1 Introdução à Lógica e Teoria de Conjuntos

1.1 Teoria de Conjuntos

Um conjunto designa-se geralmente por uma letra maiúscula, reservando-se as letras minúsculas para os seus elementos. A expressão simbólica

$$x \in A$$

significa que "x *é elemento de* A". A negação de $x \in A$ representa-se simbolicamente por

$$x \notin A$$

E lê-se "x *não pertence a* A" (ou "x não *é elemento de* A").

Um conjunto pode ser escrito em **extensão** (quando o número dos seus elementos for finito e suficientemente pequeno) enumerando explicitamente todos os seus elementos colocados entre chavetas e separados por vírgulas ou em **compreensão**, enunciando uma propriedade caracterizadora dos seus elementos (isto é, uma propriedade que só os seus elementos possuam).

Exemplo TC1

(1) Conjunto das vogais descrito em extensão,

$$V=\{a,e,i,o,u\}$$

(2) Conjunto dos números naturais pares descrito em compreensão

$$P = \{ p \in \mathbb{N} : p = 2q \text{ para algum } q \in \mathbb{N} \}$$

Conjunto universal e conjunto vazio

Pareceria razoável que intuitivamente se considerasse como conjunto qualquer colecção de objectos (reais ou imaginários). No entanto, tal atitude conduz a situações paradoxais.

Se se adoptar a concepção intuitiva de conjunto então pode dizer-se que alguns conjuntos são membros de si próprios enquanto que outros não o são. Um conjunto de elefantes, por exemplo, não é um elefante e, portanto, não é um elemento de si próprio; no entanto, o conjunto de todas as ideias abstractas é, ele próprio, uma ideia abstracta, pelo que pertence a si próprio. As propriedades "*ser membro de si próprio*" e "*não ser membro de si próprio*" parecem ser propriedades perfeitamente adequadas para definir conjuntos. Mas, como se verá estas propriedades conduzem à criação de um paradoxo.

Suponha-se que se define o conjunto A como sendo o conjunto de todos os conjuntos que não são membros de si próprio, isto é,

$$A = \{\mathrm{X} : \mathrm{X} \notin \mathrm{X}\}.$$

Coloca-se a questão de saber se A é ou não elemento de si próprio. Se A não for elemento de si próprio, $A \notin A$, então satisfaz a propriedade definidora de A e, portanto, $A \in A$; se A pertence a si próprio, $A \in A$ então não satisfaz a propriedade definidora de A e, portanto, $A \notin A$. De cada uma das possíveis hipóteses pode deduzir-se a sua negação, o que constitui um paradoxo.

Para eliminar possibilidades deste tipo supor-se-á, de ora em diante, que os conjuntos considerados são todos constituídos por elementos de um conjunto U suficientemente grande, chamado **conjunto universal** ou universo do discurso.

Em Matemática há conjuntos que constituem muito frequentemente os universos do discurso. Alguns exemplos, dos mais importantes, são:

$\mathbb{R} = \{x : x \text{ é um número real}\}$ número

$\mathbb{Q} = \{x : x \text{ é um número racional}\}$

$\mathbb{Z} = \{x : x \text{ é um número inteiro}\}$

$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$

Os símbolos $\varnothing$ ou **{ }** usam-se para denotar o **conjunto vazio** (conjunto sem elementos) que pode ser escrito em compreensão por $\{x : x \neq x\}$, $\varnothing = \{x : x \neq x\}$.

Conjuntos finitos e conjuntos infinitos

Um conjunto diz-se **finito** se for possível contar os seus elementos, ou seja, se for o conjunto vazio ou se for possível estabelecer uma correspondência bijectiva entre os seus elementos e os elementos de um conjunto da forma $\{1, 2, 3, \ldots, n\}$ para algum $n \in \mathbb{N}$. Dir-se-á **infinito** caso contrário. O conjunto dos números inteiros positivos inferiores a 100 é um conjunto finito enquanto que o conjunto de todos os números inteiros positivos é um conjunto infinito.

Se A for um conjunto finito, designar-se-á por **cardinalidade de** A o número dos seus elementos, o qual se representa por **card(** A **)** ou $\#A$. Um conjunto com cardinalidade igual a 1 diz-se **singular**.

Quando um conjunto é infinito, é impossível defini-lo em extensão; logo, se um conjunto puder ser definido em extensão, então certamente será um conjunto finito.
Por vezes para definir certos conjuntos infinitos usa-se uma notação parecida com a definição de um conjunto em extensão: é o caso de

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$$

Refira-se que as reticências representam a quase totalidade dos elementos de $\mathbb{N}$ qualquer que seja o número de elementos que apareçam no início.

Igualdade de conjuntos

Dois conjuntos são iguais se e só se tiverem os mesmos elementos.

Se um conjunto A for igual a um conjunto B escreve-se $A = B$. Para verificar se dois conjuntos são iguais basta verificar se todo o elemento de A é elemento de B e se todo o elemento de B é elemento de A. Se todo o elemento de A for também elemento de B (independentemente do facto de todo o elemento de B poder ser ou não elemento de A) dir-se-á que o conjunto A **está contido** no conjunto B, o que se denota por $A \subseteq B$; neste caso também se diz que A é um subconjunto de B. Se os conjuntos A e B forem iguais então ter-se-á $A \subseteq B$ e, simultaneamente $B \subseteq A$; reciprocamente, se $A \subseteq B$ e $B \subseteq A$ se verificarem simultaneamente então tem-se $A = B$. Se $A \subseteq B$ e $A \neq B$ dir-se-á que A é um subconjunto próprio ou uma parte própria de B e escreve-se $A \subset B$. De acordo com estas definições resulta que quaisquer que sejam os conjuntos A e B

$$\varnothing \subseteq A, \quad A \subseteq A, \quad A = B \text{ se e só se } \left[A \subseteq B \text{ e } B \subseteq A \right]$$

Considere-se a prova de, por exemplo, $\varnothing \subseteq A$ qualquer que seja o conjunto A. A única forma de mostrar que esta inclusão é falsa é verificar que $\varnothing$ possui um elemento que não pertence a A; ora como $\varnothing$ não possui elementos então esta relação verifica-se sempre.

1.1.1 Operações com conjuntos

Sendo A e B dois conjuntos, denota-se por $A \cup B$ a **união** (ou **reunião**) de A com B, que é o conjunto cujos elementos são os elementos de A e os elementos de B. Mais geralmente, se $A_1, A_2, \ldots, A_n$ forem conjuntos então a sua união

$$\begin{aligned} \bigcup_{i=1}^{n} A_i &= A_1 \cup A_2 \cup \ldots \cup A_n \\ &= \left\{ x : x \in A_i \text{ para algum } i = 1, 2, \ldots, n \right\} \end{aligned}$$

é o conjunto constituído pelos elementos que pertencem pelo menos a um dos conjuntos A_i, $i = 1, 2, \ldots, n$.

A **intersecção** de dois conjuntos A e B, denota-se por $A \cap B$, é o conjunto cujos elementos pertencem simultaneamente a A e B. Analogamente, se $A_1, A_2, \ldots, A_n$ forem conjuntos então

$$\bigcap_{i=1}^{n} A_i = A_1 \cap A_2 \cap \ldots \cap A_n$$
$$= \{x : x \in A_i \text{ para algum } i = 1, 2, \ldots, n\}.$$

Dois conjuntos A e B dizem-se **disjuntos** se e só se $A \cap B = \varnothing$, isto é, se não possuírem elementos comuns.
Dados conjuntos $A_i, i \in I$, dizemos que eles são disjuntos dois a dois se quaisquer $i, j \in I$, com $i \neq j$, se tem $A_i \cap A_j = \varnothing$.

A **diferença** de A e B é o conjunto $A \setminus B$ definido por

$$A \setminus B = \{x : x \in A \text{ e } x \notin B\}$$

ou seja, é o conjunto constituído pelos elementos de A que não pertencem a B. Se, em particular, se fizer $A = \mathcal{U}$, o universo do discurso, então o conjunto $\mathcal{U} \setminus B = \{x : x \notin B\}$ dá-se o nome de **conjunto complementar** de B e denota-se por $\overline{B}$ ou B^c.

Conjunto das partes de um conjunto

Podem construir-se conjuntos cujos elementos são eles próprios, no todo ou em parte, conjuntos. Assim, por exemplo, a letra x, o conjunto $\{a, b\}$, o conjunto $\{\varnothing\}$ e o número 4 podem constituir um novo conjunto que é o seguinte

$$\{x, \{a, b\}, \{\varnothing\}, 4\}.$$

Dado um conjunto arbitrário, é possível construir novos conjuntos cujos elementos são partes do conjunto inicial. Em particular, sendo A um conjunto qualquer, denota-se por $\mathcal{P}(A)$ o conjunto constituído por todos os subconjuntos (próprios ou impróprios) de A, isto é,

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

Se A é finito tem-se $\operatorname{Card}(\mathrm{P}(A)) = 2^{\operatorname{card}(A)}$.

O produto cartesiano de A por B, designa-se por $A \times B$ e é dado por

$$A \times B = \{(a,b) : a \in A \wedge b \in B\}.$$

Analogamente, podemos considerar o produto cartesiano de n conjuntos:

$$A_1 \times A_2 \times \ldots \times A_n = \{(a_1, a_2, \ldots, a_n) : a_1 \in A_1 \wedge a_2 \in A_2 \wedge \ldots \wedge a_n \in A_n\}$$

Por definição, $A^n = A \times A \times \ldots \times A$.

Se $A_1, A_2, \ldots, A_n$ são conjuntos finitos, então

$$\operatorname{card}(A_1 \times A_2 \times \ldots \times A_n) = \operatorname{card} A_1 \times \operatorname{card} A_2 \times \ldots \times \operatorname{card} A_n.$$

Exemplo TC2

Se $A = \{a,b,c\}$ então $\mathrm{P}(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\}\}$ é o conjunto das partes de A, com cardinalidade igual a 8.

Teorema (Propriedade Distributiva**)**

Sendo A, B, C três conjuntos arbitrários, ter-se-á:

a) $A \cap (B \cup C)$

b) $A \cup (B \cap C)$

Teorema (Leis de Morgan**)**

Sendo A e B dois conjuntos arbitrários, ter-se-á:

a) $\overline{(A \cap B)} = \overline{A} \cup \overline{B}$

b) $\overline{(A \cup B)} = \overline{A} \cap \overline{B}$

Exercícios– Teoria de Conjuntos

1. Mostra que se A for um subconjunto do conjunto vazio então $A = \emptyset$.

2. Dado um conjunto arbitrário A,
   a) Será A elemento do conjunto $\{A\}$?
   b) Será $\{A\}$ elemento do conjunto $\{A\}$?
   c) Será $\{A\}$ um subconjunto de $\{A\}$

3. Seja $A = \{1,2,\{3\}\}$. Quais das afirmações seguintes são verdadeiras?
   a) $1 \in A$;
   b) $\{1\} \in A$;
   c) $\{1\} \subseteq A$;
   d) $3 \in A$;
   e) $\{3\} \in A$;
   f) $\{3\} \subseteq A$;
   g) $\{\{3\}\} \subseteq A$;
   h) $\emptyset \in A$;
   i) $\emptyset \subseteq A$;

4. Descreva em compreensão os conjuntos seguintes:

$A = \{5,10,15,20,\ldots\}$

$B = \{7,17,27,37,\ldots\}$

$C = \{300,301,302,\ldots,399,400\}$

$D = \{1,4,9,16,25,36,49,\ldots\}$

$E = \{1, 1/2, 1/4, 1/8, 1/16,\ldots\}$

5. Indique quais dos conjuntos que se seguem são iguais:

$A = \{-1,1,2\}$

$B = \{-1,,2,1\}$

$C = \{0,1,2\}$

$D = \{2, 1, -1, -2\}$

$E = \{x : x^2 = 4 \quad ou \quad x^2 = 1\}$

6. Determine em extensão os seguintes conjuntos:

$A = \{x^2 - x : x \in \{0, 1, 2, 3\}\}$

$B = \{(-1)^n : n \in IN_0\}$

$C = \{x \in IN_0 : x^2 + 22 = 13x\}$

$D = \{x \in IN_0 : (x+1)(x+2) < 11\}$

7. Diga quais dos seguintes conjuntos que se seguem são finitos e quais são infinitos:

a) O conjunto das linhas do plano que são paralelas ao eixo dos xx'.
b) O conjunto das letras do alfabeto.
c) O conjunto dos múltiplos de 5.
d) O conjunto dos animais existentes na Terra.
e) O conjunto das raízes da equação $x^{38} + 42x^{23} - 17x^{18} - 2x^5 + 19 = 0$.
f) O conjunto das circunferências centradas na origem.

8. Determine quais dos conjuntos seguintes são iguais:

$A = \{-n + 1 : n \in Z\}$

$B = \{2m + 2 : m \in Z\}$

$C = Z$

$D = \{-2p + 2 : p \in Z\}$

$E = \{5^q : q \in Z\}$

$F = \{2r : r \in Z\}$

$G = \{5^{-s+1} : s \in Z\}$

9. Qual é a cardinalidade dos seguintes conjuntos:

$\{1, 2, \varnothing\}, \quad \{1, \{1, \varnothing\}\}, \quad \{\varnothing\}, \quad \{1\}, \quad \{\{1\}\}$

10. Determine a cardinalidade do conjunto

$$S=\left\{\frac{p}{q}: p,q\in IN \wedge p,q\leq 10\right\}$$

11. Seja $U=\{0,1,2,3,4,5,6,7,8,9\}$ o conjunto universal. Dados os conjuntos $A=\{1,3,5,7\}$, $B=\{2,3,4,5,6\}$ e $C=\{0,2,4,6,8\}$, defina em extensão os conjuntos $A\cap B,\ B\cup C,\ B\cup\overline{C},\ A\cap(B\cup C), (A\cap B)\cup(A\cap C)$
$(A\cap B)\cup C,\ A\cup\emptyset,\ B\cap\emptyset,\ A\cap C, \overline{U}$

12. Sejam A, B, C três conjuntos quaisquer contidos no universo U. Verifique as seguintes igualdades:

a) $A\cup\overline{A}=U$

b) $A\cap\overline{A}=\emptyset$

c) $A\cap B\subseteq A$

d) $A\cup B\supseteq A$

e) $\overline{\overline{A}}=A$

f) $A\setminus B=A\cap\overline{B}$

13. Em que circunstâncias são verdadeiras as igualdades que se seguem:

$A\cup B=A\cap B$

$A\cap\overline{B}=A$

$A\cap B=B$

$(A\cup B)\cap\overline{B}=A$

$(A\cap\overline{B})\cup B=A\cup B$

14. O facto de ser $A\cup B=D$ implica que seja $D\setminus B=A$? Se não, o que pode concluir-se do facto de ser $A\cup B=D$ e $D\setminus B=A$?

15. Sejam A e B dois subconjuntos do universo $U=\{1,2,3,4,5,6\}$ tais que

$$A \cup B = \{1,2,3,4\}, \quad A \cap B = \{3\}, \quad A \setminus B = \{1,2\}$$

Determine A, B e $B \setminus A$.

16. Verifique, justificando, se as afirmações seguintes são verdadeiras ou falsas.

a) Se $A \subseteq C$ e $B \subseteq C$ então $A \cup B \subseteq C$.
b) Se $C \subseteq A$ e $C \subseteq B$ então $C \subseteq A \cap B$.
c) Se $A \subseteq B$ e $B \subseteq C$ então $A \subseteq C$.
d) Se $A \not\subset B$ e $B \subseteq C$ então $A \not\subset C$.
e) Se $A \cap C = B \cap C$ então $A = B$.

17. Determinar o conjunto das partes do conjunto

I. $A = \{1\}$
II. $B = \{1,2\}$
III. $C = \{1,2,3\}$

18. Sendo $M = \{1,2,3,4\}$ determinar $\{x \in M : x \notin \varnothing\}$. Quantos elementos terá o conjunto das partes de M ?

19. Descrever os elementos do conjunto $\mathrm{P}(\mathrm{P}(\mathrm{P}(\varnothing)))$ onde $\mathrm{P}(\varnothing)$ designa o conjunto das partes do conjunto vazio $\varnothing$.

20. Sejam os conjuntos $A = \{a, \{b\}\}$ e $B = \{a, b, \{a, b\}\}$. Determine:

a) $A \cap B$
b) $A \cup B$
c) $\mathrm{P}(A)$ (conjunto das partes de A)
d) $B \cap \mathrm{P}(A)$

21. Determinar o conjunto das partes do conjunto das partes do conjunto $\{a\}$.

22. Dados dois conjuntos A e B. Verifique que:

a) $(A \cap B) \cup (A \cap \overline{B}) = A$

b) $\overline{(A \setminus B)} = \overline{A} \cup B$

23. Usando um diagrama de Venn apropriado verifique:

a) A demonstração do teorema da propriedade distributiva;

b) A demonstração do teorema das Leis de Morgan.

24. Sendo P, Q, R três conjuntos, indicar quais das afirmações que se seguem são verdadeiras.

a) Se P é um elemento de Q e Q é um subconjunto de R, então P é um elemento de R.

b) Se P é um elemento de Q e Q é um subconjunto de R, então P é também um subconjunto de R.

c) Se P é um subconjunto de Q e Q é um elemento de R, então P é um elemento de R.

d) Se P é um subconjunto de Q e Q é um elemento de R, então P é um subconjunto de R.

25. Sendo P, Q, R três conjuntos, provar:

a) $(P \setminus Q) | R = P \setminus (Q \cup R)$

b) $(P \setminus Q) | R = (P \setminus R) \setminus Q$

c) $(P \setminus Q) | R = (P \setminus R) \setminus (Q \setminus R)$

26. Chama-se diferença simétrica de dois conjuntos A e B ao conjunto constituído pelos elementos que pertencem a A ou a B, mas não a ambos simultaneamente.

a) Denotando por $A \oplus B$ a diferença simétrica de A e B, mostrar que $A \oplus B = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$.

b) Representar num diagrama de Venn a diferença simétrica de dois conjuntos A e B quaisquer.

c) Se a diferença simétrica entre dois conjuntos quaisquer A e B for igual ao conjunto A que poderá dizer a respeito de A e B?

d) Verifique se as igualdades seguintes são verdadeiras ou falsas.

I. $A \oplus A = A$

II. $A \oplus (A \oplus A) = A$

1.2 Elementos de Teoria da Dedução

Geralmente a matemática divide-se em partes chamadas **teorias matemáticas**. O desenvolvimento de uma qualquer teoria é constituído por três etapas fundamentais:

(1) a construção dos objectos matemáticos da teoria;
(2) a formação de relações entre estes objectos;
(3) a pesquisa das relações que são verdadeiras, ou seja, a demonstração de teoremas.

Objectos matemáticos são, por exemplo, os números, as funções ou as figuras geométricas; a Teoria dos Números, a Análise Matemática e a Geometria são, respectivamente, as teorias matemáticas que os estudam. Os objectos matemáticos (provavelmente) não existem na natureza; são apenas modelos abstractos de objectos reais mais ou menos complicados. As relações entre os objectos matemáticos são afirmações (ou proposições ou sentenças), verdadeiras ou falsas, que podem enunciar-se a seu respeito e que, de algum modo, correspondem a propriedades hipotéticas dos objectos reais que eles modelam.

Para provar os seus resultados a matemática usa um determinado processo de raciocínio que se baseia na **Lógica** (bivalente) que adopta como regras fundamentais de pensamento os dois princípios seguintes:

<u>Princípio da não contradição</u>: Uma proposição não pode ser verdadeira e falsa (ao mesmo tempo).

<u>Princípio do terceiro excluído</u>: Uma proposição ou é verdadeira ou é falsa (isto é, verifica-se sempre um destes casos e nunca um terceiro).

A matemática, como qualquer outra ciência, utiliza a sua linguagem própria constituída por **termos** – palavras ou símbolos – e **proposições** que são combinações de termos de acordo com determinadas regras. Numa teoria matemática qualquer podem distinguir-se dois tipos de termos:

(1) **termos lógicos**, que não são específicos daquela teoria e fazem parte da linguagem matemática geral, e
(2) **termos específicos** da teoria que se está a considerar.

Termos lógicos como, por exemplo, "*variável*", "*relação*", etc. são comuns a todas as teorias matemáticas. Pelo contrário, "*ponto*", "*recta*" e "*ângulo*" são termos específicos da geometria, enquanto que "*número*", "<", "*adição*" são termos específicos da teoria dos números, etc.
O papel principal da lógica em matemática é o de comunicar as ideias de forma precisa evitando erros de raciocínio.

1.2.1 Conjectura e demonstração

Chama-se **demonstração formal** a uma sequência finita $p_1, p_2, \ldots, p_n$ de proposições cada uma das quais ou é um axioma (proposição cuja veracidade se admite *à priori*) ou resulta de proposições anteriores por regras de inferência (que são formas muito simples e frequentes de argumentação válida, tradicionalmente designadas por silogismos). Cada uma das proposições $p_j, 1 \leq j \leq n$ é designada por **passo** da demonstração. Neste sentido, **teorema** será o último passo de uma dada demonstração, isto é, demonstrar um teorema consiste na realização de uma demonstração cujo último passo é o teorema em questão.
Fora da Lógica raramente se fazem demonstrações formais rigorosas: o que em geral se faz é estabelecer os passos fundamentais da demonstração suprimindo todos os

detalhes lógicos que, muitas vezes, não ajudam a esclarecer a verdadeira natureza da proposição sob análise. Estes procedimentos designar-se-ão simplesmente por demonstrações (ou demonstrações matemáticas) por contraposição a demonstrações formais.

Exemplo TC3

Na tabela que se segue, para cada número natural n de 2 a 10, calculou-se o número $2^n - 1$ obtendo-se os seguintes resultados:

n	é primo?	$2^n - 1$	é primo?
2	Sim	3	Sim
3	Sim	7	Sim
4	Não	15	Não
5	Sim	31	Sim
6	Não	63	Não
7	Sim	127	Sim
8	Não	255	Não
9	Não	511	Não
10	Não	1023	não

Observando cuidadosamente a tabela parece verificar-se o seguinte: sempre que n é um número primo, o número $2^n - 1$ também é primo! Será verdade?

Em matemática dá-se o nome de conjectura a este tipo de afirmações cujo valor lógico de verdade ou falsidade necessita de ser provado. Assim, esta tabela suscita as duas conjecturas seguintes:

Conjectura I

Dado um número inteiro n superior a 1, se n for primo então o número $2^n - 1$ é primo.

Conjectura II

Dado um número inteiro n superior a 1, se n não for primo o número $2^n - 1$ também não é primo.

Destas duas conjecturas a primeira pode refutar-se imediatamente: para tal é suficiente continuar a desenvolver a tabela para valores de n superiores a 10. Assim, para $n = 11$ vem

$$2^{11} - 1 = 2047 = 23 \times 89$$

o que mostra que a conjectura é falsa: 11 é um número superior a 1 e é primo, mas $2^{11} - 1$ é um número composto. O número 11, neste caso, constitui o que se designa geralmente por **contra-exemplo** para a conjectura: um simples contra-exemplo é suficiente para mostrar que a conjectura é falsa. Mas há mais contra-exemplos: 23 e 29, por exemplo, são outros contra-exemplos.

Considere-se agora a segunda conjectura: estendendo a tabela a outros números inteiros não primos superiores a 10 não se encontra nenhum contra-exemplo. Isto, contudo, não nos permite concluir que a conjectura é verdadeira pois por muito que se prolongue a tabela nunca será possível experimentar todos os números compostos possíveis: eles são em número infinito! Poderá haver contra-exemplos que sejam tão grandes que nem com os actuais meios computacionais seja possível testá-los. Para demonstrar ou refutar a conjectura é necessário adoptar então outros métodos.

A conjectura II é, de facto, verdadeira.

Demonstração

Visto que n não é primo então existem inteiros positivos a e b maiores que 1 tais que $a < n$ e $b < n$ e $n = ab$. Sendo $x = 2^b - 1$ e $y = 1 + 2^b + 2^{2b} + \ldots + 2^{(a-1)b}$, então

$$\begin{aligned}
xy &= \left(2^b - 1\right) \cdot \left(1 + 2^b + 2^{2b} + \ldots + 2^{(a-1)b}\right) \\
&= 2^b \cdot \left(1 + 2^b + 2^{2b} + \ldots + 2^{(a-1)b}\right) - \left(1 + 2^b + 2^{2b} + \ldots + 2^{(a-1)b}\right) \\
&= \left(2^b + 2^{2b} + 2^{3b} + \ldots + 2^{ab}\right) - \left(1 + 2^b + 2^{2b} + \ldots + 2^{(a-1)b}\right) \\
&= 2^{ab} - 1 \\
&= 2^n - 1
\end{aligned}$$

Visto que $b<n$ pode concluir-se que $x=2^b-1<2^n-1$; por outro lado, como $b>1$ então $x=2^b-1>2^1-1=1$ donde se segue que $y<xy=2^n-1$. Então 2^n-1 pode decompor-se num produto de dois números inteiros positivos x e y maiores que 1 e menores que 2^n-1 o que prova que 2^n-1 não é primo. □

Uma vez que se provou que a conjectura II é verdadeira, esta passou a adquirir o estatuto de teorema, podendo então escrever-se:

Teorema

Dado um número inteiro n superior a 1, se n não for primo então o número 2^n-1 também não é primo.

1.2.2 Lógica Proposicional

Tal como referido no ponto anterior, a demonstração de conjecturas é essencial em matemática. A Lógica estuda os métodos de raciocínio, especialmente os que podem expressar-se sob a forma de argumentos. Um argumento consiste numa série (finita) de proposições declarativas, chamadas premissas, a partir das quais se infere uma outra proposição, a conclusão. Há vários tipos de argumentos: os dois principais são os argumentos indutivos e os argumentos dedutivos. O primeiro, usado no dia a dia pelas ciências empíricas, parte de dados da experiência para concluir que uma dada proposição, provavelmente, é verdadeira. Os dados da experiência tornam provável a veracidade da conclusão, mas não a garantem em absoluto.

Um argumento dedutivo, pelo contrário, garante que se todas as premissas forem verdadeiras a conclusão também o será. A argumentação dedutiva está na base das demonstrações matemáticas.

Proposições ou **sentenças** são os elementos básicos da lógica que são afirmações precisas (verdadeiras ou falsas, mas não ambas as coisas). Por exemplo, "*2 é maior que 3*" é uma proposição cujo valor lógico é o de "*falsidade*" enquanto que "*todos os* *triângulos têm três lados e três ângulos*" é uma proposição cujo valor lógico é o de "*verdade*". Por outro lado "$x < 3$" não é uma proposição (depende do valor que venha a ser atribuído à variável x). Representar-se-ão por letras (geralmente minúsculas) as proposições genéricas (ou variáveis proposicionais) e por 1 e 0 os valores lógicos de "*verdade*" e "*falsidade*", respectivamente.

Exemplo TC4

As afirmações

1. A Lua é feita de queijo verde.
2. $\left(e^{\pi}\right)^2 = e^{2\pi}$
3. 6 é um número primo.
4. o milionésimo dígito na dízima de $\sqrt{2}$ é 6.

São exemplos de proposições. Por outro lado,

1. Será $\left(e^{\pi}\right)^2$ igual a $e^{2\pi}$?
2. Se ao menos todos os dias pudessem ser como este!
3. Toda a gente é aardlingueede.
4. Esta proposição é falsa.

Claramente não são proposições.

Por vezes combinam-se várias proposições para obter proposições compostas: neste caso, em geral, pretende-se obter os valores lógicos das proposições compostas em função dos valores lógicos conhecidos das proposições mais simples que as compõem.

Uma conectiva lógica que modifica o valor de uma dada proposição "p" é a sua negação "**não** p", denotada geralmente por "$\neg p$", que é uma proposição falsa quando "p" é verdadeira e verdadeira quando "p" é falsa. Isto pode expressar-se à custa da chamada tabela de verdade da negação:

p	$\neg p$
1	0
0	1

Existem várias formas pelas quais se podem combinar duas proposições. Em particular, as conectivas "**e**" e "**ou**", *conjunção* e *disjunção*, denotadas geralmente por "$\wedge$" e "$\vee$", respectivamente, são definidas pelas seguintes tabelas de verdade:

p	q	$p \wedge q$	$p \vee q$
1	1	1	1
1	0	0	1
0	1	0	1
0	0	0	0

A conjunção de duas proposições é verdadeira quando e só quando duas proposições forem *simultaneamente* verdadeiras; a disjunção é verdadeira desde que *pelo menos* uma das proposições seja verdadeira.

A conectiva "$\Rightarrow$" que se lê "**se ..., então ...**", designa-se por "**implicação**", obedece à seguinte tabela de verdade:
Quando temos a implicação $p \Rightarrow q$ dizemos que p é o antecedente e q o consequente.

p	q	$p \Rightarrow q$
1	1	1
1	0	0
0	1	1
0	0	1

Considere-se, por fim, a conectiva lógica "p se e só se q", por vezes abreviada para "p sse q", e geralmente denotada por "$p \Leftrightarrow q$". A sua tabela de verdade é dada por

p	q	$p \Leftrightarrow q$
1	1	1
1	0	0
0	1	0
0	0	1

A proposição " $p \Leftrightarrow q$ " é verdadeira quando " p " e " q " são ambas verdadeiras ou ambas falsas e falsa quando " p " e " q " têm valores lógicos distintos. É fácil verificar que " $p \Leftrightarrow q$ " têm o mesmo significado lógico que a proposição "$(p \Rightarrow q) \wedge (q \Rightarrow p)$". Para confirmar basta escrever a tabela de verdade para esta proposição e verificar que é idêntica.

p	q	$p \Rightarrow q$	$q \Rightarrow p$	$(p \Rightarrow q) \wedge (q \Rightarrow p)$
1	1	1	1	1
1	0	0	1	0
0	1	1	0	0
0	0	1	1	1

Na prática usa-se frequentemente esta relação: para mostrar que uma proposição da forma " $p \Leftrightarrow q$ " é verdadeira decompõe-se essa proposição nas duas partes " $p \Rightarrow q$ " e " $q \Rightarrow p$ " e mostra-se separadamente que cada uma delas é verdadeira.

1.2.2.1 Tautologias e contradições

Chama-se **tautologia** a uma proposição que é sempre verdadeira quaisquer que sejam os valores atribuídos às variáveis proposicionais que a compõem. Dito de outra forma, chama-se tautologia a uma proposição cuja tabela de verdade possui apenas 1s na última coluna.

Exemplo TC5

Exemplo de tautologia é a proposição $p \vee (\neg p)$, o princípio do terceiro excluído,

p	$\neg p$	$p \vee (\neg p)$
1	0	1
0	1	1

Se p designar a proposição "*5 é uma raiz primitiva de 17*" então $p \vee (\neg p)$ é sempre verdadeira independentemente do significado (ou sentido) atribuído à expressão "*raiz primitiva de*".

Chama-se **contradição** à negação de uma tautologia: trata-se de uma proposição cuja tabela de verdade apenas possui 0s na última coluna.

Nota

Não deve confundir-se contradição com proposição falsa, assim como não deve confundir-se tautologia com proposição verdadeira. O facto de uma tautologia ser sempre verdadeira e uma contradição ser sempre falsa deve-se à sua forma lógica (sintaxe) e não ao significado que se lhes pode atribuir (semântica).
A tabela de verdade

p	q	$p \vee q$	$p \Rightarrow (p \vee q)$	$p \Rightarrow q$	$\neg q$	$p \wedge (\neg q)$	$(p \Rightarrow q) \wedge [p \wedge (\neg q)]$
1	1	1	1	1	0	0	0
1	0	1	1	0	1	1	0
0	1	1	1	1	0	0	0
0	0	0	1	1	1	0	0

Mostra que $p \Rightarrow (p \vee q)$ é um tautologia, enquanto que $(p \Rightarrow q) \wedge [p \wedge (\neg q)]$ é uma contradição.

1.		$p \vee \neg p$	
2.		$\neg[p \wedge (\neg p)]$	
3.		$p \Rightarrow p$	
4.	a)	$p \Leftrightarrow (p \vee p)$	idempotência
	b)	$p \Leftrightarrow (p \wedge p)$	idempotência
5.		$\neg\neg p \Leftrightarrow p$	dupla negação
6.	a)	$(p \vee q) \Leftrightarrow (q \vee p)$	comutatividade
	b)	$(p \wedge q) \Leftrightarrow (q \wedge p)$	comutatividade
	c)	$(p \Leftrightarrow q) \Leftrightarrow (q \Leftrightarrow p)$	comutatividade
7.	a)	$(p \vee (q \vee r)) \Leftrightarrow ((p \vee q) \vee r)$	associatividade
	b)	$(p \wedge (q \wedge r)) \Leftrightarrow ((p \wedge q) \wedge r)$	associatividade
8.	a)	$(p \wedge (q \vee r)) \Leftrightarrow ((p \wedge q) \vee (p \wedge r))$	distributividade
	b)	$(p \vee (q \wedge r)) \Leftrightarrow ((p \vee q) \wedge (p \vee r))$	distributividade
9.	a)	$(p \vee 0) \Leftrightarrow p$	identidade
	b)	$(p \wedge 0) \Leftrightarrow 0$	identidade
	c)	$(p \vee 1) \Leftrightarrow 1$	identidade
	d)	$(p \wedge 1) \Leftrightarrow p$	identidade
10.	a)	$\neg(p \wedge q) \Leftrightarrow (\neg p \vee \neg q)$	leis de Morgan
	b)	$\neg(p \vee q) \Leftrightarrow (\neg p \wedge \neg q)$	leis de Morgan
11.	a)	$(p \Leftrightarrow q) \Leftrightarrow [(p \Rightarrow q) \wedge (q \Rightarrow p)]$	equivalência
	b)	$(p \Leftrightarrow q) \Leftrightarrow [(p \wedge q) \vee (\neg p \wedge \neg q)]$	equivalência
	c)	$(p \Leftrightarrow q) \Leftrightarrow (\neg p \Leftrightarrow \neg q)$	equivalência
12.	a)	$(p \Rightarrow q) \Leftrightarrow (\neg p \vee q)$	implicação
	b)	$\neg(p \Rightarrow q) \Leftrightarrow (p \wedge \neg q)$	implicação

13.	$(p \Rightarrow q) \Leftrightarrow (\neg q \Rightarrow \neg p)$	contrarecíproca
14.	$(p \Rightarrow q) \Leftrightarrow [(p \wedge \neg q) \Rightarrow 0]$	redução ao absurdo
15. a)	$[(p \Rightarrow r) \wedge (q \Rightarrow r)] \Leftrightarrow [(p \vee q) \Rightarrow r]$	
b)	$[(p \Rightarrow q) \wedge (p \Rightarrow r)] \Leftrightarrow [p \Rightarrow (q \wedge r)]$	
16.	$[(p \wedge q) \Rightarrow r] \Leftrightarrow [p \Rightarrow (q \Rightarrow r)]$	
17.	$p \Rightarrow (p \vee q)$	adição
18.	$(p \wedge q) \Rightarrow p$	simplificação
19.	$[p \wedge (p \Rightarrow q)] \Rightarrow q$	*modus ponens*
20.	$[(p \Rightarrow q) \wedge \neg q] \Rightarrow \neg p$	*modus tollens*
21.	$[(p \Rightarrow q) \wedge (q \Rightarrow r)] \Rightarrow (p \Rightarrow r)$	silogismo hipotético
22.	$[(p \vee q) \wedge \neg p] \Rightarrow q$	silogismo disjuntivo
23.	$(p \Rightarrow 0) \Rightarrow \neg p$	absurdo
24.	$[(p \Rightarrow q) \wedge (r \Rightarrow s)] \Rightarrow [(p \vee r) \Rightarrow (q \vee s)]$	
25.	$(p \Rightarrow q) \Rightarrow [(p \vee r) \Rightarrow (q \vee r)]$	

Na tabela acima apresentam-se alguns exemplos importantes de tautologias onde p, q, r, s designam variáveis proposicionais (isto é, afirmações que ou são verdadeiras ou falsas, mas não ambas as coisas) e 1 e 0 designam as proposições tautologia e contraditória, respectivamente.

Definição

Duas proposições a e b dizem-se **logicamente equivalentes** se tiverem os mesmos valores lógicos em todas as circunstâncias, ou seja, se a proposição $a \Leftrightarrow b$ for uma tautologia.

Dir-se-á que a proposição a **implica logicamente** a proposição b se a veracidade da primeira arrastar necessariamente a veracidade da segunda, ou seja, se a proposição $a \Rightarrow b$ for uma tautologia.

1.2.3 Teoremas e demonstrações

Sejam p, q, r três proposições das quais se sabe seguramente que p e q são proposições verdadeiras. Se for possível provar a implicação

$$(p \wedge q) \Rightarrow r$$

é verdadeira (isto é, que a veracidade de p e de q resulta sempre a veracidade de r), então pode argumentar-se que r é necessariamente verdadeira. Se, numa contenda, as proposições p e q forem aceites como verdadeiras por ambas as partes assim como a implicação anterior, então a veracidade de r resulta logicamente de pressupostos. A uma tal proposição (composta) dá-se o nome de ***argumento*** e constitui o método usado numa discussão para convencer uma parte das razões que assistem à outra.

Chama-se **argumento** a uma sequência finita de proposições organizadas na forma seguinte

$$(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \Rightarrow q$$

Onde $p_1, p_2, \ldots, p_n$ são designadas as **premissas** (ou **hipóteses**) e q a **conclusão** (ou **tese**). Ao fazer a leitura desta implicação é costume inserir uma das loções "portanto", "por conseguinte", "logo", etc., lendo-se, por exemplo, "$p_1, p_2, \ldots, p_n$ portanto q". Para sugerir esta leitura usa-se, frequentemente, a seguinte notação

$$\begin{array}{l} p_1 \\ \vdots \\ \underline{p_n} \\ q \end{array} \qquad \text{ou} \quad p_1, \ldots, p_n / q$$

Interessa distinguir entre argumentos correctos ou válidos e argumentos incorrectos ou inválidos.

Definição

Um argumento $p_1, \ldots, p_n / q$ diz-se **correcto** ou **válido** se a conclusão for verdadeira sempre que as premissas $p_1, p_2, \ldots, p_n$ forem simultaneamente verdadeiras e diz-se **incorrecto** ou **inválido** no caso contrário, isto é, se alguma situação permitir que as premissas sejam todas verdadeiras e a conclusão falsa.

Construção de demonstrações elementares

A demonstração de teoremas é feita de muitas formas dependendo em geral do próprio conteúdo do teorema. Os próprios teoremas são formulados de muitas maneiras distintas. Uma das mais frequentes é a que envolve uma conclusão do tipo

$$p \Rightarrow q$$

Para demonstrar a veracidade desta implicação começa-se por supor que p é uma proposição verdadeira para depois se concluir que então q também é verdadeira. [Note-se que se p for falsa a implicação é sempre verdadeira quer q seja verdadeira quer seja falsa.] Observe-se também que desta forma se prova a validade da implicação $p \Rightarrow q$ e não a veracidade de q. Para provara a veracidade de q seria necessário para além de provar a veracidade da implicação $p \Rightarrow q$ que se afirmasse a veracidade de p: supor que p é verdadeira não é a mesma coisa que afirmar que p é verdadeira.

Exemplo TC6

Suponha-se que a e b são números reais. Provar que se $0 < a < b$ então $a^2 < b^2$.

Os dados do problema são as afirmações $a \in \mathbb{R}$ e $b \in \mathbb{R}$ e o objectivo é o de obter uma conclusão da forma $p \Rightarrow q$ onde p é a afirmação $0 < a < b$ e q é a afirmação $a^2 < b^2$. Supor que p é uma proposição verdadeira é equivalente a juntar p aos dados do problema. Assim, equivalentemente, pode ter-se

hipóteses	tese
$a \in \mathbb{R}, b \in \mathbb{R}$	$a^2 < b^2$
$0 < a < b$	

A técnica de demonstração, neste caso, obtém-se por comparação das duas desigualdades $a < b$ e $a^2 < b^2$. Multiplicando a primeira desigualdade por a (que é um número real positivo!) vem

$$a^2 < ab$$

e multiplicando-a agora por b (que também é um número real positivo) vem

$$ab < b^2$$

Desta forma, obtém-se que $a^2 < ab < b^2$ e, portanto, por transitividade, $a^2 < b^2$ como se pretendia mostra.

Mais formalmente, poder-se-ia apresentar este exemplo da seguinte forma:

Teorema

Suponha-se que a e b são dois números reais. Se $0 < a < b$ então $a^2 < b^2$.

Demonstração

Suponha-se que $0 < a < b$. Multiplicando a desigualdade $a < b$ pelo número positivo a conclui-se que $a^2 < ab$ e, de modo semelhante, multiplicando-a por b obtém-se $ab < b^2$ e, portanto, $a^2 < b^2$ como se pretendia mostrar. Consequentemente, se $0 < a < b$ então $a^2 < b^2$. $\square$

Para provar uma implicação da forma $p \Rightarrow q$, muitas vezes, é mais fácil supor $\neg q$ e provar então que se verifica $\neg p$ obtendo-se assim $\neg q \Rightarrow \neg p$, o que, como se sabe, equivale logicamente a $p \Rightarrow q$.

Exemplo TC7

Suponha-se que a, b e c são três números reais e que $a > b$. Mostrar que se $ac \leq bc$ então $c \leq 0$.

A demonstração neste caso tem o seguinte esquema:

hipóteses	tese
$a \in \mathbb{R}, b \in \mathbb{R}, c \in \mathbb{R}$	$ac \leq bc \Rightarrow c \leq 0$
$a > b$	

A contra-recíproca da tese é a implicação

$$\neg(c \leq 0) \Rightarrow \neg(ac \leq bc)$$

Ou seja,

$$c > 0 \Rightarrow ac > bc$$

e, portanto, pode realizar-se a demonstração de acordo com o seguinte esquema

hipóteses	tese
$a \in \mathbb{R}, b \in \mathbb{R}, c \in \mathbb{R}$	$ac > bc$
$a > b$	
$c > 0$	

A tese resulta agora imediatamente de se multiplicar a desigualdade $a > b$ por $c > 0$. Mais formalmente,

Teorema

Sejam a, b, c três números reais tais que $a > b$. Se $ac \leq bc$ então $c \leq 0$.

Demonstração

A prova será feita pela contra-recíproca. Suponha-se que $c > 0$. Então, multiplicando ambos os membros da desigualdade $a > b$ por c obter-se-á $ac > bc$. Consequentemente, $ac \leq bc \Rightarrow c \leq 0$ como se pretendia mostrar. $\square$

As regras que permitem passar de hipóteses feitas e resultados já demonstrados a novas proposições são conhecidas por **regras de inferência**. A mais usada, conhecida por **modus ponens**, é a seguinte:

$$\begin{array}{l} p \Rightarrow q \\ \underline{p \quad\;\;} \\ \;\; q \end{array}$$

Se a proposição p e a implicação $p \Rightarrow q$ forem verdadeiras, então q é necessariamente verdadeira.

A proposição q é logicamente implicada por p e $p \Rightarrow q$ o que se escreve

$$p,\ p \Rightarrow q \pounds q$$

De um modo geral. $p_1, p_2, \ldots, p_n \pounds q$ é uma regra de inferência se e só se $p_1 \wedge p_2 \wedge \ldots \wedge p_n \Rightarrow q$ for uma tautologia.

Outras regras de inferência,

$p, p \Rightarrow q \pounds q$ modus ponens

$p \Rightarrow q, q \Rightarrow r \pounds p \Rightarrow r$

$p \Rightarrow q, \neg q \pounds \neg p$ modus tollens

$p \pounds p \vee q$

$p \wedge q \pounds p$

$p, q \pounds p \wedge q$

1.2.4 Lógica com quantificadores

1.2.4.1 Variáveis e conjuntos

No desenvolvimento de qualquer teoria matemática aparecem muitas vezes afirmações sobre objectos genéricos da teoria que são representados por letras designadas por **variáveis**.

Se representarmos por x um número inteiro positivo genérico, pode ser necessário analisar (sob o ponto de vista lógico) afirmações do tipo "x *é um número primo*". Esta afirmação não é uma proposição, o seu valor lógico tanto pode ser o de verdade como o de falsidade. Uma afirmação deste tipo denota-se por "$p(x)$" para mostrar que "p" depende da variável x obtendo-se, assim, uma **fórmula** com uma **variável livre**. A afirmações (com variáveis livres) associam-se os chamados conjuntos de verdade que são os conjuntos de valores para os quais $p(x)$ é verdadeira. Escreve-se

$$A=\{x: p(x)\}$$

e lê-se A é o conjunto cujos elementos satisfazem $p(x)$ ou para os quais $p(x)$ é verdadeira.

Conjuntos de verdade e conectivas lógicas

Suponha-se que A é um conjunto de verdade de uma fórmula $p(x)$ e B é o conjunto de verdade de uma fórmula $q(x)$. Então,

$$A=\{x: p(x)\} \equiv \{x \in U : p(x)\}$$
$$B=\{x: q(x)\} \equiv \{x \in U : q(x)\}$$

O conjunto de verdade da fórmula $p(x) \wedge q(x)$ é tal que

$$\{x \in U : p(x) \wedge q(x)\} = \{x \in U : x \in A \wedge x \in B\} = A \cap B$$

De modo semelhante,

$$\{x \in U : p(x) \vee q(x)\} = \{x \in U : x \in A \vee x \in B\} = A \cup B$$

1.2.4.2 Os quantificadores universal e existencial

Uma fórmula $p(x)$, contendo uma variável x, pode ser verdadeira para alguns valores de x pertencentes ao universo do discurso e falsa para outros. Por vezes, pretende-se dizer que uma dada fórmula $p(x)$ se verifica para todos os elementos de x (do universo). Escreve-se então

"*para todo o* $x, p(x)$" ou "*qualquer que seja* $x, p(x)$"

e representa-se simbolicamente por

$$\forall x\ p(x)$$

O símbolo $\forall$ é designado por **quantificador universal**. A fórmula anterior é equivalente a

$$\forall x\left[x \in U \Rightarrow p(x)\right]$$

A quantificação pode ser feita apenas sobre uma parte de U. Assim, se D designar um subconjunto próprio de U e $p(x)$ for uma fórmula com uma variável cujo domínio é D, então

$$\forall x \in D\ p(x) \text{ ou } \forall x\left[x \in D \Rightarrow p(x)\right]$$

afirma que $p(x)$ se verifica para todo o $x \in D$.

Se, por exemplo, $D = \{a_1, a_2, \ldots, a_n\}$ a fórmula anterior é (logicamente) equivalente à conjunção $p(a_1) \wedge p(a_2) \wedge \ldots \wedge p(a_n)$.

Exemplo TC8

Suponha que $p(x)$ é a fórmula $x^2 + 1 > 0$. Então, $\forall x\left[x \in \mathbb{R} \Rightarrow p(x)\right]$ é uma proposição verdadeira, enquanto que $\forall x\left[x \in \mathbb{C} \Rightarrow p(x)\right]$ é uma proposição falsa.

Escreve-se

$$\exists x \; p(x)$$

Para significar que existe (no universo do discurso) pelo menos um elemento x para o qual $p(x)$ se verifica, o que pode ler-se da seguinte forma

"*existe pelo menos um* x *tal que* $p(x)$".

De outra forma, $\exists x\left[x \in \mathrm{U} \wedge p(x)\right]$ onde, U designa o universo do discurso. O símbolo $\exists$ é chamado o **quantificador existencial**.

Se D for um subconjunto de U e $p(x)$ for uma fórmula com uma variável cujo domínio é D, então $\exists x \; p(x)$ ou $\exists x\left[x \in D \wedge p(x)\right]$ é uma fórmula com o quantificador existencial.

Se, por exemplo, $D=\{a_1, a_2, \ldots, a_n\}$ a fórmula anterior é (logicamente) equivalente à disjunção $p(a_1) \vee p(a_2) \vee \ldots \vee p(a_n)$.

O valor lógico (de verdade ou falsidade) de uma proposição quantificada depende do domínio considerado. As duas proposições

$$\forall x\left[x \in \mathbb{Q} \Rightarrow x^2-2=0\right]$$
$$\exists x\left[x \in \mathbb{Q} \wedge x^2-2=0\right]$$

São falsas enquanto que as duas seguintes

$$\forall x\left[x \in \mathbb{R} \Rightarrow x^2-2=0\right]$$
$$\exists x\left[x \in \mathbb{R} \wedge x^2-2=0\right]$$

a primeira é falsa, mas a segunda é verdadeira.

Interessa também considerar quando o domínio da variável da fórmula $p(x)$ é o conjunto vazio. Que valor lógico terão as expressões da forma

$$\forall x\left[x\in\varnothing\Rightarrow p(x)\right] \quad \text{e} \quad \exists x\left[x\in\varnothing\wedge p(x)\right]$$

Visto que $x\in\varnothing$ é sempre falso, então a primeira expressão é uma proposição sempre verdadeira. Quanto à segunda proposição ela tem a forma de uma conjunção de proposições, das quais uma é sempre falsa, logo a proposição é sempre falsa.

Por vezes emprega-se o quantificador existencial numa situação simultânea de unicidade, ou seja, quer-se afirmar não só que $\exists x\ p(x)$ mas ainda que a fórmula $p(x)$ se transforma numa proposição verdadeira só para um elemento do domínio de quantificação. Neste caso emprega-se a abreviatura

$$\exists!x\ p(x)$$

Que significa "*existe um e só um* x *tal que* $p(x)$".

Quantificação múltipla

Uma fórmula matemática pode ter mais do que uma variável. Considere-se, por exemplo, a afirmação

"para *todo o número real* x *existe um número real* y *tal que* $x+y=5$"

simbolicamente, $\forall x\,\exists y\left[x+y=5\right]$, que constitui uma proposição verdadeira (sendo $y=5-x$ para cada $x\in\mathbb{R}$).

Se se trocarem os quantificadores obter-se-á

$$\exists y\ \forall x\left[x+y=5\right]$$

que significa

"*existe um número real* y *tal que para todo o número real* x *se tem* $x+y=5$".

Esta proposição é falsa, pois não existe nenhum número real y, sempre o mesmo, para o qual todo o número real x satisfaz a equação dada.

Estes exemplos ilustram a não comutatividade de dois quantificadores universal, $\forall$, e existencial, $\exists$.
Dois quantificadores da mesma espécie são sempre comutativos enquanto que dois quantificadores de espécie diferente são geralmente não comutativos, isto é, a sua permuta conduz a proposições de conteúdo distinto.

Negação de proposições quantificadas

Dadas as proposições com quantificadores $\forall x\left[x \in U \Rightarrow p(x)\right]$ e $\exists x\left[x \in U \wedge p(x)\right]$ pode ser necessário analisar (logicamente) as proposições que são a negação destas, ou seja,

$$\neg\forall x\left[x \in U \Rightarrow p(x)\right] \text{ equivale a } \exists x\left[x \in U \wedge \neg p(x)\right]$$

e

$$\neg\exists x\left[x \in U \wedge p(x)\right] \text{ equivale a } \forall x\left[x \in U \Rightarrow \neg p(x)\right]$$

De um modo genérico, têm-se as equivalências,

$$\neg\left(\forall x\ p(x)\right) \Leftrightarrow \exists x\left[\neg p(x)\right]$$
$$\neg\left(\exists x\ p(x)\right) \Leftrightarrow \forall x\left[\neg p(x)\right]$$

Conhecidas por <u>segundas leis de Morgan</u>.

Exercícios – Lógica

1. Diga, justificando, se as seguintes frases são ou não proposições (sentenças):

   a) Se a terra for plana então 2+2=4.
   b) Não é verdade que 3 seja número par ou que 7 seja primo.
   c) Para algum $n \in \mathbb{N}, 2^n = n^2$.
   d) Para todos os números reais $x, y \in \mathbb{R}, x + y = y + x$.
   e) Ele é muito inteligente.

f) Ou sais tu ou saio eu.

g) $x - y = y - x$

2. Suponha-se que p, q, r representam as seguintes sentenças:

$p \equiv$ "7 é um número inteiro par"

$q \equiv$ "3+1=4"

$r \equiv$ "24 é divisível por 8"

a) Escreva em linguagem simbólica:
   i. $3+1 \neq 4$ e 24 é divisível por 8
   ii. Não é verdade que 7 seja ímpar ou 3+1=4
   iii. Se 3+1=4 então 24 não é divisível por 8

   Construa as tabelas de verdade das proposições compostas obtidas.

b) Traduza por frases cada uma das sentenças:
   i. $p \vee (\neg q)$
   ii. $\neg(p \wedge q)$
   iii. $(\neg r) \vee (\neg q)$

3. Construa as tabelas de verdade das seguintes fórmulas lógicas (proposições compostas<9 e diga, justificando, quais delas correspondem a tautologias:

a) $\left[(p \Rightarrow q) \wedge p\right] \Rightarrow q$

b) $p \Leftrightarrow (q \Rightarrow r)$

c) $\left[p \wedge (\neg p)\right] \Rightarrow q$

4. O operador lógico conhecido por "ou exclusivo" pode ser representado por $\dot{\vee}$, tal que $p \dot{\vee} q$ é uma proposição verdadeira quando e só quando p e q tiverem valores lógicos contrários.

a) Mostre que $p \dot{\vee} q$ é equivalente a $\neg(p \Leftrightarrow q)$.

b) Construa as tabelas de verdade para $p \dot{\vee} p, (p \dot{\vee} q) \dot{\vee} r$ e $(p \dot{\vee} p) \dot{\vee} p$.

5. Mostre que cada uma das proposições que se seguem

a) $(\neg p) \vee q$
b) $(\neg q) \Rightarrow (\neg p)$
c) $\neg [p \wedge (\neg q)]$

é equivalente á implicação $p \Rightarrow q$.

6. Escreva as proposições recíprocas, inversas (contrárias) e as contra-recíprocas para cada uma das seguintes proposições:

a) $(p \wedge q) \Rightarrow r$
b) $p \Rightarrow (q \Rightarrow p)$
c) $(p \Leftrightarrow q) \Rightarrow (p \Rightarrow q)$

7. Traduza a afirmação "Sempre que chove existem nuvens no céu" através de uma implicação lógica $p \Rightarrow q$ e, e seguida, escreva as afirmações correspondentes à recíproca, à contrária e à contra-recíproca dessa implicação, indicando o valor lógico de cada uma das afirmações.

8. Escreva cada uma das frases seguintes na forma de implicação $p \Rightarrow q$:

a) Se tocares nesse bola apanhas.
b) Toca nesse bolo e arrepender-te-ás.
c) Sai ou chamo a polícia.
d) Vou-me embora se não pararem de falar.

9. Determine o antecedente e o consequente de cada uma das seguintes proposições:

a) Plantas saudáveis crescem com água suficiente.

b) Um aumento significativo no poder dos computadores é uma condição necessária para futuros avanços tecnológicos.
c) Erros serão introduzidos se efectuarmos uma modificação nesse programa.
d) Para poupar combustível é necessário instalar um bom isolamento térmico assim como janelas duplas.

10. Usando tautologias apropriadas simplifique as proposições:

a) $p \vee \left[q \wedge (\neg p) \right]$
b) $\neg\left[(\neg p) \wedge (\neg q) \right]$
c) $(p \wedge q) \vee \left[p \wedge (\neg q) \right]$

11. Por vezes usa-se o símbolo $\downarrow$ para denotar a proposição composta por duas proposições p e q que é verdadeira quando e só quando p e q são (simultaneamente) falsas e é falsa em todos os outros casos. A proposição $p \downarrow q$ lê-se *"nem p nem q"*.

a) Faça a tabela de verdade de $p \downarrow q$.
b) Expresse $p \downarrow q$ em termos das conectivas $\wedge, \vee$ e $\neg$.
c) Determine as proposições apenas constituídas pela conectiva $\downarrow$ que sejam equivalentes a $\neg p, p \wedge q$ e $p \vee q$.

12. Expresse a proposição $p \Leftrightarrow q$ usando apenas os símbolos $\wedge, \vee$ e $\neg$.

13. Mostre que $\neg\left[p \Rightarrow (q \vee r) \right]$ implica logicamente $\neg(p \Rightarrow q)$.

14. Supondo que p, q, r representam as seguintes sentenças:

$p \equiv$ "ir ao Porto"

$q \equiv$ "apanhar o comboio"

$r \equiv$ "chover"

a) Traduza através de uma proposição lógica a seguinte afirmação "Não vou ao Porto se não apanhar o comboio ou se chover".
b) Admitindo que r assume o valor lógico *falso* diga, justificando, qual o valor lógico da proposição $(p \wedge q) \Rightarrow [(\neg q \vee r) \Rightarrow \neg p]$.
c) Obtenha uma proposição logicamente equivalente à proposição da alínea anterior, mas que contenha a penas os operadores de negação e disjunção.

15. Supondo que p, q, r representam as seguintes sentenças

$p \equiv$ "Tenho gripe"

$q \equiv$ "Falto ao exame de Mat I"

$r \equiv$ "Fico aprovado a Mat I"

a) Escreva em linguagem comum cada uma das seguintes proposições:
   i. $\neg q \Leftrightarrow r$
   ii. $(p \wedge q) \vee (\neg q \wedge r)$
   iii. $(p \Rightarrow \neg r) \vee (q \Rightarrow \neg r)$

b) Verifique, formalmente, que a proposição $(p \Rightarrow \neg r) \vee (q \Rightarrow \neg r)$ é equivalente a $(p \wedge q) \Rightarrow \neg r$.

16. Encontre, justificando, proposições onde figurem apenas os operadores de conjunção e negação que sejam equivalentes a

a) $(p \vee \neg q)$
b) $(p \vee q) \wedge \neg p$

17. Considere a proposição composta $\neg(p \vee \neg q) \vee (\neg p \wedge q)$.

a) Encontre uma proposição equivalente que use a implicação lógica.
b) Diga se a proposição corresponde a uma contradição ou a uma tautologia , ou nem a uma coisa nem outra.

18. Sejam A,B,C,D quatro conjuntos e suponha-se que $A\setminus B \subseteq C\cap D$ e seja $x\in A$. Mostrar que se $x\notin D$ então $x\in B$.

19. Suponha-se que x é um número real tal que $x\neq 0$. Mostrar que se $\frac{\sqrt[3]{x}+5}{x^2+6}=\frac{1}{x}$ então $x\neq 8$.

20. Sejam a,b,c,d números reais tais que $0<a<b$ e $d>0$. Provar que se $ac>bd$ então $c>d$.

21. Analise a validade dos seguintes argumentos:

a) Bom tempo é necessário para se conseguir um bom jardim. Como o jardim está muito bonito o tempo tem estado bom.
b) Se hoje o tempo estiver bom amanhã faremos um piquenique. Mas hoje o tempo não está bom, logo, amanhã não faremos um piquenique.

22. Sendo p,q,r,s quatro proposições dadas, estabelecer a validade ou invalidade dos seguintes argumentos:

a) $(\neg p)\vee q, p \pounds q$
b) $p\Rightarrow q, r\Rightarrow(\neg q) \pounds p\Rightarrow(\neg r)$
c) $(\neg p)\vee q, (\neg r)\Rightarrow(\neg q) \pounds p\Rightarrow(\neg r)$
d) $q\vee(\neg p), \neg q \pounds p$
e) $\neg p \pounds p\Rightarrow q$
f) $p\vee q, q\Rightarrow(\neg r), (\neg r)\Rightarrow(\neg p) \pounds \neg(p\wedge q)$
g) $p\Rightarrow(\neg p) \pounds \neg p$
h) $p\Rightarrow q, (\neg r)\Rightarrow(\neg q), r\Rightarrow(\neg p) \pounds \neg p$

23. Supondo que t,c,d e f representam as seguintes sentenças:

$t\equiv$ "ver televisão"

$c \equiv$ "ir ao cinema"

$d \equiv$ "ter dinheiro"

$f \equiv$ "ir de férias"

Considere o seguinte argumento:

a1. Ele vê televisão ou vai ao cinema;

a2. Se não tem dinheiro então não vai ao cinema;

a3. Uma condição suficiente para ir de férias é ter dinheiro;

a4. Ele não vê televisão;

a5. Logo, ele vai de férias!

a) Traduza através de proposições lógicas as afirmações anteriores.
b) Mostre se o argumento é valido.

24. Sendo P e Q os conjuntos de verdade de, respectivamente, $p(x)$ e $q(x)$, determine os conjuntos de verdade das fórmulas $\neg p(x), \neg q(x), p(x) \wedge (\neg q(x))$, e interprete em termos de conjuntos de verdade as fórmulas $p(x) \Rightarrow q(x)$ e $p(x) \Leftrightarrow q(x)$.

25. Escreva as frases que se seguem usando notação lógica na qual x designa um gato e $p(x)$ significa "x gosta de creme".

a) Todos os gatos gostam de creme.
b) Nenhum gato gosta de creme.
c) Um gato gosta de creme.
d) Alguns gatos não gostam de creme.

26. Sendo A, B, C três conjuntos quaisquer, analise em termos lógicos, usando quantificadores, a proposição "se $A \subseteq B$ então A e $C \setminus B$ são disjuntos".

27. Escreva a proposição negação da proposição apresentada.

a) Algumas pessoas gostam de matemática.
b) Todas as pessoas gostam de gelado.

c) Algumas pessoas são altas e magras

28. Considere a proposição

$$Q: \quad \forall_{x\in\mathbb{N}_1} \forall_{y\in\mathbb{N}_1} \left[\left(t(x) \wedge v(y,x) \right) \Rightarrow \neg p(x,y) \right]$$

tal que, $t(x) \equiv 'x > 1'$, $v(y,x) \equiv 'y = x+1'$, $p(x,y) \equiv 'x \text{ divide } y'$ e o domínio de quantificação é o conjunto dos naturais $\mathbb{N}_1$.

a) Averigúe, justificando, o valor lógico da interpretação seguinte

$$\left[\left(t(1) \wedge v(2,1) \right) \Rightarrow \neg p(1,2) \right].$$

b) Diga, justificando, qual o valor lógico de Q.

29. Traduza em linguagem simbólica as proposições que se seguem, indicando as escolhas que são apropriadas para os domínios correspondentes.

a) $x^2 - 4 = 0$ tem uma raiz positiva.
b) Toda a solução da equação $x^2 - 4 = 0$ é positiva.
c) Nenhuma solução da equação $x^2 - 4 = 0$ é positiva.
d) Todos os estudantes que entendem lógica gostam dela.

30. Considere $j(x)$ e $t(x)$ os predicados "x ouve o jogo de futebol" e "x vai à aula de Mat I", respectivamente.

a) Usando lógica de predicados, exprima de forma conveniente as seguintes afirmações:
   i. Nem todas vão à aula de Mat I.
   ii. Nem todos os que ouvem o jogo faltam à aula.
   iii. Todos os que faltam à aula ouvem o jogo.

b) Sendo J e T os conjuntos de verdade de $j(x)$ e $t(x)$, respectivamente, formule em termos de conjuntos as três afirmações anteriores.

31. Sendo $\mathbb{N}_0$ o domínio da quantificação, indique quais das proposições que se seguem são verdadeiras e quais são falsas.

a) $\forall_x \exists_y (2x - y = 0)$

b) $\exists_y \forall_x (2x - y = 0)$

c) $\forall_x \left[x < 10 \Rightarrow \forall_y \left[y < x \Rightarrow y < 9 \right] \right]$

d) $\exists_y \exists_z (y + z = 100)$

e) $\forall_x \exists_y \left[y > x \wedge (y + x = 100) \right]$

32. Negue a proposição "toda a gente tem um parente de quem não gosta" usando a simbologia lógica.

1.3 Relações e Aplicações

1.3.1 Produto cartesiano de conjuntos

Os conjuntos $\{a,b\}$, $\{b,a\}$ e $\{a,b,a\}$ são iguais porque têm os mesmos elementos; a ordem pela qual se escrevem os elementos é irrelevante, assim como não tem qualquer significado que um elemento apareça escrito uma só vez ou várias vezes. Em determinadas situações, é necessário distinguir conjuntos com os mesmos elementos colocados por ordens diferentes ou conjuntos nos quais um mesmo elemento aparece mais que uma vez.

Definição

Sejam A e B dois conjuntos não vazios. Chama-se produto cartesiano de A por B, e representa-se por $A \times B$, ao conjunto de todos os pares ordenados (a,b) tais que $a \in A$ e $b \in B$, ou seja,

$$A \times B = \{(a,b) : a \in A \wedge b \in B\}.$$

No caso particular em que se tem $A = B$ obtém-se o conjunto

$$A^2 = \{(a, a') : a, a' \in A\}$$

Designado por quadrado cartesiano de A.

O conceito de produto cartesiano pode ser estendido a mais de dois conjuntos. Assim, o produto cartesiano de n conjuntos $A_1, A_2, \dots, A_n$, denotado por $A_1 \times A_2 \times \dots \times A_n$ é definido por

$$A_1 \times A_2 \times \dots \times A_n = \{(x_1, x_2, \dots, x_n) : x_1 \in A_1 \wedge x_2 \in A_2 \wedge \dots \wedge x_n \in A_n\}$$

Se, em particular, se tiver $A_1 = A_2 = \dots = A_n = A$ obtém-se

$$A_1 \times A_2 \times \dots \times A_n = A^n = \{(x_1, \dots, x_n) : x_i \in A \text{ para todo } i = 1, 2, \dots, n\}$$

que é a potência cartesiana de ordem n do conjunto A.

Definição

Chama-se relação binária de A para B a todo o subconjunto não vazio $\measuredangle$ do produto cartesiano $A \times B$. Se, em particular, for $A = B$ então $\measuredangle$ diz-se uma relação binária definida em A.

Exemplo TC9

Sejam dados os conjuntos $A = \{1, 2, 3\}$ e $B = \{r, s\}$. Então

$$\mathrm{R} = \{(1, r), (2, s), (3, r)\}$$

é uma relação de A para B.

Exemplo TC10

Sejam A e B conjuntos de números reais. A relação ∡ (de igualdade) define-se da seguinte forma

$$a\mathrm{R}b \quad \text{se e só se} \quad a = b$$

para todo o $a \in A$ e todo o $b \in B$.

Exemplo TC11

Seja dado o conjunto $A = \{1, 2, 3, 4, 5\} = B$. Definindo a relação ∡ (menor que) em A:

$$a\mathrm{R}b \quad \text{se e só se} \quad a < b$$

então $\mathrm{R} = \{(1,2),(1,3),(1,4),(1,5),(2,3),(2,4),(2,5),(3,4),(3,5),(4,5)\}$.

Dada uma relação ∡ do conjunto A para o conjunto B chama-se domínio e contradomínio de ∡, respectivamente, aos conjuntos assim definidos:

$$\mathrm{D}(\mathrm{R}) = \{x \in A : \exists y \left[y \in B \wedge (x, y) \in \mathrm{R} \right]\}$$
$$\mathrm{I}(\mathrm{R}) = \{y \in B : \exists x \left[x \in A \wedge (x, y) \in \mathrm{R} \right]\}$$

1.3.2 Partições e relações de equivalência

Seja A um conjunto não vazio. Chama-se partição de A a uma família P_A de subconjuntos não vazios de A tais que:

1. cada elemento de A pertence a um e um só conjunto de P_A.
2. Se A_1 e A_2 forem dois elementos distintos da partição P_A então $A_1 \cap A_2 = \varnothing$.

Os elementos de P_A são designados por <u>blocos</u> ou <u>células</u> da partição

Exemplo TC12

Seja dado o seguinte conjunto $A = \{a, b, c, d, e, f, g, h\}$ e considerem-se os seguintes subconjuntos de A:

$$A_1 = \{a, b, c, d\},\ A_2 = \{a, c, e, f, g, h\}$$
$$A_3 = \{a, c, e, g\},\ A_4 = \{b, d\},\ A_5 = \{f, h\}$$

Então $\{A_1, A_2\}$ não é uma partição de A visto que $A_1 \cap A_2 \neq \varnothing$; $\{A_1, A_5\}$ também não é uma partição visto que $e \notin A_1$ e $e \notin A_e$. A família $\mathrm{P}_A = \{A_3, A_4, A_5\}$ é uma partição de A.

Definição

Seja A um conjunto não vazio e $\measuredangle$ uma relação binária definida em A. A relação $\mathrm{R} \subseteq A^2$ dir-se-á uma **relação de equivalência** em A se satisfazer as seguintes propriedades:

a) Reflexividade: $\forall a \left[a \in A \Rightarrow a\mathrm{R}a \right]$

b) Simetria: $\forall a, b \in A \left[a\mathrm{R}b \Rightarrow b\mathrm{R}a \right]$

c) Transitividade: $\forall a, b, c \in A \left[\left[a\mathrm{R}b \wedge b\mathrm{R}c \right] \Rightarrow a\mathrm{R}c \right]$

Sendo A um conjunto e $\mathrm{R} \subseteq A^2$ uma relação de equivalência chama-se **classe de equivalência** que contém o elemento $a \in A$ ao conjunto , denotado geralmente por $[a]$, definido por

$$[a] = \{x \in A : (x, a) \in \mathrm{R}\}$$

onde o elemento $a \in A$ diz-se **representante** da classe.

Teorema

Seja $\measuredangle$ uma relação de equivalência definida num conjunto A. Então:

(1) Cada elemento de A pertence à sua classe de equivalência, isto é, $a \in [a]$, qualquer que seja $a \in A$;

(2) A reunião de todas as classes de equivalência é o conjunto A, isto é, $\cup_{a \in A} [a] = A$;

(3) Dados dois elementos $a, b \in A$ ter-se-á $a\mathrm{R}b$ quando e só quando a e b pertencerem à mesma classe de equivalência, isto é,

$$\forall a, b \in A\left[a\mathrm{R}b \Leftrightarrow [a] = [b]\right]$$

(4) As classes de equivalência de dois elementos a e b de A para as quais é falsa a proposição $a\mathrm{R}b$ são disjuntas, isto é,

$$\forall a, b \in A\left[\neg(a\mathrm{R}b) \Rightarrow [a] \cap [b] = \varnothing\right]$$

Definição

Seja A um conjunto e $\measuredangle$ uma relação de equivalência em A. Chama-se conjunto quociente de A por $\measuredangle$, e denota-se por A/R, ao conjunto de todas as classes de equivalência determinadas em A por $\measuredangle$,

$$A/\mathrm{R} = \{[a] : a \in A\}$$

Teorema

Seja $\|$ uma partição de um conjunto não vazio de A e $\measuredangle$ a relação definida em A por $a\mathrm{R}b \Leftrightarrow a$ e b pertencem ao mesmo bloco de P. Então $\measuredangle$ é uma relação de equivalência.

Exemplo TC12

Seja dado o conjunto $A = \{1, 2, 3, 4\}$ e considere-se a partição $\mathrm{P} = \{\{1, 2, 3\}, \{4\}\}$. Determinar a relação de equivalência determinada em A pela partição $\|$.

Visto que os blocos de $\|$ são $\{1, 2, 3\}$ e $\{4\}$, então

$$\mathrm{R} = \{(1,1), (1,2), (1,3), (2,1), (2,2), (2,3), (3,1), (3,2), (3,3), (4,4)\}$$

É a relação de equivalência induzida em A pela partição ‖.

1.3.3 Relações de ordem

Seja A um conjunto não vazio e $\mathrm{R} \subseteq A^2$ uma relação binária qualquer definida em A. Para indicar que o par ordenado $(a,b) \in A^2$ pertence à relação $\measuredangle$ escreve-se também frequentemente $a\mathrm{R}b$, ou seja,

$$a\mathrm{R}b \Leftrightarrow (a,b) \in \mathrm{R}$$

quaisquer que sejam $a,b \in A$.

Exemplo TC13

Se $A = \{0,1,2,3,4,5\} \subset \mathbb{N}$ e $\measuredangle$ for a relação $\leq$ usual em $\mathbb{N}$, então

$$\begin{aligned} \leq = \{&(0,0),(0,1),(0,2),(0,3),(0,4),(0,5),(1,1),(1,2),(1,3),(1,4),(1,5) \\ &(2,2),(2,3),(2,4),(2,5),(3,3),(3,4),(3,5),(4,4),(4,5),(5,5)\} \end{aligned}$$

e escreve-se $a \leq b \Leftrightarrow (a,b) \in \leq$ quaisquer que sejam $a,b \in A$.

Definição

Chama-se **relação de ordem** definida no conjunto A a uma relação binária $\mathrm{R} \subseteq A^2$ com as seguintes propriedades:

(1) Reflexividade: $\forall a\left[a \in A \Rightarrow a\mathrm{R}a\right]$

(2) Anti-simetria: $\forall a,b \in A\left[\left[a\mathrm{R}b \wedge b\mathrm{R}a\right] \Rightarrow a = b\right]$

(3) Transitividade: $\forall a,b,c \in A\left[\left[a\mathrm{R}b \wedge b\mathrm{R}c\right] \Rightarrow a\mathrm{R}c\right]$

Se adicionalmente, $\measuredangle$ satisfizer a proposição

(4) Dicotomia: $\forall a,b\left[a,b \in A \Rightarrow \left[a\mathrm{R}b \vee b\mathrm{R}a\right]\right]$

dir-se-á uma **relação de ordem total**. Se $\measuredangle$ não for uma relação de ordem total também se designa, por vezes, relação de ordem parcial.

Exemplo TC14

1. Seja $\triangleq$ a família de conjuntos. A relação em $\triangleq$ definida por " A é um subconjunto de B " é uma ordem parcial.
2. Seja A um subconjunto qualquer de números reais. A relação $\leq$ em A é uma relação de ordem total – é a chamada ordem natural.
3. A relação $\measuredangle$ definida em $\mathbb{N}$ por " $x\mathrm{R}y$ se e só se x é múltiplo de y " é uma relação de ordem parcial em $\mathbb{N}$.

Definição

Seja $\measuredangle$ uma relação de ordem definida em A; a relação $\mathrm{R}^* \subset A^2$ definida por

$$\forall a, b \in A\left[a\mathrm{R}^*b \Leftrightarrow \left[a\mathrm{R}b \wedge a \neq b\right]\right]$$

diz-se uma **relação de ordem estrita** definida em A.

Definição

Chama-se conjunto ordenado a um par ordenado (A, R) onde A é um conjunto não vazio e $\measuredangle$ uma relação de ordem (parcial ou total) em A.

Se, para $a, b \in A$ se tiver $a\mathrm{R}b$ dir-se-á que b domina a ou que a precede b.

Seja $\measuredangle$ uma relação de ordem num conjunto A. Então a relação inversa $\measuredangle^{-1}$, definida por

$$a\mathrm{R}^{-1}b \Leftrightarrow b\mathrm{R}a$$

quaisquer que sejam os elementos $a, b \in A$, é também uma relação de ordem.

Elementos extremais de um conjunto ordenado

Sendo $(A,\leq)$ um conjunto (total ou parcialmente) ordenado dá-se o nome de máximo de A ao elemento de $a \in A$, se existir, tal que

$$\forall x\left[x \in A \Rightarrow x \leq a\right]$$

ou seja, a é o máximo de A se dominar todos os outros elementos de A.

Note-se que se a ordem $\leq$ não for total pode acontecer que não exista um elemento $a \in A$ comparável com todos os elementos $x \in A$ nos termos acima indicados: neste caso A não possuirá máximo.

Um elemento $a \in A$ diz-se maximal de $(A,\leq)$ se se verificar a condição

$$\forall x \in A\left[a \leq x \Rightarrow x = a\right]$$

ou equivalentemente,

$$\neg\exists x \in A\left[a \leq x \wedge x \neq a\right].$$

Isto é, $a \in A$ é um elemento maximal de $(A,\leq)$ se não existir nenhum outro elemento em A que o domine estritamente.

Chama-se mínimo de A ao elemento $b \in A$, se existir, que satisfaz a condição

$\forall x\left[x \in A \Rightarrow b \leq x\right]$

ou seja, b é o mínimo de A se preceder todos s outros elementos de A. Tal como no caso anterior um conjunto ordenado pode não possuir mínimo.

Um elemento $b \in A$ diz-se minimal se verificar a condição

$$\forall x \in A\left[x \leq b \Rightarrow x = b\right]$$

ou equivalentemente,

$$\neg\exists x \in A\left[x \leq b \Rightarrow x \neq b\right].$$

Isto é, $b \in A$ é um elemento minimal de $(A, \leq)$ se não existir nenhum outro elemento de A que o preceda estritamente.

Exemplo TC15

O conjunto $A = \{x \in \mathbb{R} : 0 < x < 1\}$ não possui máximo nem mínimo nem possui elementos maximais nem minimais.

Teorema

Seja A um conjunto ordenado pela relação de ordem (parcial ou total) $\leq$. Se $a \in A$ é máximo então a é um elemento maximal e é o único elemento maximal de A. Se $b \in A$ é mínimo então b é um elemento minimal e é único elemento minimal de A.

Definição

Seja $(A, \leq)$ um conjunto ordenado. Chama-se **cadeia** de A a um conjunto de A que é totalmente ordenado por $\leq$.

Definição

Seja A um conjunto totalmente ordenado pela relação $\leq$. Dir-se-á que $\leq$ é uma **boa ordem** ou que A é **bem ordenado** por $\leq$ se todo o subconjunto não vazio de A possuir mínimo.

1.3.4 Funções

Definição

Seja $f \subset A \times B$ uma relação de A para B. Se, para todo o $x \in A$ existir um e um só $y \in B$ tal que $(x, y) \in f$ dir-se-á que f é uma **aplicação** (ou **função**) de A em B; para significar que f é uma aplicação de A em B costuma escrever-se

$$f : A \to B$$

e, neste caso, escreve-se $y = f(x)$ dizendo que $y \in B$ é a **imagem** por f de $x \in A$.

Dada um aplicação $f : A \to B$, ao conjunto A também se dá o nome de domínio de f e representa-se por $\mathrm{D}(f) \equiv \mathrm{D}_f$ (ou, mais simplesmente, por D).

O conjunto $\mathrm{I}(f) \equiv f(A) = \{y \in B : [\exists x [x \in A \wedge y = f(x)]]\}$ designa-se por contradomínio da aplicação f. Se $f(A) = B$ dir-se-á que f é uma **aplicação sobrejectiva** (ou aplicação sobre B) ; a aplicação $f : A \to B$ diz-se **injectiva** (ou únivoca) se cada elemento de $f(A)$ for imagem de um só elemento de A, isto é, f é injectiva se e só se

$$\forall x, x' [x, x' \in A \Rightarrow [x \neq x' \Rightarrow f(x) \neq f(x')]]$$

o que significa que elementos distintos de A têm necessariamente imagens por f diferentes em $f(A) \subset B$. Se a aplicação $f : A \to B$ for simultaneamente injectiva e sobrejectiva diz-se que f é uma **aplicação bijectiva**.

Duas aplicações f, g são iguais, escrevendo-se $f = g$, se e só se forem satisfeitas as duas condições seguintes

(1) $\mathrm{D}_f = \mathrm{D}_g \equiv \mathrm{D}$;

(2) $\forall x [x \in \mathrm{D} \Rightarrow f(x) = g(x)]$.

Sejam A, B, C três conjuntos não vazios e $f : A \to B$ e $g : B \to C$ duas aplicações de A em B e B em C, respectivamente. Chama-se aplicação composta de g com f à aplicação

$$gof : A \to C$$

definida por $gof(x) = g(f(x)) \in C$.

Teorema

A composição de aplicações é associativa.

Definição

Dado um conjunto A chama-se aplicação identidade em A à aplicação $\mathrm{id}_A : A \to A$ definida por

$$\mathrm{id}_A(x) = x$$

qualquer que seja $x \in A$.

Teorema

Sendo $f : A \to B$ uma aplicação arbitraria então $\mathrm{id}_B of = f$ e $fo\mathrm{id}_A = f$.

Seja a aplicação $f : A \to B$ e E uma parte de A. Chama-se imagem de E por f e representa-se por $f(E)$ ao conjunto

$$f(E) = \left\{ y \in B : \left[\exists x \left[x \in E \wedge y = f(x) \right] \right] \right\}$$

podendo também escrever-se

$$f(E) = \left\{ f(x) \in B : x \in E \right\}.$$

Se F for uma parte de B, chama-se imagem recíproca ou inversa de F e representa-se por

$$f^{-1}(F)=\{x\in A:[\exists y[y\in F\wedge y=f(x)]]\}$$

podendo também escrever-se equivalentemente

$$f^{-1}(F)=\{x\in A: f(x)\in F\}.$$

Teorema

Se $f:A\to B$ for uma aplicação bijectiva a correspondência recíproca, que a cada $y\in B$ associa $f^{-1}(y)$, o único elemento do conjunto $f^{-1}(\{y\})$, é uma aplicação bijectiva e $fof^{-1}=\mathrm{id}_B$, $f^{-1}of=\mathrm{id}_A$.

A aplicação $f^{-1}:B\to A$ é chamada aplicação inversa ou recíproca de $f:A\to B$.

Exercícios – Relações e Funções

1. Seja $A=\{1,2,3\}$. Para cada uma das relações $\measuredangle$ indicadas a seguir, determine os elementos de $\measuredangle$, o domínio e o contradomínio de $\measuredangle$ e, finalmente, as propriedades (de reflexividade, simetria, anti-simetria , transitividade e dicotomia) que possui $\measuredangle$:

   a) $\measuredangle$ é a relação < em A.

   b) $\measuredangle$ é a relação $\geq$ em A.

   c) $\measuredangle$ é a relação $\subset$ em $\mathrm{P}(A)$.

2. Considere o conjunto $S=\{a,b,c,d,e\}$.

a) Para a relação de equivalência $\mathrm{R}=\{(a,a),(b,b),(c,c),(d,d),(e,e),(a,c),(c,a)\}\subseteq S^2$, determine o conjunto $[a]$.

b) Indique os pares ordenados da relação de equivalência induzida em S pela partição $\{\{a,b,c\},\{d,e\}\}$

3. Seja $\measuredangle$ uma relação num conjunto não vazio A. Sendo $x\in A$ define-se a classe $\measuredangle$ de x, denotada por $[x]_{\mathrm{R}}$, por $[x]_{\mathrm{R}}=\{y\in A: y\mathrm{R}x\}$.

   Sendo $A=\{1,2,3,4\}$ e $\mathrm{R}=\{(1,2),(1,3),(2,1),(1,1),(2,3),(4,2)\}$ determinar $[1]_{\mathrm{R}}$, $[2]_{\mathrm{R}}$, $[3]_{\mathrm{R}}$ e $[4]_{\mathrm{R}}$.

4. Mostre que a relação ~ em $\mathbb{Z}$ definida por $x\sim y$ sse $x-y=2k$ para algum k em $\mathbb{Z}$ é uma relação de equivalência e determine $[3]_{\sim}$.

5. Seja $\measuredangle$ uma relação de A para B e S uma relação de B para C. Então a relação composta $\mathrm{S}o\mathrm{R}$ é a relação constituída por todos os pares ordenados (a,c) tais que $(a,b)\in\mathrm{R}$ e $(b,c)\in\mathrm{S}$.

   Sendo $A=\{p,q,r,s\}$, $B=\{a,b\}$, $C=\{1,2,3,4\}$, $\mathrm{R}=\{(p,a),(p,b),(q,b),(r,a),(s,a)\}$ e $\mathrm{S}=\{(a,1),(a,2),(b,4)\}$ determine $\mathrm{S}o\mathrm{R}$.

6. Seja $\measuredangle$ a relação no conjunto $A=\{1,2,3,4,5,6,7\}$ definida por $(a,b)\in\mathrm{R}\Leftrightarrow(a-b)$ é divisível por 4. determinar $\measuredangle$ e R^{-1}.

7. Seja $\measuredangle$ a relação definida em $\mathbb{N}_2=\{2,3,4,5,\ldots\}$ por $(a,b)\in\mathrm{R}\Leftrightarrow a$ é divisor de b.

   a) Estude $\measuredangle$ quanto à reflexividade, simetria, anti-simetria e transitividade.

   b) Determinar todos os elementos minimais e maximais do conjunto $\mathbb{N}_2$ ordenado pela relação $\measuredangle$.

8. Diga quais das relações que se seguem são equivalências e, nesses casos, indique o correspondente conjunto quociente.

   a) $\{(1,1),(2,2),(3,3),(4,4),(1,3),(3,1)\}$

   b) $\{(1,2),(2,2),(3,3),(4,4)\}$

   c) $\{(1,1),(2,2),(1,2),(2,1),(3,3),(4,4)\}$

9. Seja $A=\{1,2,3,4,5\}\times\{1,2,3,4,5\}$, e seja $\measuredangle$ definida em A por

$$(x_1,y_1)\mathrm{R}(x_2,y_2)\Leftrightarrow x_1+y_1=x_2+y_2$$

   a) Verifique que $\measuredangle$ é uma relação de equivalência em A .

   b) Determine as classes de equivalência $[(1,3)],[(2,4)]$ e $[(1,1)]$.

   c) Determine a partição de A induzida por $\measuredangle$.

10. Considere a relação $\mathrm{R}\subseteq\mathbb{Z}^2$, tal que, $\forall a,b\in\mathbb{Z}$,

$a\mathrm{R}b$ se $(a-b)$ é um número inteiro não negativo par.

   a) Verifique que $\measuredangle$ define uma relação de ordem em $\mathbb{Z}$.

   b) $\measuredangle$ é uma relação de ordem total? Justifique.

11. Seja $A=\{1,2,3,4,5,6\}$ e $f:A\to A$ a função definida por

$$f(x)=\begin{cases}x+1 & \text{se } x\neq 6\\ 1 & \text{se } x=6\end{cases}$$

   a) Determinar $f(3), f(6), fof(3)$ e $f(f(2))$.

   b) Mostrar que f é injectiva.

12. Mostrar que a função $f:\mathbb{R}\rightarrow\mathbb{R}$ dada por $f(x)=x^3$ é injectiva e sobrejectiva enquanto que a função $g:\mathbb{R}\rightarrow\mathbb{R}$ dada por $g(x)=x^2-1$ não é injectiva nem sobrejectiva.

13. Sendo $\mathbb{N}$ o conjunto dos números naturais e $f:\mathbb{N}\rightarrow\mathbb{N}$ a função definida por $f(n)=2n+5$, mostre que f é injectiva e determinar a função inversa. Será f sobrejectiva? E a função inversa será sobrejectiva?

14. Seja $X=\{p,q,r\}$, $Y=\{a,b,c,d\}$ e $Z=\{1,2,3,4\}$ e sejam $g:X\rightarrow Y$ definida pelo conjunto dos pares ordenados $\{(p,a),(q,b),(r,c)\}$ e $f:Y\rightarrow Z$ definida pelo conjunto de pares ordenados $\{(a,1),(b,1),(c,2),(d,3)\}$. Escreva a função composta fog sob a forma de um conjunto de pares ordenados.

15. Se $f(x)=ax+b$ e $g(x)=cx+d$ e $fog=gof$, determine uma equação que relacione a constantes a,b,c,d.

2 Números Naturais e Indução Matemática

2.1 Axiomática dos Números Naturais

2.1.1 Os axiomas de Dedekind-Peano

A construção axiomática de Dedekind-Peano do conjunto dos números naturais parte de três termos primitivos – zero, número natural e sucessor – e de cinco axiomas que os relacionam:

N1 O zero é um número natural e representa-se por 0.

N2 Cada número natural n tem um e um só sucessor, representado por $\textbf{suc}(n)$, que é também um número natural.

N3 O zero não é sucessor de nenhum número natural.

N4 Se m, n são dois números naturais tais que $\textbf{suc}(m) = \textbf{suc}(n)$ então $m = n$.

N5 Seja A um conjunto de números naturais. Se A for tal que

(1) $0 \in \mathrm{A}$ e

(2) $\forall n \left[n \in \mathrm{A} \Rightarrow \mathrm{suc}(n) \in \mathrm{A} \right]$

então A é o conjunto constituído por todos os números naturais que é denotado por $\mathbb{N}$.

Exemplo NN1

Mostrar, a partir da axiomática de Dedekind-Peano, que todo o número natural diferente do zero é sucessor de um número natural.

Sendo $\mathrm{A} = \left\{ n \in \mathbb{N} : n = 0 \vee \exists m \left[m \in \mathbb{N} \wedge n = \mathrm{suc}(m) \right] \right\}$ então

1. $0 \in \mathrm{A}$ (pela definição do conjunto A)
2. Suponha-se que $n \in \mathrm{A}, n \neq 0$. Então $n = \mathrm{suc}(m)$ para algum $m \in \mathbb{N}$. Consequentemente, $\mathrm{suc}(n) = \mathrm{suc}(\mathrm{suc}(m))$ e como, por **N2**, $\mathrm{suc}(m) \in \mathbb{N}$ então $\mathrm{suc}(n) \in \mathrm{A}$.

Dos dois argumentos precedentes, tendo em conta N5, vem $\mathrm{A} = \mathbb{N}$ ficando provada a afirmação.

2.1.2 Aritmética dos números naturais

A aritmética dos números naturais baseia-se em duas operações: a adição e a multiplicação.

A **adição** de números naturais é uma operação interna, denotada pelo símbolo +, que é definida recursivamente por

A1 $\forall n \left[n \in \mathbb{N} \Rightarrow \left[n + 0 = n \right] \right]$,

A2 $\forall m, n \left[m, n \in \mathbb{N} \Rightarrow \left[n + \mathrm{suc}(m) = \mathrm{suc}(n + m) \right] \right]$

Podendo mostrar-se que existe uma e só uma operação interna, definida sobre $\mathbb{N}$ que satisfaça **A1** e **A2**.

Teorema

A adição em $\mathbb{N}$ é associativa.

Teorema

A adição em $\mathbb{N}$ é comutativa.

A multiplicação de números naturais é uma operação interna denotada pelo símbolo $\cdot$ que se define recursivamente por

M1 $\forall n\left[n \in \mathbb{N} \Rightarrow [n \cdot 0 = 0]\right]$

M2 $\forall m, n\left[m, n \in \mathbb{N} \Rightarrow \left[n \cdot \text{suc}(m) = n \cdot m + n\right]\right]$

sendo, também neste caso, possível provar que existe uma e uma só operação interna definida sobre $\mathbb{N}_0$ que satisfaça **M1** e **M2**.

Teorema

A multiplicação em $\mathbb{N}$ é distributiva à direita relativamente à adição, isto é, $m(n+p) = mn + mp$, quaisquer que sejam $m, n, p \in \mathbb{N}$.

Teorema

A multiplicação em $\mathbb{N}$ é associativa.

Teorema

A multiplicação em $\mathbb{N}$ é distributiva à esquerda relativamente à adição, isto é, $(m+n)\,p = mp + np$, quaisquer que sejam $m, n, p \in \mathbb{N}$.

Teorema

A multiplicação em $\mathbb{N}$ é comutativa.

2.1.3 O conjunto ordenado $(\mathbb{N}, \leq)$

Seja em $\mathbb{N}$ a relação $\measuredangle$ definida por

$$\mathsf{R} = \left\{ (m,n) \in \mathbb{N}^2 : \exists p \left[p \in \mathbb{N} \wedge m + p = n \right] \right\}.$$

Teorema

$\measuredangle$ é uma relação de ordem total (em sentido lato) em $\mathbb{N}$.

Dados dois elementos $m, n \in \mathbb{N}$ quaisquer, sempre que $(m,n) \in \mathsf{R}$ é usual escrever $m \leq n$ (ou $n \geq m$). Se para $m, n \in \mathbb{N}$, se tiver $m \leq n \wedge m \neq n$ então escreve-se $m < n$ (ou $n > m$). O par ordenado $(\mathbb{N}, \leq)$ designa-se por **conjunto ordenado dos números naturais**.

2.2 Indução Matemática

O princípio de indução matemática, decorrente do axioma **N5**, pode ser generalizado da seguinte forma: se $\mathsf{A} \subset \mathbb{Z}$ for um conjunto bem ordenado, tal que

1. $p \in A$ e p é o menor elemento de A,
2. $\forall n \in \mathbb{Z} \left[n \geq p \Rightarrow \left[n \in \mathsf{A} \Rightarrow n+1 \in \mathsf{A} \right] \right]$

então,

$$A = \{ n \in \mathbb{Z} : n \geq p \}.$$

O princípio de indução matemática usual é um caso particular deste enunciado no qual $p = 0$.

Este princípio é usado frequentemente em Matemática para provar proposições da forma $\forall n \left[n \in \mathbb{N}_r \Rightarrow p(n) \right]$, onde $\mathbb{N}_r = \{ n \in \mathbb{Z} : n \geq r \}$ e $p(n)$ é uma fórmula com uma variável livre cujo domínio é $\mathbb{N}_r$.

Considere-se, por exemplo, a seguinte proposição

$$\forall n \left[n \in \mathbb{N}_1 \Rightarrow 1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2} \right]$$

cuja prova se pode fazer apelando ao princípio de indução matemática generalizado. Seja $p(n)$ a fórmula

$$1+2+3+\ldots+n=\frac{n(n+1)}{2}$$

e $\mathrm{A} \subseteq \mathbb{N}$ o conjunto de verdade de $p(n)$.

Fazendo $n=1$ é imediato provar que $p(1)$ é uma proposição verdadeira e, portanto, $1 \in \mathrm{A}$. Suponha-se agora que $n \in \mathrm{A}$, ou seja, que para um dado inteiro $n>1$, fixado arbitrariamente, se verifica a proposição $p(n)$ - hipótese de indução. Vejamos o que se passa com $p(n+1)$. Ora

$$\begin{aligned}1+2+3+\ldots+n+(n+1) &= (1+2+3+\ldots+n)+(n+1)\\ &= \frac{n(n+1)}{2}+(n+1)\\ &= (n+1)\left(\frac{1}{2}n+1\right)\\ &= \frac{(n+1)(n+2)}{2}\end{aligned}$$

e, portanto, da validade da proposição $p(n)$ resulta a validade da proposição $p(n+1)$. Isto significa que se $n \in \mathrm{A}$ então $n+1 \in \mathrm{A}$. Pelo princípio de indução pode concluir-se que $\mathrm{A}=\mathbb{N}_1$ o que significa que $p(n)$ se verifica para todo o $n=1,2,\ldots$.

Exemplo NN2

Sendo $x \geq 0$ um número real pretende-se mostrar que

$$\forall n\left[n \in \mathbb{N}_1 \Rightarrow (1+x)^n \geq 1+x^n\right].$$

Por questões de comodidade denote-se por $p(n)$ a fórmula $(1+x)^n \geq 1+x^n$ e aplique-se a $p(n)$ o método de indução.

Para $n=1$ obtém-se $1 \geq 1$ o que mostra que $p(1)$ é uma proposição verdadeira.

Suponha-se, hipótese de indução, que para $n>1$, arbitrariamente fixado, $p(n)$ se verifica e considere-se então $p(n+1)$:

$$
\begin{aligned}
(1+x)^{n+1} &= (1+x)^n (1+x) \\
&\geq \left(1+x^n\right)(1+x) = 1+x+x^n+x^{n+1} \\
&\geq 1+x^{n+1}.
\end{aligned}
$$

Então da validade de $p(n)$ resulta a validade de $p(n+1)$ e, portanto, pelo princípio de indução matemática pode afirmar-se que $p(n)$ se verifica qualquer que seja $n=1,2,\ldots$.

2.2.1 Formas equivalentes do princípio de indução finita

A versão do princípio de indução tal como foi estabelecido na axiomática de Dedekind-Peano é, muitas vezes, designada por **forma fraca** do princípio de indução, por oposição a uma outra formulação que lhe é equivalente e que é conhecida por **forma forte** do princípio de indução ou, mais simplesmente, por **indução completa**. A indução completa tem a seguinte formulação

Sendo A um conjunto de números naturais tal que

1. $0 \in \mathrm{A}$
2. $\forall n\left[n \in \mathbb{N} \Rightarrow \left[\{0,1,\ldots,n\} \subset \mathrm{A} \Rightarrow n+1 \in \mathrm{A}\right]\right]$

então $\mathrm{A}=\mathbb{N}$.

Para provar que as duas formulações são equivalentes é necessário fazer apelo a uma propriedade importante do conjunto $\mathbb{N}$ que é conhecida por princípio de boa ordenação.

Seja A um subconjunto qualquer do conjunto ordenado $\mathbb{N}$. Um elemento $a \in \mathrm{A}$ dir-se-á primeiro elemento de A se e só se verificar a condição

$$\forall x\left[x \in \mathrm{A} \Rightarrow a \leq x\right]$$

Podendo verificar-se que quando um tal elemento existe ele é único.

Teorema

Todo o subconjunto não vazio de $\mathbb{N}$ possui primeiro elemento.

Demonstração

Seja $A \subset \mathbb{N}$ não vazio e suponha-se, por redução ao absurdo que A não possui primeiro elemento. Designando por $\overline{A}$ o complementar de A em $\mathbb{N}$, considere-se o conjunto

$$\mathrm{T} \equiv \left\{ n \in \mathbb{N} : \forall_{m \in \mathbb{N}} \left[m \leq n \Rightarrow m \in \overline{A} \right] \right\}.$$

Como 0 não poder pertencer a A (de contrário seria certamente o primeiro elemento de A) então $0 \in \overline{A}$ e, portanto, $0 \in \mathrm{T}$. Suponha-se agora que $k \in \mathrm{T}$. Da definição de T, resulta então que os números $1, 2, \ldots, k$ pertencem todos a $\overline{A}$. Quanto a $k+1$ não pode pertencer a A pois de contrário seria o seu primeiro elemento o que é contra a hipótese feita; então $(k+1) \in \overline{A}$ e, portanto, $(k+1) \in \mathrm{T}$. Visto que

a) $0 \in \mathrm{T}$, e

b) $\forall_k \left[k \in \mathrm{T} \Rightarrow k+1 \in \mathrm{T} \right]$,

então, pelo axioma N5, segue-se que $\mathrm{T} = \mathbb{N}$. Em consequência vem $\overline{A} = \mathbb{N}$ e, portanto, $A = \varnothing$ o que contradiz a hipótese considerada. Logo, A possui primeiro elemento. □

É costume traduzir o resultado deste teorema dizendo que $\mathbb{N}$ é um conjunto **bem-ordenado**.

Teorema

Em $\mathbb{N}$ verifica-se o princípio de indução completa, ou seja, sendo A um conjunto de números naturais tal que:

1. $0 \in A$,
2. $\forall_n \left[n \in \mathbb{N} \Rightarrow \left[\{0,1,\dots,n\} \subset A \Rightarrow n+1 \in A \right] \right]$

então $A = \mathbb{N}$.

Demonstração

Seja $\overline{A}$ o complementar de A. Se $\overline{A} = \varnothing$ então o teorema está trivialmente demonstrado e, portanto, suponha-se que $\overline{A} \neq \varnothing$. Pelo princípio de boa ordenação, $\overline{A}$ possui um primeiro elemento que se designará por k. É claro que $k \neq 0$ visto que $0 \in A$ por hipótese; por outro lado, $0,1,2,\dots,k-1$ têm que pertencer a A pois de contrário algum deles seria o primeiro elemento de $\overline{A}$ e não k como se supôs. Então, pela segunda condição do teorema, ter-se-á também $k \in A$ o que contradiz a hipótese de ser k o primeiro elemento do complementar de A. Assim, ter-se-á necessariamente $\overline{A} \neq \varnothing$ e, portanto, $A = \mathbb{N}$. □

Para completar o ciclo de implicações que nos permite concluir a equivalência dos dois princípios de indução e do princípio da boa ordenação de $\mathbb{N}$, mostrar-se-á agora que o princípio de indução completa implica a indução fraca.

Teorema

Suponha-se que se verifica em $\mathbb{N}$ o princípio de indução completa e seja A um conjunto de números naturais tal que:

1. $0 \in A$
2. $\forall_n \left[n \in \mathbb{N} \Rightarrow \left[n \in A \Rightarrow n+1 \in A \right] \right]$

então $A = \mathbb{N}$.

Demonstração

Suponha-se que se verificam as duas condições acima. Visto que a proposição

$$\forall_{n\in\mathbb{N}}\left[\{0,1,\dots,n\}\subseteq A\Rightarrow n\in A\right]$$

é evidentemente verdadeira, então tem-se que

$$\forall_{n\in\mathbb{N}}\left[\left[\{0,1,\dots,n\}\subseteq A\right]\wedge\left[n\in A\Rightarrow n+1\in A\right]\right]$$

Donde resulta imediatamente,

$$\forall_{n\in\mathbb{N}}\left[\{0,1,\dots,n\}\subseteq A\Rightarrow n+1\in A\right] .$$

Pelo princípio de indução completa ter-se-á então $A=\mathbb{N}$, ficando demonstrado o teorema. □

Suponha-se que $p(n)$ é uma afirmação sobre o número natural n e que r é um número natural fixado. Então a demonstração por indução de que $p(n)$ se verifica para todo o $n\geq r$ requer os dois seguintes passos:

1. Verificar que $p(r)$ é uma proposição verdadeira.
2. Verificar que se $k\geq r$ e se $p(r), p(r+1), p(r+2),\dots, p(k)$ são proposições verdadeiras, então $p(k+1)$ também é verdadeira.

Exemplo NN3

Mostrar, por indução completa, que qualquer número natural maior do que 1 se pode decompor num produto de dois factores primos.

Seja $p(n)$ a afirmação de que quando n é um número natural maior do que 1 se pode decompor num produto de factores primos. O objectivo agora é do de provar que $p(n)$ é um proposição verdadeira qualquer que seja $n>1$.

1. $p(2)$ é, evidentemente, uma proposição verdadeira pois 2 (sendo primo) pode ser factorizado num produto de factores primos (neste caso com um só factor).

2. Suponha-se agora que $p(2), p(3), \ldots, p(k)$ são proposições todas verdadeiras. Pretende-se então mostrar que da veracidade destas proposições resulta a veracidade de $p(k+1)$.

Se $k+1$ for um número primo a afirmação é trivialmente verdadeira. Se $k+1$ não for primo então é um número composto sendo, portanto, possível encontrar dois inteiros positivos m e n tais que $k+1 = m \cdot n$ onde tanto m como n são menores do que k. Pela hipótese de indução completa, tanto m como n se podem decompor num produto de factores primos e, portanto, o mesmo acontece a $k+1$. Logo $p(k+1)$ é uma proposição verdadeira, como se pretendia mostrar.

Exemplo NN4

Para mostrar que as três formulações alternativas da indução matemática – princípio da indução finita, princípio da boa ordenação e princípio da indução completa – podem ser usadas para resolver o mesmo tipo de problemas exemplificar-se-á a demonstração da proposição

$$\forall_n \left[n \in \mathbb{N}_1 \Rightarrow 1+2+\ldots+n = n(n+1)/2 \right]$$

usando o princípio da boa ordenação.

Represente-se por $p(n)$ a fórmula

$$1+2+\ldots+n = \frac{1}{2}n(n+1).$$

Seja $A = \{ n \in \mathbb{N}_1 : \neg p(n) \}$. Se $A = \varnothing$ então a proposição fica automaticamente demonstrada. Suponha-se então que $A \neq \varnothing$. Pelo princípio da boa ordenação, A tem um primeiro elemento, k. Visto que $p(1)$ é evidentemente verdadeira, então $1 \notin A$ e, portanto, $k \neq 1$, donde se pode concluir que $k-1 \in \mathbb{N}_1$. Como, por outro lado, $k-1 \notin A$ então $p(k-1)$ é verdadeira. Então, tem-se o seguinte,

$$\begin{aligned}1+2+\ldots+(k-1)+k &= \frac{1}{2}(k-1)k+k \\ &= k\left(\frac{1}{2}(k-1)+1\right) \\ &= \frac{1}{2}k(k+1)\end{aligned}$$

O que mostra que $p(k)$ é uma proposição verdadeira. Mas isto é contraditório com o facto de k ser o primeiro elemento de A. A contradição resultou de se supor que A era não vazio o que, portanto, é falso. Ou seja, $p(n)$ verifica-se para todo o $n \in \mathbb{N}_1$.

Exemplo NN5

Mostrar, usando o princípio da boa ordenação, que $\sqrt{2}$ é um número irracional.

Suponha-se, pelo contrário, que $\sqrt{2}$ é racional; isto é, existem números $r, s \in \mathbb{N}_1$ tais que $\sqrt{2} = r/s$. Então,

$$A = \left\{x \in \mathbb{N} : x = n\sqrt{2} \text{ para algum } n \in \mathbb{N}_1\right\}$$

será um conjunto não vazio de números naturais (em particular, conterá, por hipótese, o número r). Pelo princípio da boa ordenação o conjunto A possuirá um primeiro elemento: suponha-se que é k esse elemento. Seja $m \in \mathbb{N}$ tal que $k = m\sqrt{2}$. Então $m\left(\sqrt{2}-1\right) = k - m$ é um número natural menor que m (visto que $0 < \sqrt{2}-1 < 1$) e, portanto, $q = m\left(\sqrt{2}-1\right)\sqrt{2}$ é menor que k. Mas $q = 2m - k$ o que significa que $q \in \mathbb{N}$, por um lado, e, por outro lado, $q \in A$. Esta conclusão é contraditória visto que se encontra em A um elemento menor do que k. Então A deverá ser vazio e, portanto, $\sqrt{2}$ não é um número racional.

Exercícios - Indução

1. Utilizando o princípio de indução prove que:

a) $4+10+16+\ldots+(6n-2)=n(3n+1), \quad \forall n \in \mathbb{N}$ ~

b) $1^2+2^2+3^2+\ldots+n^2=\dfrac{n(n+1)(2n+1)}{6}, \quad \forall n \in \mathbb{N}$

c) $1^2-2^2+3^2-\ldots+(-1)^{n+1}n^2=\dfrac{(-1)^{n+1}n(n+1)}{2}, \quad \forall n \in \mathbb{N}$

d) $1.3+2.4+3.5+\ldots+n.(n+2)=\dfrac{n(n+1)(2n+7)}{6}, \quad \forall n \in \mathbb{N}$

e) $1.2+2.3+3.4+\ldots+n(n+1)=\dfrac{n(n+1)(n+2)}{3}, \quad \forall n \in \mathbb{N}$

2. Prove as seguintes proposições:

a) $\forall_n \left[n \in \mathbb{N} \Rightarrow 1^3+2^3+\ldots+n^3=\left(\dfrac{n(n+1)}{2}\right)^2 \right]$

b) $\forall n \left[n \in \mathbb{N} \Rightarrow \left(1+\dfrac{1}{3}\right)^n \geq 1+\dfrac{n}{3} \right]$

3. Prove que:

a) $2n+1 \leq 2^n, \quad n \geq 3$

b) $(1+x)^n \geq 1+nx,$ com $n \in \mathbb{N}$ e $x \in \mathbb{R}$ tal que $x \geq -1$

c) $n^2 > n+1,$ com $n \geq 2$

d) $1.2.3.\ldots.n > 2^n, \quad n \geq 4$

e) $\dfrac{1}{\sqrt{1}}+\dfrac{1}{\sqrt{2}}+\dfrac{1}{\sqrt{3}}+\ldots+\dfrac{1}{\sqrt{n}} > \sqrt{n}, \quad n \geq 2$

4. Utilizando o princípio de indução prove que:

a) n^5-n é divisível por 5 $\forall n \in \mathbb{N}$

b) Se n é um número ímpar então 7^n+1 é divisível por 8.

3 Determinantes

A qualquer matriz quadrada está associado um elemento de ⌒, chamado determinante, usualmente representado por

$$\det(A) \text{ ou } |A|.$$

Este elemento surge através do estudo e investigação de sistemas de equações lineares.
Antes de definir determinante, necessitamos da noção de permutação.

6.1 Permutações

Definição
Uma aplicação biunívoca σ do conjunto $S_n = \{1, 2, \dots, n\}$ sobre si mesma é chamada uma *permutação*. Denotamos a permutação σ por

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ j_1 & j_2 & \dots & j_n \end{pmatrix} \text{ ou } \sigma = j_1\, j_2 \dots j_n \text{ onde } j_i = \sigma(i)$$

Exemplo D1
Em S_3 existem 3!=6 permutações em: 123; 132; 213; 231; 312; 321.

Definição
Consideremos uma permutação par (ou impar) caso exista um número par (ou impar) de pares (i,k) para os quais $i > k$, mas i antecede k em σ.

Exemplo D2
Consideremos a permutação σ= 35142 em S_5. 3 e 5 antecedem e são maiores que 1; portanto (3, 1) e (5, 1) satisfazem a condição anterior, tal como (3, 2), (5, 2) , (4, 2), (5, 4). Existem portanto exactamente 6 pares, logo σ é uma permutação par.

Definição

Definimos o *sinal* ou *paridade* de σ, denota-se por sgn σ, por

$$\operatorname{sgn} \sigma = \begin{cases} 1 & \text{se } \sigma \text{ par} \\ -1 & \text{se } \sigma \text{ ímpar} \end{cases}$$

Exemplo D3

No exemplo anterior, dado que a permutação é par, então o sgn σ =1**.**

6.2 Determinantes. Definição e Propriedades

6.2.1 Definição

Seja $A = \left(a_{ij}\right)$ uma matriz quadrada de ordem n sobre um corpo $\frown$.

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}$$

Consideremos um produto de n elementos de A tal que um e somente um, elemento provém de cada linha e um, e somente um , elemento provém de cada coluna.

Tal produto pode ser escrito na forma $a_{1j_1} a_{2j_2} \ldots\ldots a_{nj_n}$.

Isto é, onde os factores proveêm de linhas sucessivas; logo os primeiros índices estão na ordem natural 1, 2,..., n. Agora, como os factores proveêm de colunas diferentes, a sequência dos segundos índices forma uma permutação $\sigma = j_1 j_2 \ldots j_n$ em S_n. Reciprocamente cada permutação em S_n, determina um produto da forma acima. Assim, podemos formar $n!$ desses produtos, a partir da matriz A.

Definição

O determinante de uma matriz quadrada de ordem n, $A = \left(a_{ij}\right)$, denotado por $\det\left(A\right)$ ou $|A|$, é a seguinte soma efectuada sobre todas as permutações $\sigma = j_1 j_2 \ldots j_n$ em S_n:

$$|A| = \sum_{\sigma} (\text{sgn}\,\sigma) a_{1j_1} a_{2j_2} \ldots a_{nj_n}.$$

Isto é

$$|A| = \sum_{\sigma \in S_n} (\text{sgn}\,\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \ldots a_{n\sigma(n)}.$$

Diz-se que o determinante da matriz quadrada de ordem n, é de ordem n e é frequentemente representado por

$$|A| = \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{vmatrix}$$

6.2.2 Determinantes de 2ª ordem

Em S_2, a permutação 12 é par a permutação 21 é ímpar. Portanto

$$|A| = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}.a_{22} - a_{12}.a_{21}$$

Assim,

$$\begin{vmatrix} 4 & -5 \\ -1 & -2 \end{vmatrix} = 4(-2) - (-5)(-1) = -13$$

6.2.3 Determinantes de 3ª ordem

Em S_3, as permutações 123, 231 e 312 são pares e as permutações 321, 213 e 132 são ímpares. Portanto,

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} - a_{11}a_{23}a_{32}$$

Podemos escrever a expressão anterior da seguinte forma:

$$a_{11}(a_{22}a_{33} - a_{23}a_{32}) - a_{12}(a_{21}a_{33} - a_{23}a_{31}) + a_{13}(a_{21}a_{32} - a_{22}a_{31})$$

Que é o mesmo que

(I) $$a_{11}\begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} - a_{12}\begin{vmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{vmatrix} + a_{13}\begin{vmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{vmatrix}.$$

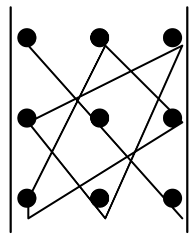
Podemos recorrer a matrizes de ordem inferior para calcular o determinante.

Para além disso esta fórmula é facilmente memorizada visto que se obtém suprimindo à matriz A a primeira linha e respectivamente, as primeiras, segundas e terceiras colunas. O determinante de ordem 2 que se obtém suprimindo a primeira linha e a j-ésima coluna deve ser multiplicado pelo elemento que ocupa a entrada $(1, j)$ (i.e. o elemento a_{1j}); os produtos obtidos devem ser considerados com sinais alternados e, finalmente adicionados.

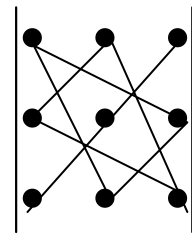
- **Regra de Sarrus**

Esta regra dá-nos um modo para determinar as parcelas e os respectivos sinais. Só é válida para determinantes de ordem 3.

Esta regra diz-nos que as parcelas <u>positivas</u> são o produto dos elementos da diagonal principal, e também, os produtos dos elementos situados nos vértices de triângulos de bases paralelas a essa diagonal; por outro lado, as parcelas <u>negativas</u> são o produto dos elementos da outra diagonal, e também, os produtos dos elementos situados nos vértices de triângulos de bases paralelas a essa diagonal. Esta regra pode ser ilustrada pelos diagramas seguintes:



Parcelas com sinal +



Parcelas com sinal –

Exemplo D4

Considere-se $A=\begin{bmatrix} 1 & 0 & 3 \\ 2 & -1 & 5 \\ 0 & -2 & 1 \end{bmatrix} \in M_3(\mathbb{R})$.

Então pela regra de Sarrus, temos

$$|A| = 1\times(-1)\times1+2\times(-2)\times3+0\times5\times0-0\times(-1)\times3-(-2)\times5\times1-2\times0\times1=-3$$

6.2.4 Outra definição de Determinante

A formula **(I)** sugere-nos a ideia de definirmos indutivamente o conceito de determinante de uma matriz quadrada sobre um corpo ⌒. Para efeito, começamos por introduzir a notação seguinte. Seja $A=\left[a_{ij}\right]\in M_n(¼)$. Denotaremos por $A(i \mid j)$ a matriz que se obtém de A suprimindo a i-ésima linha e a j-ésima coluna.

Definição

Define-se o determinante de uma matriz $A=\left[a_{ij}\right]$ de ordem $n+1$, como:

$$|A| = \sum_{j=1}^{n+1}(-1)^{1+j}a_{1j}\,|A(1|\,j)| = a_{11}\,|A(1|1)| - a_{12}\,|A(1|2)| + \cdots + (-1)^{n+2}a_{1n+1}\,|A(1|\,n+1)|$$

6.2.5 Propriedades de Determinantes

Teorema D1

O determinante de uma matriz A e da sua transposta A^T são iguais: $|A| = |A^T|$.

Demonstração

Suponhamos que $A = (a_{ij})$. Então $A^T = (b_{ij})$, onde $b_{ij} = a_{ji}$. Portanto,

$$\begin{aligned} |A^T| &= \sum_{\sigma \in S_n} (\text{sgn}\,\sigma) b_{1\sigma(1)} b_{2\sigma(2)} \ldots b_{n\sigma(n)} \\ &= \sum_{\sigma \in S_n} (\text{sgn}\,\sigma) a_{\sigma(1)1} a_{\sigma(2)2} \ldots a_{\sigma(n)n} \end{aligned}$$

Seja $\tau = \sigma^{-1}$, que é a permutação que $a_{\sigma(1)1} a_{\sigma(2)2} \ldots a_{\sigma(n)n} = a_{1\tau(1)} a_{2\tau(2)} \ldots a_{n\tau(n)}$, $\tau \in S_n$.

$$\begin{aligned} &= \sum_{\tau \in S_n} (\text{sgn}\,\tau) a_{1\tau(1)} a_{2\tau(2)} \ldots a_{n\tau(n)} \\ &= |A| \end{aligned}$$

□

Teorema D2

Seja B a matriz obtida da matriz A por:

1) Multiplicação de uma linha (coluna) por um escalar k; então $|B| = k|A|$.
2) Troca entre si de duas linhas (respectivamente, colunas) de A; então $|B| = -|A|$.

Demonstração

1) Se a i-ésima linha é multiplicada por k, então cada termo em $|A|$ é multiplicado por k; então

$$\begin{aligned} |B| &= \sum_{\sigma \in S_n} (\text{sgn}\,\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \ldots (k a_{i\sigma(j)}) \ldots a_{n\sigma(n)} \\ &= k \sum_{\sigma \in S_n} (\text{sgn}\,\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \ldots a_{i\sigma(j)_i} \ldots a_{n\sigma(n)} \\ &= k\,|A| \end{aligned}$$

ou seja, $|B| = k|A|$.

2) Vamos provar o teorema para o caso em que duas colunas são trocadas. Seja τ a transposição que troca entre si dois números correspondentes às duas colunas de A, que são trocadas entre si.

Se $A = (a_{ij})$ e $B = (b_{ij})$, então $b_{ij} = a_{i\tau(j)}$. Portanto, para qualquer permutação σ.

Assim

$$|B| = \sum_{\sigma \in S_n} (\text{sgn}\,\sigma) b_{1\sigma(1)} \ldots b_{n\sigma(n)} = \sum_{\sigma \in S_n} (\text{sgn}\,\sigma) a_{1\tau\sigma(1)} a_{2\tau\sigma(2)} \ldots a_{n\tau\sigma(n)}$$

Como τ é impar, sgn $\tau\sigma$ = sgn τ. sgn σ, assim sgn σ = –sgn $\tau\sigma$, então

$$|B| = -\sum_{\sigma \in S_n} (\text{sgn}\,\tau\sigma)\; a_{1\tau\sigma(1)} a_{2\tau\sigma(2)} \ldots a_{n\tau\sigma(n)}$$

Dado que, σ percorre todos os elementos de S_n, então $\tau\sigma$ também percorre todos os elementos de S_n, portanto $|B| = -|A|$. □

Teorema D3

Seja A uma matriz quadrada.

1) Se A tem uma linha (coluna) de zeros então $|A| = 0$.

2) Se A tem duas linhas (colunas) idênticas, então $|A| = 0$.

3) Se A é triangular superior ou triangular inferior, então $|A|$ = produto dos elementos da diagonal principal. Assim em particular $|I|$=1, onde I é a matriz identidade.

Demonstração

1) Cada parcela em $|A|$ contém um factor de cada linha; então contém um elemento da linha de zeros. Assim, cada parcela de $|A|$ é zero, logo $|A| = 0$.

2) Se trocarmos entre si duas linhas idênticas de A, ainda obtemos a matriz A. Logo, pelo teorema D2, $|A| = -|A|$, então $|A| = 0$.

3) Suponhamos que $A = (a_{ij})$ é triangular inferior, isto é, os elementos acima da diagonal principal são zeros, ou seja $a_{ij} = 0$, sempre que $i < j$. Consideremos um termo t do determinante de A:

$$t = (\text{sgn}\,\sigma) a_{1i_1} a_{2i_2} \ldots a_{ni_n}, \text{onde } \sigma = i_1 i_2 \ldots i_n.$$

Suponhamos $i_1 \neq 1$. Então, $1 < i_1$ logo, $i_{1i_1} = 0$; portanto, $t = 0$. Isto é, cada termo para o qual $i_1 \neq 1$ é zero.

Agora , suponhamos $i_1 = 1$, mas $i_2 \neq 2$. Então, $2 < i_2$; logo $a_{2i_2} = 0$; portanto $t = 0$. Assim, cada termo para o qual $i_1 \neq 1$ ou $i_2 \neq 2$ é zero.

Analogamente, obtemos cada termo para o qual $i_1 \neq 1$ ou $i_2 \neq 2$ ou.... ou $i_n \neq n$ é zero. De acordo com isso, $|A| = a_{11} a_{22} \ldots a_{nn}$. Ou seja o produto dos elementos da diagonal. $\square$

Teorema D4

Seja B a matriz obtida da matriz A por substituição de uma linha (coluna) de A pela soma dessa linha (coluna) multiplicada por um escalar; então $|B| = |A|$.

Demonstração

Suponhamos que c vezes a k-ésima linha é somada à j-ésima linha de A. Usando o símbolo $\wedge$ para denotar a j-ésima posição num termo do determinante, temos:

$$\begin{aligned} |B| &= \sum_{\sigma \in S_n} (\text{sgn}\,\sigma) a_{1i_1} a_{2i_2} \ldots \widehat{\left(c a_{ki_k} + a_{ji_j}\right)} \ldots a_{ni_n} \\ &= c \sum_{\sigma \in S_n} (\text{sgn}\,\sigma) a_{1i_1} a_{2i_2} \ldots \widehat{a_{ki_k}} \ldots a_{ni_n} + \sum_{\sigma \in S_n} (\text{sgn}\,\sigma) a_{1i_1} a_{2i_2} \ldots \widehat{a_{ji_j}} \ldots a_{ni_n} \end{aligned}$$

A primeira soma é o determinante de uma matriz, cujas k-ésimas e j-ésimas linhas são idênticas; então pelo teorema D3 , a soma é zero. A segunda soma é o determinante de A. Assim,

$$|B| = c.0 + |A| = |A|$$ □

Corolário D5

Seja A qualquer matriz quadrada $n \times n$. Então são equivalentes as seguintes afirmações:

1) A é invertível
2) $c(A) = n$
3) $|A| \neq 0$

Teorema D6

O determinante de um produto de duas matrizes A e B é igual ao produto seus determinantes: $|AB| = |A|.|B|$.

Corolário D7

Seja $A = (a_{ij}) \in M_n(\mathbb{R})$. Então $|\alpha A| = \alpha^n |A|, \quad \forall \alpha \in \mathbb{R}$.

Corolário D8

Se A é invertível então $|A^{-1}| = \dfrac{1}{|A|}$.

6.2.6 Regra de Laplace

Teorema D9 (Regra de Laplace**)**

Seja $A=\left(a_{ij}\right)\in M_n\left(¼\right)$. Então

I. $|A|=\sum_{j=1}^{n}(-1)^{i+j}a_{ij}\,|A(i\,|\,j)|$ (desenvolvimento segundo a i-ésima linha)

II. $|A|=\sum_{i=1}^{n}(-1)^{i+j}a_{ij}\,|A(i\,|\,j)|$ (desenvolvimento segundo a j-ésima coluna)

Demonstração

1) Trocando sucessivamente as linhas $l_i \leftrightarrow l_{i-1} \leftrightarrow \ldots \leftrightarrow l_2 \leftrightarrow l_1$ (num total de $i-1$ permutações) obtemos a matriz

$$A_i=\begin{bmatrix} a_{i1} & a_{i2} & \cdots & a_{in} \\ a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & & \vdots \\ a_{i-11} & a_{i-12} & \cdots & a_{i-1n} \\ a_{i+11} & a_{i+12} & \cdots & a_{i+1n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}$$

Pelo teorema D2(2), temos que $|A_i|=\left(-1\right)^{i-1}|A|$. Assim, obtemos

$$|A|=\left(-1\right)^{i-1}|A_i|=(-1)^{i-1}\sum_{j=1}^{n}(-1)^{1+j}a_{ij}\,|A_i(1|\,j)|=\sum_{j=1}^{n}(-1)^{i+j}a_{ij}\,|A(i\,|\,j)|$$

Uma vez que $A_i\left(1|\,j\right)=A\left(i|\,j\right)$ isto estabelece a igualdade 1).

Para 2), consideramos a matriz A^T. Por i), temos

$$\left|A^T\right| = \sum_{j=1}^{n} (-1)^{i+j} b_{ij} \mid B(i \mid j) \mid = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \mid A(j \mid i) \mid ,$$

uma vez que $b_{ij} = a_{ji}$ e $A^T(i|j) = A(j|i)$. Dado que $\left|A^T\right| = |A|$, então

$$|A| = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} \mid A(i \mid j) \mid . \qquad \square$$

Exemplo D5

Neste exemplo, aplicamos a regra de Laplace para o cálculo do seguinte determinante:

$$\begin{vmatrix} 2 & 0 & 1 & 0 & 0 \\ 0 & 0 & 3 & 0 & 0 \\ 1 & 4 & 0 & -3 & 1 \\ -1 & 2 & 1 & 1 & 5 \\ 2 & -3 & 5 & 3 & 3 \end{vmatrix} = (-1)^{2+3} 3 \begin{vmatrix} 2 & 0 & 0 & 0 \\ 1 & 4 & -3 & 1 \\ -1 & 2 & 1 & 5 \\ 2 & -3 & 3 & 3 \end{vmatrix} = -3(-1)^{1+1} 2 \begin{vmatrix} 4 & -3 & 1 \\ 2 & 1 & 5 \\ -3 & 3 & 3 \end{vmatrix}$$

$$= -6.3 \begin{vmatrix} 4 & -3 & 1 \\ 2 & 1 & 5 \\ -1 & 1 & 1 \end{vmatrix} = 18(4+2+15+1-20+6) = -144$$

6.3 Matriz Adjunta

Definições

- $\left|A(i|j)\right|$ chamamos o (i, j) - ésimo menor de A
- $(-1)^{i+j}\left|A(i|j)\right|$ chamamos o (i, j) - ésimo cofactor de A. Denota-se por $|A|_{ij}$.

Nesta notação, a regra de Laplace toma a forma :

$$|A| = a_{i1}|A|_{i1} + a_{i2}|A|_{i2} + \ldots + a_{in}|A|_{in} = a_{1j}|A|_{1j} + a_{2j}|A|_{2j} + \ldots + a_{nj}|A|_{nj}$$

Observemos os sinais $(-1)^{i+j}$, que acompanham os menores, são alternadamente "+" e "–" que se dispõem na forma que se segue, com os "+" na diagonal principal

$$\begin{vmatrix} + & - & + & - & \cdots \\ - & + & - & + & \ldots \\ + & - & + & - & \cdots \\ - & + & - & + & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{vmatrix}$$

Definição

Chamamos matriz adjunta de A, denota-se por $A*$ à seguinte matriz

$$A* = \begin{vmatrix} |A|_{11} & \cdots & |A|_{1n} \\ \vdots & & \vdots \\ |A|_{n1} & \cdots & |A|_{nn} \end{vmatrix}^T$$

Esta matriz dá- nos a seguinte relação entre a matriz inversa e a própria matriz:

$$AA* = |A| I_n$$

Teorema D10

Seja $A \in M_n(¼)$. Então A é invertível sse $|A| \neq 0$. Se é este o caso, temos

$$A^{-1} = \frac{1}{|A|} A*.$$

Este resultado é muito útil principalmente para matrizes dois por dois.

Exemplo D6

Vamos calcular a inversa da seguinte matriz . $A=\begin{bmatrix}3 & 4\\ 5 & 1\end{bmatrix}$.

$|A| = 3-20 = -17$

$|A|_{11} = 1;\quad |A|_{12} = -5;\quad |A|_{21} = -4;\quad |A|_{22} = 3$

Então $A^{*}=\begin{bmatrix}1 & -5\\ -4 & 3\end{bmatrix}^{T}$, e a inversa é então $A^{-1}=-\dfrac{1}{17}\begin{bmatrix}1 & -4\\ -5 & 3\end{bmatrix}$.

6.4 Sistema de Cramer

A teoria dos determinantes pode ser aplicada à resolução de um certo tipo de sistemas de equações lineares.

Com efeito, seja S um sistema de equações lineares representado matricialmente por $Ax=B$, onde $A\in M_n(¼)$ e $B\in M_{n\times 1}(¼)$ (S tem o mesmo número de incógnitas e de equações). Se $|A|\neq 0$, então $c(A)=n$ e , portanto, S é possível e determinado, isto é tem solução única. Um sistema nestas condições diz-se um SISTEMA DE CRAMER. O resultado seguinte diz-nos que a única solução de S pode ser expressa em termos de determinantes. De facto, temos:

Teorema D11

Seja S um sistema de Cramer representado matricialmente por $Ax=B$, onde $A=(a_{ij})\in M_n(¼)$ e $B=(b_{ij})\in M_{n\times 1}(¼)$. Seja $(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \frown^n$ a única solução de S.

Então

$$\alpha_j = \frac{\begin{vmatrix} a_{11} & \cdots & a_{1j-1} & b_1 & a_{1j+1} & \cdots & a_{1n}\\ a_{21} & \vdots & a_{2j-1} & b_2 & a_{2j+2} & \cdots & a_{2n}\\ \vdots & & \vdots & \vdots & \vdots & & \vdots\\ a_{1n} & \cdots & a_{nj-1} & b_n & a_{nj+n} & \cdots & a_{nn}\end{vmatrix}}{|A|}$$

Demonstração

Como $(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{R}^n$ é solução de S, temos

$$A\begin{bmatrix}\alpha_1\\ \alpha_2\\ \vdots\\ \alpha_n\end{bmatrix} = \begin{bmatrix}b_1\\ b_2\\ \vdots\\ b_n\end{bmatrix}.$$

Agora como A é invertível, podemos multiplicar a igualdade acima, à esquerda e à direita, pela matriz A^{-1}, obtendo

$$\begin{bmatrix}\alpha_1\\ \alpha_2\\ M\\ \alpha_n\end{bmatrix} = A^{-1}A\begin{bmatrix}\alpha_1\\ \alpha_2\\ M\\ \alpha_n\end{bmatrix} = A^{-1}\begin{bmatrix}b_1\\ b_2\\ M\\ b_n\end{bmatrix} = \frac{1}{|A|}A^*\begin{bmatrix}b_1\\ b_2\\ M\\ b_n\end{bmatrix}.$$

Assim temos

$$\alpha_j = \frac{1}{|A|}((-1)^{1+j}\,|A(1|\,j)|\,b_1 + (-1)^{2+j}\,|A(2|\,j)|\,b_2) + \cdots + (-1)^{n+j}\,|A(n|\,j)|\,b_n),$$

uma vez que

$$A^* = \left[|A|_{ij}\right] = \left[(-1)^{i+j}\,|A(i\,|\,j)|\right].$$

Ora pela regra de Laplace (desenvolvendo o determinante em relação à j-ésima coluna)

$$\begin{vmatrix} a_{11} & \cdots & a_{1j-1} & b_1 & a_{1j+1} & \cdots & a_{1n}\\ a_{21} & \vdots & a_{2j-1} & b_2 & a_{2j+2} & \cdots & a_{2n}\\ \vdots & & \vdots & \vdots & \vdots & & \vdots\\ a_{1n} & \cdots & a_{nj-1} & b_n & a_{nj+n} & \cdots & a_{nn}\end{vmatrix} = (-1)^{1+j}\,|A(1|\,j)|\,b_1 + (-1)^{2+j}\,|A(2|\,j)|\,b_2) + \cdots + (-1)^{n+j}\,|A(n|\,j)|\,b_n$$

Logo os α_j têm a forma desejada. □

Exemplo D7

Seja S o sistema de três equações lineares a três incógnitas sobre ○

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

Matricialmente, S é representado pelo sistema $Ax=B$, onde

$$A=\begin{bmatrix} 2 & 3 & -1 \\ 1 & 1 & 2 \\ 0 & -1 & 1 \end{bmatrix} \in M_3(\mathbb{R}) \text{ e } B=\begin{bmatrix} 1 \\ 2 \\ -3 \end{bmatrix} \in M_{3\times 1}(\mathbb{R}).$$

Como $|A|$=2+1+0–0+4–3= 4 $\neq$0, S é sistema de Cramer e a sua única solução (α_1, α_2, α_3) $\in$ ○^{3} é dada por

$$\alpha_1=\frac{\begin{vmatrix} 1 & 3 & -1 \\ 2 & 1 & 2 \\ -3 & -1 & 1 \end{vmatrix}}{|A|}, \quad \alpha_2=\frac{\begin{vmatrix} 2 & 1 & -1 \\ 1 & 2 & 2 \\ 0 & -3 & 1 \end{vmatrix}}{|A|}, \quad \alpha_3=\frac{\begin{vmatrix} 2 & 3 & 1 \\ 1 & 1 & 2 \\ 0 & -1 & -3 \end{vmatrix}}{|A|}$$

Logo,

$$\alpha_1=\frac{1+2-18-3+2-6}{4}=-\frac{11}{2},\ \alpha_2=\frac{4+3+0-0+12-1}{4}=\frac{9}{2},\ \alpha_3=\frac{-6-1+0-0+4+9}{4}=\frac{3}{2}.$$

Exercícios – Determinantes

1. Calcule os determinantes das seguintes matrizes:

a) $\begin{bmatrix} u & v \\ w & x \end{bmatrix}$, b) $\begin{bmatrix} 1 & 2 & 10 \\ 2 & 4 & 100 \\ 3 & 6 & \frac{1000}{\pi} \end{bmatrix}$, c) $\begin{bmatrix} 0 & 7 & 6 \\ 5 & 8 & 5 \\ 1 & 1 & 0 \end{bmatrix}$,

d) $\begin{bmatrix} 3 & 1 & 0 & 0 \\ 1 & 3 & 1 & 0 \\ 0 & 1 & 3 & 1 \\ 0 & 0 & 1 & 3 \end{bmatrix}$ e) $\begin{bmatrix} 1 & 3 & 2 & -1 \\ 0 & -1 & 1 & 0 \\ 2 & 3 & 1 & -2 \\ 1 & 0 & -1 & 3 \end{bmatrix}$ f) $\begin{bmatrix} 0 & 1 & 3 & -1 \\ -1 & 0 & 2 & -1 \\ 1 & 1 & 2 & 1 \\ 8 & 0 & 3 & 1 \end{bmatrix}$

2. Supondo que $\begin{vmatrix} a & b & c \\ 2 & 1 & 0 \\ 1 & 2 & 1 \end{vmatrix} = 1$, calcule os determinantes seguintes:

$$\begin{vmatrix} a & b & c \\ 3 & 3 & 1 \\ -\frac{1}{2} & -1 & -\frac{1}{2} \end{vmatrix}, \qquad \begin{vmatrix} a & b & c \\ 2a+2 & 2b+1 & 2c \\ a-1 & b-2 & c-1 \end{vmatrix}, \qquad \begin{vmatrix} 1 & -1 & -1 \\ 2 & 1 & 0 \\ 2a-1 & 2b-2 & 2c-1 \end{vmatrix}$$

3. Utilizando as propriedades dos determinantes mostre que :

$$\begin{vmatrix} a+b+2c & a & b \\ c & 2a+b+c & b \\ c & a & a+2b+c \end{vmatrix} = 2(a+b+c)^3$$

4. Resolva as seguintes equações em ○:

$$\begin{vmatrix} a+3 & -1 & 1 \\ 5 & a-3 & 1 \\ 6 & -6 & a+4 \end{vmatrix} = 0, \qquad \begin{vmatrix} 1 & a & 2 & a \\ 0 & 1 & 1 & 3 \\ 1 & a & 2a & 1 \\ 0 & 0 & 0 & a \end{vmatrix} = 0, \qquad \begin{vmatrix} a+1 & a & a & a \\ a & a+1 & a & a \\ a & a & a+1 & a \\ a & a & a & a+1 \end{vmatrix} = 0$$

5. Seja $A \in M_n(\mathbb{R})$. Prove que :

a) Se A é ortogonal então $|A| = \pm 1$.

b) Se A é anti-simétrica , i.e $A = -A^T$ e n é ímpar então $|A| = 0$.

c) Se $B \in M_n(\mathbb{R})$ é semelhante a A i.e. existe $P \in M_n(\mathbb{R})$ tal que $B = P^{-1}AP$, então $|B| = |A|$.

6. Considere a matriz $A = \begin{bmatrix} 2 & -2 & 1 \\ 0 & 3 & 0 \\ -1 & 1 & 1 \end{bmatrix} \in M_3(\mathbb{R})$.

a) Calcule $|A|$. Os vectores $v_1 = (2,0,-1), v_2 = (-2,3,1), v_3 = (1,0,1)$ constituem uma base de $\mathbb{R}^3$?

b) Determine a matriz adjunta de A , i.e. A^*.

c) Determine A^{-1}.

7. Prove que os seguintes sistemas de coeficientes reais são sistemas de Cramer e determine , usando a regra de Cramer, as suas (únicas) soluções.

$$\begin{cases} x+2y-3z=1 \\ 2x-3y+5z=-2 \\ 3x-y+z=0 \end{cases} \qquad \text{e} \qquad \begin{cases} 2x+z-t=-1 \\ x+y+z=-2 \\ 2y-z-3t=-3 \\ x+3y-2t=-4 \end{cases}$$

8. Seja S um sistema não homogéneo com $n+1$ equações lineares e n incógnitas e seja A' a sua matriz ampliada.

a) Prove que se S é possível então $|A'| = 0$.

b) Diga, justificando, se o recíproco da alínea a) é verdadeiro .