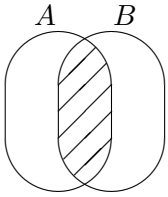
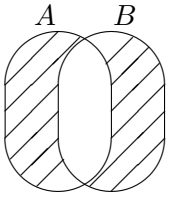
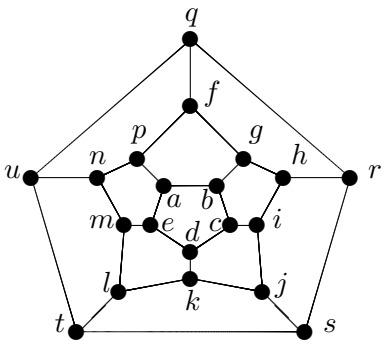
Matemática
Discreta



$A \cap B$



$A \oplus B$



Maria do Rosário Fernandes
Departamento de Matemática
Faculdade de Ciências e Tecnologia
UNL

Índice

Capítulo 1

CONJUNTOS

1.1 Definições e Exemplos

Adoptamos neste curso o conceito intuitivo de conjunto. Assim, um conjunto é uma "colecção de objectos", ou seja um "ente matemático"que resulta de considerar simultaneamente objectos diversos, ditos os seus elementos, como um todo.

Denotaremos os conjuntos por letras maiúsculas:

$$A,\ B,\ C, \ldots,\ X,\ Y,\ Z, \ldots$$

e os objectos por letras minúsculas:

$$a,\ b,\ c, \ldots,\ x,\ y,\ z, \ldots$$

Escreveremos $x \in X$ (que se lê "x pertence a X") para significar que x é um elemento de X e escreveremos $x \notin X$ (que se lê "x não pertence a X") para significar que x não é um elemento de X.

Exemplo 1.1 1. $\mathbb{N}$ *designa o conjunto dos números naturais:*

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

2. $\mathbb{Z}$ *designa o conjunto dos números inteiros:*

$$\mathbb{Z} = \{\ldots,\ -2,\ -1,\ 0,\ 1,\ 2, \ldots\};$$

3. $\mathbb{Q}$ *designa o conjunto dos números racionais:*

$$\mathbb{Q} = \{\frac{p}{q} :\ p \in \mathbb{Z},\ q \in \mathbb{Z},\ q \neq 0\};$$

4. $\mathbb{R}$ *designa o conjunto dos números reais;*

5. $\emptyset$ *ou* $\{\ \}$ *designa o conjunto vazio, isto é, o conjunto sem elementos.*

Por exemplo:

. $2 \in \mathbb{N}$, $2 \in \mathbb{Z}$, $2 \in \mathbb{Q}$, $2 \in \mathbb{R}$;

. $-2 \notin \mathbb{N}$, $-2 \in \mathbb{Z}$, $-2 \in \mathbb{Q}$, $-2 \in \mathbb{R}$;

. $\frac{1}{3} \notin \mathbb{N}$, $\frac{1}{3} \notin \mathbb{Z}$, $\frac{1}{3} \in \mathbb{Q}$, $\frac{1}{3} \in \mathbb{R}$;

. $\sqrt{3} \notin \mathbb{N}$, $\sqrt{3} \notin \mathbb{Z}$, $\sqrt{3} \notin \mathbb{Q}$, $\sqrt{3} \in \mathbb{R}$;

Outros exemplos:

1. $A = \{-2,\ \frac{1}{3},\ \sqrt{3},\ 2\}$;
2. $\{2n :\ n \in \mathbb{N}\}$-conjunto dos números naturais pares;
3. $\{2n-1 :\ n \in \mathbb{N}\}$-conjunto dos números naturais ímpares;
4. $\{n \in \mathbb{N} :\ 5 \leq n < 21\}$;
5. $\{x \in \mathbb{R} :\ x^2 > 0\}$;
6. $\{x \in \mathbb{R} :\ x^2 - 3x + 2 = 0\}$;
7. $\{x^2 - 3x + 2 :\ x \in \mathbb{R}\}$;
8. $\{\emptyset\}$;
9. $\{\{2\},\ \{1,\ 2\},\ \emptyset\}$;
10. $\{1,\ 2,\ \{\emptyset\},\ \{3,\ 4\}\}$.

Observação Os conjuntos 6. e 7. do exemplo anterior, são distintos. Enquanto que os objectos do conjunto 6. são 1 e 2, os objectos do conjunto 7. são, além do 1 e do 2, o 0,...

1.2 Representação de Conjuntos

Vejamos alguns modos de representar um conjunto X:

1. **Representação em extensão**

   Este tipo de representação caracteriza-se pela enumeração dos elementos do conjunto X.

Exemplo 1.2 (a) $\{1,\ 3,\ 5\}$;

(b) $\{6,\ 1,\ 2\}$.

2. **Representação em compreensão**

Este tipo de representação caracteriza-se por definir o conjunto X através de condições.

Exemplo 1.3 (a) $\{n \in \mathbb{N} :\ 4 \leq n \leq 13\}$;

(b) $\{x \in \mathbb{Q} :\ x^2 - 2 = 0\}$;

(c) $\{x \in \mathbb{R} :\ x^2 - 2 = 0\}$;

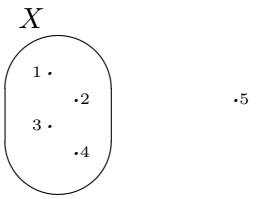
(d) $\{x^2 - 2 :\ x \in \mathbb{R}\}$.

Observação *O conjunto* (b) *é o conjunto vazio e o conjunto* (c) *é o conjunto* $\{-\sqrt{2},\ \sqrt{2}\}$.

3. **Representação por Diagrama de Venn**

Neste tipo de caracterização, os elementos de X ficam no interior de uma linha fechada.

Exemplo 1.4 *Consideremos o conjunto* $X = \{1,\ 2,\ 3,\ 4\}$ *e o objecto* 5. *A representação do conjunto* X *e dos objectos* 1, 2, 3, 4 *e* 5 *em Diagrama de Venn é a seguinte:*



1.3 Subconjuntos

Sejam A e B conjuntos.

Dizemos que A **e** B **são iguais**, e escrevemos $A = B$, se A e B possuírem os mesmos elementos:

$$\text{para qualquer objecto } x,\ x \in A \Longleftrightarrow x \in B.$$

Dizemos que A **está contido em** B (ou que A é um subconjunto de B), e escrevemos $A \subseteq B$, se todos os elementos de A forem elementos de B:

$$\text{para qualquer objecto } x,\ x \in A \Longrightarrow x \in B.$$

Dizemos que A **está estritamente contido em** B (ou que A é um subconjunto próprio de B), e escrevemos $A \subset B$, se

$$A \subseteq B \qquad \text{e} \qquad A \neq B.$$

Proposição 1.5 *Sejam A, B e C três conjuntos.*

1. *$A = B$ se, e só se, $A \subseteq B$ e $B \subseteq A$.*
2. *$A \subseteq B$ e $B \subseteq C \Longrightarrow A \subseteq C$.*

Exemplo 1.6 1. *$A = \{1,\ 2\}$, $B = \{x \in \mathbb{R} :\ x^2 - 3x + 2 = 0\}$ então $A = B$;*

2. *$A = \{1,\ 2\}$, $C = \{x \in \mathbb{N} :\ x$ é divisor de $12\}$ então*

$$A \subset C = \{1,\ 2,\ 3,\ 4,\ 6,\ 12\} = \{2,\ 4,\ 1,\ 12,\ 6,\ 3\};$$

Observação *A ordem pela qual os elementos surgem num conjunto não é significativa.*

3.

$$\begin{aligned} \{n \in \mathbb{N} :\ 2 < n < 3\} &= \{x \in \mathbb{R} :\ x^2 < 0\} \\ &= \{x \in \mathbb{Q} :\ x^2 = 2\} \\ &= \{\}. \end{aligned}$$

1.4 Par Ordenado

Sejam x e y dois objectos.
Chamamos **par não ordenado**, formado por x e y, ao conjunto $\{x,\ y\}$.

Chamamos **par ordenado**, formado por x e y, ao conjunto $(x,\ y)$, definido por

$$(x,\ y) = \{\{x\},\ \{x,\ y\}\}.$$

Dados dois objectos x e y temos $\{x,\ y\} = \{y,\ x\}$ e, se $x = y$ então $\{x,\ y\}$ é o conjunto singular $\{x\}$.

Por outro lado, a noção de par ordenado possuí a seguinte propriedade fundamental:

Teorema 1.7 *Sejam x, y, z e t quatro objectos. Então:*

$$(x,\ y) = (z,\ t) \quad \Longleftrightarrow \quad x = z \ e \ y = t.$$

Demonstração A implicação $\Longleftarrow$ é evidente.

Demonstremos $\Longrightarrow$: Por definição,

$$(x,\ y) = (z,\ t) \quad \Longleftrightarrow \quad \{\{x\},\ \{x,\ y\}\} = \{\{z\},\ \{z,\ t\}\}.$$

Consideremos separadamente dois casos:

1º caso Se $x = y$, então $\{\{x\},\ \{x,\ y\}\} = \{x\}$, pelo que $(x,\ y) = \{\{x\}\}$. Porque $\{\{x\}\} = \{\{z\},\ \{z,\ t\}\}$, então $\{\{x\}\} = \{\{z\}\} = \{\{z,\ t\}\}$. Donde, $z = x = t$. Em particular, $x = z$ e $y = t$.

2º caso Se $x \neq y$, porque $\{\{x\},\ \{x,\ y\}\} = \{\{z\},\ \{z,\ t\}\}$, então $\{\{x\}\} = \{\{z\}\}$ e $\{\{x,\ y\}\} = \{\{z,\ t\}\}$. Mas isto implica que $x = z$ e $y = t$. □

Observação : A noção de par ordenado generaliza-se de forma natural. Assim, um terno ordenado (formado pelos objectos x, y e z), $(x,\ y,\ z)$ pode ser definido (em termos de conjuntos) por

$$(x,\ y,\ z) = (x,\ (y,\ z)) = \{\{x\},\ \{x,\ \{\{y\},\ \{y,\ z\}\}\}\}.$$

Mais geralmente, um n-uplo ordenado ($n \geq 1$) (formado pelos objectos $x_1,\ x_2, \ldots, x_n$) $(x_1,\ x_2, \ldots, x_n)$ pode ser definido por

$$(x_1,\ x_2, \ldots, x_n) = (x_1,\ (x_2,\ (\ldots,\ (x_{n-1},\ x_n)\ldots))).$$

Esta noção goza da generalização da propriedade fundamental.

1.5 Operações sobre conjuntos

Sejam X e Y dois conjuntos. Chamamos:

1. **União** dos conjuntos X e Y ao conjunto

$$X \cup Y = \{z :\ z \in X \text{ ou } z \in Y\};$$

2. **Intersecção** dos conjuntos X e Y ao conjunto

$$X \cap Y = \{z :\ z \in X \text{ e } z \in Y\};$$

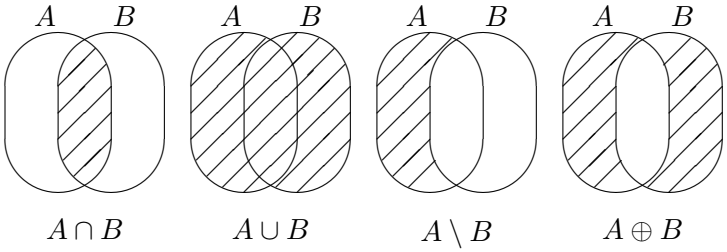
3. **Complementar** (ou diferença) de Y em X ao conjunto
$$X \setminus Y = \{z : \ z \in X \text{ e } z \notin Y\};$$

4. **Diferença simétrica** dos conjuntos X e Y ao conjunto
$$X \oplus Y = (X \cup Y) \setminus (X \cap Y);$$

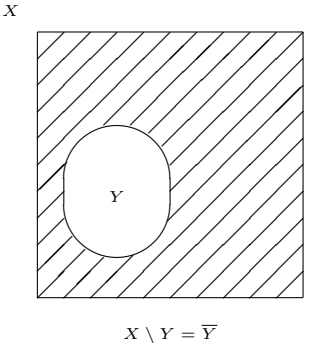
5. **Produto cartesiano** (ou produto directo) de X e Y ao conjunto
$$X \times Y = \{(x, \ y) : \ x \in X \text{ e } y \in Y\};$$

6. **Conjunto das partes** de X (potência de X) e denotamos por $\mathcal{P}(X)$ ou por 2^X, ao conjunto de todos os subconjuntos de X:
$$\mathcal{P}(X) = \{A : \ A \subseteq X\}.$$

Em termos de diagrama de Venn, temos:



Observação : Se Y é um subconjunto de X, denotaremos o complementar de Y em X, $X \setminus Y$, por $\overline{Y}$. Assim,
$$\overline{Y} = \{x \in X : \ x \notin Y\}$$
ou em termos de diagrama de Venn



Exemplo 1.8 1. *Sejam* $X = \{-5,\ 2,\ 10,\ \sqrt{5}\},\ Y = \{\sqrt{3},\ 1,\ 2\}$.

$X \cup Y = \{-5,\ 2,\ 10,\ \sqrt{5},\ \sqrt{3},\ 1\}$;

$X \cap Y = \{2\}$;

$X \setminus Y = \{-5,\ 10,\ \sqrt{5}\}$;

$X \oplus Y = \{-5,\ 10,\ \sqrt{5},\ \sqrt{3},\ 1\}$;

$X \times Y = \{(-5,\ \sqrt{3}),\ (-5,\ 1),\ (-5,\ 2),\ (2,\ \sqrt{3}),\ (2,\ 1)),\ (2,\ 2),$
$(10,\ \sqrt{3}),\ (10,\ 1),\ (10,\ 2),\ (\sqrt{5},\ \sqrt{3}),\ (\sqrt{5},\ 1),\ (\sqrt{5},\ 2)\}$;

$\mathcal{P}(Y) = \{\emptyset,\ \{\sqrt{3}\},\ \{1\},\ \{2\},\ \{\sqrt{3},\ 1\},\ \{\sqrt{3},\ 2\},\ \{1,\ 2\},\ \{\sqrt{3},\ 1,\ 2\}\}$.

2. *Sejam* $X = \{x \in \mathbb{R} :\ x > 1\},\ Y = \{x \in \mathbb{R} :\ 0 < x \leq 3\}$.

$X \cup Y = \{x \in \mathbb{R} :\ 0 < x\}$;

$X \cap Y = \{x \in \mathbb{R} :\ 1 < x \leq 3\}$;

$X \setminus Y = \{x \in \mathbb{R} :\ x > 3\}$;

$X \oplus Y = \{x \in \mathbb{R} :\ 0 < x \leq 1$ *ou* $x > 3\}$.

3. $X = \emptyset$;

$\mathcal{P}(X) = \{\emptyset\}$;

$\mathcal{P}(\mathcal{P}(X)) = \{\emptyset,\ \{\emptyset\}\}$.

1.6 Propriedades das operações sobre conjuntos

Em primeiro lugar vamos descrever algumas propriedades das operações união e intersecção de conjuntos.

Teorema 1.9 *Sejam* A, B, C *e* X *quatro conjuntos. Então,*

(1) $\begin{cases} A \cup \emptyset = A \\ A \cap \emptyset = \emptyset \end{cases}$

(2) *Se* $A \subseteq X$ $\begin{cases} A \cup X = X \\ A \cap X = A \end{cases}$

(3) *Idempotência* $\begin{cases} A \cup A = A \\ A \cap A = A \end{cases}$

(4) *Comutatividade* $\begin{cases} A \cup B = B \cup A \\ A \cap B = B \cap A \end{cases}$

(5) *Associatividade* $\begin{cases} (A \cup B) \cup C = A \cup (B \cup C) \\ (A \cap B) \cap C = A \cap (B \cap C) \end{cases}$

(6) *Distributividade* $\begin{cases} A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \\ A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \end{cases}$

Observação Sejam $X_1,\ X_2, \ldots,\ X_n$ n conjuntos. Tendo em conta que as operações $\cup$ e $\cap$ são associativas, podemos escrever sem ambiguidade

$$X_1 \cup X_2 \cup \ldots \cup X_n \quad (\text{ abreviadamente } \bigcup_{i=1}^{n} X_i)$$

e

$$X_1 \cap X_2 \cap \ldots \cap X_n \quad (\text{ abreviadamente } \bigcap_{i=1}^{n} X_i).$$

Proposição 1.10 (Leis distributivas generalizadas) *Sejam $A,\ X_1,\ X_2, \ldots,\ X_n,\ n+1$ conjuntos. Então*

$$A \cap (\bigcup_{i=1}^{n} X_i) = \bigcup_{i=1}^{n} (A \cap X_i)$$

e

$$A \cup (\bigcap_{i=1}^{n} X_i) = \bigcap_{i=1}^{n} (A \cup X_i).$$

Demonstração (da primeira igualdade)

Seja $x \in A \cap (\bigcup_{i=1}^{n} X_i)$. Então, $x \in A$ e $x \in \bigcup_{i=1}^{n} X_i$. Logo, $x \in A$ e existe $i_0 \in \{1, \ldots, n\}$ tal que $x \in X_{i_0}$. Assim sendo, $x \in A \cap X_{i_0}$ e, consequentemente, $x \in \bigcup_{i=1}^{n} (A \cap X_i)$. Portanto,

$$A \cap (\bigcup_{i=1}^{n} X_i) \subseteq \bigcup_{i=1}^{n} (A \cap X_i).$$

Reciprocamente, seja $x \in \bigcup_{i=1}^{n} (A \cap X_i)$. Então existe $i_0 \in \{1, \ldots, n\}$ tal que $x \in A \cap X_{i_0}$. Logo, $x \in A$ e $x \in X_{i_0}$, pelo que $x \in A$ e $x \in \bigcup_{i=1}^{n} X_i$. Consequentemente, $x \in A \cap (\bigcup_{i=1}^{n} X_i)$. Portanto,

$$A \cap (\bigcup_{i=1}^{n} X_i) \supseteq \bigcup_{i=1}^{n} (A \cap X_i)$$

e a primeira igualdade da proposição verifica-se. □

Proposição 1.11 *Sejam X e Y dois conjuntos. Então,*

(1) $X \subseteq X \cup Y$ *e* $X \cap Y \subseteq X$;

(2) $X \cap (X \cup Y) = X$ *e* $X \cup (X \cap Y) = X$.

A Proposição seguinte descreve-nos propriedades do complementar.

Proposição 1.12 *Sejam X um conjunto e $A,\ B \in \mathcal{P}(X)$ (A e B subconjuntos de X). Então,*

(1) $A \cap \overline{A} = \emptyset \qquad e \qquad A \cup \overline{A} = X$;
(2) *Se* $A \cap B = \emptyset$ *então* $B \subseteq \overline{A}$;
(3) *Se* $A \cup B = X$ *então* $\overline{A} \subseteq B$;
(4) *Se* $A \cap B = \emptyset$ *e* $A \cup B = X$ *então* $\overline{A} = B$;
(5) $\overline{\overline{A}} = A$.

Demonstração

(3)

$$\begin{array}{rcll} \overline{A} & = & X \cap \overline{A} & (\text{porque } A \subseteq X) \\ & = & (A \cup B) \cap \overline{A} & (\text{porque } A \cup B = X) \\ & = & (A \cap \overline{A}) \cup (B \cap \overline{A}) & (\text{distributiva}) \\ & = & \emptyset \cup (B \cap \overline{A}) & \\ & = & B \cap \overline{A} & \\ & \subseteq & B. & \end{array}$$

(4) Porque $A \cap B = \emptyset$, então por (2), $B \subseteq \overline{A}$. Porque $A \cup B = X$, usando (3) temos, $\overline{A} \subseteq B$. Portanto, $\overline{A} = B$.

(5) Como $\overline{A} \cap A = \emptyset$ e $\overline{A} \cup A = X$ (usando (1)), então por (4), concluímos que $\overline{\overline{A}} = A$. □

Teorema 1.13 (Leis de De Morgan) *Sejam X, A e B três conjuntos. Então,*

$$X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B)$$

e

$$X \setminus (A \cap B) = (X \setminus A) \cup (X \setminus B).$$

Demonstração (da primeira igualdade)

$$\begin{array}{rcl} x \in X \setminus (A \cup B) & \Leftrightarrow & x \in X \text{ e } x \notin (A \cup B) \\ & \Leftrightarrow & x \in X \text{ e } x \notin A \text{ e } x \notin B \\ & \Leftrightarrow & (x \in X \text{ e } x \notin A) \text{ e } (x \in X \text{ e } x \notin B) \\ & \Leftrightarrow & x \in (X \setminus A) \text{ e } x \in (X \setminus B) \\ & \Leftrightarrow & x \in (X \setminus A) \cap (X \setminus B). \end{array}$$

□

Teorema 1.14 (Leis de De Morgan generalizadas) *Sejam X, $A_1,\ A_2, \ldots,\ A_n$, $n+1$ conjuntos. Então*

$$X \setminus (\bigcup_{i=1}^{n} A_i) = \bigcap_{i=1}^{n} (X \setminus A_i)$$

e

$$X \setminus (\bigcap_{i=1}^{n} A_i) = \bigcup_{i=1}^{n} (X \setminus A_i).$$

Proposição 1.15 *Sejam X, A e B três conjuntos. Se $X \cap A = X \cap B$ e $X \cup A = X \cup B$ então $A = B$.*

Demonstração

$$\begin{array}{rcll} A & = & A \cap (X \cup A) & \\ & = & A \cap (X \cup B) & (\text{porque } X \cup A = X \cup B) \\ & = & (A \cap X) \cup (A \cap B) & (\text{distributiva}) \\ & = & (X \cap B) \cup (A \cap B) & (\text{porque } A \cap X = B \cap X) \\ & = & (X \cup A) \cap B & (\text{distributiva}) \\ & = & (X \cup B) \cap B & (X \cup A = X \cup B) \\ & = & B. & \end{array}$$

□

Proposição 1.16 *Sejam X um conjunto e $A,\ B \in \mathcal{P}(X)$. Então*

$$(A \cup B) \cap \overline{B} \subseteq A.$$

Demonstração Vamos demonstrar esta proposição por três processos distintos.

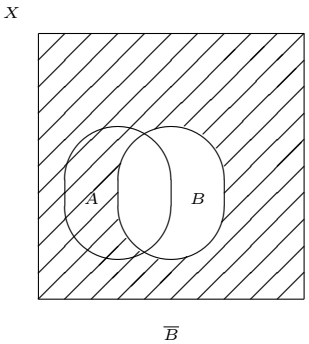
1. Utilizando as propriedades das operações sobre conjuntos.

$$\begin{array}{rcll} (A \cup B) \cap \overline{B} & = & (A \cap \overline{B}) \cup (B \cap \overline{B}) & (\text{distributiva}) \\ & = & (A \cap \overline{B}) \cup \emptyset & \\ & = & A \cap \overline{B} \subseteq A. & \end{array}$$

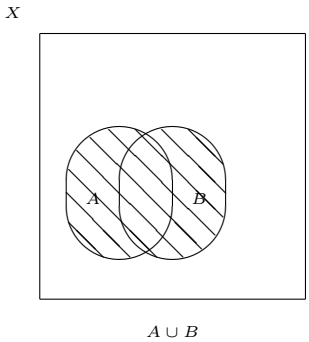
2. Utilizando a definição.

   Se $x \in (A \cup B) \cap \overline{B}$, então $x \in (A \cup B)$ e $x \in \overline{B}$, o que implica que $x \in A$.

3. Utilizando diagramas de Venn.

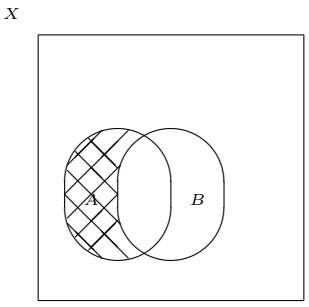


$\overline{B}$



$A \cup B$

Como a intersecção destes dois conjuntos é a parte comum aos dois, temos



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

□

1.7 Cardinalidade

Seja X um conjunto finito. Denotamos por $|X|$, o número de elementos de X.

Lema 1.17 *Sejam A, B dois conjuntos finitos tais que $A \cap B = \emptyset$ (isto é, A, B são disjuntos). Então,*

$$|A \cup B| = |A| + |B|.$$

Demonstração Usando diagrama de Venn, como $A \cap B = \emptyset$, então

pelo que $|A \cup B| = |A| + |B|$. □

Lema 1.18 *Sejam A, B dois conjuntos finitos. Então,*

$$|A \setminus B| = |A| - |A \cap B|.$$

Demonstração Porque $(A \setminus B) \cap (A \cap B) = \emptyset$ e $A = (A \setminus B) \cup (A \cap B)$, então, pelo Lema anterior,

$$|A| = |A \setminus B| + |A \cap B|.$$

Logo, $|A \setminus B| = |A| - |A \cap B|$. □

Teorema 1.19 *Sejam A, B dois conjuntos finitos. Então,*

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Demonstração Uma vez que $A \setminus B$, $B \setminus A$, $A \cap B$ são disjuntos dois a dois e a sua união é $A \cup B$, usando os Lemas anteriores,

$$\begin{aligned} |A \cup B| &= |(A \setminus B) \cup [(B \setminus A) \cup (A \cap B)]| \\ &= |A \setminus B| + |(B \setminus A) \cup (A \cap B)| \\ &= |A \setminus B| + |B \setminus A| + |A \cap B| \\ &= |A| - |A \cap B| + |B| - |A \cap B| + |A \cap B| \\ &= |A| + |B| - |A \cap B|. \end{aligned}$$

□

Corolário 1.20 *Sejam A, B e C conjuntos finitos. Então,*

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

Demonstração Usando o Teorema anterior, temos,

$$\begin{aligned} |A \cup B \cup C| &= |A \cup (B \cup C)| \\ &= |A| + |B \cup C| - |A \cap (B \cup C)| \\ &= |A| + |B| + |C| - |B \cap C| - |(A \cap B) \cup (A \cap C)| \\ &= |A| + |B| + |C| - |B \cap C| - |A \cap B| - |A \cap C| + |A \cap B \cap C|. \end{aligned}$$

□

Vejamos uma aplicação prática:

Exemplo 1.21 *Num congresso internacional de físicos, entre os* 100 *participantes de nacionalidades inglesa, francesa e alemã, pelo menos* 75 *falam inglês, pelo menos* 70 *falam francês e pelo menos* 65 *falam alemão. Quantos são, no mínimo, os participantes que falam as três línguas?*

Sejam I, F e A os conjuntos dos participantes que falam respectivamente inglês, francês e alemão.

Pelo Teorema,

$$|I \cap F| = |I| + |F| - |I \cup F| \geq 75 + 70 - 100 = 45,$$

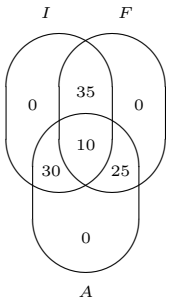
$$|I \cap A| = |I| + |A| - |I \cup A| \geq 75 + 65 - 100 = 40,$$
$$|F \cap A| = |F| + |A| - |F \cup A| \geq 70 + 65 - 100 = 35.$$

Então,

$$|I \cap F \cap A| = |I \cap (F \cap A)| = |I| + |F \cap A| - |I \cup (F \cap A)| \geq 75 + 35 - 100 = 10.$$

Portanto, pelo menos 10 *falam as três línguas.*

Em diagrama de Venn, teríamos



No caso de nos dizerem que existe um participante de cada nacionalidade, que fala unicamente a sua língua, teremos

$$|I \cup A|,\ |I \cup F|,\ |F \cup A| \leq 99.$$

Neste caso,

$$|I \cap F| \geq 46,\ |I \cap A| \geq 41,\ |F \cap A| \geq 36.$$

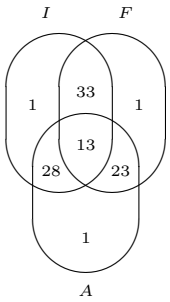
Como, 1 *só fala francês,* 1 *só fala inglês,* 1 *só fala alemão,*

$$|I \cup (F \cap A)| \leq 98.$$

Consequentemente,

$$|I \cap F \cap A| \geq 75 + 36 - 98 = 13.$$

Em diagrama de Venn,



Capítulo 2

Relações Binárias

2.1 Definições e exemplos

Sejam X e Y dois conjuntos. Uma relação entre X e Y é um subconjunto de $X \times Y$.

No caso de $X = Y$, a uma relação $R \subseteq X \times X$ entre X e X chamamos relação (binária) sobre X.

Usualmente X^2 significa $X \times X$, X^3 significa $X \times X \times X$ (conjunto dos ternos ordenados de elementos de X), e mais geralmente, X^n significa o conjunto dos n-uplos ordenados de elementos de X.

Assim, chamamos relação n-ária sobre X a qualquer subconjunto de X^n.

Exemplo 2.1 1. *Consideremos o conjunto* $X = \{1,\ 2,\ 3\}$. *O conjunto*

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

é uma relação binária sobre X *pois é um subconjunto de* X^2.

2. *Sendo* $X = \{1,\ 2,\ 3,\ 4\}$ *e* $R = \{(x,\ y) \in X^2 :\ x + y \leq 5\}$, *porque*

$$R = \{(1,\ 1),\ (1,\ 2),\ (1,\ 3),\ (1,\ 4),\ (2,\ 1),\ (2,\ 2),\ (2,\ 3),\ (3,\ 1),\ (3,\ 2),\ (4,\ 1)\} \subseteq X^2$$

então R *é uma relação binária sobre* X.

Notação Sejam X um conjunto e R uma relação binária sobre X. Dado um par $(x,\ y) \in X \times X$, escrevemos xRy ou $(x,\ y) \in R$, para designar que $(x,\ y)$ é um elemento de R. E escrevemos $x \not R y$ ou $(x,\ y) \notin R$ para designar que $(x,\ y)$ não é elemento de R.

Exemplo 2.2 *Usando o exemplo* 2. *de* **??**, *em que* $X = \{1,\ 2,\ 3,\ 4\}$ *e* $R = \{(x,\ y) \in X^2 : x + y \leq 5\}$, *temos que*

$$4R1, \quad 3\not{R}4, \quad (1,\ 1) \in R, \quad (2,\ 4) \notin R.$$

Vejamos alguns modos de **representar uma relação**:
Seja $X = \{x_1, \ldots, x_n\}$ um conjunto e R uma relação binária sobre X.

(i) Através de **matriz de adjacências**:

A matriz de adjacências de R é a matriz $A = [a_{ij}]_{n\times n} \in \mathcal{M}_{n\times n}(\{0,\ 1\})$ definida por

$$a_{ij} = \begin{cases} 1 & \text{se } (x_i,\ x_j) \in R \\ 0 & \text{se } (x_i,\ x_j) \notin R \end{cases}$$

Note-se a importância da indexação ("marcação") dos elementos de X, para a construção da matriz A.

(ii) Através de **diagrama**:

Os elementos de X são pontos do diagrama e dois pontos deste diagrama $x_i,\ x_j$ estão unidos por uma seta de x_i para x_j se o par $(x_i,\ x_j) \in R$. Esquematicamente teremos, se $(x_i,\ x_j) \in R$

$x_i \longrightarrow x_j$ se $x_i \neq x_j$

se $x_i = x_j$

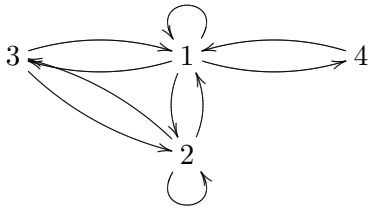
Exemplo 2.3 *Usando o exemplo* 2. *de* **??**, *em que* $X = \{1,\ 2,\ 3,\ 4\}$ *e* $R = \{(x,\ y) \in X^2 : x + y \leq 5\}$, *vimos que*

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

A matriz de adjacências de R *é*

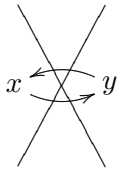
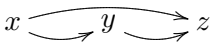
$$A = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

e o diagrama de R *é*



2.2 Classificação das relações binárias

Sejam X um conjunto e R uma relação binária sobre X. Dizemos que R é uma relação:

1. **reflexiva** se xRx, para qualquer $x \in X$; 
2. **simétrica** se xRy implica yRx, para quaisquer $x,\ y \in X$; 
3. **anti-simétrica** se xRy e yRx implica $x = y$, para quaisquer $x,\ y \in X$; 
4. **transitiva** se xRy e yRz implica xRz, para quaisquer $x,\ y,\ z \in X$. 

Exercício Sejam R uma relação binária sobre um conjunto $X = \{x_1,\ x_2, \ldots,\ x_n\}$ e $A \in \mathcal{M}_{n\times n}(\{0,\ 1\})$ a matriz de adjacências de R. A que propriedades sobre a matriz A correspondem as propriedades definidas, para R, anteriormente?

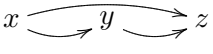
Exemplo 2.4 *Usando o exemplo* 2. *de* **??**, *temos que*
R *não é reflexiva pois* $(3,\ 3) \notin R$.
R *é simétrica pois* $(1,\ 2) \in R$ *e* $(2,\ 1) \in R$
$(1,\ 3) \in R$ *e* $(3,\ 1) \in R$
$(1,\ 4) \in R$ *e* $(4,\ 1) \in R$
$(2,\ 3) \in R$ *e* $(3,\ 2) \in R$
logo, não é anti-simétrica.
R *é transitiva.*

2.3 Relações de equivalência

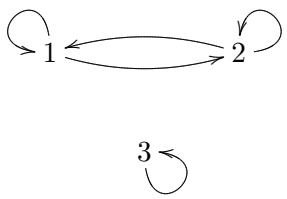
Sejam X um conjunto e R uma relação binária sobre X. R diz-se uma **relação de equivalência** se for:

. **reflexiva**; 

. **simétrica**; 

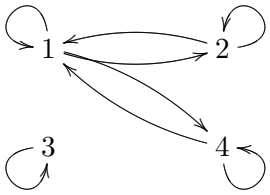
. **transitiva**. 

Exemplo 2.5 1. *Sejam* $X = \{1,\ 2,\ 3\}$ *e* $R = \{(1,\ 1),\ (1,\ 2),\ (2,\ 2),\ (2,\ 1),\ (3,\ 3)\}$



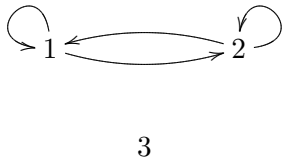
R é relação de equivalência sobre X.

2. $X = \{1,\ 2,\ 3,\ 4\}$ *e* $R = \{(1,\ 1),\ (2,\ 2),\ (3,\ 3),\ (4,\ 4),\ (1,\ 2),\ (2,\ 1),\ (1,\ 4),\ (4,\ 1)\}$



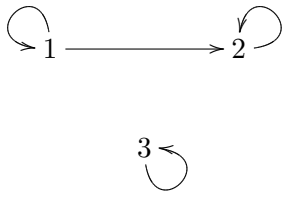
A relação R é reflexiva, simétrica e não transitiva.

3. $X = \{1,\ 2,\ 3\}$ *e* $R = \{(1,\ 1),\ (2,\ 2),\ (1,\ 2),\ (2,\ 1)\}$



R é não reflexiva, simétrica e transitiva.

4. $X = \{1,\ 2,\ 3\}$ *e* $R = \{(1,\ 1),\ (2,\ 2),\ (3,\ 3),\ (1,\ 2)\}$



R é reflexiva, não simétrica e transitiva.

5. *Sejam X um conjunto e* $\Delta = \{(x,\ x) :\ x \in X\}$. Δ *é uma relação de equivalência sobre X denominada relação identidade sobre X.*

6. *Sejam X um conjunto e $\Omega = \{(x,\ y) :\ x,\ y \in X\}$. Ω é uma relação de equivalência sobre X denominada relação universal sobre X.*

7. *Consideremos o conjunto dos números inteiros $\mathbb{Z}$, $n \in \mathbb{N}$ (fixado) e a relação R definida por:*

$$aRb \qquad \text{se, e só se, existe} \quad k \in \mathbb{Z} \text{ tal que } a - b = kn.$$

Então R é uma relação de equivalência sobre $\mathbb{Z}$. Com efeito:

I) Porque $a - a = 0 = 0 \times n$, então aRa, para qualquer $a \in \mathbb{Z}$. Assim, R é reflexiva.

II) Sejam $a,\ b \in \mathbb{Z}$ tais que aRb. Então, existe $k \in \mathbb{Z}$ tal que $a - b = kn$. Mas então,

$$b - a = (-k)n.$$

Como $(-k) \in \mathbb{Z}$, então bRa e R é simétrica.

III) Sejam $a,\ b,\ c \in \mathbb{Z}$ tais que $aRb,\ bRc$. Então, existem $k_1 \in \mathbb{Z},\ k_2 \in \mathbb{Z}$ tais que

$$a - b = k_1 n \qquad e \qquad b - c = k_2 n.$$

Consequentemente,

$$(a - b) + (b - c) = k_1 n + k_2 n.$$

Donde,

$$a - c = (k_1 + k_2)n.$$

Como $k_1 + k_2 \in \mathbb{Z}$, então aRc e R é transitiva.

Esta relação de equivalência sobre $\mathbb{Z}$ é habitualmente designada por relação de congruência módulo n. Se aRb dizemos que a é congruente com b módulo n e denotamos por $a \equiv b (mod\ n)$.

2.4 Classes de equivalência

Sejam X um conjunto e R uma relação de equivalência sobre X. Seja $a \in X$. Ao conjunto dos elementos de X que estão relacionados por R com a, que representamos por $[a]_R$ (ou simplesmente por $[a]$, se não houver ambiguidade), isto é, a

$$[a]_R = \{x \in X :\ xRa\},$$

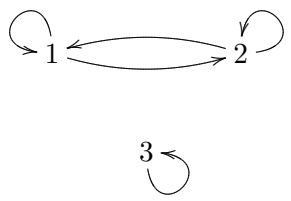
chamamos **classe de equivalência de** a (módulo R) ou classe de equivalência de R determinada por a.

Ao conjunto

$$X/R = \{[a]_R :\ a \in X\}$$

das classes de equivalência de R chamamos **conjunto quociente** de X por R.

Exemplo 2.6 1. *Consideremos a relação de equivalência R sobre $X = \{1,\ 2,\ 3\}$ do exemplo* 1. *de* **??***:*



Então, $[1]_R = \{1,\ 2\} = [2]_R$,

$[3]_R = \{3\}$.

Donde, $X/R = \{\{1,\ 2\},\ \{3\}\}$.

2. *Consideremos a relação de congruência módulo n, com n um inteiro fixado, sobre $\mathbb{Z}$, (exemplo* 7. *de* **??***) isto é, a relação definida por*

$$a \equiv b(mod\ n) \quad \Longleftrightarrow \quad (\exists k \in \mathbb{Z}) \qquad a - b = kn,$$

para quaisquer $a,\ b \in \mathbb{Z}$.

Para cada $a \in \mathbb{Z}$, denotamos por $a + n\mathbb{Z}$ o conjunto

$$a + n\mathbb{Z} = \{a + kn :\ k \in \mathbb{Z}\}.$$

É fácil ver que, dados $a,\ b \in \mathbb{Z}$

$$a \equiv b(mod\ n) \quad \Longleftrightarrow \quad b \in a + n\mathbb{Z},$$

pelo que

$$[a] = a + n\mathbb{Z} = \{\ldots, -2n + a,\ -n + a,\ a,\ n + a,\ 2n + a, \ldots\}.$$

Pode também ser demonstrado que

$$\mathbb{Z}/\equiv = \{[0],\ [1], \ldots,\ [n-1]\}.$$

Exercício

1. Mostre que a relação $\sim$ definida em $\mathbb{Z}$ por

$$m \sim n \quad \Longleftrightarrow \quad |m| = |n|,$$

para quaisquer $m,\ n \in \mathbb{Z}$, é uma relação de equivalência sobre $\mathbb{Z}$. Verifique que

$$[m]_\sim = \{-m,\ m\}, \qquad \text{para qualquer } m \in \mathbb{Z}.$$

2. Seja $x \in \mathbb{R}$. Denotemos por $\lfloor x \rfloor$ o maior inteiro menor ou igual a x. Por vezes este número é denotado por $[\![x]\!]$ (exemplos: $\lfloor 0.5 \rfloor = 0,\ \lfloor -1.2 \rfloor = -2,\ \lfloor \sqrt{2} \rfloor = 1$).

   No conjunto $\mathbb{R}$ defina-se a relação R da seguinte forma:

$$xRy \iff \lfloor x \rfloor = \lfloor y \rfloor,$$

   para quaisquer $x,\ y \in \mathbb{R}$.

   Prove que R é uma relação de equivalência sobre $\mathbb{R}$ tal que $[x] = [n,\ n+1[$ (intervalo real) com $n = \lfloor x \rfloor$, para qualquer $x \in \mathbb{R}$.

Proposição 2.7 *Sejam X um conjunto e R uma relação de equivalência sobre X. Para quaisquer $a,\ b \in X$, as seguintes afirmações são equivalentes:*

(1) *bRa;*

(2) *$b \in [a]_R$;*

(3) *$[b]_R = [a]_R$.*

Demonstração

(1) $\Rightarrow$ (2) Imediata por definição.

(2) $\Rightarrow$ (3) Admitamos que $b \in [a]_R$. Então, bRa. Tomemos $x \in [b]_R$. Então xRb. Como R é transitiva,

$$xRb,\ bRa \Rightarrow xRa,$$

donde $x \in [a]_R$. Reciprocamente, tomemos $x \in [a]_R$. Então xRa. Como bRa e R é simétrica, aRb. Usando a transitividade de R,

$$xRa,\ aRb \Rightarrow xRb,$$

temos que $x \in [b]_R$. Provámos assim que

$$x \in [a]_R \Leftrightarrow x \in [b]_R,$$

ou seja, $[a]_R = [b]_R$.

(3) $\Rightarrow$ (1) Como bRb então $b \in [b]_R = [a]_R$, pelo que $b \in [a]_R$, ou seja bRa. □

Teorema 2.8 *Sejam X um conjunto e R uma relação de equivalência sobre X. Temos:*

(1) *Para qualquer $x \in X$, $[x]_R \neq \emptyset$;*

(2) *Para quaisquer $x,\ y \in X$, $[x]_R = [y]_R$ ou $[x]_R \cap [y]_R = \emptyset$;*

(3) *$X = \bigcup_{x \in X} [x]_R$;*

(4) *A relação R fica determinada pelas suas classes de equivalência, isto é, se R' é uma relação de equivalência sobre X e $X/R = X/R'$, então $R = R'$.*

Demonstração

(1) Porque $xRx \Rightarrow x \in [x]_R \Rightarrow [x]_R \neq \emptyset$.

(2) Sejam $x,\ y \in X$ e suponhamos que $[x]_R \neq [y]_R$.

Se $[x]_R \cap [y]_R \neq \emptyset$, existia $a \in [x]_R \cap [y]_R$. Então, $a \in [x]_R$ e $a \in [y]_R$. Usando a Proposição anterior, teríamos $[x]_R = [a]_R = [y]_R$, contra a hipótese. Logo, $[x]_R \cap [y]_R = \emptyset$.

(3) Imediato tendo em conta que $x \in [x]_R \subseteq X$, para qualquer $x \in X$.

(4) Seja R' outra relação de equivalência sobre X tal que $X/R = X/R'$. Seja $x \in X$. Por hipótese, $[x]_R = [y]_{R'}$, para certo $y \in X$. Como $x \in [x]_R$, então $x \in [y]_{R'}$, pelo que usando a Proposição anterior, $[x]_R = [y]_{R'} = [x]_{R'}$. Assim,

$$(x,\ y) \in R \Leftrightarrow y \in [x]_R \Leftrightarrow y \in [x]_{R'} \Leftrightarrow (x,\ y) \in R',$$

para quaisquer $x,\ y \in X$, donde $R = R'$. □

Definição 2.9 *Seja X um conjunto. Um conjunto $\{X_i :\ i \in I\}$ de subconjuntos não vazios de X diz-se uma* **partição** *de X se:*

(1) $X = \bigcup_{i \in I} X_i$

(2) $i \neq j \Longrightarrow X_i \cap X_j = \emptyset$, *para quaisquer* $i,\ j \in I$.

Exemplo 2.10 1. *Seja X um conjunto. Se $A \in \mathcal{P}(X)$ é tal que $\emptyset \subset A \subset X$, então $\{A,\ \overline{A}\}$ é uma partição de X.*

2. *Seja $X = \{1,\ 2,\ 3,\ 4\}$. Então,*

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

são partições de X. Mas,

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

não são partições de X.

Exercício Determine todas as partições de $X = \{1,\ 2,\ 3,\ 4\}$.

Teorema 2.11 *Seja X um conjunto.*

1. *Se R é uma relação de equivalência sobre X, então X/R é uma partição de X.*

2. *Se* $\mathcal{P} = \{X_i : i \in I\}$ *é uma partição de* X *e* R *é a relação definida por:*

$$xRy \iff (\exists i \in I) \qquad x,\ y \in X_i,$$

para quaisquer $x,\ y \in X$*, então:*

(i) R *é relação de equivalência sobre* X

(ii) $\mathcal{P} = X/R$.

Demonstração

1. Tendo em atenção o Teorema anterior, é imediato que se R é uma relação de equivalência sobre X, então X/R é uma partição de X.

2. Seja $\mathcal{P} = \{X_i : i \in I\}$ uma partição de X e R a relação definida por:

$$xRy \iff (\exists i \in I) \qquad x,\ y \in X_i,$$

para quaisquer $x,\ y \in X$.

(i) Vejamos que R é uma relação de equivalência sobre X.
I) Seja $x \in X$. Como $X = \bigcup_{i \in I} X_i$, então existe $i \in I$ tal que $x \in X_i$, donde xRx. Portanto, R é reflexiva.
II) A simetria é imediata.
III) Sejam $x,\ y,\ z \in X$ tais que $xRy,\ yRz$. Então, existem $i \in I$ e $j \in I$ tais que $x,\ y \in X_i$ e $y,\ z \in X_j$. Como $y \in X_i \cap X_j$, então $X_i \cap X_j \neq \emptyset$, pelo que $i = j$. Então $x,\ z \in X_i$ e consequentemente xRz. Portanto, R é transitiva.
Logo, R é relação de equivalência.

(ii) Vejamos que $\mathcal{P} = X/R$:
Seja $[x]_R \in X/R$. Como $x \in X$, então existe $i \in I$ tal que $x \in X_i$.
Mostremos que $[x]_R = X_i$.
Se $y \in [x]_R$, então xRy. Como $\{X_j : j \in I\}$ é uma partição de X e $x \in X_i$, então $y \in X_i$. Logo, $[x]_R \subseteq X_i$.
Reciprocamente, se $z \in X_i$, então zRx e consequentemente, $z \in [x]_R$. Portanto, $[x]_R = X_i$ e $[x]_R \in \mathcal{P}$. Donde, $X/R \subseteq \mathcal{P}$.
Vejamos que $\mathcal{P} \subseteq X/R$.
Seja $X_i \in \mathcal{P}$. Porque $X_i \neq \emptyset$, seja $x \in X_i$. Como já vimos, $[x]_R = X_i$, donde $X_i \in X/R$.
Logo, $\mathcal{P} \subseteq X/R$ e consequentemente, $\mathcal{P} = X/R$. □

Exemplo 2.12 *Sendo* $X = \{1,\ 2,\ 3,\ 4,\ 5\}$ *e* $\mathcal{P} = \{\{1,\ 2\},\ \{3,\ 5\},\ \{4\}\}$ *uma partição de* X*, então* $\mathcal{P}$ *determina a relação de equivalência*

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

sobre X.

2.5 Relações de ordem parcial e relações de ordem total

Sejam X um conjunto e R uma relação binária sobre X. R diz-se uma **relação de ordem parcial** em X (r.o.p.) se for:

. **reflexiva**;

. **anti-simétrica**;

. **transitiva**.

As relações de ordem parcial são usualmente denotadas pelo símbolo $\leq$.

Seja $\leq$ uma r.o.p. sobre X. Dados $x,\ y \in X$ dizemos que x e y são **comparáveis** se $x \leq y$ ou $y \leq x$.

Uma r.o.p. sobre um conjunto X diz-se uma **relação de ordem total** (ou uma ordem linear) em X se, para quaisquer $x,\ y \in X$, x e y são comparáveis.

Sejam $\leq$ uma r.o.p. sobre X e x e $y \in X$. Usamos a notação $x < y$ para significar $x \leq y$ e $x \neq y$.

Definição 2.13 *Sejam X um conjunto e $\leq$ uma r.o.p. em X. Dizemos que o par $(X,\ \leq)$ é um* **conjunto parcialmente ordenado** *(c.p.o.).*
Se $\leq$ for uma ordem linear, dizemos que $(X,\ \leq)$ é um **conjunto totalmente ordenado** *(ou uma cadeia).*

Exemplo 2.14 1. *Seja $\leq$ a relação de ordem usual em $\mathbb{R}$. Então $(\mathbb{R},\ \leq)$ é uma cadeia. Também $(\mathbb{N},\ \leq)$, $(\mathbb{Z},\ \leq)$, $(\mathbb{Q},\ \leq)$ são cadeias (para a ordem usual).*

2. *Seja X um conjunto. A relação $\leq$ definida em $\mathcal{P}(X)$ por:*

$$A \leq B \iff A \subseteq B$$

é uma relação de ordem parcial em $\mathcal{P}(X)$, pelo que $(\mathcal{P}(X),\ \subseteq)$ é um c.p.o..

Exercício *Mostre que $(\mathcal{P}(X),\ \subseteq)$ é uma cadeia se, e só se, $X = \emptyset$ ou X é singular (isto é, $X = \{x\}$).*

3. *Em $\mathbb{N}$ definimos a seguinte relação binária (relação de divisibilidade)*

$$a|b \text{ (a divide b)} \iff (\exists c \in \mathbb{N}) \quad ac = b,$$

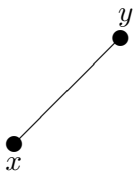
para quaisquer $a,\ b \in \mathbb{N}$. Então, $(\mathbb{N},\ |)$ é um c.p.o..

Definição 2.15 *Seja* $(X,\ \leq)$ *um c.p.o.. Dados* $x,\ y \in X$ *dizemos que* y **cobre** x *(relativamente a* $\leq$*) se* $x \leq y$ *e não existe* $z \in X$ *tal que* $x < z < y$.

2.6 Diagrama de Hasse

Sejam $X = \{x_1,\ x_2, \ldots,\ x_n\}$ e $\leq$ uma r.o.p. em X. $\leq$ pode ser representada através de um diagrama (denominado **diagrama de Hasse**) construído do seguinte modo:

Os elementos de X são pontos do diagrama e para quaisquer $x,\ y \in X$, se y cobre x, colocamos o ponto que representa y "acima"do ponto que representa x e unimo-los com um segmento de recta:



Exemplo 2.16 1. *Consideremos* $(\{1,\ 2,\ 3,\ 4\},\ \leq)$*, em que* $\leq$ *é a ordem usual em* $\mathbb{N}$. *Esta cadeia tem o seguinte diagrama de Hasse*

2. *O c.p.o.* $(\{1,\ 2, \ldots,\ 10\},\ |)$*, em que* $|$ *é relação de divisibilidade, tem a relação*

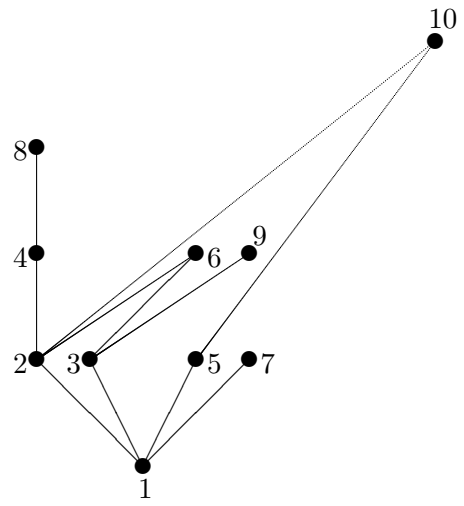
$$\leq = | = \{(1,\ 1),\ (1,\ 2),\ (1,\ 3),\ (1,\ 4),\ (1,\ 5),\ (1,\ 6),\ (1,\ 7),\ (1,\ 8),\ (1,\ 9),\ (1,\ 10),$$
$$(2,\ 2),\ (2,\ 4),\ (2,\ 6),\ (2,\ 8),\ (2,\ 10),\ (3,\ 3),\ (3,\ 6),\ (3,\ 9),\ (4,\ 4),\ (4,\ 8),$$
$$(5,\ 5),\ (5,\ 10),\ (6,\ 6),\ (7,\ 7),\ (8,\ 8),\ (9,\ 9),\ (10,\ 10)\}.$$

Na relação $|$ *retiramos os pares ordenados do tipo* $(x,\ x)$ *e do tipo* $(a,\ b)$ *com* $a \neq b$ *e para os quais existe* c *tal que* $a \neq c$, $b \neq c$ *e* $(a,\ c)$, $(c,\ b)$ *são pares de* $|$. *Assim sendo,*

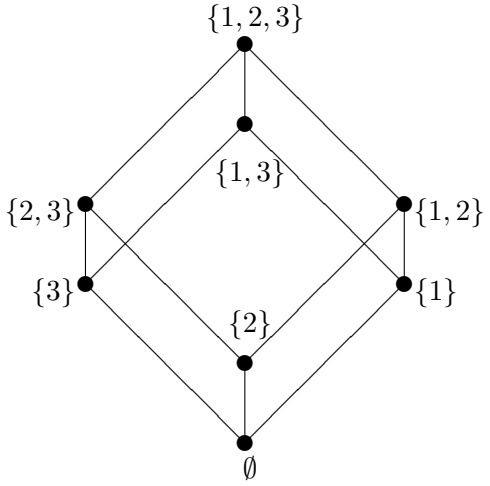
ficamos com os pares ordenados

$(1,\ 2),\ (1,\ 3),\ (1,\ 5),\ (1,\ 7),\ (2,\ 4),\ (2,\ 6),\ (2,\ 10),\ (3,\ 6),\ (3,\ 9),\ (4,\ 8),\ (5,\ 10)$

pelo que o diagrama de Hasse é



3. *O c.p.o.* $(\mathcal{P}(\{1,\ 2,\ 3\}),\ \subseteq)$ *possuí o seguinte diagrama de Hasse:*



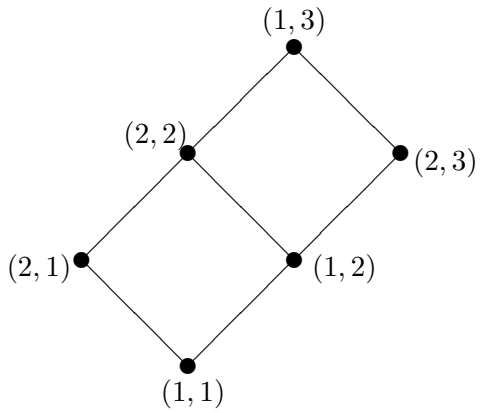
4. **Exercício** *Sejam* $(X_1,\ \leq_1)$ *e* $(X_2,\ \leq_2)$ *dois c.p.o.'s. Define-se em* $X_1 \times X_2$ *a relação binária* $\leq$ *por*

$$(x_1,\ x_2) \leq (y_1,\ y_2) \quad \Longleftrightarrow \quad x_1 \leq_1 y_1, \quad x_2 \leq_2 y_2$$

para quaisquer $x_1,\ y_1 \in X_1,\ x_2,\ y_2 \in X_2$.

Prove que $(X_1 \times X_2,\ \leq)$ *é um c.p.o..*

Nas condições do exercício anterior, se $X_1 = \{1,\ 2\}$, $X_2 = \{1,\ 2,\ 3\}$ *e* $\leq_1, \leq_2$ *são as ordens usuais, então* $(X_1 \times X_2,\ \leq)$ *possuí o seguinte diagrama de Hasse:*



Definição 2.17 *Sejam* $(X,\ \leq)$ *um c.p.o. e* $Y \subseteq X$.

1. *Chamamos* **primeiro elemento** *de* Y *(ou mínimo de* Y*) a um elemento* $a \in Y$ *tal que*

$$a \leq y, \quad \text{para qualquer } y \in Y$$

(este elemento quando existe é único).

2. *Chamamos* **último elemento** *de* Y *(ou máximo de* Y*) a um elemento* $b \in Y$ *tal que*

$$y \leq b, \quad \text{para qualquer } y \in Y$$

(este elemento quando existe é único).

Exemplo 2.18 *Considerando o exemplo* 2. *de* **??** *em que o c.p.o. é* $(\{1,\ 2, \ldots,\ 10\},\ |)$, *então* 1 *é o primeiro elemento de* $X = \{1,\ 2, \ldots,\ 10\}$ *e* X *não tem último elemento.*

Se pensarmos em $Y = \{1,\ 2,\ 5,\ 10\}$ *então*

1 *é o primeiro elemento de* Y

e

10 *é o último elemento de* Y.

Definição 2.19 *Um c.p.o.* $(X,\ \leq)$ *diz-se um* **conjunto bem ordenado** *(e* $\leq$ *uma boa ordem) se qualquer subconjunto não vazio de* X *possuí primeiro elemento.*

Teorema 2.20 (Axioma da boa ordenação) *O par* $(\mathbb{N},\ \leq)$ *em que* $\leq$ *denota a ordem usual, é um conjunto bem ordenado.*

Capítulo 3

Princípio de Indução

3.1 Princípio de Indução

Suponhamos que nos pedem para demonstrarmos o resultado

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

para todo o natural n. Noutras palavras, queremos mostrar que a expressão do lado esquerdo da igualdade é igual à fórmula que surge do lado direito da igualdade. O que se faz é o seguinte:

Por substituição de n pelo natural 1, concluímos que o resultado é verdadeiro, pois $1 = \frac{1}{2}(1)(2)$. Em seguida, supomos o resultado verdadeiro para um determinado valor de n, por exemplo para $n = k$. Ou seja, supomos que

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

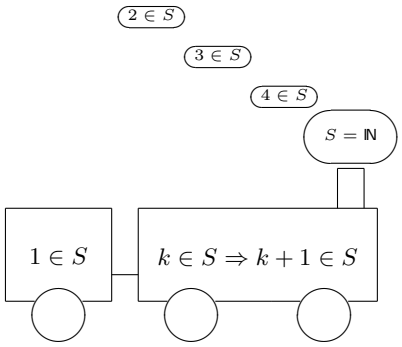
Usando este facto, podemos simplificar o lado esquerdo da igualdade quando $n = k + 1$, da seguinte forma:

$$\begin{aligned} 1 + 2 + 3 + \ldots + (k+1) &= 1 + 2 + 3 + \ldots + k + (k+1) \\ &= (\frac{1}{2}k(k+1)) + (k+1) \\ &= ((\frac{1}{2}k) + 1)(k+1) \\ &= \frac{1}{2}(k+1)(k+2). \end{aligned}$$

Portanto, se o resultado é verdadeiro para $n = k$, então também é verdadeiro para $n = k + 1$. Assim, porque o resultado é verdadeiro para $n = 1$, também é verdadeiro para $n = 2$. Usando o mesmo argumento, como é verdadeiro para $n = 2$, também o é para $n = 3$. Continuando este processo, podemos ver que o resultado é verdadeiro para todo o número natural n.

Esta técnica de demonstração é conhecida por "Princípio de Indução"e é utilizada em inúmeros casos. Em primeiro lugar veremos a formulação mais simples deste principio.

Seja S o subconjunto de $\mathbb{N}$ para o qual o resultado é verdadeiro (o nosso objectivo é mostrar que $S = \mathbb{N}$). Primeiro mostramos que $1 \in S$, e depois mostramos que se $k \in S$ então $k+1 \in S$. Através de "muita-terra pouca-terra"(figura) podemos concluir que $S = \mathbb{N}$.



Felizmente o "muita-terra pouca-terra"não é necessário, porque o principio de indução é uma consequência do Axioma da boa ordenação.

Muitas vezes, o resultado que pretendemos demonstrar não é quando o primeiro elemento é o 1, mas outro. Para estes casos o principio de indução terá de sofrer uma ligeira modificação.

Teorema 3.1 (**Princípio de Indução**) *Sejam* $m \in \mathbb{N}_0 = \mathbb{N} \cup \{0\}$, $\mathbb{N}_m = \{l \in \mathbb{N}_0 : l \geq m\}$ *e* S *um subconjunto de* $\mathbb{N}_m$ *tal que:*

(i) $m \in S$;

(ii) $k \in S \Rightarrow k + 1 \in S$, *para qualquer* $k \in \mathbb{N}_m$.

Então, $S = \mathbb{N}_m$.

Demonstração Com vista a um absurdo, admitamos que $S \neq \mathbb{N}_m$. Porque $S \subseteq \mathbb{N}_m$, então $A = \mathbb{N}_m \setminus S$ é um subconjunto não vazio de $\mathbb{N}_m$. Atendendo ao Axioma da boa ordenação, A possui um primeiro elemento t. Como $t \in \mathbb{N}_m$, então $t \geq m$. Mas por (i), $m \in S$ e como $t \notin S$, então $t > m$. Consequentemente, $t - 1 \geq m$, isto é, $t - 1 \in \mathbb{N}_m$. Porque t é o primeiro elemento de A, $t - 1 \notin A$, então $t - 1 \in S$. Assim, por (ii), $t = (t - 1) + 1 \in S$, o que é uma contradição. Portanto, $S = \mathbb{N}_m$. □

Na prática, a "demonstração por indução"é mais descritiva. O facto de o resultado ser verdadeiro para $n = m$, diz-se a **base da indução**, e a afirmação de que é verdadeiro para $n = k$ com $k \geq m$, diz-se a **hipótese de indução**. Quando estes termos são utilizados, não há necessidade de definir o conjunto S. Vejamos um exemplo.

Exemplo 3.2 *Vamos mostrar que*

$$2n + 1 \leq 2^n$$

para qualquer natural $n \geq 3$

Resolução

(Base da indução) O resultado é verdadeiro para $n = 3$ *porque* $6 + 1 = 7 \leq 8 = 2^3$.

(Hipótese de indução) Suponhamos o resultado verdadeiro para $n = k$, *com* $k \geq 3$, *ou seja,*

$$2k + 1 \leq 2^k.$$

Então,

$$\begin{aligned} 2(k+1)+1 &= (2k+1)+2 \\ &\leq 2^k + 2 \qquad \text{hipótese de indução} \\ &\leq 2^k + 2^k \\ &= 2^{k+1} \end{aligned}$$

Então o resultado é verdadeiro para $n = k+1$. *Usando o princípio de indução, podemos concluir que o resultado é verdadeiro para qualquer natural* $n \geq 3$.

Há certos resultados que para serem demonstrados, necessitam de uma hipótese de indução mais alargada. São os casos em que a hipótese de indução é alterada para "o resultado é verdadeiro para todo o $n \leq k$"em vez de "o resultado é verdadeiro para $n = k$". Esta nova hipótese de indução, dá origem ao segundo princípio de indução.

Teorema 3.3 (**Segundo princípio de Indução**) *Sejam* $m \in \mathbb{N}_0 = \mathbb{N} \cup \{0\}$, $\mathbb{N}_m = \{l \in \mathbb{N}_0 : \ l \geq m\}$ *e* S *um subconjunto de* $\mathbb{N}_m$ *tal que:*

(i) $m \in S$;

(ii) $(\forall t \in \{m, \ldots, k\},\ t \in S) \Rightarrow k + 1 \in S$, *para qualquer* $k \in \mathbb{N}_m$.

Então, $S = \mathbb{N}_m$.

Demonstração Consequência imediata do Teorema anterior. □

Exemplo 3.4 *Consideremos a sucessão* $(a_n)_{n\geq 0}$ *definida por*

$$\begin{cases} a_0 &= 1 \\ a_1 &= 2 \\ a_n &= 4a_{n-1} - 4a_{n-2} \end{cases}$$

Vamos mostrar, usando o segundo princípio de indução, que $a_n = 2^n$, *para qualquer* $n \in \mathbb{N}_0$. *Seja*

$$S = \{n \in \mathbb{N}_0 : \ a_n = 2^n\}.$$

Temos que:

(i) $a_0 = 1 = 2^0$. *Pelo que,* $0 \in S$.

(ii) *Seja* $k \in S$ *e admitamos que para todo o* t *tal que* $0 \leq t \leq k$, *se tem* $a_t = 2^t$ *(podemos supor que* $k \geq 1$, *porque para* $k = 1$ *temos* $a_1 = 2 = 2^1$, *ou seja,* $1 \in S$*). Queremos provar que* $k + 1 \in S$. *Como* $k \geq 1$, *então* $a_k = 2^k$ *e* $a_{k-1} = 2^{k-1}$. *Assim sendo,*

$$\begin{aligned} a_{k+1} &= 4a_k - 4a_{k-1} \\ &= 4.2^k - 4.2^{k-1} \\ &= 2^{k+2} - 2^{k+1} \\ &= 2^{k+1}(2-1) \\ &= 2^{k+1}. \end{aligned}$$

Pelo que $k + 1 \in S$. *Usando o segundo princípio de indução, temos que* $S = \mathbb{N}_0$.

Por último, vejamos uma aplicação do princípio de indução ao que temos vindo a estudar.

Teorema 3.5 *Seja* X *um conjunto com* n *elementos (*$n \in \mathbb{N}_0$*). Então,*

$$|\mathcal{P}(X)| = 2^n.$$

Demonstração Vamos fazer a demonstração por indução no número de elementos do conjunto X.

(Base da indução) O resultado é verdadeiro quando $|X| = 0$ porque se $|X| = 0$ então, $X = \emptyset$ e $\mathcal{P}(X) = \{\emptyset\}$. Assim sendo,

$$|\mathcal{P}(X)| = 1 = 2^0 = 2^{|X|}.$$

(Hipótese de indução) Suponhamos o resultado verdadeiro para qualquer conjunto X tal que $|X| = k$ e $k \geq 0$, ou seja,

$$|\mathcal{P}(X)| = 2^k.$$

Então, seja Y um conjunto com $k + 1$ elementos e seja $x \in Y$. Assim, porque

$$\mathcal{P}(Y) = \mathcal{P}(Y \setminus \{x\}) \cup \{Z \cup \{x\} : \ Z \in \mathcal{P}(Y \setminus \{x\})\},$$
$$\mathcal{P}(Y \setminus \{x\}) \cap \{Z \cup \{x\} : \ Z \in \mathcal{P}(Y \setminus \{x\})\} = \emptyset$$

e

$$|\mathcal{P}(Y \setminus \{x\})| = |\{Z \cup \{x\} : \ Z \in \mathcal{P}(Y \setminus \{x\})\}|,$$

podemos afirmar que

$$\begin{aligned} |\mathcal{P}(Y)| &= |\mathcal{P}(Y \setminus \{x\})| + |\{Z \cup \{x\} : \ Z \in \mathcal{P}(Y \setminus \{x\})\}| \\ &= 2^k + 2^k \qquad\qquad \text{hipótese de indução} \\ &= 2^{k+1} \end{aligned}$$

Donde, o resultado é verdadeiro para qualquer conjunto com $k + 1$ elementos. Usando o princípio de indução, podemos concluir que o resultado é verdadeiro para qualquer conjunto com n elementos. □

Capítulo 4

Aplicações

4.1 Definições e Exemplos

Sejam X e Y dois conjuntos. Uma **aplicação** (ou função) de X em Y é uma relação R de X em Y (isto é, $R \subseteq X \times Y$) tal que, para qualquer $x \in X$, existe um e um só $y \in Y$ tal que $(x, y) \in R$, simbolicamente

$$\forall x \in X \quad \exists^1 y \in Y : \ (x, y) \in R.$$

Habitualmente as aplicações são denotadas pelas letras $f,\ g,\ h, \ldots$.

Se f é uma aplicação de X em Y escrevemos

$$f : \ X \longrightarrow Y$$

e, para cada $x \in X$, denotamos por $\mathbf{f(x)}$ o único elemento de Y tal que $(x, y) \in f$. Este elemento é designado por imagem de x (por f).

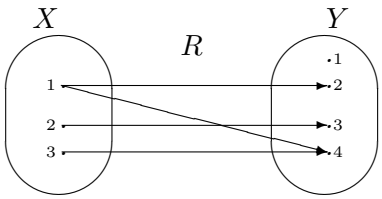
Dada uma aplicação $f : \ X \longrightarrow Y$ chamamos:

1. **conjunto de partida** (de f) a X;
2. **conjunto de chegada** (de f) a Y;
3. **imagem de f** (ou contradomínio de f) ao conjunto das imagens por f de todos os elementos $x \in X$:

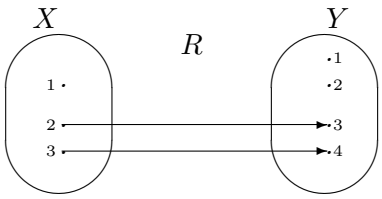
$$Im\ f = \{f(x) : \ x \in X\} = \{y \in Y : \ \exists x \in X,\ y = f(x)\}.$$

Exemplo 4.1 1. *Sejam* $X = \{1,\ 2,\ 3\}$ *e* $Y = \{1,\ 2,\ 3,\ 4\}$. *Então:*

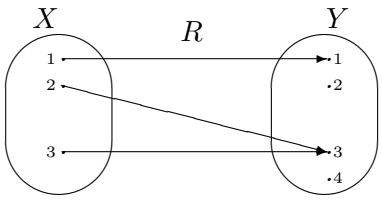
(a) $R = \{(1, 2),\ (2, 3),\ (3, 4),\ (1, 4)\}$ *é uma relação de* X *em* Y*, mas não é uma aplicação de* X *em* Y.



(b) $R = \{(2,3),\ (3,4)\}$ *é uma relação de* X *em* Y*, mas não é uma aplicação de* X *em* Y*.*

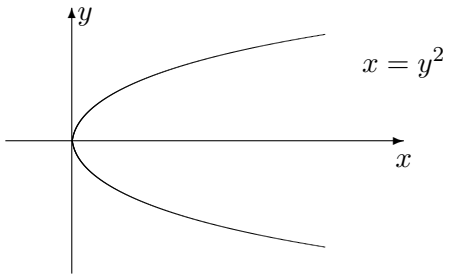


(c) $R = \{(1,1),\ (2,3),\ (3,3)\}$ *é uma aplicação de* X *em* Y*.*

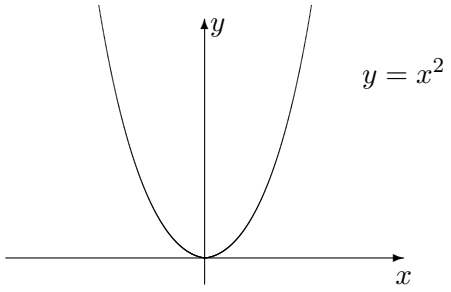


2. *Sejam* $X = Y = \mathbb{R}$*. Então:*

(a) $R = \{(x,y) \in \mathbb{R} \times \mathbb{R} :\ x = y^2\}$ *é uma relação de* $\mathbb{R}$ *em* $\mathbb{R}$*, mas não é uma aplicação de* $\mathbb{R}$ *em* $\mathbb{R}$*.*



(b) $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} : \ x^2 = y\}$ *é uma aplicação de* $\mathbb{R}$ *em* $\mathbb{R}$.



Definição 4.2 *Sejam* $f : \ X \longrightarrow Y$ *uma aplicação,* $A \subseteq X$ *e* $B \subseteq Y$*. Designa-se por:*

1. **imagem de A** *(por* f*) ao conjunto*

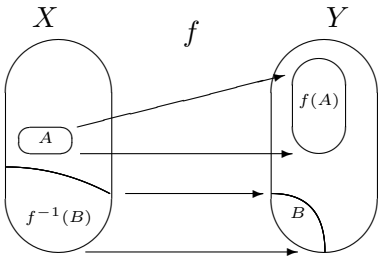
$$f(A) = \{f(x) : \ x \in A\};$$

2. **imagem recíproca** *(ou pré-imagem)* **de B** *(por* f*) ao conjunto*

$$f^{-1}(B) = \{x \in X : \ f(x) \in B\}.$$

O conjunto $f^{-1}(B)$ também é denotado por $f^{\leftarrow}(B)$ e o conjunto $f(A)$ por $f^{\rightarrow}(A)$.

Se $B = \{y\}$, denotamos também $f^{-1}(B)$ por $f^{-1}(y)$ ou $f^{\leftarrow}(y)$.

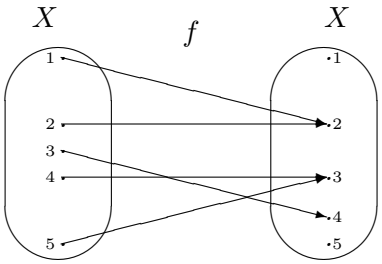


Observação Seja $X = \{x_1,\ x_2, \ldots,\ x_n\}$ um conjunto.

Então, uma aplicação $f:\ X \longrightarrow Y$ pode ser representada da seguinte forma:

$$f = \begin{pmatrix} x_1 & x_2 & \ldots & x_n \\ f(x_1) & f(x_2) & \ldots & f(x_n) \end{pmatrix}.$$

Exemplo 4.3 *Sejam* $X = \{1,\ 2,\ 3,\ 4,\ 5\}$, $f:\ X \longrightarrow X$ *a aplicação* $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 2 & 4 & 3 & 3 \end{pmatrix}$, $A = \{1,\ 2,\ 3\}$ *e* $B = \{1,\ 2,\ 3\}$. *Então,*



1. $Im\ f = \{2,\ 3,\ 4\}$
2. $f(A) = \{2,\ 4\}$
3. $f^{-1}(B) = \{1,\ 2,\ 4,\ 5\}$.

   Observe-se que $f(f^{-1}(B)) = \{2,\ 3\} \subset B$.

4.2 Classificação de aplicações

Seja $f:\ X \longrightarrow Y$ uma aplicação. Dizemos que:

1. f é **injectiva** (ou uma injecção) se

$$\forall a,\ b \in X,\ f(a) = f(b) \Rightarrow a = b$$

   (equivalentemente, se

$$\forall a,\ b \in X,\ a \neq b \Rightarrow f(a) \neq f(b));$$

2. f é **sobrejectiva** (ou uma sobrejecção) se

$$f(X) = Y$$

   isto é, se

$$\forall y \in Y\ \exists x \in X:\ y = f(x);$$

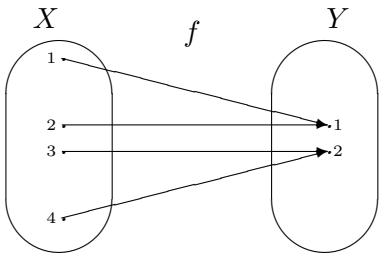
3. f é **bijectiva** (ou uma bijecção) se for simultaneamente injectiva e sobrejectiva, isto é, se

$$\forall y \in Y \ \exists^1 x \in X : \ y = f(x).$$

Exemplo 4.4 1. *A aplicação* $f : X \longrightarrow X$ *do exemplo anterior,* $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 2 & 4 & 3 & 3 \end{pmatrix}$, *não é injectiva nem sobrejectiva.*

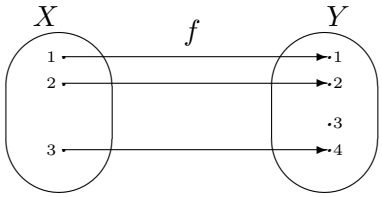
2. *A aplicação* $f : \mathbb{N} \longrightarrow \mathbb{N}$ *definida por* $f(n) = n + 1$ *para qualquer* $n \in \mathbb{N}$ *é injectiva e não é sobrejectiva.*

3. *Sejam* $X = \{1,\ 2,\ 3,\ 4\}$, $Y = \{1,\ 2\}$ *e* $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 1 & 2 & 2 \end{pmatrix}$ *uma aplicação de* X *em* Y.



f é sobrejectiva e não é injectiva.

4. *Sejam* $X = \{1,\ 2,\ 3\}$, $Y = \{1,\ 2,\ 3,\ 4\}$ *e* $f = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 4 \end{pmatrix}$ *uma aplicação de* X *em* Y.



f é injectiva e não é sobrejectiva.

5. *Seja* X *um conjunto qualquer e* $f : X \longrightarrow X$ *a aplicação definida por* $f(x) = x$, *para qualquer* $x \in X$. *Então,* f *é injectiva e sobrejectiva, donde* f *é bijectiva.*

   Esta aplicação designa-se por aplicação identidade de X *e denota-se por* 1_X *ou* id_X *ou* I_X.

Observação Sejam X e Y conjuntos e $f:\ X \longrightarrow Y$ uma aplicação. Afirmar que

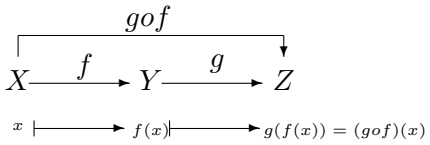
$$\forall x,\ y \in X,\ x = y \Rightarrow f(x) = f(y)$$

é o mesmo que dizer que f é uma **aplicação**. Não confundir com o conceito de injectividade!!!

4.3 Composição de aplicações

Sejam $f:\ X \longrightarrow Y$ e $g:\ Y \longrightarrow Z$ duas aplicações. A **aplicação composta** de g com f é a aplicação $gof:\ X \longrightarrow Z$ definida por

$$(gof)(x) = g(f(x)),\ \text{para qualquer } x \in X.$$



Observação Sejam $f:\ X \longrightarrow Y$ e $g:\ Y \longrightarrow Z$ duas aplicações.

1. A composta fog está definida se, e só se, $Z = X$;
2. Se $Z = X$ (as aplicações fog e gof estão definidas) não temos necessariamente $fog = gof$.

   Se $X \neq Y$, então $gof:\ X \longrightarrow X$ e $fog:\ Y \longrightarrow Y$ pelo que $fog \neq gof$.

   Mas mesmo quando $X = Y$, podemos ter $fog \neq gof$.

   Exemplo 4.5 *Sejam* $X = \{1,\ 2,\ 3\}$, $f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, $g = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ *duas aplicações de* X *em* X*. Então,*

$$fog = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = gof.$$

Proposição 4.6 *Sejam* $f:\ X \longrightarrow Y$, $g:\ Y \longrightarrow Z$ *e* $h:\ Z \longrightarrow W$ *três aplicações. Então estão definidas as aplicações* $(hog)of$ *e* $ho(gof)$ *de* X *em* W*, tendo-se*

$$(hog)of = ho(gof).$$

Demonstração Exercício. □

Teorema 4.7 *Sejam $f: X \longrightarrow Y$ e $g: Y \longrightarrow Z$ duas aplicações. Então:*

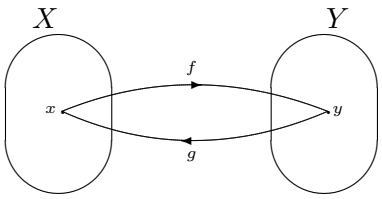
1. *Se f e g são injectivas, então gof é injectiva;*
2. *Se f e g são sobrejectivas, então gof é sobrejectiva;*
3. *Se f e g são bijectivas, então gof é bijectiva;.*

Demonstração

1. Suponhamos que f e g são injectivas. Sejam $x,\ y \in X$ tais que $(gof)(x) = (gof)(y)$. Então, $g(f(x)) = g(f(y))$. Como g é injectiva, então $f(x) = f(y)$. Como f é injectiva, então $x = y$. Logo, gof é injectiva.
2. Suponhamos que f e g são sobrejectivas. Seja $z \in Z$. Como g é sobrejectiva, então existe $y \in Y$ tal que $g(y) = z$. Como f é sobrejectiva, então existe $x \in X$ tal que $f(x) = y$. Logo,
$$z = g(y) = g(f(x)) = gof(x).$$
Portanto, gof é sobrejectiva.
3. Consequência imediata de 1. e 2. □

4.4 Aplicações invertíveis

Dizemos que uma aplicação $f: X \longrightarrow Y$ é **invertível** se existir uma aplicação $g: Y \longrightarrow X$ tal que
$$gof = id_X \qquad \text{e} \qquad fog = id_Y.$$



Proposição 4.8 *Seja $f: X \longrightarrow Y$ uma aplicação invertível. Então, existe uma e uma só aplicação $g: Y \longrightarrow X$ tal que*
$$gof = id_X \qquad e \qquad fog = id_Y.$$

Demonstração A existência é garantida por definição. Suponhamos que $g: Y \longrightarrow X$ e $h: Y \longrightarrow X$ são duas aplicações tais que

$$gof = id_X = hof \qquad \text{e} \qquad fog = id_Y = foh.$$

Então, $g = goid_Y = go(foh) = (gof)oh = id_X oh = h$. □

Definição 4.9 *Seja $f: X \longrightarrow Y$ uma aplicação invertível. Designamos por* **aplicação inversa** *de f, e denotamo-la por f^{-1}, a única aplicação $f^{-1}: Y \longrightarrow X$ tal que*

$$f^{-1}of = id_X \qquad e \qquad fof^{-1} = id_Y.$$

Observação É evidente que, se $f: X \longrightarrow Y$ é uma aplicação invertível, então a sua inversa $f^{-1}: Y \longrightarrow X$ é também invertível, tendo-se $(f^{-1})^{-1} = f$.

Proposição 4.10 *Sejam $f: X \longrightarrow Y$ e $g: Y \longrightarrow Z$ duas aplicações invertíveis. Então, a aplicação $gof: X \longrightarrow Z$ é invertível, tendo-se*

$$(gof)^{-1} = f^{-1}og^{-1}.$$

Demonstração Porque $f^{-1}: Y \longrightarrow X$ e $g^{-1}: Z \longrightarrow Y$, então está definida a composição $f^{-1}og^{-1}$. A demonstração fica concluída se provarmos que

$$(f^{-1}og^{-1})o(gof) = id_X$$

e

$$(gof)o(f^{-1}og^{-1}) = id_Z.$$

Ora,

$$(f^{-1}og^{-1})o(gof) = f^{-1}o(g^{-1}og)of = f^{-1}oid_Y of = f^{-1}of = id_X,$$

e

$$(gof)o(f^{-1}og^{-1}) = go(fof^{-1})og^{-1} = goid_X og^{-1} = gog^{-1} = id_Z.$$

□

Teorema 4.11 *Uma aplicação $f: X \longrightarrow Y$ é invertível se, e só se, é bijectiva.*

Demonstração Suponhamos que f é invertível, isto é, existe $f^{-1}: Y \longrightarrow X$ tal que

$$f^{-1}of = id_X \qquad \text{e} \qquad fof^{-1} = id_Y.$$

Vejamos primeiro que f é sobrejectiva. Seja $y \in Y$. Porque $y = (fof^{-1})(y) = f(f^{-1}(y))$ e $f^{-1}(y) \in X$, podemos concluir que

$$\forall y \in Y \quad \exists\, x \in X: \; y = f(x),$$

ou seja, f é sobrejectiva.

Demonstremos agora que f é injectiva. Sejam $a,\ b \in X$ tais que $f(a) = f(b)$. Então,

$$a = (f^{-1}of)(a) = f^{-1}(f(a)) = f^{-1}(f(b)) = (f^{-1}of)(b) = b.$$

Donde,

$$\forall a,\ b \in X, \quad f(a) = f(b) \Rightarrow a = b,$$

isto é, f é injectiva. Logo, f é bijectiva.

Reciprocamente, admitamos que f é bijectiva. Então,

$$\forall y \in Y \quad \exists^1\ x_y \in X :\ y = f(x_y).$$

Definamos a aplicação $g :\ Y \longrightarrow X$ tal que $g(y) = x_y$, para qualquer $y \in Y$.

Ora, para $y \in Y$, $(fog)(y) = f(g(y)) = f(x_y) = y$, donde $fog = id_Y$. Por outro lado, para $x \in X$, temos

$$(gof)(x) = g(f(x)) = x_{f(x)} = x,$$

donde, $gof = id_X$. Logo, f é invertível. □

Capítulo 5

Algoritmo da Divisão

5.1 Algoritmo da Divisão

O algoritmo da divisão é mais uma consequência do Axioma da boa ordenação.

Teorema 5.1 (Algoritmo da divisão) *Sejam n, $m \in \mathbb{Z}$ tais que $m \neq 0$. Então, existem dois únicos inteiros q e r tais que*

$$n = mq + r, \text{ com } 0 \leq r < |m|.$$

Demonstração Demonstremos em 1^o lugar, o Teorema quando $m > 0$. Seja

$$S = \{n - mx : \ x \in \mathbb{Z}, \ n - mx \geq 0\} \subseteq \mathbb{N}_0.$$

É claro que $S \neq \emptyset$ (Se $n \geq 0$, então $n - m(0) \in S$. Se $n < 0$, então $n - mn = (-n)(m-1) \geq 0$, pelo que $n - mn \in S$). Pelo Axioma da boa ordenação (estendido a $\mathbb{N}_0$), S possuí primeiro elemento r. Seja $q \in \mathbb{Z}$ tal que $n - mq = r$ e, portanto, tal que

$$n = mq + r.$$

Ora, $r \geq 0$, visto que $r \in S$, donde, para provar a existência, falta apenas mostrar que $r < m$. Com vista a um absurdo, suponhamos que $r \geq m$. Então,

$$n - m(q+1) = n - mq - m = r - m \geq 0,$$

pelo que $n - m(q+1) \in S$. Mas, como $m > 0$, então

$$n - m(q+1) = n - mq - m < n - mq = r,$$

o que contraria a escolha de r como primeiro elemento de S. Logo, $n = mq + r$, com $0 \leq r < m$.

Vejamos agora a unicidade. Suponhamos que $q_1,\ q_2,\ r_1$ e r_2 são inteiros tais que

$$n = mq_1 + r_1, \text{ com } 0 \leq r_1 < |m|$$

e

$$n = mq_2 + r_2, \text{ com } 0 \leq r_2 < |m|.$$

Então, $mq_1 + r_1 = mq_2 + r_2$, ou seja,

$$m(q_1 - q_2) = r_2 - r_1.$$

mas como, $0 \leq r_1 < m$ e $0 \leq r_2 < m$, então $-m < r_2 - r_1 < m$, pelo que $r_2 - r_1 = 0$, visto $r_2 - r_1$ ser um múltiplo de m. Assim, $r_1 = r_2$ e, consequentemente, $q_1 = q_2$.

Se $m < 0$, então $-m > 0$, pelo que atendendo ao que foi demonstrado, existem dois inteiros, únicos q e r tais que

$$n = (-m)q + r \quad \text{com } 0 \leq r < -m.$$

Então, $n = m(-q) + r$ com $0 \leq r < |m|$ e o Teorema verifica-se. □

Nota: Com a notação do Teorema, os inteiros q e r designam-se **quociente** e **resto**, respectivamente, da divisão de n por m.

O algoritmo da divisão justifica a representação usual dos inteiros. Seja $t \geq 2$ um inteiro. Sendo x um inteiro positivo, através do algoritmo da divisão temos:

$$x = tq_0 + r_0, \text{ com } 0 \leq r_0 < t$$

$$q_0 = tq_1 + r_1, \text{ com } 0 \leq r_1 < t$$

$$\vdots$$

$$q_{k-2} = tq_{k-1} + r_{k-1}, \text{ com } 0 \leq r_{k-1} < t$$

$$q_{k-1} = tq_k + r_k, \text{ com } 0 \leq r_k < t.$$

O processo termina quando $q_k = 0$. Eliminando os quocientes q_i, obtemos

$$x = r_k t^k + r_{k-1} t^{k-1} + \ldots + r_1 t + r_0.$$

Desta forma, x está representado (com respeito à base t) pela sequência dos restos e escreve-se, $x = (r_k r_{k-1} \ldots r_1 r_0)_t$. Convencionalmente $t = 10$ é a base dos cálculos e omitimos o valor 10, assim estamos familiarizados com a notação,

$$1456 = 1 \times 10^3 + 4 \times 10^2 + 5 \times 10 + 6.$$

A base $t = 2$ é muito utilizada nas calculadoras.

Exemplo 5.2 *Vamos escrever* 245 *na base* 2.
Dividindo sucessivamente por 2, *obtemos*

$$245 = 2 \times 122 + 1$$

$$122 = 2 \times 61 + 0$$

$$61 = 2 \times 30 + 1$$

$$30 = 2 \times 15 + 0$$

$$15 = 2 \times 7 + 1$$

$$7 = 2 \times 3 + 1$$

$$3 = 2 \times 1 + 1$$

$$1 = 2 \times 0 + 1.$$

Então,

$$(245)_{10} = (11110101)_2.$$

5.2 Máximo divisor comum

Uma das aplicações do algoritmo da divisão é o algoritmo de Euclides.

Sejam $a,\ b \in \mathbb{Z}$. Escrevemos $a|b$ para denotar que a divide b, isto é, existe $c \in \mathbb{Z}$ tal que $ac = b$.

Se $a|b$ também se diz que a é um divisor de b, ou ainda que b é um múltiplo de a.

Observação : A relação $|$ é uma relação de ordem parcial em $\mathbb{N}$, isto é, $(\mathbb{N},\ |)$ é um c.p.o., mas não o é em $\mathbb{Z}$, pois $1 \neq -1$ e $1|-1$ e $-1|1$ (não é anti-simétrica).

Teorema 5.3 *Dados dois inteiros não nulos* a *e* b, *existe um único número natural* d *(designado máximo divisor comum de* a *e* b*) tal que:*

(i) $d|a$ *e* $d|b$;

(ii) *se* $c \in \mathbb{Z}$ *é tal que* $c|a$ *e* $c|b$ *então* $c|d$.

Demonstração Algoritmo de Euclides
Porque $b \neq 0$, pelo algoritmo da divisão, existem inteiros $q_1,\ r_1$ tais que

$$a = bq_1 + r_1, \text{ com } 0 \leq r_1 < |b|.$$

Se $r_1 = 0$, então $d = b$ verifica as condições (i) e (ii) do Teorema.

Se $r_1 > 0$, aplicando novamente o algoritmo da divisão, encontramos inteiros $q_2,\ r_2$ tais que

$$b = r_1 q_2 + r_2, \text{ com } 0 \leq r_2 < r_1.$$

Se $r_2 = 0$, então $d = r_1$ verifica as condições (i) e (ii) do Teorema. Com efeito, temos que $r_1|b$ e $a = bq_1 + r_1 = r_1 q_2 q_1 + r_1 = r_1(q_2 q_1 + 1)$, pelo que também $r_1|a$. Por outro lado, seja $c \in \mathbb{Z}$ tal que $c|a$ e $c|b$. Sejam $a',\ b' \in \mathbb{Z}$ tais que $a = ca'$ e $b = cb'$. Então,

$$r_1 = a - bq_1 = ca' - cb'q_1 = c(a' - b'q_1),$$

pelo que $c|r_1$.

Se $r_2 > 0$, aplicando uma vez mais o algoritmo da divisão, encontramos inteiros $q_3,\ r_3$ tais que

$$r_1 = r_2 q_3 + r_3, \text{ com } 0 \leq r_3 < r_2.$$

Assim, procedendo deste modo, podemos encontrar sucessivamente inteiros q_i e r_i tais que

$$r_{i-2} = r_{i-1} q_i + r_i, \text{ com } 0 \leq r_i < r_{i-1}$$

até ao primeiro $k \in \mathbb{N}_0$ tal que $r_{k+1} = 0$, isto é,

$$a = bq_1 + r_1, \text{ com } 0 < r_1 < |b|$$

$$b = r_1 q_2 + r_2, \text{ com } 0 < r_2 < r_1$$

$$r_1 = r_2 q_3 + r_3, \text{ com } 0 < r_3 < r_2$$

$$r_2 = r_3 q_4 + r_4, \text{ com } 0 < r_4 < r_3$$

$$\vdots$$

$$r_{k-2} = r_{k-1} q_k + r_k, \text{ com } 0 < r_k < r_{k-1}$$

$$r_{k-1} = r_k q_{k+1}, \text{ com } r_{k+1} = 0.$$

Nestas condições, $d = r_k$ verifica as condições (i) e (ii) do Teorema. Logo, a existência está demonstrada.

Vejamos a unicidade . Suponhamos que d e d' são dois naturais que verificam as condições (i) e (ii) do Teorema. Por (i), $d|a$ e $d|b$, pelo que, como d' verifica (i) e (ii), por (ii), $d|d'$. Por outro lado, por (i), $d'|a$ e $d'|b$, pelo que, como d verifica (i) e (ii), por (ii), $d'|d$. Mas se d e d' são naturais e $d|d'$ e $d'|d$, então $d = d'$. □

Notação Dados dois números inteiros não nulos a e b, denotamos por $mdc\{a,\ b\}$ o seu máximo divisor comum.

Exemplo 5.4 *Vamos calcular* $mdc\{32060,\ 31652\}$*, usando o algoritmo de Euclides:*

$$\begin{aligned} 32060 &= 31652 \times 1 + 408 \\ 31652 &= 408 \times 77 + 236 \\ 408 &= 236 \times 1 + 172 \\ 236 &= 172 \times 1 + 64 \\ 172 &= 64 \times 1 + 44 \\ 64 &= 44 \times 1 + 20 \\ 44 &= 20 \times 2 + 4 \\ 20 &= 4 \times 5 + 0. \end{aligned}$$

Assim, $mdc\{32060,\ 31652\} = 4$.

Teorema 5.5 (Igualdade de Bézout) *Dados dois números inteiros não nulos* a *e* b*, existem números inteiros* m *e* n *(designados* **coeficientes da igualdade de Bézout***) tais que*

$$mdc\{a,\ b\} = am + bn.$$

Demonstração Seja $d = mdc\{a,\ b\}$. pelo algoritmo de Euclides, temos

$$a = bq_1 + r_1, \text{ com } 0 < r_1 < |b|$$

$$b = r_1q_2 + r_2, \text{ com } 0 < r_2 < r_1$$

$$r_1 = r_2q_3 + r_3, \text{ com } 0 < r_3 < r_2$$

$$r_2 = r_3q_4 + r_4, \text{ com } 0 < r_4 < r_3$$

$$\vdots$$

$$r_{k-2} = r_{k-1}q_k + d, \text{ com } 0 < d = r_k < r_{k-1},$$

para certo $k \in \mathbb{N}_0$. Então,

$$d = r_{k-2} - r_{k-1}q_k \qquad (*)$$

e, mais geralmente, para $i \in \{1, \ldots, k\}$,

$$r_i = r_{i-2} - r_{i-1}q_i \qquad (**)$$

(tomando $r_0 = b,\ r_{-1} = a$). Assim, partindo de (*) e substituindo sucessivamente cada r_i usando (**), obtemos d como combinação linear de a e b. □

Exemplo 5.6 *Vamos calcular os coeficientes da igualdade de Bézout para os inteiros do exemplo anterior,* $4 = mdc\{32060,\ 31652\}$*:*

$$\begin{aligned}
4 &= 44 - 21 \times 2 \\
&= 44 - (64 - 44) \times 2 = 44 \times 3 - 64 \times 2 \\
&= (172 - 64 \times 2) \times 3 - 64 \times 2 = 172 \times 3 - 64 \times 5 \\
&= 172 \times 3 - (236 - 172) \times 5 = 172 \times 8 - 236 \times 5 \\
&= (408 - 236) \times 8 - 236 \times 5 = 408 \times 8 - 236 \times 13 \\
&= 408 \times 8 - (31652 - 408 \times 77) \times 13 = 408 \times 909 - 31652 \times 13 \\
&= (32060 - 31652) \times 909 - 31652 \times 13 \\
&= 32060 \times 909 - 31652 \times 912,
\end{aligned}$$

pelo que

$$4 = 32060 \times 909 + 31652 \times (-912).$$

5.3 Mínimo múltiplo comum

Depois do máximo divisor comum surge, naturalmente, o mínimo múltiplo comum. Este valor não é mais do que consequência do Axioma da boa ordenação e do Algoritmo da divisão.

Teorema 5.7 *Dados dois inteiros não nulos* a *e* b*, existe um único natural* m *(designado mínimo múltiplo comum de* a *e* b*) tal que:*

(i) $a|m$ *e* $b|m$*,*

(ii) *se* $c \in \mathbb{Z}$ *é tal que* $a|c$ *e* $b|c$ *então* $m|c$*.*

Demonstração Consideremos o conjunto

$$S = \{x \in \mathbb{N} :\ a|x \text{ e } b|x\}.$$

Ora $S \neq \emptyset$ (por exemplo $|ab| \in S$), pelo que, pelo Axioma da boa ordenação, S tem primeiro elemento m. Por definição, m satisfaz a condição (i) do Teorema. Vejamos que também satisfaz (ii). Seja $c \in \mathbb{Z}$ tal que $a|c$ e $b|c$. Pelo algoritmo da divisão, existem inteiros q e r tais que

$$c = mq + r, \quad \text{com } 0 \leq r < m.$$

Uma vez que $a|c$ e $a|m$, então $a|r$. Por razões análogas, $b|r$. Logo, se $r > 0$, teríamos $r \in S$ e $r < m$, o que contraria a escolha de m. Portanto, $r = 0$ e consequentemente $m|c$. A prova da unicidade é deixada como exercício. □

Notação Dados dois inteiros não nulos a e b, denotamos por $mmc\{a,\ b\}$ o seu mínimo múltiplo comum.

Proposição 5.8 *Dados dois inteiros não nulos a e b, então*

$$mmc\{a,\ b\} = \frac{|ab|}{mdc\{a,\ b\}}.$$

Demonstração Como $a|\frac{|ab|}{mdc\{a,\ b\}}$ ($\frac{|ab|}{mdc\{a,\ b\}} = |a|\frac{|b|}{mdc\{a,\ b\}}$) e $b|\frac{|ab|}{mdc\{a,\ b\}}$, verifica-se (i) do Teorema. Mas $mmc\{a,\ b\}$ verifica (ii) do Teorema, portanto

$$mmc\{a,\ b\}|\frac{|ab|}{mdc\{a,\ b\}}.$$

Então existe $r \in \mathbb{Z}$ tal que

$$\frac{|ab|}{mdc\{a,\ b\}} = mmc\{a,\ b\}r.$$

Mas,

$$|a| = \frac{mmc\{a,\ b\}}{|b|}(mdc\{a,\ b\}r)$$

e

$$|b| = \frac{mmc\{a,\ b\}}{|a|}(mdc\{a,\ b\}r),$$

ou seja,

$$(mdc\{a,\ b\}r)|a \quad \text{e} \quad (mdc\{a,\ b\}r)|b.$$

Pelo Teorema **??**, $(mdc\{a,\ b\}r)|mdc\{a,\ b\}$. Donde, $r = 1$ e $mmc\{a,\ b\} = \frac{|ab|}{mdc\{a,\ b\}}$. □

Exemplo 5.9 *Vamos calcular $mmc\{32060,\ 31652\}$.*

Como $mdc\{32060,\ 31652\} = 4$, então $mmc\{32060,\ 31652\} = \frac{32060\times 31652}{4}$.

5.4 Teorema Fundamental da Aritmética

Um número inteiro p diz-se um número primo se, $p > 1$ e p apenas possuí como divisores positivos 1 e p.

Lema 5.10 *Sejam $a,\ b$ e $c \in \mathbb{Z}$ tais que $a,\ b \neq 0$, $a|bc$ e $mdc\{a,\ b\} = 1$. Então $a|c$.*

Demonstração Atendendo à igualdade de Bézout, existem inteiros m e n tais que

$$1 = am + bn.$$

Como $a|bc$, então $a|bnc$. Mas, $a|amc$, então $a|(amc + bnc)$, ou seja, $a|c$. □

Lema 5.11 *Seja p um número primo e sejam $a_1,\ a_2, \ldots,\ a_n \in \mathbb{Z}$ (com $n \in \mathbb{N}$) tais que $p|a_1a_2 \ldots a_n$. Então $p|a_i$, para algum $i \in \{1, \ldots, n\}$.*

Demonstração Por indução em n. Para $n = 1$ é imediato. Admitamos então o resultado para $n-1$, para certo $n > 1$. Sejam $a_1,\ a_2, \ldots,\ a_n \in \mathbb{Z}$ tais que $p|a_1a_2 \ldots a_n$.

Se $p|a_1a_2 \ldots a_{n-1}$, por hipótese de indução, $p|a_i$, para algum $i \in \{1, \ldots, n-1\}$.

Se $p \not| a_1a_2 \ldots a_{n-1}$, então como p é um número primo,

$$mdc\{p,\ a_1a_2 \ldots a_{n-1}\} = 1,$$

pelo Lema anterior, $p|a_n$. □

Teorema 5.12 (Teorema Fundamental da Aritmética) *Todo o número inteiro maior do que* 1 *pode ser escrito como um produto de números primos. Além disso, uma tal decomposição é única, isto é, duas decomposições apenas diferem na ordem pela qual os primos são escritos.*

Demonstração Seja S o conjunto dos números inteiros maiores do que 1, que não podem ser escritos como um produto de números primos. Provar a primeira parte do Teorema é o mesmo que provar que S é vazio. Admitamos que $S \neq \emptyset$. Então, pelo Axioma da boa ordenação, S tem um primeiro elemento n. Uma vez que S não possuí números primos, então n não é primo, donde $n = n_1n_2$, para certos $n_1,\ n_2 \in \mathbb{N}$ tais que $1 < n_1,\ n_2 < n$. atendendo ao facto de n ser o primeiro elemento de S, $n_1,\ n_2 \notin S$, donde n_1 e n_2 podem ser escritos como um produto de números primos e consequentemente, o mesmo acontece com n, o que é uma contradição. Portanto, $S = \emptyset$.

A unicidade da decomposição fica como exercício. (Sugestão: use o Lema anterior.) □

Observação Por reordenação dos factores de uma decomposição em números primos, um inteiro $n > 1$ pode ser escrito na forma

$$n = p_1^{r_1}p_2^{r_2} \ldots p_k^{r_k}, \quad \text{com } p_1 < p_2 < \ldots < p_k,$$

em que $p_1,\ p_2, \ldots,\ p_k$ são números primos e $k,\ r_1,\ \ldots,\ r_k \in \mathbb{N}$ (unicamente determinados por n). Uma decomposição deste tipo é designada por **forma standard** de n.

Exemplo 5.13 1. *Vejamos qual a forma standard de* 350.

$$\begin{array}{r|l} 350 & 2 \\ 175 & 5 \\ 35 & 5 \\ 7 & 7 \\ 1 & \end{array}$$

pelo que $350 = 2 \times 5^2 \times 7$.

2. *Vejamos que se* m *e* n *forem dois naturais maiores ou iguais a* 2, *então* $m^2 \neq 2n^2$.

   Atendendo ao Teorema fundamental da aritmética,

   $$m = 2^x h \quad e \quad n = 2^y g$$

   em que h *e* g *são produtos de números primos maiores que* 2 *e* $x,\ y \in \mathbb{N}_0$. *Então,*

   $$m^2 = 2^{2x} h^2 \quad e \quad 2n^2 = 2^{2y+1} g^2,$$

   ou seja, o 2 *em* m^2 *está elevado a uma potência par, enquanto que em* $2n^2$ *está elevado a uma potência ímpar. Portanto,* $m^2 \neq 2n^2$.

3. *Se* $n \geq 2$ *não é um número primo, então existe um número primo* p *tal que* $p|n$ *e* $p^2 \leq n$.

   Suponhamos que para todo o número primo p *tal que* $p|n$, $p^2 > n$. *Como* n *não é primo,*

   $$n = p_1 p_2 h,$$

   com $p_1,\ p_2$ *números primos. Então,*

   $$n^2 = p_1^2 p_2^2 h^2 > nn = n^2,$$

   o que é impossível. Então, existe um número primo p *tal que* $p|n$ *e* $p^2 \leq n$.

4. *Vejamos que* 79 *é um primo.*

   Se 79 *não fosse primo, pelo exemplo anterior, existiria um primo* p *tal que* $p|79$ *e* $p^2 \leq 79$. *Ora como* $9^2 = 81$, *então* $p \leq 7$. *Mas,* 79 *não é divisível por* 2, *nem por* 3, *nem por* 5, *nem por* 7. *Donde,* 79 *é primo.*

Capítulo 6

Inteiros módulo n

6.1 Álgebra em $\mathbb{Z}_n$

Uma das mais familiares partições de $\mathbb{Z}$ é em números pares e números ímpares. Esta partição corresponde à seguinte relação de equivalência R: dados $a,\ b \in \mathbb{Z}$,

$$aRb \quad \text{se, e só se,} \quad 2|(a-b).$$

A relação anterior, não é mais do que um caso particular das relações de equivalência que estudámos em 2.4. Seja $n \in \mathbb{N}$, em 2.4 definimos a relação R (relação de congruência módulo n) sobre o conjunto $\mathbb{Z}$, tal que, dados $a,\ b \in \mathbb{Z}$,

$$aRb \quad \text{se, e só se,} \quad n|(a-b).$$

Demonstrámos que R é uma relação de equivalência sobre $\mathbb{Z}$ e dissemos que, sendo $a,\ b \in \mathbb{Z}$ tais que aRb, diríamos que a é congruente com b módulo n e escreveríamos $a \equiv b(mod\ n)$. Vimos ainda, que se $a \in \mathbb{Z}$, a classe (de congruência) módulo n de a é o conjunto

$$[a]_n = \{\ldots,\ a-2n,\ a-n,\ a,\ a+n,\ a+2n,\ldots\}.$$

por exemplo, para $n = 4$, temos quatro classes distintas:
$[0]_4 = \{\ldots,\ -8,\ -4,\ 0,\ 4,\ 8,\ldots\}$,
$[1]_4 = \{\ldots,\ -7,\ -3,\ 1,\ 5,\ 9,\ldots\}$,
$[2]_4 = \{\ldots,\ -6,\ -2,\ 2,\ 6,\ 10,\ldots\}$,
$[3]_4 = \{\ldots,\ -5,\ -1,\ 3,\ 7,\ 11,\ldots\}$.

Definição 6.1 *O conjunto quociente $\mathbb{Z}/R$, em que R é a relação de congruência módulo n, é designado por conjunto dos números inteiros módulo n e denotado por $\mathbb{Z}_n$.*

Observação Dado $a \in \mathbb{Z}$, não havendo perigo de ambiguidade, denotaremos a classe módulo n de a, $[a]_n$, simplesmente por $[a]$.

Teorema 6.2 *Seja $n \in \mathbb{N}$. Então cada inteiro é congruente módulo n precisamente com um dos inteiros $0,\ 1,\ 2, \ldots,\ n-1$.*

Demonstração Seja $a \in \mathbb{Z}$. Pelo algoritmo da divisão existem q e $r \in \mathbb{Z}$ tais que $a = nq + r$ com $0 \leq r < n$. Então, $a - r = nq$, ou seja,

$$a \equiv r (mod\ n).$$

Assim, a é congruente módulo n a um dos inteiros $0,\ 1,\ 2, \ldots,\ n-1$.

Vejamos que este inteiro r é único. Suponhamos que $a \equiv s (mod\ n)$ com $0 \leq s < n$. Então, existe $t \in \mathbb{Z}$ tal que $a - s = nt$, isto é $a = nt + s$ com $0 \leq s < n$. Pela unicidade de r no algoritmo da divisão, $s = r$. □

Exemplo 6.3 *Seja $n = 13$. O inteiro -15 é congruente módulo 13 com 9, pois $-15 = 13 \times (-2) + 9$. Donde $[-15]_{13} = [9]_{13}$.*

O inteiro 25 é congruente módulo 13 com 12, pois $25 = 13 \times 1 + 12$.

Teorema 6.4 *O conjunto $\mathbb{Z}_n$ dos inteiros módulo n tem precisamente n elementos,*

$$\mathbb{Z}_n = \{[0],\ [1], \ldots,\ [n-1]\}.$$

Teorema 6.5 *Sejam $a,\ b,\ c,\ d \in \mathbb{Z}$ tais que*

$$a \equiv b (mod\ n) \quad e \quad c \equiv d (mod\ n).$$

Então,

$$a + c \equiv b + d (mod\ n) \quad e \quad ac \equiv bd (mod\ n).$$

Demonstração Exercício.

Este resultado permite-nos definir sem ambiguidade as operações $\oplus$ e $\otimes$ sobre $\mathbb{Z}_n$ seguintes:

Para quaisquer $a,\ b \in \mathbb{Z}$,

$$[a]_n \oplus [b]_n = [a + b]_n$$

$$[a]_n \otimes [b]_n = [ab]_n.$$

Teorema 6.6 *Sejam $x,\ y,\ z \in \mathbb{Z}_n$ e sejam $\overline{0} = [0]_n$ e $\overline{1} = [1]_n$. Então:*

1. $x \oplus y = y \oplus x$;

2. $(x \oplus y) \oplus z = x \oplus (y \oplus z)$;
3. $x \oplus \overline{0} = x$;
4. *Existe* $x' \in \mathbb{Z}_n$ *tal que* $x \oplus x' = x$;
5. $x \otimes y = y \otimes x$;
6. $(x \otimes y) \otimes z = x \otimes (y \otimes z)$;
7. $x \otimes \overline{1} = x$;
8. $x \otimes (y \oplus z) = (x \otimes y) \oplus (x \otimes z)$;

Demonstração Exercício.

6.2 Congruências Lineares

Chamamos **congruência linear** a uma expressão da forma

$$\mathbf{ax \equiv b (mod\ n)}$$

em que $n \in \mathbb{N}$, $a,\ b \in \mathbb{Z}$ (constantes) e x é uma variável inteira.

Uma **solução** da congruência linear

$$ax \equiv b (mod\ n)$$

é um inteiro α tal que $\mathbf{a\alpha \equiv b (mod\ n)}$.

Teorema 6.7 *Sejam* $a,\ b \in \mathbb{Z}$ *e* $n \in \mathbb{N}$. *Se* $\alpha \in \mathbb{Z}$ *é uma solução da congruência linear*

$$ax \equiv b (mod\ n),$$

então qualquer $\beta \in [\alpha]_n$ *é também uma solução.*

Demonstração Porque $a\alpha \equiv b (mod\ n)$ e $\beta \equiv \alpha (mod\ n)$, então existem $u,\ v \in \mathbb{Z}$ tais que

$$a\alpha - b = un \quad \text{e} \quad \beta - \alpha = vn.$$

Assim,

$$\begin{aligned} a\beta - b &= a(\alpha + vn) - (a\alpha - un) \\ &= a\alpha - avn - a\alpha + un \\ &= (av + u)n \end{aligned}$$

e portanto $a\beta \equiv b(mod\ n)$. □

Observação Seja $n \in \mathbb{N}$ e definamos

$$Z_n = \{0,\ 1, \ldots,\ n-1\}.$$

Uma vez que $\mathbb{Z}_n = \{[0]_n,\ [1]_n, \ldots,\ [n-1]_n\}$, o Teorema anterior diz-nos que uma congruência linear do tipo $ax \equiv b(mod\ n)$ fica completamente resolvida quando determinarmos as suas soluções em Z_n.

Exemplo 6.8 1. *Consideremos a congruência linear*

$$2x \equiv 1(mod\ 4).$$

Como, $2 \times 0 \equiv 0(mod\ 4)$, $2 \times 1 \equiv 2(mod\ 4)$,
$2 \times 2 \equiv 0(mod\ 4)$, $2 \times 3 \equiv 2(mod\ 4)$,

a congruência linear não possuí soluções em $Z_4 = \{0,\ 1,\ 2,\ 3\}$. *Portanto, não possuí quaisquer soluções (em* $\mathbb{Z}$*).*

2. *Determinemos as soluções da congruência linear*

$$2x \equiv 1(mod\ 5).$$

Como, $2 \times 0 \equiv 0(mod\ 5)$, $2 \times 1 \equiv 2(mod\ 5)$,
$2 \times 2 \equiv 4(mod\ 5)$, $2 \times 3 \equiv 1(mod\ 5)$,
$2 \times 4 \equiv 3(mod\ 5)$,

$x = 3$ *é a (única) solução da congruência linear em* $Z_5 = \{0,\ 1,\ 2,\ 3,\ 4\}$. *As soluções (em* $\mathbb{Z}$*) são pois todos os elementos do conjunto*

$$[3]_5 = \{\ldots,\ -12,\ -7,\ -2,\ 3,\ 8,\ 13, \ldots\}.$$

3. *Consideremos a congruência linear*

$$4x \equiv 4(mod\ 8)$$

e determinemos as suas soluções.

Como, $4 \times 0 \equiv 0(mod\ 8)$, $4 \times 1 \equiv 4(mod\ 8)$,
$4 \times 2 \equiv 0(mod\ 8)$, $4 \times 3 \equiv 4(mod\ 8)$,
$4 \times 4 \equiv 0(mod\ 8)$, $4 \times 5 \equiv 4(mod\ 8)$,
$4 \times 6 \equiv 0(mod\ 8)$, $4 \times 7 \equiv 4(mod\ 8)$,

1, 3, 5 *e* 7 *são soluções da congruência linear em* Z_8. *Assim, o conjunto de todas as soluções (em* $\mathbb{Z}$*) da congruência linear é*

$$[1]_8 \cup [3]_8 \cup [5]_8 \cup [7]_8.$$

Teorema 6.9 *Sejam* $a,\ b \in \mathbb{Z}$, $n \in \mathbb{N}$ *e* $d = mdc\{a,\ n\}$. *Então, a congruência linear*

$$ax \equiv b(mod\ n)$$

tem soluções se, e só se, $d|b$ *e, neste caso, possuí exactamente* d *soluções em* Z_n.

Demonstração $\Rightarrow$ Seja α uma solução da congruência linear. Então,

$$a\alpha \equiv b(mod\ n),$$

pelo que existe $r \in \mathbb{Z}$ tal que

$$a\alpha - b = rn.$$

Como $d|a$ e $d|n$, então $d|rn$, pelo que

$$d|(a\alpha - rn),$$

isto é, $d|b$.

$\Leftarrow$ Suponhamos que $d|b$. Seja $k \in \mathbb{Z}$ tal que $dk = b$. Atendendo à igualdade de Bézout, existem $u,\ v \in \mathbb{Z}$ tais que

$$d = au + nv.$$

Então,

$$b = kd = k(au + nv) = kau + knv,$$

donde

$$a(ku) - b = (-kv)n$$

e, portanto,

$$a(ku) \equiv b(mod\ n)$$

ou seja, ku é uma solução da congruência linear.

Admitamos que a congruência linear possuí pelo menos uma solução α. Vamos provar que o número de soluções em Z_n é precisamente d, ou seja, equivalentemente, que a congruência linear possuí exactamente d soluções em $\mathbb{Z}$ não congruentes módulo n duas a duas.

Sejam $m \in \mathbb{N}$ tal que $n = dm$ e

$$S = \{\alpha + lm :\ l \in \mathbb{Z}\}.$$

Comecemos por mostrar que S é o conjunto das soluções da congruência linear. Sejam $a',\ r,\ u,\ v \in \mathbb{Z}$ tais que

$$a\alpha - b = rn, \qquad a = a'd, \qquad d = au + nv.$$

Seja $l \in \mathbb{Z}$. Então,

$$\begin{aligned} a(\alpha + lm) - b &= a\alpha + alm - b \\ &= rn + la'dm \\ &= (r + la')n, \end{aligned}$$

pelo que $\alpha + lm$ é uma solução da congruência linear.

Reciprocamente, seja β uma solução da congruência linear. Então, existe $s \in \mathbb{Z}$ tal que $a\beta - b = sn$. Assim,

$$\begin{aligned} d\beta - d\alpha &= (au + nv)\beta - (au + nv)\alpha \\ &= au\beta + nv\beta - au\alpha - nv\alpha \\ &= snu + bu + nv\beta - rnu - bu - nv\alpha \\ &= snu + nv\beta - rnu - nv\alpha \\ &= (su + v\beta - ru - v\alpha)n \\ &= ((su + v\beta - ru - v\alpha)d)m, \end{aligned}$$

pelo que, $\beta - \alpha = (su + v\beta - ru - v\alpha)m$, ou seja,

$$\beta = \alpha + (su + v\beta - ru - v\alpha)m \in S.$$

Provámos então que

$$S = \{\alpha + lm : \ l \in \mathbb{Z}\}$$

é o conjunto das soluções da congruência linear.

Sejam $p, \ l \in \mathbb{Z}$ e consideremos

$$\beta_1 = \alpha + pm \qquad , \qquad \beta_2 = \alpha + lm.$$

Vejamos quando é que temos $\beta_1 \equiv \beta_2 (mod\ n)$. Ora, $\beta_1 \equiv \beta_2 (mod\ n)$ se, e só se, existe $t \in \mathbb{Z}$ tal que $\beta_1 - \beta_2 = tn$.

Porque, $\beta_1 - \beta_2 = \alpha + pm - \alpha - lm = (p - l)m$, vem $\beta_1 \equiv \beta_2 (mod\ n)$ se, e só se, $(p - l)m = \beta_1 - \beta_2 = tn = tdm$, com $t \in \mathbb{Z}$. Portanto, $\beta_1 \equiv \beta_2 (mod\ n)$ se, e só se $d|(p - l)$. Mas isto permite-nos concluir que S possuí exactamente d elementos não congruentes módulo n, por exemplo,

$$\alpha, \ \alpha + m, \ \alpha + 2m, \ldots, \ \alpha + (d - 1)m.$$

□

Observação Sejam $n \in \mathbb{N}$ e $a, \ b \in \mathbb{Z}$ tais que $d = mdc\{a, \ n\}$ também divide b. Então, atendendo ao Teorema anterior, a congruência linear

$$ax \equiv b (mod\ n)$$

possuí exactamente d soluções não congruentes módulo n duas a duas, em particular, possuí exactamente d soluções em Z_n. Como determiná-las?

Sejam $u, \ v \in \mathbb{Z}$ tais que $d = au + nv$. Sejam

$$\alpha = \frac{bu}{d} \in \mathbb{Z} \qquad e \qquad m = \frac{n}{d} \in \mathbb{Z}.$$

Então, pela demonstração do Teorema anterior,

$$\alpha, \ \alpha + m, \ \alpha + 2m, \ldots, \ \alpha + (d - 1)m$$

são d soluções não congruentes módulo n de $ax \equiv b(mod\ n)$.

Note-se que estas d soluções podem não pertencer todas a Z_n, mas atendendo aos Teoremas anteriores, podemos determinar d soluções em Z_n.

Exemplo 6.10 1. *Determinemos em Z_{15} todas as soluções da congruência linear*

$$13x \equiv 1(mod\ 15).$$

Comecemos por calcular, pelo algoritmo de Euclides, $d = mdc\{13,\ 15\}$:

$$\begin{aligned} 15 &= 13 \times 1 + 2, \\ 13 &= 2 \times 6 + 1, \\ 2 &= 2 \times 1, \end{aligned}$$

donde $d = 1$. Como $d|1$ (neste caso, $b = 1$), então a congruência linear possuí uma única solução em Z_{15}.

Como,

$$\begin{aligned} 1 &= 13 - 2 \times 6 = 13 - (15 - 13) \times 6 \\ &= 13 \times 7 + 15 \times (-6), \end{aligned}$$

temos que $u = 7$. Assim, $\alpha = \frac{1 \times 7}{1} = 7 \in Z_{15}$ é a única solução de $13x \equiv 1(mod\ 15)$ em Z_{15}.

2. *Consideremos a congruência linear*

$$224x \equiv 154(mod\ 385)$$

e determinemos todas as soluções em Z_{385}.

Como, $d = mdc\{224,\ 385\} = 7$ e 7 é um divisor de $b = 154(= 7 \times 22)$, então $224x \equiv 154(mod\ 385)$ possuí exactamente 7 soluções em Z_{385}. Por outro lado,

$$7 = 224 \times (-12) + 385 \times 7,$$

pelo que $u = -12$. Assim,

$$\alpha' = \frac{154 \times (-12)}{7} = -264,$$

é uma solução de $224x \equiv 154(mod\ 385)$. Mas, $\alpha' \notin Z_{385}$. Como, pelo Teorema, os inteiros do tipo

$$\alpha_k = \alpha' + km, \qquad com\ k \in \mathbb{Z}$$

(em que neste caso, $m = \frac{385}{7} = 55$), são soluções de $224x \equiv 154(mod\ 385)$, vamos determinar o menor α_k tal que $0 \leq \alpha_k < 385$. Mas isto significa determinar o menor inteiro não negativo α tal que

$$-264 \equiv \alpha(mod\ 55).$$

porque, $-264 = 55 \times (-5) + 11$*, então,* $\alpha = 11$*. Assim,*

$$11,\ 66,\ 121,\ 176,\ 231,\ 286,\ 341$$

são as sete soluções de $224x \equiv 154 (mod\ 385)$ *em* Z_{385}*.*

Proposição 6.11 *Seja* $n \in \mathbb{N}$ *e sejam* $a,\ a',\ b,\ b' \in \mathbb{Z}$ *tais que*

$$a \equiv a' (mod\ n) \qquad e \qquad b \equiv b' (mod\ n).$$

Então, as congruências lineares

$$ax \equiv b (mod\ n) \qquad e \qquad a'x \equiv b' (mod\ n)$$

possuem exactamente as mesmas soluções.

Demonstração Exercício.

Observação O resultado anterior permite-nos concluir que, para estudar todas as congruências lineares do tipo $ax \equiv b (mod\ n)$, $n \in \mathbb{N}$ e $a,\ b \in \mathbb{Z}$, basta estudar aquelas com $a,\ b \in Z_n$.

Proposição 6.12 *Seja* $x \in \mathbb{Z}$ *e sejam* $m,\ n \in \mathbb{N}$*. Então,*

$$[x]_{mn} \subseteq [x]_m \cap [x]_n.$$

Além disso, se $1 = mdc\{m,\ n\}$ *então*

$$[x]_{mn} = [x]_m \cap [x]_n.$$

Demonstração Exercício.

Corolário 6.13 *Sejam* $m,\ n \in \mathbb{N}$ *e sejam* $a,\ a',\ b,\ b' \in \mathbb{Z}$*. Seja* α *uma solução (comum) das congruências lineares*

$$ax \equiv b (mod\ m) \qquad e \qquad a'x \equiv b' (mod\ n).$$

Então, qualquer $\beta \in [\alpha]_{mn}$ *é ainda uma solução de ambas as congruências lineares.*

Lema 6.14 *Sejam* $m,\ n \in \mathbb{N}$ *tais que* $1 = mdc\{m,\ n\}$ *e sejam* $b,\ b' \in \mathbb{Z}$*. Então as congruências lineares*

$$x \equiv b (mod\ m) \qquad e \qquad x \equiv b' (mod\ n)$$

têm uma e uma só solução em Z_{mn}*.*

Demonstração Sejam $u,\ v \in \mathbb{Z}$ tais que

$$1 = mu + nv.$$

Então $bnv + b'mu$ é uma solução do sistema de congruências lineares

$$\begin{cases} x & \equiv b(mod\ m) \\ x & \equiv b'(mod\ n) \end{cases}$$

isto é, é uma solução comum a ambas as congruências.

Vejamos a unicidade. Seja α uma outra solução comum. Provemos que $\alpha \equiv (bnv + b'mu)(mod\ mn)$. Por hipótese, existem $r,\ s \in \mathbb{Z}$ tais que $\alpha - b = mr$, $\alpha - b' = ns$. Como,

$$\begin{aligned} \alpha - bnv - b'mu &= \alpha + (mr - \alpha)nv + (ns - \alpha)mu \\ &= \alpha + mnrv - \alpha nv + mnsu - \alpha mu \\ &= \alpha - \alpha(nv + mu) + (rv + su)mn \\ &= (rv + su)mn. \end{aligned}$$

então, temos $\alpha \equiv (bnv + b'mu)(mod\ mn)$. □

Teorema 6.15 *Seja $n \in \mathbb{N}$ tais que $1 = mdc\{m,\ n\}$ e sejam $a,\ a',\ b,\ b' \in \mathbb{Z}$. Se as congruências lineares*

$$ax \equiv b(mod\ m) \qquad e \qquad a'x \equiv b'(mod\ n)$$

têm ambas soluções então existe uma solução comum em Z_{mn}.

Demonstração Sejam α, α' soluções de

$$ax \equiv b(mod\ m) \qquad e \qquad a'x \equiv b'(mod\ n),$$

respectivamente. Atendendo ao Lema anterior, o sistema de congruências lineares

$$\begin{cases} x & \equiv \alpha(mod\ m) \\ x & \equiv \alpha'(mod\ n) \end{cases}$$

possuí uma única solução $\beta \in Z_{mn}$. Portanto, como $\beta \in [\alpha]_m$ e $\beta \in [\alpha']_n$ então β é ainda uma solução de

$$ax \equiv b(mod\ m) \qquad \text{e de} \qquad a'x \equiv b'(mod\ n),$$

como pretendido. □

Exemplo 6.16 *Determinemos em Z_{20} uma solução comum às congruências lineares*

$$4x \equiv 12(mod\ 5) \qquad e \qquad 3x \equiv 6(mod\ 4).$$

Pela Proposição, porque

$$12 \equiv 2(mod\ 5) \qquad e \qquad 6 \equiv 2(mod\ 4)$$

então as soluções de $4x \equiv 12(mod\ 5)$ *e de* $4x \equiv 2(mod\ 5)$ *são as mesmas e as soluções de* $3x \equiv 6(mod\ 4)$ *e de* $3x \equiv 2(mod\ 4)$ *são as mesmas.*

Uma solução de $4x \equiv 2(mod\ 5)$ *é* $\alpha = 3$ *e uma solução de* $3x \equiv 2(mod\ 4)$ *é* $\alpha' = 2$.

Pela demonstração do Teorema, teremos de calcular a única solução, em Z_{20}, *comum às congruências*

$$x \equiv 3(mod\ 5) \qquad e \qquad x \equiv 2(mod\ 4).$$

Como, pela igualdade de Bézout, temos

$$1 = 5 \times 1 + 4 \times (-1)$$

então

$$\beta = 2 \times 5 \times 1 + 3 \times 4 \times (-1) = -2$$

é a solução comum.

Então, porque $-2 \equiv 18(mod\ 20)$, 18 *é a única solução comum, em* Z_{20} *e também é solução das congruências iniciais.*

Capítulo 7

Relações de Recorrência

7.1 Definição e exemplos

Consideremos as seguintes instruções para gerar os termos de uma sucessão:
(1) O primeiro termo é 5;
(2) Dado um termo, o termo seguinte obtêm-se adicionando-lhe 3.

Obtemos a sucessão

$$5,\ 8,\ 11,\ 14,\ 17, \ldots$$

Se denotarmos a sucessão anterior por

$$a_0,\ a_1,\ a_2,\ a_3, \ldots$$

as instruções (1) e (2) anteriores podem ser reescritas da seguinte forma:
$(1')$ $a_0 = 5$
$(2')$ $a_n = a_{n-1} + 3$, $n \geq 1$.
A equação dada em $(2')$ é um exemplo de uma relação de recorrência.

Definição 7.1 *Uma* **relação de recorrência** *para a sucessão* $a_0,\ a_1, \ldots$ *é uma expressão que relaciona cada termo* a_n *(a partir de certa ordem p) com alguns dos seus predecessores* $a_0,\ a_1, \ldots,\ a_{n-1}$.

As condições iniciais são valores que são explicitamente dados para um número finito $(p-1)$ de termos da sucessão.

Exemplo 7.2 1. *Na sucessão anteriormente referida:*

$$5,\ 8,\ 11,\ 14,\ 17, \ldots$$

as condições iniciais são:

$$a_0 = 5$$

e a relação de recorrência é:

$$a_n = a_{n-1} + 3, \qquad n \geq 1.$$

2. *Na sucessão de Fibonacci:*

$$1,\ 2,\ 3,\ 5,\ 8,\ 13,\ 21,\ 34, \ldots$$

as condições iniciais são:

$$a_0 = 1, \quad a_1 = 2$$

e a relação de recorrência é:

$$a_n = a_{n-1} + a_{n-2}, \qquad n \geq 2.$$

3. *Uma pessoa investe* 2000 *euros e tem um juro fixo de* 14% *ao ano. Seja* a_n *a quantia de que dispõe ao fim do n-ésimo ano.*

   Vamos determinar a relação de recorrência e as condições iniciais para esta sucessão:

$$a_0,\ a_1,\ a_2,\ a_3, \ldots.$$

   Condição inicial: $a_0 = 2000$

   Relação de recorrência: $a_n = a_{n-1} + 0.14 \times a_{n-1}$, $n \geq 1$

   ou seja,

$$a_n = 1.14 \times a_{n-1},\ n \geq 1.$$

7.2 "Resolver" uma relação de recorrência

"Resolver" uma relação de recorrência, sujeita a certas condições iniciais, é determinar uma "expressão explicita" para o termo geral da sucessão.

Exemplo 7.3 1. *Considere a sucessão* $a_0,\ a_1, \ldots$ *definida pela relação de recorrência*

$$a_n = a_{n-1} + 3, \qquad n \geq 1.$$

com a condição inicial

$$a_0 = 2.$$

Como,

$$\begin{aligned} a_n &= a_{n-1} + 3 \\ &= (a_{n-2} + 3) + 3 = a_{n-2} + 2 \times 3 \\ &= (a_{n-3} + 3) + 2 \times 3 = a_{n-3} + 3 \times 3 \\ &\vdots \\ &= (a_{n-k} + 3) + (k-1) \times 3 = a_{n-k} + k \times 3 \\ &\vdots \\ &= a_1 + (n-1) \times 3 = (a_0 + 3) + (n-1) \times 3 = a_0 + n \times 3 \\ &= 2 + 3 \times n, \end{aligned}$$

temos que $a_n = 2 + 3 \times n$, *para* $n \geq 0$. *(***Exercício***: prove formalmente esta igualdade, usando o princípio de indução).*

2. *Vamos resolver a relação de recorrência*

$$a_n = 2a_{n-1}$$

sujeita à condição inicial $a_0 = 1$. *Temos*

$$a_n = 2 \times a_{n-1} = 2 \times 2 \times a_{n-2} = 2^2 \times a_{n-2} = 2^2 \times 2 \times a_{n-3} =$$

$$= 2^3 \times a_{n-3} = \ldots = 2^k \times a_{n-k} = \ldots = 2^n \times a_0 = 2^n.$$

Então, $a_n = 2^n$, *para* $n \geq 0$. *(***Exercício***: prove formalmente esta igualdade, usando o princípio de indução.)*

7.3 Relações de recorrência lineares homogéneas de grau k

Uma **relação de recorrência linear homogénea de grau k** ($k \geq 1$) com coeficientes constantes é uma expressão da forma

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \ldots + c_k a_{n-k},$$

com $c_1, \ldots, c_k$ constantes (reais) e $c_k \neq 0$.

Exemplo 7.4 1. *A relação de recorrência*

$$a_n = a_{n-1} + a_{n-2}$$

utilizada na definição da sucessão de Fibonacci, é uma relação de recorrência linear homogénea de grau 2 *com coeficientes constantes.*

2. *A expressão*
$$a_n = 2a_{n-1}$$
é uma relação de recorrência linear homogénea de grau 1 *com coeficientes constantes.*

3. *A relação de recorrência*
$$a_n = 3a_{n-1}a_{n-2}$$
não é linear.

4. *A relação de recorrência*
$$a_n = a_{n-1} + 3$$
não é homogénea.

5. *A relação de recorrência*
$$a_n = 3na_{n-1}$$
não tem coeficientes constantes.

Observação Uma relação de recorrência linear homogénea de grau 1 com coeficientes constantes é uma expressão da forma

$$a_n = ca_{n-1},$$

com c uma constante (real) não nula. É fácil concluir que podemos resolver esta relação de recorrência sujeita à condição inicial $a_0 = a$ (constante), obtendo-se

$$a_n = a.c^n, \qquad n \geq 0.$$

(**Exercício**: prove formalmente esta igualdade, usando o principio de indução.)

7.4 Relações de recorrência lineares homogéneas de grau 2

Sejam
$$a_n = c_1a_{n-1} + c_2a_{n-2} + \ldots + c_ka_{n-k}$$
uma relação de recorrência linear homogénea de grau k ($c_1, \ldots,\ c_k$ constantes reais) e $s_0,\ s_1,\ s_2, \ldots$ uma sucessão, (abreviadamente escrevemos S ou $(s_n)_{n\geq 0}$ para designar esta sucessão) dizemos que a sucessão $s_0,\ s_1,\ s_2, \ldots$ satisfaz a relação de recorrência se

$$s_n = c_1s_{n-1} + c_2s_{n-2} + \ldots + c_ks_{n-k}.$$

Exemplo 7.5 *Considere a relação de recorrência*

$$a_n = a_{n-1} + 3.$$

(i) *A sucessão S tal que $s_0,\ s_1,\ s_2, \ldots$ são respectivamente*

$$2,\ 5,\ 8,\ 11, \ldots$$

satisfaz esta relação de recorrência pois

$$s_n = s_{n-1} + 3 \qquad (n \geq 1).$$

(ii) *A sucessão T tal que $t_0,\ t_1,\ t_2, \ldots$ são respectivamente*

$$2,\ 6,\ 10,\ 14, \ldots$$

não satisfaz a relação de recorrência pois

$$2 + 4 = 6 = t_1 = t_0 + 4 \neq t_0 + 3 = 2 + 3 = 5.$$

Lema 7.6 *Seja*

$$a_n = c_1 a_{n-1} + c_2 a_{n-2}$$

($c_1,\ c_2 \in \mathbb{R}$ e $c_2 \neq 0$) uma relação de recorrência linear homogénea de grau 2 com coeficientes constantes. Sejam S, T duas sucessões que satisfazem a relação de recorrência e sejam b e d duas constantes reais. Então a sucessão

$$U = bS + dT$$

também satisfaz a relação de recorrência.

Demonstração Como S e T satisfazem a relação de recorrência, então

$$s_n = c_1 s_{n-1} + c_2 s_{n-2} \qquad (n \geq 2)$$

e

$$t_n = c_1 t_{n-1} + c_2 t_{n-2} \qquad (n \geq 2).$$

Uma vez que $u_n = bs_n + dt_n \quad (n \geq 0)$, então para $n \geq 2$,

$$\begin{aligned} u_n &= b(c_1 s_{n-1} + c_2 s_{n-2}) + d(c_1 t_{n-1} + c_2 t_{n-2}) \\ &= c_1(bs_{n-1} + dt_{n-1}) + c_2(bs_{n-2} + dt_{n-2}) \\ &= c_1 u_{n-1} + c_2 u_{n-2}. \end{aligned}$$

Pelo que U satisfaz a relação de recorrência. □

Lema 7.7 *Seja*

$$a_n = c_1 a_{n-1} + c_2 a_{n-2}$$

($c_1,\ c_2 \in \mathbb{R}$ e $c_2 \neq 0$) uma relação de recorrência linear homogénea de grau 2 com coeficientes constantes. Seja r uma raiz da equação

$$x^2 - c_1 x - c_2 = 0.$$

Então, a sucessão $(r^n)_{n \geq 0}$ satisfaz a relação de recorrência.

Demonstração Por hipótese, r é raiz de $x^2 - c_1x - c_2 = 0$, pelo que $r^2 - c_1r - c_2 = 0$, ou seja, $r^2 = c_1r + c_2$. Então,

$$c_1r^{n-1} + c_2r^{n-2} = r^{n-2}(c_1r + c_2) = r^{n-2}r^2 = r^n \qquad (n \geq 2),$$

como pretendido. □

Teorema 7.8 *Seja*

$$a_n = c_1a_{n-1} + c_2a_{n-2}$$

($c_1,\ c_2 \in \mathbb{R}$ e $c_2 \neq 0$) uma relação de recorrência linear homogénea de grau 2 com coeficientes constantes tal que a equação

$$x^2 - c_1x - c_2 = 0$$

admite duas raízes distintas r_1 e r_2. Seja $(a_n)_{n\geq 0}$ a sucessão definida pela relação de recorrência sujeita às condições iniciais

$$a_0 = \mathcal{C}_0 \qquad , \qquad a_1 = \mathcal{C}_1.$$

Então, existem constantes (reais) b e d tais que

$$a_n = br_1^n + dr_2^n, \qquad n \geq 0.$$

Demonstração Pelo Lema anterior, as sucessões $S = (r_1^n)_{n\geq 0}$ e $T = (r_2^n)_{n\geq 0}$ satisfazem a relação de recorrência. Assim, para quaisquer constantes b e d, a sucessão

$$bS + dT = U = (u^n)_{n\geq 0} \qquad (*)$$

satisfaz a relação de recorrência. Necessitamos determinar constantes b e d por forma que U também satisfaça as condições iniciais, ou seja, tais que

$$u_0 = \mathcal{C}_0 \qquad , \qquad u_1 = \mathcal{C}_1.$$

Ora, a partir de (*), temos $u_n = br_1^n + dr_2^n$, para $n \geq 0$, pelo que (considerando $n = 0$ e $n = 1$),

$$\begin{cases} u_0 &= b + d \\ u_1 &= br_1 + dr_2. \end{cases}$$

Donde, falta-nos resolver o sistema de equações lineares

$$\begin{cases} b + d &= \mathcal{C}_0 \\ br_1 + dr_2 &= \mathcal{C}_1, \end{cases}$$

nas incógnitas b e d, cuja matriz simples é

$$M = \begin{bmatrix} 1 & 1 \\ r_1 & r_2 \end{bmatrix}$$

Como $det\ M = r_1r_2 \neq 0$, então o sistema é possível e determinado. Portanto, provámos a existência de constantes b e d tais que a sucessão U também satisfaz as condições iniciais. Logo, $U = (a^n)_{n\geq 0}$. □

Exemplo 7.9 1. *Vamos resolver a relação de recorrência*

$$a_n = 5a_{n-1} - 6a_{n-2}$$

sujeita às condições iniciais

$$a_0 = 7 \qquad , \qquad a_1 = 16.$$

Comecemos por considerar a equação

$$x^2 - 5x + 6 = 0,$$

cujas raízes são $x = 2$ *e* $x = 3$. *Atendendo ao Teorema anterior, temos*

$$a_n = b2^n + d3^n, \qquad n \geq 0$$

para certas constantes b *e* d *tais que*

$$\begin{cases} b + d & = a_0 = 7 \\ 2b + 3d & = a_1 = 16, \end{cases}$$

ou seja (resolvendo o sistema),

$$\begin{cases} b & = 5 \\ d & = 2. \end{cases}$$

Logo, $a_n = 5 \times 2^n + 2 \times 3^n$, *para* $n \geq 0$.

2. *Consideremos a relação de recorrência*

$$a_n = 3a_{n-1} - 2a_{n-2}$$

sujeita às condições iniciais

$$a_0 = 200 \qquad , \qquad a_1 = 220.$$

Comecemos por analisar a equação

$$x^2 - 3x + 2 = 0,$$

cujas raízes (distintas) são $x = 1$ *e* $x = 2$. *Pelo Teorema anterior, temos*

$$a_n = b + d2^n, \qquad n \geq 0$$

para certas constantes b *e* d *tais que*

$$\begin{cases} b + d & = a_0 = 200 \\ b + 2d & = a_1 = 220, \end{cases}$$

ou seja (resolvendo o sistema),

$$\begin{cases} b & = 180 \\ d & = 20. \end{cases}$$

Logo, $a_n = 180 + 20 \times 2^n$, *para* $n \geq 0$.

Teorema 7.10 *Seja*

$$a_n = c_1 a_{n-1} + c_2 a_{n-2}$$

($c_1,\ c_2 \in \mathbb{R}$ e $c_2 \neq 0$) uma relação de recorrência linear homogénea de grau 2 com coeficientes constantes tal que a equação

$$x^2 - c_1 x - c_2 = 0$$

admite uma raiz dupla r. Seja $(a_n)_{n\geq 0}$ a sucessão definida pela relação de recorrência sujeita às condições iniciais

$$a_0 = \mathcal{C}_0 \qquad , \qquad a_1 = \mathcal{C}_1.$$

Então, existem constantes (reais) b e d tais que

$$a_n = br^n + dnr^n, \qquad n \geq 0.$$

Demonstração Atendendo ao Lema anterior, $S = (r^n)_{n\geq 0}$ satisfaz a relação de recorrência.

Como r é raiz dupla da equação $x^2 - c_1 x - c_2 = 0$, então

$$(x - r)^2 = x^2 - c_1 x - c_2,$$

isto é,

$$x^2 - 2rx + r^2 = x^2 - c_1 x - c_2,$$

pelo que $c_1 = 2r$ e $c_2 = -r^2$.

Porque a relação de recorrência é de grau 2, então $c_2 \neq 0$, donde $r \neq 0$.

Por outro lado,

$$c_1(n-1)r^{n-1} + c_2(n-2)r^{n-2} = 2r(n-1)r^{n-1} - r^2(n-2)r^{n-2} = r^n(2(n-1) - (n-2)) = nr^n,$$

pelo que $T = (nr^n)_{n\geq 0}$ satisfaz a relação de recorrência. Então, a sucessão

$$bS + dT = U = (u_n)_{n\geq 0} \qquad (*)$$

ainda satisfaz a relação de recorrência, para quaisquer constantes b e d.

Resta-nos determinar b e d por forma que U também satisfaça as condições iniciais, ou seja, tais que

$$u_0 = \mathcal{C}_0 \qquad , \qquad u_1 = \mathcal{C}_1.$$

Ora, a partir de (*), temos $u_n = br^n + dnr^n$, para $n \geq 0$, pelo que (considerando $n = 0$ e $n = 1$),

$$\begin{cases} u_0 & = \text{b} \\ u_1 & = \text{br+dr}. \end{cases}$$

Assim, temos de resolver o sistema de equações lineares

$$\begin{cases} \text{b} & = \mathcal{C}_0 \\ \text{br+dr} & = \mathcal{C}_1, \end{cases}$$

nas incógnitas b e d, o que é equivalente a

$$\begin{cases} \mathrm{b} & = \mathcal{C}_0 \\ \mathrm{d} & = \frac{\mathcal{C}_1 - r\mathcal{C}_0}{r}, \end{cases}$$

portanto, possível e determinado. □

Exemplo 7.11 *Vamos resolver a relação de recorrência*

$$a_n = 4a_{n-1} - 4a_{n-2}$$

sujeita às condições iniciais

$$a_0 = 1 \qquad , \qquad a_1 = 1.$$

Comecemos por considerar a equação

$$x^2 - 4x + 4 = 0,$$

a qual possui $x = 2$ como raiz dupla. Atendendo ao Teorema anterior, temos

$$a_n = b2^n + dn2^n, \qquad n \geq 0$$

para certas constantes b e d tais que

$$\begin{cases} b & = a_0 = 1 \\ 2b + 2d & = a_1 = 1, \end{cases}$$

ou seja (resolvendo o sistema),

$$\begin{cases} b & = 5 \\ d & = -\frac{1}{2}. \end{cases}$$

Logo, $a_n = 2^n - \frac{1}{2} \times n \times 2^n = 2^n - n2^{n-1}$, para $n \geq 0$.

Capítulo 8

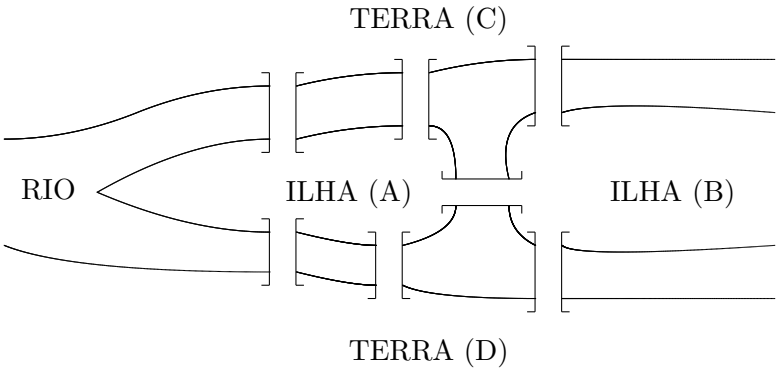
Introdução ao estudo dos Grafos

8.1 Alguns problemas clássicos

A teoria dos grafos teve a sua origem no estudo de problemas que podemos chamar de "recreativos". Vejamos alguns destes problemas.

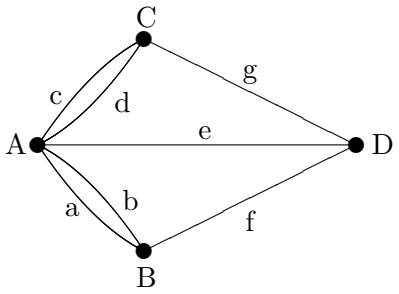
Problema das Pontes de Königsberg

Na cidade de Königsberg, antiga capital da Prússia Oriental, o rio Pregel circundava uma ilha e separava-a em duas vertentes:



No século XVIII existiam sete pontes ligando diversas regiões da cidade e conta-se que, nos seus passeios, os habitantes se divertiam a tentar encontrar um percurso que lhes permitisse atravessar cada uma das pontes uma, e uma só vez, voltando ou não ao ponto de partida. Dado as suas tentativas resultarem ifrutíferas, alguns começaram a acreditar que tal percurso não existia.

Refira-se que para a resolução deste problema podemos construir o seguinte diagrama:



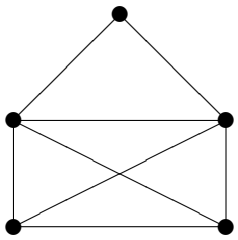
em que os "arcos"a, b, c, d, e, f, g representam as sete pontes e os "vértices"A, B, C, D representam as quatro regiões da cidade que tem interesse considerar.

Em 1736 o matemático suíço Leonhard Euler escreve um artigo, considerado o primeiro artigo de teoria de grafos, no qual demonstra a inexistência de um percurso nas condições anteriormente descritas.

Segundo refere L. Saalschütz, em 1875 foi construída uma nova ponte h, ligando as zonas representadas por B e C, após o que se tornou possível efectuar um percurso nas condições referidas. Nomeadamente,

$$\mathrm{D} \underset{f}{\text{——}} \mathrm{B} \underset{a}{\text{——}} \mathrm{A} \underset{b}{\text{——}} \mathrm{B} \underset{h}{\text{——}} \mathrm{C} \underset{g}{\text{——}} \mathrm{D} \underset{e}{\text{——}} \mathrm{A} \underset{c}{\text{——}} \mathrm{C} \underset{d}{\text{——}} \mathrm{A}$$

Problemas do mesmo tipo do anterior são aqueles em que se pretende desenhar certas figuras, como por exemplo:



sem levantar o lápis do papel e não passando sobre um "arco"já desenhado.

Para tais problemas será dada uma resposta completa no capítulo com o título de Grafos Eulerianos.

Problema do Percurso do Cavalo num Tabuleiro de Xadrez

Este problema, tratado por Euler (1759) e Vandermonde (1771) consistia no estudo da existência de uma sequência de movimentos que permitisse a um "cavalo"percorrer, através de movimentos obedecendo às regras usuais de movimentação no jogo de xadrez, as 8×8

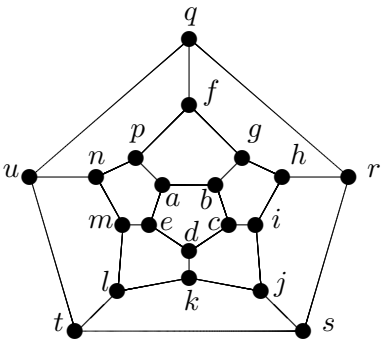
"casas"do tabuleiro uma, e uma só, vez regressando à posição de partida.

Observe-se que num tabuleiro de xadrez o número de "casas"brancas é igual ao número de "casas"pretas e que um cavalo através de um único movimento lícito passa de uma "casa"para outra de cor distinta.

Tal como anteriormente, o problema pode ser estudado considerando um diagrama com $8 \times 8 = 64$ "vértices", cada um representando um quadrado do tabuleiro e estando dois vértices ligados por um "arco"se, e só se, o cavalo puder mover-se entre as respectivas posições, através de um único movimento lícito.

Refira-se que este problema é distinto do anterior. Anteriormente pretendia-se que cada "arco"fosse "percorrido"uma, e uma só, vez. Aqui pretende-se que cada "vértice"seja "visitado"uma, e uma só, vez. Para concretizar este objectivo pode não ser necessário percorrer todos os "arcos".

No âmbito deste problema, em 1857, Hamilton apresenta na Associação Britânica de Dublin um "jogo"que, entre outras versões, tinha uma que envolvia um dodecaedro regular.



Os seus 20 "vértices"representavam 20 cidades importantes e os seus "arcos"representavam ligações entre cidades. Pretendia-se determinar um percurso que permitisse visitar todas as cidades uma, e uma só, vez e regressar à cidade de partida.

Uma solução para este problema é o percurso

$$a,\ b,\ c,\ d,\ e,\ m,\ l,\ k,\ j,\ i,\ h,\ g,\ f,\ q,\ r,\ s,\ t,\ u,\ n,\ p,\ a.$$

O problema complicava-se quando se pretendia determinar um percurso nas condições anteriores, mas que iniciasse com o trajecto

$$a,\ b,\ g,\ h,\ i.$$

Este problema conhecido por "Viagem à volta do mundo"é do mesmo tipo do "Percurso do cavalo num tabuleiro de xadrez". Ambos constituem motivação para o estudo que efectuaremos no capítulo dos Grafos Hamiltonianos, terminologia que não está completamente

justificada uma vez que, antes de Hamilton, Vandermonde e Kirkman se tinham debruçado sobre este assunto.

Em 1936, exactamente 200 anos após o artigo de Euler sobre as pontes de Königsberg, é publicado o primeiro livro sobre teoria de grafos da autoria de D. König. König é o primeiro a propor chamar "grafos"aos diagramas referidos bem como a estudar de forma sistemática as suas propriddades. Desde essa altura os trabalhos nesta área multiplicam-se, destacando-se os nomes de C. Berge, Ore, Erdos, Tutte e F. Harary.

Actualmente, os grafos são utilizados nas mais diversas áreas. Neste curso já utilizámos estes diagramas quando representámos geometricamente as relações binárias e quando desenhámos diagramas de Hasse.

8.2 Definições elementares

O nosso estudo vai centrar-se em duas espécies de grafos:
- Grafos orientados
- Grafos não orientados.

Começaremos pelos grafos orientados.

Definição 8.1 *Chamamos* **grafo orientado**, G, *a um par* $(X, \mathcal{U})$ *em que:*

(i) X *é um conjunto finito, não vazio e*

(ii) $\mathcal{U}$ *é um subconjunto do produto cartesiano* $X \times X$.

Cada elemento de X diz-se um **vértice** de G e o cardinal de X, $|X|$, designa-se por **ordem** de G.

Os elementos de $\mathcal{U}$ dizem-se os **arcos** de G e o seu cardinal é designado por **tamanho** de G.

No que respeita a notações utilizamos, em geral:

- as letras n e m, com índices se tal se revelar necessário, para designar, respectivamente, ordens e tamanhos de grafos;

- as letras $x,\ y,\ z$, eventualmente com índices, para designar vértices de grafos;

- as letras $u,\ v,\ w$, também com ou sem índices, para representar arcos de grafos.

Seja $u = (x_i,\ x_j) \in \mathcal{U}$. Diz-se que u é um arco de x_i para x_j, sendo x_i o vértice/extremidade inicial de u e x_j o vértice/extremidade final de u. Diz-se, ainda, que x_i e x_j são os vértices terminais ou as extremidades de u ou que u é incidente nos vértices x_i e x_j.

Um arco da forma $(x_i,\ x_i)$ diz-se um **laço**.

É usual representar geometricamente um grafo, no plano, fazendo corresponder a cada vértice um ponto, de tal forma que a vértices distintos correspondam pontos distintos, e fazendo corresponder a cada arco um segmento de recta ou, mais geralmente, uma curva contínua que não se intersecte a si própria, unindo os dois pontos representativos dos seus vértices terminais e não passando por nenhum outro ponto representativo de um vértice. Arcos com iguais extremidades, como $(x_i,\ x_j)$ e $(x_j,\ x_i)$, com $i \neq j$, são representados por curvas não coincidentes e sobre cada curva representativa de um arco é desenhada uma seta "apontando"no sentido do ponto representativo do vértice final.

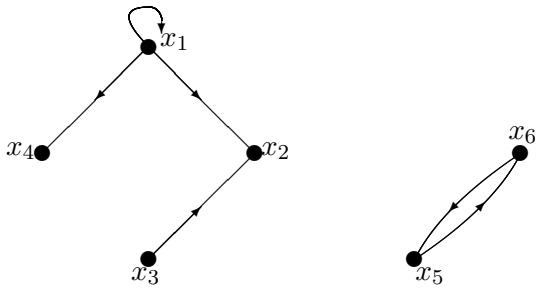
Exemplo 8.2 *Uma representação possível para o grafo $G = (X,\mathcal{U})$, em que*

$$X = \{x_1,\ x_2,\ x_3,\ x_4,\ x_5\}$$

e

$$\mathcal{U} = \{(x_1,\ x_2),\ (x_1,\ x_4),\ (x_5,\ x_6),\ (x_6,\ x_5),\ (x_1,\ x_1),\ (x_3,\ x_2)\},$$

é a seguinte:



Num grafo orientado $G = (X,\ \mathcal{U})$ dois **vértices** distintos x_i e x_j dizem-se **adjacentes** se existir, pelo menos, um arco neles incidentes, isto é, x_i e x_j, com $i \neq j$, são vértices adjacentes se $(x_i,\ x_j) \in \mathcal{U}$ ou $(x_j,\ x_i) \in \mathcal{U}$. Considera-se que um vértice x_i é adjacente a si próprio se, e só se, $(x_i,\ x_i) \in \mathcal{U}$.

Dois **arcos** distintos dizem-se **adjacentes** se têm, pelo menos, uma extremidade comum. Considera-se que um arco u é adjacente a si próprio se, e só se, u é um laço.

Num grafo orientado $G = (X,\ \mathcal{U})$ designa-se por **sucessor** (respectivamente, **predecessor**) de um vértice x todo o vértice que seja extremidade final (respectivamente, inicial) de um arco cuja extremidade inicial (respectivamente, final) seja x. O conjunto dos sucessores e o conjunto dos predecessores de x serão designados, respectivamente, por:

$$\Gamma^+(x) = \{y \in X :\ (x,\ y) \in \mathcal{U}\}$$

e

$$\Gamma^-(x) = \{y \in X : \ (y,\ x) \in \mathcal{U}\}.$$

Designaremos por $\Gamma(x)$ o conjunto dos vértices adjacentes a x.

Num grafo orientado tem-se

$$\Gamma(x) = \Gamma^+(x) \cup \Gamma^-(x).$$

Se $\Gamma^+(x) = \emptyset$ e $\Gamma^-(x) \neq \emptyset$ diz-se que x é um **poço**.
Se $\Gamma^+(x) \neq \emptyset$ e $\Gamma^-(x) = \emptyset$ diz-se que x é uma **fonte**.
Se $\Gamma(x) = \emptyset$ diz-se que x é um **vértice isolado**.

Exemplo 8.3 *Usando o exemplo anterior, no qual,* $G = (X,\mathcal{U})$ *com*

$$X = \{x_1,\ x_2,\ x_3,\ x_4,\ x_5\}$$

e

$$\mathcal{U} = \{(x_1,\ x_2),\ (x_1,\ x_4),\ (x_5,\ x_6),\ (x_6,\ x_5),\ (x_3,\ x_3),\ (x_3,\ x_2)\},$$

temos:

x_1 *e* x_2 *são vértices adjacentes.*

Os arcos $(x_1,\ x_2)$ *e* $(x_3,\ x_2)$ *são adjacentes.*

$$\Gamma^+(x_1) = \{x_2,\ x_4\}.$$

$$\Gamma(x_3) = \{x_2,\ x_3\}.$$

x_1 *é uma fonte.*

x_4 *é um poço.*

O grafo não tem vértices isolados.

De entre os grafos orientados, existe uma classe muito importante, os grafos orientados sem laços que se designam por **digrafos**.

Conforme veremos posteriormente, pode suceder que no estudo de certas propriedades dos grafos conhecer a "orientação"dos arcos, ou mais correctamente, distinguir o arco $(x_i,\ x_j)$ do arco $(x_j,\ x_i)$, com $i \neq j$, não se revele importante.

Definição 8.4 *Dizemos que* $G = (X,\ \mathcal{U})$ *é um* **grafo não orientado** *ou, ainda, que* $G = (X,\ \mathcal{U})$ *é um* **grafo simples** *se:*

(i) X *é um conjunto finito, não vazio e*

(ii) $\mathcal{U}$ *é um subconjunto de*

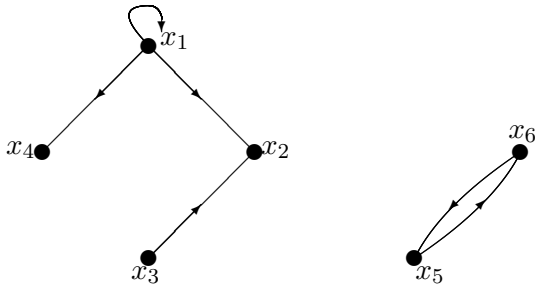
$$X \otimes X = \{\{x,\ y\} :\ x,\ y \in X,\ x \neq y\}.$$

Certas noções anteriormente dadas não têm agora significado. É o caso das noções de extremidade inicial e extremidade final de um arco, de laço, de sucessor e de predecessor de um vértice, de poço e de fonte. As restantes têm uma adaptação que julgamos ser evidente.

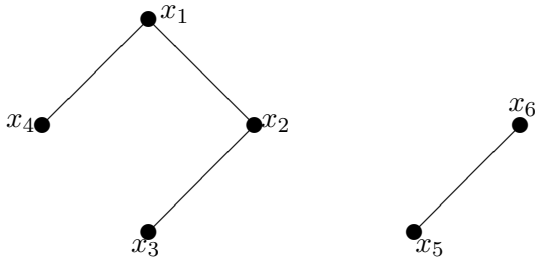
A representação geométrica dos grafos simples obedece aos mesmos princípios que a dos grafos orientados, não figurando apenas a seta representativa da orientação.

Dado um grafo orientado $G = (X,\ \mathcal{U})$ consideremos o grafo simples $G' = (X,\ \mathcal{U}')$ que se obtém, eliminando os laços em $\mathcal{U}$ e seguidamente substituindo cada par ordenado $(x_i,\ x_j) \in \mathcal{U}$ pelo conjunto $\{x,\ y\}$. G' diz-se, então, o **grafo subjacente** a G.

Exemplo 8.5 *O grafo subjacente ao grafo orientado descrito no exemplo* **??**



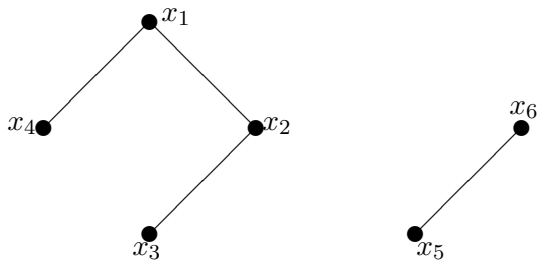
é o grafo simples



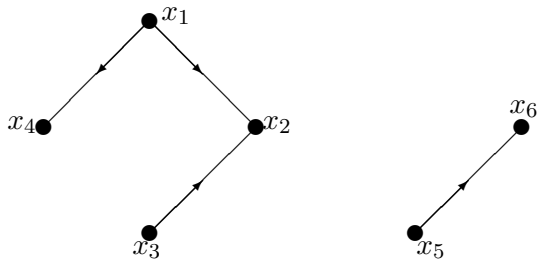
Seja $G = (X,\ \mathcal{U})$ um grafo simples e consideremos um grafo orientado $G' = (X,\ \mathcal{U}')$ em que $\mathcal{U}'$ se obteve de $\mathcal{U}$ substituindo cada arco $\{x_i,\ x_j\}$ ou por $(x_i,\ x_j)$ ou por $(x_j,\ x_i)$, sendo

a disjunção uma disjunção exclusiva. Se $\mathcal{U}$ é não vazio, podemos associar a G mais do que um grafo orientado, cada um dos quais se diz um **grafo resultante da orientação** de G.

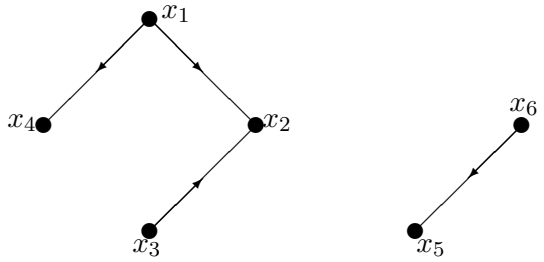
Exemplo 8.6 *Usando o grafo simples que obtivemos no exemplo anterior,*



Um grafo resultante da orientação deste será:



Um outro grafo resultante da orientação do grafo simples inicial será:



Repare-se que unicamente foi alterada a "orientação"do arco $\{x_6,\ x_5\}$. *O que nunca conseguimos é, através deste processo, obter o grafo orientado inicial.*

Na quase totalidade dos problemas que estudaremos, as definições anteriores de grafo orientado e de grafo simples são as que interessa considerar. Contudo para estudarmos

problemas do mesmo tipo do das pontes de Königsberg, teremos que considerar uma outra definição de grafo, que permita a um arco ocorrer repetido.

Definição 8.7 *Chamamos* **multigrafo orientado** *(respectivamente,* **não orientado***, a um par $G = (X, \mathcal{U})$ em que:*

(i) *X é um conjunto finito, não vazio e*

(ii) *$\mathcal{U}$ é uma família de $X \times X$ (respectivamente, $X \otimes X$).*

Se na família $\mathcal{U}$ o número máximo de vezes que um elemento ocorre é p dizemos que G é um **p-grafo** (o grafo do problema das pontes de Königsberg é um 2-grafo não orientado).

Os elementos da família $\mathcal{U}$ que são iguais dizemos que constituem **arcos paralelos**.

Assim, grafo simples é um 1-grafo não orientado e digrafo é um 1-grafo orientado sem laços.

8.3 Grau de um vértice. Sequências gráficas

Seja $G = (X, \mathcal{U})$ um multigrafo não orientado (respectivamente, multigrafo orientado). O **grau de um vértice** x define-se como o número de arcos incidentes em x (respectivamente, o número de arcos incidentes em x mais o número de laços incidentes em x). Representa-se, habitualmente, por $d_G(x)$, ou simplesmente por $d(x)$, se não houver dúvidas sobre qual é o grafo que se está a considerar.

Se G é um multigrafo orientado denomina-se **grau exterior** (respectivamente, **grau interior**) do vértice x, e representa-se por $d^+(x)$ (respectivamente, $d^-(x)$) o número de arcos de G que têm x como extremidade inicial (respectivamente, extremidade final).

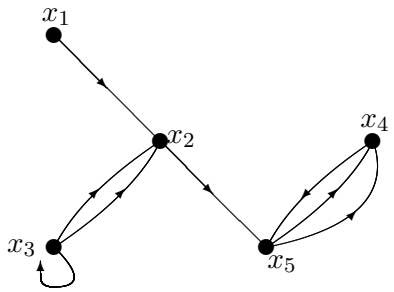
Das definições anteriores resulta que num multigrafo orientado $G = (X, \mathcal{U})$ se tem

$$d(x) = d^+(x) + d^-(x), \qquad \text{para todo o } x \in X.$$

Atenda-se, ainda, a que num grafo orientado $G = (X, \mathcal{U})$ se verifica que

$$d^+(x) = |\Gamma^+(x)| \qquad \text{e} \qquad d^-(x) = |\Gamma^-(x)|, \qquad \text{para todo o } x \in X.$$

Exemplo 8.8 *Consideremos o seguinte multigrafo orientado,*



Tem-se

$$\begin{aligned} d^+(x_1) &= 1 \quad , \quad d^-(x_1) = 0 \\ d^+(x_2) &= 1 \quad , \quad d^-(x_2) = 3, \\ d^+(x_3) &= 3 \quad , \quad d^-(x_3) = 1, \\ d^+(x_4) &= 1 \quad , \quad d^-(x_4) = 2, \\ d^+(x_5) &= 2 \quad , \quad d^-(x_5) = 2. \end{aligned}$$

O resultado mais conhecido envolvendo os graus dos vértices é o seguinte:

Teorema 8.9 *Num multigrafo não orientado (respectivamente, multigrafo orientado)* $G = (X, \mathcal{U})$ *com* m *arcos tem-se*

(i) $\sum_{x \in X} d(x) = 2m$.

(ii) *Se* $G = (X, \mathcal{U})$ *é um multigrafo orientado verifica-se ainda que* $\sum_{x \in X} d^+(x) = \sum_{x \in X} d^-(x) = m$.

Demonstração A demonstração da afirmação (ii) é imediata, se atendermos a que cada arco, independentemente de ser ou não um laço, tem uma, e uma só, extremidade inicial (respectivamente, final) contribuindo, assim, com uma parcela igual a 1 para o somatório $\sum_{x \in X} d^+(x)$ (respectivamente, $\sum_{x \in X} d^-(x)$).

A demonstração de (i) para multigrafos orientados, pode fazer-se utilizando (ii), pois

$$\sum_{x \in X} d(x) = \sum_{x \in X} (d^+(x) + d^-(x)) = \sum_{x \in X} d^+(x) + \sum_{x \in X} d^-(x) = 2m,$$

ou observando que para qualquer multigrafo, orientado ou não, cada arco tem duas extremidades (que podem ser iguais, no caso dos laços) e, portanto, por cada arco existe uma parcela igual a 2 no somatório $\sum_{x \in X} d(x)$. □

A afirmação (i) do Teorema anterior é conhecida por **Teorema do aperto de mãos**. Tal é devido ao paralelo com a seguinte situação:

Suponhamos que n pessoas se encontram numa reunião social e que algumas se cumprimentam com um aperto de mãos. Tal situação pode ser representada por um grafo simples em que as pessoas são representadas pelos vértices e em que existe um arco incidente em x_i e x_j, com $i \neq j$, se, e só se, as pessoas correspondentes a tais vértices se cumprimentam com um aperto de mãos. Neste caso o grau de um vértice x representa o número de pessoas que a pessoa correspondente a x cumprimentou apertando a mão e a igualdade (i) do Teorema afirma, então, que a soma do número de pessoas que cada um dos n presentes na reunião cumprimentou é igual ao dobro do número de mãos.

Proposição 8.10 *Num multigrafo, orientado ou não, $G = (X,\ \mathcal{U})$ é sempre par o número de vértices de G que têm grau ímpar.*

Demonstração Sejam m o número de arcos de G,

$$X_1 = \{x \in X :\ d(x) \text{ é ímpar}\}$$

e

$$X_2 = \{x \in X :\ d(x) \text{ é par}\}.$$

Tem-se,

$$\sum_{x \in X} d(x) = \sum_{x \in X_1} d(x) + \sum_{x \in X_2} d(x) = 2m.$$

Como $2m$ e $\sum_{x \in X_2} d(x)$ são números pares, concluímos que $\sum_{x \in X_1} d(x)$ é par.

Dado que a paridade da soma de $k = |X_1|$ números ímpares é a paridade de k, concluímos que $k = |X_1|$ é um número par. Como $|X_1|$ é o número de vértices de G com grau ímpar, tem-se o resultado pretendido. □

Definição 8.11 *Define-se* **sequência de graus** *de um multigrafo não orientado (respectivamente, multigrafo orientado) G, com n vértices, como sendo a sequência*

$$(d_1,\ d_2, \ldots,\ d_n),$$

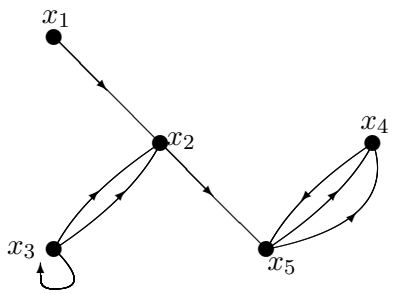
não crescente, isto é, com

$$d_1 \geq d_2 \geq \ldots \geq d_n,$$

cujos elementos são os graus dos vértices de G.

Observação No caso dos multigrafos orientados define-se de forma análoga os conceitos de **sequência de graus exteriores** e **sequência de graus interiores**.

Exemplo 8.12 *Consideremos o multigrafo orientado do exemplo anterior,*



Como foi visto,

$$d^+(x_1) = 1 \quad , \quad d^-(x_1) = 0$$
$$d^+(x_2) = 1 \quad , \quad d^-(x_2) = 3,$$
$$d^+(x_3) = 3 \quad , \quad d^-(x_3) = 1,$$
$$d^+(x_4) = 1 \quad , \quad d^-(x_4) = 2,$$
$$d^+(x_5) = 2 \quad , \quad d^-(x_5) = 2.$$

Então,

a sua sequência de graus é $(4,\ 4,\ 4,\ 3,\ 1)$*,*
a sua sequência de graus interiores é $(3,\ 2,\ 2,\ 1,\ 0)$*,*
a sua sequência de graus exteriores é $(3,\ 2,\ 1,\ 1,\ 1)$*.*

Definição 8.13 *Uma sequência de inteiros não negativos* $(d_1,\ d_2, \ldots,\ d_n)$*, com* $d_1 \geq d_2 \geq \ldots \geq d_n$*, diz-se uma* **sequência gráfica** *se existir um* **grafo simples** *cuja sequência de graus seja* $(d_1,\ d_2, \ldots,\ d_n)$*.*

Proposição 8.14 *Se* $(d_1,\ d_2, \ldots,\ d_n)$ *é uma sequência gráfica então* $(d_1,\ d_2, \ldots,\ d_n)$ *são inteiros tais que:*

(i) $0 \leq d_i \leq n-1$*, para todo o* $i \in \{1, \ldots, n\}$*,*

(ii) $\sum_{i=1}^{n} d_i$ *é um número par.*

As condições (i) e (ii) anteriores são, pois, condições necessárias para que uma sequência de inteiros, ordenada por ordem não crescente, seja uma sequência gráfica, mas não são em geral, condições suficientes. Tal verifica-se somente para $n = 1$ e $n = 2$.

Para $n = 1$ a única sequência nas condições pretendidas é a sequência (0) que é gráfica, pois o grafo simples

G

admite-a como sequência de graus.

Para $n = 2$ as únicas sequências gráficas que satisfazem (i) e (ii) simultaneamente são as sequências $(0,\ 0)$ e $(1,\ 1)$ que também são gráficas,

G G

Para os casos em que se tem $n \geq 3$ é válido o seguinte resultado:

Proposição 8.15 *Para $n \geq 3$ existem sequências não crescentes $(d_1,\ d_2, \ldots,\ d_n)$ de inteiros verificando as condições* (i) *e* (ii) *da Proposição anterior e que não são gráficas.*

Demonstração Considere-se $d_1 = n-1$ e $d_n = 0$. Se n é par tome-se $d_2 = 1$ e os restantes elementos da sequência iguais a zero. Se n é ímpar, considerem-se os restantes elementos da sequência nulos.

Finalmente concluímos que não existe nenhum grafo simples que tenha qualquer uma das sequências anteriores como sequência de graus. Se um tal grafo simples existisse teria n vértices sendo, pelo menos, um de grau $n-1$ e, portanto, adjacente a todos os outros. Mas, então, em tal grafo não existiriam vértices de grau zero. □

Proposição 8.16 *Num grafo simples, com $n \geq 2$ vértices, existem pelo menos dois vértices com o mesmo grau.*

Demonstração Se não existissem dois vértices com o mesmo grau, a sequência de graus do grafo seria

$$(n-1,\ n-2, \ldots,\ 1,\ 0),$$

que não é uma sequência gráfica. □

O Teorema seguinte permite-nos decidir se uma dada sequência é ou não gráfica e, em caso afirmativo, indicar grafos simples que a admitam como sequência de graus.

Teorema 8.17 *A sequência de inteiros não negativos*

$$S: \qquad d_1,\ d_2, \ldots,\ d_n$$

com $d_1 \geq d_2 \geq \ldots \geq d_n$, $n \geq 2$ *e* $d_1 \geq 1$ *é uma sequência gráfica se, e só se, a sequência*

$$S': \qquad d_2 - 1, \ldots,\ d_{d_1+1} - 1,\ d_{d_1+2}, \ldots,\ d_n$$

(depois de ordenada por ordem não crescente) é uma sequência gráfica.

Demonstração Suponhamos que S' é uma sequência gráfica e seja G' é um grafo simples cuja sequência de graus é S'. Sejam $x_2, \ldots, x_n$ os vértices de G' e considere-se que

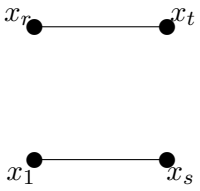
$$d_{G'}(x_i) = \begin{cases} d_i - 1 & \text{se } 2 \leq i \leq d_1 + 1 \\ d_i & \text{se } d_1 + 2 \leq i \leq n. \end{cases}$$

Seja G um grafo que se obtenha de G' acrescentando um novo vértice x_1 e os d_1 arcos $\{x_1,\ x_i\}$, para $2 \leq i \leq d_1 + 1$. G é um grafo simples cuja sequência de graus é S e, portanto, S é uma sequência gráfica.

Reciprocamente, suponhamos que S é uma sequência gráfica. De entre os grafos simples cuja sequência de graus é S, seja G um grafo com conjunto de vértices $X = \{x_1,\ x_2, \ldots,\ x_n\}$, $d(x_i) = d_i$, para $i = 1,\ 2, \ldots,\ n$, e tal que a soma dos graus dos vértices adjacentes a x_1 é máxima.

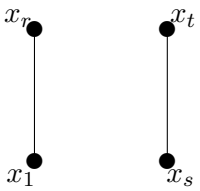
Demonstremos, primeiro que os vértices adjacentes a x_1, cujo número é d_1, têm graus $d_2,\ d_3, \ldots,\ d_{d_1+1}$.

Caso tal não suceda, existem vértices x_r e x_s, com $d_r > d_s$, tal que x_1 não é adjacente a x_r mas é adjacente a x_s. Dado que o grau de x_r é superior ao grau de x_s, podemos afirmar que existe um vértice x_t tal que x_r é adjacente a x_t, mas x_s não é adjacente a x_t.



, com $d_r > d_s$

Eliminando em G os arcos $\{x_1,\ x_s\}$ e $\{x_r,\ x_t\}$ e acrescentando os arcos $\{x_1,\ x_r\}$ e $\{x_s,\ x_t\}$,



obtemos um garfo G' cuja sequência de graus é, ainda S. Contudo, como $d_r > d_s$, em G' a soma dos graus dos vértices adjacentes a x_1 é superior à correspondente soma em G, o que contradiz a escolha de G.

Logo, em G, os vértices adjacentes a x_1 têm graus $d_2,\ d_3, \ldots,\ d_{d_1+1}$, conforme se pretendia demonstrar.

Eliminando em G o vértice x_1, e obviamente os arcos nele incidentes, obtemos um grafo simples cuja sequência de graus é a sequência que se obtém ordenando S' por ordem não crescente. □

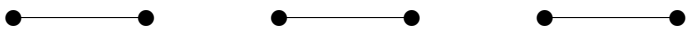
Exemplo 8.18 *Determinemos se a sequência* $(6,\ 5,\ 5,\ 4,\ 3,\ 3,\ 2,\ 2,\ 2)$ *é uma sequência gráfica.*

Tem-se:

$$
\begin{array}{ll}
S_1 : & 6,\ \underline{5,\ 5,\ 4,\ 3,\ 3,\ 2,}\ 2,\ 2 \\
S_1' : & 4,\ 4,\ 3,\ 2,\ 2,\ 1,\ 2,\ 2 \\
S_2 : & 4,\ \underline{4,\ 3,\ 2,\ 2,}\ 2,\ 2,\ 1 \\
S_2' : & 3,\ 2,\ 1,\ 1,\ 2,\ 2,\ 1 \\
S_3 : & 3,\ \underline{2,\ 2,\ 2,}\ 1,\ 1,\ 1 \\
S_3' : & 1,\ 1,\ 1,\ 1,\ 1,\ 1
\end{array}
$$

em que de S_i *para* S_i', $i \in \{1,\ 2,\ 3\}$, *se aplicou o Teorema e de* S_i' *para* S_{i+1}, $i \in \{1,\ 2\}$, *se ordenou a sequência por ordem não crescente. Embora possamos continuar a aplicar o Teorema, concluímos facilmente, que* S_3' *é uma sequência gráfica, pois um grafo simples da forma*

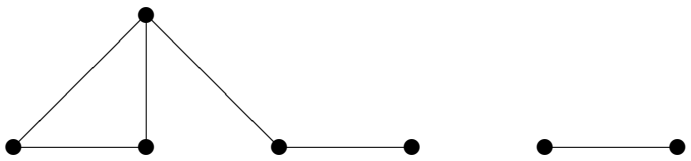
G'



tem S_3' *como sequência de graus.*

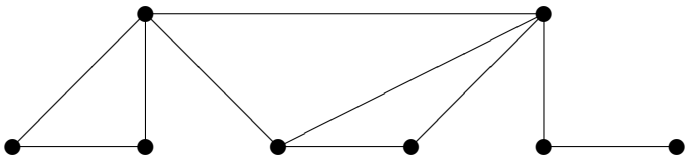
Atendendo à primeira parte da demonstração do Teorema, podemos construir um grafo simples G_3 *cuja sequência de graus é* S_3. *Teremos de acrescentar um novo vértice ao grafo e torná-lo adjacente a* 3 *vértices de grau* 1.

G_3



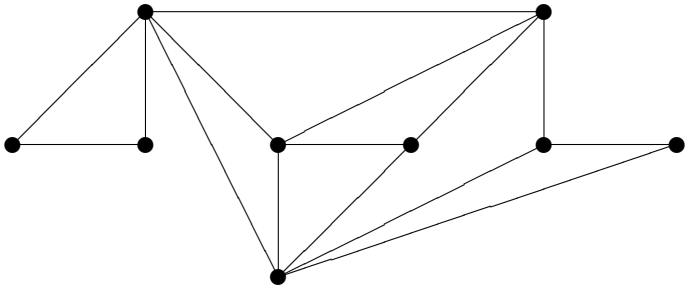
Acrescentando um novo vértice a G_3 *e tornando tal vértice adjacente a* 4 *vértices, nomeadamente ao vértice com grau* 3, *a um dos de grau* 2 *e a dois vértices com grau* 1, *obtemos um grafo cuja sequência de graus é* S_2.

G_2



Procedendo de forma análoga, concluímos que o grafo

G_1

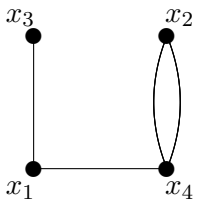


tem sequência de graus S_1.

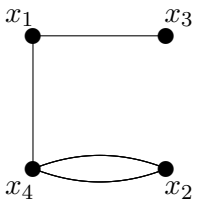
8.4 Isomorfismo de grafos

Dois multigrafos podem parecer diferentes, mas representarem o mesmo multigrafo. É o caso dos multigrafos G_1 e G_2,

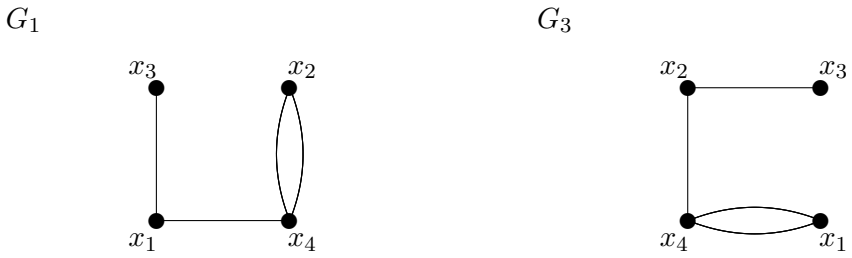
G_1



G_2



No entanto pode acontecer dois multigrafos parecerem semelhantes e representarem multigrafos distintos. É o caso dos multigrafos G_1 e G_3 (enquanto que em G_1 os vértices x_1 e x_3 são adjacentes, em G_3 não o são),



Expressamos esta semelhança dizendo que os multigrafos são **isomorfos**.

Definição 8.19 *Sejam $H_1 = (X_1,\ \mathcal{U}_1)$ e $H_2 = (X_2,\ \mathcal{U}_2)$ multigrafos não orientados (respectivamente, multigrafos orientados). Diz-se que H_1 é* **isomorfo** *a H_2 se existe uma aplicação bijectiva*

$$\varphi :\ X_1 \longrightarrow X_2$$

tal que, para quaisquer x_i e $x_j \in X_1$, o número de arcos incidentes, em H_1, nestes dois vértices (respectivamente, com extremidade inicial em x_i e extremidade final em x_j) seja igual ao número de arcos incidentes, no multigrafo H_2, em $\varphi(x_i)$ e $\varphi(x_j)$ (respectivamente, com extremidade inicial em $\varphi(x_i)$ e extremidade final em $\varphi(x_j)$).

Proposição 8.20 *A relação de isomorfismo de multigrafos não orientados (respectivamente, multigrafos orientados) é uma relação de equivalência.*

Observação

1. Atendendo à simetria da relação de isomorfismo de multigrafos (respectivamente, multigrafos orientados) podemos escrever "H_1 e H_2 são isomorfos".

2. Se $H_1 = (X_1,\ \mathcal{U}_1)$ e $H_2 = (X_2,\ \mathcal{U}_2)$ são multigrafos isomorfos, através da bijecção φ, então
$$d_{H_1}(x) = d_{H_2}(\varphi(x)), \qquad \forall x \in X_1.$$

Exemplo 8.21 *1. Os multigrafos G_1 e G_3 do exemplo que temos vindo a considerar nesta secção são isomorfos pois, sendo $X = \{x_1,\ x_2,\ x_3,\ x_4\}$ o conjunto dos vértices de G_1 e de G_3, a correspondência*

$$\varphi :\ X \longrightarrow X$$

tal que $\varphi(x_1) = x_2$, $\varphi(x_2) = x_1$, $\varphi(x_3) = x_3$, $\varphi(x_4) = x_4$ é uma bijecção que verifica

- *O número de arcos incidentes em x_1 e x_2, em G_1, é zero e é igual ao número de arcos incidentes em $\varphi(x_1) = x_2$ e $\varphi(x_2) = x_1$, em G_3.*
- *O número de arcos incidentes em x_1 e x_3, em G_1, é um e é igual ao número de arcos incidentes em $\varphi(x_1) = x_2$ e $\varphi(x_3) = x_3$, em G_3.*
- *O número de arcos incidentes em x_1 e x_4, em G_1, é um e é igual ao número de arcos incidentes em $\varphi(x_1) = x_2$ e $\varphi(x_4) = x_4$, em G_3.*
- *O número de arcos incidentes em x_2 e x_3, em G_1, é zero e é igual ao número de arcos incidentes em $\varphi(x_2) = x_1$ e $\varphi(x_3) = x_3$, em G_3.*
- *O número de arcos incidentes em x_2 e x_4, em G_1, é dois e é igual ao número de arcos incidentes em $\varphi(x_2) = x_1$ e $\varphi(x_4) = x_4$, em G_3.*
- *O número de arcos incidentes em x_3 e x_4, em G_1, é zero e é igual ao número de arcos incidentes em $\varphi(x_3) = x_3$ e $\varphi(x_4) = x_4$, em G_3.*

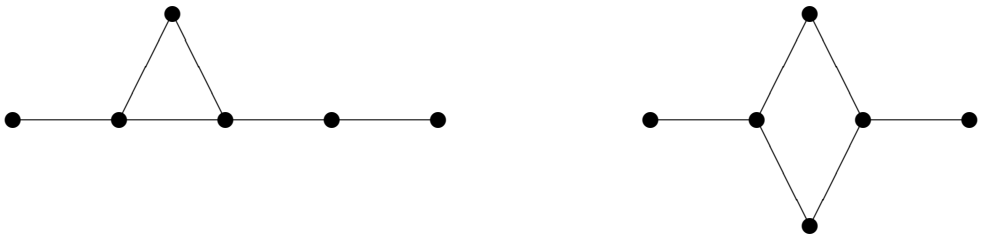
2. Os grafos simples

são isomorfos.

Proposição 8.22 *Multigrafos não orientados isomorfos(respectivamente, multigrafos orientados) têm sequências de graus iguais.*

A reciproca da Proposição anterior é falsa. Os grafos

G_1 G_3

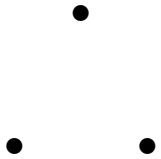


têm a mesma sequência de graus, (3, 3, 2, 2, 1, 1), mas não são isomorfos. Basta atender a que os dois vértices de grau 3 de G_1 são adjacentes, mas o mesmo não sucede aos dois únicos vértices de grau 3 de G_2.

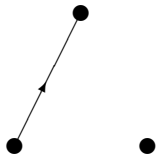
Observação Multigrafos orientados isomorfos, têm a mesma sequência de graus exteriores e a mesma sequência de graus interiores.

Existem 16 digrafos, dois a dois não isomorfos, com 3 vértices:

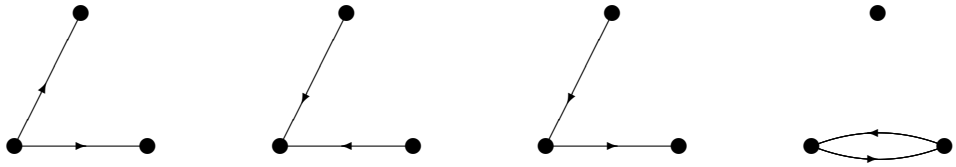
$m = 0$



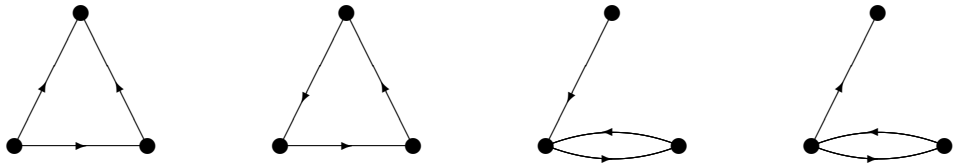
$m = 1$



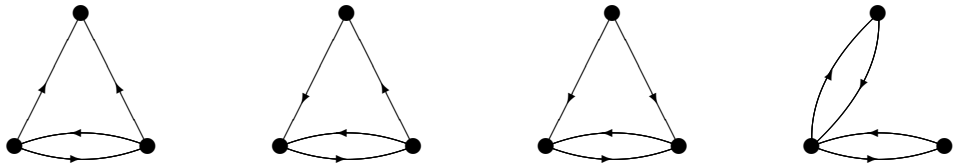
$m = 2$



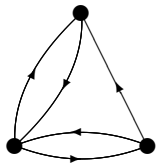
$m = 3$

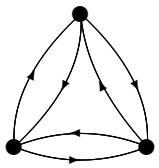


$m = 4$



$m = 5$



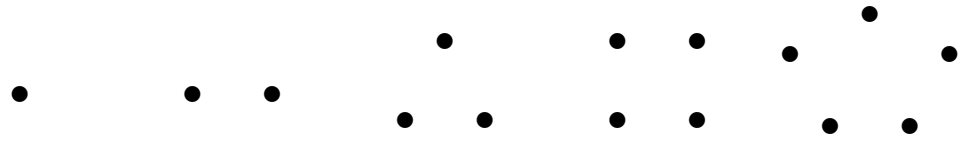
$m = 6$ 

8.5 Exemplos de grafos

Nesta secção veremos alguns grafos importantes.

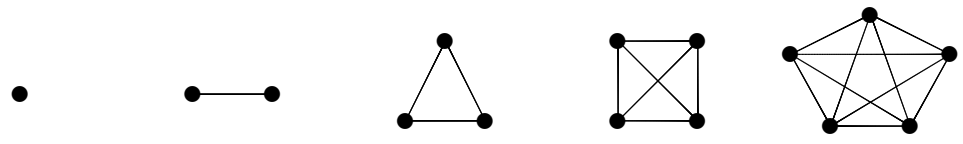
Seja $G = (X,\ \mathcal{U})$ um grafo simples. Se existe $r \in \mathbb{N}_0$ tal que, $d_G(x) = r$, para todo o $x \in X$, dizemos que G é um **grafo regular de grau r** ou r-regular.

Um grafo simples regular de grau 0, isto é, com todos os vértices isolados, diz-se um **grafo nulo** e representa-se por, no caso de ter n vértices, N_n.



N_1 N_2 N_3 N_4 N_5

Um grafo simples, com n vértices, regular de grau $n-1$, diz-se um **grafo completo** e representa-se por K_n. Este grafo tem $\binom{n}{2} = \frac{n(n-1)}{2}$ arcos, conforme se verifica aplicando o Teorema do aperto de mãos.



K_1 K_2 K_3 K_4 K_5

Proposição 8.23 *Não existem grafos regulares de grau ímpar com um número par de vértices.*

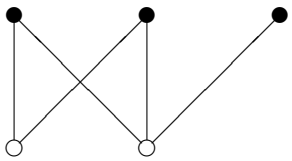
Demonstração Se $G = (X,\ \mathcal{U})$ é um grafo regular de grau r com n vértices e m arcos, então pelo Teorema do aperto de mãos tem-se

$$\sum_{x \in X} d_G(x) = rn = 2m.$$

Como o produto de dois números ímpares é ímpar, concluímos que r e n não podem ser simultaneamente ímpares. □

Diz-se que um grafo $G = (X,\ \mathcal{U})$, simples, é **bipartido**, com classes de vértices X_1 e X_2, se $\{X_1,\ X_2\}$ é uma partição de X e cada arco de G tem extremidade num elemento de X_1 e a outra extremidade num elemento de X_2. A notação utilizada é $G = (X_1 \cup X_2,\ \mathcal{U})$.

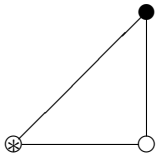
O grafo simples $G = (X_1 \cup X_2,\ \mathcal{U})$, em que os elementos de X_1 são os vértices brancos e os elementos de X_2 são os vértices pretos,



é um grafo bipartido.

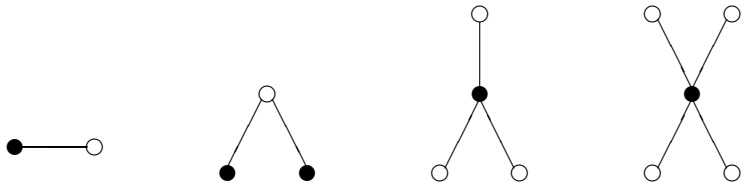
Um grafo simples $G = (X,\ \mathcal{U})$ diz-se **p-partido**, com classes de vértices $X_1, \ldots X_p$, se $\{X_1, \ldots,\ X_p\}$ é uma partição de X e nenhum elemento de $\mathcal{U}$ tem ambas as extremidades em elementos da mesma classe.

O grafo simples $G = (X_1 \cup X_2 \cup X_3,\ \mathcal{U})$, em que o elemento de X_1 é o vértice branco, o elemento de X_2 é o vértice preto e o elemento de X_3 é o vértice asterístico



é um grafo 3-partido.

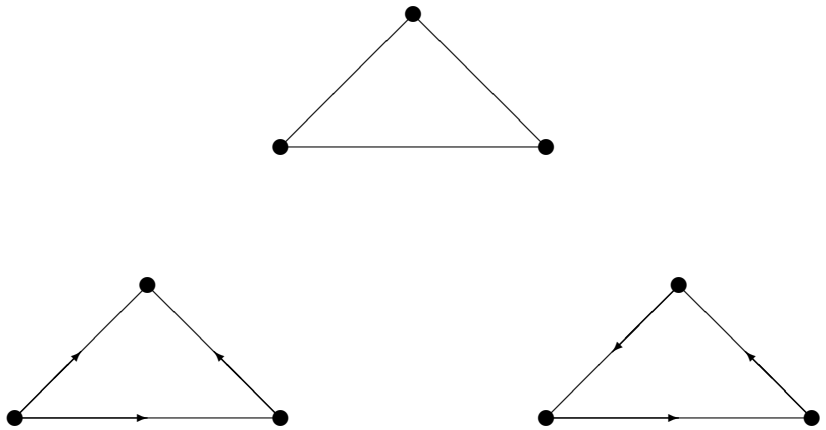
Um grafo p-partido, com $p \geq 2$, em que existe um arco unindo todo o par de vértices pertencentes a classes de vértices distintas diz-se um **grafo p-partido completo**. Se o grafo tiver $n_1, \ldots, n_p$ elementos nas classes, representá-lo-emos por $K_{n_1,\ldots,n_p}$. De entre este destacamos os $K_{1,n-1}$ que são os **grafos estrelas**.



$K_{1,1}$ $K_{1,2}$ $K_{1,3}$ $K_{1,4}$

Seja $G = (X,\ \mathcal{U})$ um grafo simples completo, com $n \geq 2$ vértices. Chamamos **torneio** ao digrafo resultante da orientação de G.

Só há dois torneios do K_3:



Diz-se que $G' = (X',\ \mathcal{U}')$ é **subgrafo** do grafo orientado (respectivamente, não orientado) $G = (X,\ \mathcal{U})$ se $X \subseteq X'$ e $\mathcal{U}' \subseteq (X' \times X') \cap \mathcal{U}$ (respectivamente, $\mathcal{U}' \subseteq (X' \otimes X') \cap \mathcal{U}$).

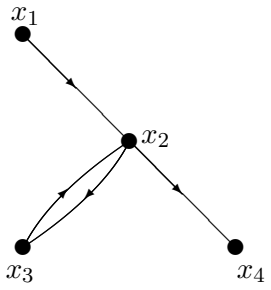
De entre os subgrafos temos que destacar:

Seja $G = (X,\ \mathcal{U})$ um grafo. Um grafo $G' = (X,\ \mathcal{U}')$ com $\mathcal{U}' \subseteq \mathcal{U}$ diz-se um **grafo parcial** de G. G' obtém-se de G eliminando em $\mathcal{U}$ os arcos pertencentes a $\mathcal{U}'' = \mathcal{U} \setminus \mathcal{U}'$, pelo que pode representar-se por $G - \mathcal{U}''$.

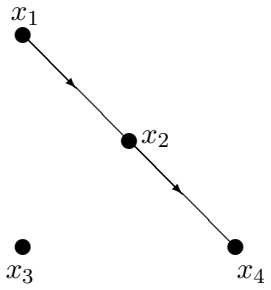
Se $G' = (X',\ \mathcal{U}')$ é um subgrafo de $G = (X,\ \mathcal{U})$ com $\mathcal{U}' \subseteq (X' \otimes X') \cap \mathcal{U}$ (se G não é orientado) ou $\mathcal{U}' \subseteq (X' \times X') \cap \mathcal{U}$ (se G é orientado), dizemos que G' é o **subgrafo de** G **gerado por** X'. Sendo $X'' = X \setminus X'$ representamos G' por $G - X''$.

Se $G = (X,\ \mathcal{U})$ é um grafo orientado (respectivamente, não orientado) e $\mathcal{U}'' \subseteq (X \times X) \setminus \mathcal{U}$ (respectivamente, $\mathcal{U}'' \subseteq (X \otimes X) \setminus \mathcal{U}$) representamos por $G + \mathcal{U}''$ o grafo $(X,\ \mathcal{U} \cup \mathcal{U}'')$.

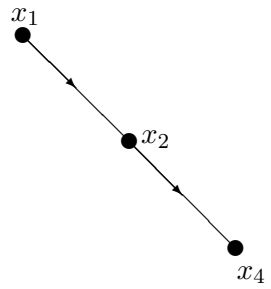
Exemplo 8.24 *Consideremos o digrafo* $G = (X,\ \mathcal{U})$



O digrafo



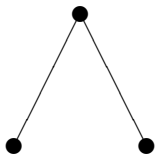
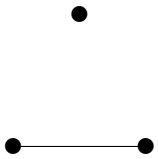
é um grafo parcial de G.
O digrafo



é o subgrafo de G *gerado por* $\{x_1,\ x_2,\ x_4\}$, *que se denota por* $G - \{x_3\}$.

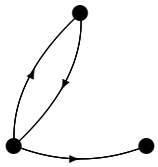
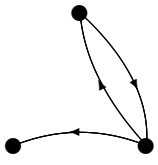
Seja $G = (X,\ \mathcal{U})$ um grafo simples. Chama-se **grafo complementar** de G e representa-se por $\overline{G}$, o grafo simples $\overline{G} = (X,\ \overline{\mathcal{U}})$ em que $\overline{\mathcal{U}} = (X \otimes X) \setminus \mathcal{U}$.

Exemplo 8.25 *Sendo*

G  $\overline{G}$ 

Seja $G = (X, \mathcal{U})$ um digrafo. Chama-se **grafo complementar** de G e representa-se por $\overline{G}$, o digrafo $\overline{G} = (X, \overline{\mathcal{U}})$ em que $\overline{\mathcal{U}} = (X \times X) \setminus \mathcal{U}$.

Exemplo 8.26 *Sendo*

G  $\overline{G}$ 

Capítulo 9

Conexidade de grafos

9.1 Noção de cadeia. Componentes conexas

Muitas das aplicações da teoria de grafos falam "ir de um vértice para outro" num grafo. Por exemplo, qual o caminho mais curto entre Lisboa e Porto? Começamos por precisar este conceito através de definições.

Definição 9.1 *Num multigrafo não orientado (respectivamente, multigrafo orientado)* $G = (X,\ \mathcal{U})$ *chama-se* **cadeia** *a uma sequência alternada de vértices e arcos de* G*, iniciada e terminada num vértice, tal que cada arco tem extremidade no vértice que imediatamente o precede na sequência e a outra extremidade no vértice que imediatamente o sucede na sequência.*

Trata-se, pois, de uma sequência da forma

$$L: \qquad x_0,\ u_1,\ x_1,\ u_2, \ldots,\ u_r,\ x_r$$

com $u_i \in \mathcal{U}$*,* $i \in \{1, \ldots r\}$*,* $x_j \in X$*,* $j \in \{0,\ 1, \ldots,\ r\}$ *e em que* $u_i = \{x_{i-1},\ x_i\}$ *(respectivamente,* $u_i = (x_{i-1},\ x_i)$ *ou* $u_i = (x_i,\ x_{i-1})$*),* $i \in \{1, \ldots,\ r\}$*.*

O vértice x_0 *diz-se o* **vértice inicial** *da cadeia* L *e o vértice* x_r *o seu* **vértice final**. *Diz-se que* x_0 *e* x_r *são as* **extremidades** *da cadeia* L*.*

Designamos, frequentemente, por cadeia $x_0 - x_r$ *uma cadeia cujo vértice inicial é* x_0 *e o vértice final é* x_r*.*

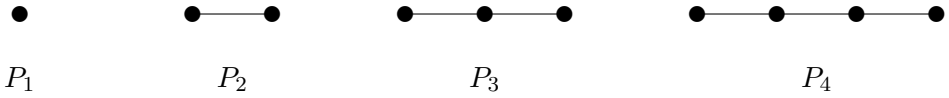
Uma cadeia cujas extremidades são iguais diz-se uma **cadeia fechada**, *caso contrário, diz-se uma* **cadeia aberta**. *O número de arcos de uma cadeia diz-se o seu* **comprimento**.

De acordo com as definições dadas, se $x \in X$*, então* x *é uma cadeia* $x - x$ *de comprimento zero. As cadeias de comprimento zero designam-se por* **cadeias triviais** *e as de comprimento não nulo por* **cadeias não triviais**.

Uma cadeia diz-se **simples** *se todos os arcos da cadeia são distintos e diz-se* **elementar** *se todos os vértices da cadeia são distintos, à excepção das extremidades que podem coincidir no caso da cadeia ser fechada.*

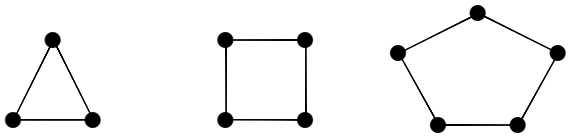
Uma cadeia simples, fechada e não trivial diz-se um **ciclo**

Um grafo simples com n vértices, sem vértices isolados e formado por uma única cadeia elementar aberta, que contenha todos os seus vértices, diz-se um **grafo cadeia** e denota-se por P_n.



P_1 P_2 P_3 P_4

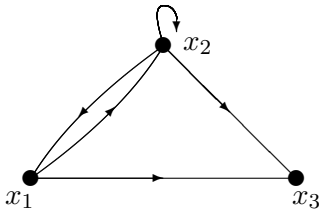
Um grafo simples com n vértices, regular de grau 2, formado por um único ciclo diz-se um **grafo ciclo** e denota-se por C_n.



C_3 C_4 C_5

Exemplo 9.2 *No grafo orientado*

G



x_2, $(x_2,\ x_2)$, x_2 *é um* **ciclo** *de comprimento* 1.

x_1, $(x_1,\ x_2)$, x_2, $(x_1,\ x_2)$, x_1 *é uma cadeia não trivial, fechada que é elementar mas não é simples.*

Observação Num multigrafo, uma cadeia fica completamente determinada se indicarmos a subsequência dos seus vértices.

Definição 9.3 *Um multigrafo $G = (X, \mathcal{U})$ (orientado ou não) diz-se* **conexo** *se para quaisquer vértices x_i e x_j existe, em G, uma cadeia $x_i - x_j$. Caso contrário diz-se* **desconexo**.

Seja $G = (X, \mathcal{U})$ um multigrafo e R a relação binária, definida em X, por

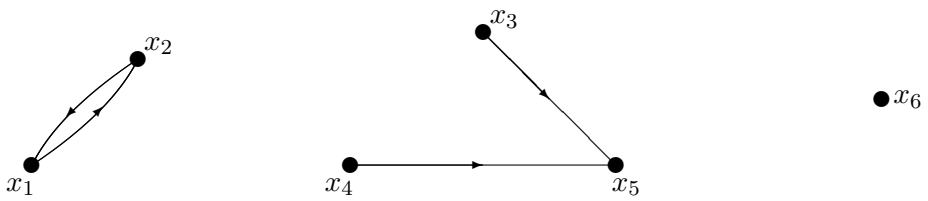
$$x_i R x_j \qquad \text{se, e só se,} \qquad \text{existe em } G \text{ uma cadeia } x_i - x_j.$$

Proposição 9.4 *R é uma relação de equivalência.*

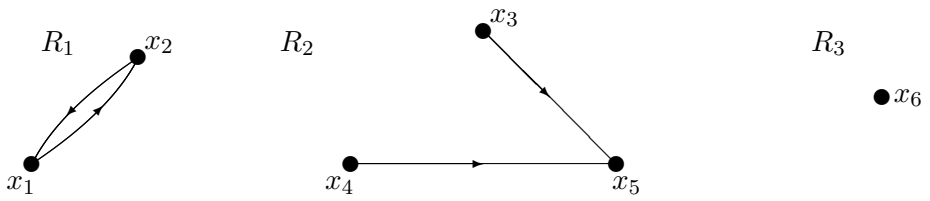
A relação de equivalência R origina uma partição de X em classes $X_1, \ldots, X_p$ cujo número p se designa por **número de conexidade** de G.

Os subgrafos de G, gerados respectivamente por $X_1, \ldots, X_p$ dizem-se as **componentes conexas** de G e representam-se por $R_1, \ldots, R_p$.

Exemplo 9.5 *Consideremos o grafo orientado $G = (X, \mathcal{U})$*



A relação de equivalência R origina uma partição de X em 3 classes
$X_1 = \{x_1,\ x_2\}$,
$X_2 = \{x_3,\ x_4,\ x_5\}$,
$X_3 = \{x_6\}$.
As componentes conexas de G são os grafos



e o número de conexidade de G é 3.

9.2 Resultados sobre conexidade

Restringindo-nos aos grafos simples, existem como veremos propriedades dos grafos que se tornam mais fáceis de demonstrar quando os mesmos são conexos. Se o grafo inicial não for conexo, basta pensarmos em cada uma das suas componentes conexas.

Proposição 9.6 *Num grafo simples $G = (X,\ \mathcal{U})$ existe uma cadeia $x_0 - x_r$ se, e só se, existe uma cadeia $x_0 - x_r$ elementar.*

Demonstração $\Longrightarrow$ Se $x_0 = x_r$, a cadeia trivial x_0 é elementar. Suponhamos que $x_0 \neq x_r$. Seja L uma cadeia $x_0 - x_r$ e x um vértice arbitrário de L. Se x ocorre mais do que uma vez na cadeia L então elimine-se a subsequência de L compreendida entre a primeira e a última ocorrência de x, bem como uma dessas ocorrências. Obtém-se, ainda, uma cadeia $x_0 - x_r$, mas em que x já não aparece repetido.

Repita-se este procedimento para todo o vértice que ocorra repetido em L. Obtém-se então uma cadeia sem vértices repetidos e, portanto, uma cadeia $x_0 - x_r$ elementar.

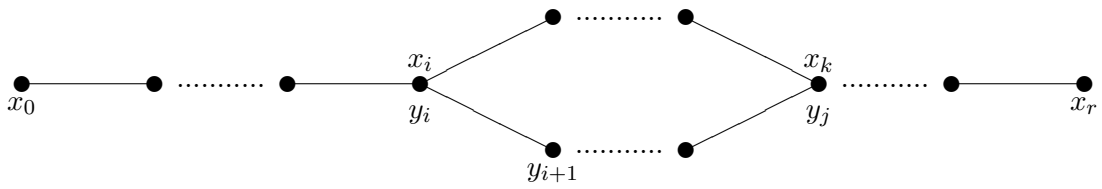
$\Longleftarrow$ Imediato. □

Proposição 9.7 *Seja $G = (X,\ \mathcal{U})$ um grafo simples e $x_0,\ x_r$ vértices distintos de G. Se em G existem duas cadeias $x_0 - x_r$ elementares distintas, então em G, existe um ciclo.*

Demonstração Sejam

$$L_1 : \quad x_0,\ x_1,\ x_2, \ldots,\ x_r \qquad \text{e} \qquad L_2 : \quad x_0,\ y_1,\ y_2, \ldots,\ x_r$$

duas cadeias $x_0 - x_r$ elementares distintas, existentes em G. Seja i o índice mínimo para o qual $x_{i+1} \neq y_{i+1}$ e j o índice mínimo tal que $j > i$ e y_j é vértice de L_1, isto é, $y_j = x_k \in L_1$.



Então,

$$x_i,\ x_{i+1}, \ldots,\ x_k,\ y_{j-1}, \ldots,\ y_{i+1},\ y_i$$

é um ciclo de G. □

Proposição 9.8 *Seja $G = (X,\ \mathcal{U})$ um grafo simples, sem ciclos. Se $u \in (X \otimes X) \setminus \mathcal{U}$ então $G + u$ tem, no máximo, um ciclo.*

Demonstração Suponhamos que em $G + u$ existiam pelo menos dois ciclos e sejam C_1 e C_2 dois desses ciclos. Se o arco u não pertencesse aos dois ciclos, então concluiríamos que $(G + u) - u = G$ tinha um ciclo, o que é impossível.

Portanto, $u = \{x,\ y\}$ é arco de C_1 e de C_2. Então existiam duas cadeias $x-y$ elementares distintas, não incluindo o arco u. Consequentemente, estas cadeias existiam também em G. Mas isto implicaria que G tinha um ciclo, o que é impossível.

Portanto, em $G + u$ existe, no máximo, um ciclo. □

Teorema 9.9 *Um grafo simples, com $n \geq 2$ vértices, é bipartido se, e só se, não tem ciclos de comprimento ímpar.*

Demonstração Vamos fazer a demonstração para o caso do grafo ser conexo.

Seja $G = (X,\ \mathcal{U})$ um grafo conexo, com classes de vértices X_1 e X_2. Seja

$$C: \qquad x_0,\ x_1,\ x_2, \ldots,\ x_{k-1},\ x_0$$

um ciclo de comprimento k, de G. Como G é bipartido, se $x_0 \in X_1$, $x_1 \in X_2$, ..., pelo que $x_{k-1} \in X_2$, ou seja, $k - 1$ é ímpar e k é par. logo, C tem comprimento par.

Reciprocamente, suponhamos que G é um grafo conexo que não tem ciclos de comprimento ímpar e demonstremos que G é bipartido. Seja x um vértice de G. Consideremos

$$X_1 = \{y \in X :\ d(x,\ y) \text{ é ímpar}\}$$

e

$$X_2 = \{y \in X :\ d(x,\ y) \text{ é par}\}$$

em que $d(x,\ y)$ é o menor comprimento das cadeias $x - y$.

É evidente que $x \in X_2$. Vejamos que G é bipartido, com as classes de vértices X_1 e X_2.

Suponhamos que existiam $z,\ w \in X_2$ (ou em X_1) tais que $\{z,\ w\} \in \mathcal{U}$. Seja $L_{x,z}$ uma cadeia $x - z$ de comprimento $d(x,\ z)$ e $L_{x,w}$ uma cadeia $x - w$ de comprimento $d(x,\ w)$. As cadeias $L_{x,z},\ L_{x,w}$ têm pelo menos um vértice em comum, x. Da esquerda para a direita, seja s o último vértice comum a $L_{x,z}$ e $L_{x,w}$. Como as cadeias $s - z$, $s - w$ têm a mesma paridade então,

$$s - z,\ \{z,\ w\},\ w - s$$

é um ciclo de comprimento ímpar. O que contradiz a hipótese. Logo, G é bipartido.

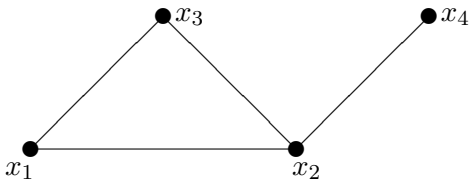
Se G não é conexo, então se G é o grafo nulo, como $n \geq 2$, G é bipartido. Se G não é nulo, sejam $R_1, \ldots,\ R_k$ as componentes conexas não nulas de G. Pelo que já foi demonstrado, R_i é um grafo bipartido, $i = 1, \ldots, k$. Sejam Y_i e Z_i as classes de vértices de R_i, $i = 1, \ldots, k$, definidas como anteriormente. Considerando

$$Y = Y_1 \cup \ldots \cup Y_k \cup Y' \qquad \text{e} \qquad Z = Z_1 \cup \ldots \cup Z_k$$

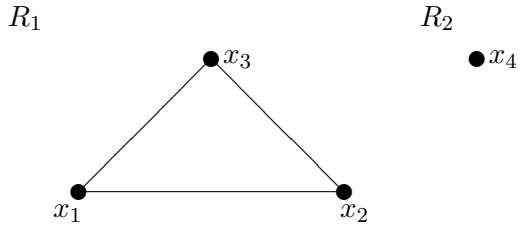
em que $Y' = \{a \in X :\ d(a) = 0\}$, então G é bipartido com classes de vértices Y e Z. □

Definição 9.10 *Seja $G = (X,\ \mathcal{U})$ um grafo simples. Diz-se que $u \in \mathcal{U}$ é uma* **ponte** *de G se o número de conexidade de $G - u$ é superior ao número de conexidade de G.*

Exemplo 9.11 *Consideremos o grafo simples conexo G*



o arco $u = \{x_2,\ x_4\}$ é uma ponte pois o grafo $G - u$ tem duas componentes conexas



Proposição 9.12 *Seja $G = (X,\ \mathcal{U})$ um grafo simples. Tem-se, $u \in \mathcal{U}$ é uma ponte se, e só se, u não faz parte de nenhum ciclo.*

Demonstração Dado que todo o arco de G tem extremidades, em vértices da mesma componente conexa, podemos supor que G é conexo.

$\Longleftarrow$ Suponhamos que $u = \{x,\ y\}$ não é ponte. Então, $G - u$ é conexo, pelo que existe uma cadeia elementar $x - y$, em $G - u$. Então,

$$x - y,\ \{x,\ y\},\ x$$

é um ciclo em G ao qual u pertence.

$\Longrightarrow$ Suponhamos que $u = \{x,\ y\}$ faz parte de um ciclo,

$$x,\ y,\ y_1, \ldots,\ y_k,\ x.$$

Sejam $x_i,\ x_j$ vértices de G, $i \neq j$. Como G é conexo, existe uma cadeia elementar $x_i - x_j$. Se u não é arco desta cadeia, então a cadeia $x_i - x_j$, é cadeia em $G - u$. Se u é arco da cadeia, então $x_i - x_j$ é cadeia

$$x_i, \ldots,\ x,\ y, \ldots,\ x_j$$

pelo que,

$$x_i, \ldots,\ x,\ y_k, \ldots,\ y_1,\ y, \ldots,\ x_j$$

também é cadeia $x_i - x_j$, só que não inclui o arco u. Portanto, cadeia em $G - u$. Logo, $G - u$ é conexo, ou seja, u não é ponte. □

Proposição 9.13 *Um grafo simples G e o seu complementar $\overline{G}$ não podem ser ambos desconexos.*

Demonstração Suponhamos que G é desconexo e vejamos que $\overline{G}$ é conexo.

Sejam $x_i,\ x_j$ dois vértices de G.

Se $x_i = x_j$, tem-se a cadeia trivial. Suponhamos que $x_i \neq x_j$. Se $\{x_i,\ x_j\}$não é arco de G, então é arco de $\overline{G}$, pelo que $x_i,\ x_j$ é cadeia $x_i - x_j$ em $\overline{G}$.

Se $\{x_i,\ x_j\}$ é arco de G, então x_i e x_j pertencem à mesma componente conexa de G. Como G é desconexo, existe um vértice x_k que não pertence à componente conexa de x_i e x_j, em G. Então, $\{x_i,\ x_k\}$ e $\{x_k,\ x_j\}$ não são arcos de G, pelo que o são de $\overline{G}$. Assim,

$$x_i,\ x_k,\ x_j$$

é cadeia $x_i - x_j$ em $\overline{G}$. Logo, $\overline{G}$ é conexo.

Se $\overline{G}$ fosse desconexo, então por um raciocínio análogo, $\overline{\overline{G}} = G$ é conexo. Logo, G e $\overline{G}$ não podem ser ambos desconexos. □

9.3 Noção de caminho. Componentes fortemente conexas

Muitas das definições que vimos neste capítulo, para um multigrafo qualquer, têm paralelo com outras que se podem estabelecer só nos multigrafos orientados. Isto é importante porque muitos dos problemas que são resolvidos através da teoria dos grafos, só se podem colocar com grafos orientados. Por exemplo, o caminho mais curto entre duas ruas de uma determinada cidade (neste problema temos de ter em linha de conta que nem todas as ruas têm os dois sentidos).

Definição 9.14 *Num multigrafo orientado $G = (X, \mathcal{U})$ chama-se* **caminho** *a uma sequência alternada de vértices e arcos de G, iniciada e terminada num vértice, tal que cada arco tem extremidade inicial no vértice que imediatamente o precede na sequência e extremidade final no vértice que imediatamente lhe sucede na sequência.*

Trata-se de uma sequência da forma

$$L: \qquad x_0,\ u_1,\ x_1,\ u_2, \ldots,\ u_r,\ x_r$$

em que $u_i = (x_{i-1},\ x_i) \in \mathcal{U}$, $i = 1, \ldots,\ r$ e $x_i \in X$, $i = 0, \ldots,\ r$.

Diz-se que x_0 (respectivamente, x_r) é o **vértice inicial** *(respectivamente,* **vértice final***) do caminho L e que L é caminho $x_0 - x_r$.*

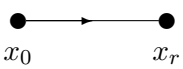
As definições de caminho fechado/aberto, comprimento de um caminho, caminho simples, caminho elementar, ..., obtêm-se substituindo, nas correspondentes definições para cadeias, "cadeia"por "caminho".

Um caminho simples, fechado e não trivial diz-se um **circuito**.

Observação

1. Se L é um caminho $x_0 - x_r$ num multigrafo orientado G então L é também uma cadeia $x_0 - x_r$.
2. Num grafo orientado pode existir um caminho $x_0 - x_r$ e não existir nenhum caminho $x_r - x_0$. Por exemplo

G



3. Num digrafo, um caminho fica completamente determinado se indicarmos apenas a subsequência dos seus vértices.

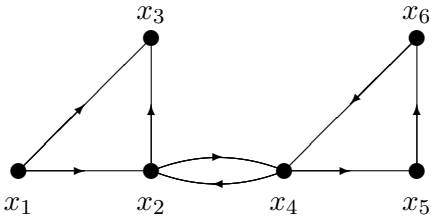
Definição 9.15 *Um multigrafo orientado $G = (X,\ \mathcal{U})$ diz-se* **fortemente conexo** *se, para quaisquer vértices $x_i,\ x_j$, existe em G um caminho $x_i - x_j$ e um caminho $x_j - x_i$.*

Seja $G = (X,\ \mathcal{U})$ um multigrafo orientado e S a relação binária, definida em X, por:

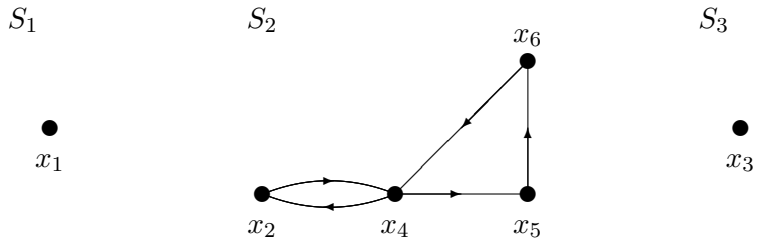
$x_i S x_j$ se, e só se, existe em G um caminho $x_i - x_j$ e um caminho $x_j - x_i$.

S é uma relação de equivalência. Sejam $X'_1, \ldots,\ X'_q$ as suas classes de equivalência. Ao número q chama-se **número de conexidade forte** de G. Os subgrafos gerados por $X'_1, \ldots,\ X'_q$ dizem-se as **componentes fortemente conexas** de G e representam-se, respectivamente, por $S_1, \ldots, S_q$.

Exemplo 9.16 *Seja $G = (X,\ \mathcal{U})$*



A relação de equivalência S, origina uma partição de X em três classes
$X'_1 = \{x_1\}$
$X'_2 = \{x_2,\ x_4,\ x_5,\ x_6\}$
$X'_3 = \{x_3\}$
e as componentes fortemente conexas de G são



Proposição 9.17 *Seja $G = (X,\ \mathcal{U})$ um multigrafo orientado. Então:*

(i) *Um arco de G pode não pertencer a nenhuma componente fortemente conexa.*

(ii) *Um arco de G não pode pertencer a mais do que uma componente fortemente conexa.*

(iii) *Um arco de G pertence a uma componente fortemente conexa se, e só se, faz parte de um circuito.*

Demonstração

(i) No grafo do exemplo anterior, o arco $(x_1,\ x_3)$ não pertence a nenhuma componente fortemente conexa.

(ii) Seja $u = (x_i,\ x_j)$ um arco de G. Como x_i pertence a uma, e uma só componente fortemente conexa, então temos o resultado.

(iii) $\Longrightarrow$ Seja $u = (x_i,\ x_j)$ um arco de G, que pertence à componente fortemente conexa S_i. Vejamos que u faz parte de um circuito.

Se $x_i = x_j$, o resultado é trivial. Suponhamos que $x_i \neq x_j$. Como S_i é um grafo fortemente conexo, existe em S_i um caminho elementar $x_j - x_i$. O arco u não pertence a este caminho, pelo que

$$x_j - x_i,\ u,\ x_j$$

é um circuito.

$\Longleftarrow$ Suponhamos que $u = (x_i,\ x_j)$ faz parte do circuito

$$x_i,\ u,\ ,\ x_j,\ u_1,\ y_1, \ldots,\ y_k,\ u_{k+1},\ x_i.$$

Então, $x_i,\ u,\ x_j$ é um caminho $x_i - x_j$, em G, e

$$x_j,\ u_1,\ y_1, \ldots,\ y_k,\ u_{k+1},\ x_i$$

é um caminho $x_j - x_i$, em G. Então u pertence a uma componente fortemente conexa. □

Proposição 9.18 *Seja G um digrafo. Se G é desconexo então o seu digrafo complementar $\overline{G}$ é fortemente conexo.*

Demonstração Suponhamos que $G = (X,\ \mathcal{U})$ é desconexo e demonstremos que, quaisquer que sejam $x_i,\ x_j \in X$, existe em $\overline{G} = (X,\ \overline{\mathcal{U}})$ um caminho $x_i - x_j$ e um caminho $x_j - x_i$.

Se $x_i = x_j$ o resultado é trivial. Suponhamos que $x_i \neq x_j$. Se $x_i,\ x_j$ não são adjacentes em G, então $(x_i,\ x_j) \notin \mathcal{U}$ e $(x_j,\ x_i) \notin \mathcal{U}$ pelo que $(x_i,\ x_j) \in \overline{\mathcal{U}}$ e $(x_j,\ x_i) \in \overline{\mathcal{U}}$. Logo, $x_i,\ x_j$ é um caminho $x_i - x_j$ em $\overline{G}$ e $x_j,\ x_i$ é um caminho $x_j - x_i$ em $\overline{G}$.

Se x_i e x_j são adjacentes em G, então pertencem à mesma componente conexa de G. Como G é desconexo, existe um vértice x_k pertencente a uma componente conexa distinta da componente a que pertencem x_i e x_j. Então, $(x_i,\ x_k)$, $(x_k,\ x_i)$, $(x_j,\ x_k)$, $(x_k,\ x_j)$ não pertencem a $\mathcal{U}$, pelo que são elementos de $\overline{\mathcal{U}}$. Mas isto implica que, $x_i,\ x_k,\ x_j$ é um caminho $x_i - x_j$, em $\overline{G}$, e $x_j,\ x_k,\ x_i$ é um caminho $x_j - x_i$, em $\overline{G}$. □

Capítulo 10

Árvores

10.1 Resultados sobre árvores

As árvores são um género de grafos muito utilizado. No capítulo anterior, conhecemos os grafos cadeia, P_n, que são conexos e verificam a seguinte propriedade: qualquer seu arco é uma ponte. Estes grafos são árvores.

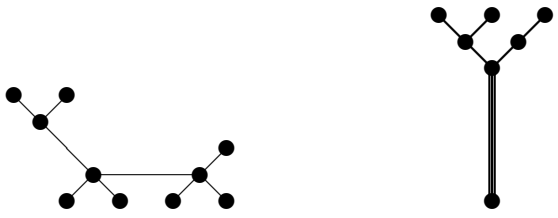
Como o próprio nome indica, quando construímos a árvore genealógica, de uma determinada família, estamos a construir um grafo que é uma árvore.

Como veremos, o estudo das árvores é feito em grafos simples.

Definição 10.1 *Designa-se por* **floresta** *um grafo sem ciclos e por* **árvore** *um grafo conexo sem ciclos.*

Observação Uma floresta é um grafo em que cada componente conexa é uma árvore.

Exemplo 10.2 *Consideremos o seguinte grafo:*



Este grafo é uma floresta composta por duas árvores.

Teorema 10.3 *Seja $G = (X,\ \mathcal{U})$ um grafo simples, com $n \geq 2$ vértices. Então são equivalentes as afirmações:*

(i) *G é um grafo conexo sem ciclos.*

(ii) *G não tem ciclos e tem $n-1$ arcos.*

(iii) *G é conexo e tem $n-1$ arcos.*

(iv) *G é conexo e se $u \in \mathcal{U}$ então $G-u$ é desconexo.*

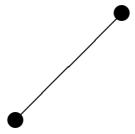
(v) *$\forall x_i,\ x_j \in X,\ x_i \neq x_j$ existe uma, e uma só, cadeia $x_i - x_j$ em G.*

(vi) *G não tem ciclos e se $u \in (X \otimes X) \setminus \mathcal{U}$ então $G+u$ tem um, e um só, ciclo.*

Demonstração

$(i) \Rightarrow (ii)$ A demonstração será feita por indução em n. Para $n = 2$ temos o resultado

G



verdadeiro.

Suponhamos o resultado verdadeiro para todo o grafo conexo sem ciclos com um número de vértices inferior ou igual a k, com $k \geq 2$. Seja $G' = (X',\ \mathcal{U}')$ um grafo conexo com $k+1$ vértices. Como G' não tem ciclos, todo o arco $u' \in \mathcal{U}'$ é uma ponte. Logo, $G' - u'$, com $u' \in \mathcal{U}'$, tem duas componentes conexas R_1 e R_2 com k_1 e k_2 vértices, respectivamente. Como R_1 e R_2 são grafos conexos sem ciclos, por hipótese de indução, o número de arcos de R_1 é $k_1 - 1$ e o número de arcos de R_2 é $k_2 - 1$. Porque $1 + k = k_1 + k_2$ e o número de arcos de G' é $1 + k_1 - 1 + k_2 - 1$, temos

$$1 + k_1 - 1 + k_2 - 1 = 1 + k - 1 = k.$$

Usando o princípio de indução podemos concluir o resultado.

$(ii) \Rightarrow (iii)$ Demonstremos que G é conexo. Suponhamos que G não é conexo e sejam $R_1, \ldots,\ R_p$ as componentes conexas de G, com $p \geq 2$. Sejam n_i e m_i, respectivamente, o número de vértices e o número de arcos de R_i, $i = 1, \ldots,\ p$.

Porque R_i é conexo sem ciclos, temos

$$m_i = n_i - 1 \qquad\qquad i = 1, \ldots,\ p.$$

então, o número de arcos de G seria

$$\sum_{i=1}^{p} m_i = \sum_{i=1}^{p} n_i - p = n - p.$$

Como $p \geq 2$, concluiríamos que o número de arcos de G

$$n - p \leq n - 2,$$

o que contradiz a hipótese.

$(iii) \Rightarrow (iv)$ Dado que G tem n vértices e $n-1$ arcos, então para qualquer $u \in \mathcal{U}$, $G - u$ tem n vértices e $n-2$ arcos. Pelo que foi visto na implicação $(i) \Rightarrow (ii)$, $G - u$ é desconexo.

$(iv) \Rightarrow (v)$ Como G é conexo, então para quaisquer dois vértices de G existe uma cadeia elementar, da qual são extremidades.

Se existissem dois vértices distintos de G que fossem extremidades de pelo menos duas cadeias distintas, então, em G, existiria um ciclo. Sendo u um arco deste ciclo, como u não era ponte, $G - u$ era conexo, o que contradiz a hipótese.

$(v) \Rightarrow (vi)$ Se em G existisse um ciclo, então sendo x e y dois vértices distintos deste ciclo, existiriam duas cadeias distintas $x - y$, o que contradiz (v). Logo, G não tem ciclos. Seja $u = \{x_i,\ x_j\} \notin \mathcal{U}$, com $x_i,\ x_j \in X$. Como por (v) existe, em G, uma cadeia $x_i - x_j$, então

$$x_i - x_j,\ u,\ x_i$$

é um ciclo em $G + u$.

Porque G não tem ciclos, então $G + u$ tem no máximo um ciclo.

$(vi) \Rightarrow (i)$ Demonstremos que G é conexo. Suponhamos que G é desconexo e sejam $x_i,\ x_j$ vértices de componentes conexas distintas. Tem-se $\{x_i,\ x_j\} \notin \mathcal{U}$. Como G não tem ciclos e não existem cadeias com extremidades em vértices de componentes conexas distintas, podemos dizer que $G+u$ não tem ciclos, o que contradiz (vi). Logo, G é conexo. □

Proposição 10.4 *Uma floresta com n vértices e p componentes conexas tem $n - p$ arcos.*

Demonstração Resulta da demonstração de $(ii) \Rightarrow (iii)$ do Teorema anterior. □

Proposição 10.5 *Existem grafos simples com n vértices e $n-1$ arcos que não são florestas e, portanto, não são árvores.*

Demonstração Seja $G = C_{n-1} \cup K_1$, com $n \geq 4$. G é grafo simples com n vértices e $n-1$ arcos, com um ciclo, portanto G não é floresta. □

Proposição 10.6 *Numa árvore, com $n \geq 2$ vértices, existem pelo menos dois vértices de grau 1.*

Demonstração Seja G uma árvore com $n \geq 2$ vértices. Seja $(d_1, \ldots, d_n)$ com $d_1 \geq \ldots \geq d_n$, a sequência de graus de G. Como G é conexo e $n \geq 2$ então, $d_n \geq 1$.

Suponhamos que G só tinha um vértice de grau 1, então

$$\sum_{i=1}^{n} d_i \geq 1 + 2(n-1).$$

Como G é uma árvore com n vértices, o número de arcos é

$$m = n - 1.$$

Aplicando o Teorema do aperto de mãos, temos a contradição,

$$2(n-1) \geq 1 + 2(n-1).$$

Logo, G tem pelo menos dois vértices de grau 1. □

Teorema 10.7 *Sejam $d_1, \ldots, d_n$, com $n \geq 2$, inteiros tais que*

$$d_1 \geq \ldots \geq d_n > 0.$$

Então, existe uma árvore cuja sequência de graus é

$$(d_1, \ldots, d_n)$$

se, e só se

$$\sum_{i=1}^{n} d_i = 2n - 2.$$

Demonstração Suponhamos que existe uma árvore G cuja sequência de graus é $(d_1, \ldots, d_n)$. Então G tem n vértices e $n-1$ arcos. Aplicando o Teorema do aperto de mãos temos

$$\sum_{i=1}^{n} d_i = 2(n-1) = 2n - 2.$$

Reciprocamente, suponhamos que $d_1, \ldots, d_n$, com $n \geq 2$, são inteiros tais que

(i) $d_1 \geq \ldots \geq d_n > 0$

(ii) $\sum_{i=1}^{n} d_i = 2n - 2$.

e demonstremos que existe uma árvore cuja sequência de graus é $(d_1, \ldots, d_n)$.

A demonstração é por indução em n.

Para $n = 2$, porque $d_1 \geq 1$, $d_2 \geq 1$ e

$$\sum_{i=1}^{n} d_i = d_1 + d_2 = 2n - 2 = 2$$

então, $d_1 = d_2 = 1$. K_2 é uma árvore com a sequência pretendida.

Suponhamos que o resultado é válido para $k-1$, com $k-1 \geq 2$, inteiros nas condições do enunciado.

Sejam $d_1, \ldots, d_k$, com $k \geq 3$, inteiros satisfazendo (i) e (ii). Se $d_k \geq 2$ então, $2k-2 = \sum_{i=1}^{k} d_i \geq 2k$ (contradição).

Portanto, $d_k = 1$. Por outro lado, se $d_1 = 1$, então

$$2k - 2 = \sum_{i=1}^{k} d_i = k,$$

o que contradiz a hipótese de $k \geq 3$. Portanto, $d_1 > 1$.

Assim, $d_1 - 1,\ d_2, \ldots,\ d_{k-1}$ são $k-1$ inteiros positivos, não necessariamente ordenados por ordem crescente, tais que

$$d_1 - 1 + d_2 + \ldots + d_{k-1} = \sum_{i=1}^{k} d_i - 1 - d_k = (2k-2) - 1 - 1 = 2(k-1) - 2.$$

Por hipótese de indução, existe uma árvore G, com $k-1$ vértices, em que os graus dos vértices são $d_1 - 1,\ d_2, \ldots,\ d_{k-1}$. Acrescente-se a G um novo vértice e torne-se este vértice adjacente a um vértice de G com grau $d_1 - 1$. Obtém-se um grafo G', com k vértices, que é ainda uma árvore e em que os graus dos vértices são

$$(d_1 - 1) + 1,\ d_2, \ldots,\ d_{k-1},\ 1 (= d_k).$$

Logo, G' é uma árvore com sequência de graus $(d_1, \ldots,\ d_k)$.

Usando o princípio de indução, obtemos o resultado. □

10.2 Árvores Maximais

Em certas situações, o grafo conexo que temos não é uma árvore, mas queremos obter, a partir do grafo inicial, um grafo parcial que seja uma árvore. Por exemplo, no problema da "viagem à volta do mundo", se não exigirmos que o viajante regresse à cidade de que partiu, o que queremos é uma árvore maximal do dodecaedro.

Teorema 10.8 *Um grafo é conexo se, e só se, admite uma árvore como grafo parcial.*

Demonstração $\Longleftarrow$ Se um grafo G admite uma árvore como grafo parcial então G admite um grafo parcial conexo, logo é conexo.

$\Longrightarrow$ Se G não tem ciclos, então G é uma árvore (grafo parcial de G).

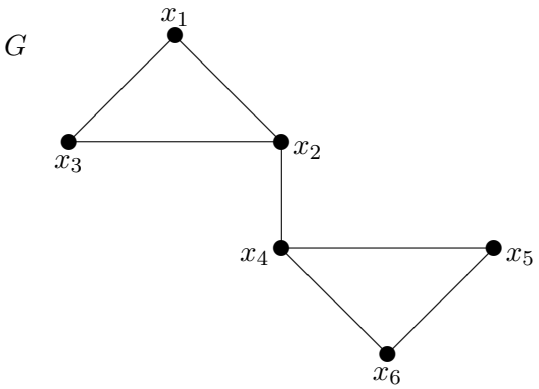
Se G tem um ciclo, seja u_1 um arco de um dos ciclos de G. Então u_1 não é ponte, pelo que $G_1 = G - u_1$ é conexo e tem um número de ciclos inferior ao número de ciclos de G.

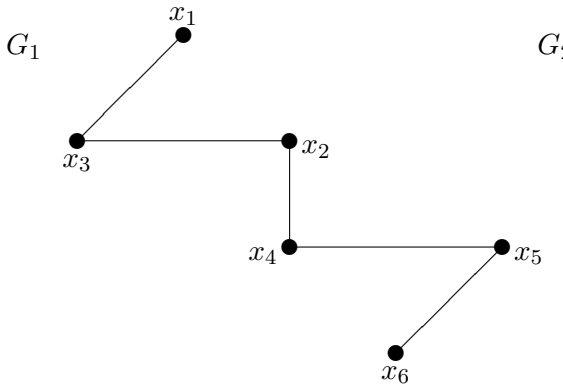
Se $G - u_1$ não tem ciclos então $G_1 = G - u_1$ é árvore (grafo parcial de G). Caso contrário, seja u_2 um arco de um ciclo de $G_1 - u_2 = G_2$.

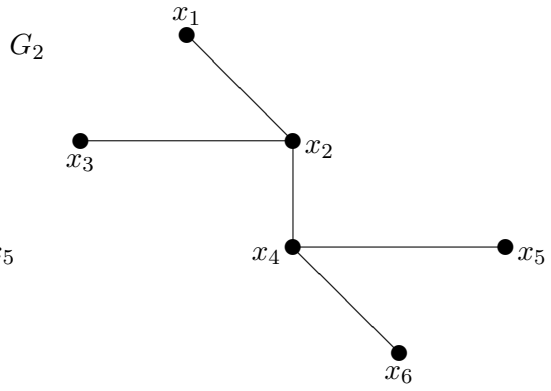
Porque o número de ciclos de G é finito, procedendo deste modo, obtemos um grafo $G_k = G_{k-1} - u_{k-1}$ que é conexo, sem ciclos. Logo G_k é árvore (grafo parcial de G). □

Definição 10.9 *Seja G um grafo (respectivamente, grafo conexo). Designa-se por* **floresta** *(respectivamente,* **árvore***)* **maximal** *de G qualquer grafo parcial de G, que tenha o mesmo número de conexidade que G e que seja* **floresta** *(respectivamente,* **árvore***).*

Exemplo 10.10 *Consideremos o seguinte grafo simples,*







G_1 e G_2 são duas árvores maximais, não isomorfas de G

Definição 10.11 *Chamamos* **grafo ponderado** *a um par $(G,\ v)$ em que $G = (X,\ \mathcal{U})$ é um grafo e v é uma aplicação de $\mathcal{U}$ no conjunto dos números reais.*

Se $u \in \mathcal{U}$ designa-se por **valor/peso do arco u** *o número real $v(u)$ e designa-se por* **valor de G**, *e representa-se por $v(G)$, o número real*

$$v(G) = \sum_{u \in \mathcal{U}} v(u).$$

Vejamos dois algoritmos para determinar árvores maximais com valor mínimo.

Algoritmo de Kruskal

Seja $(G,\ v)$ um grafo ponderado, sendo $G = (X,\ \mathcal{U})$ um grafo conexo com n vértices.

1^o) Considere-se um arco u_1 de G que não é laço e tal que

$$v(u_1) = \min_{u \in \mathcal{U}} v(u).$$

2^o) Se os arcos $u_1, \ldots,\ u_i$ já foram escolhidos, então, sendo $\mathcal{U}_i = \{u_1, \ldots,\ u_i\}$, escolha-se um arco u_{i+1} tal que

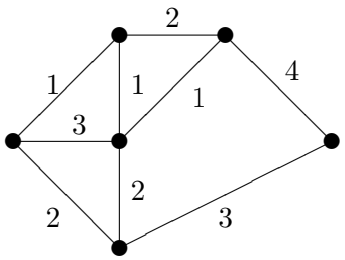
(1) $u_{i+1} \notin \mathcal{U}_i$

(2) $G' = (X,\ \mathcal{U}_i \cup \{u_{i+1}\})$ não tem ciclos

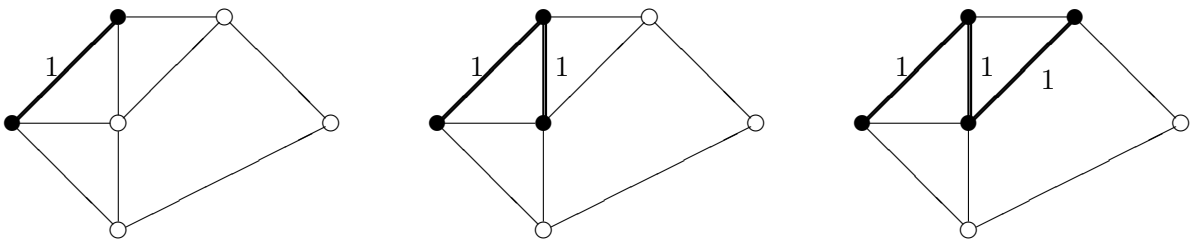
(3) u_{i+1} é de entre os arcos que verificam as condições (1) e (2), um com valor mínimo.

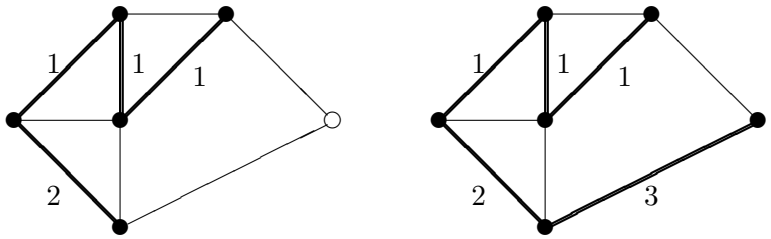
3^o) Se já foram escolhidos $n-1$ arcos, então o algoritmo termina. Caso contrário, repita-se 2^o).

Exemplo 10.12 *Consideremos o seguinte grafo ponderado*



Calculemos, usando o Algoritmo de Kruskal, uma árvore maximal de valor mínimo.





cujo valor é $1+1+1+2+3=8$

Algoritmo de Prim
Seja $(G,\ v)$ um grafo ponderado, sendo $G=(X,\ \mathcal{U})$ um grafo conexo com n vértices.

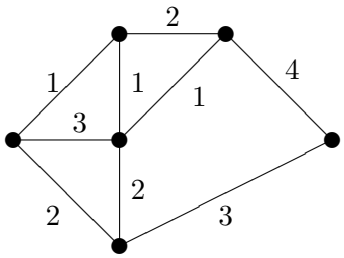
1^o) Considere-se um vértice arbitrário de G, que designamos por x_1.

2^o) Escolha-se um arco u_1 de G, incidente em x_1, que não seja laço e que tenha valor mínimo.

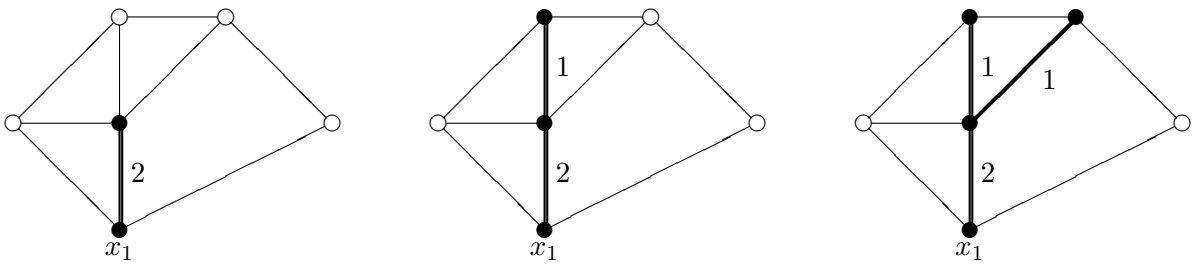
3^o) Se os arcos $u_1, \ldots,\ u_i$ já foram escolhidos, sendo as suas extremidades os elementos do conjunto $X_i = \{x_1, \ldots,\ x_{i+1}\}$, escolha-se qualquer arco $u_{i+1} = \{x_j,\ x_k\}$ tal que $x_j \in X_i$ e $x_k \notin X_i$ e u_{i+1} é, de entre todos os arcos de G com precisamente uma extremidade em X_i que ainda não foram escolhidos, um arco com valor mínimo.

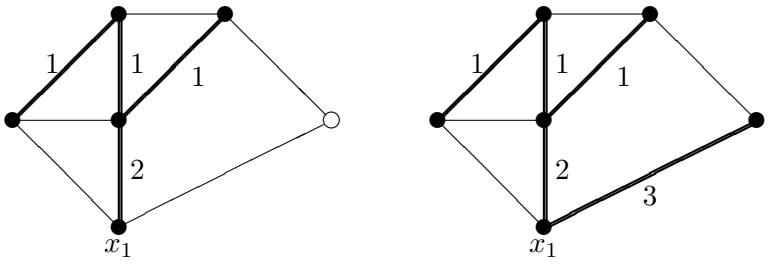
4^o) Se já foram escolhidos $n-1$ arcos, então o algoritmo termina. Caso contrário, repita-se 3^o).

Exemplo 10.13 *Com o grafo ponderado do exemplo anterior,*



calculemos uma árvore maximal de valor mínimo, mas utilizando o Algoritmo de Prim e partindo do vértice x_1.





cujo valor é $1+1+1+2+3=8$

Observação Se temos um grafo simples conexo e queremos uma sua árvore maximal, podemos usar qualquer um dos algoritmos anteriores bastando para isso, atribuir o mesmo valor a todos os arcos do grafo.

Em geral, em termos de implementação em computador, o Algoritmo de Prim é mais rápido do que o de Kruskal.

A demonstração do Algoritmo de Kruskal (respectivamente, de Prim) pode encontrar-se nas páginas 63 e 64 (respectivamente, 66 e 67) de "J. Clark, D. A. Holton, A First Look at Graph Theory, World Scientific, 1991".

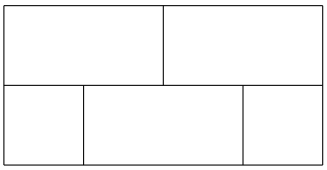
Capítulo 11

Grafos Eulerianos

11.1 Grafos Eulerianos. Algoritmo de Fleury

Como já o referimos, é neste capítulo que iremos tratar de resolver o problema das pontes de Königsberg.

Uma charada muito conhecida, deste tipo de problemas, é a seguinte:
A seguinte figura



pode ser desenhada através de quatro traços contínuos. E será possível através de três? Neste capítulo veremos que tal não é possível.

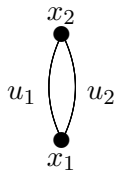
Definição 11.1 *Seja $G = (X, \mathcal{U})$ um multigrafo. Chamamos* **cadeia euleriana** *a uma cadeia simples contendo todos os arcos de G e* **ciclo euleriano** *a um ciclo contendo todos os arcos de G.*

Se G é um multigrafo orientado, substituindo na definição "cadeia"por "caminho"obtêm-se as correspondentes definições de **caminho euleriano** e de **circuito euleriano**.

Definição 11.2 *Um multigrafo diz-se* **euleriano** *se admite um ciclo euleriano e* **semi-euleriano** *se admite uma cadeia euleriana aberta.*

Observação

1. Não existem multigrafos simultaneamente eulerianos e semi-eulerianos.
2. Para determinar se um multigrafo é euleriano ou semi-euleriano não podemos considerar que é equivalente efectuar tal estudo no grafo simples que lhe está associado. Por exemplo, o multigrafo



tem um ciclo euleriano $x_1,\ u_1,\ x_2,\ u_2,\ x_1$ e o mesmo não sucede no grafo simples

3. Se um multigrafo admite uma cadeia euleriana então, no máximo, uma componente conexa do multigrafo é um multigrafo não nulo.

Teorema 11.3 (i) *Um multigrafo conexo G, com $n \geq 2$ vértices, tem um ciclo euleriano se, e só se, todo o vértice de G tem grau par.*

(ii) *Um multigrafo conexo G, com $n \geq 2$ vértices, tem uma cadeia $x - y$ euleriana, com $x \neq y$ se, e só se, x e y são os únicos vértices de G com grau ímpar.*

Demonstração Para o estudo da existência de cadeias eulerianas abertas ou fechadas, num multigrafo G podemos considerar, sem perda de generalidade, que G não tem laços.

(i) Suponhamos que $G = (X,\ \mathcal{U})$ é um multigrafo conexo, com $n \geq 2$ vértices, que tem um ciclo euleriano. Seja

$$C: \qquad x_1,\ u_1,\ x_2,\ u_2, \ldots,\ x_k,\ u_m,\ x_1$$

um ciclo euleriano de G, sendo m o número de elementos da família $\mathcal{U}$. Como G é conexo e C inclui todos os arcos de G, podemos afirmar que todo o vértice de G está

em C. Seja x um vértice de G e seja r o número de vezes que x ocorre na sequência $x_1,\ u_1,\ x_2,\ u_2, \ldots,\ x_k,\ u_m$.

Como todos os arcos de C são distintos, podemos afirmar que

$$d(x) \geq 2r,$$

mas, C inclui todos os arcos de G, logo, $d(x) = 2r$. Concluímos então que todo o vértice de G tem grau par.

Reciprocamente, suponhamos que $G = (X,\ \mathcal{U})$ é um multigrafo conexo, com $n \geq 2$ vértices, em que todo o vértice tem grau par e demonstremos por indução sobre o número m de arcos, que G tem um ciclo euleriano.

Sem perda de generalidade, consideraremos que G não tem laços. Se todo o vértice tem grau par, G é conexo e $n \geq 2$ então $m \geq 2$.

Se $m = 2$ então G é isomorfo a

que tem um ciclo euleriano.

Suponhamos que o resultado é verdadeiro para todo o multigrafo conexo, sem laços, com $n \geq 2$ vértices, com número de arcos inferior a k, em que todo o vértice tem grau par e demonstremos que é, ainda, verdadeiro para todo o multigrafo conexo, sem laços, com $n \geq 2$ vértices, com exactamente k arcos e tendo todo o vértice grau par. Seja $G = (X,\ \mathcal{U})$ um multigrafo verificando estas condições.

Como G é conexo, com $n \geq 2$ vértices, G não tem vértices de grau zero. Se G não tivesse um ciclo, G era uma árvore, o que implicava que existiriam dois vértices de grau 1, contrariando a hipótese de todo o vértice ter grau par.

Seja C um ciclo de G com comprimento máximo.

Suponhamos que C não inclui todos os arcos de G e seja $G' = (X,\ \mathcal{U}')$ o grafo parcial de G que se obtém eliminando em G os arcos de C. Em G', temos, $d_{G'}(x)$ é par, para todo o $x \in X$ porque se x é vértice de C, então

$$d_{G'}(x) = d_G(x) - 2k_x, \qquad \text{com } k_x \in \mathbb{N}$$

e se x não é vértice de C, então

$$d_{G'}(x) = d_G(x).$$

Como todo o vértice de G tem grau par, concluímos que todo o vértice de G' tem grau par. Como G é conexo e G' tem pelo menos um arco, existe um arco $u = \{x,\ y\}$

de G', com x vértice de C. Seja H a componente conexa de G' de que u faz parte. H é um multigrafo conexo, sem laços, com número de vértices superior ou igual a 2 em que todo o vértice tem grau par e com número de arcos inferior a k. Atendendo à hipótese de indução, H tem um ciclo euleriano, que contem o vértice x,

$$C': \qquad x,\ u'_1,\ y_1, \ldots,\ y_{r-1},\ u'_r,\ x,$$

em que $u'_i \in \mathcal{U}'$, $i = 1, \ldots, r$ e $y_j \in X$, $j = 1, \ldots, r-1$.

Porque x é vértice de C,

$$C: \qquad x,\ u_1,\ z_1, \ldots,\ z_{h-1},\ u_h,\ x$$

em que $u_i \in \mathcal{U}$, $i = 1, \ldots, h$ e $z_j \in X$, $j = 1, \ldots, h-1$. Então

$$x,\ u_1,\ z_1, \ldots,\ z_{h-1},\ u_h,\ x,\ u'_1,\ y_1, \ldots,\ y_{r-1},\ u'_r,\ x$$

é um ciclo em G mas com comprimento superior ao de C, que por hipótese tem comprimento máximo. Contradição. Logo, G tem um ciclo euleriano.

Usando o princípio de indução obtemos o resultado.

(ii) Seja $G = (X,\ \mathcal{U})$ um multigrafo conexo, com $n \geq 2$ vértices. Seja $z \notin X$. Atenda-se a que G tem uma cadeia $x - y$ euleriana, com $x \neq y$, se, e só se, o grafo

$$\hat{G} = (X \cup \{z\},\ \mathcal{U} \cup \{x,\ z\} \cup \{y,\ z\}), \qquad \text{com } z \notin X$$

tem um ciclo euleriano.

Por (i) tal sucede se, e só se,

$$d_{\hat{G}}(x_i) \text{ é par, para todo o } x_i \in X \cup \{z\}.$$

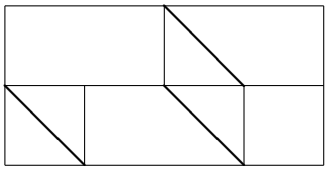
Como

$$d_{\hat{G}}(x) = d_G(x) + 1,$$
$$d_{\hat{G}}(y) = d_G(y) + 1,$$
$$d_{\hat{G}}(x_i) = d_G(x_i),$$

para todo o $x_i \in X \setminus \{x,\ y\}$, concluímos que G tem uma cadeia $x - y$ euleriana, com $x \neq y$, se, e só se, x e y são os únicos vértices de G com grau ímpar. □

Regressando à pergunta que foi feita no inicio deste capítulo: Será possível desenhar a seguinte figura com três traços contínuos?

Construamos o seguinte grafo: os vértices correspondem ao ponto de encontro de duas rectas da figura e dois vértices são adjacentes, se os dois pontos a que correspondem estes dois vértices, na figura, estão unidos por uma recta. Este grafo tem doze vértices, sendo oito deles de grau ímpar. Colocando mais três rectas na figura inicial, obtemos a figura



que pelo Teorema, pois o grafo que lhe está associado tem só dois vértices de grau ímpar, tem uma cadeia euleriana. Então, com menos de quatro traços contínuos, não conseguimos desenhar a figura inicial (cada recta que acrescentámos à figura, corresponde a uma descontinuidade).

Teorema 11.4 (i) *Um multigrafo orientado conexo $G = (X,\ \mathcal{U})$, com $n \geq 2$ vértices, tem um circuito euleriano se, e só se,*

$$d^+(x) = d^-(x),$$

para todo o $x \in X$.

(ii) *Um multigrafo orientado conexo $G = (X,\ \mathcal{U})$, com $n \geq 2$ vértices, tem um caminho $x - y$ euleriano, com $x \neq y$ se, e só se,*

$$d^+(x) = d^-(x) - 1,$$

$$d^+(y) = d^-(y) + 1,$$

$$d^+(x_i) = d^-(x_i),$$

para todo o $x_i \in X \setminus \{x,\ y\}$.

Sendo $G = (X,\ \mathcal{U})$ um multigrafo euleriano, como determinar um ciclo euleriano? O algoritmo seguinte, dá-nos a resposta.

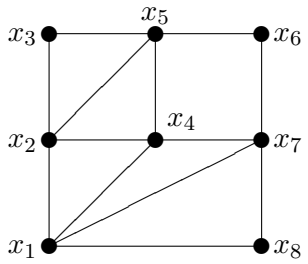
Algoritmo de Fleury
Seja $G = (X,\ \mathcal{U})$ um multigrafo euleriano.

1^o Escolha um vértice x_1 de G.

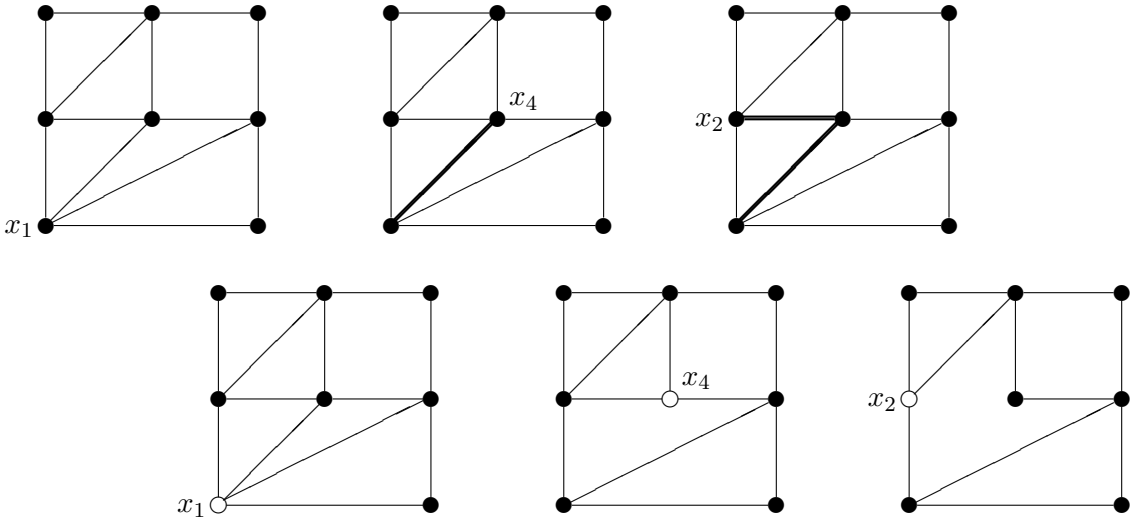
2^o Sendo $L: \quad x_1,\ u_1,\ x_2, \ldots,\ u_p,\ x_k$ uma cadeia simples, seja $u_{k+1} = \{x_k,\ x_l\}$ um arco incidente em x_k que não pertence a L e que só é ponte de $G' = (X,\ \mathcal{U} \setminus \{u_1, \ldots,\ u_k\})$ se não existir mais nenhum arco incidente em x_k de G'.

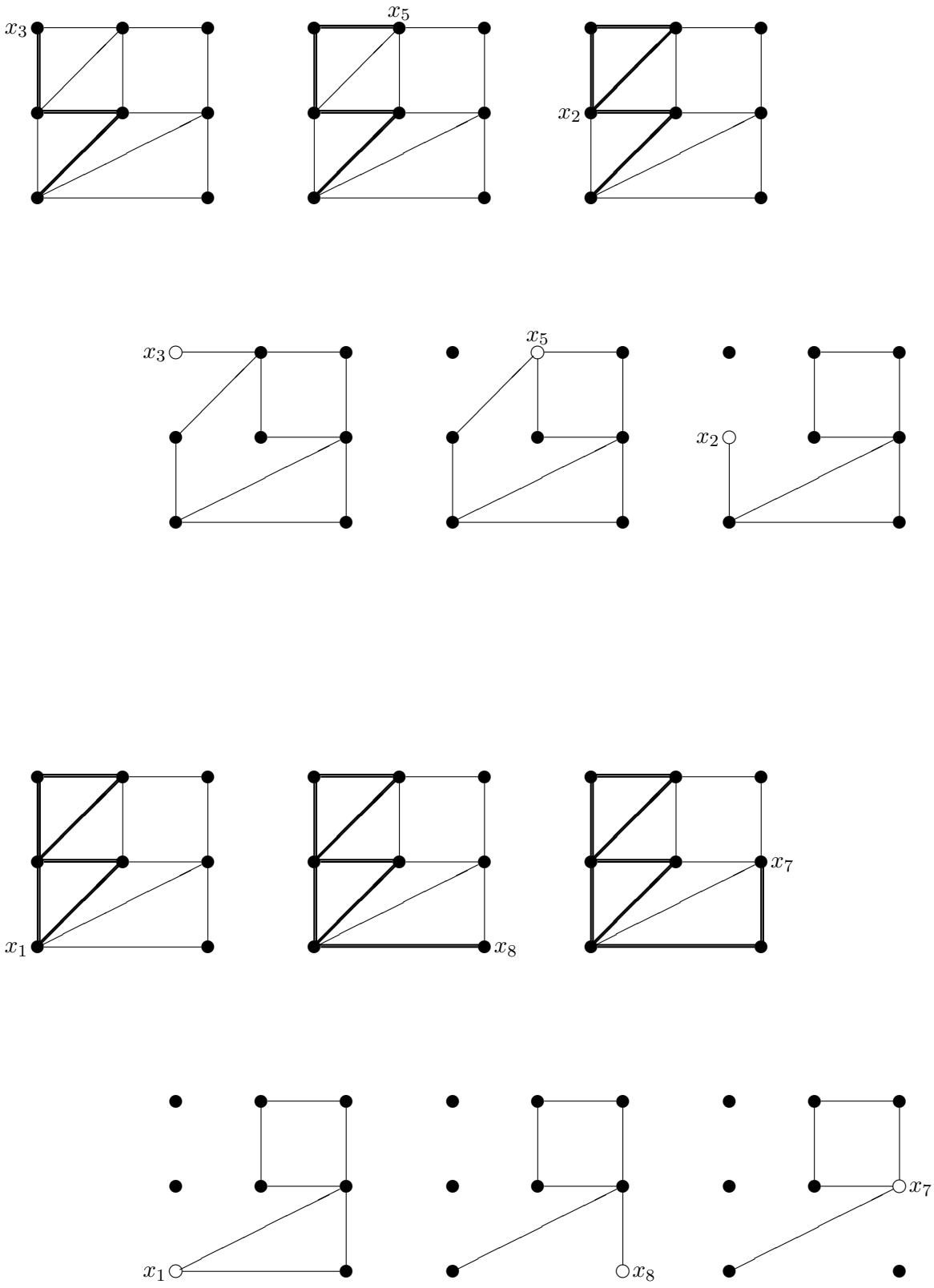
3^o Se $d_{G'}(x_l) = 1$, o algoritmo termina, caso contrário repita-se 2^o.

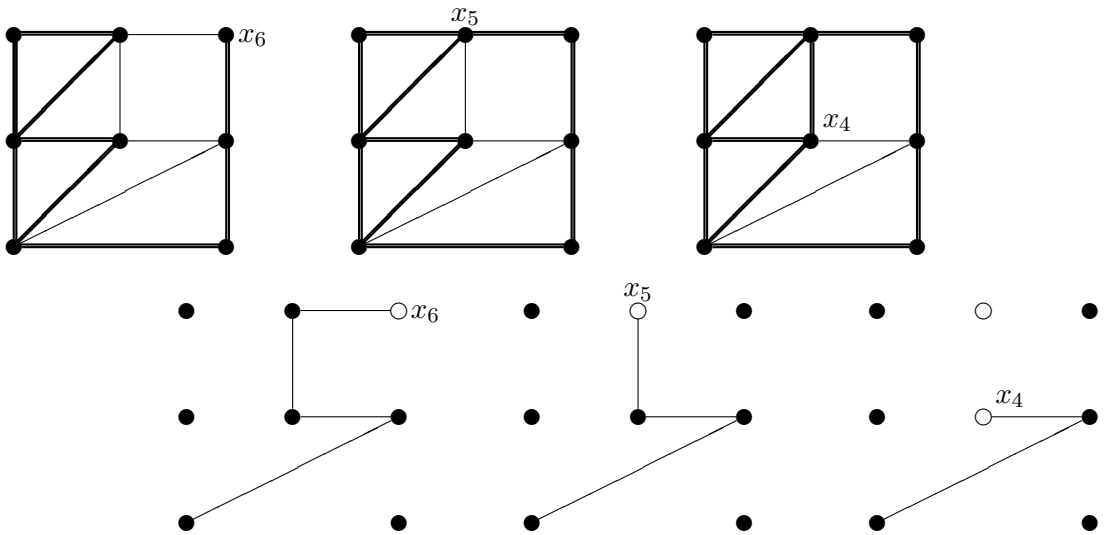
Exemplo 11.5 *Consideremos o grafo*

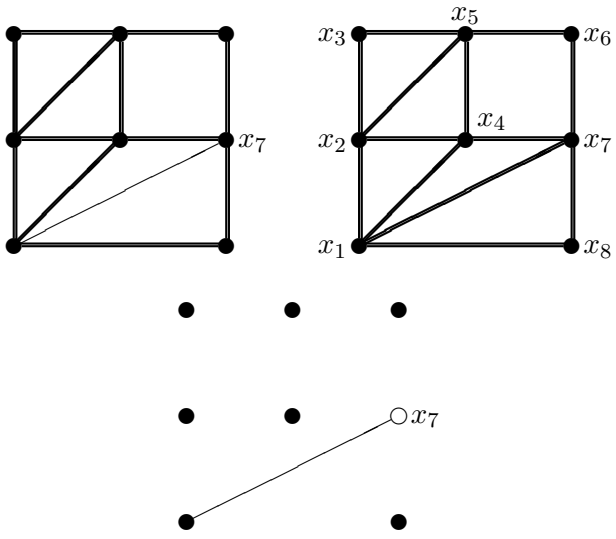


que é euleriano pois todos os seus vértices têm grau par. Utilizemos o algoritmo de Fleury para determinar um ciclo euleriano. Ao longo do esquema, há duas linhas de grafos mais próximas, em que os grafos da linha inferior estão numa coluna distinta dos da linha superior. Os grafos da linha superior indicam o arco que apanhámos cada vez que aplicámos a algoritmo (o primeiro grafo indica-nos, unicamente, o vértice em que iniciamos o ciclo), e os grafos da linha inferior indicam-nos quais são os possíveis arcos que temos para aplicar o algoritmo, a partir do vértice considerado.




x_3
x_5
x_2
x_3
x_5
x_2
x_1
x_8
x_7
x_1
x_8
x_7


x_6
x_5
x_4
x_6
x_5
x_4


x_7
x_5
x_3
x_6
x_4
x_2
x_7
x_1
x_8
x_7

Capítulo 12

Grafos Hamiltonianos

12.1 Alguns resultados sobre grafos Hamiltonianos

Consideremos o seguinte tabuleiro 3×4 em que as "casas"brancas estão identificadas com números e as "casas"pretas com letras,

f	6	e	5
3	c	4	d
b	2	a	1

É possível, através de movimentos lícitos, no jogo de xadrez, o cavalo percorrer todas as "casas"do tabuleiro, começando na "casa"número 1. Por exemplo,

$$1,\ c,\ 5,\ a,\ 3,\ e,\ 2,\ d,\ 6,\ b,\ 4,\ f.$$

Mas não existe maneira do cavalo começar e regressar à "casa"número 1, depois de percorrer todas as "casas"do tabuleiro.

Definição 12.1 *Seja $G = (X,\ \mathcal{U})$ um grafo. Chamamos* **cadeia hamiltoniana** *a uma cadeia elementar que contenha todos os vértices de G e* **ciclo hamiltoniano** *a um ciclo elementar que contenha todos os vértices de G.*

Se G é um grafo orientado substituindo, nas definições anteriores "cadeia"por "caminho"obtêm-se as correspondentes definições de **caminho hamiltoniano** e de **circuito hamiltoniano**.

Definição 12.2 *Um grafo diz-se* **hamiltoniano** *se admite um ciclo hamiltoniano e* **semi-hamiltoniano** *se admite uma cadeia hamiltoniana aberta.*

Observação

1. Todo o grafo hamiltoniano é semi-hamiltoniano.
2. Se um grafo admite uma cadeia hamiltoniana então é conexo.
3. Se um grafo orientado admite um circuito hamiltoniano então é fortemente conexo.
4. Não há perda de generalidade em enunciar os resultados referentes à existência de cadeias hamiltonianas em termos de grafos simples e os resultados referentes à existência de caminhos hamiltonianos em termos de digrafos.

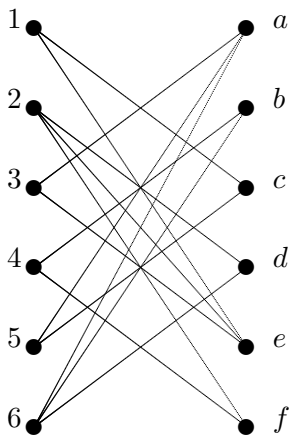
Proposição 12.3 *Se um grafo simples admite um ciclo hamiltoniano então não tem pontes.*

Demonstração Seja $G = (X,\ \mathcal{U})$ um grafo simples que admite um ciclo hamiltoniano. Logo G é conexo. Suponhamos que $u = \{x,\ y\}$ é uma ponte de G.

$G - u = G'$ tem duas componentes conexas, uma contendo o vértice x e outra o vértice y.

Seja C um ciclo hamiltoniano em G. Como C inclui todos os vértices de G, então os vértices x, y são vértices de C. Logo, existe uma cadeia $x - y$ em G', o que é impossível. □

O recíproco da Proposição anterior não é verdadeiro. O grafo associado ao problema que colocámos no inicio do capítulo, é um grafo cujos vértices correspondem às "casas"do tabuleiro e dois vértices são adjacentes se for possível ao cavalo deslocar-se duma das "casas"para a outra, através de um movimento lícito. Neste caso, tabuleiro 3×4, temos o grafo bipartido



Pretendia-se saber se existe maneira do cavalo começar e regressar à "casa"número 1, depois de percorrer todas as "casas"do tabuleiro. Para existir um tal percurso, teria de existir um ciclo hamiltoniano, neste grafo. Ora, como certos vértices têm grau dois, teríamos de ter as sequências

$$2,\ f,\ 4 \qquad\qquad 4,\ b,\ 6 \qquad\qquad 6,\ d,\ 2.$$

Mas isto obrigaria a termos o ciclo

$$2,\ f,\ 4,\ b,\ 6,\ d,\ 2$$

que não é um ciclo hamiltoniano.

Proposição 12.4 *K_n, com $n \geq 3$, tem um ciclo hamiltoniano.*

Este ciclo é o grafo parcial de K_n isomorfo a C_n.

Teorema 12.5 *Seja $G = (X,\ \mathcal{U})$ um grafo simples, com $n \geq 3$ vértices, tal que*

$$d(x) + d(x') \geq n, \qquad\qquad \forall x,\ x' \in X \text{ não adjacentes.}$$

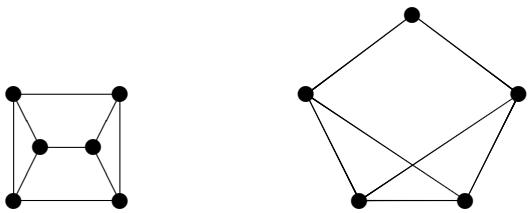
Então, G é hamiltoniano.

Corolário 12.6 *Seja $G = (X,\ \mathcal{U})$ um grafo simples, com $n \geq 3$ vértices, tal que*

$$d(x) \geq \frac{n}{2}, \qquad\qquad \forall x \in X.$$

Então, G é hamiltoniano.

Exemplo 12.7 *Consideremos os grafos*



A *B*

Usando o Corolário anterior, porque $d(x) \geq 3$, qualquer que seja o vértice do grafo A, e 6 é o número de vértices deste grafo, concluímos que o grafo tem um ciclo hamiltoniano.

No caso do grafo B, o Corolário não pode ser usado, no entanto pelo Teorema, podemos concluir que este grafo também tem um ciclo hamiltoniano.

Capítulo 13

Matrizes e Grafos

13.1 Matriz de Adjacências

Uma outra forma de representar um grafo é através de uma matriz quadrada de ordem igual à ordem do grafo.

Definição 13.1 *Chamamos* **marcação dos vértices** *de um grafo* $G = (X,\ \mathcal{U})$*, com* $|X| = n$*, a uma aplicação bijectiva* ψ *de* X *em* $\{1, \ldots,\ n\}$*.*

Um **grafo marcado** *nos vértices é um par* $(G,\ \psi)$ *em que* G *é um grafo e* ψ *é uma marcação dos vértices de* G*.*

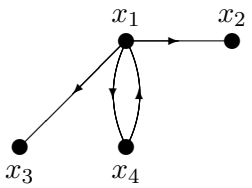
Definição 13.2 *Seja* $G = (X,\ \mathcal{U})$ *um digrafo marcado nos vértices, com* $(G,\ \psi)$ *e* $X = \{1, \ldots,\ n\}$*. Chamamos* **matriz de adjacências** *de* G*, em relação à marcação* ψ*, à matriz* $A(G) = [a_{ij}]$*, de ordem* n*, tal que*

$$a_{\psi(x_i)\psi(x_j)} = \begin{cases} 1 & se\ (x_i,\ x_j) \in \mathcal{U} \\ 0 & se\ (x_i,\ x_j) \notin \mathcal{U} \end{cases}$$

Seja $(G,\ \psi)$ um grafo marcado nos vértices, com $G = (X,\ \mathcal{U})$ e $X = \{1, \ldots,\ n\}$. Referimo-nos à marcação $(x_{i_1}, \ldots,\ x_{i_n})$ para designar a marcação ψ tal que

$$\psi(x_{i_j}) = j, \qquad\qquad j = 1, \ldots,\ n.$$

Exemplo 13.3 *Consideremos o digrafo* G



A matriz de adjacências de G, em relação à marcação $(x_1,\ x_2,\ x_3,\ x_4)$ é a matriz

$$A(G) = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

E em relação à marcação $(x_2,\ x_3,\ x_1,\ x_4)$ é a matriz

$$A'(G) = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

As matrizes de adjacências de um digrafo em relação a marcações diferentes são, em geral, diferentes.

Proposição 13.4 *Sejam A e A' matrizes de adjacências de um digrafo $G = (X,\ \mathcal{U})$ em relação a marcações diferentes dos seus vértices. Então, existe uma matriz de permutação P tal que*

$$A' = PAP^{-1}$$

(uma matriz de permutação de ordem n é uma matriz que se obtém da matriz identidade de ordem n efectuando uma troca nas suas linhas).

Observação

1. Sendo $G = (X,\ \mathcal{U})$ um digrafo com $X = \{x_1, \ldots,\ x_n\}$, referimos **marcação usual** dos vértices de G, à marcação $(x_1, \ldots,\ x_n)$. A matriz de adjacências de G, em relação à marcação usual, é a matriz $A = [a_{ij}]$ em que

$$a_{ij} = \begin{cases} 1 & \text{se } (x_i,\ x_j) \in \mathcal{U} \\ 0 & \text{se } (x_i,\ x_j) \notin \mathcal{U} \end{cases}$$

2. Através da matriz de adjacências $A = [a_{ij}]$ de um digrafo G, em relação à marcação $(x_1, \ldots, x_n)$, podemos determinar o grau exterior e o grau interior de cada vértice de G.

$$d^+(x_i) = \sum_{j=1}^{n} a_{ij},$$

isto é, é a soma dos elementos da linha i de A, ou equivalentemente, o número de elementos da linha i que são iguais a 1, e

$$d^-(x_i) = \sum_{j=1}^{n} a_{ji},$$

isto é, é a soma dos elementos da coluna i de A.

Exemplo 13.5 *Considerando o grafo do exemplo anterior, cuja matriz de adjacências em relação à marcação* $(x_1,\ x_2,\ x_3,\ x_4)$*, dos seus vértices é*

$$A(G) = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

temos

$$\sum_{j=1}^{n} a_{1j} = 3 = d^+(x_1)$$

e

$$\sum_{j=1}^{n} a_{j3} = 1 = d^-(x_3).$$

Teorema 13.6 *Seja* $G = (X,\ \mathcal{U})$ *um digrafo marcado nos vértices e* $A = [a_{ij}]$ *a matriz de adjacências de* G*, em relação à marcação usual* $(x_1, \ldots, x_n)$*. Então, na matriz*

$$AA^T = [s_{ij}]$$

s_{ij} *representa o número de sucessores simultâneos de* x_i *e* x_j*, isto é,*

$$s_{ij} = |\Gamma^+(x_i) \cap \Gamma^+(x_j)|.$$

Demonstração O elemento da linha i coluna j de AA^T é

$$s_{ij} = a_{i1}a_{j1} + a_{i2}a_{j2} + \ldots + a_{in}a_{jn}.$$

Se $i = j$ tem-se

$$\begin{aligned} s_{ij} &= a_{i1}^2 + a_{i2}^2 + \ldots + a_{in}^2 \\ &= a_{i1} + a_{i2} + \ldots + a_{in} = d^+(x_i) \end{aligned}$$

e, portanto, s_{ii} é igual ao número de sucessores de x_i.

Se $i \neq j$, os vértices x_i e x_j têm o vértice x_k como sucessor simultâneo se, e só se, $(x_i,\ x_k) \in \mathcal{U}$ e $(x_j,\ x_k) \in \mathcal{U}$. Mas isto sucede se, e só se, $a_{ik} = 1$ e $a_{jk} = 1$, ou ainda, se, e só se, $a_{ik}a_{jk} = 1$. Pelo que o resultado se verifica. □

Definição 13.7 *Seja $G = (X,\ \mathcal{U})$ um* **grafo simples***, com $X = \{1, \ldots,\ n\}$. Chama-se* **matriz de adjacências** *de G, em relação à marcação $(x_1, \ldots,\ x_n)$ dos seus vértices, à matriz $A(G) = [a_{ij}]$, de ordem n, tal que*

$$a_{ij} = \begin{cases} 0 & \text{se } i = j \text{ ou } \{x_i,\ x_j\} \notin \mathcal{U} \\ 1 & \text{se } \{x_i,\ x_j\} \in \mathcal{U} \end{cases}$$

Observação

1. A matriz de adjacências de um grafo simples tem todos os elementos diagonais nulos.
2. A matriz de adjacências de um grafo simples tem a propriedade de ser simétrica, isto é, $A = A^T$.

Teorema 13.8 *Seja $A = [a_{ij}]$ a matriz de adjacências de um grafo simples $G = (X,\ \mathcal{U})$, em relação à marcação usual $(x_1, \ldots,\ x_n)$. Então, na matriz*

$$A^k = [a_{ij}^{(k)}], \qquad \text{com } k \in \mathbb{N},$$

$a_{ij}^{(k)}$ é igual ao número de cadeias $x_i - x_j$ com comprimento k, existentes em G.

Demonstração Faremos a demonstração por indução em k.

Para $k = 1$, o resultado é válido, pois para $i = j$, $a_{ij} = 0$ e, para $i \neq j$, $a_{ij} = 1$ se, e só se, $\{x_i,\ x_j\} \in \mathcal{U}$. Como num grafo simples não existem arcos paralelos, a_{ij} representa o número de cadeias $x_i - x_j$, com comprimento 1, existentes em G.

Suponhamos então que na matriz $A^{l-1} = [a_{ij}^{(l-1)}]$, $a_{ij}^{(l-1)}$ é igual ao número de cadeias $x_i - x_j$, de G, com comprimento $l - 1$, e demonstremos que em $A^l = [a_{ij}^{(l)}]$, $a_{ij}^{(l)}$ é igual ao número de cadeias $x_i - x_j$, de G, com comprimento l.

Tem-se

$$A^l = A^{l-1}A$$

pelo que

$$a_{ij}^{(l)} = \sum_{s=1}^{n} a_{is}^{(l-1)} a_{sj}.$$

De acordo com a hipótese de indução, $a_{is}^{(l-1)}$ é igual ao número de cadeias $x_i - x_s$, de G, com comprimento $l-1$. Então,

$$a_{is}^{(l-1)} a_{sj}$$

é igual ao número de cadeias $x_i - x_j$, de G, com comprimento $(l-1)+1 = l$ e tendo como penúltimo vértice x_s. Logo, o resultado é verdadeiro para l. Pelo princípio de indução, temos que o resultado é verdadeiro. □

Observação Substituindo no Teorema anterior, "grafo simples"por "digrafo"e "cadeia"por "caminho", obtemos um resultado válido.

Exemplo 13.9 *Com o exemplo anterior, vejamos se em G existem caminhos $x_4 - x_3$ de comprimento 2. Ora,*

$$A(G)^2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix}.$$

Como esta matriz, tem na posição $(4,\ 3)$ um elemento não nulo, usando o Teorema, existe um caminho de $x_4 - x_3$, em G.

Bibliografia

[1] N. L. Biggs, **Discrete Mathematics**, Oxford Science Publications, **1994**

[2] T. S. Blyth e E. F. Robertson, **Sets and Mappings**, Chapman and Hall, **1986**

[3] I. C. Esquível, **Grafos e Aplicações**, Texto teórico, **1997**

[4] A. J. Franco de Oliveira, **Teoria de Conjuntos**, Livraria Escolar Editora, **1986**

[5] R. Johnsonbaugh, **Discrete Mathematics**, Prentice Hall International, **1997**

[6] S. Lipschutz, **Set Theory and Related Topics**, Schaum´s Outline Series, Mc Graw-Hill, **1964**

[7] M. Queysanne, **Algèbre**, Librairie Armand Colin, **1964**

[8] K. A. Ross e C. R. B. Wright, **Discrete Mathematics**, Prentice Hall International, **1999**

[9] R. J. Wilson e J. J. Watkins , **Graphs an Introductory Approach**, Wiley, **1990**