PAM preprint. Collection: *Cadernos de Matemática - Série de Divulgação* CM 06/D-1 Institution: *University of Aveiro* (submitted January 12, 2006)

Elementos de Matemática

Domingos Moreira Cardoso e Domenico Antonino Catalano

Departamento de Matemática da Universidade de Aveiro,

Dezembro de 2005

dcardoso@mat.ua.pt, domenico@mat.ua.pt

Conteúdo

Capítulo 1

Nota Prévia

Este texto foi elaborado para servir de base à disciplina de Elementos de Matemática, criada na sequência da reforma efectuada em 2001 na Universidade de Aveiro. A disciplina de Elementos de Matemática que entrou em funcionamento no ano lectivo de 2001/2002, foi incluída no primeiro semestre do primeiro ano das licenciaturas em Ensino de Matemática e Matemática Aplicada e Computação, com uma carga horária semanal de apenas duas horas teórico-práticas, para facilitar a transição entre o Ensino Secundário e o Ensino Superior. Os seus principais objectivos são a introdução da linguagem e ferramentas matemáticas básicas e o exercício da capacidade de síntese e interpretação de textos matemáticos.

Embora este texto tenha circulado, desde de 2001, pelos alunos desta disciplina, só agora decidimos publica-lo na série de divulgação dos Cadernos de Matemática.

Domingos M. Cardoso e Domenico A. Catalano

Dezembro de 2005.

Capítulo 2

Introdução

A Matemática, tal como a generalidade das outras Ciências teve (e continua a ter) um forte desenvolvimento, particularmente depois do século $XVIII$, considerado por alguns autores como o século de transição entre a Matemática Clássica e a Matemática Contemporânea (ver, por exemplo, [Dieudonné, 1990]). Porém, em relação às restantes Ciências apresenta a desvantagem dessa evolução ser apenas conhecida dos matemáticos. Com efeito, a exigência de uma reflexão continuada e aprofundada para a compreensão das modernas teorias matemáticas afasta a possibilidade de acesso dos que não lhe dedicam o tempo, o empenho e a perseverança adequadas. Mesmo para a generalidade dos investigadores de outras Ciências que utilizam frequentemente modelos matemáticos nos seus trabalhos, essa utilização raramente vai além da Matemática Clássica.
Algumas correntes actuais dividem os matemáticos em construtores de teorias (*theory builders*) e resolvedores de problemas (*problem solvers*) mais do que em matemáticos puros e matemáticos aplicados. Muitos matemáticos, porém, consideram-se uma mistura destes dois tipos e ainda é muito comum a divisão da Matemática em Matemática Fundamental (ou Pura) e Matemática Aplicada. Esta última distingue-se da primeira essencialmente pela natureza da sua motivação. Com efeito, contrariamente ao que geralmente acontece com a Matemática Fundamental, a Matemática Aplicada começa por ser motivada por problemas concretos (dos quais muitas vezes se afasta) e esta característica leva a designa-la também por Matemática Motivada [**?**].
A Matemática Fundamental ou Aplicada é, antes de mais, um modo de pensar. Os que a praticam e compreendem entram num mundo maravilhoso de objectos abstractos e seus relacionamentos que por sua vez, quando convenientemente agrupados, permitem a dedução de novos objectos e diferentes relações em certos casos com resultados surpreendentes e quase sempre reveladores de uma harmonia espantosa com o contexto em que surgem. O que caracteriza um matemático é a sua insaciável curiosidade e o seu persistente desejo de vencer os desafios intelectuais, com que permanentemente se confronta, recorrendo à formalização, à abstracção e à dedução.
Com a disciplina de *Elementos de Matemática,* pretende-se despertar o interesse dos que iniciam os seus estudos superiores em Matemática pelo trabalho continuado na sua compreensão, procurando-se facilitar o contacto com os seus conceitos básicos, a identificação de diferentes níveis de abstracção, a utilização de uma linguagem apropriada ao rigor que a caracteriza e o desenvolvimento de raciocínios lógico-dedutivos.

Capítulo 3

Linguagem Matemática e Lógica Informal

Usualmente refere-se que a actividade matemática começa quando a partir da percepção de um certo número de objectos nos separamos desses objectos particulares e, em vez deles, consideramos o inteiro correspondente. Mais geralmente, elevando o nível de abstracção, os desenvolvimentos matemáticos passam pela criação de diferentes entidades que representamos por variáveis as quais, por sua vez, denotamos usualmente por letras. Embora se utilizem, indiscriminadamente, os vários alfabetos, é comum recorrer-se ao alfabeto grego na representação de variáveis com significado especial. Segue-se a lista das letras minúsculas e maiúsculas do alfabeto grego.

α	A	alfa	ν	N	niu
β	B	beta	ξ	Ξ	xi
γ	Γ	gama	o	O	omicron
δ	Δ	delta	π	Π	pi
ϵ	E	epsilon	ρ	P	ró
ζ	Z	zeta	σ	Σ	sigma
η	H	eta	τ	T	tau
θ	Θ	teta	υ	Υ	upsilon
ι	I	iota	ϕ	Φ	fi
κ	K	kapa	χ	X	chi
λ	Λ	lambda	ψ	Ψ	psi
μ	M	miu	ω	Ω	ómega.

Em Matemática, os conceitos e estruturas em jogo são introduzidas por *definições* que os caracterizam rigorosamente. No que se segue vamos começar por definir um dos conceitos mais fundamentais, o conceito de conjunto, bem como as relações e operações básicas que lhe estão associadas.

3.1 Noção de Conjunto

A noção de conjunto é, aparentemente, bem conhecida, mas, em geral, de um modo muito subjectivo, tanto mais que a necessária abrangência da sua definição coloca algumas dificuldades ao seu entendimento. Com efeito, define-se conjunto como

sendo *uma colecção de objectos* pelo que, praticamente, tudo são conjuntos. Essa abrangência deu até origem ao aparecimento de alguns paradoxos (os quais, por sua vez, chegaram mesmo a provocar uma crise profunda nos fundamentos da Matemática no princípio do século XX)[1]. O paradoxo mais famoso é o paradoxo de Bertrand Russel que foi escrito numa carta enviada a Frege, em 1902, na seguinte forma: *Seja C o conjunto de todos os conjuntos que são membros de si próprios e seja D o conjunto de todos os conjuntos que não são membros de si próprios. A pergunta que se coloca é: o conjunto D é ou não membro de si próprio.* Se D é membro de si próprio, então pertence a C e não a D pelo que não é membro de si próprio. Por outro lado, se D não é membro de si próprio então pertence a D pelo que é membro de si próprio. O paradoxo consiste no facto de ambas as situações (uma das quais inevitável) produzirem uma contradição. Outra versão deste paradoxo é designada por paradoxo do barbeiro, onde se questiona *quem barbeia o barbeiro que barbeia todos os que não se barbeiam a si próprios (e apenas estes)?* Esta crise, embora não totalmente superada, esbateu-se com as contribuições de Zermelo em 1908, Fraenkel e Skolem em 1922 e von Neumann em 1924, entre outros, os quais, de um modo geral, procuraram evitar as antinomias à custa de certas restrições impostas a um conjunto para ser considerado como tal.
Mais formalmente vamos proceder à definição de conjunto, conjunto vazio e de elementos de um conjunto.

Definição 3.1.1 *Um conjunto é uma colecção de objectos. Um conjunto vazio é um conjunto sem qualquer objecto e denota-se por $\varnothing$. Os elementos de um conjunto são os objectos que fazem parte da colecção que o constitui.*

Ao longo deste texto vamos denotar os conjuntos por letras maiúsculas e os seus possíveis elementos por letras minúsculas. Para se indicar que α é um elemento de A, escrevemos $\alpha \in A$, o que significa que α pertence a A. Muitas vezes estamos interessados em estudar conjuntos cujos elementos pertencem a um mesmo conjunto que designamos por *conjunto universal*. Neste caso, sendo $\mathcal{U}$ o conjunto universal e sendo A um conjunto de elementos de $\mathcal{U}$ também dizemos que A é um subconjunto de $\mathcal{U}$ e escrevemos $A \subseteq \mathcal{U}$. Dados dois conjuntos A e B de elementos do conjunto universal $\mathcal{U}$,

- dizemos que A é igual a B, escrevendo $A = B$, se A e B têm exactamente os mesmos elementos,

[1]Na verdade, ao longo da história da Matemática, desde a Antiguidade grega até aos nossos dias, existiram três crises profundas sobre os seus fundamentos. A primeira ocorreu no século V a.C., com a descoberta de que a diagonal e o lado de um quadrado não admitem a mesma unidade de medida (contrariando a convicção dos pitagóricos de que todas as grandezas da mesma espécie seriam comensuráveis). Esta crise embora ficasse resolvida com os estudos de Eudoxo (370 a. C.) sobre os incomensuráveis, os quais aparecem no quinto livro dos Elementos de Euclides (300 a. C.), só bastante mais tarde foi definitivamente superada com a moderna teoria dos números irracionais desenvolvida por Dedekind (em 1872). A segunda crise teve lugar no final do século $XVII$ (embora os paradoxos de Zenão, da impossibilidade do movimento (450 a. C.), constituíssem já um seu pronúncio) na sequência dos trabalhos de Newton e Leibnitz sobre os infinitésimos e só veio a ser resolvida no século XIX, com a introdução dos limites por Cauchy e a subsequente aritmetização da análise desenvolvida por Weierstrass e seus seguidores. Finalmente, a terceira crise eclodiu com os paradoxos ou antinomias descobertos na sequência do desenvolvimento da teoria dos conjuntos de Cantor. Para mais detalhes consultar, por exemplo, [Eves, 1997].

- dizemos que A é um subconjunto de B (ou que A está contido em B) e escrevemos $A \subseteq B$, se todos os elementos de A pertencem a B e ainda que A é um subconjunto estrito de B (ou que A está contido estritamente em B) e escreve-se $A \subset B$, se A é um subconjunto de B que não é igual a B.

Assim, enquanto na inclusão em sentido lato é irrelevante se A é ou não igual a B, na inclusão em sentido estrito a igualdade dos conjuntos A e B está completamente posta de parte.
Existem dois modos fundamentais de explicitar os elementos de um conjunto. Por extensão, com a indicação exaustiva de todos os seus elementos (por exemplo, $A = \{1, 10, x, 9, y\}$) ou por compreensão, com indicação do predicado[2] (por exemplo, $B = \{x : P(x)\}$, onde $P(x)$ denota um predicado a satisfazer por todos os elementos x do conjunto universal implicitamente assumido, $\mathcal{U}$, para pertencerem ao conjunto B). Em ambos os casos, quer a descrição exaustiva, quer o predicado caracterizador, são usualmente limitados pelas chavetas { e }.
Existem conjuntos particularmente importantes em Matemática, com os quais, pelo menos informalmente, já todos tomaram contacto, como sejam, *o conjunto dos número naturais* que denotaremos por $\mathbb{N}$, o conjunto dos número inteiros que denotaremos por $\mathbb{Z}$, o conjunto dos números racionais que denotaremos por $\mathbb{Q}$, o conjunto dos número reais que denotaremos por $\mathbb{R}$, etc.
É claro que podemos definir conjuntos à custa de outros conjuntos, por exemplo, $C = \{x \in \mathbb{Z} : -5 < x \leq 3\}$. Neste caso, o conjunto C é explicitado em compreensão, i.e, na forma $C = \{x : P(x)\}$, com $P(x)$ significando que x deve ser inteiro, não superior a 3 e maior que -5.
Note-se que a definição de um conjunto por compreensão obriga à utilização de variáveis cujos valores percorrem um certo conjunto universal implicitamente assumido.

Definição 3.1.2 *Dado um conjunto finito arbitrário, X, designa-se por cardinalidade de X e denota-se por $|X|$ o número de elementos de X. No caso de existir um número natural superior a esse número de elementos diz-se que X tem cardinalidade finita, caso contrário diz-se que tem cardinalidade infinita.*

Como consequência desta definição pode concluir-se, por exemplo, que a cardinalidade do conjunto vazio é zero, i.e, $|\varnothing| = 0$ e que, sendo C o conjunto acima referido, $|C| = 8$.

Tendo em conta que os conjuntos e subconjuntos são colecções de objectos com determinadas propriedades ou que satisfazem determinadas condições, as questões matemáticas, de um modo geral, podem reduzir-se ao reconhecimento de objectos (ou conjuntos de objectos) enquanto elementos (ou subconjuntos) de um determinado conjunto. Assim, sendo $X = \{x : P(x)\}$, se todos os objectos que satisfazem o predicado $P(x)$ também satisfazem o predicado $Q(x)$, podemos concluir que sendo $Y = \{y : Q(y)\}$, então $X \subseteq Y$. Nestes casos, em linguagem matemática, dizemos que $P(x)$ implica $Q(x)$ ou, de modo semelhante, se um objecto x satisfaz a propriedade

[2]Por agora, pode entender-se um predicado como sendo uma ou várias propriedades, ou condições, que podem (ou não) ser satisfeitas pelos elementos abrangidos.

ou condição P então também satisfaz a propriedade ou condição Q e escrevemos

$$P(x) \Rightarrow Q(x).$$

Esta implicação significa, então, que o conjunto dos objectos com a propriedade P está contido no conjunto dos objectos com a propriedade Q.

Exemplo 3.1.3 *Seja Y=$\{y$: y é inteiro múltiplo de 4$\}$ e seja X=$\{x$: x é inteiro par$\}$. É claro que $Y \subset X$, o que significa que*

$$z \text{ inteiro múltiplo de } 4 \Rightarrow z \text{ inteiro par.}$$

Quando $P(x) \Rightarrow Q(x)$ e $Q(x) \Rightarrow P(x)$, diz-se que $P(x)$ é equivalente a $Q(x)$ e escreve-se

$$P(x) \Leftrightarrow Q(x).$$

Nestas condições, $P(x) \Leftrightarrow Q(x)$ significa, por um lado que

$$X = \{x : P(x)\} \subseteq \{y : Q(y)\} = Y \tag{3.1}$$

e por outro que

$$Y = \{y : Q(y)\} \subseteq \{x : P(x)\} = X. \tag{3.2}$$

Como consequência podemos concluir que

$$X = \{x : P(x)\} = \{y : Q(y)\} = Y.$$

Com efeito, de acordo com (3.1), todos os elementos de X são elementos de Y e, de acordo com (3.2), não existe um elemento de Y que não seja elemento de X.
Se o conjunto $Z = \{z : S(z)\}$ é vazio, tal significa que nenhum objecto verifica a propriedade ou condição S. Por outro lado, se $X = \{x : P(x)\} \not\subseteq \{y : Q(y)\} = Y$ tal significa que a implicação $P(x) \Rightarrow Q(x)$ é falsa.

3.2 Linguagem Proposicional

As afirmações que são verdadeiras ou falsas, designam-se, em linguagem matemática, por proposições. Segue-se a definição formal de proposição.

Definição 3.2.1 *Uma proposição é uma afirmação que é verdadeira ou falsa.*

Exemplo 3.2.2 *São exemplos de proposições as seguintes:*

(a) A equação $x^2 - 4 = 0$ tem duas soluções inteiras.

(b) Se $n \in \mathbb{N}$ então $n^5 - n$ é divisível por 30.

(c) $n \in \mathbb{N} \Rightarrow 2^n > \sum_{k=0}^{n} \binom{n}{k}$. [3]

São exemplos de afirmações que não são proposições as seguintes:

[3] $\binom{n}{k}$ denota o número de combinações de n objectos k a k.

(d) $x^2 - 4 = 0$.

(e) Apreciem a paisagem.

(f) x *é maior do que* y.

Note-se que embora (a), (b) e (c) sejam proposições, apenas (a) e (b) são proposições verdadeiras.
Quando se define $C = \{x : P(x)\}$, onde x é uma variável que percorre o conjunto universal implicitamente considerado, embora $P(x)$ possa tomar valores verdadeiros ou falsos, não se pode dizer que $P(x)$ é uma proposição. Com efeito, assumindo que para certos valores da variável x, $P(x)$ é verdadeiro e para outros falso, sem se concretizar x não faz sentido atribuir o valor verdadeiro ou falso a $P(x)$. Porém, fixando $P(x)$ para um valor particular de x, já se pode afirmar que se trata de uma proposição. Por exemplo, admitindo que $P(x)$ significa x *é par* (onde x é uma variável que toma valores inteiros), fazendo $x = 5$, $P(5)$ (que significa 5 *é par*) é uma proposição (que no caso é falsa).
Para evitar ambiguidades passaremos a denotar as proposições por letras minúsculas. Assim, no caso anterior, podemos denotar a proposição $P(5)$ simplesmente por p.
Uma proposição diz-se *atómica* quando não se pode decompor noutras proposições e diz-se *composta* no caso contrário. Por exemplo, dadas duas proposições atómicas p e q, podemos combina-las de modo a obter a proposição composta

$$p \Rightarrow q$$

que se designa por *proposição condicional* ou *implicação* e se lê *se* p *então* q ou p *implica* q [4]. Esta proposição significa que se p é verdadeiro então q também é verdadeiro. Como consequência, também se diz q **se** p ou p **somente se** q, sendo ainda usual dizer-se que p é suficiente (ou uma condição suficiente) para q e que q é necessária (ou uma condição necessária) para p.

Exemplo 3.2.3 *A proposição* **se o cão tem fome então o cão come muito** *é uma proposição condicional que se pode denotar por* $p \Rightarrow q$*, onde* p *representa a proposição atómica* **o cão tem fome** *e* q *a proposição atómica* **o cão come muito**. *Neste caso,* **o cão tem fome** *é uma condição suficiente para a proposição* **o cão come muito** *e esta, por sua vez, é uma condição necessária para a proposição* **o cão tem fome**.

Uma proposição composta caracteriza-se completamente à custa da tabela dos valores lógicos que adquire, VERDADEIRO (V) ou FALSO (F), quando se percorrem todos os possíveis valores lógicos das proposições atómicas que a constituem, a qual se designa por *tabela de verdade*. No caso da proposição composta $p \Rightarrow q$ (que é falsa apenas quando p é verdadeiro mas q é falso) a tabela de verdade que lhe corresponde é a que a seguir se indica.

[4] As vezes, a proposição condicional $p \Rightarrow q$ é denota também por $q \Leftarrow p$.

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

Por vezes presumimos um conjunto de proposições todas verdadeiras, noutros casos supomos que pelo menos uma, de entre um conjunto delas, é verdadeira, e, noutras situações ainda, interessa-nos negar o valor lógico de uma certa proposição. Para traduzir todos estes contextos e obter proposições compostas mais complexas, a linguagem proposicional faz uso das conjunções, disjunções e negações.
A tabela que se segue explicita as tabelas de verdade da conjunção p **e** q (que denotaremos por $p \wedge q$), da disjunção p **ou** q (que denotaremos por $p \vee q$) e da negação **não** p (que denotaremos por $\neg p$).

p	q	$p \wedge q$	$p \vee q$	$\neg p$
V	V	V	V	F
V	F	F	V	F
F	V	F	V	V
F	F	F	F	V

A partir das tabelas de verdade da conjunção, disjunção e negação, com facilidade se determinam tabelas de verdade de proposições compostas mais complexas, que também designaremos por expressões proposicionais (ou lógicas). Par tal, torna-se conveniente a identificação das variáveis proposicionais que, por sua vez, denotam outras proposições (atómicas ou compostas) e a determinação dos valores lógicos de subexpressões sucessivamente mais complexas. Por exemplo, para se determinar a tabela de verdade da expressão lógica $\neg p \vee q$, poderemos adoptar o procedimento associado á tabela a seguir representada.

p	q	$\neg p$	$\neg p \vee q,$
V	V	F	V
V	F	F	F
F	V	V	V
F	F	V	V

Segue-se um exemplo, um pouco mais complexo que o anterior, onde apenas se apresentam os valores lógicos de algumas subexpressões da expressão proposicional cuja tabela de verdade se pretende determinar.

Exemplo 3.2.4 *Determinação da tabela de verdade de* $[(p \wedge q) \vee r] \wedge [\neg(p \wedge r)]$.

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

Dadas duas proposições p e q, a proposição composta $(p \Rightarrow q) \wedge (q \Rightarrow p)$ denota-se por $p \Leftrightarrow q$ e designa-se por equivalência entre p e q. Neste caso lê-se p **se e somente se (sse)** q para significar que as proposições p e q têm exactamente os mesmos valores lógicos. Consequentemente, $p \Leftrightarrow q$ é uma proposição composta que toma o valor lógico verdadeiro quando e apenas quando as proposições p e q têm os mesmos valores lógicos. Com efeito, esta conclusão pode ser retirada da respectiva tabela de verdade.

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

Deve observar-se que uma variável proposicional não denota necessariamente uma proposição atómica. Com efeito, pode tornar-se conveniente denotar uma proposição composta por uma certa variável proposicional, pelo que todas as conclusões que obtivermos acerca de expressões lógicas se mantêm válidas quando qualquer das variáveis é substituída por uma proposição composta (assumindo-se, obviamente, que essa proposição composta toma os mesmos valores lógicos da variável que a representa).
O que acabamos de referir leva-nos a introduzir o conceito de fórmula bem formada da linguagem proposicional, uma vez que, embora estas fórmulas sejam sequências de símbolos de um determinado conjunto, nem todas as sequências de símbolos fazem sentido do ponto de vista da linguagem proposicional. No nosso caso, o conjunto de símbolos adoptado inclui as letras minúsculas de um qualquer alfabeto (que representam variáveis proposicionais) e, por agora, o conjunto de símbolos especiais $\{(,), \neg, \wedge, \vee, \Rightarrow, \Leftarrow, \Leftrightarrow\}$. Os parêntesis são utilizados apenas para tornar clara uma determinada subexpressão (note-se que, por exemplo, $\neg p \wedge q$ é diferente de $\neg(p \wedge q)$). Mais formalmente, uma fórmula bem formada da linguagem proposicional pode definir-se do seguinte modo:

Definição 3.2.5 *Qualquer variável representando uma proposição atómica é uma fórmula bem formada. Se r é uma fórmula bem formada então (r) é também uma fórmula bem formada. Por outro lado, admitindo que p e q representam fórmulas bem formadas, $\neg p$, $p \vee q$, $p \wedge q$, $p \Rightarrow q$, $p \Leftarrow q$ e $p \Leftrightarrow q$ são ainda fórmulas bem formadas.*

Neste texto, as fórmulas bem formadas da linguagem proposicional são designadas, simplesmente, por fórmulas da linguagem proposicional.
Existem certas fórmulas da linguagem proposicional que são sempre verdadeiras quaisquer que sejam os valores lógicos das suas variáveis (como por exemplo, $p \vee \neg p$) e outras que são sempre falsas (como por exemplo, $p \wedge \neg p$). As primeiras designam-se por *tautologias* e as segundas por *contradições*.

Definição 3.2.6 *Duas expressões lógicas, r e s, dizem-se equivalentes se $r \Leftrightarrow s$ é uma tautologia.*

Com base nesta definição, podemos concluir que duas expressões lógicas, com as mesmas variáveis, são equivalentes quando têm a mesma tabela de verdade. Por outro

lado, podemos afirmar que tanto a conjunção como a disjunção são comutativas, no sentido em que $p \vee q$ é equivalente a $q \vee p$ (ou seja, $(p \vee q) \Leftrightarrow (q \vee p)$ é uma tautologia) e $p \wedge q$ é equivalente a $q \wedge p$ (ou seja, $(p \wedge q) \Leftrightarrow (q \wedge p)$ é uma tautologia), conforme decorre, imediatamente, das respectivas tabelas de verdade.

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

De igual modo se conclui que $p \Rightarrow q$ é equivalente a $\neg p \vee q$, bem como as seguintes propriedades do *Cálculo Proposicional*.

- Leis de De Morgan

  $\neg(p \wedge q)$ é equivalente a $\neg p \vee \neg q$,
  $\neg(p \vee q)$ é equivalente a $\neg p \wedge \neg q$.

- Associatividade

  $p \wedge (q \wedge r)$ é equivalente a $(p \wedge q) \wedge r$,
  $p \vee (q \vee r)$ é equivalente a $(p \vee q) \vee r$.

- Idempotência

  $p \wedge p$ é equivalente a p,
  $q \vee q$ é equivalente a q.

- Distributividade

  $p \wedge (q \vee r)$ é equivalente a $(p \wedge q) \vee (p \wedge r)$,
  $p \vee (q \wedge r)$ é equivalente a $(p \vee q) \wedge (p \vee r)$.

- Dupla negação

  $\neg(\neg p)$ é equivalente a p.

Tendo presente os conceitos de tautologia e contradição, e assumindo p como uma proposição arbitrária, podemos concluir ainda que

- $p \wedge$ (tautologia) é equivalente a p,
- $p \vee$ (tautologia) é uma tautologia,
- $\neg$(tautologia) é uma contradição,
- $p \wedge$ (contradição) é uma contradição,
- $p \vee$ (contradição) é equivalente a p,
- $\neg$(contradição) é uma tautologia.

Recorrendo a estas últimas propriedades, poderemos simplificar algumas fórmulas de modo a obter fórmulas equivalentes com menos variáveis proposicionais. Por exemplo, em vez de $p \vee (q \wedge \neg p)$ podemos considerar a fórmula equivalente $p \vee q$ (dado que $p \vee (q \wedge \neg p)$ é equivalente a $(p \vee q) \wedge (p \vee \neg p)$ a qual, por sua vez, é equivalente a $p \vee q$, tendo em conta que, $p \vee \neg p$ é uma tautologia).
Para além do conectivo *ou* (que se designa também por *ou inclusivo*) e se denota por $\vee$, por vezes adopta-se o *ou exclusivo* que se denota por $\dot{\vee}$. Este *ou exclusivo* aplicado às proposições p e q, produz a proposição $p \dot{\vee} q$ que significa p *ou* q *mas não ambos*. Assim, a proposição $p \dot{\vee} q$ é verdadeira quando uma e apenas uma das proposições p ou q é verdadeira.
Seguem-se alguns exercícios.

- **Exercícios**

1. Determine as tabelas de verdade das proposições
   (a) $(p \Rightarrow q) \Rightarrow r$.
   (b) $(p \Rightarrow q) \Leftrightarrow (\neg q \Rightarrow \neg p)$.
   (c) $(r \Rightarrow (\neg q \vee p)) \Leftarrow (p \Rightarrow \neg q)$.
   (d) $p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$.
   (e) $p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$.
   (f) $\neg(p \wedge q) \wedge (\neg p \vee \neg(\neg q \vee (\neg p \vee q)))$.
2. Verifique quais os pares de expressões lógicas, a seguir indicados, incluem expressões lógicas equivalentes.
   (a) $(p \Rightarrow q)$ e $\neg p \Leftarrow \neg q$.
   (b) $\neg(p \wedge \neg q)$ e $\neg p \vee q$.
   (c) $\neg(\neg p)$ e p.
   (d) $\neg(p \vee \neg q)$ e $\neg p \wedge q$.
   (e) $((p \wedge q) \vee (p \wedge \neg q)) \wedge (r \vee \neg r)$ e p.
   (f) $(p \wedge q) \Leftarrow p$ e $(p \wedge q) \vee \neg p$.
3. Indique qual ou quais das expressões a seguir indicadas são tautologias, contradições ou nem uma coisa nem outra.
   (a) $p \Rightarrow (\neg p \Rightarrow q)$.
   (b) $(p \wedge q) \Rightarrow (p \vee q)$.
   (c) $p \Rightarrow (q \Rightarrow (q \Rightarrow p))$.
   (d) $p \vee (q \vee \neg p)$.
   (e) $p \wedge \neg(q \vee \neg q)$.
   (f) $p \vee \neg(q \vee \neg q)$.
4. Simplifique (se possível) as fórmulas proposicionais a seguir indicadas.
   (a) $\neg(p \vee (q \wedge (\neg r)) \wedge q$.
   (b) $\neg(\neg p \wedge \neg q)$.
   (c) $\neg(\neg p \vee q) \vee (p \wedge \neg r)$.
   (d) $(p \wedge q) \vee (p \wedge \neg q)$.
   (e) $(p \wedge r) \vee [\neg r \wedge (p \vee q)]$.

(f) $(\neg p \vee q) \wedge (p \wedge \neg q)$.

5. Tendo em conta que a proposição p *ou* q *mas não ambos*, que se designa por *ou exclusivo*, se denota por $p \dot{\vee} q$, responda às questões a seguir indicadas.
   (a) Determine a tabela de verdade de $p \dot{\vee} q$.
   (b) Encontre uma fórmula equivalente a $p \dot{\vee} q$, utilizando apenas os conectivos lógicos $\wedge$, $\vee$ e $\neg$.
   (c) Justifique a resposta da alínea anterior com recurso às respectivas tabelas de verdade.
   (d) Verifique se a fórmula proposicional $(p \dot{\vee} q) \Leftrightarrow (\neg p \dot{\vee} \neg q)$ é (ou não) uma tautologia.
   (e) Concluia que $(p \dot{\vee} \neg q) \wedge (\neg p \dot{\vee} q)$ é equivalente a $(p \wedge q) \vee (\neg p \wedge \neg q)$.
   (f) Simplifique a expressão lógica $(p \dot{\vee} \neg q) \dot{\vee} (\neg p \vee q)$.

3.3 Operações sobre Conjuntos

Com base nos conectivos lógicos anteriormente introduzidos estamos em condições de avançar, um pouco mais, no estudo dos conjuntos, particularmente no estudo das operações sobre conjuntos.
É muito comum representar os conjuntos de uma forma pictórica, por intermédio de diagramas, conhecidos por *diagramas de Venn*. A figura a seguir ilustra este tipo de representação, denotando dois conjuntos A e B com intersecção não vazia.

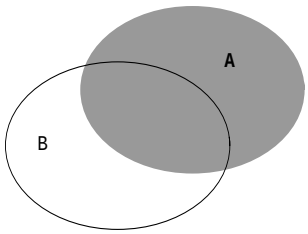

Figura 3.1: Diagrama de Venn de dois conjuntos A e B com intersecção não vazia.

Vamos começar por definir formalmente as principais operações sobre conjuntos, ou seja, a intersecção, a união, a diferença, a diferença simétrica e a complementação.

Definição 3.3.1 *Sejam A e B dois subconjuntos de um certo universo $\mathcal{U}$.*

- *A intersecção de A e B denota-se por $A \cap B$ e é definida pelo conjunto*

$$A \cap B \;=\; \{x : (x \in A) \wedge (x \in B)\}. \tag{3.3}$$

- *A união de A e B denota-se por $A \cup B$ e é definida pelo conjunto*

$$A \cup B \;=\; \{x : (x \in A) \vee (x \in B)\}. \tag{3.4}$$

- *A diferença entre A e B denota-se por $A \setminus B$ e é definida pelo conjunto*

$$A \setminus B = \{x : (x \in A) \wedge (x \notin B)\}. \tag{3.5}$$

- *A diferença simétrica entre A e B denota-se por $A\Delta B$ e é definida pelo conjunto*

$$A\Delta B = \{x : (x \in A) \dot{\vee} (x \in B)\}. \tag{3.6}$$

- *O complementar de A denota-se por $\overline{A}$ e é definido pelo conjunto*

$$\overline{A} = \{x : x \notin A\}. \tag{3.7}$$

Assumindo que $A = \{x : P(x)\}$ e $B = \{y : Q(y)\}$ são dois subconjuntos do universo $\mathcal{U}$, em alternativa às definições anteriores, podemos afirmar que

1. $$A \cap B = \{x : P(x) \wedge Q(x)\}. \tag{3.8}$$

   Com efeito,

   $$\begin{aligned} A \cap B &= \{x : (x \in A) \wedge (x \in B)\} && \text{(de acordo com (3.3))} \\ &= \{x : P(x) \wedge Q(x)\} && \text{(de acordo com a definição de } A \text{ e } B). \end{aligned}$$

2. $$A \cup B = \{x : P(x) \vee Q(x)\}. \tag{3.9}$$

   Com efeito,

   $$\begin{aligned} A \cup B &= \{x : (x \in A) \vee (x \in B)\} && \text{(de acordo com (3.4))} \\ &= \{x : P(x) \vee Q(x)\} && \text{(de acordo com a definição de } A \text{ e } B). \end{aligned}$$

3. $$\overline{A} = \{x : \neg P(x)\}. \tag{3.10}$$

   Com efeito,

   $$\begin{aligned} \overline{A} &= \{x : x \notin A\} && \text{(de acordo com (3.7))} \\ &= \{x : \neg(x \in A)\} \\ &= \{x : \neg P(x)\} && \text{(tendo em conta a definição de } A). \end{aligned}$$

4. $$A \setminus B = \{x : P(x) \wedge \neg Q(x)\}. \tag{3.11}$$

   Com efeito,

   $$\begin{aligned} A \setminus B &= \{x : (x \in A) \wedge (x \notin B)\} && \text{(de acordo com (3.5))} \\ &= \{x : (x \in A) \wedge \neg(x \in B)\} \\ &= \{x : P(x) \wedge \neg Q(x)\} && \text{(de acordo com a definição de } A \text{ e } B). \end{aligned}$$

5.

$$A\Delta B = \{x : P(x)\dot{\vee}Q(x)\} = (A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A). \quad (3.12)$$

Com efeito,

$$\begin{aligned} A\Delta B &= \{x : (x \in A)\dot{\vee}(x \in B)\} && \text{(tendo em conta (3.6))} \\ &= \{x : ((x \in A) \vee (x \in B)) \wedge \neg((x \in A) \wedge (x \in B))\} && \text{(de acordo com a definição de ou exclusivo)} \\ &= \{x : (x \in A) \vee (x \in B)\} \setminus \{x : (x \in A) \wedge (x \in B)\} && \text{(de acordo com (3.11))} \\ &= (A \cup B) \setminus (A \cap B) && \text{(de acordo com (3.9) e (3.8)).} \end{aligned}$$

Por outro lado, da igualdade

$$A\Delta B = \{x : ((x \in A) \vee (x \in B)) \wedge \neg((x \in A) \wedge (x \in B))\}$$

vem que $A\Delta B = \{x : \neg((x \in A) \wedge (x \in B)) \wedge ((x \in A) \vee (x \in B))\}$ e, consequentemente,

$$\begin{aligned} A\Delta B &= \{x : (\neg((x \in A) \wedge (x \in B)) \wedge (x \in A)) \vee (\neg((x \in A) \wedge (x \in B)) \wedge (x \in B))\} \\ &\qquad \text{(tendo em conta a distributividade)} \\ &= \{x : \neg((x \in A) \wedge (x \in B)) \wedge (x \in A)\} \cup \{x : \neg((x \in A) \wedge (x \in B)) \wedge (x \in B)\} \\ &\qquad \text{(de acordo com (3.4))} \\ &= \{x : (\neg(x \in A) \vee \neg(x \in B)) \wedge (x \in A)\} \cup \\ &\quad \{x : (\neg(x \in A) \vee \neg(x \in B)) \wedge (x \in B)\} \qquad \text{(pelas leis de De Morgan)} \\ &= \{x : \neg(x \in B) \wedge (x \in A)\} \cup \{x : \neg(x \in A) \wedge (x \in B)\} \\ &\qquad \text{(pela distributividade)} \\ &= (A \setminus B) \cup (B \setminus A) \qquad \text{(tendo em conta (3.5)).} \end{aligned}$$

Sendo A, B e C três subconjuntos arbitrários de um certo universo, $\mathcal{U}$, com facilidade se concluem as seguintes propriedades das operações sobre conjuntos:

- $A \setminus A = \varnothing = \varnothing \setminus A$.
- $A \setminus \varnothing = A$.
- $A \setminus B = B \setminus A \Leftrightarrow A = B$.
- $\overline{(\overline{A})} = A$.
- $\overline{\varnothing} = \mathcal{U}$ e $\overline{\mathcal{U}} = \varnothing$.
- Comutatividade: $A \cap B = B \cap A$, $A \cup B = B \cup A$.
- Associatividade: $A \cap (B \cap C) = (A \cap B) \cap C$, $A \cup (B \cup C) = (A \cup B) \cup C$.

- Distributividade:
$$\begin{aligned} A \cap (B \cup C) &= (A \cap B) \cup (A \cap C), \\ A \cup (B \cap C) &= (A \cup B) \cap (A \cup C). \end{aligned}$$

- Leis de De Morgan:
$$\begin{aligned} A \setminus (B \cup C) &= (A \setminus B) \cap (A \setminus C), \\ A \setminus (B \cap C) &= (A \setminus B) \cup (A \setminus C), \\ \overline{A \cup B} &= \overline{A} \cap \overline{B}, \\ \overline{A \cap B} &= \overline{A} \cup \overline{B}. \end{aligned}$$

Recordando que dois conjuntos A e B são iguais quando têm os mesmos elementos, podemos concluir que se $A \subseteq B$ e $B \subseteq A$ então $A = B$. Em Matemática, este tipo de afirmações, que muitas vezes tomam a forma:
se certas suposições (usualmente designadas por hipóteses) são verdadeiras então uma dada conclusão (usualmente designada por tese) é também verdadeira,
designam-se por *teoremas*.

Os teoremas são resultados matemáticos já provados com argumentos lógico-dedutivos aceites como válidos para fundamentar as respectivas conclusões. Porém, embora esta aceitabilidade dos argumentos utilizados nas provas (ou demonstrações) dos teoremas tenha hoje um tratamento relativamente homogéneo, nem sempre foi assim. Particularmente, no princípio do século XX, apareceram duas correntes de pensamento matemático (os *Intuicionistas* e os *Formalistas*) com concepções completamente distintas do que deveria ser uma demonstração. A escola (ou corrente) intuicionista, que nasceu com o matemático holandês Brouwer $(1881-1966)$, defende que a Matemática deve ser desenvolvida apenas por métodos construtivos finitos, enquanto a escola formalista, criada por David Hilbert $(1862-1943)$, encara a Matemática como estudo de sistemas simbólicos formais.
A concepção matemática dos intuicionistas tem como consequência que a prova da existência de uma certa entidade só é aceite quando se mostra que ela é construtível num número finito de passos, não bastando mostrar, por exemplo, que a não existência da entidade em causa implica uma contradição. Esta limitação significa que muitas das demonstrações da Matemática Contemporânea não são aceites pelos intuicionistas. Outra consequência importante da exigência da construtibilidade finita é a não aceitação universal da *lei do terceiro excluído* que, para os intuicionistas, só é válida em conjuntos finitos. Este facto implica a não aceitação (no caso geral) da demonstração por *reductio ad absurdum*. A seu favor, porém, tudo aponta, na *Matemática Intuicionista*, para a ausência de contradições internas (o que, conforme já se referiu, não acontece nas abordagens clássicas)[5]. Por sua vez, os formalistas consideram a Matemática como um jogo de desenvolvimentos abstractos onde se vão produzindo novas fórmulas de símbolos a partir das anteriores, segundo regras muito precisas. Hilbert acreditava que, a partir de um conjunto de certas regras e procedimentos com os quais se obteriam as novas fórmulas que traduziriam os novos resultados, se construiria um sistema não contraditório, i.e, onde não fosse possível produzir uma contradição (fórmula do tipo $p \wedge \neg p$.). Porém, tal revelou-se impossível, conforme veio a provar Kurt Gödel em 1931 (por métodos aceites por todas as prin-

[5]Apesar do esforço de vários investigadores no sentido de reconstruir toda a Matemática dentro das limitações da *Matemática Intuicionista*, o seu desenvolvimento tem-se revelado pouco produtivo e, muitas vezes, mais complicado que as abordagens clássicas.

cipais correntes matemáticas[6]). A demonstração, apresentada por Gödel, de que o sistema de Hilbert não é completo (i.e., contém proposições indecidíveis, entre as quais a sua própria consistência) tornaram visíveis limitações, até então insuspeitas, dos métodos matemáticos formais e vieram estabelecer a separação entre *verdadeiro* e *demonstrável*.

Em Matemática, as afirmações não provadas, relativamente às quais existe a expectativa de se vir a encontrar uma prova, designam-se por *conjecturas* e, tais afirmações, enquanto não se provam ou refutam, fazem parte dos desafios da investigação matemática corrente.

Uma conjectura famosa que se tem revelado difícil de provar ou refutar (constituindo um dos maiores desafios matemáticos contemporâneos) é a conjectura de Goldbach onde se afirma que *todo o inteiro par superior a* 2 *é soma de dois primos* [7].

É fácil ver que $4 = 2+2$, $6 = 3+3$, $8 = 3+5$, $10 = 3+7$, $12 = 7+5$, $14 = 7+7$, etc, porém, como o número de inteiros positivos pares é infinito, é impossível proceder à verificação exaustiva de todos eles. Assim, a prova (ou refutação) desta conjectura deverá recorrer aos conceitos abstractos de número par maior do que 2 (ou seja, $2k$, com k natural maior do que 1) e de número primo. Deve observa-se que para se refutar esta conjectura "basta"encontrar um *contraexemplo*, i.e., um número natural $k > 1$ tal que para todo o número primo arbitrário menor que $2k$, p, se verifica que $2k - p$ é um número composto (ou seja, é tal que entre os seus divisores consta, pelo menos, um inteiro maior do que 1 e menor do que $2k - p$).

De agora em diante, sempre que se tornar conveniente, apresentaremos, formalmente, as conclusões decorrentes dos conceitos e propriedades previamente estabelecidas na forma de teoremas, com a apresentação das respectivas provas ou a indicação de que devem ser efectuadas como exercício, de modo a incutir o hábito e a desenvolver as técnicas de demonstração.

Exemplificando, com a condição suficiente para a igualdade de conjuntos, anteriormente referida, tem-se:

Teorema 3.3.2 *Dados os conjuntos A e B, se $A \subseteq B$ e $B \subseteq A$ então $A = B$.*

Demonstração: Tendo em conta que $(A \subseteq B) \wedge (B \subseteq A)) \Rightarrow (A = B)$ é equivalente a $(A \neq B) \Rightarrow \neg((A \subseteq B) \wedge (B \subseteq A))$, vamos provar este teorema provando a última implicação. Suponha-se $A \neq B$, o que significa que ou existe $x \in A$ tal que $x \notin B$ ou existe $y \in B$ tal que $y \notin A$. Logo ou $A \not\subseteq B$ ou $B \not\subseteq A$, pelo que concluímos que a proposição $\neg(A \subseteq B) \vee \neg(B \subseteq A)$ é verdadeira, o que completa a demonstração. **qed**

[6]Existe ainda uma terceira escola, a *Logicista*, que reduz a Matemática a um ramo da Lógica. Segundo esta corrente a Lógica em vez de ser um instrumento da Matemática passa a ser a sua génese. Os principais impulsionadores desta filosofia foram Whitehead ($1861 - 1947$) e Russel ($1872 - 1970$) os quais, com a publicação da célebre obra *Principia mathematica*, estabeleceram as bases para o estudo da Matemática segundo os modelos e desenvolvimentos determinados pela Lógica.

[7]Na verdade, numa carta datada de 1742, Christian Goldbach (1690-1764) conjecturou que

todo o inteiro superior a 5 *se pode exprimir como soma de três primos.*

Logo (tendo em conta que um primo é um inteiro maior do que 1, sem divisores menores do que ele e maiores do que 1) conclui-se que, se a conjectura for verdadeira, sendo k um inteiro par maior do que 5 tal que $k = x + y + z$, com x, y e z primos, então um deles é 2 (que é um primo par). Assim, supondo $x = 2$, conclui-se que $k - x = y + z$, o que implica que todo o inteiro par superior a 3 seja soma de dois primos. Note-se também que no caso do inteiro k maior do que 5 ser ímpar, vem que $k - 3$ é um inteiro par maior do que 2.

A conjectura de Goldbach foi reescrita, tal como hoje se apresenta, por Leonhard Euler (1707-1783).

As iniciais **qed** (iniciais de *quod erat demonstrandum*) ou **cqd** (iniciais de *como se queria demonstrar*), classicamente utilizadas para indicarem o fim da demonstração, são modernamente substituídas por outros símbolos, como por exemplo $\diamondsuit$ ou $\blacksquare$.
O teorema que se segue estabelece duas propriedades interessantes da inclusão de conjuntos.

Teorema 3.3.3 *Dados os conjuntos X, Y e Z verifica-se:*

1. *Se $X \subseteq Z$ e $Y \subseteq Z$ então $X \cup Y \subseteq Z$.*
2. *Se $Z \subseteq X$ e $Z \subseteq Y$ então $Z \subseteq X \cap Y$.*

Demonstração: 1. Se $z \in X \cup Y$ então ou $z \in X$ ou $z \in Y$. Em qualquer dos casos, uma vez que $X \subseteq Z$ e $Y \subseteq Z$, conclui-se que $z \in Z$. Logo $X \cup Y \subseteq Z$.
2. Esta prova fica como exercício. **qed**

A união e a intersecção pode estender-se, de um modo natural, a famílias finitas ou infinitas de conjuntos. Com efeito, considerando a família de conjuntos $\{A_i\}_{i\in I}$, onde I denota um conjunto de índices, vem que

$$\bigcup_{i\in I} A_i = \{x : x \in A_i \text{ para algum } i \in I\}, \tag{3.13}$$

$$\bigcap_{i\in I} A_i = \{x : x \in A_i \text{ para todo } i \in I\}. \tag{3.14}$$

Uma família de conjuntos $\{A_i\}_{i\in I}$ diz-se *disjunta* se $\bigcap_{i\in I} A_i = \varnothing$ e diz-se *dois a dois disjunta* se $i \neq j \Rightarrow A_i \cap A_j = \varnothing$. Por exemplo, dada a família de conjuntos $\{[\frac{1}{i}, i]\}_{i\in\mathbf{N}}$ que corresponde à família de intervalos $[1,1]$, $[\frac{1}{2},2]$, $[\frac{1}{3},3]$, etc, vem que

$$\forall p < q \qquad [\frac{1}{p}, p] \cap [\frac{1}{q}, q] = [\frac{1}{p}, p]$$

e ainda que

$$\bigcup_{i\in\mathbf{N}} [\frac{1}{i}, i] =]0, +\infty[, \qquad \bigcap_{i\in\mathbf{N}} [\frac{1}{i}, i] = \{1\}$$

concluindo-se que a família $\{[\frac{1}{i}, i]\}_{i\in\mathbf{N}}$ não é nem disjunta nem dois a dois disjunta.

Os conjuntos definidos em (3.13) e (3.14) sugerem a introdução de símbolos matemáticos adequados a estas situações, os quais se designam por quantificadores. Assim, em linguagem simbólica, em vez de (3.13) poderia escrever-se

$$\bigcup_{i\in I} A_i = \{x : \exists i \in I \ (x \in A_i)\},$$

onde $\exists i \in I$, significa *existe i pertencente a I*. Este quantificador designa-se por quantificador existencial [8].
Quando se pretende indicar que existe um único elemento que satisfaz determinada propriedade (ou condição), por exemplo, que dado $x \in \mathbb{R}\backslash\{0\}$ existe um único $y \in \mathbb{R}$,

[8] Note-se que $\exists y \in Y \ Q(y)$ significa, em linguagem simbólica mais precisa, $\exists y \ (y \in Y \wedge Q(y))$.

tal que $x \times y = y \times x = 1$, escreve-se $\exists! y \in \mathbb{R}\ (x \times y = y \times x = 1)$.
Por outro lado, em linguagem simbólica, em vez de (3.14) poderia escreve-se

$$\bigcap_{i \in I} A_i = \{x : \forall i \in I\ (x \in A_i)\},$$

onde $\forall i \in I$, significa *para todo i pertencente a I*. Este quantificador designa-se por quantificador universal [9].
Os quantificadores existenciais e universais são utilizados em fórmulas que envolvem variáveis, para limitarem ou estenderem o âmbito em que se verifica(m) determinada(s) propriedade(s). Os quantificadores podem agrupar-se, de modo adequado, numa mesma fórmula.
A seguir, exemplificam-se algumas fórmulas que envolvem vários quantificadores.

Exemplo 3.3.4 1. $(\forall n \in \mathbb{N} \setminus \{1\})\ (\exists p\ (p \text{ é primo e } n < p < 2n))$.
2. $\forall x\ ((x \in \mathbb{R} \wedge x \geq 0) \Rightarrow \exists y\ (y \in \mathbb{R} \wedge y^2 = x))$.

Em fórmulas que envolvem quantificadores é crucial reconhecer o alcance de cada um deles, i.e, a parte da fórmula sobre a qual actua. No caso do exemplo 3.3.4, em 1, o alcance do quantificador universal é a fórmuala

$$\exists p\ (p \text{ é primo e } n < p < 2n)$$

e o alcance do quantificador existencial é a fórmula

$$p \text{ é primo e } n < p < 2n.$$

Por vezes torna-se conveniente negar expressões que envolvem quantificadores. Após uma análise cuidada das expressões $\forall x\ P(x)$ e $\exists y\ Q(y)$, concluem-se as seguintes equivalências:

$$\neg(\forall x\ \ P(x)) \equiv \exists x\ \neg P(x); \tag{3.15}$$
$$\neg(\exists y\ \ Q(y)) \equiv \forall y\ \neg Q(y). \tag{3.16}$$

O símbolo $\equiv$ denota a *equivalência* entre a fórmula à sua esquerda e a fórmula à sua direita.
A partir de (3.15) e de (3.16) estamos em condições de determinar fórmulas simplificadas equivalentes à negação de fórmulas mais complexas que envolvem vários quantificadores. Por exemplo, para obtermos a negação da expressão

$$\forall x_1\ \exists x_2\ \exists x_3\ \forall x_4\ P(x_1, x_2, x_3, x_4),$$

podemos proceder do seguinte modo:

$$\begin{aligned}
\neg(\forall x_1 \exists x_2 \exists x_3 \forall x_4\ P(x_1, x_2, x_3, x_4)) &\equiv \exists x_1 \neg(\exists x_2 \exists x_3 \forall x_4\ P(x_1, x_2, x_3, x_4)) \\
&\equiv \exists x_1 \forall x_2 \neg(\exists x_3 \forall x_4\ P(x_1, x_2, x_3, x_4)) \\
&\equiv \exists x_1 \forall x_2 \forall x_3 \neg(\forall x_4\ P(x_1, x_2, x_3, x_4)) \\
&\equiv \exists x_1 \forall x_2 \forall x_3 \exists x_4\ \neg P(x_1, x_2, x_3, x_4).
\end{aligned}$$

[9] Note-se que $\forall x \in X\ P(x)$ significa, em linguagem simbólica mais precisa, $\forall x\ (x \in X \Rightarrow P(x))$.

Segue-se um teorema onde se estabelecem algumas propriedades das operações sobre famílias de conjuntos, cuja prova envolve a negação de expressões com quantificadores.

Teorema 3.3.5 *Seja A um subconjunto e $\{B_i\}_{i\in I}$ uma família de subconjuntos de um mesmo universo. Então verificam-se as seguintes igualdades:*

1. $A \setminus (\bigcap\limits_{i\in I} B_i) = \bigcup\limits_{i\in I} (A \setminus B_i)$.
2. $A \setminus (\bigcup\limits_{i\in I} B_i) = \bigcap\limits_{i\in I} (A \setminus B_i)$.
3. $\overline{\bigcap\limits_{i\in I} B_i} = \bigcup\limits_{i\in I} \overline{B_i}$.
4. $\overline{\bigcup\limits_{i\in I} B_i} = \bigcap\limits_{i\in I} \overline{B_i}$.

Demonstração: 1. $\begin{array}{lcl} x \in A \setminus (\bigcap_{i\in I} B_i) & \Leftrightarrow & (x \in A) \ \wedge \ (x \notin \cap_{i\in I} B_i) \\ & \Leftrightarrow & (x \in A) \ \wedge \ \neg(x \in \cap_{i\in I} B_i) \\ & \Leftrightarrow & (x \in A) \ \wedge \ \neg(\forall i \in I \ x \in B_i) \\ & \Leftrightarrow & (x \in A) \ \wedge \ (\exists i \in I \ x \notin B_i) \\ & \Leftrightarrow & \exists i \in I \ (x \in A \ \wedge \ x \notin B_i) \\ & \Leftrightarrow & \exists i \in I \ (x \in A \setminus B_i) \\ & \Leftrightarrow & x \in \bigcup_{i\in I} (A \setminus B_i). \end{array}$

2. $\begin{array}{lcl} x \in A \setminus (\bigcup_{i\in I} B_i) & \Leftrightarrow & (x \in A) \wedge (x \notin \cup_{i\in I} B_i) \\ & \Leftrightarrow & (x \in A) \wedge \neg(\exists i \in I \ x \in B_i) \\ & \Leftrightarrow & (x \in A) \wedge (\forall i \in I \ x \notin B_i) \\ & \Leftrightarrow & \forall i \in I \ (x \in A \wedge x \notin B_i) \\ & \Leftrightarrow & \forall i \in I \ (x \in A \setminus B_i) \\ & \Leftrightarrow & x \in \bigcap_{i\in I} (A \setminus B_i). \end{array}$

3. $\begin{array}{lcl} x \in \overline{\bigcap_{i\in I} B_i} & \Leftrightarrow & x \notin \cap_{i\in I} B_i \\ & \Leftrightarrow & \neg(x \in \cap_{i\in I} B_i) \\ & \Leftrightarrow & \neg(\forall i \in I \ x \in B_i) \\ & \Leftrightarrow & \exists i \in I \ x \notin B_i \\ & \Leftrightarrow & \exists i \in I \ x \in \overline{B_i} \\ & \Leftrightarrow & x \in \bigcup_{i\in I} \overline{B_i}. \end{array}$

4. $\begin{array}{lcl} x \in \overline{\bigcup_{i\in I} B_i} & \Leftrightarrow & x \notin \cup_{i\in I} B_i \\ & \Leftrightarrow & \neg(x \in \cup_{i\in I} B_i) \\ & \Leftrightarrow & \neg(\exists i \in I \ x \in B_i) \\ & \Leftrightarrow & \forall i \in I \ x \notin B_i \\ & \Leftrightarrow & \forall i \in I \ x \in \overline{B_i} \\ & \Leftrightarrow & x \in \bigcap_{i\in I} \overline{B_i}. \end{array}$ **qed**

Segue-se mais um teorema que envolve quantificadores.

Teorema 3.3.6 $\forall n \ ((n \in \mathbb{N} \setminus \{1\} \ \textit{é impar}) \Rightarrow \exists k \ (k \in \mathbb{N} \ \wedge \ n^2 = 8k + 1))$.

Demonstração: Qualquer número natural ímpar, $n > 1$, se pode escrever na forma $n = 2p + 1$, para algum $p \in \mathbb{N}$. Logo vem que

$$(2p+1)^2 \ = \ 4p\,(p+1) + 1. \tag{3.17}$$

E claro que $p\,(p+1)$ é um número par e, consequentemente, $p\,(p+1) = 2k$ para algum $k \in \mathbb{N}$. Substituindo, em (3.17), $p\,(p+1)$ por $2k$, obtém-se $n^2 = 8k + 1$. **qed**

3.4 Relações e Funções

As relações entre conjuntos desempenham um papel importantíssimo na linguagem matemática e na dedução de muitos resultados, pelo que, antes de mais, convém introduzir o respectivo conceito formal. Para tal vamos utilizar outros conceitos, como sejam o de par ordenado e o de produto cartesiano de conjuntos.

Definição 3.4.1 *Dado dois elementos de um dado universo, x e y, o par ordenado (x, y) define-se como sendo o conjunto $\{\{x\}, \{x, y\}\}$, ou seja, $(x, y) = \{\{x\}, \{x, y\}\}$. Adicionalmente diz-se que x é o primeiro elemento e y é o segundo elemento.*

Com base nesta definição, estamos em condições de introduzir o teorema que se segue.

Teorema 3.4.2 $(x, y) = (u, v) \Leftrightarrow (x = u \wedge y = v)$.

Demonstração:

($\Leftarrow$) Suponha-se $x = u$ e $y = v$, então $\{x\} = \{u\}$ e $\{x, y\} = \{u, v\}$ e, consequentemente, $\{\{x\}, \{x, y\}\} = \{\{u\}, \{u, v\}\}$, o que significa, de acordo com a definição 3.4.1, que $(x, y) = (u, v)$.

($\Rightarrow$) Suponha-se $(x, y) = (u, v)$, ou seja,

$$\{\{x\}, \{x, y\}\} = \{\{u\}, \{u, v\}\}. \tag{3.18}$$

- Suponha-se $x = y$.
  Então, da igualdade (3.18), obtém-se $\{\{x\}\} = \{\{u\}, \{u, v\}\}$. Como consequência $|\{\{x\}\}| = |\{\{u\}, \{u, v\}\}|$, pelo que $\{u\} = \{u, v\}$, ou seja, $u = v$. Logo, mais uma vez, tendo em conta (3.18), concluem-se as igualdades $x = y = u = v$.
- Suponha-se $x \neq y$.
  Então a igualdade (3.18) implica que se tenha $\{x\} \in \{\{u\}, \{u, v\}\}$ e $\{x, y\} \in \{\{u\}, \{u, v\}\}$.
  - Uma vez que $|\{x\}| < |\{u, v\}|$, então $\{x\} \neq \{u, v\}$ e, consequentemente, $\{x\} \in \{\{u\}, \{u, v\}\} \setminus \{\{u, v\}\} \Leftrightarrow \{x\} \in \{\{u\}\} \Leftrightarrow \{x\} = \{u\} \Leftrightarrow x = u$.
  - Uma vez que $|\{x, y\}| > |\{u\}|$, então $\{x, y\} \neq \{u\}$ e, consequentemente, $\{x, y\} \in \{\{u\}, \{u, v\}\} \setminus \{\{u\}\} \Leftrightarrow \{x, y\} \in \{\{u, v\}\} \Leftrightarrow \{x, y\} = \{u, v\}$. Por outro lado, uma vez que $x = u$ podemos concluir que $\{x, y\} \setminus \{x\} = \{u, v\} \setminus \{u\}$ o que significa $\{y\} = \{v\} \Leftrightarrow y = v$. **qed**

Os resultados que se obtêm como consequência imediata de um (ou vários) teorema(s) designam-se por *Corolários* do(s) teorema(s) a que está (estão) associado(s). Como exemplo segue-se um corolário do teorema 3.4.2.

Corolário 3.4.3 $(x, y) = (y, x) \Leftrightarrow x = y$.

A prova deste corolário é deixada como exercício.

A definição de pares ordenados pode estender-se, recursivamente, aos n-uplos ordenados, com $n \geq 3$, da seguinte forma

$$\begin{array}{ccccc}
(x_1, x_2, x_3) & = & (x_1, (x_2, x_3)) & & \\
(x_1, x_2, x_3, x_4) & = & (x_1, (x_2, x_3, x_4)) & = & (x_1, (x_2, (x_3, x_4))) \\
\vdots & & \vdots & & \\
(x_1, x_2, \ldots, x_n) & = & (x_1, (x_2, x_3, \ldots, x_n)) & = & (x_1, (x_2, (x_3, \ldots, x_n)))
\end{array}$$

ou, de um modo equivalente,

$$\begin{array}{ccc} \{\{x_1\},\{x_1,(x_2,x_3)\}\} & = & \{\{x_1\},\{x_1,\{\{x_2\},\{x_2,x_3\}\}\}\} \\ \{\{x_1\},\{x_1,(x_2,x_3,x_4)\} & = & \{\{x_1\},\{x_1,\{\{x_2\},\{x_2,(x_3,x_4)\}\}\}\} \\ \vdots & \vdots & \vdots \\ \{x_1,\{x_1,(x_2,\ldots,x_n)\}\} & = & \{\{x_1\},\{x_1,\{\{x_2\},\{x_2,(x_3,\ldots,x_n)\}\}\}\}. \end{array}$$

Definição 3.4.4 *Dados dois conjuntos arbitrários, A_1 e A_2, designa-se por produto cartesiano destes conjuntos e denota-se por $A_1 \times A_2$ (no caso de $A = A_1 = A_2$, o respectivo produto cartesiano denota-se simplesmente por A^2), o conjunto dos pares ordenados (x_1, x_2) tais que $x_1 \in A_1$ e $x_2 \in A_2$. Por sua vez, designa-se por relação binária entres os conjuntos A_1 e A_2 todo o subconjunto do produto cartesiano $A_1 \times A_2$.*

Por exemplo, de acordo com a definição 3.4.4, dados os conjuntos $A = \{1, 2, 3\}$ e $B = \{a, b, c, d, e, f\}$, o subconjunto $\mathcal{R} \subset A \times B$ tal que

$$\mathcal{R} = \{(1, a), (1, f), (2, b), (2, d), (2, f)\}$$

é uma relação binária entre os conjuntos A e B. Dado o conjunto universal $\mathcal{U}$, ainda podemos considerar o conjunto dos seus subconjuntos (ou seja, o conjunto das suas partes) o qual denotaremos por $\mathcal{P}(\mathcal{U})$ onde se inclui, naturalmente, o conjunto vazio. Com estes conceitos, pode encarar-se a relação de pertença dos elementos de um certo conjunto universal $\mathcal{U}$ em relação às suas partes, como uma relação binária entre $\mathcal{U}$ e $\mathcal{P}(\mathcal{U})$, ou seja, $\in \subset \mathcal{U} \times \mathcal{P}(\mathcal{U})$.

Exemplo 3.4.5 *Seja $\mathcal{U} = \{x, y\}$, donde vem que $\mathcal{P}(\mathcal{U}) = \{\varnothing, \{x\}, \{y\}, \{x, y\}\}$. Como consequência podemos concluir que*

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

Dada uma relação binária, $\mathcal{R}$, é muito comum escrever-se $x\mathcal{R}y$ em vez de $(x, y) \in \mathcal{R}$. Assim, em coerência com este modo de escrita, de acordo com o exemplo 3.4.5, para se afirmar que os pares $(x, \{x\})$, $(x, \{x, y\})$, $(y, \{y\})$ e $(y, \{x, y\})$ pertencem à relação binária $\in$ pode escrever-se $x \in \{x\}$, $x \in \{x, y\}$, $y \in \{y\}$ e $y \in \{x, y\}$.
Mais geralmente, dado um conjunto arbitrário $X \subseteq \mathcal{U}$, $\mathcal{P}(X) = \{Y : Y \subseteq X\}$. O conjunto das partes de X também se designa por conjunto potência (ou, simplesmente, potência) de X .

Sendo $\mathcal{R}$ uma relação, entre os conjuntos X e Y, designa-se por *domínio* de $\mathcal{R}$ e denota-se por *dom*$(\mathcal{R})$, o conjunto $\{x \in X : \exists y \in Y, (x, y) \in \mathcal{R}\}$ e por *contradomínio* (ou *imagem*) de $\mathcal{R}$ e denota-se por *codom*$(\mathcal{R})$, o conjunto $\{y \in Y : \exists x \in X, (x, y) \in \mathcal{R}\}$. Dado um elemento $x \in X$ designa-se por *imagem* de x por $\mathcal{R}$, e denota-se por $\mathcal{R}(x)$, o conjunto $\mathcal{R}(x) = \{y \in Y : (x, y) \in \mathcal{R}\}$ e por *imagem recíproca*, por $\mathcal{R}$, de um elemento $y \in Y$, e denota-se por $\mathcal{R}^{-1}(y)$ o conjunto $\mathcal{R}^{-1}(y) = \{x \in X : (x, y) \in \mathcal{R}\}$. Por sua vez, designa-se por relação inversa de $\mathcal{R}$ e denota-se por $\mathcal{R}^{-1}$ o subconjunto de $Y \times X$ definido por $\mathcal{R}^{-1} = \{(y, x) \in Y \times X : (x, y) \in \mathcal{R}\}$.

Definição 3.4.6 *Dado um conjunto A, uma relação binária, $\mathcal{R}$, definida nele (i.e, $\mathcal{R} \subseteq A \times A$) diz-se que é*

- *reflexiva, se* $\forall x \in A\ (x,x) \in \mathcal{R}$.
- *simétrica, se* $\forall x,y \in A\ (x,y) \in \mathcal{R} \Rightarrow (y,x) \in \mathcal{R}$.
- *anti-simétrica, se* $\forall x,y \in A\ (x,y) \in \mathcal{R} \wedge (y,x) \in \mathcal{R} \Rightarrow x = y$.
- *transitiva, se* $\forall x,y,z \in A\ (x,y) \in \mathcal{R} \wedge (y,z) \in \mathcal{R} \Rightarrow (x,z) \in \mathcal{R}$.

Definição 3.4.7 *Uma relação binária diz-se uma relação*

- *de equivalência se é reflexiva, simétrica e transitiva,*
- *de ordem parcial se é reflexiva, anti-simétrica e transitiva.*

Se $\mathcal{R}$ é uma relação de equivalência definida em X, então para cada $x \in X$, o conjunto $[x] = \{y \in X : (x,y) \in \mathcal{R}\}$ designa-se por *classe de equivalência* de x.

Teorema 3.4.8 *Seja* $\sim$ *uma relação de equivalência definida num conjunto* X *e* $x,y \in X$. *Se* $[x] \neq [y]$ *então* $[x] \cap [y] = \varnothing$.

Demonstração: Em vez de provarmos a implicação $[x] \neq [y] \Rightarrow [x] \cap [y] = \varnothing$, vamos provar a implicação equivalente $[x] \cap [y] \neq \varnothing \Rightarrow [x] = [y]$. Supondo $[x] \cap [y] \neq \varnothing$, $\exists z \in [x] \cap [y]$ tal que $x \sim z \ \wedge \ y \sim z$ ou ainda $x \sim z \ \wedge \ z \sim y$ (uma vez que, sendo $\sim$ uma relação simétrica, $y \sim z \Leftrightarrow z \sim y$. Consequentemente

$$\begin{array}{rcl} \alpha \in [x] & \Leftrightarrow & x \sim \alpha \text{ (pela definição de } [x]) \\ & \Leftrightarrow & \alpha \sim x \text{ (pela simetria de } \sim) \\ & \Leftrightarrow & \alpha \sim z \text{ (pela transitividade de } \sim \text{ e uma vez que } \alpha \sim x \sim z) \\ & \Leftrightarrow & \alpha \sim y \text{ (pela transitividade de } \sim \text{ e uma vez que } \alpha \sim z \sim y) \\ & \Leftrightarrow & \alpha \in [y] \text{ (pela definição de } [y].) \end{array}$$

qed

Uma relação de equivalência definida num conjunto X determina uma *partição* de X, i.e., uma subdivisão de X em subconjuntos dois a dois disjuntos (classes de equivalência) cuja união é X. O conjunto de tais classe designa-se por *conjunto quociente* e denota-se por $X/\mathcal{R}$.

São exemplos de relações de equivalência

- a relação de paralelismo entre rectas do plano,
- a relação *quando dividido por* 5 *tem o mesmo resto que* [10] definida no conjunto $\mathbb{Z}$.

Quando num conjunto X está definida uma relação de ordem parcial, $\mathcal{R}$, diz-se que X é um conjunto parcialmente ordenado, denotando-se por $(X,\mathcal{R})$.

[10] Este tipo relações *quando dividido por* p *tem o mesmo resto que*, com $p \in \mathbb{N}$, designam-se por relações de congruência módulo p e denotam-se por $\equiv \pmod p$. Assim, $x \equiv y \pmod p$ significa que $\exists k \in \mathbb{Z}$ tal que $x = p \times k + y$. No caso de $p = 5$, com facilidade se verifica que $\mathbb{Z}/\equiv \pmod p = \{[0],[1],[2],[3],[4]\}$, onde $\mathbb{Z}/\equiv \pmod p$ denota o conjunto quociente definido pela relação de equivalência $\equiv \pmod p$.

São exemplos de relações de ordem parcial

- a relação de menor ou igual que no conjunto dos números naturais determina o conjunto parcialmente ordenado $(\mathbb{N}, \leq)$,
- a relação de inclusão entre conjuntos que na família das partes de um conjunto A determina o conjunto parcialmente ordenado $(\mathcal{P}(A), \subseteq)$.

Definição 3.4.9 *Uma função definida num conjunto A e com imagem em B*

$$\begin{array}{rcl} f : A & \rightarrow & B \\ x & \rightsquigarrow & f(x), \end{array} \tag{3.19}$$

é uma relação $f \subseteq A \times B$ tal que se $(\alpha, \beta), (a, b) \in f \ \wedge \alpha = a$ então $\beta = b$. O conjunto A designa-se por conjunto de partida e o conjunto B por conjunto de chegada. Usualmente, escreve-se $f(\alpha) = \beta$ em vez de $(\alpha, \beta) \in f$.

Como as funções são casos particulares de relações, os conceitos de *domínio*, *imagem* (ou *contradomínio*), *imagem recíproca*, *inversa*, etc, de funções, são idênticos ao das relações.
Quando se denota uma função f como em (3.19), tal significa que $dom(f) \subseteq A$ e que $codom(f) \subseteq B$. As funções em que $dom(f) = A$ (i.e, em que o domínio coincide com o conjunto de partida A) também se designam por *aplicações*. Porém, na prática, é muito comum não fazer qualquer distinção entres os conceitos de função e de aplicação.

Alternativamente à definição 3.4.9, pode definir-se função da seguinte forma.

Definição 3.4.10 *Uma relação binária f é uma função se*
$\forall x \in dom(f) \ \exists! y \in codom(f)$ *tal que* $(x, y) \in f$.

Se $A = \varnothing$, então a única função entre A e B é o conjunto vazio. Porém, sendo f uma aplicação, se $A \neq \varnothing$ e $B = \varnothing$, de acordo com a definição 3.4.10, não existe qualquer aplicação entre A e B, nem mesmo a determinada pelo conjunto vazio.
Supondo $|A| = p$ e $|B| = q$, para a definição da aplicação f, existem q escolhas possíveis para cada um dos elementos de A, pelo que existem

$$\underbrace{q \times \ldots \times q}_{p \text{ vezes}} \ = \ q^p \tag{3.20}$$

aplicações possíveis entre A e B.
Uma vez que dado um conjunto arbitrário C, tal que $|C| = n$, a cardinalidade de $\mathcal{P}(C)$ é 2^n, tendo em conta que $|A \times B| = p \times q$, podemos concluir que

$$|\mathcal{P}(A \times B)| \ = \ 2^{p \times q}. \tag{3.21}$$

Assim, no caso de algum dos conjuntos A ou B ser vazio, existe uma única relação que designamos por relação vazia (obtendo-se $2^{pq} = 2^0 = 1$).
Com base nas igualdades (3.20) e (3.21) e tendo em conta que uma aplicação é também uma relação, podemos concluir que o número de aplicações entre A e B é

não superior ao número de relações entre os mesmos conjuntos e, consequentemente, que

$$\forall p, q \in \mathbb{N} \;\; q^p \leq 2^{pq}.$$

Desta forma concluímos uma desigualdade algébrica com raciocínios de natureza combinatória.

Uma função $f : A \to B$ diz-se *injectiva* se $\forall x, y \in dom(f)\ f(x) = f(y) \Rightarrow x = y$ e diz-se *sobrejectiva* se $\forall y \in B\ \exists x \in A$ tal que $f(x) = y$. Uma função que é injectiva e sobrejectiva diz-se *bijectiva*. Duas funções f e g são iguais (i.e, $f = g$) se têm o mesmo domínio D e $\forall x \in D\ f(x) = g(x)$.

Exemplo 3.4.11 *Dadas as funções*

$$\begin{array}{ll} f(x) = x^3 + x^2 - x - 1, & x \in \mathbb{Z} \\ g(x) = x^3 + x^2 - x - 1, & x \in \mathbb{R} \\ h(x) = (x^2 - 1)(x + 1) & x \in \mathbb{R} \end{array}$$

com facilidade se conclui que $f \neq g$ e $g = h$.

De agora em diante, vamos denotar por $\mathbb{N}_k$ o conjuntos dos primeiros k naturais, i.e, $\mathbb{N}_k = \{1, 2, \ldots, k\}$.

Definição 3.4.12 *Uma sequência finita de um conjunto A é uma função*

$$\begin{array}{rcl} f : \mathbb{N}_k & \to & A \\ n & \rightsquigarrow & f(n) = a_n, \end{array}$$

ou seja, $f(1) = a_1, f(1) = a_2, \ldots, f(k) = a_k$. Dizendo-se, neste caso, que se trata de uma sequência de comprimento k.

Sendo f uma sequência de comprimento n, usualmente denotamos-la pelo n-uplos ordenados de elementos de A, $(a_1, \ldots, a_n)$.

As sequências infinitas de elemento de um conjunto A, designam-se por sucessões de elementos de A. Logo, podemos definir uma sucessão de elementos de A como sendo uma função $f : \mathbb{N} \to A$. As sucessões $(a_1, a_2, \ldots)$ denotam-se habitualmente por

$$\{a_n\}_{n \in \mathbf{N}} \text{ ou } (a_n)_{n \in \mathbf{N}}.$$

Dada uma função $f : X \to Z$ e um subconjunto $Y \subseteq X$, designa-se por *restrição* de f a Y e denota-se por $f|_Y$ a função $f|_Y : Y \to Z$ tal que $\forall y \in Y\ f|_Y(y) = f(y)$. Neste caso, sendo $g = f|_Y$, também se diz que f é uma extensão de g.

Muitos problemas práticos resumem-se, matematicamente, à determinação de uma função que satisfaz certas restrições. Como exemplo, podemos considerar o clássico *problema do casamento*.

- Sendo $M = \{m_1, \ldots, m_n\}$ e $H = \{h_1, \ldots, h_n\}$ os conjuntos, respectivamente, de mulheres e homens por casar e supondo que cada mulher m_i determina um subconjunto $H_i \subseteq H$ de homens com os quais considera aceitável casar-se, o *problema do casamento* consiste em saber se, conhecidos todos os subconjuntos H_i para $i = 1, \ldots n$, é possível (ou não) casar todas as mulheres (e, consequentemente, todos os homens) com um homem (mulher) diferente, de entre os aceitáveis.
  O modelo matemático deste problema, em termos de conjuntos e funções, consiste em, dado o conjunto de índices $I = \{1, \ldots, n\}$ e a família de subconjuntos não vazios de H, $\{H_i\}_{i\in I}$, determinar uma função injectiva

$$\begin{array}{rcl} f : I & \to & \bigcup\limits_{i\in I} H_i \\ i & \rightsquigarrow & f(i) \in H_i. \end{array}$$

  A injectividade da função f assegura que a solução proposta não contempla a possibilidade de duas mulheres casarem com o mesmo homem e a condição $f(i) \in H_i$ assegura que cada mulher casa com um homem aceitável para ela.

O conjunto $\{f(1), \ldots, f(n)\}$, no modelo apresentado, designa-se, usualmente, por sistema de representantes distintos da família de conjuntos $\{H_i\}_{i\in I}$.
Existem algumas condições que, a verificarem-se, impedem a obtenção de uma solução para o problema. Por exemplo, se existem k conjuntos, $H_{j_1}, \ldots, H_{j_k}$ tais que

$$|H_{j_1} \cup \ldots \cup H_{j_k}| < k,$$

é claro que o problema não tem solução.
Em 1935 o matemático Philip Hall provou que se $\forall k \in \{1, \ldots, n\}$ a união de quaisquer k conjuntos da família $\{H_i\}_{i\in I}$ tem cardinalidade não inferior a k, então o *problema do casamento* tem solução.

Definição 3.4.13 *Dadas duas relações $\mathcal{R}_1$ entre A e B e $\mathcal{R}_2$ entre B e C, designa-se por composição de $\mathcal{R}_1$ com $\mathcal{R}_2$, a relação que se denota por $\mathcal{R}_2 \circ \mathcal{R}_1$ (e, usualmente, se lê $\mathcal{R}_2$ após $\mathcal{R}_1$) definida por*

$$\mathcal{R}_2 \circ \mathcal{R}_1 = \{(a, c) \in A \times C : \exists b \in B \ \ (a, b) \in \mathcal{R}_1 \ \wedge \ (b, c) \in \mathcal{R}_2\}.$$

No caso particular das funções, considerando-se $f : A \to B$ e $g : B \to C$, a composição $g \circ f$ corresponde à função

$$\begin{array}{rcl} g \circ f : A & \to & C \\ x & \rightsquigarrow & (g \circ f)(x) = g(f(x)). \end{array}$$

Por exemplo, sendo $g : \mathbb{Z} \to \mathbb{R}$ tal que $g(x) = 2x + 3$ e sendo $f : \mathbb{Z} \to \mathbb{Z}$ tal que $f(n) = n^2 - 3n + 1$. Então a função composta $g \circ f : \mathbb{Z} \to \mathbb{Z}$ vem dada por

$$(g \circ f)(n) = g(f(n)) = g(n^2 - 3n + 1) = 2(n^2 - 3n + 1) + 3 = 2n^2 - 6n + 5.$$

Se $dom(g) \cap codom(f) = \varnothing$, então a composição $g \circ f$ é a função vazia.
A composição de duas funções pode estender-se (de um modo natural) a três ou mais funções. Com efeito, dada a família de funções $f_i : A_i \to A_{i+1}$, para $i = 1, \ldots, p$, a função composta $f_p \circ f_{p-1} \ldots \circ f_1$ corresponde à função

$$\begin{array}{ccccccc} A_1 & \overset{f_1}{\to} & A_2 & \ldots & A_p & \overset{f_p}{\to} & A_{p+1} \\ x & \rightsquigarrow & f_1(x) & \ldots & f_{p-1}(\ldots(f_1(x))\ldots) & \rightsquigarrow & f_p(f_{p-1}(\ldots(f_1(x))\ldots) \end{array}$$

Exercícios

1. Dados os conjuntos A, B e C, prove as seguintes afirmações.
   (a) $(A \cup B) \times C = (A \times C) \cup (B \times C)$.
   (b) $(A \cap B) \times C = (A \times C) \cap (B \times C)$.
   (c) $(A \setminus B) \times C = (A \times C) \setminus (B \times C)$.
   (d) Se A e B são conjuntos não vazios então
   $$A \times B = B \times A \;\Leftrightarrow\; A = B$$
   (e) Se $A_1 \in \mathcal{P}(A)$ e $B_1 \in \mathcal{P}(B)$, então $A_1 \times B_1 \in \mathcal{P}(A \times B)$.
   (f) $\varnothing \times A = \varnothing$.
2. Seja T uma colecção de linhas telefónicas para encaminhamento de chamadas para os quartos de um hotel e seja Q o conjunto desses quartos. Assumindo que cada quarto tem exactamente um telefone responda às seguintes questões.
   (a) Mostre que o produto cartesiano $T \times Q$ corresponde ao conjunto de todas as possíveis ligações a partir dos quartos.
   (b) Supondo que $T = \{t_1, \ldots, t_{35}\}$ e $Q = \{q_1, \ldots, q_{35}\}$ e ainda que estão em progresso chamadas a partir de todos os quartos com número primo e só a partir destes, indique qual o subconjunto de $T \times Q$ que lhe corresponde.
3. Prove que $A \times B = \varnothing \;\Leftrightarrow\; (A = \varnothing \;\vee\; B = \varnothing)$.
4. A partir da definição, prove a implicação
   $$(x_1, x_2, x_3) = (y_1, y_2, y_3) \Rightarrow \forall i \in \{1, 2, 3\}\; x_i = y_i.$$
5. Sendo $\{A_i\}_{i \in I}$ uma família de conjuntos de um certo universo que também contém o conjunto S, prove a igualdade $(\bigcup_{i \in I} A_i) \times S = \bigcup_{i \in I}(A_i \times S)$.
6. Dados os subconjuntos A, B e C de um mesmo universo e tendo em conta que B^A denota o conjunto das aplicações com conjunto de partida A e conjunto de chegada B, responda às seguintes questões.
   (a) Explicite os elementos do conjunto $\{a, b\}^{\{1,2,3\}}$.
   (b) Prove que se $A \subseteq B$ então $A^C \subseteq B^C$.
   (c) Prove que se $B \neq C$ então $A^B \cap A^C = \varnothing$.

7. Considere as funções a seguir indicadas e diga quais as que são injectivas, sobrejectivas e bijectivas.

   (a) $f : \mathbb{N} \to \mathbb{N}$ tal que $f(n) = n^3$.

   (b) $g : \{a, b, c\} \to \{1, 2, 3\}$ tal que $g = \{(a, 2), (b, 1), (c, 3)\}$

   (c) $h : \mathbb{R}^+ \to \mathbb{R}$ tal que $h(x) = \log(x)$, onde $\mathbb{R}^+$ denota o conjunto dos números reais positivos.

8. Considerando os conjuntos A e B, tais que $|A| = 3$ e $|B| = 3$, responda às questões a seguir indicadas.

   (a) Quantas aplicações distintas se podem definir entre o conjunto de partida A e o conjunto de chegada B?

   (b) Quantas das funções referidas na alínea (a) são injectivas?

   (c) Quantas das funções referidas na alínea (a) são sobrejectivas?

9. Prove o teorema a seguir indicado.[11]

   Teorema 3.4.14 *Considere a função $f : A \to B$ e os subconjuntos de A, X e Y.*

   - *Então $f(X \cap Y) \subseteq f(X) \cap f(Y)$.*
   - *Adicionalmente, se f é injectiva, então $f(X \cap Y) = f(X) \cap f(Y)$.*

10. Dadas as funções
$$\begin{array}{rcl} f : \mathbb{R} & \to & \mathbb{R} \\ x & \rightsquigarrow & f(x) = \frac{1}{x^2+2}, \end{array} \quad \text{e} \quad \begin{array}{rcl} g : \mathbb{R} & \to & \mathbb{R} \\ y & \rightsquigarrow & g(y) = 2y - 1, \end{array}$$
determine as funções compostas $f \circ g$ e $g \circ f$.

[11] Dada uma função $f : A \to B$, $X \subseteq A$ e $Y \subseteq B$, usualmente, denota-se por $f(X)$ o conjunto $\{b \in B : \exists x \in X \ f(x) = b\}$ e por $f^{-1}(Y)$ o conjunto $\{a \in A : \exists y \in Y \ f(a) = y\}$.

Capítulo 4

Contextos e Estratégias de Demonstração

4.1 Teorias Matemáticas

Em matemática é de fundamental importância estabelecer o valor lógico de uma proposição. Por isso, os matemáticos são pessoas muito cépticas, raramente acreditam num resultado antes de obterem uma prova. Algumas proposições são evidentes e aceites como verdadeiras pela maioria dos matemáticos. Outras são menos evidentes e necessitam de uma demonstração. As proposições evidentes, ou as proposições que, no contexto matemático que está a ser tratado, aceitamos como verdadeiras, são chamadas *axiomas.* Tendo *regras de produção*, isto é, regras que permitam construir a partir de uma proposição verdadeira outras proposições verdadeiras, é possível determinar o valor lógico de outras proposições. Genericamente, designamos por *teoremas* todas as proposições verdadeiras que decorrem dos axiomas e da aplicação das regras de produção. O conjunto dos axiomas, regras de produção e teoremas constituem o que designamos por *teoria* ou *sistema matemático.*

Exemplo 4.1.1 *Considere-se um sistema matemático onde as proposições são palavras do alfabeto $\{A, b, c\}$, com um único axioma A e cujas regras de produção são as seguintes:*

- ($R1$) *Proposições obtidas a partir de uma proposição verdadeira, substituindo A por bAc, são proposições verdadeiras.*
- ($R2$) *Proposições obtidas a partir de uma proposição verdadeira, eliminando A, são proposições verdadeiras.*

Vamos mostrar que, no contexto deste sistema matemático, a proposição bbcc é um teorema.

Teorema 4.1.2 *bbcc.*

Demonstração: *De A por ($R1$) tem-se bAc. De bAc, ainda por ($R1$), tem-se $bbAcc$. Finalmente de $bbAcc$, da aplicação de ($R2$) decorre bbcc.* **qed**

Mais geralmente, é possível mostrar que qualquer proposição da forma

$$\underbrace{b...b}_{n} A \underbrace{c \ldots c}_{n} \qquad \textit{ou} \qquad \underbrace{b \ldots b}_{n} \underbrace{c \ldots c}_{n},$$

onde n é um inteiro positivo, é um teorema desta teoria.

A escolha dos axiomas de um determinado sistema matemático pode ser uma tarefa difícil. Em particular, o sistema de axiomas deve ser *consistente* , isto é, se t é um teorema então $\neg t$ não é um teorema.

Exemplo 4.1.3 *Considere-se o sistema matemático constituído pelos conjuntos* $A = \{1, 2\}$, $B = \{a, b, c\}$ *e uma aplicação* $f : A \to B$ *satisfazendo o axioma:*

$$\forall y \in B \quad \left|f^{-1}(y)\right| = 1.$$

Dentro desta teoria, temos o seguinte teorema.

Teorema 4.1.4 *A aplicação* f *é sobrejectiva.*

Este teorema é consequência directa da definição de aplicação sobrejectiva e do axioma. Por outro lado, ainda dentro desta teoria, temos também o teorema que a seguir se apresenta juntamente com a respectiva demonstração.

Teorema 4.1.5 f *não é sobrejectiva.*

Demonstração: $|codom(f)| = |\{f(1), f(2)\}| \leq 2 < 3 = |B|$. *Logo* $\exists y \in B$ *tal que* $y \notin codom(f)$. *Como consequência,* f *não é sobrejectiva.* **qed**

Também é conveniente que o sistema de axiomas seja *independente,* ou seja, que não haja axiomas que sejam consequência dos outros axiomas. Se um axioma é consequência dos outros axiomas, isto é, se um axioma pode ser obtido como teorema a partir dos outros axiomas, a teoria que se obtém do sistema de axiomas, com ou sem esse axioma, é a mesma. Sendo assim, esse axioma pode ser retirado.
Outra condição que o sistema de axiomas deve satisfazer é ser constituído por proposições evidentes que não estejam, por isso, em contradição com a intuição matemática. Os *Elementos* de Euclides (c. 300 a.C.) é o primeiro livro matemático com o objectivo de fundamentar uma área da matemática, neste caso a geometria, como teoria matemática. Os axiomas de Euclides para a geometria[1] foram aceites como intuitivamente evidentes pela maioria dos matemáticos da sua época e de épocas posteriores, com a excepção do seguinte axioma, conhecido por *axioma das paralelas.*

[1] Os axiomas que Euclides escolheu para a geometria dividem-se em postulados e noções comuns e são os seguintes:

Postulado 1. Dados dois pontos existe uma única recta que os contém.

Postulado 2. Todo o segmento de recta está contido numa única recta.

Postulado 3. Dado um ponto C e um número real $r > 0$, existe uma única circunferência de centro C e raio r.

Postulado 4. Todos os ângulos rectos são iguais.

Postulado 5. *Axioma das paralelas*: dada uma recta e um ponto não pertencente a essa recta, existe uma única recta que contém o ponto e é paralela à recta dada.

Noção comum 1. Duas quantidades iguais a uma terceira são iguais.

Noção comum 2. Se a quantidades iguais adicionarmos a mesma quantidade, as somas obtidas são iguais.

Noção comum 3. Se a quantidades iguais subtrairmos a mesma quantidade, as diferenças obtidas são iguais.

Noção comum 4. Objectos coincidentes são iguais.

Noção comum 5. O todo é maior do que a parte.

- Dada uma recta e um ponto não pertencente a essa recta, existe uma única recta que contém o ponto e é paralela à recta dada.

Nem todos os matemáticos da época de Euclides e das épocas seguintes aceitaram esta proposição como axioma da geometria. Alguns tentaram substitui-lo por outro que fosse mais evidente. Outros tentaram mostrar, sem sucesso, que este axioma era consequência dos outros nove axiomas da geometria de Euclides. Só 2100 anos após a publicação dos Elementos de Euclides é que os matemáticos tomaram consciência do facto que a geometria proposta por Euclides era uma das possíveis definições de geometria. Substituindo o axioma das paralelas por outro(s) axioma(s) definiram-se outras geometrias. As teorias decorrentes das novas definições foram catalogadas sob o nome de geometrias não-euclidianas.
Uma teoria diz-se *completa* se, para toda a proposição p, p ou $\neg p$ é um teorema. Caso contrário diz-se que a teoria é *incompleta*. Como já foi anteriormente referido, o teorema de incompletude de Gödel mostra que existem teorias incompletas. Numa teoria incompleta existem portanto proposições verdadeiras que não são teoremas.

4.2 Estratégias de Demonstração

Raramente, na prática, um teorema é dado com o sistema de axiomas e as regras de produção da teoria da qual faz parte. De um modo geral, os teoremas são deduzidos a partir dos axiomas utilizando certas regras de produção, como sejam, as *regras lógicas* ou *regras de inferência*, as quais têm como fundamento o sistema lógico adoptado.
Uma das regras de inferência mais utilizadas é a que se designa por *modus ponens* e a seguir se descreve.

- *Modus ponens* - se p e $p \Rightarrow q$ são proposições verdadeiras, então q é uma proposição verdadeira.[2]

Uma vez estabelecida uma proposição como teorema, também podemos utiliza-la para a demonstração de outros teoremas. Como exemplo, considere-se o teorema a seguir indicado.

Teorema 4.2.1 *Sejam x e y números reais. Se $x > 3$ e $y < 2$, então $x^2 - 2y > 5$.*

Supondo que as proposições

$$\text{se } x > 3 \text{ então } x^2 > 9, \tag{4.1}$$
$$\text{se } y < 2 \text{ então } -2y > -4, \tag{4.2}$$
$$\text{se } u > 9 \wedge v > -4 \text{ então } u + v > 5, \tag{4.3}$$

estão adquiridas como teoremas, podemos utiliza-las na demonstração do teorema 4.2.1.

Demonstração: [do teorema 4.2.1] Suponhamos que $x > 3$ e $y < 2$. Então, podemos utilizar os seguintes passos.

[2]Note-se que $(p \wedge (p \Rightarrow q)) \Rightarrow q$ é uma tautologia.

1. Dado que $x > 3$ e (4.1) são proposições verdadeiras, concluímos que $x^2 > 9$ é uma proposição verdadeira.
2. Por outro lado, tendo em conta que $y < 2$ e (4.2) são proposições verdadeiras, concluímos que $-2y > -4$ é também uma proposição verdadeira.
3. Das proposições verdadeiras $x^2 > 9 \wedge -2y > -4$ e (4.3) decorre, finalmente, a proposição verdadeira $x^2 - 2y > 5$. **qed**

Note-se que na demonstração, primeiramente consideramos as hipóteses do teorema, as quais supomos verdadeiras. Em 1. e 2. utilizamos modus ponens para justificar as desigualdades $x^2 > 9$ e $-2y > -4$. Em 3. a conclusão obtida decorre das proposições verdadeira obtidas em 1. e 2., da implicação (4.3) e da aplicação (novamente) de modus ponens. É claro que se as proposições (4.1), (4.2) e (4.3) não fossem teoremas, não as poderíamos utilizar na demonstração do teorema 4.2.1.

Como exemplo de um pretenso teorema que não o é (falso teorema) podemos considerar a seguinte proposição, a qual, para facilitar a exposição, vamos designar por teorema (?).

Teorema 4.2.2 (?) *Sejam x e y números reais e $x > 3$. Então $x^2 - 2y > 5$.*

Conforme já se referiu, existem no entanto certos hipotéticos resultados cuja prova ou refutação[3] se desconhece e que se designam, usualmente, por *conjecturas*. Para se provar que uma conjectura (ou um pretenso teorema, como é caso do teorema (?) 4.2.2) é falsa, basta encontrar um *contraexemplo*, isto é, basta mostrar que pode acontecer que a tese seja falsa embora as hipóteses sejam verdadeiras. No caso concreto do teorema 4.2.2, fazendo $x = 4$ e $y = 6$, é fácil verificar que embora a hipótese seja verdadeira ($4 = x > 3$), a tese é falsa (uma vez que $4^2 - 2 \times 6 = x^2 - 2y \not> 5$).

Uma estratégia de demonstração frequentemente utilizada é a *demonstração por contraposição*, baseada na equivalência entre as implicações $p \Rightarrow q$ e $\neg q \Rightarrow \neg p$.
Assim, sendo p a hipótese do teorema e q a tese, tendo em conta esta equivalência, a demonstração do teorema pode fazer-se, concluindo que sendo a tese, q, falsa, então a hipótese, p, é também falsa.

Teorema 4.2.3 *Se n é um número natural tal que $2^n - 1$ é primo, então n é primo.*

Demonstração: (Se $n = 1$ a hipótese é falsa, pelo que vamos considerar $n > 1$). Suponhamos que n não é primo. Então existem $a, b \in \mathbb{N}$ tais que $a < n$, $b < n$ e $n = ab$. Seja $x = 2^b - 1$ e $y = \sum_{k=0}^{a-1} 2^{kb} = 1 + 2^b + 2^{2b} + ... + 2^{(a-1)b}$. Então

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

[3] Refutar uma conjectura, consiste em provar que é falsa.

Sendo $b < n$, tem-se que $x = 2^b - 1 < 2^n - 1$. Sendo $ab = n > a$, tem-se que $b > 1$ e portanto $x = 2^b - 1 > 1$. Então $y < xy = 2^n - 1$. De $x < 2^n - 1$, $y < 2^n - 1$ e $xy = 2^n - 1$ concluímos que $2^n - 1$ não é primo. **qed**

Em vários teoremas a tese apresenta-se na forma

$$\text{Se } p \text{ então } q \quad (q \text{ se } p)$$

Para a demonstração de um tal teorema temos que supor que a hipótese h é verdadeira e mostrar que, em tais condições, a tese $p \Rightarrow q$ é também verdadeira. Uma vez que a proposição $p \Rightarrow q$ é sempre verdadeira quando p é falsa, basta mostrar que $p \Rightarrow q$ é verdadeira quando h e p são verdadeiras. Porém, supondo h e p verdadeiras, $p \Rightarrow q$ é verdadeira se e só se q é verdadeira. Como consequência, um teorema com hipótese h e tese $p \Rightarrow q$ é equivalente ao teorema com hipótese $h \wedge p$ e tese q. Assim, em ambos os casos, a demonstração pode fazer-se supondo h e p verdadeiras e provando que, em tais condições, q é verdadeira. Em alternativa, a prova deste mesmo teorema poderia ser feita mostrando que se h é verdadeira, então a proposição $\neg q \Rightarrow \neg p$ é também verdadeira, ou seja, se h e $\neg q$ são verdadeiras, então $\neg p$ é também verdadeira.
Seguem-se alguns exemplos de teoremas do tipo dos que acabamos de descrever.

- **Teorema 4.2.4** *Sejam a, b e c números inteiros. Se a é divisor de b e b é divisor de c, então a é divisor de c.*

- **Teorema 4.2.5** *Sejam x, y, z números reais e seja $x > y$. Se $xz \leq yz$, então $z \leq 0$.*

Para a demonstração do teorema 4.2.4 relembramos a seguinte definição *x é divisor de y se $\exists m \in \mathbb{Z}$ tal que $y = mx$.*

Demonstração: [Demonstração do teorema 4.2.4] Suponhamos que a, b e c são inteiros e sejam $m, n \in \mathbb{Z}$ tais que $b = ma$ e $c = nb$. Para provar que a é divisor de c, basta encontrar um $k \in \mathbb{Z}$ tal que $c = ka$. Como $c = nb$ e $b = ma$, temos que $c = nma$. Uma vez que $nm \in \mathbb{Z}$ concluímos assim que a é divisor de c. **qed**

Demonstração: [Demonstração do teorema 4.2.5] Sejam x, y, z números reais e seja $x > y$. Supondo $z > 0$ vem que $xz > yz$.[4] **qed**

Note-se que, nesta última demonstração, mantivemos inalterada a hipótese.
Como exercício verifique que o pretenso teorema a seguir indicado é falso.

Teorema 4.2.6 (?) *Sendo x, y, z números reais, se $z > 0$, então $xz > yz$.*

Outra estratégia de demonstração é a *demonstração por (redução ao) absurdo.* Sendo p a hipótese do teorema e q a tese, assumindo que p e $\neg q$ são verdadeiras, tentamos encontrar uma contradição c, por exemplo, que um certo teorema seja falso. Note-se que, sendo p verdadeira e c falsa, $p \wedge \neg q \Rightarrow c$ é verdadeira se e só se q é verdadeira. Embora este raciocínio justifique completamente, do ponto de vista lógico, a demonstração por absurdo, ainda há pouco tempo existiam matemáticos que a recusavam. Uma das mais famosas demonstrações por absurdo é a demonstração de Euclides da existência de un número infinito de números primos.

[4] Observe-se que $(x > y \wedge z > 0) \Rightarrow xz > yz$ é um axioma da definição do conjunto dos números reais.

Teorema 4.2.7 *Se P é o conjunto dos números primos, então P tem cardinalidade infinita.*

Demonstração: Suponhamos que existe um número finito de números primos os quais designamos por $p_1, p_2, \ldots, p_n$. Sendo $m = p_1 p_2 ... p_n + 1$, é claro que m é maior de qualquer primo e, por conseguinte, não é primo. Uma vez que $\forall i \in \{1, \ldots, n\}$ a divisão de m por p_i dá resto 1, nenhum dos números primos $p_1, \ldots, p_n$ é divisor de m. Porém, tal facto, contradiz um teorema da teoria dos números que afirma que todo o número inteiro superior a 1 é primo ou produto de números primos. **qed**

Exemplo 4.2.8 *Sendo A, B e C conjuntos tais que $A \setminus B \subseteq C$, mostre que $A \setminus C \subseteq B$.*

Tendo em conta que $A \setminus C \subseteq B$ significa $\forall x \ (x \in A \setminus C \Rightarrow x \in B)$ e utilizando a seguinte regra de inferência, chamada *generalização universal*:

se para um x arbitrário $P(x)$ é verdadeira, então $\forall x \ P(x)$ é verdadeira,

basta mostrar que de $A \setminus B \subseteq C$ (hipótese) decorre que $x \in A \setminus C \Rightarrow x \in B$ (tese). Como vimos, a demonstração deste teorema é a mesma da demonstração do teorema que tem como hipóteses $A \setminus B \subseteq C$ e $x \in A \setminus C$ e como tese $x \in B$. Querendo mostrar o teorema por absurdo, iremos assumir que $A \setminus B \subseteq C$, $x \in A \setminus C$ e $x \notin B$ e tentar encontrar uma contradição.

Demonstração: Seja $A \setminus B \subseteq C$ e $x \in A \setminus C$. Suponhamos que $x \notin B$. Então, $x \in A$ e $x \notin B$, ou seja, $x \in A \setminus B$. Uma vez que, por hipótese, $A \setminus B \subseteq C$, então $x \in C$ em contradição com $x \in A \setminus C$. Logo $x \in B$. Sendo x um elemento arbitrário de $A \setminus C$, concluímos que $A \setminus C \subseteq B$. **qed**

Exercícios

1. Encontre um contraexemplo para a seguinte conjectura: Seja n um numero natural não primo maior do que 2. Então $2n + 13$ não é um número primo.

2. Sejam A, B, C e D conjuntos tais que $A \setminus B \subseteq C \cap D$ e seja $x \in A$. Mostre que se $x \notin D$, então $x \in B$.

3. Sejam x, y números reais. Mostre que $\frac{x+y}{2} < y$, se $x < y$.

4. Seja x um número real diferente de zero. Mostre que se $\frac{\sqrt[3]{x}+5}{x^2+6} = \frac{1}{x}$, então $x \neq 8$.

5. Sejam a, b, c e d números reais tais que $0 < a \leq b$ e $d > 0$. Mostre que se $ac > bd$, então $c > d$.

6. Sejam x e y números reais tais que $3x + 2y \leq 5$. Mostre que se $x > 1$, então $y < 1$.

7. Considere o teorema a seguir indicado.

   Teorema 4.2.9 *Supondo $a \in \mathbb{R} \setminus \{4\}$, se $\frac{2a-5}{a-4} = 3$ então $a = 7$.*

   - Encontre o erro na seguinte demonstração: Seja $a = 7$. Então $\frac{2a-5}{a-4} = \frac{2\times 7-5}{7-4} = \frac{9}{3} = 3$. Portanto, $a = 7$ se $\frac{2a-5}{a-4} = 3$.
   - Dê uma demonstração correcta do teorema.

4.3 Outras Regras de Inferência

Além das regras de inferência que já vimos (modus ponens e generalização universal) existem outras regras de inferência frequentemente adoptadas. Como exemplo, vamos destacar as seguintes.

- Se $p \Rightarrow q$ e $q \Rightarrow r$ são verdadeiras, então $p \Rightarrow r$ é verdadeira. (*Silogismo*).
- Se $p \Rightarrow q$ e $\neg q$ são verdadeiras, então $\neg p$ é verdadeira. (*Modus tollens*).
- Se p é verdadeira, então $p \vee q$ é verdadeira. (*Adição*).
- Se $p \wedge q$ é verdadeira, então p é verdadeira. (*Especialização*).
- Se p e q são ambas verdadeiras, então $p \wedge q$ é verdadeira. (*Conjunção*).

É possível verificar todas estas regras pelas respectivas tabelas de verdade. Existem regras de inferência também muito adoptadas, que envolvem quantificadores, como sejam, as seguintes:

- Se $P(a)$ é verdadeira, então $\exists x\ P(x)$ é verdadeira.
- Se $\exists x\ P(x)$ é verdadeira, então $P(a)$ é verdadeira para um a particular.
- Se $\forall x\ P(x)$ é verdadeira, então $P(a)$ é verdadeira para um a arbitrário.

4.4 O Princípio de Indução

Em vários teoremas a tese apresenta-se da forma

$$\forall n\ \ P(n),$$

onde o universo ao qual o elemento n pertence é o conjunto dos números naturais, $\mathbb{N}$. Embora, como vimos anteriormente, para a demonstração de um tal teorema seja suficiente supor n arbitrário e mostrar que $P(n)$ se verifica, na prática, sem o princípio de indução, haveria grande dificuldade em demonstrar muitos destes teoremas. É intuitivamente óbvio que se $P(1)$ é verdadeiro e o predicado $P(n+1)$ [5] é verdadeiro, sempre que o predicado $P(n)$ é verdadeiro, então $\forall n\ P(n)$ é verdadeiro. Com efeito, nestas condições, uma vez que $P(1)$ é uma proposição verdadeira, também $P(2)$ é verdadeira e como $P(2)$ é verdadeira também $P(3)$ é verdadeira e assim sucessivamente. Temos assim a seguinte regra de inferência, chamada *princípio de indução* na seguinte versão:

$$(P(1) \wedge \forall n \in \mathbb{N}\ (P(n) \Rightarrow P(n+1))) \ \ \Rightarrow \ \ \forall n \in \mathbb{N}\ P(n)$$

Por exemplo, seja $P(n)$ o seguinte predicado: *Um conjunto com n elementos contem 2^n subconjuntos*. Pelo princípio de indução, para provar $\forall n \in \mathbb{N}\ P(n)$ temos que verificar o seguinte:

[5] Um predicado é uma aplicação que para uma dada lista de constantes se transforma numa proposição (ou seja, faz corresponder o valor verdadeiro ou falso). Por exemplo, supondo que o predicado $M(x, y)$ denota

x é múltiplo de y,

conclui-se que $M(8, 2)$ é uma proposição verdadeira e $M(3, 2)$ é uma proposição falsa.

1. $P(1)$.
   Suponhamos que A contém só um elemento, isto é, $A = \{x\}$. Então os subconjuntos de A são dois, $\varnothing$ e A. Uma vez que $2 = 2^1$ concluímos que $P(1)$ se verifica.

2. $\forall n \in \mathbb{N}\ (P(n) \Rightarrow P(n+1))$.
   Seja n um número natural arbitrário e suponha-se que $P(n)$ se verifica *(hipótese de indução)*. Seja A um conjunto com $n+1$ elementos e $x \in A$. Então $B = A \setminus \{x\}$ tem n elementos e portanto, por hipótese de indução, 2^n subconjuntos. Se C é um subconjunto de B, então C e $C \cup \{x\}$ são subconjuntos de A. Por outro lado, todo o subconjunto de A ou não contém x e é portanto um subconjunto C de B, ou contém x e é portanto da forma $C \cup \{x\}$, onde C é um subconjunto de B. Concluímos assim que o número de subconjuntos de A é duas vezes o número de subconjuntos de B, isto é, A tem $2 \times 2^n = 2^{n+1}$ subconjuntos. Desta forma acabamos de provar $P(n) \Rightarrow P(n+1)$, para n arbitrário, donde podemos concluir que $\forall n\ (P(n) \Rightarrow P(n+1))$.

Como $P(1)$ e $\forall n\ (P(n) \Rightarrow P(n+1))$ são, neste caso, verdadeiros, o princípio de indução garante que $\forall n\ P(n)$ é verdadeira. Acabamos assim de mostrar o seguinte teorema:

Teorema 4.4.1 *Para todo o conjunto A, se $|A| = n$ então $|\mathcal{P}(A)| = 2^n$.*

É claro que, em geral, numa demonstração por indução, a parte mais difícil, e portanto a parte onde é mais fácil cometer erros, é a segunda parte da demonstração, que consiste em provar que $\forall n\ (P(n) \Rightarrow P(n+1))$. No próximo exemplo ilustramos um tipo frequente de erro.

Exemplo 4.4.2 *Querendo provar que todas as pessoas têm o mesmo sexo, vamos dar uma demonstração (errada) por indução.*

Seja $P(n)$ a seguinte proposição: "Em todo o conjunto de n pessoas não há duas pessoas de sexo diferente." Evidentemente, não havendo duas pessoas num conjunto com 1 única pessoa, $P(1)$ é verdadeira.

Suponhamos agora que o predicado $P(n)$ é verdadeiro, onde n é um número natural arbitrário. Queremos provar que $P(n+1)$ é também verdadeiro. Seja então $A = \{a_1, a_2, ..., a_{n+1}\}$ um conjunto com $n+1$ pessoas. Então $B = A \setminus \{a_1\}$ e $C = A \setminus \{a_2\}$ são conjuntos com n pessoas. Por hipótese de indução todas as pessoas em B têm o mesmo sexo e todas as pessoas em C têm o mesmo sexo. Como a_3 pertence tanto a B como a C todas as pessoas de $B \cup C = A$ têm o mesmo sexo de a_3. Sendo A arbitrário, tem-se assim que $P(n) \Rightarrow P(n+1)$ e sendo n arbitrário concluímos $\forall n\ (P(n) \Rightarrow P(n+1))$.

Pelo princípio de indução (neste caso incorrectamente concluído) tem-se então que $\forall n\ P(n)$.

Aparentemente a demonstração poderia parecer correcta, mas, num certo ponto da demonstração assumimos a existência de um elemento $a_3 \in A$, ou seja, assumimos que $n + 1 = |A| \geq 3$. Na prática provamos $P(1)$ e $\forall n \geq 2\ P(n) \Rightarrow P(n+1)$. Falta, portanto, provar $P(1) \Rightarrow P(2)$. Uma vez que $P(1) \Rightarrow P(2)$ é falsa, como é fácil provar

com um contraexemplo, nem todas as pessoas têm o mesmo sexo.
Observe-se que não estamos a considerar 0 como sendo um número natural e que, portanto, o primeiro (mais pequeno) número natural é 1 . Em alguns casos será conveniente considerar 0 como sendo um número natural. Nestes casos o princípio de indução será: $(P(0) \wedge \forall n\ (P(n) \Rightarrow P(n+1))) \Rightarrow \forall n \geq 0\ P(n)$.

Exemplo 4.4.3 *Mostre que para todos os inteiros $n \geq 0$ o número $4^{2n+1} + 3^{n+2}$ é um múltiplo de* 13.

Demonstração:

1. Para $n = 0$ tem-se que $4^{2\times 0+1} + 3^{0+2} = 4 + 9 = 13$ que é evidentemente um múltiplo de 13.
2. Suponhamos que $4^{2n+1} + 3^{n+2}$ é um múltiplo de 13, isto é, $4^{2n+1} + 3^{n+2} = 13k$ para um $k \in \mathbb{N}$. Vamos mostrar que $4^{2(n+1)+1} + 3^{(n+1)+2}$ é também um múltiplo de 13.

$$\begin{aligned} 4^{2(n+1)+1} + 3^{(n+1)+2} &= 4^2 \times 4^{2n+1} + 3^{n+3} = 4^2 \times (4^{2n+1} + 3^{n+2} - 3^{n+2}) + 3^{n+3} \\ &= 4^2 \times (13k - 3^{n+2}) + 3^{n+3} = 4^2 \times 13k - 4^2 \times 3^{n+2} + 3 \times 3^{n+2} \\ &= 13 \times 4^2 \times k - (4^2 - 3) \times 3^{n+2} \\ &= 13 \times (16k - 3^{n+2}), \end{aligned}$$

que é um múltiplo de 13. **qed**

Mais geralmente, sendo n_0 um inteiro positivo ($n_0 \geq 0$), tem-se a seguinte versão do princípio de indução:

$$(P(n_0) \wedge \forall n \geq n_0\ (P(n) \Rightarrow P(n+1))) \Rightarrow \forall n \geq n_0\ P(n). \tag{4.4}$$

Outra versão do princípio de indução, que G. Peano [6] incluiu no sistema de axiomas da teoria dos números naturais é a seguinte:
Se $S \subseteq \mathbb{N}$ satisfaz as condições

(a) $1 \in S$,

(b) $n \in S \Rightarrow n + 1 \in S$,

então $S = \mathbb{N}$.
É fácil ver que se $S = \{n \geq n_0 : P(n)\}$, então este princípio é equivalente a (4.4).
Uma variante desta última versão, do princípio de indução, chamada *princípio de indução completa* é a seguinte:

[6] Giuseppe Peano (1858-1932), no livro *Arithmetices Principia Nova Methodo Exposita (1889)*, além do princípio de indução, introduz os seguintes axiomas:

- 1 é um número natural.
- 1 não é sucessor de nenhum número natural.
- Todo o número natural tem um sucessor.
- Se os sucessores de a e b são iguais, então a e b são iguais.

Se o conjunto S satisfaz as condições

(a) $1 \in S$,

(b) $\{k : k < n\} \subset S \Rightarrow n \in S$,

então $S = \mathbb{N}$.
Sendo $S = \{n : P(n)\}$, temos a seguinte regra de inferência

$$P(1) \wedge \forall n \ ((\forall k < n \ P(k)) \Rightarrow P(n)) \Rightarrow \forall n \ P(n).$$

Como exemplo, vamos mostrar que todo o número natural pode ser escrito como produto de um número ímpar por uma potência de 2, sendo estes números únicos, ou seja, vamos mostrar o seguinte teorema:

Teorema 4.4.4 *Se $n \in \mathbb{N}$, então existe um e um só par (a, b) de números inteiros não negativos tais que $n = 2^a(2b + 1)$.*

Demonstração: Uma vez que $1 = 2^0 \times 1$, o número 1 pode ser escrito na forma enunciada no teorema. Adicionalmente, $2^0 \times 1$ é a única maneira de escrever 1 como produto de um número ímpar por uma potência de 2. Com efeito, se $2^a(2b+1) = 1$, então $2^a = 1$ e $2b+1 = 1$.
Seja agora $n > 1$. Queremos provar que se todo o $k < n$ pode ser escrito, de forma única, como produto de um número natural ímpar por uma potência de 2, então também n pode ser escrito do mesmo modo.
Se n é ímpar, então $n = 2b + 1$ e, consequentemente, $n = 2^a(2b + 1)$, com $a = 0$. Por outro lado, como n não é divisível por 2, concluímos que a só pode ser 0 e que, por conseguinte, o par (a, b) é único.
Se n é par, então $n = 2m$. Sendo $m < n$, por hipótese de indução, $\exists!(a, b)$ tal que $m = 2^a(2b + 1)$. Então $n = 2m = 2^{a+1}(2b + 1)$. Se $n = 2^{c+1}(2d + 1)$, então $m = 2^c(2d + 1)$ de onde concluímos $(c, d) = (a, b)$. Consequentemente, n pode ser escrito de forma única como produto de um número ímpar por uma potência de 2. **qed**

Exercícios

1. Mostre que $\sum_{k=1}^{n} k = 1 + 2 + ... + n = \frac{n(n+1)}{2}$. Sendo $m \in \mathbb{N}$, a partir desta igualdade determine uma fórmula para $\sum_{k=m}^{m+n} k = m + (m + 1) + ... + (m + n)$.

2. Mostre que $n^2 \geq n$ para todo o **inteiro** n.

3. Mostre que para todo o $n \geq 0$ o número $n^4 - 4n^2$ é divisível por 3.

4. Mostre que $2^n > n^3$ para todo o $n \geq 10$.

5. Mostre que para todo o $n \geq 2$ se verifica que $\frac{1}{1\times2} + \frac{1}{2\times3} + ... + \frac{1}{(n-1)\times n} = 1 - \frac{1}{n}$.

6. Seja S um subconjunto de $\mathbb{N}$ tal que $3 \in S$ e tal que se $x \in S$, então $x + 3 \in S$. Mostre que S contem todos os múltiplos positivos de 3.

7. Mostre que se $x \in \mathbb{R}$ e $x \neq 1$, então
$\sum_{i=0}^{n-1} x^i = x^0 + x^1 + x^2 + ... + x^{n-1} = \frac{x^n-1}{x-1}$.

8. Mostre que se $q \geq 2$, então $\forall n \in \mathbb{N} \ n < q^n$.

4.5 Recursão

Dada uma função f de domínio $\mathbb{N}$, ou seja, uma sucessão, utilizando a mesma ideia do princípio de indução, basta indicar $f(1)$ e como se obtém $f(n+1)$ a partir de $f(n)$, para conseguir a imagem por f de um elemento qualquer de $\mathbb{N}$. Por exemplo, sendo f definida da seguinte forma:

$$\begin{array}{rcl} f(1) & = & 1 \\ \forall n \in \mathbb{N}\ f(n+1) & = & (n+1)f(n) \end{array}$$

tem-se que $f(1) = 1$, $f(2) = 2f(1) = 2$, $f(3) = 3f(2) = 3 \times 2 = 6$, $f(4) = 4f(3) = 4 \times 6 = 24, \ldots$. É agora fácil ver que $f(n)$ não é mais do que n factorial, que se denota por $n!$, isto é, $f(n) = n! = n(n-1)(n-2)\ldots 1$.
Definições deste tipo designam-se por *definições recursivas*. O exemplo dado corresponde à definição da função factorial. Outro exemplo de definição recursiva é o seguinte:

Dado $a \in \mathbb{R}$ definimos a^1 como sendo a e a^{n+1} como sendo $a \times a^n$, ou seja,

$$\begin{array}{rcl} a^1 & = & a \\ \forall n \in \mathbb{N} \quad a^{n+1} & = & a \times a^n \end{array}$$

Desta definição temos que $a^1 = a$, $a^2 = a \times a$, $a^3 = a \times a \times a$, etc.

Dada uma sucessão, $(a_n)_{n\in\mathbb{N}}$, de números reais é frequente considerar as seguintes sucessões $(s_n)_{n\in\mathbb{N}}$ e $(p_n)_{n\in\mathbb{N}}$ definidas, ambas, recursivamente do seguinte modo:

$$\begin{array}{ll} s_1 = a_1 & \\ \forall n \in \mathbb{N} \quad s_{n+1} = s_n + a_{n+1} & \end{array} \qquad \begin{array}{ll} p_1 = a_1 & \\ \forall n \in \mathbb{N} \quad p_{n+1} = p_n \times a_{n+1}. & \end{array}$$

Usualmente denota-se s_n por $\sum_{i=1}^{n} a_i$ e p_n por $\prod_{i=1}^{n} a_i$, sendo fácil ver que, da definição, decorre

$$\sum_{i=1}^{n} a_i = a_1 + a_2 + \ldots + a_n \quad \text{e} \quad \prod_{i=1}^{n} a_i = a_1 \times a_2 \times \ldots \times a_n.$$

Por exemplo se $\forall n \in \mathbb{N}\ a_n = n$ tem-se que $\sum_{i=1}^{n} a_i = \sum_{i=1}^{n} i = 1 + 2 + \ldots + n$ e $\prod_{i=1}^{n} a_i = \prod_{i=1}^{n} i = 1 \times 2 \times \ldots \times n = n!$.

Teorema 4.5.1 $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

Demonstração: Vamos mostrar o teorema por indução. Se $n = 1$, então $\sum_{i=1}^{1} i = 1$ e $\frac{n(n+1)}{2} = \frac{1\times 2}{2} = 1$. Portanto a tese é verdadeira para $n = 1$. Vamos agora supor que a tese é verdadeira para um n arbitrário (hipótese de indução) e mostrar que é verdadeira também

para $n+1$. Por definição $\sum_{i=1}^{n+1} i = (\sum_{i=i}^{n} i) + (n+1)$ e, uma vez que, por hipótese de indução, $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$ concluímos que

$$\sum_{i=1}^{n+1} i = \frac{n(n+1)}{2} + (n+1) = \frac{n(n+1)+2(n+1)}{2} = \frac{(n+1)(n+2)}{2}$$

como se pretendia. **qed**

A primeira demonstração deste teorema foi dada por Karl Friedrich Gauss (1777-1855) quando ainda era um aluno da escola secundária[7].

Uma das sucessões mais famosas definida recursivamente é a *sucessão de Fibonacci*[8]. A sua definição é a seguinte:

$$a_0 = 0, \quad a_1 = 1, \quad \forall n \geq 2 \quad a_n = a_{n-2} + a_{n-1}$$

Note-se que, sendo a_n soma dos dois termos da sucessão que o precedem, é necessário indicar os dois primeiros valores da sucessão.
Os primeiros termos da sucessão de Fibonacci, são os seguintes:

$$\begin{aligned} a_0 &= 0, \\ a_1 &= 1, \\ a_2 &= a_0 + a_1 = 1, \\ a_3 &= a_1 + a_2 = 2, \\ a_4 &= a_2 + a_3 = 3, \\ a_5 &= a_3 + a_4 = 5, \\ a_6 &= a_4 + a_5 = 8, \\ &\ldots \end{aligned}$$

A sucessão de Fibonacci, além da caracterização recursiva anteriormente referida, pode definir-se pela seguinte fórmula:

$$a_n = \frac{(\frac{1+\sqrt{5}}{2})^n - (\frac{1-\sqrt{5}}{2})^n}{\sqrt{5}}\,. \tag{4.5}$$

Embora à primeira vista nada o indique, note-se que a expressão $\frac{(\frac{1+\sqrt{5}}{2})^n - (\frac{1-\sqrt{5}}{2})^n}{\sqrt{5}}$ determina, $\forall n \in \mathbb{N}$, um número natural.

[7] Conta-se que, sendo Gauss um aluno irrequieto, o seu professor de matemática, para o calar, mandou-o somar os primeiros cem números naturais. O professor ficou surpreendido com a rapidez da resposta e, mais ainda, com o facto de ela ser correcta. Gauss explicou o resultado obtido com a tabela:

$$\begin{array}{ccccccccc} 1 & + & 2 & + & 3 & + & \ldots & + & 100 \\ 100 & + & 99 & + & 98 & + & \ldots & + & 1 \end{array}$$

onde a soma de cada coluna é igual a 101 e a soma das 100 colunas corresponde ao dobro do somatório pretendido.

[8] Leonardo Pisano (acerca de 1170-1250), chamado também Fibonacci, foi um matemático italiano. Parece que Fibonacci descobriu a sucessão que tem o seu nome estudando um conjunto de coelhos e a sua reprodução.

A demonstração da igualdade (4.5) é deixada como exercício, com a sugestão de utilização do princípio de indução completa.

Exercícios

1. Para $n \geq k \geq 0$ define-se $\binom{n}{k}$ como sendo $\frac{n!}{k!(n-k)!}$, onde $0! = 1$ por definição.

   (a) Mostre que $\forall n \geq k > 0 \quad \binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$.

   (b) Mostre que $\forall x, y \in \mathbb{R}\ \forall n \in \mathbb{N}$

   $$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

2. Sejam $(a_n)_{n\in\mathbb{N}}$, $(b_n)_{n\in\mathbb{N}}$ sucessões de números reais e $c \in \mathbb{R}$. Mostre que $\forall n \in \mathbb{N}$

   $$\sum_{i=1}^{n}(a_i + b_i) = \sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i \qquad \text{e que} \qquad \sum_{i=1}^{n}(ca_i) = c\sum_{i=1}^{n} a_i$$

3. Seja $(a_n)_{n\in\mathbb{N}}$ definida recursivamente por

   $$\begin{aligned} a_1 &= 0 \\ \forall n \in \mathbb{N} \quad a_{n+1} &= 2a_n + n \end{aligned}$$

   Mostre que $\forall n \in \mathbb{N} \quad a_n = 2^n - n - 1$.

4. Seja $(a_n)_{n\in\mathbb{N}}$ definida recursivamente por

   $$\begin{aligned} a_1 &= 2 \\ \forall n \in \mathbb{N} \quad a_{n+1} &= (a_n)^2 \end{aligned}$$

   Encontre uma fórmula para a_n e demonstre-a.

Bibliografia

[Eves, 1997] Eves, H. *Introdução à História da Matemática*, Editora da Universidade Estadual de Campinas - UNICAMP, Campinas, (1997).

[Dieudonné, 1990] Dieudonné, J. *A Formação da Matemática Contemporãnea*, Publicações Dom Quixote, Lisboa, (1990).

[Gerstein, 2001] Gerstein, L. J. *Introduction to Mathematical Structures and Proofs*, Springer, NY, (2001).

[SDUA, cota/localização: 510A.74]

[Kisačanin, 1998] Kisačanin, B. *Mathematical Problems and Proofs: Combinatorics, Number Theory and Geometry*, Plenum Press, NY, (1998).

[SDUA, cota/localização: 511A.64]

[Velleman, 1998] Velleman, D. J. *How to Prove It: a structured approach*, Cambridge University Press, Cambridge, (1998).

[SDUA, cota/localização: 510A.178]

[Wiitala, 1987] Wiitala, A. S. *Discrete Mathematics - a unified approach*, McGraw-Hill, NY, (1987).

[SDUA, cota/localização: 519.1A.94]