e diz-se hipótese generalizada do contínuo a afirmação de que, qualquer que seja o cardinal infinito γ, não existe número cardinal entre γ e 2^{γ}.

***

5. Ordinais - Na Teoria dos Conjuntos, dá-se o nome de axioma de Zermelo ou axioma da escolha à afirmação seguinte: Tomada uma família $\mathcal{F}$, não vazia, cujos elementos são conjuntos não vazios $A, B, C, \ldots$, existe uma função unívoca de conjunto φ, cujo argumento percorre $\mathcal{F}$ e que toma valores $\varphi(A) \in A$, $\varphi(B) \in B$, etc.. Equivalente ao enunciado anterior é êste outro: tomado um conjunto não vazio $\mathfrak{M} = \{a, b, c, \ldots\}$, existe uma função unívoca de conjunto cujo argumento percorre o conjunto dos subconjuntos não vazios $A, B, C, \ldots$, de $\mathfrak{M}$, e que tem valores $\varphi(A) \in A$, $\varphi(B) \in B$, etc..

O axioma de Zermelo implica, como vamos vêr, que todo o conjunto possa ser bem ordenado (teorema da boa ordenação); o teorema da boa ordenação, por sua vez, implica a condição seguinte (condição de Kuratowski): num conjunto parcialmente ordenado $\mathfrak{M}$, não vazio, toda a cadeia não vazia pode ser mergulhada numa cadeia maximal (isto é, que não é sub-

cadeia de outra cadeia de $\mathcal{M}$); e a condição de Kuratowski implica o axioma de Zermelo, de modo que as três afirmações anteriores são equivalentes.

*

A fim de provarmos a implicação axioma de Zermelo → boa ordenação, vamos fazer algumas considerações gerais. Tomemos um ordinal $\mathfrak{b}$. Pode haver em $\mathfrak{b}$ um *último elemento* z, isto é, um elemento tal que, para todo $x \in \mathfrak{b}$, se tenha $x < z$, se $x \neq z$. Se existe um último elemento, ele é necessariamente único.

Dado $t \in \mathfrak{b}$, suponhamos que t não é último elemento. Então, tal que $t < \gamma$. No conjunto dos γ, há um primeiro elemento $t' \in \mathfrak{b}$, gozando da propriedade que não existe $x \in \mathfrak{b}$ para o qual $t < x < t'$. Traduz-se êste fato, dizendo que todo o elemento de $\mathfrak{b}$ que não seja o último, tem um *sucessor*. Mas, sendo dado um elemento arbitrário de $\mathfrak{b}$, não podemos dizer que seja sucessor de um elemento. Se $1 \in \mathfrak{b}$ não é primeiro elemento, diz-se que é um *número limite*, se, de fato, não é um sucessor.

*

Exemplos:- I) O conjunto $\mathcal{N} = \{1, 2, 3, \ldots\}$ dos números naturais constitui um ordinal sem último elemento. Cada elemento tem um sucessor, e, salvo o primeiro, todo o elemento é um sucessor.

II) Se se escreve $\mathfrak{b} = \{1, 2, 3, \ldots; a\}$, onde a é o último elemento, então a é um número limite.

*

Exercícios:- I') Um número limite λ pode ser definido pela propriedade seguinte: dado $x < \lambda$, existe sempre y pertencente ao ordinal tal que $x < y < \lambda$.

II') Dado um ordinal $\mathfrak{b}$ (ou, mesmo, um conjunto ordenado $\mathfrak{O}$), diz-se um *ideal* de $\mathfrak{b}$ uma parte $\mathfrak{C} \subseteq \mathfrak{b}$ nas condições seguintes: se $c \in \mathfrak{b}$ é um elemento de $\mathfrak{C}$, então $x \in \mathfrak{C}$, qualquer que seja $x < c$. Mostrar que, para que $\mathfrak{B} \neq \mathfrak{b}$ seja um ideal, é necessário e basta que $\mathfrak{B} = \mathfrak{b}_x$, significando-se com $\mathfrak{b}_x$ a totalidade dos elementos de $\mathfrak{b}$ que precedem x.

*

Um exemplo de ordinal: Se $x < y$, em $\mathfrak{b}$, então $\mathfrak{b}_x \in \mathfrak{b}_y$ e reciprocamente. Os ideais de $\mathfrak{b}$ formam um conjunto bem ordenado para a relação $\in$. O *ideal vazio* é o seu primeiro elemento, e, dado que $\mathfrak{b}$ verifica a definição de ideal, o *ideal impróprio* $\mathfrak{b}$ é o último elemento.

*

Consideremos agora um conjunto $\mathfrak{L} \neq \emptyset$ qualquer. Dado um subconjunto próprio A, de $\mathfrak{L}$, tomemos $\mathfrak{L} - A$ e associemos a cada um dêstes últimos subconjuntos (não vazios), de harmonia com o axioma de Zermelo, um elemento $f(\mathfrak{L} - A) \in \mathfrak{L} - A$. Define-se assim uma correspondência $A \to \eta(A)$, tomando $\eta(A) = f(\mathfrak{L} - A)$.

Um subconjunto $\mathfrak{L}$, de $\mathfrak{L}$, diz-se uma *cadeia-H*, se satisfaz às duas condições seguintes: 1) $\mathfrak{L}$ é um conjunto bem ordenado, para uma eventual relação de ordem introduzida em $\mathfrak{L}$; 2) para cada $x \in \mathfrak{L}$, tem-se $x = \eta(\mathfrak{L}_x)$. Em particular, para primeiro elemento, tem-se $c_0 = \eta(\mathfrak{b}_{c_0}) = \eta(\Phi) = f(\mathfrak{L})$. Vamos demonstrar dois teoremas sôbre estas cadeias-H, a partir dos quais será

depois simples chegar à boa ordenação.

*

Teorema 1:- Se L e M são duas cadeias-H, uma delas é um ideal de outra. Partamos de L e M, supostas não vazias. Tomando um ideal B não vazio de L, suponhamos que todos os ideais próprios de B são ideais de M. Vamos vêr que, então, ou M é um ideal de L, ou B é um ideal de M. Se B não tem último elemento, para cada $b \in B$, existe x tal que $b < x$. Cada elemento de B pertencerá a um ideal próprio de B: $b \in B_x$. Mas, como $\cup B_x = B$, vê-se que B como união dos B_x, que são ideais de M é um ideal de M. Se B tem último elemento t, ter-se $B = \{B', t\}$, onde $B' = B - \{t\}$. B' é um ideal próprio de B, portanto um ideal de M. Pode acontecer que se tenha $M = B'$, e, então, M é um ideal de L; mas, se $M \neq B'$, pode dar-se a M a forma $M = \{B', w, \ldots\}$, onde w é o primeiro elemento de M que não pertence a B'. Como L é uma cadeia-H, as igualdades $\eta(L_t) = \eta(B') = t$ são válidas; e, como M é igualmente uma cadeia-H, tem-se também $\eta(M_w) = \eta(B') = w$. Conclui-se $t = w$, portanto $M = \{B', t, \ldots\}$, o que mostra que B é um ideal de M. Temos assim demonstrado o que desejavamos. Regressando ao teorema propriamente dito, se L não é um ideal de M, há, entre os ideais de L, um primeiro ideal B, não vazio, que não é um ideal de M. Todos os ideais próprios de B são ideais de M, e, assim, conforme os raciocínios feitos, o único caso em que B não é ideal de M é aquele em que M é ideal de L. O teorema está demonstrado.

*

Observação:- Tomando o conjunto vazio como uma cadeia-H, a hipótese de uma das cadeias ser vazia implica que ela seja um ideal da outra (próprio ou impróprio). Foi por isto que raciocinámos supondo L, B, M não vazios.

*

Exercício:- A existência de cadeias-H não vazias, se L não é vazio, não é difícil de provar. Vimo já que, uma vez fixada a função de escolha f, o primeiro elemento de qualquer cadeia-H é $c_0 = \eta(\phi) = f(L)$. A partir daqui constroem-se cadeias-H com dois, tres, etc. elementos. Uma qualquer destas cadeias é um ideal de toda a cadeia-H que a contém.

*

Teorema 2:- O conjunto união das cadeias-H é uma cadeia-H. Representemos por $U = \cup L_\alpha$ a união das cadeias-H. O índice α serve para as distinguir: $L_\alpha \neq L_\beta$, se $\alpha \neq \beta$. Se não há em jôgo duas cadeias-H, podemos representar uma cadeia-H simplesmente por L. Para vermos que U é ordenada, tomemos $x, y \in U$ e suponhamos $x \in L_\alpha$, $y \in L_\beta$. Se L_α, por exemplo, é um ideal de L_β, ter-se-á, em L_β, $x < y$ ou $y < x$, se $x \neq y$. Esta mesma relação de ordem subsiste, se x e y pertencem a outras cadeias-H, diferentes daquelas. Para se provar que U é bem ordenado, resta vêr que todo o subconjunto não vazio F, de U, tem primeiro elemento. Se se tem $f \in F$, será $f \in L_\alpha$. A intersecção $F \cap L_\alpha$ não é vazia e tem um primeiro elemento, visto estar contida em L_α. Seja t_0 êsse primeiro

elemento. Se se torna agora $f_1 \in F$, ou é $f_1 \in L_\alpha$ e, então, $f_1 \in L \cap F_\alpha$, assim como $f_0 \leq f_1$; ou $f_1 \notin L_\alpha$ e, então, $f_1 \in L_\beta$. Nesta hipótese, L_α é um ideal de L_β, portanto $f_0 < f_1$. U é, de facto, bem ordenado. Para acabar a demonstração, precisamos de ver que, para cada $x \in U$, é $x = \eta(U_x)$. Se $x \in U$, é $x \in L_\alpha$; para cada $y \in U$, se $y \notin L_\alpha$, temos $y \in L_\beta$, de sorte que L_α é ideal de L_β e $x < y$. Resulta daqui que, tomando $x \in U$, se $x \in L$, ter-se-á $t \in L$, para cada $t \in U$ tal que $t \leq x$. Isto quer dizer que L é um ideal de U. Ter-se-á $L_x = U_x$, $\eta(U_x) = \eta(L_x) = x$, como se desejava.

*

Estamos agora em condições de estabelecer fàcilmente o Teorema da boa ordenação, o qual, pelos raciocínios anteriores é bem uma consequência do axioma de Zermelo.

*

Teorema 3:- Todo o conjunto L admite uma boa ordenação. A cadeia-H, que, no teorema precedente designámos por U contém todos os elementos do conjunto L, como vamos ver. Se fôsse $U \neq L$, o conjunto $L - U$ não seria vazio e $\eta(U) = f(L-U) = v$. Ora o conjunto $L = \{U, v\}$, no qual v é considerado último elemento, é um conjunto bem ordenado, mantendo a ordenação obtida para U. Mas, o mesmo conjunto é uma cadeia-H, visto que, pondo $x = v$, tem-se $L_x = L_v = U$ e $\eta(L_v) = \eta(U) = v$, e, sendo $x \in U$ qualquer, tem-se igualmente $\eta(L_x) = x$. O absurdo de havermos encontrado uma cadeia-H maior que U resulta de havermos suposto $U \neq L$.

*

Exercício:- Concluir o axioma de Zermelo da hipótese da boa ordenação.

*

Dentro do esquema proposto no começo dêste número, vamos provar êste

*

Teorema 4:- A boa ordenação implica a condição de Kuratowski-Tomemos um conjunto parcialmente ordenado M e uma cadeia C, de M. Para a boa ordenação de M, obtem-se um conjunto bem ordenado L, no qual a relação de ordem será designada por $<$. O sinal $\leq$ será reservado para a relação de ordem parcial dada sobre M e que subsiste em C. Consideremos então o conjunto $\{1, 2\}$. Dado $a \in M$, poremos $\psi(a) = 1$, se as duas hipóteses seguintes são verificadas: i) todo o $b < a$ para o qual $\psi(b) = 1$ é comparável com a, no sentido, é claro, que se tem $b \leq a$, ou $a \leq b$; ii) para o próprio a, tomando $c \in C$, ou é $c \leq a$ ou $a \leq c$, qualquer que seja c. Se a não satisfaz estas duas condições, então $\psi(a) = 2$.

Vê-se fàcilmente que o conjunto M, dos elementos a para os quais $\psi(a) = 1$, forma uma cadeia maximal que contém C. Com efeito: se $c_0 \in C$, tem-se $\psi(c_0) = 1$, porque a condição ii) é verificada, e a condição i) também o é, visto que, supondo $b < c_0$ e $\psi(b) = 1$, a hipótese $\psi(b) = 1$ implica imediatamente $b \leq c$ ou $c \leq b$, quando $c \in C$, e esta implicação é realizada em particular tomando $c = c_0$; por outro lado, se a e a' são dois elementos de M para os quais $\psi(a) = 1$,

$\psi(a')=1$, suponhamos que, para a boa ordenação se tem $a'<a$; então, em virtude da condição i), ou $a'\supseteq a$ ou $a\supseteq a'$. O conjunto $\underline{M}$ forma uma cadeia. A cadeia é maximal porque, se existisse uma cadeia maior que $\underline{M}$, existiria uma cadeia $\underline{N}$, maior do que $\underline{C}$, composta de $\underline{M}$ e de um elemento $d\notin M$. O elemento $\underline{d}$ satisfaria a condição ii). Tomando, em seguida, $b<d$, com $\psi(b)=1$, pelo facto de $\underline{b}$ e $\underline{d}$ pertencerem à mesma cadeia $\underline{N}$, concluíamos $b\supseteq d$ ou $d\supseteq b$, pelo que seria $\psi(d)=1$, em contradição com a hipótese de $\underline{d}$ não pertencer a $\underline{M}$. O teorema está demonstrado.

*

Para acabarmos o nosso objectivo, resta provar êste

*

Teorema 5:- A condições de Kuratowski implica o axioma de Zermelo.

Dado o conjunto $\mathcal{L}\neq\phi$, consideremos as funções (unívocas) θ, ψ, ω, ... que podem ser definidas pelas condições $\theta(A)\in A$, $\psi(A)\in A$, etc, para alguns dos subconjuntos de $\mathcal{L}$. Tomando duas destas funções θ e ψ, escreveremos $\theta\supseteq\psi$, sempre que se tome um conjunto $S\subseteq\mathcal{L}$, para o qual $\theta(S)$ existe, e se tenha então $\psi(S)=\theta(S)$. ψ será eventualmente definida para certos subconjuntos para os quais θ não existe. No conjunto parcialmente ordenado formado pelas funções em questão, tomemos uma cadeia maximal C_θ. Esta cadeia permite a construção de uma função unívoca φ, extensão de todas as funções de cadeia, desde que se ponha $\varphi(A)=\theta(A)$,

de cada vez que haja uma função θ da cadeia para a qual $\theta(A)$ existe. A função φ é a função desejada, porque ela está definida para todos os subconjuntos não vazios de $\mathcal{L}$, como vamos vêr. Se T_0 fôsse um subconjunto para o qual φ não existisse, então a função $\bar\varphi$ tal que $\bar\varphi(A)=\varphi(A)$, quando φ existe, e $\bar\varphi(T_0)=t_0\in T_0$, onde t_0 é escolhido arbitrariamente em T_0, seria uma função que, junta às funções de cadeia C_θ, permitia a construção de uma cadeia maior que C_θ. O teorema está demonstrado.

***

6. O princípio de Zorn - Sob a designação de princípio de máximo, entende-se o enunciado seguinte: se, num conjunto parcialmente ordenado $\mathcal{M}$, não vazio, toda a cadeia não vazia $\underline{C}$ admite um majorante $v(C)$, então $\mathcal{M}$ contém elemento maximal.

Vamos verificar que o princípio de máximo é equivalente à condição de Kuratowski, e, portanto, ao axioma de Zermelo. Nas aplicações à Matemática, o princípio de máximo revela-se particularmente útil e de emprêgo relativamente fácil.

*

Teorema 1:- A condição de Kuratowski e o princípio de máximo são equivalentes. Admitamos a condição de Kuratowski. Tomado $\mathcal{M}$ não vazio, seja C_θ uma cadeia maximal e designemos por $v(C_\theta)$ um majo-

rante de C_θ. Então, $v(C_\theta)$ é um elemento maximal, visto que a existência de a tal que $v(C_\theta) < a \in M$ permitiria a construção de uma cadeia maior do que C_θ. Reciprocamente, admitamos o princípio de maximo. Então, dada uma cadeia C, de M, consideremos a família $\{C_\alpha\}_{\alpha \in \Delta}$ das cadeias de M que contêm C. A família Δ constitui um conjunto parcialmente ordenado. Se se considerar uma cadeia $\mathcal{C}$ formada por elementos $C_\beta \in \Delta$, o conjunto $\bigcup C_\beta$, formado pelos elementos dos diferentes C_β constitui um elemento da família Δ, que é um majorante $v(\mathcal{C})$. Há em Δ um elemento maximal.

*

Se, na demonstração anterior, se substituir majorante $v(\mathcal{C})$ por supremo $\sup(\mathcal{C})$, os raciocínios subsistem. Vale, por isso, o

*

Teorema 2: - Se, num conjunto parcialmente ordenado, toda a cadeia tiver supremo, há no conjunto elemento maximal. Este enunciado constitui o princípio de Zorn. O seu uso revela-se com frequência muito vantajoso em face do axioma de Zermelo.

Dá-se o nome de conjunto indutivo a todo o conjunto parcialmente ordenado em que qualquer cadeia tem supremo.

* * *

7. Aplicações - À existência de conjuntos bem ordenados, liga-se, de modo semelhante ao que foi feito na Teoria dos números naturais, um segundo princípio de indução transfinita, que pode enunciar-se assim:

Um conjunto b_0, subconjunto dum conjunto bem ordenado b, que, se contém todos os elementos $b \in b$ para os quais $b < b_0$, contém b_0, coincide com b. Nas aplicações, ainda de modo semelhante ao que acontece na Teoria dos números naturais, o segundo princípio de indução transfinita pode ser substituído pelo seguinte princípio de indução transfinita: Dados o conjunto bem ordenado b e o subconjunto b_0, ter-se-á $b_0 = b$, se b_0 contiver o primeiro elemento de b, e se, além disto, contendo b_0, contém o seu sucessor, e, contendo os elementos que precedem um número limite, contém esse número limite.

*

Deixamos ao leitor os seguintes

*

Exercícios: - I) Demonstre o segundo princípio de indução transfinita e bem assim o princípio de indução transfinita.

II) Dados dois ordinais b e b', um deles é isomorfo dum ideal do outro. [Nota: Uma aplicação bijectiva $b \xrightarrow{\theta} b'$ de b sobre b' diz-se um isomorfismo se respeita a ordenação: $b_1 \to \theta(b_1) = b'_1$, $b_2 \to \theta(b_2) = b'_2$ são tais que $b'_1 < b'_2$, se $b_1 < b_2$].

III) Mostrar que o problema da tricotomia também se resolve pela positiva, no caso dos cardinais transfinitos.

IV) De todo o conjunto infinito é possível extrair um conjunto numerável infinito, o que permite se diga que o infinito numerável é o menor

dos cardinais infinitos.

V) O ordinal $\underline{\omega}$ do infinito numerável é o mais pequeno dos ordinais infinitos. É um ordinal limite.

***

8. Aritmética dos cardinais – As operações com os números cardinais ou a aritmética dos cardinais é muito simples. Dados dois conjuntos disjuntos $\underline{A}$ e $\underline{B}$, de cardinais $\underline{\alpha}$ e $\underline{\beta}$, respectivamente, chama-se soma $\alpha+\beta$ o número cardinal de $A \cup B$ (ou, bem entendido, de qualquer outro conjunto que lhe seja equipotente). O produto $\alpha\beta$ é o número cardinal do produto cartesiano $A \times B$. Vê-se que $\alpha+\beta=\beta+\alpha$, $\alpha\beta=\beta\alpha$, $\alpha \leq \alpha+\beta$, $\alpha \leq \alpha\beta$. Nesta última relação supõe-se que β não é o cardinal do vazio.

* Exercícios:- I) Mostrar que são válidas as igualdades $\alpha_1+(\alpha_2+\alpha_3)=(\alpha_1+\alpha_2)+\alpha_3$, $\alpha_1(\alpha_2\alpha_3)=(\alpha_1\alpha_2)\alpha_3$, $\alpha_1(\alpha_2+\alpha_3)=\alpha_1\alpha_2+\alpha_1\alpha_3$.

II) Mostrar que $\alpha_1 \leq \beta_1$, $\alpha_2 \leq \beta_2$ implicam $\alpha_1+\alpha_2 \leq \beta_1+\beta_2$, $\alpha_1\alpha_2 \leq \beta_1\beta_2$, o mesmo acontecendo se se tiverem duas famílias $\{\alpha_i\}$ e $\{\beta_i\}$ de cardinais, desde que $\alpha_i \leq \beta_i$.

*

O problema da exponenciação liga-se ao problema do produto cartesiano de conjuntos. Dada uma família $\{C_a\}$, $(a \in \Sigma)$, diz-se produto cartesiano dos C_a e representa-se por $\prod_{a \in \Sigma} C_a$ o conjunto dos elementos de forma $(c_a, c_b, \ldots)$, com $c_a \in C_a$, $c_b \in C_b$, etc..

*

Regressando à exponenciação de cardinais, começemos por supôr que os cardinais em jôgo são diferentes do cardinal do vazio. Então, tomemos $\underline{A}$ e $\underline{B}$, de cardinais respectivos $\underline{\alpha}$ e $\underline{\beta}$; o número cardinal de $\prod_{j \in B} C_j$, $(C_j=A)$, será α^β. Vê-se que são válidas as igualdades seguintes:

$$\alpha^\beta \cdot \alpha^\gamma = \alpha^{\beta+\gamma}; \quad (\alpha\beta)^\gamma = \alpha^\gamma \cdot \beta^\gamma; \quad (\alpha^\beta)^\gamma = \alpha^{\beta\gamma}; \quad \alpha^1=\alpha; \quad 1^\alpha = 1.$$

Dá-se validade em geral a todos os casos das igualdades anteriores, se α^β fôr interpretado como A^B, isto é, como o conjunto de todas as aplicações de $\underline{B}$ em $\underline{A}$. Por exemplo, $\alpha=0$, $\beta=0$ dão $0^0=1$; $\alpha \neq 0$, $\beta=0$ dão $\alpha^0=1$. Quanto a $\alpha=0$, $\beta \neq 0$, poremos $0^\beta=0$.

*

O teorema de que passamos a ocupar-nos é muito importante, porque simplifica enormemente a aritmética dos cardinais.

*

Teorema 1:- Supondo α e β dois cardinais tais que $\alpha \neq 0$, β infinito $\alpha \leq \beta$, então $\alpha+\beta=\alpha\beta=\beta$. A demonstração apoia-se sobre dois lemas.

*

Lema 1 :- A igualdade $\aleph_0^2 = \aleph_0$ é válida. Admitamos que $\aleph_0$ se encontra realizado pelo conjunto N dos números naturais e consideremos o produto cartesiano $N \times N$, cujos elementos dispomos do modo seguinte:

$$(1,1);\ (1,2);\ (1,3);\ \ldots;\ (1,n);\ \ldots$$

$$(2,1);\ (2,2);\ (2,3);\ \ldots;\ (2,n);\ \ldots$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$(m,1);\ (m,2);\ (m,3);\ \ldots;\ (m,n);\ \ldots$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

O processo de diagonalização que consiste em escrever estes elementos em correspondência biunívoca com os elementos de $\mathbb{N}$, conforme o esquema:

$1 \to (1,1)$; $2 \to (1,2)$; $3 \to (2,1)$; $4 \to (1,3)$; $5 \to (2,2)$; $6 \to (3,1)$; etc.,

mostra que, com efeito, o número cardinal de $\mathbb{N} \times \mathbb{N}$ é $\aleph_0^2 = \aleph_0$.

*

Lema 2 (Hessenberg): — Se α é um número cardinal infinito, tem-se $\alpha^2 = \alpha$.

Realizemos α pelo conjunto A. Em seguida, suponhamos N um conjunto que realiza o infinito numerável, mas suposto contido em A: $N \subseteq A$. Quanto a $\mathbb{N}$, sabemos que existe uma aplicação bijectiva $\varphi_0 : N \to N \times N$. Consideremos então os subconjuntos B tais que $N \subseteq B \subseteq A$ e para os quais é possível uma aplicação bijectiva $B \xrightarrow{\varphi} B \times B$ que seja um prolongamento de φ_0. Obtemos assim um conjunto

$$\Delta = \{(N, \varphi_0); (B, \varphi); \dots\},$$

no qual se introduz uma relação de ordem parcial, pondo $(B, \varphi) \leq (B', \varphi')$ se $B \subseteq B'$ e φ' prolonga φ. Se se toma agora uma cadeia de Δ cujos elementos sejam (B_j, φ_j), $(j \in J)$, vê-se que $(\bigcup B_j, \Phi)$, com $\Phi(x) = \varphi_j(x)$, se x é um ponto para o qual haja um φ_j definido, é o limite superior da cadeia no conjunto parcialmente ordenado Δ. Seja, então, (C, Ψ) um elemento maximal de Δ. O número cardinal γ, de C, verifica a condição $\gamma^2 = \gamma$. Se demonstrarmos que se tem $\gamma = \alpha$, o lema ficará provado. Se pudesse ter-se $\gamma \neq \alpha$, ter-se-ia $\gamma < \alpha$, pois que $C \subseteq A$. Vamos chegar a um absurdo

com a hipótese $\gamma < \alpha$. Nesta hipótese, ponha-se $A - C = D$, ou $A = C \cup D$; então, ter-se-á $\alpha = \gamma + \delta$, onde δ é o número cardinal de D, visto que C e D são disjuntos. Mas não pode ter-se $\delta \geq \gamma$, visto que, se assim fôsse, as relações $\alpha \geq \gamma + \gamma = 2\gamma \geq \gamma^2 = \gamma$ seriam válidas, contradizendo $\gamma < \alpha$. Portanto, de $\gamma < \alpha$, conclui-se $\gamma < \delta$. Existe $E \subset D$ de número cardinal γ. E tem-se $C \sim E \subset D = A - C$, $F = C \cup E$, $F \subseteq A$, onde C e E são conjuntos disjuntos. Justamente, provaremos a existência de uma aplicação bijectiva f, de F sobre $F \times F$, que prolonga Ψ e que leva, pois, ao absurdo desejado. De facto, $F \times F = (C \cup E) \times (C \cup E) = (C \times C) \cup (C \times E) \cup (E \times C) \cup (E \times E)$, sendo disjuntos os últimos conjuntos. Utilizando o símbolo $\operatorname{card}(X)$ para representar o número cardinal de X, vê-se que

$$\operatorname{card}(F \times F) = \operatorname{card}(C \times C) + \operatorname{card}[(C \times E) \cup (E \times C) \cup (E \times E)].$$

O último número cardinal, tendo em conta a equipotência de C e E, tem o valor $\gamma^2 + \gamma^2 + \gamma^2 = 3\gamma \geq \gamma^2 = \gamma$, o que dá $3\gamma = \gamma$. Existe uma aplicação bijectiva g, de E sobre o conjunto entre parênteses rectos. Existe em seguida uma aplicação bijectiva f, de F sobre $F \times F$, definida do modo seguinte: se $x \in C$, então $f(x) = \Psi(x) \in C \times C$; se $x \in E$, então $f(x) = g(x) \in (C \times E) \cup (E \times C) \cup (E \times E)$. A igualdade desejada $\gamma = \alpha$ fica pois completamente provada.

* Regressemos ao teorema. Por um lado, se $\alpha \leq \beta$, tem-se $\alpha + \beta \leq \beta + \beta = 2\beta \leq \beta^2 = \beta$; por outro lado, visto que $\beta \leq \alpha + \beta$, tem-se $\alpha + \beta = \beta$. De modo análogo; de um lado, $\alpha\beta \leq \beta^2 = \beta$, por outro, se $\alpha \neq 0$, tem-se também $\beta \leq \alpha\beta$, portanto $\alpha\beta = \beta$.

* Corolário 1:- Os subconjuntos finitos dum conjunto de número cardinal $\alpha \geq \aleph_0$ formam um conjunto cujo número cardinal é α. De facto, o número cardinal do conjunto dos subconjuntos contendo um só elemento é $\leq \alpha$; o do conjunto dos subconjuntos contendo dois elementos é também $\leq \alpha$ por estar compreendido entre $\alpha^2 = \alpha$ e $\leq \alpha$. Em seguida, o cardinal do conjunto dos subconjuntos contendo 3 elementos, igualmente compreendido entre α e $\leq \alpha^2$, é de novo $\leq \alpha$, etc.. O número cardinal β que se deseja é o do conjunto $B = \bigcup A_j$, $(j \in \aleph)$, onde cada A_j (correspondente a j) tem o cardinal $\leq \alpha$. Se se toma um elemento $b \in B$, suponde $b = a \in A_j$, vê-se que estes elementos b estão em correspondência biunívoca com os elementos (j, a). Tem-se $\beta \leq \aleph_0 \alpha = \alpha$.

* Exercícios:- I') Se γ e γ', conforme a hipótese do contínuo, são cardinais transfinitos consecutivos, tem-se $\gamma^\gamma = \gamma'$.

II') Dados dois cardinais transfinitos γ_0 e γ, com $\gamma_0 < \gamma$, tem-se $\gamma' = \gamma_0^\gamma$.

* Observações finais sobre o Capítulo - Muitas das questões de que nos ocupámos neste Capítulo não tiveram o tratamento que mereciam. O leitor é convidado a servir-se do livro de A. Almeida Costa, "Cours d'Algèbre générale I", Lisboa, Fundação Gulbenkian, assim como do livro de J. Santos Guerreiro, "Curso de Matemáticas gerais", I volume, Lisboa, Escolar Editora, para completar o estudo de algumas das referidas questões. Diga-se, todavia, que a exposição aqui feita é julgada suficientemente coerente.

BIBLIOGRAFIA

G. Birkhoff: [1] - Lattice theory, New York, 1948.

N. Bourbaki: [1] - Théorie des ensembles (fascicule de résultats"), Paris, 1951; [2] - Théorie des ensembles, Chap. I e II, Paris, 1954.

P. M. Cohn: [1] - Universal algebra, Londres, 1965.

A. Fraenkel: [1] - Einleitung in die Mengenlehre, New York, 1945.

B. van der Waerden: [1] - Moderne Algebra I, Berlin, 1930.

Capítulo II

Semigrupos. Números inteiros

§ 1. Semigrupos

***

1. Algebrização de conjuntos - Tomado um conjunto $\mathcal{L}$ não vazio, consideremos o produto cartesiano $\mathcal{L}\times\mathcal{L}$ e uma aplicação dêste produto no conjunto $\mathcal{L}$. A cada par ordenado $(a,b)\in\mathcal{L}\times\mathcal{L}$ faz-se corresponder, de modo unívoco, um elemento $c\in\mathcal{L}$. Escreveremos $a.b=c$ ou $ab=c$, para significar a aplicação em causa e diremos, tal como se fez em $(\mathbb{Z},2,1)$, que se definiu sobre o suporte $\mathcal{L}$ uma operação binária.

Podemos definir igualmente operações unárias, cada uma delas aplicando um conjunto $\mathcal{U}$ em $\mathcal{U}$, ou, até, operação de ordem zero, cada uma delas aplicando o conjunto vazio num elemento de $\mathcal{U}$ (que é, assim, um elemento fixo definindo a operação).

Um conjunto dotado de operações diz-se um espaço algébrico. Com o simbolismo $\mathcal{T}=(\mathcal{L}/\cdot)$ significaremos que $\mathcal{T}$ é um grupóide sobre o suporte $\mathcal{L}$, dotado da operação $(\cdot)$. O final desta operação pode ser diferente, desde que se ponham em causa vários grupóides, como por exemplo: $(\mathcal{U}/\circ)$, $(\mathcal{U}/*)$, etc..

Tomemos $\mathcal{T}=(\mathcal{L}/\cdot)$. Diz-se que $\underline{e}$ é uma identidade à esquerda, ou um elemento neutro à esquerda, se $e.a=a$, $\forall a\in\mathcal{T}$. Uma identidade à direita, ou um elemento neutro à direita, que designaremos excepcionalmente pela letra grega $\underline{\varepsilon}$, é um elemento tal que $a\varepsilon=a$, $\forall a\in\mathcal{T}$. Uma identidade bilateral, ou elemento neutro, ou elemento um, ou identidade, é um elemento $\underline{u}$ que verifica as igualdades $ua=au=a$, $\forall a\in\mathcal{T}$. Se $\underline{e}$ e $\underline{\varepsilon}$ existem, então $e.\varepsilon=\varepsilon=e$ e resulta que as duas identidades unilaterais são iguais. Temos $e=\varepsilon=u$.

Um grupóide é finito ou infinito, conforme fôr finito ou infinito o número dos seus elementos. Em todos os casos, o número cardinal do suporte é chamado a ordem do grupóide. Estas noções estendem-se naturalmente a um sistema algébrico qualquer.

Fixemos $a\in\mathcal{T}$ e seja $\underline{x}$ um elemento qualquer de $\mathcal{T}$. O facto de ser xa um elemento variável, bem determinado para cada x, mostra que, pondo $y=xa$ se define, por via de $\underline{a}$, uma aplicação $A_a^{(d)}$ de $\mathcal{L}$ em $\mathcal{L}$, segundo o esquema

$$x\longrightarrow xa=y=xA_a^{(d)}.$$

A notação $A_a^{(d)}$ lembra: i) por intermédio da letra $\underline{A}$ que se trata de uma aplicação; ii) por intermédio da letra $\underline{a}$, que tal aplicação é definida pelo elemento $\underline{a}$; iii) por intermédio da letra $\underline{d}$, que o elemento $\underline{a}$ é multiplicador,

à direita, dos elementos de $\mathcal{G}$. De modo análogo se tem uma aplicação

$$x \to a x = y = z\, A_a^{(e)},$$

onde agora o índice superior e, em $A_a^{(e)}$, lembra que a é multiplicador à esquerda. Observe-se, de resto, que $x A_a^{(a)} = a A_x^{(e)}$. Quando $A_a^{(a)}$ é uma permutação de $\mathcal{I}$ $(I, 1, 3)$, diz-se que a é um elemento não singular à direita; se $A_a^{(e)}$ é uma permutação de $\mathcal{I}$, então a é um elemento não singular à esquerda. Um elemento diz-se não singular, se é não singular tanto à direita como à esquerda.

*

Exemplo:- Uma identidade à esquerda (à direita) é um elemento não singular à esquerda (à direita). Define a transformação identidade.

*

Exemplos de grupoides:- I) Na tabela junta, chamada tabela de Cayley, define-se um grupoide ordem três:

	e	a	b
e	e	a	b
a	b	a	b
b	b	a	a

Nesta tabela, como aliás em qualquer tabela análoga, encontra-se o produto xy de dois elementos, procurando x sobre a linha vertical que precede o traço vertical e procurando y sobre a linha horizontal que precede o traço horizontal; então encontra-se o produto xy na intersecção da uma linha horizontal que passa por x com a linha vertical que passa por y. Neste exemplo, e é uma identidade esquerda.

II) Tomemos $\mathcal{I}$ e o conjunto $\mathcal{P}(\mathcal{I})$ das suas partes. Se $A, B \in \mathcal{P}(\mathcal{I})$, define-se um produto $A \cdot B$, pondo $A \cdot B = A \cap B$. O elemento $\mathcal{I}$ é então a identidade.

III) Façamos, em $\mathcal{P}(\mathcal{I})$, $A \cdot B = A \cup B$. O elemento ϕ é a identidade.

IV) O conjunto das aplicações dum conjunto em si, com a regra de produto dada em $(I, 3, 1)$, forma um grupoide. Uma parte destas aplicações é constituída pelas permutações. Entre estas últimas, a permutação identidade é o elemento um do grupoide.

*

Tomemos um grupoide $\mathcal{G} = (\mathcal{I}, \cdot)$. Se A e B são dois subconjuntos de $\mathcal{I}$, define-se um produto AB como o conjunto $\{ab, \ldots\}$ formado pelos produtos ab, $\forall a \in A$, $\forall b \in B$. Dizer que $AB = BA$, significa:

$\forall a \in A$ e $\forall b \in B$, $\exists\, b' \in B$ e $a' \in A$ tais que $ab = b'a'$;

$\forall \bar{b} \in B$ e $\forall \bar{a} \in A$, $\exists\, \bar{b}' \in B$ e $\bar{a}' \in A$ tais que $\bar{b}\bar{a} = \bar{a}'\bar{b}'$.

Suponhamos, em particular, que se tem $AA \subseteq A$ para um certo $A \subseteq \mathcal{I}$. Neste caso A toma naturalmente o nome de subgrupoide de $\mathcal{G}$. Um subgrupoide é próprio, se for diferente do grupoide, de contrário diz-se impróprio. Um ideal à esquerda dum grupoide é um subconjunto E com a propriedade $\mathcal{G}E \subseteq E$; um ideal à direita D é caracterizado pela inclusão $D\mathcal{G} \subseteq D$; e um ideal bilateral (ou ideal) é um subconjunto que é ao mesmo tempo ideal à esquerda e à direita.

*

Um grupoide diz-se abeliano se o produto é comutativo. Neste caso não há distinção entre os diferentes tipos de ideais.

*

Exemplos: I') No grupoide multiplicativo dos números naturais, um conjunto da forma $\{m\}\mathcal{N}$, ou $m\mathcal{N}$, onde m é fixo, é um ideal.

II') No grupoide do exemplo II), o conjunto $A\,\mathcal{P}(L) = \{A\}\mathcal{P}(L)$ é um ideal

III') No grupoide do exemplo I), $\{a,b\}$ é um ideal e $\{a\}$ é um ideal esquerdo.

***

2. Grupoides de elementos não singulares – Se todos os elementos dum grupoide $\mathcal{G}$ são não singulares, as aplicações $A_a^{(d)}$ e $A_a^{(e)}$ são permutações $T_a^{(d)}$ e $T_a^{(e)}$, respectivamente. Um tal grupoide diz-se um quase-grupo; e, se existe elemento identidade, diz-se um loop.

*

Exercício: - Um quase-grupo pode definir-se dizendo: trata-se dum conjunto com uma operação binária de produto, tal que é possível determinar de modo unívoco o terceiro elemento de uma igualdade $a.b=c$, desde que os outros dois sejam conhecidos.

***

3. Primeiras propriedades dos semigrupos – Quando a operação binária dum grupoide $\mathcal{G}$ é associativa, o grupoide diz-se um semigrupo: $a(bc) = (ab)c$.

Uma parte A dum semigrupo para a qual $AA \subseteq A$ é um semigrupo que se designa por subsemigrupo.

Quando existe identidade o semigrupo recebe o nome de monoide. E, se existe um elemento 0 tal que $0.a = a.0 = 0$, $\forall a \in \mathcal{G}$, êste elemento será único e toma o nome de zero. Quando o produto de dois elementos diferentes de zero é diferente de zero, o zero diz-se trivial.

*

Exemplos: - I) O conjunto dos números naturais, tomando a soma como operação, constitui um semigrupo abeliano.

II) O conjunto dos números naturais iguais ou superiores a um número natural dado, tomando o produto como operação, é um semigrupo abeliano O conjunto $\mathcal{N}$ é um monoide.

III) O conjunto dos números cardinais, finitos ou transfinitos, iguais ou inferiores a um cardinal transfinito, tanto para a soma como para o produto de cardinais, constitui um semigrupo. No caso do produto existe um zero trivial.

IV) O conjunto $\mathcal{P}(L)$, tanto para a operação $\cap$ como para a operação $\cup$ é um monoide abeliano. Em ambos os casos existe elemento zero, não trivial no 1.º e trivial no 2.º

V) O conjunto das aplicações dum conjunto em si, com a operação de produto, forma um monoide, em geral não abeliano.

VI) Sobre qualquer conjunto $\mathcal{L}$ definem-se dois semigrupos triviais, definidos pela operação de produto $x.y=y$ [ou $x.y=x$].

*

O subsemigrupo gerado por um subconjunto $\{a, \dots, b, \dots, c, \dots, t, \dots\}$ de elementos de $\mathcal{T}$ é o mais pequeno subsemigrupo que contém aqueles elementos. Trata-se do conjunto de elementos da forma $cd\dots f$, cada um deles contendo um número finito de "factores" pertencentes ao subconjunto dado.

*

Certas relações que vamos dar e que resultam da propriedade associativa são de grande importância. Do facto de se ter $a(bc)=(ab)c$, conclui-se que pode escrever-se mais simplesmente abc, para representar o valor comum dos dois membros da igualdade. Duma maneira geral, vamos verificar que se pode interpretar o símbolo $a_1 a_2 \dots a_n$ como o produto de n elementos, pela simples razão de que todas as interpretações possíveis do mesmo símbolo levam a um mesmo resultado. Sabemos que é assim para o símbolo $a_1 a_2 a_3$. Admitamos, em seguida, que se interprete o símbolo $a_1 a_2 \dots a_n$ pela relação de indução seguinte: $a_1 a_2 \dots a_{n-1} a_n = (a_1 a_2 \dots a_{n-1}) a_n$. Mostraremos que, supondo $A = a_1 \dots a_n$, $B = a_{n+1} \dots a_p$, $(p \geq n+1)$, se tem com efeito

$$AB = a_1 \dots a_p. \qquad (1)$$

Se $p = n+1$, isto é, se $B = a_{n+1}$, tem-se $AB = (a_1 \dots a_n) a_{n+1} = a_1 \dots a_p$. Admitamos agora que a igualdade (1) está demonstrada para $p = n+k-1$, $(k \geq 2)$; prová-la-emos para $p = n+k$. Ponhamos $B' = a_{n+1} \dots a_{n+k-1}$. Tem-se

$AB' = a_1 a_2 \dots a_{n+k-1}$, por hipótese. Escrevendo em seguida $AB'.a_{n+k} = A.B'a_{n+k}$ em virtude de ser $B'a_{n+k} = a_{n+1} \dots a_{n+k-1} a_{n+k} = B$, vê-se que $AB'.a_{n+k} = AB$. Por outro lado, $AB'.a_{n+k} = a_1 \dots a_{n+k}$, donde o resultado que queríamos estabelecer.

Quando todos os factores dum produto são iguais a um elemento a, poremos $a_1 \dots a_n = a^n$. Desta definição tira-se

$$a^m . a^n = a^{m+n}, \quad (a^m)^n = a^{mn},$$

igualdades que se demonstram por indução.

*

Exercícios: - I') O conjunto dos elementos $z \in \mathcal{T}$ tais que $za = az$, $\forall a \in \mathcal{T}$, diz-se centro de $\mathcal{T}$. O centro é um semigrupo, que pode ser vazio.

II') Num sistema algébrico com uma operação binária $(.)$, um elemento a diz-se simplificável à direita, se toda a relação $x.a = y.a$ implicar $x = y$. Se um "subespaço" $A \subseteq \mathcal{T}$ toma o nome de parte unitária à direita do referido espaço (sistema), se possuir a propriedade seguinte: supondo $a_1, a_2 \in A$ e $x.a_1 = a_2$, com $x \in \mathcal{T}$, então $x \in A$. Mostrar que, num semigrupo, o conjunto dos elementos simplificáveis à direita forma uma parte unitária à direita que é um semigrupo.

***

4) Ideais - Os diferentes tipos de ideais definem-se para os semi-grupos do mesmo modo que se fez para os grupóides.

* Exemplos: I) No semigrupo multiplicativo dos números naturais, o conjunto dos múltiplos dum número natural é um ideal. Sucede assim, em particular, com os números pares.

II) Se $A \subseteq L$ é um elemento fixo de $\mathcal{P}(L)$ e se introduz aqui a operação $\cap$, o conjunto dos elementos de $\mathcal{P}(L)$ constituído pelos subconjuntos de L contidos em A é um ideal.

III) Substituindo no exercício precedente a operação $\cap$ pela operação $\cup$ e os subconjuntos contidos em A pelos subconjuntos que contêm A, obtém-se um ideal de $\mathcal{P}(L)$.

IV) As duas tabelas juntas representam semi-grupos:

·	A	B	C	D
A	A	A	A	A
B	A	A	A	A
C	A	A	C	C
D	A	A	C	C,

·	A	B	C	D
A	A	A	C	C
B	A	B	C	D
C	A	C	C	A
D	A	D	C	B.

Verifica-se que, na primeira tabela, $\{A\}$, $\{A,D\}$ e $\{A,C\}$ são ideais; e que, na segunda tabela, $\{A\}$ é um ideal à esquerda, mas não à direita, enquanto que $\{A,C\}$ é um ideal.

V) No semigrupo definido pela regra $\alpha.\gamma = \gamma$, um elemento constitui por si só um ideal à esquerda.

* Quando, no produto de dois subconjuntos dum semi-grupo, um dos subconjuntos contiver um só elemento a, escrevêremos aB em vez de $\{a\}B$.

* O ideal à direita gerado por a é o menor ideal que contém a. Trata-se do conjunto reunião $a \cup a\Gamma$. Do mesmo modo, o ideal à esquerda gerado por a é o conjunto reunião $a \cup \Gamma a$, e o ideal gerado por a é o conjunto reunião $a \cup a\Gamma \cup \Gamma a \cup \Gamma a \Gamma$. Também se utiliza de modo cómodo o ideal vazio.

* A totalidade dos ideais à direita (à esquerda, bilaterais) forma um semigrupo multiplicativo. Se entendermos por soma de ideais o conjunto unido dos elementos que os compõem, a totalidade dos ideais à direita (à esquerda, bilaterais) forma igualmente um semigrupo. Os diferentes semigrupos são abelianos. O ideal vazio é a identidade da soma e o próprio semigrupo Γ é a identidade.

Se, em vez da operação de soma, introduzirmos a operação $\cap$, têm-se conclusões análogas. Mas, agora, o ideal vazio é o zero e o semigrupo Γ é a identidade.

* Exercícios: I') Tomando o produto (·) como operação, há conclusões análogas às anteriores. Os respectivos semigrupos podem, todavia, não ser abelianos.

II') Mostrar que o ideal vazio de um semigrupo é um zero trivial do semigrupo dos ideais do semigrupo, quando se toma $\cap$ como operação binária.

*

Notações: Utilizaremos os símbolos seguintes: $(\ )_d$, ou, mais geralmente, $(a,b,c,\ldots)_d$ para significar ideal à direita gerado pelos elementos do interior do parêntesis; $(\ )_e$, assim como $(a,b,c,\ldots)_e$ para significar ideal à esquerda nas mesmas condições e (a), $(a,b,c,\ldots)$ para representar os ideais bilaterais gerado pelos elementos contidos nos símbolos. Assim, por exemplo:

$$(a,b,c,\ldots)_d = a\cup b\cup c\cup\ldots\cup a\gamma\cup b\gamma\cup c\gamma\cup\ldots = S,$$

$$(a,b,c,\ldots)_e = a\cup b\cup c\cup\ldots\cup\gamma a\cup\gamma b\cup\gamma c\cup\ldots = T,$$

$$(a,b,c,\ldots) = S\cup T\cup\gamma a\gamma\cup\gamma b\gamma\cup\gamma c\gamma\cup\ldots$$

*

Tomemos $e\in\Gamma$. Se se tem $e=e\cdot e=e^2$, diz-se que e é um elemento idempotente. Então, $e\Gamma$ é o ideal à direita gerado por e, $\bar{e}$ é o ideal à esquerda gerado por e e tem-se $e\Gamma e=e\Gamma\cap\bar{\Gamma}e$

***

4. Unidades - Tomemos um semigrupo com identidade u. Neste caso, podemos dar à noção de elemento não singular introduzida em $(\mathfrak{M},1,1)$ uma interpretação que vamos assinalar. Suponhamos a e a' dois elementos do semigrupo tais que $aa'=u$. Diremos, então, que a é uma unidade direita e que a' é o seu inverso direito; analogamente, a' é

uma unidade esquerda e a o seu inverso esquerdo. Designaremos por unidade, todo o elemento que seja unidade direita e esquerda. Suposto a uma unidade, de $aa'=u=a''a$, tira-se $a''(aa')=a''=(a''a)a'=ua'=a'$. Assim: quando um elemento é uma unidade, o seu inverso direito é também o seu inverso esquerdo. Diz-se que a possui inverso e representa-se êste por a^{-1}.

Quando a é uma unidade direita, a equação $ay=b$ tem, pelo menos a solução $a'b$, se a' é inverso direito de a. Não pode dizer-se que a solução seja única. No que respeita à equação $xa=b$, encontra-se uma situação inversa: se tem uma solução, ela será única, visto que $xa=x'a$ implica $(xa)a'=x=(x'a)a'=x'$.

Posto isto, analisemos as relações entre as unidades e os elementos não singulares. Se a é não singular à esquerda, $A_a^{(e)}=T_a^{(e)}$ é uma permutação e $(T_a^{(e)})^{-1}$ existe. A equação $ay=b$ tem a solução $b(T_a^{(e)})^{-1}$; em particular a equação $ay=u$ dá $y=u(T_a^{(e)})^{-1}=a'$, portanto $aa'=u$.

Um elemento não singular à esquerda é uma unidade direita. Mostraremos em seguida que é também uma unidade esquerda. Com efeito: $(a'a)T_a^{(e)}=a(a'a)=(aa')a=a$; por conseguinte, $a'a=a(T_a^{(e)})^{-1}=(au)(T_a^{(e)})^{-1}=u$. Tem-se pois:

*

Teorema 1: - Num semigrupo com identidade, todo o elemento não singular à esquerda é uma unidade. Inversamente: seja a uma

unidade e $\bar{a}^{-1}$ o seu inverso. As duas equações $xa=b$, $ay=b$ têm uma única solução. A da primeira é $b\bar{a}^{-1}$ e a da segunda é $\bar{a}^{-1}b$. Como $\underline{b}$ é arbitrário, $T_a^{(1)}$ e $T_a^{(2)}$ são transformações, de sorte que $\underline{a}$, além de ser não singular à esquerda é não singular. Portanto:

*

Teorema 2:- Num semigrupo com identidade, todo o elemento não singular à esquerda (à direita) é um elemento não singular. Os elementos não singulares são unidades e reciprocamente.

*

Exercício:- Verificar: i) que as unidades direitas e as unidades esquerdas formam semigrupos; ii) que as unidades formam um semigrupo, interseção dos dois anteriores; iii) que $(ab)^{-1}=b^{-1}a^{-1}$, se $\underline{a}$ e $\underline{b}$ são unidades.

* * *

5. Grupos - Um semigrupo de unidades diz-se um grupo. Um grupo $\mathcal{G}$ é definido, pois, pelos seguintes postulados:

1. $\mathcal{G}$ é fechado para o produto (o produto de dois elementos de $\mathcal{G}$ é um elemento de $\mathcal{G}$).

2. O produto é associativo.

3. Existe elemento um.

4. Todos os elementos de $\mathcal{G}$ são unidades.

A axiomática anterior pode ser substituída por esta outra:

G_1. $\mathcal{G}$ é fechado para o produto.

G_2. O produto é associativo.

G_3. Existe uma identidade direita ε.

G_4. Todo o elemento tem um inverso direito relativo a ε.

É imediato que êste segundo sistema de postulados é consequência do primeiro. Inversamente, admitindo o segundo, vamos passar ao primeiro. Dados $a\in\mathcal{G}$, escrevamos $aa'=\varepsilon$ e suponhamos $a'a''=\varepsilon$. Então $(a'a)(a'a'')=(a'a)\varepsilon=a'a$; por outro lado, tem-se $(a'a)(a'a'')=a'(aa')a''=a'\varepsilon a''=a'a''=\varepsilon$, de sorte que $a'a=\varepsilon$. A partir dêste facto, verificaremos que ε é a identidade. Fixemos um elemento $\underline{b}$. Sabemos que $b\varepsilon=b$, e agora devemos estabelecer que também se tem $\varepsilon b=b$. Supondo $bb'=\varepsilon$, é $(bb')(b\varepsilon)=\varepsilon(b\varepsilon)=\varepsilon b$; mas é, por outro lado, $(bb')(b\varepsilon)=b(b'b)\varepsilon=b\varepsilon\varepsilon=b$, pelo que $\varepsilon b=b$.

*

Exercício:- Um grupo pode ser caracterizado como um semigrupo para o qual as equações $ax=b$, $ya=b$, ($\underline{a}$, $\underline{b}$ dados), são solúveis. [Nota: A equação $ay=a$ tem solução, que designaremos por $\underline{\varepsilon}$. A equação $ya=c$, de solução $\underline{\gamma}$, dá $(\gamma a)\varepsilon=c\varepsilon=\gamma(a\varepsilon)=\gamma a=c$, de sorte que $\underline{\varepsilon}$ é uma identidade à direita].

*

Observação: - Um grupo pode definir-se como um sistema algébrico que é ao mesmo tempo semigrupo e quase-grupo.

*

Exemplos: I) Num monoide o conjunto das unidades forma um grupo. Em particular, no monoide das aplicações dum conjunto em si, as permutações do conjunto formam um grupo.

II) Nas tabelas juntas são definidos grupos finitos:

·	u	e
u	u	a
a	a	u

,

·	u	a	b
u	u	a	b
a	a	b	u
b	b	u	a

.

III) Tomemos o conjunto $\mathcal{L} = \{1, 2, \dots, n\}$. Conforme a segunda parte do exemplo I), as permutações de $\mathcal{L}$ formam o que se chama o grupo simétrico de ordem n (aqui a palavra "ordem" não significa o número de elementos do grupo), que representaremos por $\mathcal{P}_n$. Para cada $\varphi \in \mathcal{P}_n$, tem-se $b = \varphi(k) = i_k$, $(k = 1, 2, \dots, n)$. Escreveremos

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ i_1 & i_2 & i_3 & \cdots & i_n \end{pmatrix}.$$

Não se torna necessário colocar na primeira linha horizontal do 2º membro os números naturais $1, 2, \dots, n$ pela sua ordem natural. Essa ordem pode ser qualquer, desde que sob cada número natural seja colocado o número correspondente. Assim, se se põe

$$\psi = \begin{pmatrix} i_1 & \cdots & i_n \\ j_1 & \cdots & j_n \end{pmatrix} = \begin{pmatrix} 1 & 2 & \cdots & n \\ k_1 & k_2 & \cdots & k_n \end{pmatrix}, \text{ vê-se que } \psi\varphi = \begin{pmatrix} 1 & 2 & \cdots & n \\ j_1 & j_2 & \cdots & j_n \end{pmatrix}.$$

Em geral é $\psi\varphi \neq \varphi\psi$. Com as notações usadas aqui, o produto $\psi\varphi$ significa primeiramente φ depois ψ.

* * *

6. A lei de corte nos semigrupos. Grupos finitos - Tomemos um semigrupo e substituamos as afirmações de que as equações $xa = b$ e $cy = b$ são sempre solúveis por esta outra, que designaremos por postulado S_4: se as equações $xa = b$ e $ay = b$ forem solúveis, a solução é única. Os semigrupos em questão, entre os quais se situam os grupos, têm propriedades que traduziremos pelos dois teoremas a seguir:

*

Teorema 1: - Um semigrupo verificando o postulado S_4 satisfaz à lei do corte. Reciprocamente, a lei do corte implica o postulado S_4. Valendo S_4, escrevamos $xa = x'a = b$. A equação $xa = b$ tem uma única solução x, pelo que se terá $x = x'$. Reciprocamente, valendo a lei do corte, a equação $xa = b$, se for solúvel só pode ter a solução x, dado que $xa = x'a$ leva a $x = x'$. O mesmo se diz da equação $cy = b$.

*

Teorema 2: - Todo o semigrupo finito em que vale a lei do corte (à direita e à esquerda) é um grupo. Admitamos que a é um elemento fixo do semigrupo

e suponhamos que x percorre o semigrupo. Os elementos $xa, x'a, \ldots$ são todos diferentes, pois $xa = x'a$ levaria a $x = x'$. Então o conjunto dos elementos xa é o conjunto de todos os elementos do semigrupo, o que mostra ser sempre solúvel a equação $xa = b$. O mesmo se diz da equação $ay = b$, daí resultando, conforme o exercício do número anterior, que o semigrupo é um grupo.

*

Deixamos aqui as duas caracterizações seguintes dos grupos finitos:

1. G é um grupo finito, se e só se fôr um semigrupo finito com lei de corte.

2. G é um grupo (finito ou não), se fôr um preparoide com identidade direita ε, no qual todo o elemento é unidade direita relativamente a ε, e onde, se fôr r o inverso direito de ε, relativamente a ε, se tem $ab = ac.rb$ [Nota: Quando se trata de grupos finitos, esta última propriedade de G tem interpretação interessante na tabela do grupo. Como se vê, não se faz a hipótese da associatividade. O leitor encontra no livro "Cours d'Algèbre générale" de Almeida Costa a interpretação aludida].

***

7. Morfismos - Tomemos um espaço algébrico $\mathcal{G}$, tal como foi definido no nº 1. Se tivermos um segundo espaço algébrico $\mathcal{G}'$ com operadores em correspondência biunívoca com os de $\mathcal{G}$, utilizaremos os mesmos símbolos como operadores nos dois espaços. Seja, então,

$$\mathcal{G} = \{a, b, c, \ldots\}, \quad \mathcal{G}' = \{a', b', c', \ldots\}$$

e representemos por $\lambda_0, \mu_0, \ldots$ os operadores de ordem zero, com $\lambda, \mu, \ldots$ os operadores unários e com $\lambda^*, \mu^*, \ldots$ os operadores binários. Uma aplicação $\mathcal{G} \to \mathcal{G}'$ tal que $\lambda_0 \to \lambda_0$, $\mu_0 \to \mu_0$, etc. e tal que ainda que

$$a\lambda \to (a\lambda)\theta = (a\theta)\lambda = a'\lambda, \quad b\lambda \to (b\lambda)\theta = (b\theta)\lambda = b'\lambda, \text{ etc.}$$

$$a\lambda^* b \to (a\lambda^* b)\theta = (a\theta)\lambda^*(b\theta) = a'\lambda^* b', \text{ etc.},$$

diz-se um morfismo. Bem entendido que $a\lambda, b\lambda, \ldots$ significam o resultado, em $\mathcal{G}'$, da aplicação unária λ aos elementos $a, b, \ldots$, enquanto que o símbolo $a\lambda^* b$ significa o resultado, em $\mathcal{G}'$, da aplicação binária λ^* aos par ordenado a, b. Quando todos os elementos de $\mathcal{G}'$ são utilizados como imagem, o morfismo toma o nome de epimorfismo. Se, no morfismo a correspondência é biunívoca, temos um monomorfismo. Se um morfismo é simultaneamente epimorfismo e monomorfismo, diz-se um isomorfismo. O morfismo no hipótese de $\mathcal{G}'$ ser o próprio $\mathcal{G}$ toma o nome de endomorfismo, o monomorfismo designa-se por meromorfismo e o isomorfismo toma o nome de automorfismo.

Uma parte $\mathcal{G}_1$ de $\mathcal{G}$, fechada para as operações de $\mathcal{G}$ diz-se um subsistema algébrico. Num sentido inverso, introduziremos o conceito de extensão dum espaço algébrico, que será um espaço algébrico do qual o espaço algébrico inicial é um subespaço. Os operadores supõem-se transportados para a extensão. Dum modo geral, diz-se que um sistema algébrico $\mathcal{G}$ está mergulhado num

sistema algébrico $\mathcal{G}$, se os dois sistemas têm as mesmas operações e os mesmos operadores e se existe uma parte $\mathcal{G}_0 \subseteq \mathcal{G}$ isomorfa a $\mathcal{F}$.

§ 2. Semigrupos abelianos. Números inteiros

***

1. Semigrupos abelianos - Tomemos um semigrupo com um produto comutativo, ou seja um semigrupo abeliano, e consideremos os números $1, 2, \cdots, n$, assim como uma permutação destes números: $i_1, i_2, \cdots, i_n$. Vamos mostrar que o produto de n factores do semigrupo goza da propriedade seguinte:

$$a_1 a_2 \cdots a_n = a_{i_1} a_{i_2} \cdots a_{i_n}.$$

Sabemos que sucede assim quando $n = 2$. Suponhamos em seguida $i_k = n$. Então, supondo que a igualdade em questão é válida para $n-1$ factores, prová-la-emos para n factores. Com efeito:

$$a_{i_1} \cdots a_{i_{k-1}} \cdot a_{i_k} \cdot a_{i_{k+1}} \cdots a_{i_n} = a_{i_1} \cdots a_{i_{k-1}} \cdot a_n \cdot a_{i_{k+1}} \cdots a_{i_n} =$$

$$= a_{i_1} \cdots a_{i_{k-1}} a_{i_{k+1}} \cdots a_{i_n} \cdot a_n = a_1 \cdots a_{n-1} a_n = a_1 \cdots a_n,$$

desde que se tenha em conta a definição de produto de n elementos (n.º 3, § anterior), assim como a associatividade, a comutatividade e a hipótese de indução.

No caso dos semigrupos abelianos, emprega-se quási sempre o sinal + para representar a operação binária correspondente. Assim, poremos:

$$a_1 + \cdots + a_n = (a_1 + \cdots + a_{n-1}) + a_n;$$

$$A + B = a_1 + \cdots + a_p, \ (p \geq n+1), \quad A = a_1 + \cdots + a_n, \quad B = a_{n+1} + \cdots + a_p;$$

$$na = a + \cdots + a \ \ (\text{com } a \text{ escrito } n \text{ vezes});$$

$$na + ma = (n+m)a; \quad n \cdot ma = (nm)a.$$

O elemento um, se existir, será representado pelo símbolo 0 (zéro): $a + 0 = 0 + a = a$.

Uma regra importante que não é verificada no caso não comutativo é a seguinte: $n(a+b) = na + nb$. Fazendo uso do sinal $(\cdot)$, terá de escrever-se $(ab)^n = a^n . b^n$.

*

No caso dos grupos abelianos aditivos, também se dá ao grupo a designação de módulo.

*

Teorema 1: - Todo o semigrupo abeliano verificando a lei do corte pode ser mergulhado num grupo abeliano. Dado o semigrupo abeliano $(\mathcal{E}, .) = \{a, b, c, \cdots\}$, consideremos o conjunto $\mathcal{G}_0 = \{(a,b); (c,d); \cdots\}$ de pares ordenados $(a,b), \cdots$ e introduzamos sobre $\mathcal{G}_0$ a relação de equivalência seguinte: $(a,b) \rho (c,d)$, se e só se $ad = bc$. A classe de que (a,b) é um representante será designada por $[a,b]$. Então, mergulha-se o espaço cociente $\mathcal{G}_0/\rho = \{[a,b]; [c,d]; \cdots\}$, definindo $\mathcal{G} = \mathcal{G}_0/\rho$ por meio dum produto, conforme a igualdade seguinte: $[a,b] \cdot [c,d] = [ac, bd]$. Vamos ver que $\mathcal{G}$ é um grupo abeliano. Em primeiro lugar a definição desde de produto é independente dos representantes das classes, pois que, supondo $(a,b) \rho (a',b')$, tem-se $ab' = a'b$ e $[a',b'][c,d] = [a'c, b'd] = [ac, bd]$, visto que $a'cbd = b'dac$. É também evidente que o produto é comutativo

e associativo. Resta verificar que uma equação da forma $[a,b]+[x,y]=[c,d]$ tem a solução $[x,y]=[bc,ad]$. Reconhece-se, em seguida, que $(\mathcal{L}/.)$ está mergulhado em $\mathcal{G}$, mostrando que existe em $\mathcal{G}$ uma parte isomorfa ao semigrupo. Para isto, basta fazer corresponder ao elemento $a\in(\mathcal{L}/.)$ o elemento $[ab,b]$, onde b é um elemento qualquer de $(\mathcal{L}/.)$. A correspondência é com efeito um isomorfismo.

* Exercícios: - I) Reconhecer a parte da demonstração do teorema precedente onde se faz uso da lei do corte.

II) Verificar o isomorfismo relativo à inversão.

*

O problema de inversão que acaba de ser resolvido toma um aspecto muito importante no caso que passamos a estudar, empregando, aliás, a notação aditiva. Um semigrupo $\mathcal{L}=(L/+)$ diz-se um *semigrupo abeliano ordenado*, se é abeliano e verifica as duas condições seguintes: 1) $\mathcal{L}$ é um conjunto ordenado, para uma eventual relação de ordem; 2) se $a,b,c\in\mathcal{L}$ e $a<b$, então $a+c<b+c$, $\forall c\in\mathcal{L}$. Tem-se êste teorema:

*

Teorema 2: - *Supondo $\mathcal{L}$ um semigrupo abeliano ordenado onde a lei do corte é verificada, há um e um só processo de fazer a ordenação do grupo abeliano $\mathcal{G}$, em que se mergulhou $\mathcal{L}$, de modo a conservar a relação de ordem dada em $\mathcal{L}$.* Seja $a<b$. Deverá ter-se $[a+c,c]<[b+c,c]$. Esta relação é satisfeita, se se faz $[a,b]<[c,d]$, quando $a+d<b+c$. Vamos verificar que $\mathcal{G}$ é um *grupo abeliano ordenado*, isto é, é um grupo abeliano que satisfaz

estas duas condições indicadas para os semigrupos ordenados. De facto: dados $[a,b]$ e $[c,d]$, ou se tem $a+d<b+c$, ou, pelo contrário, é $b+c<a+d$, supondo que os dois elementos de que partimos não são iguais. No primeiro caso, é $[a,b]<[c,d]$, enquanto que no segundo é $[c,d]<[a,b]$. Por outro lado, a transitividade é evidente. Emfim, se $[a,b]<[c,d]$, tem-se $[a,b]+[f,g]<[c,d]+[f,g]$.

Temos assim um processo que leva a mergulhar o semigrupo no grupo, conservando a ordenação daquele. Para se vêr que o processo é único, notemos que, quando $[a,b]<[c,d]$, se não se tivesse $a+d<b+c$, ter-se-ia $b+c<a+d$, o que arrastaria $[b+c+f,f]+[f,b+d+f]<[a+d+f,f]+[f,b+d+f]$, isto é $[c,d]<[a,b]$.

***

2 - *Os números inteiros* - Os números naturais constituem, como vimos, um semigrupo abeliano aditivo $\mathcal{N}$ onde é válida a lei do corte. Assim, $\mathcal{N}$ pode mergulhar-se num grupo abeliano aditivo $\mathcal{Z}$, que se diz o conjunto dos *números inteiros*. Êstes números são portanto classes $[a,b]$, onde a e b são números naturais. A identidade de $\mathcal{Z}$ é a classe $[a,a]$, que se representará pelo símbolo 0, conforme a convenção feita no número anterior. Vê-se com efeito que $[c,d]+[a,a]=[c+a,d+c]=[c,d]$. O elemento inverso (simétrico) da classe $[a,b]$ é a classe $[b,a]$, pois que $[a,b]+[b,a]=[a+b,a+b]=0$. Um número natural $a=[a+b,b]$ será representado pelo próprio a. Além disso, utilizaremos o símbolo $-\alpha=[b,a]$ para designar o simétrico de $\alpha=[a,b]$.

Constata-se o seguinte: um número inteiro é um número natural $\neq 0$, ou é 0, ou é $-a$. É o que vamos ver. Formemos uma classe $[c,d]$. Quando $d=c$, então $[c,d]=0$. Se $d \neq c$, admitamos que para a ordenação dos números naturais conhecida, temos $d<c$, isto é $c=d+f$, onde $f \in \mathbb{N}$. Escreve-se $[c,d]=[f+d,d]=f$, e, por consequência, a classe é um número natural. Se, pelo contrário, for $c<d$, então $d=g+c$ e $[d,c]=[g+c,c]=g$, o que dá $[c,d]=-g$. O nosso conjunto $\mathbb{Z}$ é o seguinte:

$$\mathbb{Z} = \{1, 2, 3, \dots, n, \dots; 0; -1, -2, -3, \dots, -n, \dots\}.$$

Sabemos mais que a ordenação dos números naturais em questão, arrasta para os números inteiros uma ordenação segundo a regra $[a,b]<[c,d]$, se e só se $a+d<b+c$. Os números inteiros que precedem zero dizem-se negativos e os que seguem zero chamam-se positivos.

*

Exercício: - Verificar que os números naturais são os números positivos, que os números da forma $-a$ são os inteiros negativos e que, se $a<b$, então $-b<-a$.

*

A ordenação dos números inteiros que acabamos de obter leva a escrever $\mathbb{Z}$ sob a forma seguinte:

$$\mathbb{Z} = \{\dots, -n, \dots, -3, -2, -1, 0, 1, 2, 3, \dots, n, \dots\}.$$

No sistema algébrico dos números inteiros, que é um módulo, podemos introduzir uma operação de "produto", pondo

$$[a,b]\cdot[c,d] = [ac+bd, ad+bc].$$

Com efeito, admitamos que $[a,b]=[a',b']$, $[c,d]=[c',d']$, de sorte que

$a+b'=b+a'$, $c+d'=d+c'$. Vamos verificar que a regra de produto em causa dando

$$[a',b']\cdot[c',d'] = [a'c'+b'd', a'd'+b'c'],$$

se tem a igualdade

$$[ac+bd, ad+bc] = [a'c'+b'd', a'd'+b'c'].$$

Para isso temos de provar a igualdade

$$ac+bd+a'd'+b'c' = ad+bc+a'c'+b'd'. \qquad (1)$$

Ora $(a+b')c+(a'+b)d+(c+d')a'+(c'+d)b' = (a'+b)c+(a+b')d+(c'+d)a'+$ $+(c+d')b'$, e assim

$$ac+b'c+a'd+bd+ca'+d'a'+c'b'+db' =$$

$$= a'c+bc+ad+b'd+c'a'+da'+cb'+d'b',$$

que é justamente a relação (1).

*

Exercício: - Mostrar que o produto dos números inteiros se identifica com o dos números naturais, quando os inteiros em causa são números naturais.

*

Designemos por x, y, z números inteiros. São verificadas as regras seguintes no conjunto $\mathbb{Z}$: i) de $x<y$, $0<z$, tira-se $xz<yz$; ii) de $0<x$, $0<y$, tira-se $0<xy$, $0<xy$; iii) de $x<y$, deduz-se $x+z<y+z$; iv) de $0<x$, $y<0$, deduz-se $xy<0$, v) de $x<0$, $y<0$, tira-se $0<xy$. A regra ii) mostra que o produto dum número inteiro positivo por um número inteiro negativo é um inteiro negativo; e a regra v) mostra que o produto de dois números inteiros negativos é um número inteiro positivo.

Limitemo-nos a verificar a regra i). Sendo $x=[a,b]$, $y=[c,d]$,

$z=[f,g]$, com as hipóteses $a+d<b+c$, $g<f$. Então

$$xz=[af+bg,\ ag+bf],\quad yz=[cf+dg,\ cg+df],$$

e devemos estabelecer a relação $af+bg+cg+df<ag+bf+cf+dg$, ou, se se põe $f=g+h$, a relação $ag+ah+bg+cg+dg+dh<ag+bg+bh+cg+ch+hg$, que se simplifica e toma a forma

$$ah+cg+dg+dh<bh+cg+ch+hg. \qquad (2)$$

Ora $(a+d)<(c+b)$, por consequência $ah+dh<ch+bh$, donde se tira

$$(ah+dh)+(cg+dg)<(ch+bh)+(cg+dg),$$

que é precisamente (2).

* Exercício:- Verificar as regras i), ii), iii), iv) e v)

* Importa ter em conta que o produto dum inteiro qualquer pelo elemento zero é igual a zero, e que, se o produto de dois elementos é zero, um dos factores é zero. Quanto à primeira afirmação, se se emprega a representação $[a,b]$, vê-se que $[a,b]\cdot[c,c]=[ac+bc,ac+bc]=0$; e, quanto à segunda, se se supõe $xy=0$, não pode ter-se $0<x$, $0<y$; $0<x$, $y<0$; $x<0$, $0<y$; $x<0$, $y<0$; terá-se necessàriamente $x=0$ ou $y=0$.