Objectivo: Com alguma frequência nos preocupamos com a resolução de problemas. No entanto, alguns dos problemas mais interessantes da Matemática não têm solução.

Propomo-nos falar sobre alguns destes problemas e de alguns conceitos matemáticos que se desenvolveram à volta deles.

Pretendemos mostrar que a dificuldade da matemática reside nela mesma, e que as respostas que consegue dar tanto a fenómenos físicos como sociais, são justificação mais do que suficiente para o seu estudo aprofundado.

Com esta experiência convidamos-te a dar o primeiro passo em direcção ao interior do edificio matemático, apresentando-te os números inteiros, racionais, irracionais, algébricos e transcendentes.

1. Considerações sobre a Matemática

Vamos começar por apresentar alguns problemas fundamentais da Matemática. Nesta categoria encontram-se três problemas geométricos e também três resultados revolucionários do século XX. Relativamente aos primeiros, temos:

Duplicação do cubo: Dado um cubo, construir usando somente régua e compasso, um cubo de volume igual ao dobro do volume do cubo dado.

Trissecção de um ângulo: Dividir, usando somente régua e compasso, um ângulo em três partes iguais.

Quadratura do círculo: Construir, usando somente régua e compasso, um quadrado de área igual à de um círculo de raio um.

Estes problemas de formulação simples estiveram na base da evolução da matemática em geral, no entanto a matemática que nasceu para dar respostas a estes problemas superou largamente os objectivos.

Até ao século XIX não se demonstrou a impossibilidade destas construções, continuando os matemáticos a tentar demonstrar a possibilidade de efectuar tais construções.

Para a resolução destes problemas desenvolveram-se a teoria das equações algébricas ou diofantinas. Mostrou-se que os números que se podem construir com régua e compasso são os que se definem por operações de raízes quadradas.

Na resolução destes problemas contribuíu o desenvolvimento das teorias das curvas analíticas, das equações cúbicas e quárticas, e a teoria de Galois e dos números transcendentes.

Estes problemas implicitamente contêm processos infinitos, que tentaremos explicar no decorrer destas experiências, e que ilustram a complexidade da ciência matemática. De facto, as respostas que hoje conseguimos dar a um nível elementar, destas questões, acompanhou toda a evolução do homem e da própria matemática.

Estes factos devem estar presentes quando tentamos apresentar uma teoria matemática, pois na sua essencia contém algum dos problemas fundamentais da matemática. Note-se que um problema descontextuado é o principio fundamental para que não mereça que se sofra por ele, e como a matemática não é fácil, os matemáticos passamos a ter um problema adicional. Relativamente a problemas do século XX temos:

Teorema da incompletude de Gödel: Em qualquer sistema matemático axiomático, haverá sempre proposições que não são demonstráveis nem refutáveis.

Principio da incerteza de Heisenberg: Afirma a impossibilidade de determinar exactamente a posição e momento de uma particula num instante qualquer e que o produto das incertezas é superior a uma constante dada.

Teorema sobre as funções de escolha social de Kenneth Arrow: Não existe uma forma infalível de obter as preferências individuais, e garantir o cumprimento de certas condições mínimas razoaveis, i.e. é impossivel criar um sistema de votação que não apresente defeitos graves em algum momento.

Como exemplo de aplicação do teorema de Gödel temos o quinto axioma da geometria euclideana, conhecido como o axioma das paralelas, e que estabelece: *por um ponto exterior a uma recta dada, passa uma e uma só recta paralela à recta dada.* Durante seculos se tentou, em vão, demonstrar este axioma a partir dos restantes quatro. Tal é impossível, sendo as suas negações consistentes com os demais axiomas, dando origem a várias geometrias não-euclideanas.

Como negar o axioma das paralelas?

Como consequências directas deste axioma temos, por exemplo, que a soma dos ângulos internos de um triângulo é 180°, ou que a distância mais curta entre dois pontos pertencentes a um mesmo plano é o comprimento do segmento de recta que os une. Numa geometria não-euclideana estes dois resultados são falsos.

Na verdade, basta situarmo-nos em alto mar e procurar a distância mais curta entre dois pontos para nos darmos conta da necessidade de definir outra geometria que dê resposta a esta questão.

Como consequência do teorema de Heisenberg, temos que perdem sentido os modelos determinísticos para a natureza. Entrámos também na era das vitórias psicológicos.

Relativamente ao último teorema, vemos com frequência, depois de uma votação, vários candidatos reclamar vitórias parciais, ainda que somente um tenha sido eleito. Isto acontece por todos os candidatos, definirem à partida objectivos que não vão ser avaliados na votação.

Estes teoremas levam-nos a concluir que a tolerância é, um valor a incluir na ciência matemática, um estímulo à criatividade e uma ponte para a compreensão da universilidade da ciência matemática.

2. Conjuntos

Nesta secção não vamos abordar ferramentas para resolver problemas difíceis quaisquer, mas tão só introduzir linguagem matemática que porventura parcialmente conhecem, útil em qualquer dóminio da matemática: vamos dar breves resumos da teoria ingénua dos conjuntos, da linguagem das relações, aplicações e funções, e dos números. Se esta parte vos parecer 'seca', o seu poder mostrar-se-á em breve de modo que pedimos um pouco de paciência.

Pode defender-se que o conceito de *conjunto* é o fundamental em toda a matemática, isto porque com ele definem-se directa ou indirectamente quase todos os outros objectos nela estudados. Para Georg Cantor (1845-1918), o criador da teoria dos conjuntos um conjunto é uma colecção de objectos bem distintos da nossa reflexão ou intuição, concebida como um todo. Estes objectos são os elementos do conjunto. Embora se tenha mostrado que esta definição é demasiado ampla para evitar contradições (ver notas no fim), é seguramente uma boa descrição daquilo que se tem em mente ao falar dum conjunto. Contradições artificialmente construidas à parte é mais importante, para avançar em matemática, sentir como se relacionam os objectos e quais as suas propriedades, do que o que propriamente dito *são*; recorre-se às definições de preferência só aquando se examina de forma crítica o que se expôs. Exceptuando especialistas, o matemático usa no seu dia a dia a teoria ingenua dos conjuntos para as tarefas, no entanto importantes, de conferir precisão e concisão às suas ideias. Desta teoria vamos expôr a seguir os rudimentos.

Se um objecto a é elemento de um conjunto A, escreve-se $a \in A$, no caso oposto $a \notin A$. É conveniente introduzir o simbolo $\emptyset$ para o conjunto vazio. É definido pela propriedade $a \notin \emptyset$ para todos os objectos a. Se um conjunto não for demasiado grande, os seus elementos são frequentemente listados assim: $A = \{a, b, c, \ldots\}$. Dois conjuntos A, B são identicos (ou iguais), i.e. $A = B$ se para cada objecto x se tem $x \in A$ se, e somente se, $x \in B$. Desta definição de identidade de conjuntos decorre que dois conjuntos indicados por listas são iguais se diferem apenas na ordem em que os elementos aparecem na lista. Também decorre que repetições não alteram um conjunto. Por exemplo $\{a, 1, 2\} = \{2, a, 1\} = \{a, a, a, 2, 1, 1\}$.

Sejam A, B dois conjuntos. Diz-se que A é *subconjunto* ou A está *contido* em B, ou B é *superconjunto* de A, se todo o elemento de A é elemento de B; escreve se isto $A \subseteq B$ ou equivalente $B \supseteq A$. Se adicionalmente se souber que $A \neq B$ escreve-se por vezes $A \subset B$, e diz-se que A é subconjunto *próprio* de B, ou B superconjunto próprio de A. A família de todos os subconjuntos de um conjunto Ω diz-se o *conjunto das partes* de Ω; e escreve-se 2^Ω, ou $\mathcal{P}(\Omega)$. A primeira notação em breve nos vai parecer natural. Assim, dizer $A \in 2^\Omega$, é o mesmo que dizer $A \subseteq \Omega$.

Abrevia-se a frase "o conjunto dos x para os quais ...", pela notação $\{x : ...\}$. Dados conjuntos A, B define-se a *união* dos conjuntos A, B, escrito $A \cup B$, como sendo o conjunto dos elementos x que são elementos de A ou elementos de B; ou seja: $A \cup B = \{x : x \in$

A ou $x \in B\}$. Um **ou** simples não é utilizado no sentido exclusivo. De forma semelhante definem-se *intersecção* de A, B por $A \cap B = \{x : x \in A \text{ e } x \in B\}$; e *diferença* de A, B por $A \setminus B = \{x : x \in A \text{ mas } x \notin B\}$ respectivamente. A *diferença simétrica* é definida por $A \triangle B = (A \cup B) \setminus (A \cap B)$: é o conjunto dos elementos que estão ou em A ou em B (o **ou**... **ou** é exclusivo).

Dados conjuntos A e B não vazios podemos seleccionar $a \in A$ e $b \in B$ para formar o par (a, b). Pares (a, b) e (a', b') são iguais se, e somente se, $a = a'$, e $b = b'$. Ilustremos que tudo pode ser definido pela noção de conjunto: com efeito pode definir-se $(a, b) := \{a, \{a, b\}\}$. Este último conjunto tem exactamente as propriedades que queremos de pares. O conjunto dos pares (a, b) com $a \in A, b \in B$ que assim podemos formar é dito *produto cartesiano* de A por B: $A \times B := \{(a, b) : a \in A, b \in B\}$.

É frequente que se trabalha com subconjuntos A de um certo *universo* Ω; o universo pode ser por exemplo o conjunto dos números naturais, ou o conjunto dos reais, ou (em aplicações da matemática) o conjunto de todas as pessoas, etc. Se o universo for claro do contexto, então define-se $A^c = \Omega \setminus A$ como sendo o *complementar* de A em Ω. Em certos contextos também pode ser conveniente criar-se um universo, simplesmente unindo os conjuntos que se apresentam.

Problema 2.1. *A seguir sejam A, B, C conjuntos num universo Ω. Então temos as seguintes regras de cálculo:*
i. Leis da comutatividade: $A \cup B = B \cup A \quad e \quad A \cap B = B \cap A\,.$ *ii. Leis da associatividade:* $(A \cup B) \cup C = A \cup (B \cup C) \quad e \quad (A \cap B) \cap C = A \cap (B \cap C)\,.$ *iii. Leis da distributividade:*

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \quad e \quad A \cup (B \cap C) = (A \cup B) \cap (A \cup C)\,.$$

iv. Leis de De Morgan: $A^c \cup B^c = (A \cap B)^c \quad e \quad A^c \cap B^c = (A \cup B)^c\,.$
v. $(A^c)^c = A$; $A \subseteq B$ *se, e somente se,* $A^c \supseteq B^c$; $A \cup A^c = \Omega$; $A \cap A^c = \emptyset$.
vi. $A \times (B \cup C) = (A \times B) \cup (A \times C)$.
vii. $(A \times B) \cap (A' \times B') = (A \cap A') \times (B \cap B')$.

Prova. Vamos provar, em pormenor, a primeira regra da distributividade, (regra iii_1) para darmos uma ideia como demonstrar tais identidades; o leitor tente provar as restantes.

Seja $x \in A \cap (B \cup C)$. Então $x \in B \cup C$, logo $x \in B$ ou $x \in C$ (definição da união). Por hipótese temos também $x \in A$. Assim, se $x \in B$, então $x \in A \cap B$; se $x \in C$, então $x \in A \cap C$. Em ambos os casos $x \in (A \cap B) \cup (A \cap C)$. Como x foi arbitrário (em $A \cap (B \cup C)$ mostrámos que $\text{esq}(\text{iii}_1) \subseteq \text{dir}(\text{iii}_1)$. (Isto é: o lado esquerdo de iii_1 é subconjunto do lado direito de iii_1.) Seja agora $x \in \text{dir}(\text{iii}_1)$, i.e. $x \in (A \cap B) \cup (A \cap C)$. Então $x \in A \cap B$ ou $x \in A \cap C$. Se $x \in A \cap B$ então $x \in A$; como também $x \in B$, decorre $x \in B \cup C$, e portanto $x \in A \cap (B \cup C)$. De forma análoga obtém-se de $x \in A \cap C$ que $x \in A \cap (B \cup C)$. Como x foi arbitrário, mostrámos $\text{esq}(\text{iii}_1) \supseteq \text{dir}(\text{iii}_1)$. Assim temos em suma iii_1, pela própria definição da identidade de conjuntos. □

Os simbolos $\cup, \cap, \setminus, \triangle, \times$, exprimem operadores, são *operacionais*, na medida em que nos exortam formar a partir de conjuntos dados, novos conjuntos (operacionais são também, por exemplo, os simbolos $+, \cdot$ na teoria dos números naturais); os símbolos $\subseteq, \subset$, etc., ao contrário, são *relacionais*: relacionam dois conjuntos (símbolos relacionais são também, por exemplo, os símbolos $\leq, |$ na teoria dos números naturais).

As simbologias para união e intersecção encontram-se também de forma generalizadas: se I for um conjunto-index e a cada $i \in I$ associado um conjunto A_i, então escreve-se $\bigcup_{i \in I} A_i$ para designar o conjunto de todos os x que estão em pelo menos um dos conjuntos A_i; ou seja $\bigcup_{i \in I} A_i = \{x : \text{ existe um } i \in I \text{ tal que } x \in A_i\}$; de forma analoga define-se $\bigcap_{i \in I} A_i = \{x : \text{ para todos os } i \in I x \in A_i\}$. Se o conjunto-index for $I = \{1, 2, \ldots, n\}$, utilizam-se as alternativas $\bigcup_{i=1}^n A_i$ e $\bigcap_{i=1}^n A_i$ para designar estas união e intersecção. Definem-se também produtos cartesianos com mais que dois factores: se $A_1, \ldots, A_n$ forem conjuntos então $A_1 \times A_2 \times ... \times A_k = \{(a_1, a_2, \ldots, a_k) : a_1 \in A_1, a_2 \in A_2, \ldots, a_k \in A_k\}$.

Observação . O problema 2.1 podem ser de forma natural generalizadas a uniões/intersecções/complementos/produtos cartesianos envolvendo mais que dois conjuntos. Por exemplo

$$A \cap (B_1 \cup B_2 \cup B_3) = (A \cap B_1) \cup (A \cap B_1) \cup (A \cap B_1);$$

etc.

Dois conjuntos A, B dizem-se *disjuntos* se não tiverem elementos em comum, i.é. se $A \cap B = \emptyset$. Uma família de conjuntos $A_1, \ldots, A_k$ define uma *partição* de um conjunto Ω, se os A_i forem mutuamente disjuntos e a sua união for Ω, i.e., se

$$A_i \cap A_j = \emptyset \text{ para } i \neq j \qquad \text{e} \qquad A_1 \cup A_2 \cup \ldots \cup A_k = \Omega\,.$$

Utiliza-se frequentemente a simbologia $A_1 \uplus A_2 \uplus \ldots \uplus A_k = \Omega$ para indicar que $A_1, \ldots, A_k$ formam uma partição de Ω.

Mais sobre conceitos ligados intimamente à teoria dos conjuntos, sobretudo o conceito da cardinalidade diremos nas secções ...

3. Correspondências, Relações, Aplicações e Funções

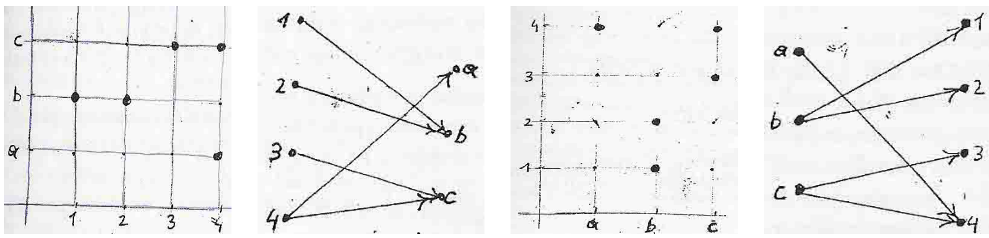
Fixemos os conjuntos X, Y . Uma *correspondência* de X para Y é um terno (X, G, Y) onde G é subconjunto qualquer de $X \times Y$: $G \subseteq X \times Y$. G diz-se *grafo da correspondência.* Define-se $G^{-1} = \{(y, x) : (x, y) \in G\}$. Então (Y, G^{-1}, X) diz-se *correspondência inversa.*

Exemplo (a). Sejam $X = \{1, 2, 3, 4\}, Y = \{a, b, c\}$. Então

$$G = \{(1, b), (2, b), (3, c), (4, a), (4, c)\}$$

é grafo duma correspondência de X para Y.

Como X, Y são conjuntos pequenos podemos visualizar esta correspondência. Duas maneiras mostraram-se particularmente ùteis. Na figura 1.(a), a imagem suscitada a quem conhece sistemas cartesianos: os elementos do grafo G são indicados por pontos gordos; é habito identificar os elementos de X em $X \times Y$ (as primeiras coordenadas) com os elementos dum eixo horizontal, e os elementos de Y ('segundas coordenadas') com o eixo vertical. Na figura 1.(b), o mesmo grafo é indicado por arestas. Uma imagem como esta última diz-se frequentemente um *grafo bipartito* orientado (por causa das setas). É hábito identificar os elementos de X com nós à esquerda, os elementos de Y com nós à direita. Os grafos inversos são mostrados nas figuras 1.(c) e 1.(d). Correspondências surgem de

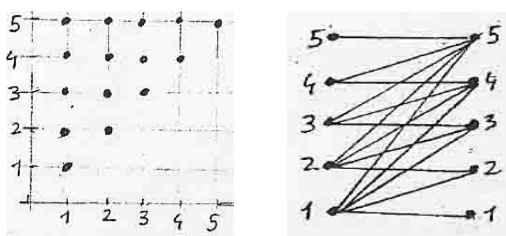


(a) (b) (c) (d)

Figura 1. Representação de Grafos

forma natural em aplicações da matemática ao estudo de situações sociais: veja-se por exemplo o teorema do casamento (p.). Dentro da matemática, são as relações binárias e as aplicações que que dão origem a correspondências.

Exemplo (b). Uma relação bem conhecida a todos é a relação '$\leq$'. À esquerda sua imagem cartesiana; à direita a mesma relação como grafo bipartito, para o caso $X = Y = \{1, 2, 3, 4, 5\}$. Marcámos um ponto (x, y) como sendo gordo ou traçámos uma aresta (x, y)



(a) (b)

Figura 2. Grafos de Representações

se, e somente se, $x \leq y$.

O que nós chamámos (de acordo com pelo menos uma enciclopédia "standard" da matemática) grafo duma correspondência, é em muitas obras chamado uma relação binária, termo que a enciclopédia reserva para grafos G decidíveis: isto é se existir um método para decidir para qualquer par $(x, y) \in X \times Y$ se sim ou não $(x, y) \in G$. Não vamos ser aqui demasiado rigorosos, e utilizar as palavras **correspondência**, **grafo**, e **relação** de formas permutáveis, escolhendo a palavra segundo o que melhor parece reflectir o actual uso. Escreve-se para relações R em vez de $(x, y) \in R$ também xRy (generalizando notações tais como $x \leq y, x = y, x \equiv y$ (a última notação é utilizada para congruências na teoria dos números).

Correspondências podem ser em certas circunstâncias, compostas. Se (X, G, Y) e (Y, H, Z) forem correspondências, então define-se uma nova correspondência

$$(X, H \circ G, Z) := \{(x, z) : \exists y \in Y xGy \text{ e } yHz\}.$$

Dado um conjunto X, a *diagonal* de X é denotada e definida por $\Delta_X = \{(x, x) : x \in X\}$.

As seguintes definições se tem mostrado particularmente úteis no trabalho com relações.

Definição 3.1. Seja R uma relação num conjunto X.
· R diz-se *reflexiva* se $\Delta_X \subseteq R$. (i.e. se para todos os $x \in X$, xRx.)
· R diz-se *simétrica* se $R = R^{-1}$.
· R diz-se *antisimétrica* se xRx' e $x'Rx$ implicar que xRx;
· R diz-se *transitiva* se xRx' e $x'Rx''$ implica xRx''
· R diz-se *relação de ordem* se for reflexiva, antisimétrica, e transitiva.
· R diz-se *relação de equivalência* se for reflexiva, simétrica e transitiva.

Exemplo . Seja $X = \{0, 1, 2, 3, 4\}$. Então:
· $R = \{(0, 0), (1, 1), (1, 2), (2, 2), (3, 3)\}$ é uma relação reflexiva.
· $R = \{(0, 2), (1, 2), (2, 0), (2, 1), (3, 3)\}$ é uma relação simétrica.
· $R = \{(0, 0), (0, 3), (1, 1), (2, 2)\}$ é relação antisimétrica.
· $R = \{(0, 0), (0, 1), (1, 0), (0, 2), (1, 1), (1, 2), (2, 0), (2, 1), (0, 3)\}$ é transitiva.
· $R = \{(0, 0), (1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 4), (3, 3), (3, 4), (4, 4)\}$ é relação de ordem.
· $R = \{(0, 0), (0, 3), (1, 4), (2, 2), (3, 0), (3, 3), (4, 1), (4, 4)\}$ é relação de equivalência.

Uma correspondência (X, f, Y) diz se uma *aplicação* ou *função* de X para Y, se para cada x o conjunto $f(x) = \{y : (x, y) \in f\}$ for singular: Se $(x, y) \in f$ e $(x, y') \in f$, então $y = y'$. Escreve-se (em abuso linguístico/notacional) $f(x) = y$ (em vez de f(x)={y}). O conjunto X diz-se *domínio* da aplicação, e Y diz-se *conjunto da chegada*. O conjunto $f(X) := \{f(x) : x \in X\}$ diz-se *conjunto imagem* de f. Para $Y' \subseteq Y$ define-se a *imagem inversa* de Y' por $f^{-1}(Y') = \{x \in X : f(x) \in X\}$.

Exercício 3.1. Seja $f : X \to Y$ uma aplicação, sejam $X_1, X_2 \subseteq X$ e $Y_1, Y_2 \subseteq Y$. Então têm-se as seguintes afirmações:
· $f(X_1 \cap X_2) \subseteq f(X_1) \cap f(X_2)$ e $f(X_1 \cup X_2) = f(X_1) \cup f(X_2)$.
· $f^{-1}(Y_1 \cap Y_2) = f^{-1}(Y_1) \cap f^{-1}(Y_2)$ e $f^{-1}(Y_1 \cup Y_2) = f^{-1}(Y_1) \cup f^{-1}(Y_2)$.
· $f^{-1}(X \setminus X_1) = Y \setminus f^{-1}(X_1)$.

Importantes são ainda as seguintes definições:

Uma função $f : X \to Y$ diz-se *injectiva* se $f(x) = f(x')$ implica $x = x'$; f diz-se *sobrejectiva* se para cada y existir um x tal que $f(x) = y$; finalmente f diz-se *bijectiva* se for injectiva e sobrejectiva. Uma *permutação* é uma função bijectiva $f : X \to X$. Seja $f : X \to Y$ e $y \in Y$. Diremos que y *é alvo de* f *aplicado a* x (ou ... f *para* x) se $y = f(x)$.

Podemos agora definir mais alguns conceitos ligados à teoria dos conjuntos: lembrem-se que ainda não sabemos nada de números. Um conjunto Ω é *finito*, se não existir $\Omega' \subset \Omega$ e aplicação bijectiva $f : \Omega' \to \Omega$. Também não podemos dizer de forma directa quando é que um conjunto tem apenas um elemento. Um conjunto S diz-se *singular* se não pode ser escrito como união $S = A \cup B$ com A, B disjuntos e não-vazios. Embora ainda não possamos dizer quantos elementos um conjunto tem, ou seja, qual a sua cardinal, podemos dizer se ou não dois conjuntos tem a mesma cardinal: conjuntos A e B *têm a mesma cardinal* se existir uma aplicação bijectiva $f : A \to B$.

4. Números

O conceito que o leigo associa primeiro com a matemática é o conceito do número. Este conceito sofreu ao longo da história humana repetidas extensões: uma das primeiras actividades matemáticas terá sido a contagem; actividade esta que leva ao conceito do número natural; depois introduziram-se provavelmente por razões mercantis os números negativos; já os gregos chamaram a duas distâncias comensuráveis, se existir um distância tal que as primeiras duas são múltiplos inteiros da terçeira. Podemos dizer que falaram de números racionais. Diz a lenda que ficaram chocados quando descobriram que diagonal e lado dum quadrado não estão em relação comensurável; em linguagem moderna isto equivale a que $\sqrt{2}$ é irracional. A teoria dos números irracionais isto é a passagem rigorosa dos racionais para os reais é uma conquista do século XIX. Nos últimos anos do século XVIII passou-se ainda dos números reais para os complexos (o real na altura identificava-se com a recta ou com os números decimais, sem-se ter tido ainda uma noção rigorosa do cálculo com eles)

Na secção presente, não vamos dar um desenvolvimento completo da teoria destes vários tipos dos números, mas tão-só um esboço que em anos futúros poderão pormenorizar: mais importante é que tenham uma percepção de como as coisas se enfiam.

5. Os Números Naturais

Um conjunto totalmente ordenado tal que cada subconjunto tem um elemento mínimo diz-se um conjunto *bem ordenado*. Um conjunto bem ordenado tal que cada elemento do mesmo é tambem subconjunto do mesmo, diz-se um número *ordinal*. É hábito denotar números ordinais por letras gregas: $\alpha, \beta, \ldots$.

De acordo com que todos os conceitos matemáticos podem ser defininidos através do conceito conjunto, esqueçam-se por um momento que pensam já conhecer os números naturais. Considerem a seguinte sequência de definições: $0 = \emptyset$, $1 = \{0\}$, $2 = \{0, 1\}$, $3 = \{0, 1, 2\}$, ... etc. Temos que $0 \in 1$ (segundo definição de 1); e é também verdade que $0 \subseteq 1$, pois $\emptyset$, o conjunto vazio, é subconjunto de qualquer conjunto. Da mesma forma temos $0 \in 2$ e também $0 \subseteq 2$ etc. Temos $1 \in 2$. E temos também $1 \subseteq 2$, pois $\{0\} \subseteq \{0, 1\}$. etc. Segundo a nossa construção vemos também que dado qualquer subconjunto de $\{0, 1, 2, ...\}$

existe um único elemento que é elemento de todos os outros: Consideremos por exemplo $\{2, 3, 4, 5\}$. Então $2 \in 3, 2 \in 4, 2 \in 5$. Vemos que, se escrevermos $m < n$ para dizer $m \in n$, então o nosso conjunto $\{0, 1, 2, \ldots\}$ é bem ordenado. O sucessor dum número ordinal α, denotado α' é o conjunto de todos ordinais menores ou igual a α: $\alpha' = \{\zeta : \zeta \leq \alpha\}$. Por exemplo o sucessor de 2 é 3: 2'=3; e 3 é exactamente a familia dos ordinais$\leq$ 2. Define se a adição de ordinais indutivamente assim $\alpha + 0 = \alpha$; $\alpha + \beta' = (\alpha + \beta)'$. Vejamos exemplos $2 + 0 = 2$. $2 + 1 = 2 + 0' = (2 + 0)' = 2' = 3$; $1 + 1 = 1 + 0' = (1 + 0)' = 2$. $1 + 2 = 1 + 1' = (1 + 1)' = 2' = 3$. Também definem-se produtos de números ordinais tal que como caso especial se obtém as habituais regras de cálculo para números naturais.

Saltando pormenores, podemos afirmar que esta teoria dá o que noutras abordagens menos conjuntistas é conhecido por teoria dos naturais segundo Giuseppe Peano. Continuando a notação x' para o sucessor de um número x, Peano exigiu para os naturais, que se denotam $\mathbb{N}$, cinco postulados: i. $1 \in \mathbb{N}$; ii. Se $x \in \mathbb{N}$, então $x' \in \mathbb{N}$; iii. Se $x \in \mathbb{N}$, então $x' \neq 1$. iv. $x' = y'$, então $x = y$. v. Se um conjunto satisfaz as duas condições a) $1 \in M$ e b) $x \in M$ implica $x' \in M$, então $\mathbb{N} \subseteq M$.

Nós podemos agora definir a cardinal de um conjunto finito: seja n um número natural, e M um conjunto finito. Então pode provar-se que existe um único número natural m (entendido como ordinal, e portanto como conjunto no sentido acima exposto) tal que existe uma bijecção entre M e m. Neste caso m diz-se o numero cardinal de M, e escreve-se $|M| = m$, lido à cardinal de M é m.'

6. Princípio de Indução

O Princípio da Indução é um eficiente instrumento para a demonstração de factos referentes aos números naturais. Por isso deve adquirir-se prática em sua utilização. Por outro lado, é importante também conhecer o significado e sua posição dentro da Matemática. Entender o Princípio da Indução é praticamente o mesmo que entender os números naturais.

Apresentamos a seguir uma breve exposição sobre os números naturais, onde o Princípio da Indução se insere adequadamente e mostra sua força teórica.

Deve-se a Giussepe Peano (1858-1932) a constatação de que se pode elaborar toda a teoria dos números naturais a partir de quatro factos básicos, conhecidos atualmente como os *axiomas de Peano*, i.e. o conjunto $\mathbb{N}$ dos números naturais possui quatro propriedades fundamentais, das quais resultam, como conseqüências lógicas, todas as afirmações verdadeiras que se podem fazer sobre esses números:

- **(A):** Existe uma função $s : \mathbb{N} \to \mathbb{N}$, que associa a cada $n \in \mathbb{N}$ um elemento $s(n) \in \mathbb{N}$, chamado o sucessor de n.
- **(B):** A função s é injetiva.
- **(C):** Existe um único elemento, 1, no conjunto $\mathbb{N}$, tal que $1 \in s(n)$ para todo $n \in \mathbb{N}$.

(D): Se um conjunto $X \subset \mathbb{N}$ é tal que $1 \in \mathbb{N}$ e $s(X) \subset X$ (isto é, $n \in X \Rightarrow s(n) \in X$), então $X = \mathbb{N}$.

Um dos axiomas de Peano, o último, possui claramente uma natureza mais elaborada do que os demais. Ele é conhecido como o *axioma de indução*.

O significado informal do axioma (D) é que todo número natural pode ser obtido a partir de 1 por meio de repetidas aplicações da operação de tomar o sucessor.

O papel fundamental do axioma da indução na teoria dos números naturais e, mais geralmente, em toda a Matemática, resulta do facto de que ele pode ser visto como um método de demonstração, chamado o *Método de Indução Matemática*, ou *Princípio da Indução Finita*, ou *Princípio da Indução*, conforme explicaremos agora.

Teorema (Princípio da Indução). *Seja P uma propriedade referente a números naturais. Se 1 goza de P e se, além disso, o fato de o número natural n gozar de P implica que seu sucessor $s(n)$ também goza, então todos os números naturais gozam da propriedade P.*

Nas demonstrações por indução, a condição de que a propriedade P é válida para o número natural n (da qual deve decorrer que P vale também para $s(n)$) chama-se *hipótese de indução*.

O Princípio da Indução não é utilizado somente como método de demonstração. Ele serve também para definir funções $f : \mathbb{N} \to Y$ que têm como dominio o conjunto $\mathbb{N}$ dos números naturais. Para se definir uma função $f : \mathbb{N} \to Y$ exige-se em geral que seja dada uma regra bem determinada, a qual mostre como se deve associar a cada elemento $x \in X$ um único elemento $y = f(x) \in Y$.

Entretanto, no caso particular em que o domínio da função é o conjunto $\mathbb{N}$ dos números naturais, a fim de definir uma função $f : \mathbb{N} \to Y$ não é necessário dizer, de uma só vez, qual é a relação que dá o valor $f(n)$ para todo $n \in \mathbb{N}$. Basta que se tenha conhecimento dos seguintes dados:

(1) O valor $f(1)$;
(2) Uma regra que permita calcular $f(s(n))$ quando se conhece $f(n)$.

Esses dois dados permitem que se conheça $f(n)$ para todo número natural n.
(Diz-se então que a função f foi definida por recorrência.) Com efeito, se chamarmos de X o conjunto dos números naturais, n, para os quais se pode determinar $f(n)$, o dado (1) acima diz que $1 \in X$ e o dado (2) assegura que $n \in X \Rightarrow s(n) \in X$. Logo, pelo axioma da indução, tem-se $X = \mathbb{N}$.

Aplicaremos agora o Princípio da Indução para demonstrar um facto geométrico. Sabe-se que, traçando diagonais internas que não se cortam, pode-se decompor qualquer polígono em triângulos justapostos. Isto é evidente quando o polígono é convexo: basta fixar um vértice e traçar as diagonais a partir dele. Se o polígono não é convexo, a prova requer mais cuidados.

Problema 6.1. *Qualquer que seja a maneira de decompor um polígono P, de n lados, em triângulos justapostos por meio de diagonais internas que não se intersectam, o número de diagonais utilizadas é sempre $n-3$.*

Proof. Com efeito, dado n, suponhamos que a proposição acima é verdadeira para todo polígono com menos de n lados. Seja então dada uma decomposição do polígono P, de n lados, em triângulos justapostos, mediante diagonais internas. Fixemos uma dessas diagonais. Ela decompõe P como reunião de dois polígonos justapostos P_1, de n_1 lados, e P_2, de n_2 lados (cf. figura 3), onde $n_1 < n$ e $n_2 < n$, logo a proposição vale para os polígonos P_1 e P_2. Evidentemente, $n_1 + n_2 = n + 2$. As d diagonais que efetuam a

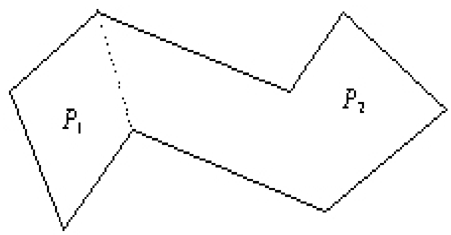


Figura 3. Polígono não Convexo

decomposição de P agrupam-se da seguinte forma: $n_1 - 3$ delas decompõem P_1, $n_2 - 3$ decompõem P_2 e uma foi usada para separar P_1 de P_2. Portanto $d = n_1 - 3 + n_2 - 3 + 1 = n_1 + n_2 - 5$. Como $n_1 + n_2 = n + 2$, resulta que $d = n - 3$. □

Exercício 6.1. Descobrir o erro em paradoxos que resultam do uso inadequado do método de indução.

(1) Todo número natural é pequeno.
(2) Toda função $f : X \to Y$, cujo domínio é um conjunto finito X, é constante.

7. Alguns processos infinitos

Imaginemos que chegamos a um Hotel onde previamente fizemos uma reserva. O recepcionista diz-nos que não sabe nada da reserva e que o Hotel está completo.

Podemos responder-lhe que o problema não é o Hotel estar completo mas sim o ter um número finito de quartos?

A resposta é válida pois a aplicação $f : \mathbb{N} \to \mathbb{N}$ definida por $f(n) = n+1$ é sobrejectiva.

Vê-se da mesma forma que o cardinal do conjunto dos números inteiros coincide com o cardinal do conjunto dos números pares, ímpares, múltiplos de 7 ou até com o do conjunto dos números primos.

Alguns destes resultados mais ou menos estranhos são devidos a George Cantor. A ele devemos também que a teoria dos conjuntos seja a linguagem comum da Matemática abstracta.

O conjunto dos números naturais tem cardinalidade numerável.

Analisemos a existência de conjuntos com cardinalidade superior à do numerável.

Cantor demonstrou que o conjunto dos números racionais, $\mathbb{Q}$, é numerável. De facto, os elementos deste conjunto são da forma a/b, com $a, b \in \mathbb{Z}$ e $b \neq 0$, e construimos a aplicação bijectiva de $\mathbb{Q}$ em $\mathbb{Z}$ por

$$1/1 \mapsto 1\,, \quad 1/2\,, 2/1 \mapsto 2\,, 3\,, \quad 1/3\,, 3/1 \mapsto 4\,, 5\,, \quad \ldots$$

e como os conjuntos $\mathbb{Z}$ e $\mathbb{N}$ têm a mesma cardinalidade, temos o que queríamos demonstrar.

Indique a expressão analítica da aplicação anterior.

Cantor demonstrou também que entre o conjunto dos números reais, $\mathbb{R}$ e $\mathbb{Q}$ não existe uma correspondência biunivoca. A sua hipótese do contínuo diz que não existe um subconjunto dos números reais com cardinalidade superior à de $\mathbb{N}$ e inferior à de $\mathbb{R}$.

Mais tarde Paul Cohen mostrou que este axioma é independente dos axiomas da teoria dos conjuntos, pelo que a hipótese do contínuo ou a sua negação são consistentes, com alguma teoria dos conjuntos.

Voltando ao nosso hotel infinito. Suponhamos que a infinidade numerável de quartos tem uma infinidade numerável de janelas.

Justifique que a cardinalidade do conunto das janelas é numerável.

Suponhamos agora que o conjunto das janelas está numerado, e que às 23h59m as dez primeiras janelas se estragam, ao mesmo tempo de reparamos a primeira. Nos trinta segundos seguintes estragam-se as janelas 11 à 20, enquanto reparamos a segunda janela. Nos quinze segundos seguintes, estragam-se as janelas 21 à 30 e a terceira janela é reparada. Continuando este fenómeno a acontecer até às doze badaladas, i.e. 24h.

Quantas janelas se estargaram e foram reparadas até às 24h?

8. Números algébricos e transcendentes

Devemos convir que se a um número lhe dessem a possibilidade de escolher não gostaria de ser irracional. No entanto, a cardinalidade do conjunto dos números irracionais é, como já vimos, superior à de $\mathbb{Q}$ e coincide com a de $\mathbb{R}$. Vamos introduzir um novo subconjunto de números reais.

Definição 8.1. Um *número real* ξ diz-se *algébrico* se existirem $c_j \in \mathbb{Z}$ tais que ξ é raiz do polinómio $f(x) = c_0x^n + c_1x^{n-1} + \cdots + c_n$. Caso contrário diz-se *transcendente*.

O conjunto dos números algébricos é numerável? Do raciocínio empregue para mostrar que o conjunto das janelas do nosso Hotel é numerável, concluíu que o conjunto dos números algébricos é numerável.

O conjunto dos números transcendentes tem a potência do contínuo?

De facto, consideremos o número algébrico, ξ, que é uma raíz da equação

$$f(x) = c_0x^n + c_1x^{n-1} + \cdots + c_n = 0\,, \quad c_j \in \mathbb{Z}\,, \quad j = 0, 1, \ldots, n\,,$$

que não tem raízes múltiplas nem racionais. Então dado $x = p/q$ com $p, q \in \mathbb{Z}$ com $q > 0$, temos

$$|f(p/q)| = \frac{|c_0 p^n + c_1 p^{n-1} q + \cdots + c_n q^n|}{q^n} \geq \frac{1}{q^n}\,.$$

Se p/q é uma das aproximações racionais de ξ a menos de $1/q$ temos a partir do teorema do valor médio de Lagrange que

$$|f(p/q)| = |f(\xi) - f(p/q)| = |\xi - p/q|\,|f'(\eta)|\,, \quad \eta \in]p/q\,,\,\xi[\,.$$

Assim, para q suficientemente grande $|f'(\eta)| < 2f'(\xi)$, e portanto $|\xi - p/q| > 1/(2|f'(\xi)|q^n)$, e para $q > 2||f'(\xi)||$ temos $\xi - p/q > 1/q^{n+1}$.

Estes argumentos levam-nos à existência de números reais que não são algébricos, i.e. são trancendentes.

Definição 8.2. Seja ξ um *número real* tal que para uma infinidade de números naturais m, existe uma infinidade de $q \in \mathbb{Z}$ tais que $|\xi - p/q| < 1/q^m$, é dito *de Liouville.*

Como exemplo de número de Liouville temos os números da forma

$$\sum_{n=1}^{\infty} \frac{c_n}{b^{n!}}\,, \text{ com } \ 0 \leq c_n < b\,, \text{ e } \ \sum_{n=1}^{\infty} c_n = +\infty\,.$$

onde $b > 1$ e a sucessão $(c_n) \subset \mathbb{Z}^+$ é não constante apartir de uma determinada ordem.

Note que o conjunto ds números de Liouville tem cardinalidade superior à do numerável, e como é um subconjunto de $\mathbb{R}$ tem a potência do contínuo.

Apresente uma bijecção entre o conjunto dos números de Liouville e $[1, +\infty[$.

Como exemplos de números transcendentes temos o π e o e. Como definir-los? O que representam?

Definição π: É o cociente entre o perímetro de uma circunferência e o seu diâmetro, i.e. o limite do cociente dos perímetros dos polígonos regulares de n lados inscritos numa circunferência de raio r, pelo diâmetro da circunferência. Construímos estes polígonos como mostra a figura 4. O lado deste polígonos, a_n, vem dado em termos do número

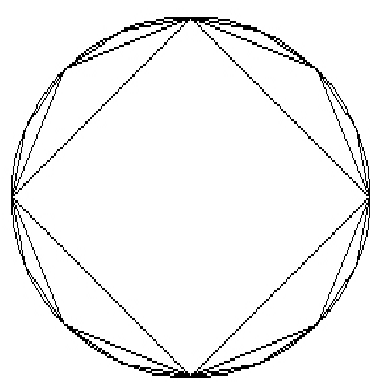


FIGURA 4. Polígonos que convergem para a circunferência

de lados n, por $a_n = 2r\sin(180°/n)$, $n \in \mathbb{N}$ (verificar!). Assim o perímetro p_n dos polígonos regulares de n lados, P_n, inscritos na circunferência dada, toma a forma $p_n = 2rn\sin(180°/n)$, $n \in \mathbb{N}$, pelo que $\pi = \lim\limits_{n\to\infty} n\sin(180°/n)$.

Para analisarmos este limite, represente-se geometricamente o $\sin a$ e $\tan a$ com $a \in]0, 90°[$ (cf. figura 5). Assim, para todo o $a \in]0, 90°[$ temos $\sin a \leq a \leq \tan a$, ou ainda $1 \leq a/\sin a \leq 1/\cos a$. Agora considerando uma sucessão infinitesimal, arbitrária $(a_n) \subset \mathbb{R}^+$, temos que $1 \leq a_n/\sin a_n \leq 1/\cos a_n$, $n \in \mathbb{N}$, e como $\lim\limits_{n\to+\infty} \cos a_n = 1$ concluímos que $\lim\limits_{n\to+\infty} a_n/\sin a_n = 1$. Da arbitrariedade da sucessão infinitesimal (a_n) temos que $\lim\limits_{a\to0^+} \sin a/a = 1$. Verifica que $\lim\limits_{a\to0^-} \sin a/a = 1$ (exercício). Logo π radianos $= 180°$.

Definição de e: Considere as funções, φ , ϕ , definidas em $\mathbb{R}^+$ por $\varphi(x) = (1 + 1/x)^x$ e $\phi(x) = (1 + 1/x)^{x+1}$. Mostre que:

(1) φ é crescente e ϕ é decrescente em $\mathbb{R}^+$.
   Indicação: Considere a desigualdade $x^\alpha < 1 + \alpha(x - 1)$, válida para $\alpha \in]0, 1[$ e $x \in]1, +\infty[$, e tome sucessivamente $x = 1 + 1/b$ e $\alpha = b/a < 1$, e $x = 1 - 1/(b + 1)$ e $\alpha = (b + 1)/(a + 1)$.

(2) Para $x, y \in \mathbb{R}^+$ com $x > y$ temos $\varphi(y) < \varphi(x) < \phi(x) < \phi(y)$.

(3) $0 < \phi(t) - \varphi(t) = \varphi(t)/t$.

Agora, como φ é uma função monótona e limitada, inferiormente por $\varphi(1) = 2$ e superiormente por $\phi(1) = 4$, temos que existe o $\lim\limits_{t\to+\infty} \varphi(t)$. Da última alínea, vemos que não só existe o limite $\lim\limits_{t\to+\infty} \phi(t)$ como coincide com o o anterior. A este valor comum designamos por e .

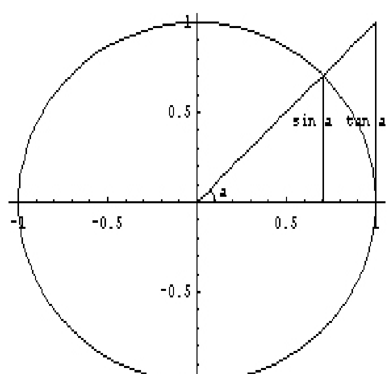


FIGURA 5. Relação entre o seno e a tangente de um ângulo