notas para a disciplina

Tópicos de Matemática Discreta

licenciatura em Engenharia Informática

Universidade do Minho 2006/2007

Cláudia Mendes Araújo

Noções elementares de lógica

1 Proposições

Os elementos básicos da lógica são as proposições. Uma *proposição* é uma afirmação formal sobre a qual se pode dizer, objectivamente, se é verdadeira ou falsa (assume um e um só *valor lógico*: verdadeiro - denotado por V ou 1 - ou falso - denotado por F ou 0). Usaremos as letras minúsculas $p, q, r, s, t, \ldots$ (possivelmente com índices - $p_0, p_1, p_2, \ldots$) para representar proposições.

A afirmação "5 é um número par" é uma proposição (no caso falsa) já que o seu valor lógico não depende do sujeito que o atribui. O mesmo acontece com a afirmação "$x^2 = -1$ não tem soluções reais", sendo esta proposição verdadeira. Não recorrendo a afirmações que envolvam expressões matemáticas, existem afirmações que são proposições. Por exemplo, "O traje académico da UM é amarelo, com listas de todas as cores do arco-íris". Também a afirmação "Existe vida em Marte" é uma proposição. Esta afirmação será verdadeira ou falsa (mas não ambas as coisas), apesar de não sabermos o seu valor lógico. Outras afirmações existem, por seu turno, que por falta de objectividade na atribuição do valor lógico, não podem ser consideradas proposições. A título de exemplo, a afirmação "Os alunos da UM são os melhores alunos universitários do país". A não objectividade da afirmação parece óbvia. Ainda outro exemplo, "Esta proposição é falsa".

Existem, ainda, outras afirmações que sendo de índole matemática, não é possível aferir-lhes o valor lógico. Por exemplo, "$x \geq 6$" tem o seu valor lógico dependente do valor que se atribui a x.

Podemos combinar várias proposições por forma a obter novas proposições, as chamadas *proposições compostas*, usando operadores lógicos como o "não", o "e" e o "ou".

1.1 Negação

[Exemplo] "5 não é um número par" é a negação da proposição "5 é um número par".

Se uma proposição é falsa, a sua negação é verdadeira, e se é verdadeira, a sua negação é falsa. Assim, a operação lógica de negação tem o efeito de trocar o valor lógico de qualquer proposição a que seja aplicada. Podemos expressar, de forma bastante clara, o significado das operações lógicas usando as chamadas *tabelas de verdade*.

Dada uma proposição p, denotamos por $\neg p$ a sua negação (lemos "não p" ou "é falso p"). A tabela de verdade da negação de uma proposição p tem duas linhas que correspondem às

duas possibilidades de valor lógico de p:

p	$\neg p$
V	F
F	V

Ou seja, a negação de uma proposição é verdadeira exactamente quando tal proposição é falsa.

1.2 Conjunção e disjunção

Vimos já como podemos *criar* uma nova proposição à custa da negação. Com a conjunção e a disjunção podemos *criar* uma proposição à custa de um par de proposições.

[Exemplo] A afirmação "5 é um número primo e existe vida em Marte" é uma conjunção de duas proposições, enquanto que a afirmação "5 é um número primo ou existe vida em Marte" é uma disjunção de duas proposições.

Dadas duas proposições p e q, denotamos por $p \wedge q$ a sua conjunção (lemos "p e q"). A tabela de verdade da conjunção é a seguinte:

p	q	$p \wedge q$
V	V	V
V	F	F
F	V	F
F	F	F

Ou seja, a conjunção de duas proposições é verdadeira somente no caso em que ambas são verdadeiras.

Dadas duas proposições p e q, denotamos por $p \vee q$ a sua disjunção (lemos "p ou q"). A disjunção é definida pela seguinte tabela:

p	q	$p \vee q$
V	V	V
V	F	V
F	V	V
F	F	F

Note-se que a disjunção de duas proposições é falsa somente quando ambas as proposições são falsas.

[Exemplo] Consideremos as afirmações do exemplo anterior. Referimos já que "existe vida em Marte" é uma proposição cujo valor lógico ainda desconhecemos. Suponhamos que não existe, de facto, vida em Marte. Sabemos, contudo, que 5 é um número primo. Assim, a proposição composta "5 é um número primo e existe vida em Marte" será falsa (porque uma

das proposições que a compõem é falsa), enquanto que a afirmação "5 é um número primo ou existe vida em Marte" será verdadeira (já que uma das proposições que a compõem é verdadeira).

Consideremos, agora, as chamadas *proposições condicionais*.

1.3 Proposições condicionais

Sejam p e q proposições. Define-se implicação $p \Rightarrow q$ (e lê-se "p implica q", "se p, então q", "p é suficiente para q", "q é necessário para p", "q se p", "p somente se q" ou ainda "q sempre que p") através da tabela seguinte:

p	q	$p \Rightarrow q$
V	V	V
V	F	F
F	V	V
F	F	V

Ou seja, $p \Rightarrow q$ é verdadeira quando é impossível que q seja falsa sendo p verdadeira.

Chamamos *antecedente* ou *hipótese* à proposição p e *consequente* ou *conclusão* à proposição q.

[Exemplos] Alguns exemplos:

- A expressão "Se amanhã é Sábado, então hoje é Sexta" é obviamente verdadeira: de facto, se partimos da veracidade do antecedente "amanhã é Sábado", sabemos que o consequente "hoje é Sexta" é, também, verdadeiro.
- A proposição "Se todos os números inteiros são pares, então 5 é divisível por 2" é verdadeira: com efeito, se todos os inteiros são pares, sendo 5 um inteiro, podemos concluir que 5 é par e, portanto, que 5 é divisível por 2.
- A proposição "Se *bonjour* é francês, então *auf wiedersehen* é italiano" é falsa: note-se que o antecedente é verdadeiro mas o consequente é falso.

Consideremos, agora, as afirmações seguintes:

> Se estou doente, então vou ao médico.
>
> Se vou ao médico, então estou doente.

Estas são proposições bastante diferentes. O que significa dizer que ambas são verdadeiras? A conjunção das duas pode ser expressa da seguinte forma:

> Vou ao médico se e só se estou doente.

Dadas duas proposições p e q, define-se a equivalência $p \Leftrightarrow q$ (e lê-se "p é equivalente a q", "p se e só se q" ou ainda "p é necessário e suficiente para q") através da seguinte tabela de verdade:

p	q	$p \Leftrightarrow q$
V	V	V
V	F	F
F	V	F
F	F	V

Ou seja, uma equivalência é verdadeira quando as proposições que a compõem têm o mesmo valor lógico.

[Exemplos] Alguns exemplos:

- "$1 + 3 = 4$ é equivalente a $4 = 1 + 3$"
- "$1 + 1 = 1$ se e só se chover canivetes"

2 Fórmulas, tautologias e equivalências lógicas

[Definição] Uma *fórmula (proposicional)* é uma expressão obtida a partir das letras $p, q, r, s, t, \ldots$ (possivelmente com índices) – a que chamaremos *variáveis proposicionais* – através dos símbolos que representam as várias operações lógicas estudadas ($\neg$, $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$) – chamaremos a estes símbolos *conectivos proposicionais* –, e com base nas seguintes regras:

r1. toda a variável proposicional é uma fórmula;

r2. se φ é uma fórmula, então $(\neg\varphi)$ é uma fórmula;

r3. se φ e ψ são fórmulas, então $(\varphi \wedge \psi)$ é uma fórmula;

r4. se φ e ψ são fórmulas, então $(\varphi \vee \psi)$ é uma fórmula;

r5. se φ e ψ são fórmulas, então $(\varphi \Rightarrow \psi)$ é uma fórmula;

r6. se φ e ψ são fórmulas, então $(\varphi \Leftrightarrow \psi)$ é uma fórmula.

[Exemplo] A expressão $((p \wedge (\neg q)) \vee r)$ é uma fórmula, como demonstra o seguinte raciocínio:

1. p, q e r são fórmulas pela regra $(r1)$ da definição de fórmulas;
2. $(\neg q)$ é uma fórmula por (1) e pela regra $(r2)$ da definição de fórmulas;
3. $(p \wedge (\neg q))$ é uma fórmula por (1), por (2) e pela regra $(r3)$ da definição de fórmulas;
4. $((p \wedge (\neg q)) \vee r)$ é uma fórmula por (1), por (3) e pela regra $(r4)$ da definição de fórmulas.

[Observação] Os parênteses extremos e os parênteses à volta de negações são geralmente omitidos por simplificação de escrita. Por exemplo, a expressão $(p \wedge \neg q) \vee r$ será utilizada como uma representação da fórmula $((p \wedge (\neg q)) \vee r)$.

A cada fórmula proposicional temos associado um valor lógico e as tabelas de verdade tornam-se bastante úteis quando pretendemos determinar o valor lógico de uma fórmula mais complexa.

[Exemplo] Por exemplo, construamos a tabela de verdade da fórmula $\neg(p \wedge q)$. Em primeiro lugar, tomamos todas as combinações possíveis de valores lógicos para p e q. Temos 4 casos distintos:

p	q
V	V
V	F
F	V
F	F

Façamos a conjunção $p \wedge q$ em primeiro lugar:

p	q	$p \wedge q$
V	V	V
V	F	F
F	V	F
F	F	F

Por último, a negação:

p	q	$p \wedge q$	$\neg(p \wedge q)$
V	V	V	F
V	F	F	V
F	V	F	V
F	F	F	V

Ou seja, a fórmula $\neg(p \wedge q)$ é verdadeira excepto quando ambas p e q são verdadeiras.

Na construção da tabela de verdade associada a uma dada fórmula proposicional, temos de ter em conta as várias combinações possíveis de valores lógicos para as variáveis proposicionais que a compõem. Se uma fórmula φ tem n variáveis proposicionais (distintas), então existem 2^n combinações possíveis de valores lógicos para as variáveis proposicionais de φ. Assim, a tabela de verdade de φ terá 2^n linhas.

[Exemplo] A tabela de verdade da fórmula $(\neg p \vee q) \wedge r$ é a seguinte:

p	q	r	$\neg p$	$\neg p \vee q$	$(\neg p \vee q) \wedge r$
V	V	V	F	V	V
V	V	F	F	V	F
V	F	V	F	F	F
V	F	F	F	F	F
F	V	V	V	V	V
F	V	F	V	V	F
F	F	V	V	V	V
F	F	F	V	V	F

[Definição] Chama-se *tautologia* a uma fórmula que seja sempre verdadeira, independentemente dos valores lógicos das variáveis proposicionais que a compõem. Por outras palavras, uma tautologia é uma fórmula cuja tabela de verdade associada tem apenas V's na última coluna.

[Exemplo] A fórmula $p \vee \neg p$ é uma tautologia, como podemos comprovar na tabela de verdade associada:

p	$\neg p$	$p \vee \neg p$
V	F	V
F	V	V

[Definição] Uma fórmula diz-se uma *contradição* se o valor lógico que lhe está associado é sempre o falso, independentemente dos valores lógicos das variáveis proposicionais que a compõem. Por outras palavras, uma contradição é uma fórmula cuja tabela de verdade associada tem apenas F's na última coluna.

[Exemplo] A fórmula $p \wedge \neg p$ é uma contradição, como podemos comprovar na tabela de verdade associada:

p	$\neg p$	$p \wedge \neg p$
V	F	F
F	V	F

[Definição] Duas fórmulas proposicionais φ e ψ dizem-se *(logicamente) equivalentes* se a fórmula $\varphi \Leftrightarrow \psi$ é uma tautologia. Neste caso, $\varphi \Leftrightarrow \psi$ diz-se uma *equivalência (lógica)*.

[Exemplo] As fórmulas $p \vee \neg q$ e $\neg(\neg p \wedge q)$ são equivalentes, uma vez que a fórmula proposicional $(p \vee \neg q) \Leftrightarrow (\neg(\neg p \wedge q))$ é uma tautologia:

p	q	$\neg p$	$\neg q$	$p \vee \neg q$	$\neg p \wedge q$	$\neg(\neg p \wedge q)$	$(p \vee \neg q) \Leftrightarrow (\neg(\neg p \wedge q))$
V	V	F	F	V	F	V	V
V	F	F	V	V	F	V	V
F	V	V	F	F	V	F	V
F	F	V	V	V	F	V	V

[Proposição] Dadas fórmulas φ, ψ e σ, temos as seguintes equivalências lógicas:

$((\varphi \vee \psi) \vee \sigma) \Leftrightarrow (\varphi \vee (\psi \vee \sigma))$	$((\varphi \wedge \psi) \wedge \sigma) \Leftrightarrow (\varphi \wedge (\psi \wedge \sigma))$	associatividade
$(\varphi \vee \psi) \Leftrightarrow (\psi \vee \varphi)$	$(\varphi \wedge \psi) \Leftrightarrow (\psi \wedge \varphi)$	comutatividade
$(\varphi \vee \varphi) \Leftrightarrow \varphi$	$(\varphi \wedge \varphi) \Leftrightarrow \varphi$	idempotência
$(\varphi \vee (\varphi \wedge \neg\varphi)) \Leftrightarrow \varphi$	$(\varphi \wedge (\varphi \vee \neg\varphi)) \Leftrightarrow \varphi$	elemento neutro
$(\varphi \vee (\varphi \vee \neg\varphi)) \Leftrightarrow (\varphi \vee \neg\varphi)$	$(\varphi \wedge (\varphi \wedge \neg\varphi)) \Leftrightarrow (\varphi \wedge \neg\varphi)$	elemento absorvente
$\neg(\varphi \wedge \psi) \Leftrightarrow (\neg\varphi \vee \neg\psi)$	$\neg(\varphi \vee \psi) \Leftrightarrow (\neg\varphi \wedge \neg\psi)$	leis de De Morgan
$\neg\neg\varphi \Leftrightarrow \varphi$		dupla negação
$(\varphi \Leftrightarrow \psi) \Leftrightarrow ((\varphi \Rightarrow \psi) \wedge (\psi \Rightarrow \varphi))$		
$(\varphi \Rightarrow \psi) \Leftrightarrow (\neg\varphi \vee \psi)$		

Demonstração. Mostremos a equivalência lógica $\neg(\varphi \wedge \psi) \Leftrightarrow (\neg\varphi \vee \neg\psi)$ (as restantes provas ficam para exercício). Atendendo à tabela de verdade

φ	ψ	$\neg\varphi$	$\neg\psi$	$\varphi \wedge \psi$	$\neg(\varphi \wedge \psi)$	$\neg\varphi \vee \neg\psi$	$\neg(\varphi \wedge \psi) \Leftrightarrow (\neg\varphi \vee \neg\psi)$
V	V	F	F	V	F	F	V
V	F	F	V	F	V	V	V
F	V	V	F	F	V	V	V
F	F	V	V	F	V	V	V

podemos concluir que $\neg(\varphi \wedge \psi) \Leftrightarrow (\neg\varphi \vee \neg\psi)$ é uma tautologia e, portanto, uma equivalência lógica. □

3 Alguns métodos de prova

As afirmações de teor matemático carecem sempre de uma sucessão de argumentos, encadeados entre si de uma forma logicamente correcta. Enumeraremos algumas formas distintas de demonstração.

3.1 Prova de uma implicação

A formulação de um resultado do tipo $p \Rightarrow q$ é bastante frequente. Para demonstrar directamente a veracidade de um tal resultado, temos de encontrar uma prova de q, assumindo a veracidade de p.

[Exemplo] O enunciado do seguinte resultado é do tipo $p \Rightarrow q$, sendo apresentada uma sua prova directa:

Proposição_ Se a e b são números reais tais que $0 < a < b$, então $a^2 < b^2$.

Demonstração_ Sejam a e b dois números reais tais que $0 < a < b$. Pretendemos mostrar que $a^2 < b^2$. Temos que

$$\begin{aligned} a < b &\Rightarrow a \cdot a < a \cdot b \\ &\Leftrightarrow a^2 < ab. \end{aligned}$$

e

$$\begin{aligned} a < b &\Rightarrow a \cdot b < b \cdot b \\ &\Leftrightarrow ab < b^2. \end{aligned}$$

Assim,

$$a^2 < ab < b^2,$$

pelo que $a^2 < b^2$. □

[Observação] Provar $p \Leftrightarrow q$ passa por encontrar uma prova de $p \Rightarrow q$ e uma prova de $q \Rightarrow p$.

Quando se pretende demonstrar uma implicação, é conveniente lembrar que $p \Rightarrow q$ é equivalente a $\neg q \Rightarrow \neg p$. Em certas ocasiões, mostrar $\neg q \Rightarrow \neg p$ é mais fácil do que mostrar $p \Rightarrow q$. Diz-se, nesses casos, que a prova é feita por contraposição.

[Exemplo] A demonstração do seguinte resultado, cujo enunciado é do tipo $p \Rightarrow q$, é feita por contraposição:

Proposição_ Se um natural n é tal que $n^2 > 25$, então $n > 5$.

Demonstração_ Mostremos, por contraposição, que se $n \leq 5$, então $n^2 \leq 25$. Ora, se $n \leq 5$, sabemos que $n \in \{1, 2, 3, 4, 5\}$. Logo, $n^2 = 1$ ou $n^2 = 4$ ou $n^2 = 9$ ou $n^2 = 16$ ou $n^2 = 25$. Portanto, $n^2 \leq 25$. □

[Exemplo] Eis outro exemplo de uma prova de uma implicação por contraposição:

Proposição_ Todo o número natural primo maior que 2 é ímpar.

Demonstração_ Esta afirmação pode ser reescrita da seguinte forma: para $n > 2$,

$$n \text{ primo } \Rightarrow n \text{ ímpar.}$$

Para mostrar o resultado por contraposição, assumamos que n não é ímpar, ou seja, que n é par. Portanto, existe $k \in \mathbb{N}$ tal que $n = 2k$. Ora, 2 é então divisor de n, pelo que n não é primo. □

3.2 Prova por contradição ou redução ao absurdo (reductio ad absurdum)

Por forma a provar p, podemos assumir $\neg p$ e procurar uma contradição.

[Exemplo] A seguinte prova é feita por redução ao absurdo:

Proposição_ Existe um número infinito de números primos.

Demonstração_ Admitamos, por absurdo, que existem apenas n números primos, denotados por $p_1, p_2, \ldots, p_n$. Consideremos o número $x = p_1 p_2 \ldots p_n + 1$. É óbvio que x não é divisível por nenhum dos números $p_1, p_2, \ldots, p_n$, já que o resto da divisão é sempre 1. Então, x é primo, o que contradiz a nossa hipótese inicial de que existem apenas n números primos. Logo, essa hipótese inicial está errada e, portanto, existe um número infinito de números primos. □

[Observação] Suponhamos que se pretende mostrar $p \Rightarrow q$. Note-se que $p \Rightarrow q$ é logicamente equivalente a $\neg (p \wedge \neg q)$. A redução ao absurdo consiste em assumir a veracidade da conjunção $p \wedge \neg q$ e procurar uma contradição. Por conseguinte, $\neg (p \wedge \neg q)$ será verdadeira, tal como $p \Rightarrow q$.

4 Quantificadores

Nas proposições a que fizemos referência nas secções anteriores, cada afirmação dizia respeito a um objecto em particular. No entanto, é bastante frequente encontrarmos, no estudo de qualquer teoria matemática, afirmações sobre objectos genéricos que são representados por letras chamadas *variáveis*.

Representando por x um número natural genérico, podemos analisar, do ponto de vista da lógica, afirmações do tipo "x é um número primo". Tal afirmação não é, de facto, uma proposição: o seu valor lógico pode ser o de verdade ou o de falsidade. A frase "x é um número primo" torna-se uma proposição quando a variável x é substituída por um determinado número natural. Chamaremos a este tipo de afirmações *predicados* e usaremos a notação $p(x), q(x), r(x), \ldots$ para representar predicados na variável x. Se $p(x)$ representar o predicado "x é um número primo", facilmente se verifica que $p(5)$ é uma proposição verdadeira, enquanto que $p(6)$ é uma proposição falsa.

Os quantificadores permitem considerar afirmações relativas a uma classe de objectos.

As afirmações

"Todo o número natural par é soma de dois ímpares"

"Existe um número par que é primo"

são afirmações que invocam quantificadores. Ao primeiro, que se revela pelas expressões "todo", "para todo", "qualquer que seja", chamamos *quantificador universal*, e denota-se por $\forall$. Ao segundo, pela expressão "existe", "para algum", chamamos *quantificador existencial*, e denota-se por $\exists$.

Uma proposição do tipo "Para todo o x, $p(x)$" ou "Qualquer que seja x, $p(x)$", onde $p(x)$ é um predicado na variável x, pode, então, ser reescrita na forma "$\forall_x\ p(x)$" e será verdadeira quando a proposição $p(t)$ for verdadeira para todo o elemento t do domínio de variação da variável x, o chamado *universo de quantificação*. Consequentemente, a afirmação "$\forall_x\ p(x)$"

será falsa se existir um elemento t do universo de quantificação para o qual a proposição $p(t)$ é falsa.

[Exemplo] A afirmação "Todo o número natural par é soma de dois ímpares" é verdadeira (de facto, dado um qualquer natural par n, podemos escrevê-lo como $n = (n-1)+1$, sendo $n-1$ e 1 números ímpares). Já a proposição "Todo o número primo é ímpar" é falsa (basta considerar o número 2 que é primo e par).

Uma proposição do tipo "Existe x tal que $p(x)$" ou "Para algum x, $p(x)$", onde $p(x)$ é um predicado na variável x, pode ser reescrita na forma "$\exists_x\ p(x)$", sendo verdadeira quando a proposição $p(t)$ é verdadeira para algum elemento t do universo de quantificação. Por conseguinte, a proposição "$\exists_x\ p(x)$" será falsa quando $p(t)$ é falsa para todo o elemento t do universo de quantificação.

[Exemplo] A afirmação "Existe um natural n tal que $2n-2 < n$" é verdadeira (basta considerar $n = 1$), enquanto que a proposição "Existe um real x tal que $x^2 + 1 = 0$" é falsa (uma vez que $x^2 \neq -1$, para todo o real x).

[Observação] Quando o universo de uma dada quantificação é um determinado conjunto X, escrevemos, por vezes, $\exists_{x\in X}\ p(x)$ (resp. $\forall_{x\in X}\ p(x)$) em vez de $\exists_x\ p(x)$ (resp. $\forall_x\ p(x)$).

A negação de proposições que envolvam quantificadores requer atenção especial. Se $p(x)$ é um predicado na variável x, temos as seguintes equivalências lógicas:

$$\neg\forall_x\ p(x) \Leftrightarrow \exists_x\ \neg p(x)$$

$$\neg\exists_x\ p(x) \Leftrightarrow \forall_x\ \neg p(x)$$

Introdução à Teoria Elementar de Conjuntos

1 Conjuntos

Um *conjunto* é uma colecção de objectos chamados os seus *elementos* ou *membros*. Notaremos os conjuntos por letras maiúsculas $A, B, C, \ldots, X, Y, Z, \ldots$, possivelmente com índices, e os objectos por letras minúsculas $a, b, c, \ldots, x, y, z, \ldots$, também possivelmente com índices.

Escreveremos $x \in A$ (que se lê "x pertence a A") se x é um dos elementos do conjunto A e $x \notin A$ (que se lê "x não pertence a A") quando x não é um elemento de A.

[Exemplo] São conjuntos as colecções dos números naturais, inteiros, racionais ou reais, representados por $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ e $\mathbb{R}$, respectivamente. Temos, por exemplo, que $2 \in \mathbb{N}$, $0 \notin \mathbb{N}$, $-4 \in \mathbb{Z}$, $\sqrt{3} \notin Q$ e $\pi \in \mathbb{R}$.

Um conjunto pode ser descrito por *extensão* – fazendo-se uma enumeração dos seus elementos, colocados entre chavetas e separados por vírgulas – ou por *compreensão* – enunciando-se uma propriedade que caracterize os seus elementos.

[Exemplo] O conjunto dos números naturais menores do que 5 pode ser descrito por extensão da seguinte forma

$$\{1, 2, 3, 4\}.$$

O conjunto dos naturais pares pode ser definido, por compreensão, do seguinte modo

$$\{n \in \mathbb{N} : n = 2k \text{ para algum } k \in \mathbb{N}\}.$$

Representamos por $\emptyset$ ou $\{\ \}$ o *conjunto vazio*, ou seja, o conjunto sem elementos. Observe-se que podemos descrever o conjunto vazio, por compreensão, da seguinte forma:

$$\emptyset = \{x : x \neq x\},$$

uma vez que não existe nenhum elemento x que satisfaça a condição $x \neq x$.

Dizemos que dois conjuntos são *iguais* se tiverem os mesmos elementos. Escrevemos $A = B$ se os conjuntos A e B forem iguais, isto é, se para qualquer objecto x se tiver

$$x \in A \Leftrightarrow x \in B.$$

Quando existe pelos menos um elemento de um dos conjuntos A ou B que não pertença ao outro, dizemos que os conjuntos A e B são *diferentes* e escrevemos $A \neq B$.

Se todo o elemento de um conjunto A for, também, elemento de um conjunto B, dizemos que A *está contido em* B ou que A *é subconjunto de* B. Escrevemos $A \subseteq B$. Note-se que $A \subseteq B$ se para qualquer objecto x,

$$x \in A \Rightarrow x \in B,$$

isto é, se

$$\forall_{x \in A}\ x \in B.$$

Quando $\neg(A \subseteq B)$, dizemos que A *não está contido em* B ou que A *não é subconjunto de* B e escrevemos $A \not\subseteq B$. Observe-se que $A \not\subseteq B$ se

$$\exists_{x \in A}\ x \notin B.$$

Dizemos, ainda, que A *está propriamente contido em* B ou que A *é um subconjunto próprio de* B, e escrevemos $A \subset B$, se $A \subseteq B$ e $A \neq B$.

[Exemplo] Dados os conjuntos $A = \{1, 2, 4\}$, $B = \{1, 2, 3\}$ e $C = \{1, 2, 3, 4\}$, temos que $A \subset C$, $B \subset C$ e $A \not\subseteq B$.

[Exemplo] $\mathbb{N} \subset \mathbb{N}_0 \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

Com base nas definições apresentadas, facilmente se obtêm os seguintes resultados:

[Proposição] Sejam A, B e C conjuntos. Temos que

1. $\emptyset \subseteq A$.
2. $A \subseteq A$.
3. se $A \subseteq B$ e $B \subseteq C$, então $A \subseteq C$.
4. ($A \subseteq B$ e $B \subseteq A$) se e só se $A = B$.

Demonstração. (1.) Suponhamos que $\emptyset \not\subseteq A$. Sabemos, então, que existe um elemento de $\emptyset$ que não pertence a A. Mas $\emptyset$ não possui elementos! Logo, $\emptyset \subseteq A$.

(2.) É óbvio que todo o elemento de A é elemento de A. Portanto, $A \subseteq A$.

(3.) Admitamos, agora, que $A \subseteq B$ e $B \subseteq C$ e mostremos que $A \subseteq C$. Seja x um elemento arbitrário de A. Como $A \subseteq B$, sabemos que $x \in B$. Assim, dado que $B \subseteq C$, $x \in C$. Provámos, deste modo, que para qualquer objecto x, $x \in A \Rightarrow x \in C$. Portanto, $A \subseteq C$.

(4.) Vejamos, de seguida, que ($A \subseteq B$ e $B \subseteq A$) se e só se $A = B$. Admitamos, primeiro, que $A \subseteq B$ e $B \subseteq A$ e mostremos que $A = B$. Como $A \subseteq B$, todo o elemento de A é elemento de B, e como $B \subseteq A$, todo o elemento de B é elemento de A. Portanto, A e B têm os mesmos elementos, ou seja, $A = B$. Reciprocamente, admitamos que $A = B$ e provemos que $A \subseteq B$ e $B \subseteq A$. Consideremos um elemento arbitrário x de A. Como $A = B$, estes conjuntos têm os mesmos elementos. Portanto, $x \in B$. Assim, todo o elemento de A é elemento de B, pelo que $A \subseteq B$. De modo análogo se verifica que $B \subseteq A$. □

2 União, intersecção e complementação de conjuntos

[Definição] Sejam A e B subconjuntos de um conjunto X, chamado o *universo*.

- A *união* ou *reunião* de A com B, notada por $A \cup B$, é o conjunto cujos elementos são os elementos de A e os elementos de B, ou seja,

$$A \cup B = \{x \in X \ : \ x \in A \vee x \in B\}.$$

- A *intersecção* de A com B, notada por $A \cap B$, é o conjunto cujos elementos pertencem simultaneamente a A e a B, isto é,

$$A \cap B = \{x \in X \ : \ x \in A \wedge x \in B\}.$$

- O *complementar de* B A, notado por $A \setminus B$, e também designado por *diferença de* A *com* B, notada por $A - B$, é o conjunto cujos elementos pertencem a A mas não a B, ou seja,

$$A \setminus B = \{x \in X \ : \ x \in A \wedge x \notin B\}.$$

  Quando A é o universo X, ao conjunto $A \setminus B = X \setminus B$ dá-se o nome de *complementar de* B, representado por B^c ou $\overline{B}$.

[Exemplo] Consideremos os subconjuntos $A = \{-1, 0, 1, \pi, 10\}$ e $B =]-1, 3]$ de $\mathbb{R}$. Temos que $A \cup B = [-1, 3] \cup \{\pi, 10\}$, $A \cap B = \{0, 1\}$, $A \setminus B = \{-1, \pi, 10\}$ e $\overline{B} =]-\infty, -1] \cup]3, +\infty]$.

Vejamos, de seguida, algumas propriedades destas operações com conjuntos. Comecemos pela operação de união de conjuntos.

[Proposição] Sejam A, B e C subconjuntos de um conjunto X. Então,

1. $A \subseteq A \cup B$ e $B \subseteq A \cup B$.
2. $A \cup \emptyset = A$.
3. $A \cup A = A$.
4. $A \cup X = X$.
5. $A \cup B = B \cup A$.
6. $(A \cup B) \cup C = A \cup (B \cup C)$.
7. se $A \subseteq B$, $A \cup B = B$.

Demonstração. Demonstraremos as propriedades (1.), (2.) e (7.), ficando as restantes como exercício.

(1.) Seja $x \in A$. Então, é óbvio que a proposição $x \in A \vee x \in B$ é verdadeira. Assim, é verdade que $x \in A \cup B$. Portanto, para todo o objecto x, $x \in A \Rightarrow x \in A \cup B$, donde $A \subseteq A \cup B$. De modo semelhante se verifica que $B \subseteq A \cup B$.

(2.) Sabemos que $A \subseteq A \cup \emptyset$, pela propriedade (1.). Para mostrar que $A \cup \emptyset = A$, resta provar que $A \cup \emptyset \subseteq A$. Consideremos, para tal, $x \in A \cup \emptyset$. Por definição, temos, então, que $x \in A \vee x \in \emptyset$. Dado que $\emptyset$ não possui elementos, podemos afirmar que $x \in A$. Portanto, para todo o objecto x, $x \in A \cup \emptyset \Rightarrow x \in A$, pelo que $A \cup \emptyset \subseteq A$.

(7.) Admitamos que $A \subseteq B$ e mostremos que $A \cup B = B$. Pela propriedade (1.), temos que $B \subseteq A \cup B$. Logo, resta mostrar que $A \cup B \subseteq B$. Seja $x \in A \cup B$. Dado que todo o elemento de A é também elemento de B, segue-se que

$$x \in A \cup B \Rightarrow x \in A \vee x \in B \Rightarrow x \in B \vee x \in B \Rightarrow x \in B.$$

Assim, para todo o objecto x, $x \in A \cup B \Rightarrow x \in B$, ou seja, $A \cup B \subseteq B$. □

No seguinte resultado, descrevemos algumas propriedades da operação de intersecção de conjuntos.

[Proposição] Sejam A, B e C subconjuntos de um conjunto X. Então,

1. $A \cap B \subseteq A$ e $A \cap B \subseteq B$.
2. $A \cap \emptyset = \emptyset$.
3. $A \cap A = A$.
4. $A \cap X = A$.
5. $A \cap B = B \cap A$.

6. $(A \cap B) \cap C = A \cap (B \cap C)$.
7. se $A \subseteq B$, $A \cap B = A$.

Demonstração. Demonstraremos, apenas, as propriedades (1.), (3.) e (7.). As restantes ficam como exercício.

(1.) Seja $x \in A \cap B$. Então, $x \in A \wedge x \in B$. Em particular, $x \in A$. Logo, para todo o objecto x, $x \in A \cap B \Rightarrow x \in A$, pelo que $A \cap B \subseteq A$. Analogamente se verifica que $A \cap B \subseteq B$.

(3.) Atendendo à propriedade (1.), sabemos que $A \cap A \subseteq A$. Para provar que $A \cap A = A$, resta, pois, mostrar que $A \subseteq A \cap A$. Temos que, para todo o objecto x,

$$x \in A \Rightarrow x \in A \wedge x \in A \Rightarrow x \in A \cap A,$$

donde $A \subseteq A \cap A$.

(7.) Suponhamos que $A \subseteq B$ e vejamos que $A \cap B = A$. Pela propriedade (1.), temos que $A \cap B \subseteq A$. Resta, então, mostrar que $A \subseteq A \cap B$. Seja $x \in A$. Atendendo a que todo o elemento de A é também elemento de B, temos que

$$x \in A \Rightarrow x \in A \wedge x \in A \Rightarrow x \in A \wedge x \in B \Rightarrow x \in A \cap B.$$

Provámos, deste modo, que, para todo o objecto x, $x \in A \Rightarrow x \in A \cap B$, isto é, $A \subseteq A \cap B$.□

[Observação] Sejam $A_1, A_2, \ldots, A_n$ subconjuntos de um conjunto X. Tendo em conta que as operações de união e de intersecção de conjuntos gozam da propriedade associativa, podemos escrever sem ambiguidade

$$A_1 \cup A_2 \cup \ldots \cup A_n$$

e

$$A_1 \cap A_2 \cap \ldots \cap A_n.$$

A união dos conjuntos $A_1, A_2, \ldots, A_n$ é usualmente notada por

$$\bigcup_{i=1}^{n} A_i$$

e a intersecção por

$$\bigcap_{i=1}^{n} A_i.$$

Assim,

$$\bigcup_{i=1}^{n} A_i = \{x \in X : x \in A_1 \vee x \in A_2 \vee \ldots \vee x \in A_n\}$$

e

$$\bigcap_{i=1}^{n} A_i = \{x \in X : x \in A_1 \wedge x \in A_2 \wedge \ldots \wedge x \in A_n\}.$$

[Proposição] Sejam A, B e C conjuntos. Então,

1. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
2. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Demonstração. Exercício. □

O seguinte resultado descreve propriedades da complementação de conjuntos.

[Proposição] Sejam A, B e C subconjuntos de um conjunto X. Então,

1. $A \cap \overline{A} = \emptyset$ e $A \cup \overline{A} = X$.
2. $A \setminus \emptyset = A$ e $A \setminus X = \emptyset$.
3. se $A \subseteq B$, $A \setminus B = \emptyset$.
4. $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$.
5. $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$.
6. $\overline{(A \cup B)} = \overline{A} \cap \overline{B}$.
7. $\overline{(A \cap B)} = \overline{A} \cup \overline{B}$.
8. $\overline{(\overline{A})} = A$.

Demonstração. Demonstraremos, apenas, as propriedades (1.), (2.) e (6.). As restantes ficam como exercício.

(1.) Vejamos que $A \cap \overline{A}$ não possui elementos. Para tal, suponhamos que existe $x \in A \cap \overline{A}$. Então, $x \in A \wedge x \in \overline{A}$. Mas, se $x \in \overline{A}$, $x \notin A$. Assim, $x \in A \wedge x \notin A$, uma contradição. Esta contradição resultou de supormos que existia pelo menos um elemento em $A \cap \overline{A}$. Portanto, $A \cap \overline{A}$ não possui elementos, ou seja, $A \cap \overline{A} = \emptyset$. Mostremos, agora, que $A \cup \overline{A} = X$. Como A e $\overline{A}$ são subconjuntos de X, o conjunto $A \cup \overline{A}$, cujos elementos são os elementos de A e os de $\overline{A}$, está, obviamente, contido em X. Assim, para provar que $A \cup \overline{A} = X$, resta mostrar que $X \subseteq A \cup \overline{A}$. Consideremos, então, $x \in X$. Obviamente, $x \in A \vee x \notin A$ é uma proposição verdadeira (o elemento x pertence a A ou não pertence a A). Ora, se $x \notin A$, sabemos que $x \in \overline{A}$. Portanto,

$$x \in X \Rightarrow x \in A \vee x \notin A \Rightarrow x \in A \vee x \in \overline{A} \Rightarrow x \in A \cup \overline{A}.$$

Podemos, então, concluir que $X \subseteq A \cup \overline{A}$.

(2.) Por definição, $A \setminus \emptyset$ é o conjunto cujos elementos pertencem a A e não pertencem a $\emptyset$. Como $\emptyset$ não possui elementos, não estamos a excluir qualquer elemento de A. Portanto, $A \setminus \emptyset$ é o conjunto cujos elementos pertencem a A, ou seja, $A \setminus \emptyset = A$. Relativamente ao conjunto $A \setminus X$, suponhamos que tem pelo menos um elemento x. Então, $x \in A \wedge x \notin X$. Mas, se $x \in A$, dado que A é um subconjunto de X, $x \in X$. Temos, então, que $x \in X \wedge x \notin X$, uma contradição. A contradição resultou de supormos que $A \setminus X$ tinha pelo menos um elemento. Logo, $A \setminus X$ não possui elementos, ou seja $A \setminus X = \emptyset$.

(6.) Sabemos que $\overline{(A \cup B)} = \overline{A} \cap \overline{B}$ se e só se, para todo o objecto x,

$$x \in \overline{(A \cup B)} \Leftrightarrow x \in \overline{A} \cap \overline{B}.$$

Ora, para todo o objecto x,

$$\begin{aligned} x \in \overline{(A \cup B)} &\Leftrightarrow x \notin A \cup B \Leftrightarrow \neg(x \in A \cup B) \\ &\Leftrightarrow \neg(x \in A \vee x \in B) \Leftrightarrow \neg(x \in A) \wedge \neg(x \in B) \\ &\Leftrightarrow (x \notin A) \wedge (x \notin B) \Leftrightarrow x \in \overline{A} \wedge x \in \overline{B} \\ &\Leftrightarrow x \in \overline{A} \cap \overline{B}. \end{aligned}$$

Logo, $\overline{(A \cup B)} = \overline{A} \cap \overline{B}$. □

3 Conjunto potência

Podemos construir conjuntos cujos elementos são eles próprios conjuntos. Por exemplo, os conjuntos $\{0,1\}$, $\emptyset$ e $\{a\}$ podem constituir um novo conjunto: $A = \big\{\{0,1\}, \emptyset, \{a\}\big\}$. Neste caso, temos que os elementos do conjunto A são $\{0,1\}$, $\emptyset$ e $\{a\}$, e escrevemos

$$\{0,1\} \in A,\ \emptyset \in A,\ \{a\} \in A.$$

Pensando em inclusão de conjuntos e, mais concretamente, nos subconjuntos de um dado conjunto, sabemos que o conjunto vazio é (sempre) subconjunto de qualquer conjunto. Em particular, é subconjunto do conjunto A considerado. Assim, é verdade que

$$\emptyset \subseteq A.$$

No entanto, já não é verdadeira a relação $\{0,1\} \subseteq A$, uma vez que os elementos do conjunto $\{0,1\}$ (que são o 0 e o 1) não são elementos de A. De facto, os subconjuntos do conjunto A são os seguintes:

$$\emptyset,\ \big\{\emptyset\big\},\ \big\{\{0,1\}\big\},\ \big\{\{a\}\big\},\ \big\{\emptyset,\{0,1\}\big\},\ \big\{\emptyset,\{a\}\big\},\ \big\{\{0,1\},\{a\}\big\},\ \big\{\emptyset,\{0,1\},\{a\}\big\}.$$

Dado um conjunto arbitrário A, definimos o conjunto potência de A da seguinte forma:

[Definição] Seja A um conjunto. Chamamos *conjunto potência de A* ou *conjunto das partes de A* ao conjunto dos subconjuntos de A, que notaremos por $\mathcal{P}(A)$. Isto é,

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

[Exemplo] Sejam $A = \{1,2\}$, $B = \big\{1, \{1\}\big\}$ e $C = \emptyset$. Temos que

$$\mathcal{P}(A) = \big\{\emptyset, \{1\}, \{2\}, \{1,2\}\big\},$$

$$\mathcal{P}(B) = \big\{\emptyset, \{1\}, \big\{\{1\}\big\}, \big\{1, \{1\}\big\}\big\}$$

e

$$\mathcal{P}(C) = \{\emptyset\}.$$

O seguinte resultado descreve algumas propriedades do conjunto potência.

[Proposição] Sejam A e B conjuntos. Então,

1. $\emptyset \in \mathcal{P}(A)$ e $A \in \mathcal{P}(A)$.
2. se $A \subseteq B$, $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.
3. se A tem n elementos, $\mathcal{P}(A)$ tem 2^n elementos.

Demonstração. Demonstraremos, apenas, a propriedade (1.). A demonstração da propriedade (2.) fica como exercício. Omitimos a prova da propriedade (3.), que poderá ser encontrada em bibliografia adequada.
(1.) Vimos já que $\emptyset \subseteq A$ e que $A \subseteq A$, ou seja, que $\emptyset$ e A são subconjuntos de A. Sendo $\mathcal{P}(A)$ o conjunto dos subconjuntos de A, segue-se que $\emptyset$ e A são, de facto, elementos de $\mathcal{P}(A)$. □

4 Produto cartesiano

[Definição] Sejam A e B conjuntos. Chamamos *produto cartesiano de A por B* ao conjunto dos pares ordenados (a, b) em que a primeira coordenada, a, é um elemento de A, e a segunda coordenada, b, é um elemento de B. Notaremos este conjunto por $A \times B$. Temos que

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

[Observação] Dois pares ordenados (a_1, b_1) e (a_2, b_2) são iguais se e somente se $a_1 = a_2$ e $b_1 = b_2$.

[Exemplo] Sejam $A = \{4, 5\}$, $B = \{1, 2, 3\}$ e $C = \emptyset$. Temos que

$$A \times B = \big\{(4,1), (4,2), (4,3), (5,1), (5,2), (5,3)\big\},$$

$$B \times A = \big\{(1,4), (1,5), (2,4), (2,5), (3,4), (3,5)\big\},$$

e

$$A \times C = C \times A = B \times C = C \times B = \emptyset.$$

A noção de produto cartesiano de dois conjuntos generaliza-se de forma natural:

[Definição] Sejam $A_1, A_2, \ldots, A_n$ conjuntos ($n \geq 2$). O *produto cartesiano de $A_1, A_2, \ldots, A_n$*, notado por $A_1 \times A_2 \times \ldots \times A_n$, é o conjunto dos n–úplos ordenados $(a_1, a_2, \ldots, a_n)$ em que $a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n$, ou seja,

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

Se $A_1 = A_2 = \ldots = A_n = A$, escrevemos A^n em alternativa a $A \times A \times \ldots \times A$.

[Observação] Dois n–úplos ordenados $(a_1, a_2, \ldots, a_n)$ e $(b_1, b_2, \ldots, b_n)$ são iguais se e somente se $a_1 = b_1$ e $a_2 = b_2$ e $\ldots$ e $a_n = b_n$.

[Exemplo] Sejam $A = \{4, 5\}$, $B = \{1, 2, 3\}$ e $C = \{7\}$. Temos que

$$A \times B \times C = \big\{(4,1,7), (4,2,7), (4,3,7), (5,1,7), (5,2,7), (5,3,7)\big\}$$

e

$$A^2 = \big\{(4,4), (4,5), (5,4), (5,5)\big\}.$$

[Observação] Se os conjuntos $A_1, A_2, \ldots, A_n$ têm $p_1, p_2, \ldots, p_n$ elementos, respectivamente, o produto cartesiano $A_1 \times A_2 \times \ldots \times A_n$ tem $p_1 \times p_2 \times \ldots \times p_n$ elementos.

Indução nos Naturais

Consideremos a proposição "$\forall_{n \in \mathbb{N}}\ n^2 > 2n + 1$". Facilmente se verifica que esta proposição é falsa: com efeito, notando o predicado $n^2 > 2n + 1$ na variável n por $p(n)$, temos que $p(1)$ e $p(2)$ são proposições falsas, já que $1^2 \not> 2 \times 1 + 1$ e $2^2 \not> 2 \times 4 + 1$. No entanto, se continuarmos a verificar a desigualdade $n^2 > 2n + 1$ para outros valores de n, podemos ver que $p(3), p(4), p(5)$ e $p(6)$ são proposições verdadeiras. E começamos a desconfiar que $p(n)$ é uma proposição verdadeira se $n \geq 3$.

Consideremos, agora, o predicado $q(n)$: "$5^n - 1$ é múltiplo de 4". Temos que $5^1 - 1 = 4$, $5^2 - 1 = 24 = 6 \times 4$, $5^3 - 1 = 124 = 31 \times 4$ e $5^4 - 1 = 624 = 156 \times 4$. Assim, as proposições $q(1), q(2), q(3)$ e $q(4)$ são verdadeiras, o que nos leva a desconfiar que a proposição "$\forall_{n \in \mathbb{N}}\ 5^n - 1$ é múltiplo de 4" é, também, verdadeira.

Mas como poderemos provar estes resultados? Estes e muitos outros resultados, que envolvem propriedades respeitantes aos números naturais, podem ser demonstrados usando o *Princípio de Indução*. Esta forma de demonstração é bastante poderosa e usada intensivamente em vários ramos da matemática.

[Teorema (Princípio de Indução (Simples) para $\mathbb{N}$)] Seja $p(n)$ um predicado sobre o conjunto dos números naturais. Se

1. $p(1)$ é uma proposição verdadeira,
2. para $k \in \mathbb{N}$, $p(k+1)$ é uma proposição verdadeira sempre que $p(k)$ é verdadeira,

então $p(n)$ é verdadeira, para todo $n \in \mathbb{N}$.

A condição (1.) é chamada de *base de indução* e a condição (2.) de *passo de indução*. Na aplicação do Princípio de Indução, chamamos *hipótese de indução* a "$p(k)$ é verdadeira".

[Exemplo] Consideremos, de novo, o predicado $q(n)$: "$5^n - 1$ é múltiplo de 4" e mostremos que "$\forall_{n\in\mathbb{N}}\ q(n)$" é uma proposição verdadeira.

(1.) Atendendo a que $5^1 - 1 = 4$, temos que $5^1 - 1$ é, efectivamente, um múltiplo de 4, pelo que $q(1)$ é verdadeira.

(2.) Seja $k \in \mathbb{N}$ e suponhamos que $q(k)$ é verdadeira. Assim, $5^k - 1$ é múltiplo de 4, donde existe $m \in \mathbb{N}$ tal que $5^k - 1 = 4m$ ou, equivalentemente, tal que $5^k = 4m + 1$. Mostremos, então, que também $q(k + 1)$ é verdadeira. Temos:

$$\begin{aligned} 5^{k+1} - 1 &= 5^k \times 5 - 1 = (4m + 1) \times 5 - 1 \\ &= 4m \times 5 + 5 - 1 = 4m \times 5 + 4 \\ &= 4(5m + 1). \end{aligned}$$

Portanto, $5^{k+1} - 1$ é múltiplo de 4 e $q(k+1)$ é verdadeira. Provámos, deste modo, que $q(k+1)$ é verdadeira sempre que $q(k)$ é verdadeira.

De (1.) e (2.), aplicando o Princípio de Indução para $\mathbb{N}$, podemos concluir que "$\forall_{n\in\mathbb{N}}\ 5^n - 1$ é múltiplo de 4" é uma proposição verdadeira.

É imprescindível que se verifiquem as condições (1.) e (2.) de forma a que se possa invocar o Princípio de Indução para $\mathbb{N}$. De facto, no exemplo do predicado $p(n)$ apresentado anteriormente, (2.) é válida sem no entanto se ter a validade de (1.), sendo portanto a proposição $\forall_{n\in\mathbb{N}}\ p(n)$ falsa. Para estes casos, recorremos ao chamado *Princípio de Indução para* $\mathbb{N}$ *de base* n_0.

[Teorema (Princípio de Indução para $\mathbb{N}$ de base n_0)] Sejam $p(n)$ um predicado sobre o conjunto dos números naturais e $n_0 \in \mathbb{N}$. Se

1. $p(n_0)$ é uma proposição verdadeira,
2. para $k \geq n_0$, $p(k + 1)$ é uma proposição verdadeira sempre que $p(k)$ é verdadeira,

então $p(n)$ é verdadeira, para todo $n \in \mathbb{N}$ tal que $n \geq n_0$.

[Exemplo] Consideremos, uma vez mais, o predicado $p(n)$: "$n^2 > 2n + 1$" e mostremos que "$\forall_{n\in\mathbb{N},n\geq 3}\ p(n)$" é uma proposição verdadeira.

(1.) Atendendo a que $3^2 > 2 \times 3 + 1$, temos que $p(3)$ é verdadeira.

(2.) Seja $k \in \mathbb{N}$ tal que $k \geq 3$ e suponhamos, por hipótese de indução, que $p(k)$ é verdadeira. Então, $k^2 > 2k + 1$. Vejamos que também $p(k + 1)$ é verdadeira, ou seja, que

$$(k + 1)^2 > 2(k + 1) + 1 = 2k + 3.$$

Temos:

$$\begin{aligned} (k + 1)^2 &= k^2 + 2k + 1 \\ &> (2k + 1) + 2k + 1 \\ &= 2k + 2k + 2. \end{aligned}$$

Como $2k+2>3$, segue-se que $(k+1)^2>2k+3$ e, por conseguinte, $p(k+1)$ é verdadeira.

De (1.) e (2.), aplicando o Princípio de Indução para $\mathbb{N}$ de base 3, podemos concluir que "$\forall_{n\in\mathbb{N},n\geq 3}\ n^2>2n+1$" é uma proposição verdadeira.

Funções

[Definição] Sejam A e B conjuntos. Uma *função* ou *aplicação de A em B* é uma correspondência de A para B que a cada elemento a de A faz corresponder um único elemento b de B.

Para indicar que f é uma função de A em B, escrevemos

$$f : A \longrightarrow B$$

e, para cada $x\in A$, notamos por $f(x)$ o único elemento y de B que f faz corresponder a x. Este elemento é designado por *imagem por f de x*. Dada uma função $f : A \longrightarrow B$, chamamos

- *domínio* ou *conjunto de partida* de f a A;
- *codomínio* ou *conjunto de chegada* de f a B;
- *imagem* ou *contradomínio* de f ao conjunto das imagens por f de todos os elementos de A:
$$Im\ f=\{f(x)\ :\ x\in A\}.$$

[Exemplo] A expressão $y=x^2$ determina uma função f de $\mathbb{R}$ em $\mathbb{R}$ que a cada $x\in\mathbb{R}$ faz corresponder o elemento x^2 de $\mathbb{R}$. Podemos apresentar esta função f da seguinte forma:

$$\begin{array}{rccc} f & : & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & & x & \longmapsto & x^2 \end{array}$$

[Definição] Sejam A, B, C e D conjuntos e $f : A \longrightarrow B$ e $g : C \longrightarrow D$ funções. Dizemos que f e g são iguais se $A=C$, $B=D$ e, para todo o $x\in A$, $f(x)=g(x)$.

[Definição] Dado um conjunto A, chamamos *função identidade* de A à função $id_A : A \longrightarrow A$ definida por $id_A(x)=x$, qualquer que seja $x\in A$.

[Definição] Uma função f de um conjunto A num conjunto B diz-se *constante* se existe $b\in B$ tal que, para todo o $x\in A$, $f(x)=b$.

[Exemplo] A função $f:\{1,2\}\longrightarrow\{3,4,5\}$ definida por $f(1)=f(2)=5$ é constante.

[Definição] Sejam $f : A \longrightarrow B$ uma função, $X\subseteq A$ e $Y\subseteq B$. Designamos por

- *imagem de X por f* o conjunto $f(X)=\{f(x)\ :\ x\in X\}$;

- *imagem inversa* ou *pré-imagem de Y por f* o conjunto $f^{\leftarrow}(Y) = \{x \in A \ : \ f(x) \in Y\}$.

Observe-se que a imagem de A por f é o conjunto $Im\ f$ anteriormente definido.

[Exemplo] Consideremos a função $f : \mathbb{R} \longrightarrow \mathbb{R}$ definida por $f(x) = x^2$, para todo o $x \in \mathbb{R}$. Temos

- $f\big(\{-2, 0, 1\}\big) = \{0, 1, 4\}$
- $f\big(\{-1, 1\}\big) = \{1\}$
- $Im\ f = f(\mathbb{R}) = \mathbb{R}_0^+$
- $f^{\leftarrow}\big(\{0, 2, 4\}\big) = \{-2, -\sqrt{2}, 0, \sqrt{2}, 2\}$
- $f^{\leftarrow}\big(\{-1\}\big) = \emptyset$
- $f^{\leftarrow}(\mathbb{R}) = \mathbb{R}$

[Proposição] Sejam $f : A \longrightarrow B$ uma função, $X_1, X_2 \subseteq A$ e $Y_1, Y_2 \subseteq B$. Então

1. $f\big(\emptyset\big) = \emptyset$.
2. $f^{\leftarrow}\big(\emptyset\big) = \emptyset$.
3. $f^{\leftarrow}(B) = A$.
4. $f(A) \subseteq B$.
5. $f(X_1 \cup X_2) = f(X_1) \cup f(X_2)$.
6. $f^{\leftarrow}(Y_1 \cup Y_2) = f^{\leftarrow}(Y_1) \cup f^{\leftarrow}(Y_2)$.
7. $f^{\leftarrow}(Y_1 \cap Y_2) = f^{\leftarrow}(Y_1) \cap f^{\leftarrow}(Y_2)$.

Demonstração. Demonstraremos, apenas, as propriedades (5.), (6.) e (7.). A demonstração das restantes propriedades fica como exercício.

(5.) Mostremos, primeiro, que $f(X_1 \cup X_2) \subseteq f(X_1) \cup f(X_2)$. Seja $y \in f(X_1 \cup X_2)$. Então, existe $x \in X_1 \cup X_2$ tal que $y = f(x)$. Ora, $x \in X_1 \cup X_2 \Leftrightarrow x \in X_1 \vee x \in X_2$. Caso $x \in X_1$, temos que $y \in f(X_1)$. Caso $x \in X_2$, temos que $y \in f(X_2)$. Portanto, $y \in f(X_1) \vee y \in f(X_2)$, ou seja, $y \in f(X_1) \cup f(X_2)$. Assim, $f(X_1 \cup X_2) \subseteq f(X_1) \cup f(X_2)$. Vejamos, agora, que $f(X_1) \cup f(X_2) \subseteq f(X_1 \cup X_2)$. Para tal, consideremos $y \in f(X_1) \cup f(X_2)$. Por definição, temos que $y \in f(X_1) \vee y \in f(X_2)$. Se $y \in f(X_1)$ então existe $x \in X_1$ tal que $y = f(x)$. Se $y \in f(X_2)$ então existe $x \in X_2$ tal que $y = f(x)$. Assim, $y = f(x)$ com $x \in X_1$ ou $x \in X_2$. Como $x \in X_1 \vee x \in X_2 \Leftrightarrow x \in X_1 \cup X_2$, segue-se que $y = f(x)$ com $x \in X_1 \cup X_2$, ou seja, que $y \in f(X_1 \cup X_2)$. Portanto, $f(X_1) \cup f(X_2) \subseteq f(X_1 \cup X_2)$.

(6.) Para todo o objecto x, temos que

$$\begin{aligned} x \in f^{\leftarrow}(Y_1 \cup Y_2) &\Leftrightarrow f(x) \in Y_1 \cup Y_2 \\ &\Leftrightarrow f(x) \in Y_1 \vee f(x) \in Y_2 \\ &\Leftrightarrow x \in f^{\leftarrow}(Y_1) \vee x \in f^{\leftarrow}(Y_2) \\ &\Leftrightarrow x \in f^{\leftarrow}(Y_1) \cup f^{\leftarrow}(Y_2). \end{aligned}$$

Logo, $f^{\leftarrow}(Y_1 \cup Y_2) = f^{\leftarrow}(Y_1) \cup f^{\leftarrow}(Y_2)$.

(7.) Para todo o objecto x, temos que

$$\begin{aligned} x \in f^{\leftarrow}(Y_1 \cap Y_2) &\Leftrightarrow f(x) \in Y_1 \cap Y_2 \\ &\Leftrightarrow f(x) \in Y_1 \wedge f(x) \in Y_2 \\ &\Leftrightarrow x \in f^{\leftarrow}(Y_1) \wedge x \in f^{\leftarrow}(Y_2) \\ &\Leftrightarrow x \in f^{\leftarrow}(Y_1) \cap f^{\leftarrow}(Y_2). \end{aligned}$$

Logo, $f^{\leftarrow}(Y_1 \cap Y_2) = f^{\leftarrow}(Y_1) \cap f^{\leftarrow}(Y_2)$. □

[Observação] Nas condições do resultado anterior, nem sempre é verdade que $f(X_1 \cap X_2) = f(X_1) \cap f(X_2)$. Consideremos, por exemplo, a função $f : \mathbb{R} \longrightarrow \mathbb{R}$ definida por $f(x) = x^2$, para todo o $x \in \mathbb{R}$. Dados $X_1 = \{-1, 2\}$ e $X_2 = \{1, 2\}$, temos que

$$f(X_1 \cap X_2) = f\big(\{2\}\big) = \{4\}$$

e

$$f(X_1) \cap f(X_2) = f\big(\{1, 2\}\big) \cap f\big(\{-1, 2\}\big) = \{1, 4\}.$$

Portanto, neste caso, $f(X_1 \cap X_2) \neq f(X_1) \cap f(X_2)$.

1 Composição de funções

Consideremos duas funções $f : A \longrightarrow B$ e $g : B \longrightarrow C$. Seja a um elemento arbitrário de A. Atendendo à definição de função, sabemos que existe um e um só $b \in B$ tal que $b = f(a)$. Dado que $b \in B$ e que g é uma função de B para C, existe um único $c \in C$ tal que $c = g(b)$. Temos que

$$c = g(b) = g\left(f(a)\right).$$

Vimos, assim, que, para cada $a \in A$, existe um e um só $c \in C$ tal que $c = g\left(f(a)\right)$. Podemos, então, afirmar que a relação de A para C que a cada $a \in A$ faz corresponder o elemento $g\left(f(a)\right)$ de C é uma função.

[Definição] Dadas duas funções $f : A \longrightarrow B$ e $g : B \longrightarrow C$, designamos por *função composta de g com f*, e notamos por $g \circ f$, a função de A em C que a cada elemento x de A associa o elemento $g(f(x))$ de C, ou seja, $g \circ f$ é a função

$$\begin{array}{rccc} g \circ f : & A & \longrightarrow & C \\ & x & \longmapsto & g(f(x)). \end{array}$$

[Exemplo] Consideremos as funções

$$\begin{array}{rccc} f : & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & x + 2 \end{array} \quad \text{e} \quad \begin{array}{rccc} g : & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & 3x + 1. \end{array}$$

Temos que

$$\begin{array}{rccl} g \circ f: & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & g(f(x)) = g(x+2) = 3(x+2)+1 = 3x+7 \end{array}$$

e

$$\begin{array}{rccl} f \circ g: & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & f(g(x)) = f(3x+1) = (3x+1)+2 = 3x+3. \end{array}$$

[Observação] A composição de funções não é, em geral, comutativa, como ilustra o exemplo anterior (de facto, no exemplo anterior, $f \circ g \neq g \circ f$).

A composição de funções goza de algumas propriedades das quais destacamos as que se seguem.

[Proposição] Dadas funções $f : A \longrightarrow B$, $g : B \longrightarrow C$ e $h : C \longrightarrow D$, as funções $(h \circ g) \circ f$ e $h \circ (g \circ f)$ são iguais.

Demonstração. O conjunto de partida de $(h \circ g) \circ f$ é o conjunto A, tal como o de $h \circ (g \circ f)$, e o conjunto de chegada de $(h \circ g) \circ f$ é o conjunto D, assim como o de $h \circ (g \circ f)$. Além disso, para todo o $x \in A$,

$$\begin{aligned} \Big(\big(h \circ g\big) \circ f\Big)(x) &= \big(h \circ g\big)\big(f(x)\big) \\ &= h\Big(g\big(f(x)\big)\Big) \\ &= h\Big(\big(g \circ f\big)(x)\Big) \\ &= \Big(h \circ \big(g \circ f\big)\Big)(x). \end{aligned}$$

Logo, as aplicações $(h \circ g) \circ f$ e $h \circ (g \circ f)$ são iguais. □

[Observação] Nas condições do resultado anterior, escrevemos $h \circ g \circ f$ para indicar $(h \circ g) \circ f$ e $h \circ (g \circ f)$.

[Proposição] Dada uma função $f : A \longrightarrow B$, temos que $f \circ id_A = f$ e $id_B \circ f = f$.

Demonstração. Exercício. □

2 Funções injectivas, sobrejectivas e bijectivas

[Definição] Seja $f : A \longrightarrow B$ uma função. Dizemos que

- f é *injectiva* se

$$\forall_{x_1, x_2 \in A} \quad (f(x_1) = f(x_2) \Rightarrow x_1 = x_2)$$

ou, equivalentemente, se

$$\forall_{x_1, x_2 \in A} \quad (x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2))\,;$$

- f é *sobrejectiva* se

$$\forall_{y\in B}\ \exists_{x\in A}\quad f(x)=y$$

  ou, equivalentemente, se $f(A)=B$;

- f é *bijectiva* se é simultaneamente injectiva e sobrejectiva.

[Exemplo] A função $f:\mathbb{N}\longrightarrow\mathbb{N}$ definida por $f(n)=n+1$, para todo o natural n, é injectiva mas não sobrejectiva. De facto, dados dois naturais n e m,

$$\begin{aligned} f(n)=f(m) &\Rightarrow n+1=m+1\\ &\Rightarrow n=m, \end{aligned}$$

pelo que f é injectiva. Além disso, $1\in\mathbb{N}$ e não existe $n\in\mathbb{N}$ tal que $f(n)=1$, uma vez que $n+1=1\Leftrightarrow n=0\notin\mathbb{N}$, donde f não é sobrejectiva.

[Exemplo] A função $f:\mathbb{R}\longrightarrow\mathbb{R}_0^+$ definida por $f(x)=x^2$, para todo o real x, é sobrejectiva mas não injectiva. Com efeito, dado um qualquer real não negativo y, existe $x\in\mathbb{R}$ tal que $f(x)=y$: basta considerar $x=\sqrt{y}$. Portanto, f é sobrejectiva. Dado que $f(-1)=f(1)=1$, podemos afirmar que f não é injectiva.

[Exemplo] A função $f:\mathbb{R}\longrightarrow\mathbb{R}$ definida por $f(x)=2x$, para todo o real x, é bijectiva. Dados dois reais x_1 e x_2,

$$\begin{aligned} f(x_1)=f(x_2) &\Rightarrow 2x_1=2x_2\\ &\Rightarrow x_1=x_2, \end{aligned}$$

pelo que f é injectiva. Dado $y\in\mathbb{R}$, existe $x\in\mathbb{R}$ tal que $f(x)=y$: basta considerar $x=\frac{y}{2}$. Portanto, f é sobrejectiva. Sendo injectiva e sobrejectiva, f é bijectiva.

[Proposição] Sejam $f:A\longrightarrow B$ e $g:B\longrightarrow C$ funções. Temos que

1. se f e g são injectivas então $g\circ f$ é injectiva.
2. se f e g são sobrejectivas então $g\circ f$ é sobrejectiva.
3. se f e g são bijectivas então $g\circ f$ é bijectiva.

Demonstração. (1.) Admitamos que f e g são injectivas. Sejam x_1 e x_2 elementos de A tais que $\big(g\circ f\big)(x_1)=\big(g\circ f\big)(x_2)$. Então, $g\big(f(x_1)\big)=g\big(f(x_2)\big)$. Como g é injectiva, podemos afirmar que $f(x_1)=f(x_2)$. Sendo f injectiva, segue-se que $x_1=x_2$. Portanto, para quaisquer $x_1,x_2\in A$,

$$\big(g\circ f\big)(x_1)=\big(g\circ f\big)(x_2)\Rightarrow x_1=x_2,$$

pelo que $g\circ f$ é injectiva.

(2.) Suponhamos que f e g são sobrejectivas. Seja $y\in C$. Pretendemos mostrar que existe $x\in A$ tal que $y=\big(g\circ f\big)(x)$. Como $y\in C$ e g é sobrejectiva, sabemos que existe $z\in B$ tal

que $y = g(z)$. Dado que $z \in B$ e f é sobrejectiva, podemos afirmar que existe $x \in A$ tal que $z = f(x)$. Assim, $y = g(z) = g\big(f(x)\big) = \big(g \circ f\big)(x)$. Provámos, deste modo, que

$$\forall_{y \in C} \ \exists_{x \in A} \ \ y = \big(g \circ f\big)(x),$$

ou seja, que $g \circ f$ é sobrejectiva.

(3.) Consequência imediata de (1.) e (2.). □

A demonstração do seguinte resultado pode ser encontrada em bibliografia adequada.

[Teorema] Seja $f : A \longrightarrow B$ uma função. Então, f é bijectiva se e só se existe uma e uma só função $g : B \longrightarrow A$ tal que $g \circ f = id_A$ e $f \circ g = id_B$.

3 Funções invertíveis

[Definição] Seja $f : A \longrightarrow B$ uma função bijectiva. Chamamos *função inversa de* f à única função $g : B \longrightarrow A$ tal que $g \circ f = id_A$ e $f \circ g = id_B$. Escrevemos $f^{-1} = g$ e dizemos que f é uma função invertível.

[Observação] Nas condições da definição anterior, $g : B \longrightarrow A$ é, também, uma função bijectiva, sendo f a sua inversa. Assim, $\big(f^{-1}\big)^{-1} = f$. Dizemos que f e g são funções inversas.

[Exemplo] As funções

$$\begin{array}{rccc} f: & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & x+2 \end{array} \qquad \text{e} \qquad \begin{array}{rccc} g: & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & x-2 \end{array}$$

são inversas. De facto, para qualquer real x, temos

$$\big(g \circ f\big)(x) = g\big(f(x)\big) = g(x+2) = (x+2) - 2 = x = id_{\mathbb{R}}(x)$$

e

$$\big(f \circ g\big)(x) = f\big(g(x)\big) = f(x-2) = (x-2) + 2 = x = id_{\mathbb{R}}(x).$$

Portanto, $g \circ f = id_{\mathbb{R}}$ e $f \circ g = id_{\mathbb{R}}$.

[Proposição] Sejam $f : A \longrightarrow B$ e $g : B \longrightarrow C$ funções bijectivas. Então, $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Demonstração. Note-se que $g \circ f$ é uma função bijectiva de A em C, pelo que $(g \circ f)^{-1}$ é uma função de C em A. Além disso, f^{-1} é uma função de B em A e g^{-1} é uma função de C em B. Portanto, $f^{-1} \circ g^{-1}$ é, também, uma função de C em A. Temos, pois, que $(g \circ f)^{-1}$ e $f^{-1} \circ g^{-1}$ têm o mesmo conjunto de partida e o mesmo conjunto de chegada.

Dado um qualquer elemento x de C, temos que

$$\begin{aligned}
\big(f^{-1}\circ g^{-1}\big)(x) &= \big(f^{-1}\circ g^{-1}\circ id_C\big)(x)\\
&= \Big(f^{-1}\circ g^{-1}\circ \big(g\circ f\big)\circ \big(g\circ f\big)^{-1}\Big)(x)\\
&= \Big(f^{-1}\circ \big(g^{-1}\circ g\big)\circ f\circ \big(g\circ f\big)^{-1}\Big)(x)\\
&= \Big(f^{-1}\circ id_B\circ f\circ \big(g\circ f\big)^{-1}\Big)(x)\\
&= \Big(\big(f^{-1}\circ f\big)\circ \big(g\circ f\big)^{-1}\Big)(x)\\
&= \Big(id_A\circ \big(g\circ f\big)^{-1}\Big)(x)\\
&= \big(g\circ f\big)^{-1}(x).
\end{aligned}$$

Podemos, então, concluir que as funções $(g\circ f)^{-1}$ e $f^{-1}\circ g^{-1}$ são iguais.

Relações binárias

1 Relações binárias

[Definição] Sejam A e B conjuntos. Uma *relação binária* de A para B é um subconjunto R do produto cartesiano $A\times B$. Ao conjunto A chamamos *conjunto de partida* e ao conjunto B *conjunto de chegada* da relação. Se $A=B$, R diz-se uma *relação binária* em A.

[Notação] Sejam A e B conjuntos e R uma relação binária de A para B. De forma a simplificar a escrita, escrever-se-á $a\ R\ b$ (lê-se "a está relacionado por R com b") para notar $(a,b)\in R$, e $a\not R\, b$ (lê-se "a não está relacionado por R com b") para indicar que $(a,b)\notin R$.

[Exemplo] Consideremos os conjuntos $A=\{1,2,3\}$ e $B=\{a,b\}$. O conjunto

$$R=\{(1,a),(1,b),(2,b),(3,a)\}$$

é uma relação binária de A para B. Facilmente se verifica que $1\ R\ a$ e $2\not R\ a$.

[Exemplo] Seja $A=\{1,2,3\}$. São relações binárias em A os conjuntos

$$R=\{(1,1),(1,3),(2,2),(3,3),(3,2)\},\quad S=\{(2,1)\},\quad \emptyset \quad\text{e}\quad A\times A.$$

Facilmente se verifica que $x\ R\ x$ para todo o $x\in A$ e $1\not S\ 1$.

Dados dois conjuntos A e B, o conjunto de *todas* as relações binárias de A para B é exactamente o conjunto potência $\mathcal{P}(A\times B)$. À relação $\emptyset$ chamamos *relação vazia* e à relação $A\times B$ *relação universal*.

[Observação] Se um conjunto A tem n elementos e um conjunto B tem m elementos, sabemos que $A \times B$ tem nm elementos e, consequentemente, que $\mathcal{P}(\mathcal{A} \times \mathcal{B})$ tem 2^{nm} elementos. Assim, existem 2^{nm} relações binárias diferentes de A para B.

[Definição] Seja R uma relação binária de um conjunto A para um conjunto B. Chamamos *domínio* de R ao conjunto

$$dom(R) = \{a \in A \ : \ \exists_{b \in B} \ \ a \ R \ b\}$$

e *contradomínio* de R ao conjunto

$$contradom(R) = \{b \in B \ : \ \exists_{a \in A} \ \ a \ R \ b\}.$$

Note-se que o domínio de uma relação $R \subseteq A \times B$ é um subconjunto do conjunto de partida da relação, A, e que o contradomínio é um subconjunto do conjunto de chegada da relação, B.

[Exemplo] Sejam $A = \{1, 2, 3, 5\}$, $B = \{3, 4, 5, 6, 7\}$ e R a relação binária de A para B definida por $a \ R \ b$ se e só se $a \geq b$, para quaisquer $a \in A$ e $b \in B$. Temos que

$$R = \{(3, 3), (5, 3), (5, 4), (5, 5)\}.$$

Assim,

$$dom(R) = \{3, 5\}$$

e

$$contradom(R) = \{3, 4, 5\}.$$

Facilmente se verifica que se R e S são relações binárias de um conjunto A para um conjunto B então também $R \cup S$, $R \cap S$ e $R \setminus S$ são relações binárias de A para B.

[Definição] Sejam A e B conjuntos. Para cada relação binária R de A para B definimos a chamada *relação inversa* de R, notada por R^{-1}, por

$$R^{-1} = \{(b, a) \in B \times A \ : \ (a, b) \in R\}.$$

Observe-se que R^{-1} é uma relação binária de B para A.

[Exemplo] Consideremos, uma vez mais, os conjuntos $A = \{1, 2, 3, 5\}$ e $B = \{3, 4, 5, 6, 7\}$ e a relação binária R de A para B definida por $a \ R \ b$ se e só se $a \geq b$, para quaisquer $a \in A$ e $b \in B$. Vimos já que

$$R = \{(3, 3), (5, 3), (5, 4), (5, 5)\}.$$

Assim,

$$R^{-1} = \{(3, 3), (3, 5), (4, 5), (5, 5)\},$$

ou seja, R^{-1} é a relação binária de B para A definida por $x \ R^{-1} \ y$ se e só se $x \leq y$, para quaisquer $x \in B$ e $y \in A$.

[Proposição] Sejam R e S relações binárias de um conjunto A para um conjunto B. Temos

1. $\left(R^{-1}\right)^{-1} = R$.
2. se $R \subseteq S$ então $R^{-1} \subseteq S^{-1}$.

Demonstração. Exercício. □

[Definição] Sejam R uma relação binária de um conjunto A para um conjunto B e S uma relação binária de B para um conjunto C. A *relação binária composta de S com R*, também designada por *S após R* e notada por $S \circ R$, é a relação definida por

$$S \circ R = \{(x, y) \in A \times C : \exists_{z \in B}\ (x, z) \in R \wedge (z, y) \in S\}.$$

$S \circ R$ é, portanto, uma relação binária de A para C. Dado $(x, y) \in A \times C$, temos que $x\ (S \circ R)\ y$ se existe $z \in B$ para o qual $x\ R\ z$ e $z\ S\ y$.

[Exemplo] Consideremos os conjuntos $A = \{1, 2, 3\}$, $B = \{a, b\}$ e $C = \{u, v, w\}$ e as relações binárias

$$R = \{(1, a), (2, b), (3, a)\},$$

de A para B, e

$$S = \{(a, u), (a, w), (b, v), (b, w)\},$$

de B para C. A relação $S \circ R$, de A para C, é dada por

$$S \circ R = \{(1, u), (1, w), (2, v), (2, w), (3, u), (3, w)\}.$$

[Exemplo] Consideremos o conjunto $A = \{1, 2, 3\}$ e as relações binárias em A

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

e

$$S = \{(3, 2), (3, 3)\}.$$

A relação $S \circ R$ é dada por

$$S \circ R = \{(1, 2), (1, 3)\},$$

$R \circ S$ é dada por

$$R \circ S = \{(3, 1)\}$$

e $R \circ R$ é dada por

$$R \circ R = \{(1, 1), (2, 2), (2, 3)\}.$$

[Proposição] Sejam A, B, C e D conjuntos. Dadas uma relação binária R de A para B, uma relação binária S de B para C e uma relação binária T de C para D, temos

1. $(T \circ S) \circ R = T \circ (S \circ R)$.

2. $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$.

Demonstração. (1.) Mostremos que $(T \circ S) \circ R \subseteq T \circ (S \circ R)$. Para tal, consideremos um elemento arbitrário (x, y) de $(T \circ S) \circ R$ e mostremos que $(x, y) \in T \circ (S \circ R)$. Dado que $x\ ((T \circ S) \circ R)\ y$, sabemos que existe $z \in B$ tal que $x\ R\ z$ e $z\ (T \circ S)\ y$. Como $z\ (T \circ S)\ y$, existe $w \in C$ tal que $z\ S\ w$ e $w\ T\ y$. Assim, $x\ R\ z$ e $z\ S\ w$, donde $x\ (S \circ R)\ w$. Atendendo a que $x\ (S \circ R)\ w$ e a que $w\ T\ y$, podemos concluir que $x\ (T \circ (S \circ R))\ y$, ou seja, que $(x, y) \in T \circ (S \circ R)$, como pretendíamos demonstrar. Logo, $(T \circ S) \circ R \subseteq T \circ (S \circ R)$. De modo análogo se verifica que $T \circ (S \circ R) \subseteq (T \circ S) \circ R$.

(2.) Para todo o objecto (x, y), temos

$$\begin{aligned}
(x, y) \in (S \circ R)^{-1} &\Leftrightarrow (y, x) \in S \circ R \\
&\Leftrightarrow \exists_{z \in B}\ (y, z) \in R \wedge (z, x) \in S \\
&\Leftrightarrow \exists_{z \in B}\ (z, y) \in R^{-1} \wedge (x, z) \in S^{-1} \\
&\Leftrightarrow \exists_{z \in B}\ (x, z) \in S^{-1} \wedge (z, y) \in R^{-1} \\
&\Leftrightarrow (x, y) \in R^{-1} \circ S^{-1}
\end{aligned}$$

Portanto, $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$. □

Atendamos, agora, a determinados tipos de relações binária num dado conjunto.

[Definição] Sejam A um conjunto e R uma relação binária em A. A relação R diz-se

- *reflexiva* se
$$\forall_{a \in A}\ (a, a) \in R$$
- *simétrica* se
$$\forall_{a,b \in A}\ \big((a, b) \in R \Leftrightarrow (b, a) \in R\big)$$
- *anti-simétrica* se
$$\forall_{a,b \in A}\ \Big(\big((a, b) \in R \wedge (b, a) \in R\big) \Rightarrow a = b\Big)$$
- *transitiva* se
$$\forall_{a,b,c \in A}\ \Big(\big((a, b) \in R \wedge (b, c) \in R\big)\ \Rightarrow (a, c) \in R\Big)$$

[Observação] Note-se que uma relação binária R em A é anti-simétrica se e somente se

$$\forall_{a,b \in A}\ \big(((a, b) \in R \wedge a \neq b) \Rightarrow (b, a) \notin R\big)$$

[Exemplo] Consideremos o conjunto $A = \{1, 2, 3\}$ e as relações binárias

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

$$S = \{(1, 1), (1, 2), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3)\},$$

$$T = \{(1,1),(1,2),(2,1),(2,3),(3,2),(3,3)\}$$

e

$$U = \{(1,1),(1,3),(2,1),(2,2),(2,3),(3,3)\}$$

em A.

Observe-se que $(1,1),(2,2),(3,3)$ são elementos de S e de U, pelo que estas relações são reflexivas. Já o par $(3,3)$ não pertence a R, donde R não é reflexiva. Também T é uma relação não reflexiva, uma vez que o par $(2,2)$ não é um seu elemento.

Note-se que $(2,3) \in R$ mas $(3,2) \notin R$. Assim, a relação R não é simétrica. Por argumentos semelhantes, podemos afirmar, também, que S e U não são simétricas. No que respeita à relação T, temos que $(a,b) \in T \Leftrightarrow (b,a) \in T$, para quaisquer $a, b \in \{1,2,3\}$. Portanto, T é simétrica.

Atendendo a que não existem elementos $a, b \in A$ distintos tais que $(a,b) \in R$ e $(b,a) \in R$, podemos afirmar que R é uma relação anti-simétrica. Por argumentos análogos, concluímos, também, que U é anti-simétrica. Já as relações S e T não são anti-simétricas, já que $(2,3),(3,2) \in S$ e $(1,2),(2,1) \in T$.

Note-se que $(2,3) \in R$ e $(3,1) \in R$. No entanto, $(2,1) \notin R$. Portanto, R não é uma relação transitiva. Também $(2,3) \in S$ e $(3,1) \in S$, mas $(2,1) \notin S$. Logo, a relação S não é transitiva. Relativamente à relação T, temos que $(2,3) \in T$ e $(3,2) \in T$, mas $(2,2) \notin T$. Por conseguinte, também T é não transitiva. Atendamos, agora, à relação U. Facilmente se verifica a veracidade das seguintes proposições:

$$\begin{gathered}
\big((1,1) \in U \wedge (1,1) \in U\big) \wedge (1,1) \in U,\\
\big((1,1) \in U \wedge (1,3) \in U\big) \wedge (1,3) \in U,\\
\big((1,3) \in U \wedge (3,3) \in U\big) \wedge (1,3) \in U,\\
\big((2,1) \in U \wedge (1,1) \in U\big) \wedge (2,1) \in U,\\
\big((2,1) \in U \wedge (1,3) \in U\big) \wedge (2,3) \in U,\\
\big((2,2) \in U \wedge (2,1) \in U\big) \wedge (2,1) \in U,\\
\big((2,2) \in U \wedge (2,2) \in U\big) \wedge (2,2) \in U,\\
\big((2,2) \in U \wedge (2,3) \in U\big) \wedge (2,3) \in U,\\
\big((2,3) \in U \wedge (3,3) \in U\big) \wedge (2,3) \in U,\\
\big((3,3) \in U \wedge (3,3) \in U\big) \wedge (3,3) \in U.
\end{gathered}$$

Podemos, portanto, afirmar que

$$\forall_{a,b,c \in A} \ \Big(\big((a,b) \in U \wedge (b,c) \in U\big) \Rightarrow (a,c) \in U\Big),$$

pelo que U é transitiva.

2 Relações de equivalência

[Definição] Seja A um conjunto. Uma relação binária R em A diz-se uma *relação de equivalência* se R é reflexiva, simétrica e transitiva.

Vejamos alguns exemplos.

[Exemplo] Consideremos o conjunto $\mathbb{N}$ dos números naturais e a relação R, que facilmente se demonstra ser de equivalência, definida por

$$a \ R \ b \ \Leftrightarrow \ 3 \text{ divide } a - b,$$

para quaisquer $a, b \in \mathbb{N}$. Note-se que

- $a \ R \ 1$ se e só se 3 divide $a - 1$, ou seja, se existe $k \in \mathbb{N}$ tal que $a - 1 = 3k$, ou seja, tal que $a = 3k + 1$. Assim, $a \ R \ 1$ se e só se o resto da divisão de a por 3 é 1.
- $a \ R \ 2$ se e só se 3 divide $a - 2$, isto é, se e só se o resto da divisão de a por 3 é 2.
- $a \ R \ 3$ se e só se 3 divide $a - 3$, ou seja, se e só se o resto da divisão de a por 3 é 0.
- Em $\mathbb{N}$, na divisão de um número por 3, os únicos restos possíveis são $0, 1$ e 2. Portanto, dado um natural a, temos que ou $a \ R \ 1$ ou $a \ R \ 2$ ou $a \ R \ 3$.

Dividimos, assim, o conjunto $\mathbb{N}$ em 3 classes disjuntas.

[Exemplo] Consideremos, agora, o conjunto $A = \{3, 5, 6, 7, 8\}$ e a relação de equivalência S em A definida por

$$a \ S \ b \ \Leftrightarrow \ a \text{ e } b \text{ têm o mesmo número de divisores naturais,}$$

para quaisquer $a, b \in A$. Note-se que

- os elementos $3, 5$ e 7 têm exactamente dois divisores naturais cada um [a unidade e o próprio].
- os elementos 6 e 8 têm quatro divisores naturais cada um.

Assim, os naturais $3, 5$ e 7 estão todos relacionados, dois a dois, por S e não estão em relação por S nem com o 6 nem com o 8. Além disso, o 6 está em relação por S com o 8 (e vice-versa). Podemos, então, considerar uma divisão do conjunto A definida pela relação S: por um lado temos o subconjunto $\{3, 5, 7\}$ e por outro o subconjunto $\{6, 8\}$. Dividimos, deste modo, o conjunto A em 2 classes disjuntas.

Analisemos, de seguida, esta ideia de divisão de um conjunto em classes disjuntas associada a uma classe de equivalência. As seguintes definições são essenciais.

[Definição] Sejam A um conjunto e R uma relação de equivalência em A. Para cada elemento a de A chamamos *classe de equivalência de a módulo R* ou, caso não haja ambiguidade, *classe de equivalência de a* ao conjunto $\{b \in A : a \ R \ b\}$, denotado por $[a]_R$. Ao conjunto de todas as classes de equivalência dos elementos de A chamamos *conjunto quociente de A por R* e denotámo-lo por A/R. Temos, então, que $A/R = \{[a]_R : a \in A\}$.

[Definição] Sejam A um conjunto e $\pi \subseteq \big(\mathcal{P}(A) \setminus \{\emptyset\}\big)$ [1]. Dizemos que π é uma *partição de* A se

- para todo o elemento a de A existe $X \in \pi$ tal que $a \in X$.
- se $X, Y \in \pi$ e $X \neq Y$ então $X \cap Y = \emptyset$.

Uma partição será, então, uma divisão de um conjunto em subconjuntos (não vazios) disjuntos. Nos exemplos acima, o conjunto suporte ficou divido em três, no primeiro caso, e em dois subconjuntos disjuntos, no segundo caso.

Vejamos que uma relação de equivalência num dado conjunto define sempre uma partição desse conjunto. Com efeito, se R é uma relação de equivalência sobre um conjunto A, temos que

- $[a]_R = [b]_R$ sempre que $a \ R \ b$:

  Note-se que

  $$[a]_R = \{c \in A : a \ R \ c\} \text{ e } [b]_R = \{d \in A : b \ R \ d\}$$

  Admitamos que $a \ R \ b$. Então, atendendo à simetria de R, $b \ R \ a$. Dado $x \in [a]_R$, temos que $a \ R \ x$. Como $b \ R \ a$ e $a \ R \ x$, temos, pela transitividade de R, que $b \ R \ x$. Logo, $x \in [b]_R$. Provámos, deste modo, que $[a]_R \subseteq [b]_R$. A inclusão $[b]_R \subseteq [a]_R$ pode ser demonstrada usando argumentos análogos. Assim, $[a]_R = [b]_R$.

- $[a]_R \cap [b]_R = \emptyset$ se $a \not R \ b$:

  Suponhamos que existe $x \in [a]_R \cap [b]_R$. Então, $a \ R \ x$ e $b \ R \ x$. Atendendo à simetria de R, segue-se que $x \ R \ b$. Assim, $a \ R \ x$ e $x \ R \ b$, pelo que, por transitividade, $a \ R \ b$. Logo, $[a]_R \cap [b]_R = \emptyset$ se $a \not R \ b$.

Consideremos, então, $\pi = A/R$. Facilmente se verifica que π é uma partição de A.

[Exemplo] Consideremos, uma vez mais, o conjunto $A = \{3, 5, 6, 7, 8\}$ e a relação de equivalência S em A definida por

$$a \ S \ b \ \Leftrightarrow \ a \text{ e } b \text{ têm o mesmo número de divisores naturais,}$$

para quaisquer $a, b \in A$. Referimos anteriormente que os naturais $3, 5$ e 7 estão todos relacionados, dois a dois, por S e não estão em relação por S nem com o 6 nem com o 8. Sabemos, também, que o 6 está em relação por S com o 8 (e vice-versa). Assim,

- $[3]_S = [5]_S = [7]_S = \{3, 5, 7\}$.
- $[6]_S = [8]_S = \{6, 8\}$.

[1] π é, portanto, um conjunto de subconjuntos não vazios de A

- $A/S = \{[3]_S, [5]_S, [6]_S, [7]_S, [8]_S\} = \{\{3,5,7\},\{6,8\}\}$.

Observe-se que $\pi = A/S$ é formado por dois conjuntos ($\{3,5,7\}$ e $\{6,8\}$) cuja união é A e cuja intersecção é o conjunto vazio. $\pi = A/S$ é, com efeito, uma partição de A.

Vejamos, agora, que uma partição de um conjunto A define uma relação de equivalência em A. Consideremos, então, um conjunto A e uma sua partição π. Seja R a relação binária em A definida por

$$a \ R \ b \ \Leftrightarrow \text{existe } X \in \pi \text{ tal que } a, b \in X,$$

para quaisquer $a, b \in A$. Prova-se que R é, de facto, uma relação de equivalência.

[Exemplo] Consideremos o conjunto $A = \{1,2,3,4,5,6\}$ e a sua partição $\pi = \{\{1\},\{2,4,6\},\{3,5\}\}$. Seja R a relação de equivalência em A definida por

$$a \ R \ b \ \Leftrightarrow \text{existe } X \in \pi \text{ tal que } a, b \in X,$$

para quaisquer $a, b \in A$. Podemos, assim, afirmar que

- $1 \ R \ 1$ pois $1 \in \{1\}$.
- $2 \ R \ 4$ uma vez que $2, 4 \in \{2,4,6\}$ (e, por conseguinte, $4 \ R \ 2$).
- $4 \ R \ 6$ dado que $4, 6 \in \{2,4,6\}$ (e, consequentemente, $6 \ R \ 4$).
- $3 \ R \ 5$ pois $3, 5 \in \{3,5\}$ (e, consequentemente, $5 \ R \ 3$).
- $1 \not R \ 2$ pois 1 e 2 não pertencem a um mesmo subconjunto de A pertencente a π (e, por conseguinte, $2 \not R \ 1$).

Rapidamente se conclui que

$$R = \{(1,1),(2,2),(4,4),(6,6),(2,4),(4,2),(2,6),(6,2),(4,6),(6,4),(3,3),(5,5),(3,5),(5,3)\}.$$

Em conclusão, podemos afirmar que definir uma partição de um conjunto A é o mesmo que definir uma relação de equivalência em A.

3 Relações de ordem parcial

[Definição] Seja A um conjunto. Uma relação binária R em A diz-se uma *relação de ordem parcial* se R é reflexiva, anti-simétrica e transitiva.

[Exemplo] A relação "menor ou igual" no conjunto dos números inteiros não é simétrica. De facto, $3 \leq 4$, mas $4 \not\leq 3$. No entanto, se dois inteiros n e m satisfazem $n \leq m$ e $m \leq n$, sabemos que $n = m$. A relação "menor ou igual" é, portanto, anti-simétrica. Com efeito,

é uma relação de ordem parcial em $\mathbb{Z}$ (dado um qualquer inteiro n, $n \leq n$, pelo que $\leq$ é reflexiva; $\leq$ é anti-simétrica; dados quaisquer inteiros n, m e k, se $n \leq m$ e $m \leq k$, segue-se que $n \leq k$, pelo que $\leq$ é transitiva).

[Definição] Sejam A um conjunto não vazio e R uma relação de ordem parcial em A. O par (A, R) diz-se um *conjunto parcialmente ordenado (c.p.o.)*.

[Exemplos] Os seguintes pares são exemplos de c.p.o.'s:

- $(\mathbb{Z}, \leq)$
- $(\mathbb{N}, |)$, em que $|$ é a relação "divide" em $\mathbb{N}$ (dado um qualquer natural n, $n|n$, donde $|$ é uma relação reflexiva; para quaisquer dois naturais n e m, se $n|m$ e $m|n$, é claro que $n = m$ e, portanto, $|$ é anti-simétrica; dados quaisquer naturais n, m e k, se $n|m$ e $m|k$, temos que $n|k$, pelo que $|$ é transitiva)
- $(\mathcal{P}(A), \subseteq)$, em que A é um conjunto qualquer (dado um qualquer subconjunto X de A, $X \subseteq X$, donde dado um qualquer elemento X de $\mathcal{P}(A)$, $X \subseteq X$ e $\subseteq$ é uma relação reflexiva em $\mathcal{P}(A)$; para quaisquer dois subconjuntos X e Y de A, se $X \subseteq Y$ e $Y \subseteq X$, é óbvio que $X = Y$ e, portanto, podemos afirmar que $\subseteq$ é anti-simétrica; dados quaisquer subconjuntos X, Y e Z de A, se $X \subseteq Y$ e $Y \subseteq Z$, temos que $X \subseteq Z$, pelo que $\subseteq$ é transitiva)

[Notação] As ordens parciais mais familiares são as relações $\leq$ ("menor ou igual") e $\geq$ ("maior ou igual") em $\mathbb{R}$. Por isso, muitas vezes notamos um c.p.o. simplesmente por $(A, \leq)$ ou por $(A, \geq)$, embora as ordens $\leq$ ou $\geq$ possam não corresponder às relações usuais em $\mathbb{R}$ notadas por aqueles símbolos.

[Definição] Dado um c.p.o. $(A, \leq)$ e dados $a, b \in A$, escrevemos

- $a \leq b$ e lemos "a é menor ou igual a b" se $(a, b) \in \leq$;
- $a \not\leq b$ e lemos "a não é menor ou igual a b" se $(a, b) \notin \leq$;
- $a \geq b$ e lemos "a é maior ou igual a b" se $b \leq a$;
- $a \not\geq b$ e lemos "a não é maior ou igual a b" se $b \not\leq a$;
- $a < b$ e lemos "a é menor que b" se $a \leq b$ e $a \neq b$;
- $b > a$ e lemos "b é maior que a" se $a < b$;
- $a||b$ e lemos "a e b são incomparáveis" se $a \not\leq b$ e $b \not\leq a$;
- $a << b$ e lemos "b é sucessor de a" se $a < b$ e $\neg(\exists_{c \in A} \ a < c < b)$;
- $b >> a$ se $a << b$.

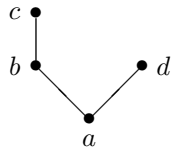
Um c.p.o. $(A, \leq)$, em que A é finito, pode ser representado por meio de um *diagrama de Hasse* como se descreve de seguida:

- cada elemento a de A é representado por um ponto;
- se a e b são elementos de A tais que $a < b$ então b é representado acima de a. Além disso, se $a << b$, é desenhado um segmento de recta unindo os respectivos pontos.

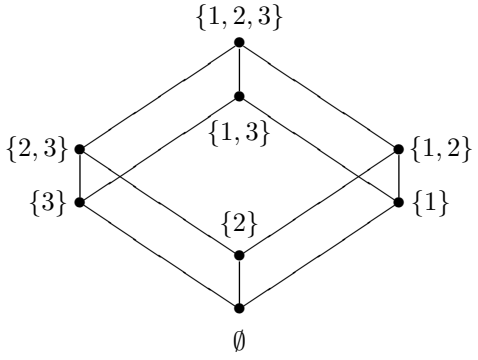
[Exemplo] Consideremos o conjunto $A = \{a, b, c, d\}$ e a relação binária

$$\leq = \big\{(a,a), (b,b), (c,c), (d,d), (a,b), (a,c), (b,c), (a,d)\big\}.$$

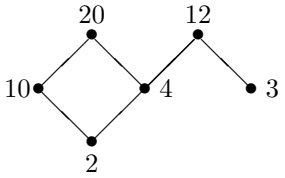
em A. Facilmente se verifica que o par $(A, \leq)$ é um c.p.o. e que $a << b$, $b << c$ e $a << d$. Assim, o diagrama de Hasse associado a este c.p.o. é o seguinte:



[Exemplo] Consideremos o c.p.o. $\Big(\mathcal{P}\big(\{1,2,3\}\big), \subseteq\Big)$. O diagrama de Hasse associado é o seguinte:



[Exemplo] Consideremos o c.p.o. $\big(\{2,3,4,10,12,20\}, |\big)$. O diagrama de Hasse associado é o seguinte:



Definimos, de seguida, alguns elementos especiais num c.p.o..

[Definição] Dados um c.p.o. $(A, \leq)$, $X \subseteq A$ e $a \in A$, dizemos que a é

- *máximo* de $(A, \leq)$ se $\forall_{x \in A} \;\; x \leq a$;
- *mínimo* de $(A, \leq)$ se $\forall_{x \in A} \;\; a \leq x$;
- *elemento maximal* de $(A, \leq)$ se $\nexists_{x \in A} \;\; a < x$;

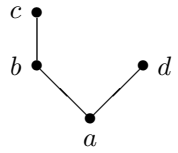
- *elemento minimal* de $(A, \leq)$ se $\nexists_{x \in A} \ x < a$;
- *majorante* de X se $\forall_{x \in X} \ x \leq a$;
- *minorante* de X se $\forall_{x \in X} \ a \leq x$;
- *supremo* de X se a é majorante de X e $a \leq x$ para qualquer majorante x de X;
- *ínfimo* de X se a é minorante de X e $x \leq a$ para qualquer minorante x de X;
- *máximo* de X se a é majorante de X e $a \in X$;
- *mínimo* de X se a é minorante de X e $a \in X$;

Dados um c.p.o. $(A, \leq)$ e um seu subconjunto X, notamos, se existirem, por $\max X$, $\min X$, $\sup X$ e $\inf X$ respectivamente o máximo, o mínimo, o supremo e o ínfimo de X.

[Exemplo] Consideremos, de novo, o conjunto $A = \{a, b, c, d\}$ e a relação binária

$$\leq = \big\{(a,a), (b,b), (c,c), (d,d), (a,b), (a,c), (b,c), (a,d)\big\}.$$

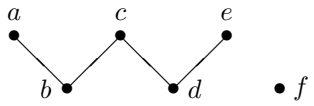
em A. Vimos já que o diagrama de Hasse associado a este c.p.o. é o seguinte:



Note-se que $(A, \leq)$ não tem máximo: de facto, $a \not\geq b$, $b \not\geq d$, $c \not\geq d$ e $d \not\geq c$. No entanto, $(A, \leq)$ admite mínimo: a. Facilmente se verifica que os elementos maximais de $(A, \leq)$ são c e d e que existe um só elemento minimal do c.p.o.: a.

Consideremos, agora, os subconjuntos $X = \{a, b, c\}$ e $Y = \{b, d\}$. O elemento c é o único majorante de X e a é o seu único minorante. Além disso, $\max X = c$, $\min X = a$, $\sup X = c$ e $\inf X = a$. Relativamente ao subconjunto Y, não admite nem majorantes nem minorantes. Assim, não existem máximo, mínimo, supremo ou ínfimo de Y.

[Exemplo] Consideremos o c.p.o. $\big(A = \{a, b, c, d, e, f\}, \leq\big)$ cujo diagrama de Hasse associado é o seguinte:



Facilmente se verifica que $(A, \leq)$ não admite nem máximo nem mínimo, que os elementos maximais do c.p.o. são a, c, e e f, e que os seus elementos minimais são b, d e f. Observe-se que f é simultaneamente maximal e minimal.