J. SEBASTIÃO E SILVA

COMPÊNDIO DE MATEMÁTICA

1.º volume

1.º tomo

Curso Complementar do Ensino Secundário

Edição GEP

LISBOA

CAPÍTULO III

NÚMEROS INTEIROS E CÁLCULO COMBINATÓRIO

1. **Número de elementos dum conjunto.** A noção de número apresenta-se pela primeira vez ao espírito do homem como resultado da *operação de contagem*. O homem primitivo conta as ovelhas dum rebanho, fazendo corresponder a cada ovelha uma determinada pedra, de modo que a duas ovelhas distintas correspondam sempre duas pedras distintas; assim, o conjunto de pedras utilizadas na contagem representa o *número* de ovelhas do rebanho, de tal modo que, se, por exemplo, vier a faltar uma ovelha, há sempre possibilidade de dar pela ausência, ao tentar estabelecer de novo a correspondência entre as ovelhas e as pedras.

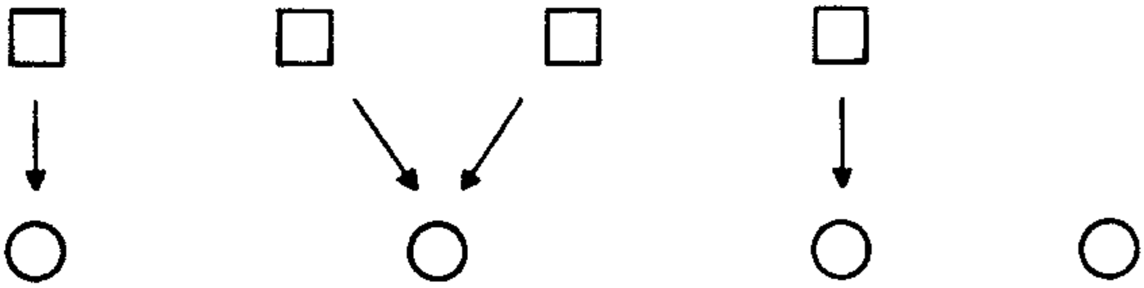
Aparece-nos aqui um novo conceito — o de *correspondência* — que, tal como os conceitos de elemento, conjunto e sequência, não definimos, mas apenas procuraremos esclarecer por meio de exemplos.

Sejam A e B dois conjuntos. Se, a cada elemento de A, fizermos corresponder um elemento, *e um só,* de B, diz-se que fica estabelecida uma *correspondência unívoca entre* A *e* B (1). Por exemplo, a seguinte figura indica uma correspondência unívoca entre dois conjuntos, sendo os elementos do primeiro representados por quadrados,

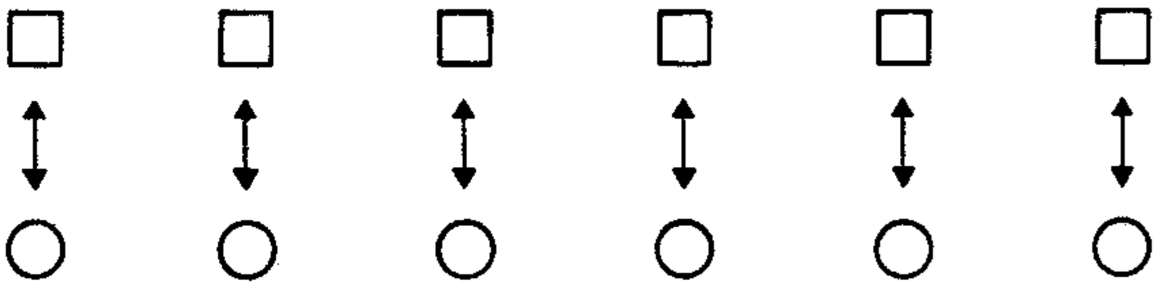
---

(1) Trata-se aqui, a bem dizer, duma relação binária, subconjunto de A x B. Mas isso será discutido mais tarde.

os do segundo por círculos e a correspondência por meio de setas que vão de cada quadrado ao círculo correspondente:



Se, a cada elemento de um conjunto A, corresponder um determinado elemento de B, de modo que, reciprocamente, cada elemento de B corresponda deste modo a um elemento de A, *e um só*, a correspondência diz-se *biunívoca* ou correspondência *um-a-um entre* A *e* B. Exemplo figurado:



No exemplo anterior de contagem das ovelhas por meio de pedras, o que se faz é *estabelecer uma correspondência biunívoca entre o conjunto das ovelhas e um conjunto de pedras.* Deste modo, se vier a faltar alguma ovelha, já não será possível estabelecer uma correspondência biunívoca entre o conjunto das ovelhas presentes e o conjunto das pedras, pois sobrará, pelo menos, uma pedra.

Vejamos ainda outros exemplos de correspondência:

I. Consideremos uma estante que tenha vários livros em cada prateleira. Há, neste caso, uma correspondência unívoca entre o conjunto dos livros e o conjunto das prateleiras, pois a cada livro corresponde uma prateleira *e uma só*: aquela onde o livro está colocado.

Mas uma prateleira corresponde assim a mais de um livro: a correspondência não é, pois, biunívoca.

II. Numa dada turma dum liceu, a cada aluno corresponde uma (e só uma) carteira — aquela onde se senta. Se as carteiras são individuais e se todas são ocupadas, a correspondência é biunívoca entre os dois conjuntos e o *número de alunos é, portanto, igual ao número das carteiras.* Caso contrário, isto é, se as carteiras não são individuais ou se há carteiras não ocupadas a correspondência será unívoca, mas não será em geral biunívoca entre os dois conjuntos.

DEFINIÇÃO. *Dados dois conjuntos* A *e* B, *diz-se que* A *é equipotente a* B, *sse é possível definir uma correspondência biunívoca entre* A *e* B.

Vê-se logo, intuitivamente, que a relação *equipotente* assim definida é reflexiva, simétrica e transitiva, portanto uma *relação de equivalência.* Posto isto:

DEFINIÇÃO. *Diz-se que dois conjuntos* A *e* B *têm o mesmo número de elementos (ou a mesma potência), sse* A *e* B *são sequipotentes.*

Deste modo, o *número de elementos* dum conjunto A (também chamado *número cardinal* ou simplesmente *cardinal de* A) é, por assim dizer, a propriedade que esse conjunto tem de comum com todos os conjuntos que se possam pôr em correspondência biunívoca com A ([1]). Por conseguinte, o número de elementos de A poderá ser representado indistintamente por qualquer desses conjuntos (equipotentes a A) incluindo o próprio A.

Por exemplo, no caso das ovelhas, o seu número pode ser representado pelo próprio conjunto das ovelhas ou pelo referido conjunto

---

([1]) Modernamente, o número de elementos dum conjunto é em geral concebido *extensivamente,* isto é, como *classe* de conjuntos e não como *propriedade* característica dessa classe.

de pedras ou por qualquer outro conjunto que se possa pôr em correspondência biunívoca com o primeiro. É frequente as crianças indicarem com os dedos o número de anos que têm. Alguns pastores contam as cabeças dum rebanho por meio de entalhes feitos num cajado. E ainda hoje, em certas ocasiões, contamos os elementos dum conjunto, fazendo corresponder a cada elemento um risco num papel; assim se geram símbolos tais como:

I, II, III, IIII, IIIII, IIIIII, IIIIIII, etc.

que podem ser tomados como designações de *números*. Encontramos vestígios deste processo elementar nos símbolos I, II, III, IIII da numeração romana. Mas note-se como já os símbolos IIII, IIIII, ... são substituídos pelas suas *abreviaturas* IV, V, ..., a fim de evitar uma escrita demasiado longa. É assim, por meio de *convenções simbólicas*, que os sistemas de numeração começam a simplificar-se e a aperfeiçoar-se no decorrer dos séculos. O mais perfeito dos sistemas hoje usados habitualmente — o da numeração decimal, que será estudado mais tarde em pormenor — nasceu de pôr os objectos contados em correspondência com dedos das duas mãos, uma ou mais vezes.

Chama-se *número natural* (ou *número inteiro positivo*) o número de elementos dum conjunto finito qualquer, não vazio. Os números naturais são, habitualmente, designados pelos símbolos da numeração decimal:

$$1, 2, 3, \ldots, 10, 11, \ldots, 100, 101, 102, \ldots$$

Por sua vez, o conjunto de *todos* os possíveis números naturais é designado pelo símbolo $\mathbb{N}$. A experiência que adquirimos diariamente no uso dos números naturais induz-nos a admitir que o *conjunto* $\mathbb{N}$ é *infinito*.

Por outro lado, somos levados a atribuir aos conjuntos vazios também um número, que se chama *zero* e se designa pelo símbolo 0. *Portanto, dizer que um conjunto é vazio equivale a dizer que o número dos seus elementos é zero.* Assim se nos apresenta, para comodidade de linguagem, uma primeira extensão da ideia de número. Os números naturais e o número zero recebem a designação comum de *números inteiros absolutos* (ou *números inteiros não negativos*); representaremos por N_0 este conjunto. Assim, temos:

$$\mathbb{N} = \{1, 2, 3, 4, \ldots\}$$
$$\mathbb{N}_0 = \{0, 1, 2, 3, 4, \ldots\}$$
$$\mathbb{N}_0 = N \cup \{0\} \quad \text{e portanto} \quad \mathbb{N} \subset \mathbb{N}_0$$

O número de elementos dum conjunto finito A *é designado pelo símbolo* $\# A$. Se A é vazio, tem-se $\# A = 0$. Se A não é vazio, tem-se $\# A \in \mathbb{N}$.

Em particular: $\# A = 1 \Leftrightarrow \exists^1 x : x \in A$.

2. **Reunião de dois conjuntos disjuntos e soma de dois números.** A noção intuitiva que todos temos de 'conjunto finito' implica as duas seguintes propriedades:

1) *Todo o subconjunto dum conjunto finito é ainda finito.*

2) *A reunião de dois conjuntos finitos é ainda um conjunto finito.*

Ora, o conceito de *reunião de conjuntos* dá lugar ao conceito de *soma de números,* do seguinte modo:

DEFINIÇÃO. *O número de elementos de* $A \cup B$ *é chamado soma do número de elementos de* A *com o número de elementos de* B, *sse* A *e* B *são disjuntos (isto é, se* $A \cap B = \varnothing$*).*

Sejam *a* e *b* dois números naturais quaisquer. Então existem, pelo menos, dois conjuntos finitos A e B, não vazios, tais que:

$$\# A = a, \quad \# B = b$$

Estes conjuntos A e B podem ser ou são disjuntos. Porém, a experiência quotidiana leva-nos a admitir, por *indução* (ver Cap. I, n.º 17), o seguinte facto:

3) *Quaisquer que sejam os números naturais* a, b, *é sempre possível determinar dois conjuntos finitos* A *e* B *disjuntos, tais que* $\# A = a, \# B = b$.

Ora, nesta hipótese, segundo 2), a reunião de A com B é um conjunto finito e, por definição, $\# (A \cup B)$ é soma de *a* com *b*. Por conseguinte:

I. PROPOSIÇÃO DE EXISTÊNCIA. *Para todo o par ordenado de números naturais* a *e* b, *existe (pelo menos) um número natural* c, *tal que* c *é soma de* a *com b*.

Por outro lado, é fácil ver que:

II. PROPOSIÇÃO DE UNICIDADE. *Para todo o par ordenado de números naturais* a *e* b, *não pode existir mais de um número natural* c *que seja soma de* a *com* b.

Com efeito, suponhamos que *c* e *c'* são soma de *a* com *b*. Quer isto dizer que existem dois conjuntos A e B disjuntos tais que:

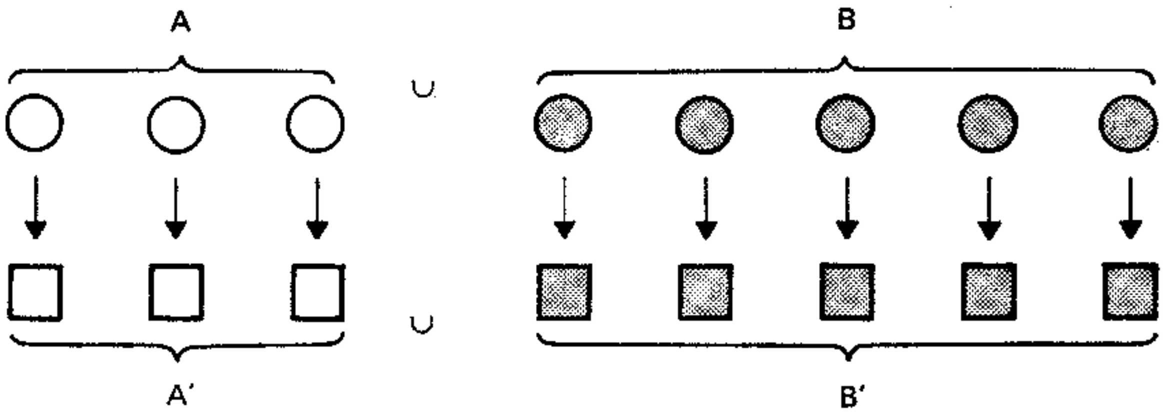
$$\# A = a, \quad \# B = b, \quad \# (A \cup B) = c$$

e dois conjuntos A' e B' disjuntos tais que:

$$\# A' = a, \quad \# B' = b, \# (A' \cup B') = c'$$

Mas, como $\# A = \# A'$ e $\# B = \# B'$, existem correspondências biunívocas entre A e A', e entre B e B'. E, como $A \cap B = \varnothing$, $A' \cap B' = \varnothing$, essas correspondências permitem definir uma correspondência biunívoca entre $A \cup B$ e $A' \cup B'$. Logo $\# (A \cup B) = \# (A' \cup B')$ ou seja $c = c'$.

EXEMPLO FIGURADO:



Assim, a cada par ordenado de números naturais a *e* b, *fica a corresponder um, e um só, número natural, que se chama a soma de* a *com* b. A soma de *a* com *b* é representada pela notação a + b.

Chama-se *adição* a operação que faz corresponder a cada par (a, b) de números naturais o número a + b.

A proposição I exprime-se dizendo que a adição em $\mathbb{N}$ é *sempre possível* e a proposição II, dizendo que a adição em $\mathbb{N}$ é *unívoca* (ou *uniforme*). De tudo isto resulta, aplicando o PRINCIPIO LÓGICO DE SUBSTITUIÇÃO, a seguinte propriedade válida no universo $\mathbb{N}$:

$$a = a' \wedge b = b' \Rightarrow a + b = a' + b'$$

Notemos, agora que, todas estas considerações relativas a *números naturais* (conjunto $\mathbb{N}$) se estendem a *números inteiros absolutos* (conjunto $\mathbb{N}_0$). Como, por definição, 0 é o número de elementos do conjunto vazio e

$$A \cup \varnothing = A \quad \textit{qualquer que seja o conjunto } A,$$

segue-se que:

$$a + 0 = a, \ \forall a \in \mathbb{N}_0$$

Exprime-se este facto, dizendo que 0 *é elemento neutro* da adição em $\mathbb{N}_0$ (em $\mathbb{N}$ não existe elemento neutro da adição).

3. **Comutatividade e associatividade da adição. Adição iterada.** É evidente que a comutatividade e a associatividade da reunião de conjuntos tem como consequência a comutatividade e associatividade da adição de números. Assim, quaisquer que sejam a, b, c $\in \mathbb{N}_0$, tem-se:

$$a + b = b + a \quad \text{(PROPRIEDADE COMUTATIVA)}$$

$$(a + b) + c = a + (b + c) \quad \text{(PROPRIEDADE ASSOCIATIVA)}$$

Por exemplo, se $a = \# A$, $b = \# B$, com $A \cap B = \emptyset$, tem-se:

$$a + b = \# (A \cup B) = \# (B \cup A) = b + a$$

e analogamente para a associatividade.

Mas note-se que há propriedades da reunião que não se transmitem à adição de números. Por exemplo, vimos que, entre os subconjuntos dum universo U, há um *elemento absorvente*, para a reunião, que é precisamente U. Ora, não há nenhum elemento absorvente para a adição em $\mathbb{N}_0$, isto é, nenhum elemento n tal que

$$a + n = n \quad , \quad \forall a \in \mathbb{N}_0.$$

Por outro lado, tem-se:

$$A \cup A = A, \forall A \subset U \quad \textit{(propriedade de idempotência)}$$

ao passo que, em $\mathbb{N}_0$, só poderá $a + a = a$ quando $a = 0$; exceptuado este caso, é sempre $a + a \neq a$.

Seja agora *n* um número natural diferente de 1. Chama-se *soma de* n *números* $a_1, a_2, \ldots, a_n$ o número que se obtém adicionando o primeiro com o segundo, adicionando depois o resultado com o terceiro, e assim sucessivamente, até chegar ao último. A soma dos *n* números dados (chamados *parcelas*) representa-se pela notação:

$$a_1 + a_2 + \ldots + a_n$$

ou ainda pela notação mais condensada e mais correcta:

$\sum_{k=1}^{n} a_k$ (ler: *somatório de* a_k *de* 1 *a* n)

Em particular, para n = 2, 3, 4, ..., temos:

$$\sum_{k=1}^{2} a_k = a_1 + a_2 , \quad \sum_{k=1}^{3} a_k = (a_1 + a_2) + a_3$$

$$\sum_{k=1}^{4} a_k = ((a_1 + a_2) + a_3) + a_4, \ldots$$

Deste modo, partindo do conceito de *soma de dois números,* é definido o conceito de *soma de três ou mais números*. A operação assim definida para mais de dois dados é chamada *adição iterada*(1). Define-se, inclusivamente, *soma de um único número* como sendo esse mesmo número, isto é, pondo simbolicamente:

$$\sum_{k=1}^{1} a_k = a_1$$

Seja por exemplo $a_k = k$, para k = 1, 2, ... Então:

$$\sum_{k=1}^{n} a_k = \sum_{k=1}^{n} k = 1 + 2 \ldots + n = \frac{n(n+1)}{2}$$

Temos estado a usar exclusivamente a letra k como *índice de adição,* mas trata-se, neste caso, de uma *variável aparente* (também

---

(1) Também chamada *adição sucessiva*. O adjectivo 'iterado' é sinónimo de 'repetido'.

aqui chamada *índice mudo*), sujeita à mesma regra de substituição das variáveis aparentes em quantificadores (pág. 71). Assim, tem-se:

$$\sum_{k=1}^{n} a_k = \sum_{i=1}^{n} a_i = \sum_{p=1}^{n} a_p = \sum_{y=1}^{n} a_y = \ldots$$

É claro que poderíamos definir directamente *soma de* n *números* $a_1, \ldots a_n$ (com *n* natural qualquer), a partir da reunião de n conjuntos, $A_1, \ldots, A_n$, tais que $\# A_1 = a_1, \ldots, \# A_n = a_n$, sendo estes conjuntos disjuntos dois a dois, isto é, sendo $A_j \cap A_k = \varnothing$ para $j \neq k$. Com efeito, tem-se neste caso:

$$a_1 + a_2 + \ldots + a_n = \# (A_1 \cup A_2 \cup \ldots \cup A_n)$$

ou, abreviadamente:

$$\sum_{k=1}^{n} a_k = \# \bigcup_{k=1}^{n} A^k$$

Mas, note-se que estamos a considerar apenas um número finito de parcelas, ao passo que a reunião de conjuntos se pode definir para uma infinidade de parcelas (ver Cap. II, n.º 13).

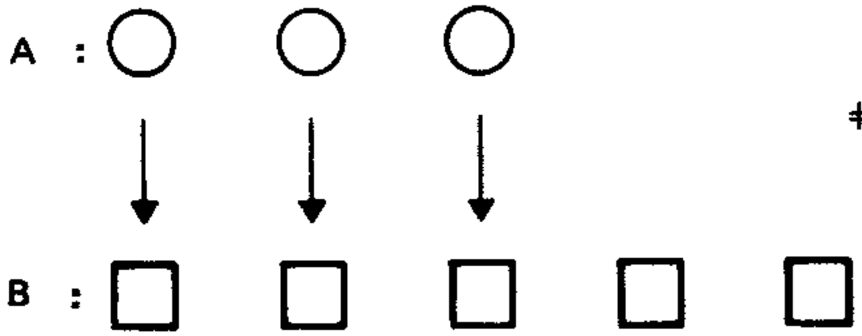
Entretanto, é fácil ver que a comutatividade e a associatividade se estendem à adição iterada sob as seguintes formas:

COMUTATIVIDADE GENERALIZADA. *A soma de vários números não se altera quando se muda a ordem das parcelas.*

ASSOCIATIVIDADE GENERALIZADA. *A soma de vários números não se altera quando se substituem duas ou mais parcelas pela sua soma.*

4. **Relação de grandeza entre números.** Diz-se que o número de elementos dum conjunto A *é menor que* o número de elementos

dum conjunto B, quando A é equipotente a uma parte de B, mas não é equipotente a B. Para indicar que um número *a* é menor que um número *b* escreve-se $a < b$; neste caso também se escreve $b > a$ e se diz que b *é maior que* a. Exemplo figurado:



$\# A < \# B$

Pela experiência que temos com os conjuntos finitos sabemos que:

Um conjunto finito nunca é equipotente a uma sua parte estrita [1].

Daqui e da definição anterior resulta que *a inclusão estrita entre conjuntos finitos* A *e* B *(não vazios) dá lugar à relação de grandeza, expressa pelo sinal* $<$*, entre números naturais;* isto é:

$$(1) \qquad A \subset B \wedge A \neq B \Rightarrow \# A < \# B$$

A relação $<$ é estendida a $\mathbb{N}_0$ mediante a seguinte definição:

$$0 < a \Leftrightarrow 0 \neq a \quad (\forall a \in \mathbb{N}_0)$$

que mantém a propriedade (1).

É fácil ver agora que:

I. *A relação* $<$ *é anti-reflexiva,* isto é:

$$x < y \Rightarrow x \neq y \quad (\text{em } \mathbb{N} \text{ ou } \mathbb{N}_0)$$

---

(1) Como veremos adiante, esta propriedade não é válida para conjuntos infinitos e pode, por isso, ser tomada para definição de 'conjunto finito'.

Além disso prova-se, como indicaremos mais adiante, que:

II. *A relação $<$ é anti-simétrica,* isto é:

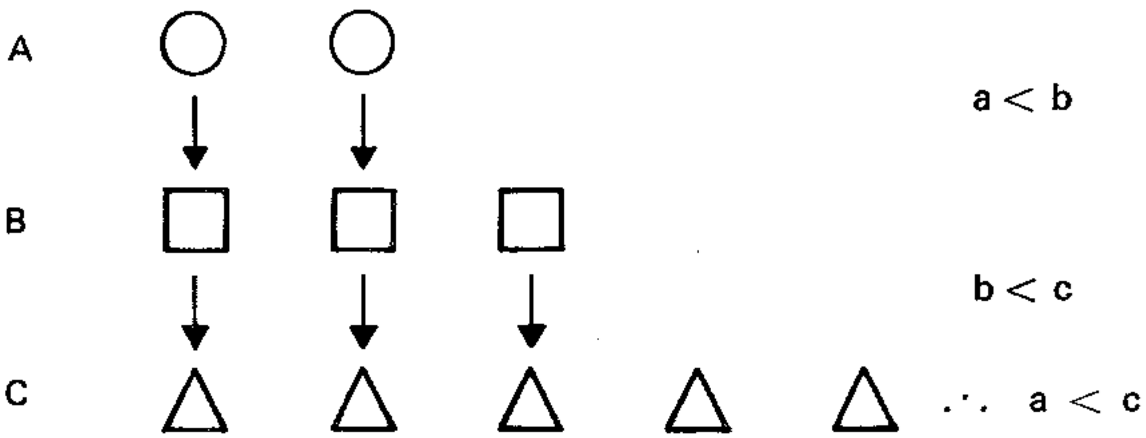
$$x < y \Rightarrow y \nless x$$

Por sua vez, a transitividade da relação de inclusão dá lugar à transitividade da relação de grandeza $<$ (em $\mathbb{N}$ ou $\mathbb{N}_0$):

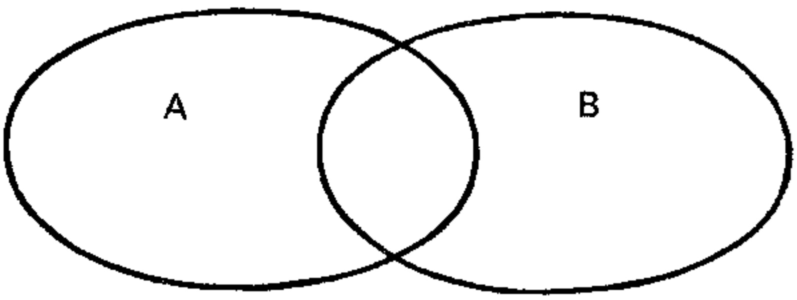
III. $$a < b \wedge b < c \Rightarrow a < c$$

Esquema demonstrativo:

$$a = \# A, \; b = \# B, \; c = \# C$$



Mas, surge agora uma propriedade nova. Já tínhamos visto (pág. 92) que, dados dois conjuntos A e B, pode acontecer que nenhum deles esteja contido no outro. Porém, a experiência quotidiana conduz-nos, *por indução,* à seguinte lei:



Dados dois conjuntos finitos A *e* B *não vazios, é sempre possível estabelecer uma correspodência biunívoca entre um deles e um subconjunto do outro.*

Passando a números. esta lei traduz-se pela seguinte propriedade:

IV. *Dados dois números naturais* a, b, *tem-se sempre: ou* $a < b$ *ou* $b < a$ *ou* $a = b$. Simbolicamente:

$$\forall a, b \in \mathbb{N}: \quad a < b \vee b < a \vee a = b$$

Exprime-se este facto, dizendo que a relação $<$ é *tricotómica*. A conjunção das propriedades I, II e IV é chamada PROPRIEDADE DA TRICOTOMIA FORTE e pode enunciar-se do seguinte modo:

IV'. *Dados dois números naturais* a, b, *verifica-se sempre uma, e uma só, das seguintes hipóteses:*

$$a < b, \quad b < a, \quad a = b$$

5. **Relação de grandeza lata.** A partir da relação $<$ define-se a relação $\leqslant$, chamada *relação de grandeza lata,* tal como se segue:

DEFINIÇÃO. $\quad a \leqslant b \Leftrightarrow a < b \vee a = b$

E não oferece dificuldade verificar que as propriedades I, II, III e IV são, agora, substituídas pelas seguintes:

I'. $a = b \Rightarrow a \leqslant b$ (REFLEXIVA)

II'. $a \leqslant b \wedge b \leqslant a \Rightarrow a = b$ (ANTI-SIMÉTRICA LATA)

III'. $a \leqslant b \wedge b \leqslant c \Rightarrow a \leqslant c$ (TRANSITIVA)

IV'. $\forall a, b \in \mathbb{N}: a \leqslant b \vee b \leqslant a$ (DICOTÓMICA)

É manifesto que a relação $\leqslant$ entre números traduz a relação $\subset$ entre conjuntos:

$$A \subset B \Rightarrow \# A \leqslant \# B$$

Todavia, a relação $\subset$, que é reflexiva, anti-simétrica lata e transitiva (como a relação $\leqslant$), *não é dicotómica,* como já observámos.

6. **Adição e relação de grandeza.** Das propriedades anteriores deduzem-se algumas outras que vamos demonstrar:

PROPOSIÇÃO 1. *A soma de dois números naturais é sempre maior que qualquer desses números; isto é, simbolicamente:*

$$a < a + x, \quad \forall a, x \in \mathbb{N}$$

Demonstração:

Seja $a = \# A$, $x = \# X$, sendo A e X conjuntos finitos disjuntos e não vazios. Então:

$$a + x = \# (A \cup X), \quad A \subset A \cup X \quad \text{e} \quad A \neq A \cup X$$

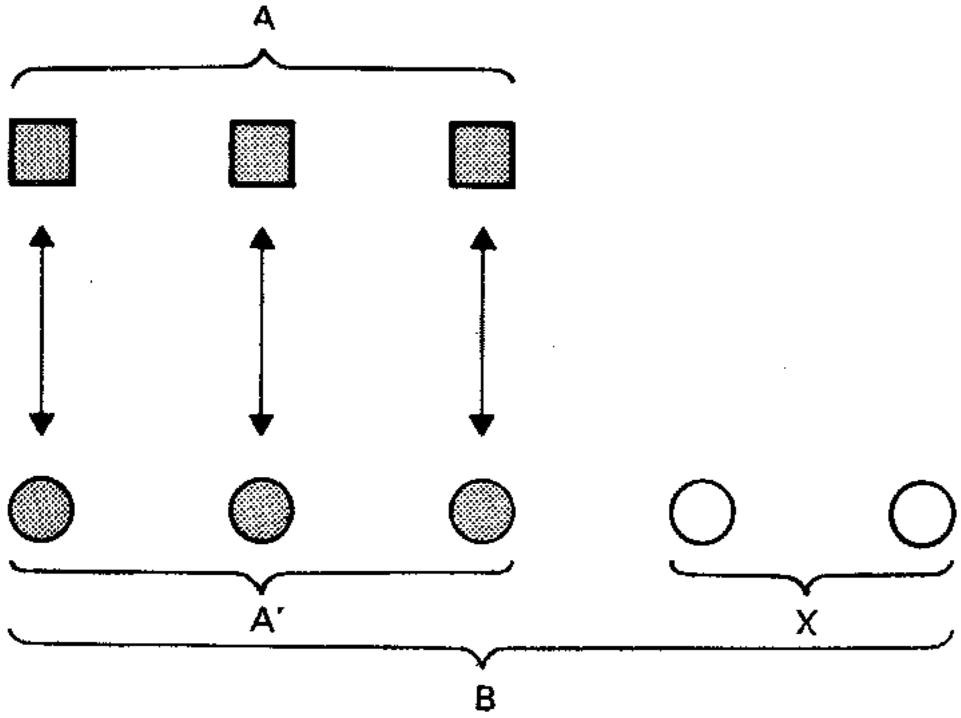
E, como a inclusão estrita entre conjuntos finitos implica a relação $<$ entre números (n.º 4), vem $a < a + x$.

PROPOSIÇÃO 2. *Dados dois números naturais* a *e* b *tais que* $a < b$, *existe sempre (pelo menos) um número natural* x *tal que* $a + x = b$; *isto é, simbolicamente:*

$$\forall a, b \in \mathbb{N}: \ a < b \Rightarrow \exists x, a + x = b$$

Demonstração:

Seja $a = \# A$, $b = \# B$ e $a < b$. Então podemos estabelecer uma correspondência biunívoca entre A e um conjunto A′ contido estritamente em B. Ponhamos $B \setminus A' = X$; então $A' \cup X = B$ e $A' \cap X = \varnothing$, de modo que, se pusermos $\# X = x$, virá $a + x = b$.



A conjunção das proposições 1 e 2 pode enunciar-se como segue (no universo $\mathbb{N}$):

(1) $$\boxed{a < b \Leftrightarrow \exists x, \quad a + x = b}$$

Esta proposição poderia mesmo ser tomada como definição do conceito de 'menor que' ($<$) a partir do conceito de 'soma' ($+$), no universo $\mathbb{N}$*: Diz-se que* $a < b$*, sse existe pelo menos um* x *tal que* $a + x = b$.

De (1) e das propriedades da adição deduzem-se novas proposições. Assim:

PROPOSIÇÃO 3. $a < b \Rightarrow a + c < b + c, \ \forall a, b, c \in \mathbb{N}$.

Demonstração:

Suponhamos $a < b$. Então existe $x \in \mathbb{N}$ tal que $a + x = b$. Ora, pelas propriedades associativa e comutativa da adição, tem-se:

$$(a + c) + x = a + (c + x) = a + (x + c) = (a + x) + c = b + c$$

Assim: $(a + c) + x = b + c$ e portanto $a + c < b + c$.

A proposição 3 pode ser enunciada em linguagem comum dizendo *'Quando uma das parcelas aumenta, a soma aumenta'* ou ainda *'Adicionando o mesmo número a ambos os membros duma relação de grandeza, a relação mantém-se'*. Exprime-se esta facto dizendo que a adição é uma operação *monótona.*

OBSERVAÇÃO. As propriedades anti-simétrica e transitiva da relação $<$ em $\mathbb{N}$ poderiam igualmente ser deduzidas de (1), aplicando a propriedade anti-reflexiva e as propriedades da adição. Essas deduções podem ser feitas como exercício.

Por sua vez, da proposição 3 deduz-se:

PROPOSIÇÃO 4. $a + c = b + c \Rightarrow a = b, \ \forall a, b, c \in \mathbb{N}$

Demonstração:

Suponhamos $a + c = b + c$. Segundo a propriedade da tricotomia, só pode ser $a < b$ ou $b < a$ ou $a = b$. Mas se fosse $a < b$ viria, pela monotonia de adição, $a + c < b + c$, e então não poderia ser $a + c = b + c$ (propriedade anti-reflexiva).

Analogamente, se fosse $b < a$, viria $b + c < a + c$, e não poderia ser $a + c = b + c$. Por conseguinte só pode ser $a = b$. (COMPARE ESTA DEMONSTRAÇÃO COM O EXEMPLO DE POLISSILOGISMO DADO NO CAPÍTULO I, N.º 17).

A propriedade da adição que acabámos de demonstrar é chamada PROPRIEDADE DA REDUÇÃO ou PROPRIEDADE DO CORTE, pois que se passa de $a + c = b + c$ para $a = b$, *cortando* o termo *c* em ambos os membros da primeira igualdade.

Daqui, por sua vez, deduz-se o seguinte:

COROLÁRIO. *Dados dois números* a, $b \in \mathbb{N}$, *não pode existir mais de um* $x \in \mathbb{N}$ *tal que* $a + x = b$.

Com efeito, se x e y são números naturais tais que $a + x = b$ e $a + y = b$, então $a + x = a + y$, donde, pela propriedade do corte, $x = y$. Portanto, simbolicamente:

$$a + x = b \wedge a + y = b \Rightarrow x = y$$

7. **Subtracção.** A análise anterior permite-nos estudar, em toda a generalidade, o seguinte problema:

Dados dois números a, $b \in \mathbb{N}$, *achar um número* $x \in \mathbb{N}$ *tal que* $a + x = b$.

Pelo que vimos, este problema só é *possível* (isto é, só *tem solução*), quando $a < b$. Mas neste caso, além de possível, é *determinado* (isto é, tem uma *única solução*). Simbolicamente:

$$\begin{cases} b \leqslant a \Rightarrow \sim \exists\, x, \quad a + x = b & \textit{(nenhuma solução)} \\ a < b \Rightarrow \exists^1 x, \quad a + x = b & \textit{(uma e uma só solução)} \end{cases}$$

Neste último caso, o número x procurado é chamado *diferença entre* b *e* a e representado por $b - a$. Fica, pois, assim definida uma operação (subtracção) que faz corresponder ao par ordenado (b, a) o número $b - a$ (*b* é então chamado o *aditivo* e *a* o *subtractivo).* Porém, ao contrário da adição, esta operação em $\mathbb{N}$:

— *Não é sempre possível.*

— *Não é comutativa.*

— *Não é associativa.* P. ex. $(8 - 5) - 2 \neq 8 - (5 - 2)$.

Todavia, como vimos, a subtracção em $\mathbb{N}$ é *unívoca* (isto é, a diferença, quando existe, é única). Além disso, facilmente se demonstram, como exercício, as duas seguintes proposições:

$$a < b \Rightarrow a - c < b - c \quad (\text{se } c < a)$$

$$a < b \Rightarrow c - a > c - b \quad (\text{se } b < c)$$

que se podem enunciar dizendo: *A diferença aumenta quando o aditivo aumenta e diminui quando o subtractivo aumenta.* Também podemos exprimir este facto dizendo que a subtracção é *crescente à esquerda e decrescente à direita* (PROPRIEDADES DE MONOTONIA DA SUBTRACÇÃO).

8. **Multiplicação.** Já vimos como se define a adição iterada ou adição de várias parcelas $a_1, \ldots, a_n$, cujo resultado se representa por $a_1 + \ldots + a_n$ ou por $\sum_{k=1}^{n} a_k$ (com $n \in \mathbb{N}$). Pode acontecer, em particular, que as *n* parcelas sejam um mesmo número $a \in \mathbb{N}$:

$$a_k = a, \quad \text{para} \quad k = 1, \ldots, n$$

Neste caso, a soma $\sum_{1}^{n} a_k$ é chamada *produto de* n *por* a e representa-se por $n \times a$, $n.a$ ou simplesmente $n\,a$. Chama-se multiplicação a operação que faz corresponder ao par ordenado de números naturais *n* e *a (factores)* o número natural *n a (produto)*.

Como a adição é *sempre possível* e *unívoca* em $\mathbb{N}$, o mesmo acontece com a multiplicação. Além disso sabe-se (e havemos de demonstrá-lo) que a multiplicação em $\mathbb{N}$ é:

I. *Comutativa:* $ab = ba, \ \forall a, b \in \mathbb{N}$

II. *Associativa:* $(ab)\,c = a\,(bc), \ \forall a, b, c \in \mathbb{N}$

III. *Distributiva* a respeito da adição:

$$(a + b)\ c = ac + bc, \ \forall a, b, c \in \mathbb{N}$$

IV. *Monótona:* $a < b \Rightarrow ac < bc, \quad \forall a, b, c \in \mathbb{N}$

Da definição resulta ainda que:

V. $$1.a = a \quad , \quad \forall a \in \mathbb{N}$$

Exprime-se este facto dizendo que 1 é *elemento neutro* da multiplicação.

A *multiplicação iterada* é definida como fizemos para a adição. Chama-se *produto de* n *números* $a_1, \dots a_n$ (com *n* natural $\neq 1$) o número que se obtém, multiplicando a_1 por a_2, multiplicando depois $a_1\, a_2$ por a_3 e assim sucessivamente até a_n. O resultado final é representado por $a_1 \dots a_n$, mais correctamente, por:

$$\prod_{j=i}^{n} a_j \quad \text{(ler } \textit{produto dos } a_j \textit{ de } 1 \text{ a } n\text{)}$$

Note-se que o índice j é aqui uma variável aparente (*índice mudo)*, tal como nos somatórios.

Põe-se ainda, *por definição:*

$$\prod_{k=1}^{1} a_k = a_1$$

Tal como a adição, a multiplicação iterada possui as PROPRIEDADES ASSOCIATIVA E COMUTATIVA GENERALIZADAS.

EXEMPLOS IMPORTANTES:

I. Se os *n* factores $a_1, \dots, a_n$ são todos iguais a um mesmo número *a,* o seu produto é, por definição, a *potência* n *de* a, que se representa por a^n. Chama-se *potenciação* a operação que faz corresponder, ao par ordenado (a, n) de números naturais *a (base)* e *n (expoente)*, o número natural a^n *(potência)*. A potenciação é, como se vê, *sempre possível e unívoca* (em $\mathbb{N}$), mas não é comutativa (p. ex. $2^3 \neq 3^2$) nem associativa [p. ex. $[(2^3)^2 \neq 2^{(3^2)}]$. Possui, no entanto, propriedades bem conhecidas (relativas ao produto de potências com a mesma base ou com o mesmo expoente), que serão demonstradas posteriormente.

II. Suponhamos $a_k = k$, para $k = 1, 2, \ldots$ Então:

$$\prod_{k=1}^{1} k = 1, \quad \prod_{k=1}^{2} k = 1 \times 2 = 2, \quad \prod_{k=1}^{3} k = 1 \times 2 \times 3 = 6, \ldots$$

Assim, dum modo geral, $\prod_{k=1}^{n} k$ é o produto $1 \times 2 \times \ldots \times n$ dos *n* primeiros números naturais. Este produto é chamado *factorial de* n e representa-se por $n!$. Será, pois, *por definição:*

$$n! = \prod_{k=1}^{n} k, \quad \forall\, n \in \mathbb{N}.$$

9. **Divisão exacta.** Da monotonia da multiplicação deduz-se, tal como para a adição, a PROPRIEDADE DO CORTE:

$$ac = bc \Rightarrow a = b, \quad \forall a,\ b,\ c \in \mathbb{N}.$$

A demonstração é perfeitamente análoga à que se fez para a adição. Daqui, por sua vez, deduz-se:

COROLÁRIO. *Dados dois números naturais,* a, n, *não pode existir mais de um número natural* x *tal que* $n x = a$. *Simbolicamente:*

$$n x = a \wedge n y = a \Rightarrow x = y \quad (\text{em } \mathbb{N})$$

Por outro lado, demonstra-se que o *produto de dois números naturais é sempre superior ou igual a qualquer dos factores* (igual, só quando um, pelo menos, dos factores é 1). Simbolicamente:

(1) $$n\,x \geqslant n, \quad \forall\, n, x \in \mathbb{N}$$

Estas propriedades ajudam-nos a estudar o seguinte problema:

Dados dois números $a, n \in \mathbb{N}$, *determinar um número* $x \in \mathbb{N}$, *tal que* $n\,x = a$.

A propriedade (1) diz-nos que a condição $a \geqslant n$ é *necessária* para que o problema seja possível (ou resolúvel). Porém, tal condição não é suficiente: p. ex. temos $5 > 3$ e não existe nenhum número natural x tal que $3\,x = 5$.

Por outro lado, o anterior corolário da propriedade do corte diz-nos que, *quando o problema é resolúvel, tem uma única solução.* Neste caso, diz-se que *a é divisível por* n (ou múltiplo de n), e o número x tal que $n\,x = a$ é chamado o *quociente exacto de* a *por* n e representado por qualquer das notações:

$$\frac{a}{n}, \quad a/n \quad \text{ou} \quad a:n \text{ (1)}$$

Por exemplo, $\frac{6}{3} = 2$, visto que $3 \times 2 = 6$.

Na referida hipótese, chama-se *divisão exacta* a operação que faz corresponder ao par ordenado (a, n) o número a/n (*a* é então chamado o *dividendo* e n o *divisor)*. Como se viu, *a divisão exacta não é sempre possível, mas, quando possível, é unívoca em* $\mathbb{N}$. Além disso, a divisão não é comutativa nem associativa: p. ex. $(24:6):2 \neq 24:(6:2)$. Mas é *crescente à direita* e *decrescente à esquerda* (isto é, *o quociente aumenta quando o dividendo aumenta e diminui quando o divisor aumenta).*

---

(1) A última destas notações, para designar o quociente, tende a cair em desuso.

10. **Multiplicação em $\mathbb{N}_0$.** Por definição:

(1) $$0 \times a = 0, \quad \forall a \in \mathbb{N}_0$$

Com esta definição suplementar a multiplicação definida em $\mathbb{N}$ é estendida a $\mathbb{N}_0$, continuando a ser *sempre possível, unívoca, associativa, comutativa e distributiva a respeito da adição*. Porém, a propriedade da monotonia é alterada; é claro que temos agora, em $\mathbb{N}_0$:

$$a < h \Rightarrow ac < bc, \quad \text{sse} \quad c \neq 0$$

A proposição (1) (definição) exprime-se dizendo que 0 é *elemento absorvente* da multiplicação.

Consideremos, agora, o problema da divisão exacta em $\mathbb{N}_0$: *Dados* $a, n \in \mathbb{N}_0$, *achar* $x \in \mathbb{N}^0$ *tal que* $nx = a$. Há, agora, a distinguir 4 casos:

Se $a \neq 0$ e $n \neq 0$, estamos no caso anterior (em $\mathbb{N}$).

Se $a = 0$ e $n \neq 0$, o problema é possível e determinado: $x = 0$.

Se $a \neq 0$ e $n = 0$, o problema é impossível, visto que então $nx = 0$, $\forall x \in \mathbb{N}_0$.

Se $a = 0$ e $n = 0$, o problema é possível mas *indeterminado:* qualquer $x \in \mathbb{N}_0$ verifica a condição $nx = a$.

11. **Números infinitos.** O conceito de *número de elementos* dum conjunto A, tal como foi definido no n.º 1 deste Capítulo, não se limita ao caso em que A é finito.

Em qualquer hipótese, o número de elementos dum conjunto A (também chamado *potência de* A, *número cardinal de* A ou simplesmente *cardinal de* A) é designado pela notação $\#$ A. Assim, por definição:

$$\# A = \# B \Leftrightarrow A \text{ é equipotente a } B$$

Diz-se que o número de elementos de A é *infinito*, sse A é infinito. Por exemplo, # $\mathbb{N}$ é infinito.

Por outro lado, escreve-se $\# A < \# B$, sse A é equipotente a uma parte B, *mas não a* B. Esta definição desde logo implica a propriedade anti-reflexiva da relação $<$:

$$a < b \Rightarrow a \neq b.$$

Vimos atrás que a inclusão estrita entre conjuntos A e B *finitos* se traduz na relação $<$ entre números, isto é:

$$A \subset B \wedge A \neq B \Rightarrow \# A < \# B$$

Quer isto dizer que o *número de elementos dum conjunto finito é sempre maior que o número de elementos de uma sua parte estrita.* É este um facto que *induzimos* da nossa experiência quotidiana sobre conjuntos finitos, e que se exprime em linguagem comum dizendo: 'O todo é sempre maior que qualquer parte (estrita)'.

Porém, logo no primeiro contacto com os conjuntos infinitos surge-nos um facto surpreendente:

Se A *é um conjunto infinito, existe pelo menos uma sua parte estrita, cujo número de elementos é igual ao de* A.

Consideremos por exemplo o conjunto $\mathbb{N}$ e designemos por P o conjunto dos números pares positivos (2, 4, 6, ...). Temos então evidentemente $P \subset N$ e $P \neq N$. Porém, se fizermos corresponder a cada número natural n o número par 2n (o dobro de n), conforme o seguinte esquema:

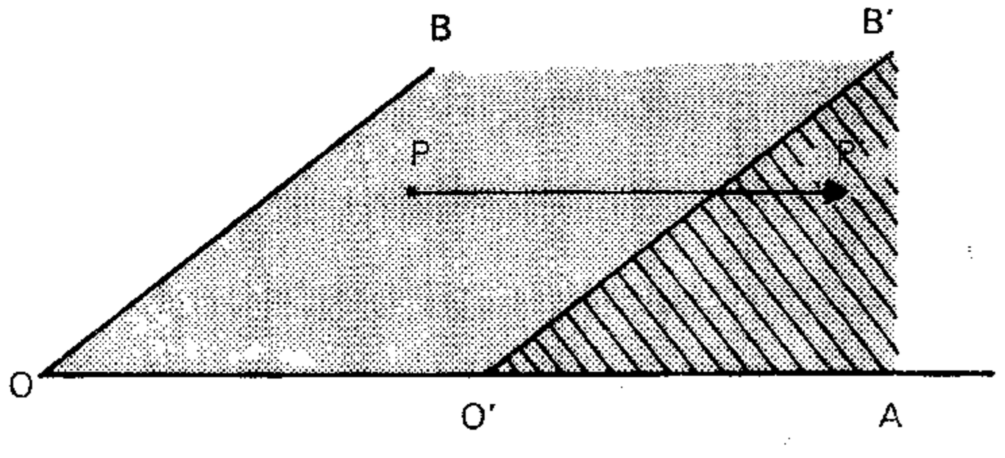
$$\begin{array}{lccccccc}
\mathbb{N}: & 1 & 2 & 3 & 4 & \cdots & n & \cdots \\
 & \downarrow & \downarrow & \downarrow & \downarrow & & \downarrow & \\
P: & 2 & 4 & 6 & 8 & \cdots & 2n & \cdots
\end{array}$$

é fácil ver que fica assim definida uma correspondência biunívoca entre os conjuntos $\mathbb{N}$ e P. Com efeito, a *todo o* $n \in \mathbb{N}$ corresponde *um e um só* $m \in P$, que é $m = 2n$. Reciprocamente, para *todo o* $m \in P$, existe *um e um só* $n \in \mathbb{N}$ tal que $2n = m$ e que é $n = m/2$. Por conseguinte, temos:

$$\# P_2 = \# \mathbb{N}$$

apesar de P *ser uma parte estrita de* $\mathbb{N}$. Analogamente se prova que $\mathbb{N}$ é equipotente ao *conjunto dos números naturais ímpares, ao conjunto dos números naturais múltiplos de* 3, etc., etc..

Outro exemplo. Consideremos um ângulo convexo A Ô B; este é uma das partes em que fica dividido um plano por duas semi-rectas com origem comum, portanto um conjunto *infinito* de pontos.



Sabe-se que é possível, de muitas maneiras, passar ao ângulo A Ô' B' *contido estritamente no primeiro, por meio duma translação;* este facto é-nos sugerido intuitivamente pelo exemplo dum esquadro que desliza ao longo duma régua. Ora, é fácil ver que essa translação faz corresponder a cada ponto P do primeiro ângulo um determinado ponto P' do segundo e que fica assim estabelecida uma correspondência biunívoca entre os dois conjuntos de pontos. *Logo o número de pontos do conjunto* A Ô B *é igual ao número de pontos da sua parte estrita* A Ô' B'.

Recordemos que, no Cap. I, n.º 8, tínhamos renunciado a dar uma definição de 'conjunto finito'. Pois bem: uma definição de 'conjunto finito', adoptada por muitos matemáticos, é precisamente a seguinte:

DEFINIÇÃO. *Diz-se que um conjunto A é finito, sse não existe nenhuma parte estrita de A equipotente a A.*

(Subentende-se nesta definição que o conjunto vazio não é equipotente a nenhum conjunto não vazio).

Convém, desde já, notar que existem *diferentes* números infinitos. Assim, provaremos mais adiante que o número de elementos de $\mathbb{N}$ é *menor* que o número de elementos de $\mathbb{R}$ (conjunto dos números reais), isto é:

$$\# \mathbb{N} < \# \mathbb{R}$$

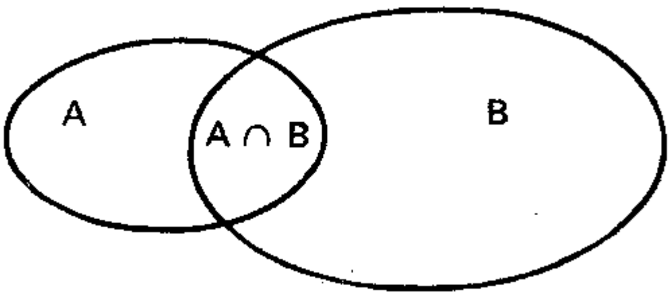
Existem números maiores que $\# \mathbb{R}$, mas presume-se (embora ninguém o tenha demonstrado) que não existe nenhum número *a* compreendido estritamente entre $\# \mathbb{N}$ e $\# \mathbb{R}$. Por outro lado, demonstra-se que $\# \mathbb{N}$ *é o menor de todos os números cardinais infinitos que se possam apresentar.* Este número é designado pelo símbolo $\aleph_0$, em que o sinal $\aleph$ é a primeira letra maiúscula do alfabeto hebraico (lê-se 'alefa').

12. **Objecto do cálculo combinatório. Número de elementos da reunião de dois ou mais conjuntos.** O cálculo combinatório tem por objecto o estudo de problemas relativos ao número de elementos de diferentes conjuntos que podem ser obtidos a partir de conjuntos dados, por meio de operações lógicas, tais como a reunião, a intersecção, a multiplicação cartesiana, etc. No estudo do cálculo combinatório limitar-nos-emos a conjuntos finitos, embora esse estudo

se possa estender a conjuntos infinitos. Começaremos pelo caso da reunião e da intersecção.

Já vimos que dados dois conjuntos A e B (finitos), se tem, por definição:

$$\# (A \cup B) = \# A + \# B, \quad \text{se} \quad A \cap B = \emptyset$$



Porém, se a intersecção de A com B não é vazia, esta fórmula deixa de ser válida. Suponhamos, por exemplo, que A representa o conjunto dos habitantes duma dada cidade que são *empregados do Estado* e B o conjunto dos habitantes da mesma cidade que são *empregados de entidades particulares*. Então será $A \cup B$ o conjunto dos habitantes dessa cidade que estão empregados. Mas não podemos, sem mais, escrever, neste caso:

$$\# (A \cup B) = \# A + \# B,$$

pois pode haver elementos comuns a A e a B, que são contados duas vezes. A fórmula correcta será, então, como é fácil ver:

$$\# (A \cup B) = \# A + \# B - \# (A \cap B)$$

Representando a reunião $A \cup B$ por $A + B$ e a intersecção $A \cap B$ por $A\,B$, como se faz muitas vezes, a fórmula anterior escreve-se:

$$\# (A + B) = \# A + \# B - \# (A\,B)$$

Consideremos, agora, três conjuntos finitos A, B e C quaisquer. Como exercício, pode verificar-se que:

$$\# (A + B + C) = \# A + \# B + \# C - \# (AB) - \# (AC) - - \# (BC) + \# (ABC)$$

No caso geral de *n* conjuntos finitos $A_1, \ldots, A_n$ quaisquer, chega-se à fórmula:

$$\# \left(\sum_{i=1}^{n} A_i \right) = \sum_{i=1}^{n} \# A_i - \sum_{1 \leqslant i < j}^{n} \# (A_i A_j) +$$

$$+ \sum_{1 \leqslant i < j < k}^{n} \# (A_i A_j A_k) - \ldots + (-1)^{n-1} \# (A_1 A_2 \ldots A_n)$$

Esta, que apresentamos aqui apenas a título de curiosidade, pode ser chamada FÓRMULA DE DANIEL DA SILVA, pois foi o matemático português Daniel da Silva, do século passado, quem a introduziu, embora sob forma diversa, no seu trabalho *Propriedades gerais e resolução directa das congruências binómias; introdução à teoria dos números.*

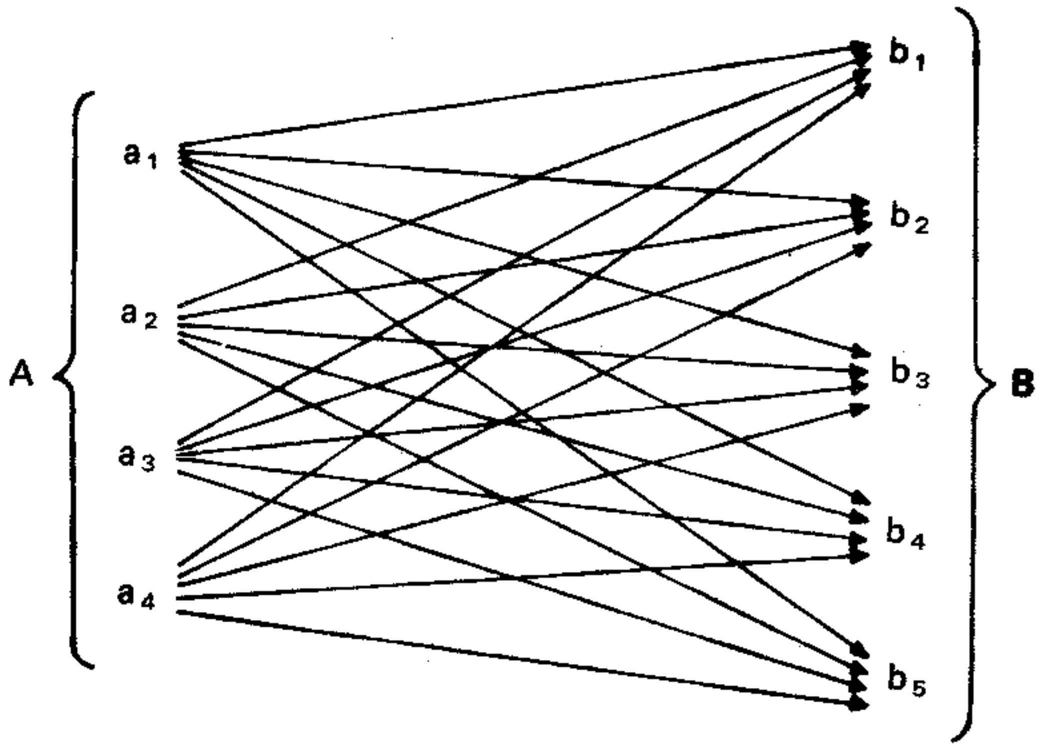
13. **Número de elementos do produto cartesiano de dois ou mais conjuntos.** Comecemos por um exemplo simples. Suponhamos que numa sala de baile se encontram 4 rapazes, que designaremos por a_1, a_2, a_3, a_4, e 5 raparigas, que designaremos por b_1, b_2, b_3, b_4, b_5. Ponhamos:

$$A = \{a_1, a_2, a_3, a_4\}$$

$$B = \{b_1, b_2, b_3, b_4, b_5\}$$

Quantos pares diferentes se podem formar, ao todo, sendo cada par constituído por um rapaz e uma rapariga?

É claro que se pede aqui o número de elementos do conjunto $A \times B$. Este produto cartesiano pode ser obtido como se descreve no seguinte diagrama, em que cada seta indica um par ordenado (em primeiro lugar um rapaz e em segundo uma rapariga):



De maneira mais sistemática, os pares ordenados podem ser obtidos como se indica na seguinte tabela de duas entradas:

$A \times B$

A \ B	b_1	b_2	b_3	b_4	b_5
a_1	a_1b_1	a_1b_2	a_1b_3	a_1b_4	a_1b_5
a_2	a_2b_1	a_2b_2	a_2b_3	a_2b_4	a_2b_5
a_3	a_3b_1	a_3b_2	a_3b_3	a_3b_4	a_3b_5
a_4	a_4b_1	a_4b_2	$e\ {}_4b_3$	a_4b_4	a_4b_5

Como se vê, para maior simplicidade, usámos aqui a notação '$a_j\ a_k$' para designar cada par ordenado (a_j, a_k).

Quanto aos números de elementos de A × B, o cálculo é bem simples. Cada rapaz pode figurar em 5 pares diferentes, visto haver 5 raparigas; portanto, como há 4 rapazes, podem formar-se ao todo 4 × 5 pares diferentes. O número pedido é, pois, 20.

Sejam agora A e B dois conjuntos finitos quaisquer, não vazios, e seja m = # A, n = # B. Como B tem *n* elementos, cada elemento de A dá origem exactamente a *n* pares diferentes de A × B. Portanto, como A tem *m* elementos, será m × n o número de elementos de A × B.

Se um, pelo menos, dos conjuntos A e B é vazio, é claro que nenhum par pode ser formado e assim A × B também é vazio. Por conseguinte, quaisquer que sejam os conjuntos finitos A e B, temos sempre:

$$\# (A \times B) = \# A \times \# B$$

Esta fórmula é mesmo adoptada, por muitos autores, para definição de produto de números. Tal definição permite dar demonstrações intuitivas das propriedades comutativa e distributiva da multiplicação. Assim, para a *propriedade comutativa,* basta observar que, fazendo corresponder a cada elemento (a, b) de A × B o elemento (b, a) de B × A, se estabelece uma correspondência biunívoca entre A × B e B × A, e portanto:

$$\# (A \times B) = \# (B \times A) = \# B \times \# A$$

Quanto à *propriedade distributiva,* é fácil ver que, sendo A, B e C conjuntos finitos quaisquer, se tem:

$$(A \cup B) \times C = (A \times C) \cup (B \times C)$$

e que, se A e B são disjuntos, também $A \times C$ e $B \times C$ são disjuntos (exemplifique com $A = \{a_1, a_2, a_3\}$, $B = \{b_1, b_2\}$ e $C = \{c_1, c\ , c_3, c_4\}$). Portanto, se pusermos $\# A = m$, $\# B = n$, $\# C = p$, virá:

$$(m + n)p = mp + np$$

Para a *propriedade associativa,* temos de recorrer ao conceito de produto cartesiano de três conjuntos. Sejam A, B e C três conjuntos finitos quaisquer; já sabemos que:

$$A \times B \times C = \{ (x, y, z) : x \in A, y \in B, z \in C \}$$

Mas, é claro que os ternos ordenados (x, y, z) podem ser obtidos associando a cada par (x, y) de $A \times B$ um elemento z de C. Fica, assim, manifestamente definida uma *correspondência biunívoca:*

$$((x, y), z) \rightarrow (x, y, z)$$

entre $(A \times B) \times C$ e $A \times B \times C$, visto que, a cada elemento ((x, y), z) de $(A \times B) \times C$ corresponde um e um só elemento (x, y, z) de $A \times B \times C$ e, reciprocamente, cada elemento (x, y, z) de $A \times B \times C$ corresponde, deste modo, a um único elemento ((x, y), z) de $(A \times B) \times C$. Analogamente se estabelece uma correspondência biunívoca entre $A \times (B \times C)$ e $A \times B \times C$. Portanto, se pusermos $\# A = m$, $\# B = n$, $\# C = p$, será:

$$\# (A \times B \times C) = \# (A \times B) \times \# C = (m\,n)\,p$$

$$\# (A \times B \times C) = \# A \times \# (B \times C) = m\,(n\,p)$$

donde $(m\,n)\,p = m\,(n\,p)$. Ao mesmo tempo se vê que:

$$\boxed{\# (A \times B \times C) = \# A \times \# B \times \# C}$$

É claro que este resultado pode ser estendido a um número natural *n* qualquer de conjuntos finitos, $A_1, \ldots, A_n$. Será, então:

$$\# \ (A_1 \times A_2 \times \ldots \times A_n) = \# A_1 \times \# A_2 \times \ldots \times \# An$$

ou seja, em notação mais correcta:

$$\# \prod_{j=1}^{n} A_j = \prod_{j=1}^{n} \# A_j$$

Em particular, os *n* conjuntos A_j podem ser todos um mesmo conjunto A. Neste caso, o seu produto cartesiano é A^n e tem-se:

$$\# A^n = (\# A)^n$$

EXEMPLOS:

I. Um cofre tem três discos, cada um com as mesmas 24 letras, e só pode ser aberto quando se coloca uma determinada letra de cada um dos discos numa determinada posição. Supondo que se ignora o segredo do cofre, de quantas maneiras diferentes se podem colocar as letras dos discos nas referidas posições?

É evidente que as *maneiras diferentes de colocar as letras* são dadas por todas as sequências de 3 letras escolhidas no conjunto das 24 letras consideradas. Designemos por $\mathcal{A}$ este conjunto; será então $\mathcal{A}^3$ o conjunto de todas as referidas sequências e assim o número pedido será:

$$\# \mathcal{A}^3 = (\# \mathcal{A})^3 = 24^3 = 138247$$

II. Quantos números diferentes de 5 algarismos se podem representar com os algarismos 1, 3, 9, no sistema decimal?

É claro que os referidos números, tais como 1 9 3 9 1, 9 1 3 1 9, 1 1 1 1 1, etc., estão em correspondência biunívoca com as sequências de 5 algarismos, escolhidos entre os três algarismos 1, 3, 9.

Designando por A o conjunto destes algarismos, será A^5 o conjunto das referidas sequências e, portanto, será:

$$\# A^5 = (\# A)^5 = 3^5 = 243$$

III. Quantos números diferentes de 4 algarismos se podem representar com os algarismos 0, 2, 4, 6, 8, no sistema decimal?

O problema, agora, é ligeiramente mais difícil, porque não há expressões decimais de números que comecem por 0. Assim, designando por A o conjunto dos algarismos 2, 4, 6, 8 e por B o conjunto dos algarismos 0, 2, 4, 6, 8, o número pedido será:

$$\# (A \times B^3) = (\# A) \times (\# B)^3 = 4 \times 5^3 = 500$$

Um problema análogo será o seguinte:

Quantos números inferiores a 10 000 se podem representar, no sistema decimal, com os algarismos 0, 2, 4, 6, 8?

Muitos outros problemas, relativos aos mais diversos domínios, se podem resolver aplicando os resultados anteriores sobre produtos cartesianos.

14. Número de subconjuntos dum conjunto finito. Sendo A um conjunto qualquer, designa-se por $\mathcal{P}$ (A) o conjunto de todos os subconjuntos de A, isto é, simbolicamente:

$$\mathcal{P}(A) = \{X : X \subset A\}$$

Entre os conjuntos pertencentes a $\mathcal{P}$ (A) figuram o conjunto vazio e o próprio conjunto A (recordemos que $\mathcal{P}$ (A) é um conjunto de tipo 2 em relação a A).

Quando A é finito, a contagem dos elementos de $\mathcal{P}$ (A) pode fazer-se de maneira simples, aplicando a teoria do produto cartesiano.

Com efeito, se for $\# A = n$, podemos dispor os elementos de A numa sequência de *n* elementos distintos:

$$a_1 \; a_2 \; \ldots \; a_n$$

Nestas condições, todo o subconjunto C de A pode ser definido, fazendo corresponder a cada elemento a_i de A o número 1 ou o número 0, conforme $a_i \in C$ ou $a_i \notin C$. Assim, cada subconjunto C de A fica representado por uma sequência de n elementos do conjunto $\{0, 1\}$. Por exemplo, se $n = 4$, as sequências

$$0\,1\,1\,0, \quad 1\,0\,0\,1, \quad 1\,1\,1\,1, \quad 0\,0\,0\,0,$$

representam, respectivamente, os conjuntos:

$$\{a_2, a_3\}, \; \{a_1, a_4\}, \; \{a_1, a_2, a_3, a_4\} = A, \; \varnothing$$

Tornando ao caso geral, é evidente que, por este processo, fica estabelecida uma correspondência biunívoca entre os subconjuntos de A e as sequências de *n* elementos de $\{0, 1\}$, isto é, entre $\mathcal{P}(A)$ e $\{0, 1\}^n$. O número de elementos de $\mathcal{P}(A)$ será igual ao de $\{0, 1\}^n$ ou seja 2^n. Assim, para todo o conjunto finito A, será

$$\boxed{\# \mathcal{P}(A) = 2^{\# A}}$$

Este facto leva alguns autores a designarem pelo símbolo 2^A o conjunto $\mathcal{P}(A)$.

EXERCÍCIO. Calcular o número total de relações binárias que se podem definir num conjunto finito A com *n* elementos. Deduzir daí o número de relações binárias (e portanto de operações binárias) que se podem definir no conjunto $\{V, F\}$ dos valores lógicos. Respostas: 2^{n^2}, 16.

15. **Arranjos e permutações.** Consideremos o seguinte problema:

Dispondo de peças de pano de 4 cores diferentes e desejando fazer bandeiras tricolores com faixas de pano verticais, quantas bandeiras diferentes se podem obter?

Subentende-se, neste enunciado, que duas bandeiras são diferentes, se e só se é verificada uma das duas seguintes condições: *a*) as bandeiras não têm as mesmas cores; *b*) as bandeiras são formadas pelas mesmas cores em ordem diferente, relativamente à haste. Torna-se então evidente que o problema consiste em contar as *sequências de* 3 *cores diferentes,* escolhidas entre as 4 que são dadas. Assim, se designarmos estas cores por a, b, c, d, as sequências:

a b c, a b d, d a b, b c a, etc.

representam bandeiras tricolores diferentes, como se pretende; ao passo que as sequências

a b a, a c c, b b b, etc.

não interessam ao problema. Ora bem:

DEFINIÇÃO. *Dá-se o nome de arranjos às sequências constituídas por elementos todos distintos (isto é, às sequências em que não figurem elementos repetidos).*

Note-se que as sequências também são chamadas *arranjos com possível repetição* ou *arranjos completos.*

Assim, o problema anterior consiste em determinar o número total dos arranjos formados por 3 cores entre as 4 cores dadas. Para isso, comecemos por considerar os arranjos com *uma só* cor, evidentemente em número de 4:

a, b, c, d

Notemos, agora, que se pode passar dos arranjos com uma cor para *todos* os arranjos com 2 cores, colocando sucessivamente, à direita de cada um dos primeiros, *uma das cores restantes,* cujo número é 4 - 1 = 3. Assim, os 4 primeiros dão origem a 4 × 3 arranjos com 2 cores:

$$\begin{tikzcd}[row sep=small] & ab \\ a \arrow[ur] \arrow[r] \arrow[dr] & ac \\ & ad \end{tikzcd} \quad \begin{tikzcd}[row sep=small] & ba \\ b \arrow[ur] \arrow[r] \arrow[dr] & bc \\ & bd \end{tikzcd} \quad \begin{tikzcd}[row sep=small] & ca \\ c \arrow[ur] \arrow[r] \arrow[dr] & cb \\ & cd \end{tikzcd} \quad \begin{tikzcd}[row sep=small] & da \\ d \arrow[ur] \arrow[r] \arrow[dr] & db \\ & dc \end{tikzcd}$$

Analogamente, podemos passar dos arranjos com 2 cores para *todos* os arranjos com 3 cores, colocando sucessivamete, à direita de cada um dos primeiros, uma das cores que *nele não figuram,* e cujo número é 4 - 2 = 2. Assim, os 4 × 3 arranjos com 2 cores dão origem a 4 × 3 × 2 arranjos com 3 cores:

$$\begin{tikzcd}[row sep=small] & abc \\ ab \arrow[ur] \arrow[dr] & \\ & abd \end{tikzcd} \quad \begin{tikzcd}[row sep=small] & acb \\ ac \arrow[ur] \arrow[dr] & \\ & acd \end{tikzcd} \quad \begin{tikzcd}[row sep=small] & adc \\ ad \arrow[ur] \arrow[dr] & \\ & adb \end{tikzcd}$$

$$\begin{tikzcd}[row sep=small] & bac \\ ba \arrow[ur] \arrow[dr] & \\ & bad \end{tikzcd} \quad \begin{tikzcd}[row sep=small] & bca \\ bc \arrow[ur] \arrow[dr] & \\ & bcd \end{tikzcd} \quad \begin{tikzcd}[row sep=small] & bda \\ bd \arrow[ur] \arrow[dr] & \\ & bdc \end{tikzcd}$$

$$\begin{tikzcd}[row sep=small] & cab \\ ca \arrow[ur] \arrow[dr] & \\ & cad \end{tikzcd} \quad \begin{tikzcd}[row sep=small] & cba \\ cb \arrow[ur] \arrow[dr] & \\ & cbd \end{tikzcd} \quad \begin{tikzcd}[row sep=small] & cda \\ cd \arrow[ur] \arrow[dr] & \\ & cdb \end{tikzcd}$$

$$\begin{tikzcd}[row sep=small] & dab \\ da \arrow[ur] \arrow[dr] & \\ & dac \end{tikzcd} \quad \begin{tikzcd}[row sep=small] & dba \\ db \arrow[ur] \arrow[dr] & \\ & dbc \end{tikzcd} \quad \begin{tikzcd}[row sep=small] & dca \\ dc \arrow[ur] \arrow[dr] & \\ & dcb \end{tikzcd}$$

E como não pode haver, evidentemente, outros arranjos com 3 cores, o número pedido será $4 \times 3 \times 2 = 24$. (Recordemos que o número total de sequências de 3 cores é $4 \times 4 \times 4 = 64$).

Este raciocínio pode estender-se ao caso geral. Dados dois números naturais n, p, tais que $p \leqslant n$, *o número total de arranjos que se podem formar com* p *elementos escolhidos entre os* n *elementos dum dado conjunto* U é designado pelo símbolo

$$^{n}A_{p}$$

que se lê '*número de arranjos de* n *elementos tomados* p *a* p' ou simplesmente '*arranjos de* n, p *a* p'. Comecemos por considerar os arranjos com um só elemento, escolhido entre os *n* elementos do conjunto U; o número destes arranjos é, evidentemente:

$$^{n}A_{1} = n$$

Seja agora k qualquer número natural tal que $1 \leqslant k \leqslant p$. Se já tivermos obtido *todos* os arranjos com k elementos e se $k < p$, é claro que obtemos *todos* os arranjos com $k + 1$ elementos, colocando à direita de cada um dos primeiros um dos *n* elementos que *nele ainda não figuram* e cujo número é $n - k$. Assim, cada arranjo com k elementos dá origem a $n - k$ arranjos com $k + 1$ elementos, e, portanto:

$$^{n}A_{k+1} = {}^{n}A_{k} \times (n - k)$$

Fazendo sucessivamente $k = 1, 2, \ldots, p - 1$, virá:

$$^{n}A_{2} = {}^{n}A_{1} \times (n - 1),\ {}^{n}A_{3} = {}^{n}A_{2} \times (n - 2),\ \ldots,$$
$$^{n}A_{p} = {}^{n}A_{p-1} \times [n - (p - 1)]$$

Daqui, por substituições sucessivas, lembrando que $^{n}A_{1} = n$ e que $n - (p-1) = n - p + 1$, vem finalmente:

$$^{n}A_{p} = n\,(n - 1)\,(n - 2)\,\ldots\,(n - p + 1)$$

ou, em notação mais correcta:

(1) $$\boxed{{}^{n}A_{p} = \prod_{k=o}^{p-1} (n\text{-}k)} \qquad (n,\ p \in \mathbb{N},\ p \leqslant n)$$

Esta fórmula pode traduzir-se dizendo:

O número de arranjos de n *elementos* p *a* p *é igual ao produto de* p *números naturais consecutivos a partir de* n *em ordem decrescente.*

Por exemplo:

$$ {}^{6}A_{4} = \underbrace{6 \times 5 \times 4 \times 3}_{4 \text{ factores}} = 360$$

Recordemos que o número de sequências com 4 elementos é $6 \times 6 \times 6 \times 6 = 6^4 = 1296$. A diferença vem, como vimos, do facto de os arranjos serem sequências com elementos todos diferentes. Dum modo geral, dados dois números naturais, n, p quaisquer (podendo agora ser $p > n$ ou $p \leqslant n$) designaremos pelo símbolo:

$${}^{n}A'p \quad (\text{ler } '\textit{arranjos completos de } n,\ p \textit{ a } p)$$

o número total de sequências que se podem formar com p elementos escolhidos entre *n* elementos dum conjunto dado. Será, pois:

$${}^{n}A'_{p} = n^{p} \qquad (\forall\ n,\ p \in \mathbb{N})$$

Na fórmula (1) pode acontecer em particular que se tenha $n = p$. Então, obtém-se:

$${}^{n}A_{n} = \prod_{k=o}^{r-1} (n-k) = n \times (n-1) \times \ldots \times 2 \times 1$$

$$= 1 \times 2 \times \ldots \times (n-1) \times n = \prod_{j-1}^{n} j$$

Ora, já vimos (pág. 152) que o produto dos *n* primeiros números naturais, se chama *factorial de* n e se designa pelo símbolo n!. Assim:

$$^{n}A_{n} = n!$$

DEFINIÇÃO. *Chama-se permutação dum conjunto finito* U *qualquer arranjo que se possa formar com todos os elementos de* U.

O número total de permutações dum conjunto de *n* elementos é representado pelo símbolo P_n, que se lê 'permutações de *n*'. Assim:

$$\boxed{P_n = {}^{n}A_n = n!}$$

Para exemplo e exercícios, ver *Compêndio de Álgebra*(1), 7.º *ano*, última edição.

16. **Combinações.** Sobre este assunto, seguir o referido *Compêndio.*

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

Índice

Composto e impresso na
Tipografia Guerra — Viseu
e concluiu-se
em Dezembro de 1974

GABINETE DE ESTUDOS E PLANEAMENTO
DO MINISTÉRIO DA EDUCAÇÃO E CULTURA