Aula 3 – Conjuntos Finitos, Enumeráveis e Não-Enumeráveis

Metas da aula: Apresentar a definição de conjunto finito e de número de elementos de um conjunto finito. Definir conjunto enumerável e conjunto não-enumerável.

Objetivos: Ao final desta aula, você deverá ser capaz de:

- Saber o significado e o uso da definição matemática de conjunto finito bem como demonstrar fatos simples envolvendo esse conceito;
- Saber o significado e o uso da definição matemática de conjunto enumerável bem como demonstrar fatos simples envolvendo esse conceito.

Conjuntos Finitos e Infinitos

O Produto Interno Bruto (PIB) dos Estados Unidos da América, no ano de 2005, foi calculado em 12.452.000.000.000 (doze trilhões, quatrocentos e cinqüenta e dois bilhões) de dólares e o do Brasil, no mesmo ano de 2005, foi calculado em 795.000.000.000 (setecentos e noventa e cinco bilhões) de dólares. Essas estimativas deram aos EUA e ao Brasil, respectivamente, a 1ª e a 11ª posição na classificação das maiores economias do mundo.

O fato para o qual queremos chamar atenção aqui não tem nada a ver com economia.

O ponto que queremos ressaltar é que, no nosso dia-a-dia, por exemplo, na leitura de um jornal, podemos nos deparar com números tão grandes que nenhum ser humano na face da Terra seria capaz de contar 1, 2, 3,. . . , até chegar a eles, sem saltar nenhum número intermediário, simplesmente porque seriam necessários centenas ou milhares de anos para fazê-lo, estimando-se que levássemos, digamos, *em média*, 1/2 segundo para recitar cada um deles. Mesmo assim, você não hesitaria em afirmar prontamente que os números referentes aos PIBs citados representam quantidades *finitas*, seja lá o que isso realmente signifique em última instância.

O fato é que a noção de conjunto finito é extremamente primitiva, e o ser humano criou sistemas numéricos capazes de representar qualquer quantidade finita muito antes de se preocupar em obter uma definição matemática precisa do que venha ser conjunto finito. Muito ao contrário, a definição que se procurou dar em tempos muito mais recentes (há menos de um século e meio) tinha, diante de si, o desafio de possibilitar a demonstração matemática de fatos absolutamente evidentes para o senso comum como, por exemplo, o de que "a união de uma quantidade finita de conjuntos finitos é um conjunto finito". Afinal, temos certeza de que um trilhão é uma quantidade finita porque sabemos que um trilhão corresponde a mil grupos de um bilhão de elementos e, por sua vez, um bilhão corresponde a mil grupos de um milhão, que por sua vez corresponde a mil grupos de mil etc. Por ora basta; vamos à definição matemática.

Definição 3.1

1. Dizemos que o conjunto vazio $\emptyset$ tem 0 **elementos**.
2. Se $n \in \mathbb{N}$, dizemos que um conjunto A tem n **elementos** se existe uma bijeção do conjunto $J_n := \{1, 2, \ldots, n\}$ sobre A. Se A tem n elementos, dizemos que n é a *cardinalidade de* A e denotamos, $n = \#(A)$, ou $n = \operatorname{card}(A)$.
3. Um conjunto é dito **finito** se, ou é vazio, ou tem n elementos para algum $n \in \mathbb{N}$.
4. Um conjunto A é dito **infinito** se ele não é finito.

Como a inversa de uma bijeção é uma bijeção, segue que o conjunto A tem n elementos se e somente se existe uma bijeção de A sobre J_n. Do mesmo modo, como a composisão de duas bijeções é uma bijeção, temos que um conjunto A tem n elementos se e somente se existe uma bijeção de A sobre um outro conjunto B que possui n elementos. Além disso, um conjunto C é finito se e somente se existe uma bijeção de C sobre um conjunto D que é finito.

Uma vez apresentada a definição matemática do que venha ser um conjunto ter n elementos é preciso, antes de mais nada, que se verifique a unicidade deste n, isto é, que um mesmo conjunto não pode possuir, de acordo com a definição, mais de um número n de elementos. Além disso, poderia acontecer que, com a definição dada, fosse possível mostrar que $\mathbb{N}$ é finito, o que iria contrariar a noção primitiva que temos desse conceito. Assim, é preciso mostrar que a definição acima implica que $\mathbb{N}$ é infinito, como manda o senso comum.

Teorema 3.1 (Unicidade)
Se $m, n \in \mathbb{N}$ e $m < n$, então não pode existir uma bijeção $f : J_m \to J_n$. Em particular, se A é finito $\#(A)$ é um número único.

Prova: Suponhamos, por absurdo, que existam $m, n \in \mathbb{N}$, com $m < n$, tal que existe uma bijeção $f : J_m \to J_n$. Então, o conjunto C dos $n \in \mathbb{N}$ para os quais existe $m < n$ tal que existe uma bijeção entre J_m e J_n é não-vazio.

Pelo Princípio da Boa Ordenação esse conjunto possui um menor elemento n_0. Assim, existem $m_0 < n_0$ e uma bijeção $f : J_{m_0} \to J_{n_0}$. Claramente $n_0 > 1$, pois do contrário não haveria $m \in \mathbb{N}$ com $m < n_0$. Se $f(m_0) = n_0$ então $f|J_{m_0-1}$ é uma bijeção entre J_{m_0-1} e J_{n_0-1}, o que contradiz o fato de n_0 ser o menor elemento de C. Por outro lado, se $f(m_0) \neq n_0$, tomemos $m_1 \in J_{m_0}$ tal que $f(m_1) = n_0$ e $n_1 \in J_{n_0}$ tal que $f(m_0) = n_1$. Definimos $g : J_{m_0} \to J_{n_0}$ pondo $g(m_0) = n_0$, $g(m_1) = n_1$, e $g(m) = f(m)$, para todo $m \in J_{m_0} \setminus \{m_1, m_0\}$. Claramente, g é uma bijeção, dado que f o é. Então, temos que $g|J_{m_0-1}$ é uma bijeção entre J_{m_0-1} e J_{n_0-1}, o que nos dá novamente uma contradição e prova a primeira parte do teorema.

Quanto a $\#(A)$ ser um número único, se isso não fosse verdade existiriam $m, n \in \mathbb{N}$, com $m < n$, e duas bijeções $f : J_m \to A$ e $g : J_n \to A$. Nesse caso, $f \circ g^{-1}$ seria uma bijeção de J_m sobre J_n o que contradiz a parte já provada do teorema. Logo, $\#(A)$ é um número único.

□

Teorema 3.2
O conjunto $\mathbb{N}$ dos números naturais é um conjunto infinito.

Prova: Suponhamos por absurdo que $\mathbb{N}$ é finito. Nesse caso existe $m \in \mathbb{N}$ e uma bijeção $f : J_m \to \mathbb{N}$. Seja $n := f(m)$. Definimos $g : \mathbb{N} \to \mathbb{N} \setminus \{n\}$ pondo $g(k) = k$, se $k < n$, e $g(k) = k + 1$, se $k \geq n$. Então g é uma bijeção (por quê?). Por outro lado, como f é bijeção, então $h := f|J_{m-1}$ é uma bijeção entre J_{m-1} e $\mathbb{N} \setminus \{n\}$. Logo, $g^{-1} \circ h$ é uma bijeção de J_{m-1} sobre J_m o que nos dá uma contradição em vista do Teorema 3.1. Logo, $\mathbb{N}$ é um conjunto infinito.

□

O próximo resultado estabelece algumas propriedades elementares de conjuntos finitos e infinitos.

Teorema 3.3

(a) Se A é um conjunto com m elementos e B é um conjunto com n elementos e se $A \cap B = \emptyset$, então $A \cup B$ tem $m+n$ elementos.

(b) Se A é um conjunto com m elementos e $C \subset A$ é um conjunto com 1 elemento então $A \setminus C$ é um conjunto com $m-1$ elementos.

(c) Se C é um conjunto infinito e B é um conjunto finito, então $C \setminus B$ é um conjunto infinito.

Prova: Provemos (a). Seja f uma bijeção de J_m sobre A e g uma bijeção de J_n sobre B. Definimos $h : J_{m+n} \to A \cup B$ pondo $h(i) := f(i)$, para $i = 1, \dots, m$, e $h(i) = g(i-m)$, para $i = m+1, \dots, m+n$. Você poderá verificar sem dificuldade que h é uma bijeção de J_{m+n} sobre $A \cup B$.

A demonstração de (b) segue diretamente de (a). A prova de (c) segue também de (a), mas por contradição, supondo, por absurdo, que C é um conjunto infinito, B é um conjunto finito e que $C \setminus B$ é um finito. Os detalhes dessas demonstrações são deixados para você como exercício (veja Exercício 2 ao final desta aula).

$\square$

O fato de que um subconjunto de um conjunto finito também é um conjunto finito é intuitivamente óbvio mas precisa ser demonstrado partindo-se da definição dada acima. Como veremos, a prova, embora simples, requer um pouco mais de trabalho que o esperado.

Teorema 3.4
Suponhamos que A e B sejam conjuntos e que $A \subset B$.

(a) Se B é um conjunto finito então A é um conjunto finito.

(b) Se A é um conjunto infinito então B é um conjunto infinito.

Prova: Provemos, inicialmente, (a). Se $A = \emptyset$ então já sabemos que A é finito e nada há para demonstrar. Suponhamos então que $A \neq \emptyset$. A prova será feita por indução sobre o número de elementos de B. Se B tem 1 elemento então o único subconjunto não-vazio de B é ele próprio. Logo $A = B$ e, portanto, A é finito.

Suponhamos que todo subconjunto de um conjunto com n elementos é finito; essa é a proposição $P[n]$ cuja veracidade tomamos como hipótese. Provemos que, neste caso, vale $P[n+1]$, isto é, que todo subconjunto de um conjunto com $n+1$ elementos é finito. Seja, então, B um conjunto com

$n+1$ elementos, $A \subset B$ e seja $f : J_{n+1} \to B$ uma bijeção. Se $f(n+1) \notin A$, então $A \subset B_1 := B \setminus \{f(n+1)\}$ e, pelo ítem (b) do Teorema 3.3, B_1 tem n elementos. Logo, pela hipótese de indução $P[n]$, nesse caso A é finito. Por outro lado, se $f(n+1) \in A$, então $A_1 := A \setminus \{f(n+1)\}$ é subconjunto de B_1 que tem n elementos. Logo, A_1 é finito. Mas então, pelo ítem (a) do Teorema 3.3, $A = A_1 \cup \{f(n+1)\}$ é finito.

A afirmação (b) é a contrapositiva de (a). Recordemos que a contrapositiva de uma proposição da forma $p \Rightarrow q$ é a proposição $\sim q \Rightarrow \sim p$ e que essas duas proposições são equivalentes, isto é, possuem tabelas-verdade idênticas.

$\square$

Conjuntos Enumeráveis

Os conjuntos infinitos são divididos em duas classes complementares: a dos que são *enumeráveis* e a dos que são *não-enumeráveis*.

Definição 3.2
Diz-se que um conjunto A é **enumerável** se ele é finito ou se existe uma bijeção $f : \mathbb{N} \to A$. No segundo caso, diremos que A é **infinito enumerável**, quando quisermos enfatizar o fato do conjunto ser infinito, que decorre imediatamente da existência da referida bijeção e do fato de que $\mathbb{N}$ é infinito. A bijeção f de $\mathbb{N}$ sobre A é chamada uma enumeração dos elementos de A e, denotando-se $a_k = f(k)$, podemos escrever $A = \{a_1, a_2, a_3, \cdots\}$. Diz-se que um conjunto A é **não-enumerável** se ele não é enumerável.

Pelas propriedades das bijeções, é claro que A é infinito enumerável se e somente se existe uma bijeção de A sobre $\mathbb{N}$. Outrossim, A é infinito enumerável se e somente se existe uma bijeção de A sobre um conjunto B que é infinito enumerável. De modo mais geral, A é enumerável se e somente se existe uma bijeção de A sobre um conjunto B enumerável.

Exemplos 3.1

(a) O conjunto $\mathbf{P} = \{2n \ : \ n \in \mathbb{N}\}$ dos números naturais pares é infinito enumerável, já que $f : \mathbb{N} \to \mathbf{P}$ definida por $f(n) = 2n$, para $n \in \mathbb{N}$, é uma bijeção de $\mathbb{N}$ sobre $\mathbf{P}$. Do mesmo modo, o conjunto dos números naturais ímpares $\mathbf{I} = \{2n-1 \ : \ n \in \mathbb{N}\}$ é infinito enumerável, já que $g : \mathbb{N} \to \mathbf{I}$ definida por $g(n) = 2n-1$ é uma bijeção de $\mathbb{N}$ sobre $\mathbf{I}$.

(b) O conjunto $\mathbb{Z}$ dos números inteiros é enumerável.

Podemos descrever uma enumeração para $\mathbb{Z}$ de modo esquemático na forma

$$\begin{array}{ccccccc} 0, & -1, & 1, & -2, & 2, & -3, & 3, \cdots . \\ \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{array}$$

Isto é, o 1 é aplicado sobre 0, os números naturais pares são aplicados sobre os inteiros negativos e os números naturais ímpares sobre os inteiros positivos, ou seja, os números naturais. A bijeção correspondente, $f : \mathbb{N} \to \mathbb{Z}$, é definida de modo explícito por

$$f(k) = \begin{cases} \frac{(k-1)}{2}, & \text{se } k \text{ é ímpar} \\ -\frac{k}{2}, & \text{se } k \text{ é par} \end{cases} .$$

(c) A união de dois conjuntos enumeráveis disjuntos é um conjunto enumerável.

Sejam A e B conjuntos enumeráveis, com $A \cap B = \emptyset$. Se A e B são finitos $A \cup B$ é finito pelo Teorema 3.3 e, portanto, é enumerável. Se um deles, digamos, A, é finito, com $A = \{a_1, \dots, a_p\}$, e o outro, B, é infinito enumerável, com $B = \{b_1, b_2, b_3, \dots\}$, então definimos uma bijeção $f : \mathbb{N} \to A \cup B$ pondo $f(k) := a_k$, para $k = 1, \dots, p$, e $f(k) := b_{k-p}$, para $k > p$. Portanto, $A \cup B$ é infinito enumerável. Finalmente, se A e B são infinitos enumeráveis, com $A = \{a_1, a_2, a_3, \dots\}$ e $B = \{b_1, b_2, b_3, \dots\}$, definimos uma bijeção $f : \mathbb{N} \to A \cup B$ pondo $f(k) = a_{\frac{(k+1)}{2}}$, se k é ímpar, e $f(k) = b_{\frac{k}{2}}$, se k é par. De modo esquemático representamos essa enumeração na forma

$$\begin{array}{cccccc} a_1, & b_1, & a_2, & b_2, & a_3, & b_3, \cdots \\ \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow \\ 1 & 2 & 3 & 4 & 5 & 6 \end{array}$$

Teorema 3.5
Todo subconjunto $A \subset \mathbb{N}$ é enumerável.

Prova: Se A é finito então A é enumerável, por definição, e nada há para provar. Se A é infinito, definimos uma bijeção f de $\mathbb{N}$ sobre A pondo $f(1) := a_1$, onde a_1 é o menor elemento de A, $f(2) := a_2$, sendo a_2 o menor elemento de $A \backslash \{a_1\}$, e assim por diante. Isto é, supondo que $f(1) := a_1, \dots, f(n) := a_n$ tenham sido definidos, com $a_1 < a_2 < \cdots < a_n$, definimos $f(n+1) := a_{n+1}$, onde a_{n+1} é o menor elemento de $A \backslash \{a_1, \dots, a_n\}$. Afirmamos que $f : \mathbb{N} \to A$ assim definida é uma bijeção. Claramente f é injetiva pois $f(m) < f(n)$, se

$m < n$. Em particular, $f(\mathbb{N})$ é um conjunto infinito enumerável pois f é uma bijeção de $\mathbb{N}$ sobre $f(\mathbb{N})$. Por outro lado, se houvesse $a \in A$ tal que $a \notin f(\mathbb{N})$, então a seria necessariamente maior que todos os elementos de $f(\mathbb{N})$ e, portanto, teríamos $f(\mathbb{N}) \subset J_a$, o que, pelo Teorema 3.4(a), contradiz o fato de $f(\mathbb{N})$ ser infinito.

$\square$

O resultado a seguir mostra que subconjuntos de conjuntos enumeráveis também são conjuntos enumeráveis.

Teorema 3.6
Suponhamos que A e B são conjuntos e que $A \subset B$.

(a) Se B é enumerável, então A é enumerável.

(b) Se A é não-enumerável, então B é não enumerável.

Prova: Provemos inicialmente (a). Se B é finito, então A é finito, pelo Teorema 3.4(a), e, portanto, é enumerável. Suponhamos então que B é infinito enumerável. Nesse caso, existe uma bijeção $g : B \to \mathbb{N}$, de B sobre $\mathbb{N}$. Pondo $h := g|A$, temos que h é uma bijeção de A sobre um subconjunto de $\mathbb{N}$, isto é, h é uma bijeção de A sobre um conjunto enumerável, pelo Teorema 3.5. Logo, A é enumerável.

A afirmação (b) é eqüivalente a (a) pois é a sua contrapositiva.

$\square$

Teorema 3.7
As seguintes afirmações são eqüivalentes.

(a) A é um conjunto enumerável.

(b) Existe uma sobrejeção de $\mathbb{N}$ sobre A.

(c) Existe uma injeção de A para $\mathbb{N}$.

Prova: (a)$\Rightarrow$(b) Se A é finito, existe uma bijeção f de algum conjunto J_n sobre A e então definimos $g : \mathbb{N} \to A$ por

$$g(k) := \begin{cases} f(k), & \text{para } k = 1, \dots, n, \\ f(n), & \text{para } k > n. \end{cases}$$

Então, g é uma sobrejeçào de $\mathbb{N}$ sobre A. Se A é infinito enumerável, então existe uma bijeção f de $\mathbb{N}$ sobre A, a qual é, em particular, uma sobrejeção de $\mathbb{N}$ sobre A.

(b)$\Rightarrow$(c) Se f é uma sobrejeção de $\mathbb{N}$ sobre A, definimos $g : A \to \mathbb{N}$ pondo $g(a)$ igual ao menor elemento do conjunto não-vazio de números naturais $f^{-1}(a) := \{n \in \mathbb{N} \, : \, f(n) = a\}$. Como $f(g(a)) = a$, segue que g é injetiva (por quê?).

(c)$\Rightarrow$(a) Se g é uma injeção de A para $\mathbb{N}$, então g é uma bijeção de A sobre $g(A) \subset \mathbb{N}$. Pelo Teorema 3.6(a), $g(A)$ é enumerável, donde se conclui que o conjunto A é enumerável.

$\square$

Teorema 3.8
O conjunto $\mathbb{N} \times \mathbb{N}$ é infinito enumerável.

Prova: Lembremos que $\mathbb{N} \times \mathbb{N}$ consiste de todos os pares ordenados (m, n) com $m, n \in \mathbb{N}$. Obtemos uma enumeração para os elementos de $\mathbb{N} \times \mathbb{N}$ de modo esquemático na forma:

$$\begin{array}{ccccccc} (1,1), & (1,2), & (2,1), & (1,3), & (2,2), & (3,1), & (1,4), \cdots, \\ \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{array}$$

no sentido crescente da soma $m + n$ e de m (Fig. **3.1**).

A fórmula explícita para a bijeção de $\mathbb{N}$ sobre $\mathbb{N} \times \mathbb{N}$ representada esquematicamente como acabamos de descrever será dada na seção Prossiga ao final desta aula.

Uma outra forma de mostrar que $\mathbb{N} \times \mathbb{N}$ é a seguinte. Você deve se lembrar de que um número natural é dito *primo* se os únicos números naturais dos quais ele é múltiplo são o 1 e ele próprio. Pode-se provar sem dificuldade que todo número natural admite uma única decomposição em fatores primos (veja Exercício 14, abaixo). Observe então que a função $g(m, n) := 2^m 3^n$ é uma injeção de $\mathbb{N} \times \mathbb{N}$ para $\mathbb{N}$, como conseqüência da unicidade da decomposição dos números naturais em fatores primos. Assim, pelo Teorema 3.7(c), $\mathbb{N} \times \mathbb{N}$ é enumerável. De passagem, observamos que, como é usual, escrevemos, de forma mais simples, $g(m, n)$ em vez de $g((m, n))$.

$\square$

Teorema 3.9
O conjunto dos números racionais $\mathbb{Q}$ é infinito enumerável.

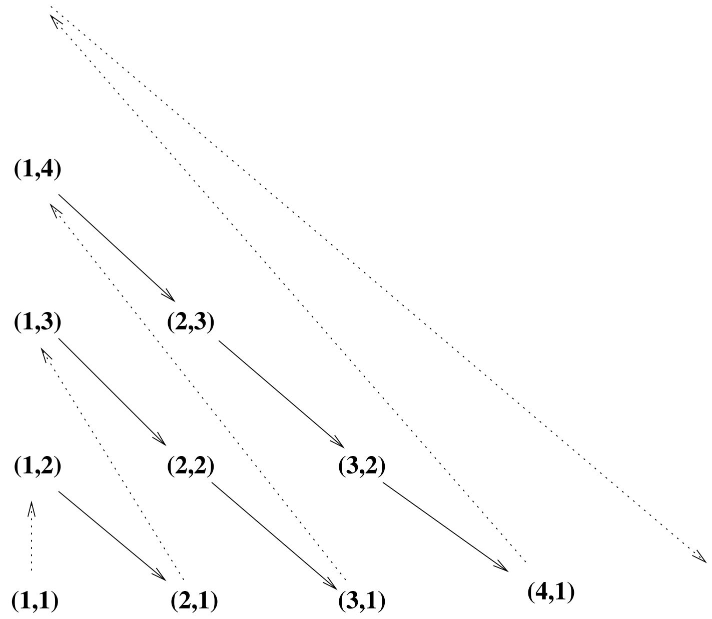

Figura **3.1**: Enumeração de $\mathbb{N} \times \mathbb{N}$ pelo processo diagonal

Prova: Lembre-se de que $\mathbb{Q}$ é definido por $\mathbb{Q} = \{\frac{m}{n} : m, n \in \mathbb{Z},\ n \neq 0\}$. Já provamos que $\mathbb{Z}$ é (infinito) enumerável e, portanto, $\mathbb{Z} \setminus \{0\}$ também é, pelos Teoremas 3.6(a) e 3.3(c). Assim, existem bijeções $g_1 : \mathbb{N} \to \mathbb{Z}$ e $g_2 : \mathbb{N} \to \mathbb{Z} \setminus \{0\}$. Então, $G((j,k)) = (g_1(j), g_2(k))$ é uma bijeção de $\mathbb{N} \times \mathbb{N}$ sobre $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ (por quê?). Como $\mathbb{N} \times \mathbb{N}$ é enumerável, então $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ é enumerável. Portanto, existe uma bijeção $h_1 : \mathbb{N} \to \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$.

Agora, a função $h_2 : \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) \to \mathbb{Q}$ definida por $h_2(m,n) = \frac{m}{n}$ é uma sobrejeção de $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ sobre $\mathbb{Q}$ (por quê?). Logo $f := h_2 \circ h_1$ é uma sobrejeção de $\mathbb{N}$ sobre $\mathbb{Q}$. Pelo Teorema 3.7(b) concluímos que $\mathbb{Q}$ é enumerável. Como $\mathbb{Q}$ contém $\mathbb{N}$ e este último é infinito, segue também que $\mathbb{Q}$ é infinito.

□

A Figura **3.2** representa o esquema do processo diagonal para enumeração dos elementos de $\mathbb{Q}$ implicitamente empregado na prova anterior.

O próximo resultado estabelece que a união de uma coleção (possivelmente infinita) enumerável de conjuntos enumeráveis é também um conjunto enumerável.

Teorema 3.10
Se A_m é um conjunto enumerável para cada $m \in \mathbb{N}$, então a união $A := \bigcup_{m=1}^{\infty} A_m$ é enumerável.

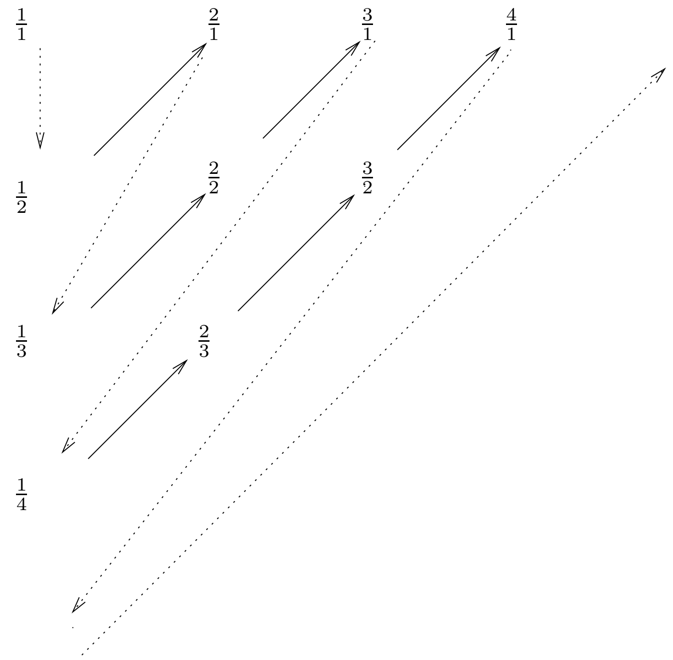

Figura **3.2**: Enumeração de $\mathbb{Q}$ pelo processo diagonal.

Prova: Em vista do Teorema 3.7, precisamos apenas mostrar que existe uma sobrejeçào de $\mathbb{N}$ sobre A. Para cada $m \in \mathbb{N}$, seja g_m uma sobrejeção de $\mathbb{N}$ sobre A_m; tal sobrejeçào existe já que A_m é enumerável. Definimos $g : \mathbb{N} \times \mathbb{N} \to A$ por

$$g(m, n) = g_m(n).$$

Afirmamos que g é uma sobrejeção; deixaremos a você a demonstração simples desse fato (veja Exercício 8, abaixo). Como $\mathbb{N} \times \mathbb{N}$ é enumerável, existe uma bijeção e, portanto, uma sobrejeção $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$, donde $g \circ f$ é uma sobrejeção de $\mathbb{N}$ sobre A. Aplicando o Teorema 3.7 outra vez, concluímos que A é enumerável. Observe que o caso da união de uma coleção finita de conjuntos enumeráveis $A_1, \dots, A_n$ decorre do que acabamos de provar; basta fazer $A_k = A_n$, para $k = n + 1, n + 2, \dots$.

$\square$

Para concluir, vamos enunciar e provar um belíssimo teorema devido a Georg Cantor (1845-1918) a quem também devemos a idéia genial do processo diagonal para mostrar que $\mathbb{N} \times \mathbb{N}$ e $\mathbb{Q}$ são enumeráveis. A prova que daremos é igualmente devida a Cantor e também envolve um raciocínio "diagonal", como veremos.

Teorema 3.11 (Teorema de Cantor)
Se A é um conjunto qualquer, então não existe nenhuma sobrejeção de A sobre o conjunto $\mathcal{P}(A)$ de todos os subconjuntos de A.

Prova: Suponhamos que $g : A \to \mathcal{P}(A)$ é uma sobrejeção. Para cada $a \in A$, $g(a)$ é um subconjunto de A e, portanto, a pode ou não ser um elemento de $g(a)$. Então, definimos o conjunto

$$D := \{a \in A \,:\, a \notin g(a)\}.$$

Como D é subconjunto de A e, por conseguinte, $D \in \mathcal{P}(A)$, e como g é sobrejeção, então $D = g(a_0)$ para algum $a_0 \in A$. Devemos ter $a_0 \in D$, ou $a_0 \notin D$. Se $a_0 \in D$, então, como $D = g(a_0)$, $a_0 \in g(a_0)$, o que contradiz a definição de D. Da mesma forma, se $a_0 \notin D$, então $a_0 \notin g(a_0)$ e, pela definição de D, devemos ter $a_0 \in D$, o que também nos dá uma contradição. Portanto, não pode existir uma tal sobrejeção.

$\square$

O Teorema de Cantor implica, em particular, que $\mathcal{P}(\mathbb{N})$ é não-enumerável, já que não pode existir uma bijeçào de $\mathbb{N}$ sobre $\mathcal{P}(\mathbb{N})$.

Exercícios 3.1

1. Prove que um conjunto A é finito se e somente se existe uma bijeçào de A sobre um conjunto finito B.
2. Dê os detalhes da prova das partes (b) e (c) do Teorema 3.3.
3. Seja $A := \{1, 2\}$ e $B := \{a, b, c\}$.
   (a) Determine o número de injeções diferentes de A para B.
   (b) Determine o número de sobrejeções diferentes de A para B.
4. Exibir uma bijeção uma bijeção entre $\mathbb{N}$ e todos os números ímpares maiores que 11.
5. Exiba uma bijeção entre $\mathbb{N}$ e um seu subconjunto próprio.
6. Prove que A é enumerável se e somente se existe uma bijeção de A sobre um conjunto B enumerável.
7. Dê um exemplo de uma coleção enumerável de conjuntos finitos cuja união não é finita.

8. Prove que a função $g : \mathbb{N} \times \mathbb{N} \to A$, definida na demonstração do Teorema 3.10 é de fato uma sobrejeção.

9. Prove que o conjunto dos números primos é infinito enumerável. (Dica: Para provar que esse conjunto é finito, argumente por contradição.)

10. Obtenha uma representação $\mathbb{N} = A_1 \cup A_2 \cup \cdots \cup A_n \cup \cdots$ tal que os conjuntos A_1, A_2,..., A_n, ...sejam infinitos e dois a dois disjuntos.

11. Use o Princípio da Indução Matemática para provar que se A tem n elementos então $\mathcal{P}(A)$ tem 2^n elementos.

12. Seja $A \subset \mathbb{N}$ infinito. Prove que existe uma única bijeção crescente $f : \mathbb{N} \to A$ $(m < n \Rightarrow f(m) < f(n))$. (Dica: Para provar a existência de uma tal função use reiteradas vezes o Princípio da Boa Ordenação e o fato de que A é infinito.)

13. Prove que a coleção $\mathcal{F}(\mathbb{N})$ de todos os subconjuntos *finitos* de $\mathbb{N}$ é enumerável.

14. Prove que todo número natural possui uma única representação como produto de potências de números primos. (Dica: Use o Princípio da Indução Forte para mostrar que existe uma tal representação. A unicidade decorre da definição de número primo e do fato que se n é um múltiplo de m, então todo divisor de m é um divisor de n.)

15. Inspirado pela demonstração do Teorema de Cantor, prove que o conjunto das funções $f : \mathbb{N} \to \{0, 1\}$ é não-enumerável.

Prossiga: O Processo Diagonal de Cantor.

Como os grandes gênios do futebol, Cantor era totalmente investido daquele "sentimento diagonal do homem-gol", evocado nos versos da canção "O futebol" de Chico Buarque. Em um punhado de momentos de pura genialidade, Cantor recorreu a "ataques pela diagonal" para furar bloqueios que guardavam verdadeiras maravilhas matemáticas atrás de si.

Vamos a seguir determinar mais precisamente a bijeção $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ representada pictoricamente na Figura **3.1** e com isso completar a prova do Teorem 3.8.

Em vez de buscar diretamente uma expressão para f, é bem mais simples exibir uma expressão para a inversa de f, $g : \mathbb{N}\times\mathbb{N} \to \mathbb{N}$. Portanto, o que temos a fazer é encontrar uma expressão para g e provar que essa expressão realmente representa uma bijeção; neste caso, teremos também provado que a inversa de g, isto é, f, é uma bijeção de $\mathbb{N}$ sobre $\mathbb{N} \times \mathbb{N}$.

Inicialmente, observemos que $\mathbb{N} \times \mathbb{N}$ pode ser visto como uma coleção de diagonais: a primeira delas contém apenas o ponto $(1, 1)$; a segunda contém 2 pontos $(1, 2)$ e $(2, 1)$; a terceira contém 3 pontos $(1, 3)$, $(2, 2)$, $(3, 1)$ etc. Assim, a k-ésima diagonal contém k pontos (m, n) cuja soma das coordenadas é constante $m + n = k + 1$. Em particular, o número de pontos incluídos da primeira até a k-ésima diagonal (inclusive) é:

$$S(k) := 1 + 2 + \cdots + k = \frac{1}{2}k(k + 1).$$

A segunda equação foi verificada no Exemplo 2.1(a). Ora, para um ponto (m, n) qualquer, sabemos que ele pertence à $(m + n - 1)$-ésima diagonal, e a sua ordem na enumeração estabelecida no processo diagonal será igual ao número de pontos contidos nas diagonais que antecedem a diagonal à qual ele pertence, isto é, $S(m + n - 2)$ mais o valor de sua primeira coordenada m. Sendo sssim, definimos:

$$g(m, n) := S(m + n - 2) + m, \qquad \text{para } (m, n) \in \mathbb{N} \times \mathbb{N}. \tag{3.1}$$

Conclusão da Prova do Teorema 3.8: Vamos então mostrar que g definida em (3.1) é uma bijeção de $\mathbb{N} \times \mathbb{N}$ sobre $\mathbb{N}$. Mostremos inicialmente que g é injetiva. Se $(m, n) \neq (m', n')$, então:

ou (i) $m + n \neq m' + n'$;

ou (ii) $m + n = m' + n'$ e $m \neq m'$.

De fato, chamando de P a proposição $m + n \neq m + n$ e Q a proposição $m \neq m'$, então (i) é P e (ii) é $\sim P$ e Q. Assim, a negação da proposição "(i) ou (ii)" é a proposição "$\sim P$ e (P ou $\sim Q$)" que é equivalente a "$\sim P$ e $\sim Q$", isto é, $m + n = m' + n'$ e $m = m'$, que, por sua vez, é equivalente a $(m, n) = (m', n')$.

Caso tenhamos (i), podemos supor $m + n < m' + n'$. Notemos que vale

$$S(k + 1) = S(k) + (k + 1). \tag{3.2}$$

Então, usando (3.2), o fato, que daí decorre, de que S é crescente, e também que $m' > 0$, temos

$$\begin{aligned} g(m, n) &= S(m + n - 2) + m \leq S(m + n - 2) + (m + n - 1) \\ &= S(m + n - 1) \leq S(m' + n' - 2) \\ &< S(m' + n' - 2) + m' = g(m', n'). \end{aligned}$$

Caso tenhamos (ii), então

$$g(m,n) - m = S(m+n-2) = S(m'+n'-2) = g(m',n') - m',$$

donde se conclui, igualmente, que $g(m,n) \neq g(m',n')$. Portanto, g é injetiva.

Mostremos agora que g também é sobrejetiva. Claramente $g(1,1) = 1$. Se $r \in \mathbb{N}$, com $r \geq 2$, encontraremos $(m_r, n_r) \in \mathbb{N} \times \mathbb{N}$ com $g(m_r, n_r) = r$. Como $r < S(r)$, então o conjunto $C_r := \{k \in \mathbb{N} : S(k) \geq r\}$ é não-vazio. Usando o Princípio da Boa Ordenação, seja $k_r > 1$ o menor elemento em C_r. Em particular, $S(k_r - 1) < r$. Assim, como $r \geq 2$, usando (3.2), temos

$$S(k_r - 1) < r \leq S(k_r) = S(k_r - 1) + k_r.$$

Seja $m_r := r - S(k_r - 1)$, de modo que $1 \leq m_r \leq k_r$, e seja $n_r := k_r - m_r + 1$, de modo que $1 \leq n_r \leq k_r$ e $m_r + n_r - 1 = k_r$. Daí segue que

$$g(m_r, n_r) = S(m_r + n_r - 2) + m_r = S(k_r - 1) + m_r = r.$$

Portanto, g é uma sobrejeção de $\mathbb{N} \times \mathbb{N}$ sobre $\mathbb{N}$. Como já provamos que g é uma injeção, segue que g é uma bijeção e, portanto, $\mathbb{N} \times \mathbb{N}$ é enumerável.

$\square$

Recomendamos fortemente que você faça uma pesquisa na internet sobre a vida e a obra de Georg Cantor, usando um sítio de buscas como o "http://www.google.com" ou visitando diretamente, por exemplo, a página da web: http://pt.wikipedia.org/wiki/Georg_Cantor.