Capítulo 0: Conjuntos, funções, relações

Notação. Usaremos **Nat** para representar o conjunto dos números naturais; **Int** para representar o conjunto dos números inteiros. Para cada $n \in$ **Nat**, [n] representa o conjunto dos naturais menores ou iguais a n:

$$[n] = \{\ i \in \textbf{Nat} \mid 0 < i \leq n\ \}.$$

Este conjunto [n] é às vezes representado por {1, 2, …, n}, convencionando-se que nos casos especiais n = 0 e n = 1, essa notação indica, respectivamente, o conjunto vazio $\varnothing$ e o conjunto unitário {1}.

Produto Cartesiano. O produto cartesiano de dois conjuntos A e B é o conjunto $A \times B$ de pares ordenados de elementos de A e B:

$$A \times B = \{\ (x, y) \mid x \in A \ \text{ e } \ y \in B\ \}.$$

Esse conceito pode ser estendido, usando n-tuplas, para definir o produto cartesiano de n conjuntos:

$$A_1 \times A_2 \times \dots A_n = \{\ (x_1, x_2, \dots x_n\ ) \mid \text{para cada } i \in [n], x_i \in A_i\ \}$$

Podemos definir potências de um conjunto, a partir da definição de produto Cartesiano:

$$A^n = A \times A \times \dots A \text{ (n vezes)} = \{\ (x_1, x_2, \dots x_n) \mid \text{para } i \in [n], x_i \in A\}.$$

Naturalmente, $A^1 = A$.

<u>Exemplo</u>: Sejam A = { a, b, c }, B = { d, e }. Então,

$$A \times B = \{\ (a, d), (a, e), (b, d), (b, e), (c, d), (c, e)\ \}$$

$$B \times A = \{\ (d, a), (d, b), (d, c), (e, a), (e, b), (e, c)\ \}$$

$$A^1 = A = \{\ a, b, c\ \}$$

$$A^2 = A \times A = \{\ a, b, c\ \} \times \{\ a, b, c\ \} =$$
$$= \{\ (a, a), (a, b), (a, c), (b, a), (b, b), (b, c), (c, a), (c, b), (c, c)\ \}$$

□

Relações. Podemos agora definir relação: dados n conjuntos A_1, A_2, …, A_n, uma relação em A_1, A_2, …, A_n é um conjunto qualquer de tuplas de elementos de A_1, A_2, …, A_n. Portanto, usando a definição acima, R é uma *relação* em A_1, A_2, …, A_n se

$$R \subseteq A_1 \times A_2 \times \dots \times A_n.$$

Um caso especial que será muito importante no que se segue é o caso n=2, com $A_1=A_2=A$. R é uma *relação binária* em um conjunto A, se $R \subseteq A \times A$.

Funções. Outro caso especial é o das funções: uma relação f em $A \times B$, ou seja, um conjunto $f \subseteq A \times B$, é uma *função*, com *domínio* A e *codomínio* B, se para cada $x \in A$ existe em f um único $y \in B$ tal que $(x, y) \in f$. Essa unicidade pode também ser expressa por

$(x, y) \in f$ e $(x, z) \in f$ implicam em $y = z$.

Naturalmente, esse valor único de y que f faz corresponder a x é indicado pela notação habitual f(x), e podemos escrever também $f: x \mapsto y$. Escrevemos $f: A \to B$, para indicar que f é uma função com domínio A e codomínio B.

Definimos o *contradomínio* de $f: A \to B$ como sendo o conjunto

$\{ y \in B \mid (\exists x \in A) \ (f(x) = y) \}$.

Exemplo: Se considerarmos o conjunto **Int** dos números inteiros, e a função *suc*: **Int** $\to$ **Int** que a cada valor em **Int** associa seu sucessor, poderemos escrever

para cada $i \in$ **Int**, *suc*(i) = i + 1,

ou

suc: $i \mapsto i + 1$

ou ainda

suc = { …, (-2, -1), (-1, 0), (0, 1), (1, 2), … }

□

Injeção, sobrejeção, bijeção. Dizemos que uma função $f: A \to B$ é uma *injeção* se para cada $b \in B$ existe no máximo um $a \in A$ tal que $f(a) = b$; dizemos que $f: A \to B$ é uma *sobrejeção* se para cada $b \in B$ existe no mínimo um $a \in A$ tal que $f(a) = b$; dizemos que f é uma *bijeção* se f é ao mesmo tempo, uma injeção e uma sobrejeção.

No caso de sobrejeções (e bijeções), codomínio e contradomínio são iguais.

Alternativamente, podemos falar em funções *injetoras*, *sobrejetoras* ou *"sobre"*, e *bijetoras*.

Conjuntos enumeráveis. Um conjunto A é *enumerável* se é vazio, ou se existe uma função sobrejetora f: **Nat** $\to$ A.

O nome *enumerável* se deve ao fato de que, se A não é vazio, a sequência f(0), f(1), f(2), f(3), … é uma lista infinita da qual fazem parte todos os elementos de A, ou seja, uma *enumeração* de A. Em particular, como não estão proibidas repetições em uma enumeração, temos:

Fato: Todos os conjunto finitos são enumeráveis.
Dem.: Exercício.

□

No que se segue, estaremos interessados principalmente em conjuntos enumeráveis infinitos. Neste caso, podemos usar uma *numeração*, em vez de uma *enumeração*. Por numeração entendemos aqui uma função como a função g mencionada na propriedade abaixo, que associa a cada elemento de A um número natural distinto.

<u>Fato:</u> Um conjunto infinito é enumerável, se e somente se existe uma função injetora g: A → **Nat**.
Dem. (⇒) Seja A um conjunto enumerável infinito. Pela definição, existe uma função sobrejetora f: **Nat** → A. Podemos definir a injeção g:A → **Nat** fazendo, para cada a ∈ A, g(a) ser igual ao menor valor de i tal que f(i) = a. Assim, a função g é definida para qualquer valor de a, porque f é sobrejetora. Além disso, g é injetora, porque, pela própria definição, g(a) = g(b) implica em f(g(a)) = f(g(b)).

(⇐) Seja A um conjunto tal que existe uma injeção g:A → **Nat**. Uma vez que A não é vazio, seja q um elemento qualquer de A. Defina agora a sobrejeção f: **Nat** → A por

$$f(i) = \begin{cases} a, & \text{se existir um a tal que } g(a) = i \\ q, & \text{se não existir} \end{cases}$$

Note que f é bem definida para todos os valores de i, porque g é uma injeção, e, para cada i, pode haver, no máximo, um a tal que g(a) = i; f é uma sobrejeção, porque g é definida para todos os elementos de A.

□

<u>Fato:</u> Um conjunto infinito A é enumerável se e somente se existe uma bijeção
f: A → **Nat**.
Dem.: Exercício.

□

<u>Fato:</u> Entre dois conjuntos infinitos enumeráveis A e B existe sempre uma bijeção
f: A→B.
Dem.: Exercício.

□

<u>Exemplo:</u> O conjunto **Nat** é enumerável.
Basta tomar f como sendo a função identidade I: **Nat** → **Nat**, que é, claramente, uma bijeção.

□

<u>Exemplo:</u> O conjunto $\mathbf{Nat}^2$ = **Nat** × **Nat** de pares de números naturais é enumerável.

Podemos fazer a caracterização de diversas maneiras:

1. através da injeção g:$\mathbf{Nat}^2$ → **Nat** definida por g((i,j)) = $2^i\,3^j$. Esta numeração dos pares de inteiros é às vezes chamada de *numeração de Goedel*. Esse processo pode ser estendido a potências superiores de **Nat**. Por exemplo, podemos associar à tripla (i, j, k) o número $2^i\,3^j\,5^k$. Para n-uplas, poderiam ser usados como bases os primeiros n números primos.
2. definindo diretamente a ordem de enumeração:

```
repita para cada k = 0, 1, 2, …
        enumere os pares (i, j) tais que i+j = k, na ordem crescente de i:
                (0, k), (1, k-1), …, (k-1, 1), (k, 0).
```

Isso corresponde a

(0, 0), (0, 1), (1, 0), (0, 2), (1, 1), (2, 0), (0, 3) …

ou seja, a uma sobrejeção f: **Nat** $\rightarrow$ **Nat** dada por

f(0) = (0,0), f(1) = (0,1), f(2) = (1,0), f(3) = (0,2), …

□

Exemplo: O conjunto **Int** dos inteiros é enumerável.
Basta usar uma enumeração como 0, -1, +1, -2, +2, -3, +3, …

□

Teorema: O conjunto P(**Nat**) dos subconjuntos de **Nat** não é um conjunto enumerável.

Dem.: por "diagonalização".

Uma vez que a definição de conjunto enumerável se baseia na existência de uma função com certas propriedades, devemos mostrar que tal função não existe, e a demonstração será feita por contradição (ou redução ao absurdo).

Suponhamos que o conjunto P(**Nat**) é enumerável. Isto significa que existe uma enumeração de P(**Nat**), ou seja uma sobrejeção f: **Nat** $\rightarrow$ P(**Nat**). Assim, para cada elemento A de P(**Nat**) (um conjunto A de naturais), existe um número i tal que f(i) = A.

Vamos considerar o conjunto X definido a seguir:

$X = \{ j \in \mathbf{Nat} \mid j \notin f(j) \}$

Como X é um conjunto de naturais, $X \in$ P(**Nat**). Entretanto, veremos que X não faz parte da enumeração acima. Seja k qualquer. Duas possibilidades podem ocorrer:

- ou $k \in f(k)$, e neste caso $k \notin X$,
- ou $k \notin f(k)$, e neste caso $k \in X$.

Em qualquer das possibilidades, portanto, os conjuntos X e f(k) diferem em pelo menos um elemento. Assim, $X \neq f(k)$ para todos os k. Desta forma, X não faz parte da enumeração definida por f, caracterizando-se a contradição. Consequentemente, P(**Nat**) não é enumerável.

□

Esta técnica de demonstração recebeu o nome de *diagonalização*. Representamos um conjunto $A \subseteq$ **Nat** por uma sequência infinita de 0's e 1's: se $i \in A$, o i-ésimo símbolo da sequência será 1; caso contrário, será 0. Assim, se fizéssemos uma tabela infinita com uma linha correspondendo a cada conjunto f(k), $k \in$ **Nat**, o conjunto X seria definido invertendo o que se encontra na diagonal da tabela: se na posição (i,i) se encontra um 1, indicando que $i \in f(i)$, na linha correspondente a X teríamos um 0 na i-ésima coluna, indicando que $i \notin X$, e (vice-versa) se na posição i,i se encontra um 0, indicando que $i \notin f(i)$, na linha correspondente a X teríamos um 1 na i-ésima coluna, indicando que $i \in X$.

Desta forma, podemos ver que, para qualquer i, $f(i) \neq X$. Para isso, basta notar que i pertence a exatamente um dos dois conjuntos f(i) e X. Portanto, qualquer que fosse a enumeração de P(**Nat**), X não pertenceria a ela.

Esta técnica será usada neste curso em diversas ocasiões para demonstrações semelhantes à anterior; foi usada por Cantor, para mostrar que a cardinalidade de um conjunto P(A) é sempre superior à cardinalidade de A. O mesmo vale aqui: a cardinalidade de todos os conjuntos enumeráveis infinitos A é a mesma, equivalente à de **Nat**, mas a cardinalidade dos conjuntos potência P(A) é superior à de **Nat**, sendo equivalente à de P(**Nat**). Falando *informalmente*,

- "todo conjunto enumerável tem o mesmo número de elementos que **Nat**."
- "há mais elementos em P(**Nat**) do que em **Nat**."
- "para qualquer conjunto A enumerável, P(A) tem o mesmo número de elementos que P(**Nat**)."

<u>Fato:</u> Se um conjunto A é enumerável, e se B é um subconjunto de A, B também é enumerável.
Dem. Exercício.

□

Exercícios:
(1) Mostre que, se A e B são conjuntos enumeráveis, então A×B também é enumerável.
Sugestão: se A e B são enumeráveis, existem numerações n_A: A→**Nat** e n_B: B→**Nat**; seja então g: **Nat**^{2} → **Nat** a mesma numeração de **Nat**^{2} vista anteriormente; considere então a função n: A×B → **Nat** definida por

$$n((a, b)) = g(n_A (a), n_B (b)).$$

(2) Uma das definições possíveis para par ordenado é a seguinte: definimos o par ordenado (a, b) como sendo o conjunto {{a, b}, {a}}. Mostre que, com esta definição, vale a propriedade fundamental:

(a, b) = (c, d) se e somente se a=c e b=d.

(3) Podemos definir uma tripla (ou 3-tupla) a partir da definição de par ordenado:

(a, b, c) = ((a, b), c).

Isto corresponde a definir **Nat**^{3} como **Nat**^{2}×**Nat**. Mostre que com esta definição, vale a propriedade fundamental:

(a, b, c) = (d, e, f) se e somente se (a=d) e (b=e) e (d=f).

(4) Para definir uma numeração dos elementos de **Nat**, podemos usar as funções F_1 e F_2 definidas a seguir:

$$F_1 ((i,j,k)) = 2^i\, 3^j\, 5^k$$

$$F_2 ((i,j,k)) = g((i, g((j,k)))),$$

onde g é a função definida anteriormente:

$$g((i,j)) = 2^i\, 3^j.$$

Experimente calcular F_1 ((5, 5, 5)) e F_2 ((5, 5, 5)).

□

Relações binárias. Quando tratamos de relações binárias, normalmente usamos uma notação mais simples para indicar que (x, y) é um elemento de uma relação binária R em

A: escrevemos apenas x R y. Essa notação é semelhante à usada para relações comuns, como as relações de ordem $<$, $\leq$, etc.: não escrevemos $(x, y) \in \leq$, mas, mais simplesmente, $x \leq y$.

Vamos a seguir introduzir algumas propriedades de relações binárias. Seja R uma relação binária em um conjunto A ($R \subseteq A^2$). Então dizemos que

- R é reflexiva se para qualquer $x \in A$, $x R x$;
- R é simétrica se, para quaisquer $x, y \in A$, $x R y$ implica $y R x$.
- R é transitiva se, para quaisquer $x, y, z \in A$, $x R y$ e $y R z$ implicam em $x R z$.

Exemplos: As relações $<$, $\leq$, $=$, $\neq$ são relações binárias definidas no conjunto **Nat**, e tem as propriedades indicadas a seguir:

	reflexiva	*simétrica*	*transitiva*
$<$	não	não	sim
$\leq$	sim	não	sim
$=$	sim	sim	sim
$\neq$	não	sim	não

□

Equivalência. Uma relação R é uma *relação de equivalência* (ou simplesmente uma *equivalência*) se é reflexiva, simétrica, e transitiva.

Exemplo: A relação = no conjunto **Nat** é uma relação de equivalência; outros exemplos de relações de equivalência são as relações de paralelismo entre retas, de semelhança de triângulos, de congruência módulo n. (Dois naturais x e y são *congruentes módulo n* se o resto da divisão de x por n é igual ao resto da divisão de y por n.)

□

Composição de relações: definimos a composição de relações da forma a seguir: se $R \subseteq A \times B$ e $S \subseteq B \times C$ são relações, definimos a relação $R \circ S \subseteq A \times C$, a composição de R e S, por

$$R \circ S = \{ (x, z) \in A \times C \mid \exists\, y \in B, (x, y) \in R \text{ e } (y, z) \in S \}.$$

Se as relações R e S são funções, a composição $R \circ S$ se reduz exatamente à composição de funções: se $(x, y) \in R$ e $(y, z) \in S$, temos $y = R(x)$, $z = S(y) = S(R(x))$, e portanto $(R \circ S)(x) = S(R(x))$, como era de se esperar[1].

Exemplo: Sejam as relações

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

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

Temos:

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

$S \circ R = \{ (2, 2), (2, 3), (2, 4), (3, 3), (3, 4), (4, 4) \}$

□

[1] Alguns autores preferem a ordem inversa: $(R \circ S)(x) = R(S(x))$. A diferença é apenas de notação.

Exemplo: Sejam as relações

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

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

Já que R e S são funções, o mesmo vale para as composições:

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

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

□

Operações com relações binárias. Se R é uma relação binária num conjunto A (isto é, $R \subseteq A \times A$), podemos definir as potências R^i de R, para $i \in$ **Nat** de forma recursiva:

$$R^0 = I_A = \{ (x, x) \mid x \in A \}$$

$$R^{i+1} = R^i \circ R, \text{ para } i \in \mathbf{Nat}$$

Fato:

1. A relação I_A é a identidade para a composição de relações, associada ao conjunto A, ou seja, para qualquer $R \subseteq A^2$, $R \circ I_A = I_A \circ R = R$.
2. Para qualquer $R \subseteq A^2$, $R^1 = R$.
3. Para quaisquer $R \subseteq A^2$, $i, j \in$ **Nat**, $R^i \circ R^j = R^j \circ R^i$, ou seja, potências da mesma relação sempre comutam.

Dem.: Exercício.

□

Exemplo: Sejam $A = \{ 1, 2, 3, 4 \}$ e $R = \{ (1,2), (1,3), (1,4), (2,3), (2,4), (3,4) \}$.As potências de R são:

$R^0 = I = \{ (1,1), (2,2), (3,3), (4,4) \}$.

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

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

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

$R^4 = R^5 = \ldots = \emptyset$.

No caso do exemplo, podemos provar que $(x, y) \in R$ se $y-x \geq 1$. Assim, em geral, $(x, y) \in R^i$ se $y-x \geq i$. Naturalmente, no conjunto A, a maior diferença possível é 3, e todas as potências além da terceira são relações vazias: nunca podem ser satisfeitas.

□

Fechamento. Definimos o *fechamento reflexivo-transitivo* R^* de uma relação binária R em um conjunto A através de

$x R^* y$ se e somente se para algum $i \in$ **Nat**, $x R^i y$,

ou, equivalentemente,

$$R^* = \bigcup_{i=0}^{\infty} R^i = R^0 \cup R^1 \cup R^2 \cup R^3 \cup \cdots$$

Exemplo: Seja a relação R, no conjunto **Nat** definida por

$x R y$ se e somente se $y = x + 1$.

Temos $x R^i y$ se e somente se $y = x + i$, de forma que $x R^* y$ se e somente $y \geq x$.

□

O nome de fechamento reflexivo-transitivo de R dado à relação R* se deve ao fato de que R* é a menor relação (no sentido da inclusão de conjuntos) que contém R e é reflexiva e transitiva. Ou seja, qualquer relação S

(1) que satisfaça x R y implica x S y (isto é, $S \supseteq R$) e
(2) que seja reflexiva e transitiva

satisfaz também $S \supseteq R^*$.

De forma semelhante, a notação R^+ é frequentemente utilizada para descrever o fechamento transitivo da relação R:

$$R^+ = \bigcup_{i=1}^{\infty} R^i = R^1 \cup R^2 \cup R^3 \cup \cdots$$

ou seja, x R^+ y se e somente se para algum i>0, x R^i y.

Exemplo: Seja a mesma relação R do exemplo anterior. Neste caso, temos
x R^+ y se e somente se y > x.

□

Partições. Dado um conjunto A, definimos uma *partição* de A como sendo uma família de conjuntos (chamados de *blocos da partição*) $\Pi = \{ B_i \mid i \in I \}$ com as seguintes propriedades:

(1) para cada $i \in I$, $B_i \neq \emptyset$. — *nenhum bloco é vazio*

(2) $\bigcup \Pi = \bigcup_{i \in I} B_i = A$ — *a união dos blocos é A*

(3) se $i \neq j$, $B_i \cap B_j = \emptyset$. — *blocos são disjuntos dois a dois*

Dessa maneira, cada elemento a de A pertence a exatamente um bloco da partição P.

Observação: Na maioria das vezes o conjunto I usado para indexar os elementos da família Π será um conjunto enumerável, um subconjunto dos naturais.

Exemplo: Seja o conjunto A = { a, b, c, d, e }. Temos a seguir alguns exemplos de partições de A:

{ { a, b, c, d, e } }
{ { a }, { b }, { c }, { d }, { e } }
{ { a, b }, { c, d, e } }
{ { a, e }, { b, c, d } }

□

Exercício: Escreva todas as partições de { a, b, c, d, e }.

□

Classes de equivalência. Seja R uma equivalência em um conjunto A. Definimos a classe de equivalência [*a*] de $a \in$ A da seguinte maneira:

$[a] = \{ x \in A \mid x \, R \, a \}$,

ou seja, a classe de equivalência de $a \in A$ é o conjunto dos elementos de A que são equivalentes a a. Note que como R é uma equivalência, $a \in [a]$, para qualquer a.

Exemplo: Seja a equivalência R em A = {a, b, c, d, e, f}, dada pelas seguintes propriedades:

(1) R é uma equivalência

(2) a R b, b R c, d R e.

(3) x R y somente se isto decorre de (1) e (2).

Temos então, examinando todos os casos possíveis:

a R a, b R b, c R c, d R d, e R e, f R f *(reflexividade)*
b R a, c R b, e R d *(simetria)*
a R c, c R a *(transitividade)*

e R é composta dos pares: (a, a), (a, b), (a, c), (b, a), (b, b), (b, c), (c, a), (c, b), (c, c), (d, d), (d, e), (e, d), (e, e), (f, f).

Assim podemos ver diretamente que [a] = [b] = [c] = { a, b, c }, que [d] = [e] = { d, e } e que [f] = { f }.

□

Conjunto quociente. Definimos o conjunto quociente A/R de A por uma equivalência R em A, através de

$A/R = \{ [x] \mid x \in A \}$,

ou seja, A/R é o conjunto das classes de equivalência de R em A.

Exemplo: Sejam A e R como no exemplo anterior. As classes de equivalência de R formam uma partição de A, que é exatamente o conjunto quociente A/R:

A/R = { { a, b, c }, { d, e }, { f } }

□

Fato: Seja R uma equivalência em um conjunto A. Então A/R é uma partição de A.

Dem.:

(1) note que as classes de equivalência não são vazias: à classe $[a]$ pertence pelo menos o elemento a;

(2) a união das classes de equivalência é A, porque cada elemento a de A pertence a pelo menos uma classe de equivalência: $a \in [a]$.

(3) Classes de equivalência diferentes são disjuntas. Com efeito, suponha que duas classes $[a]$ e $[b]$ tem sua interseção não vazia, com um elemento c em comum: $c \in [a]$ e $c \in [b]$. Neste caso, usando o fato de que R é simétrica e transitiva, temos c R a, c R b, e, portanto, a R b. Assim, pela propriedade transitiva, x R a se e somente se x R b, e $[a] = [b]$. Consequentemente, as classes de equivalência são disjuntas duas a duas, e formam uma partição de A.

□

Fato: Dada uma partição P de um conjunto A, a relação R definida por

x R y se e somente se x e y fazem parte do mesmo bloco de P

é uma relação de equivalência em A, e A/R = P.
Dem.: Exercício.

□

Indução finita. Muitas das demonstrações que veremos nas seções seguintes utilizam uma técnica conhecida por *indução finita*. A idéia fundamental é simples: suponha que desejamos provar que a propriedade P vale para todos os elementos de **Nat**, isto é, que queremos provar que, para todo x ∈ **Nat**, P(x).

Uma propriedade fundamental de **Nat** é que **Nat** é composto por um elemento especial, 0, e por seus sucessores. Dito de outra forma, **Nat** é o menor conjunto que contém 0 e é fechado para a função *sucessor s*. Esquematicamente,

Nat = { 0, *s*(0), *s*(*s*(0)), *s*(*s*(*s*(0))), *s*(*s*(*s*(*s*(0))))… }.

Assim, se provarmos

I. *(base da indução)*

P(0)

II. *(passo de indução)*

Para qualquer i ∈ **Nat**, P(i) implica P(s(i)).

estaremos provando P para todos os naturais, pois teremos

(0)	P(0)	(I)
(1)	P(0) ⇒ P(1)	(II)
(2)	P(1) ⇒ P(2)	(II)
(3)	P(2) ⇒ P(3)	(II)
…		

e, portanto, P(0), P(1), P(2), P(3), …

Exemplo: Suponhamos que queremos demonstrar a fórmula da soma dos elementos de uma progressão geométrica de razão $q \neq 1$,

a_0 , a_1 , a_2 , a_3 , …,
com $a_{i+1} = a_i\, q$.

A fórmula da soma é

$$S_n = f(n) = \frac{(a_n q - a_0)}{(q-1)}$$

Devemos provar inicialmente a *base de indução* (para n=0): $S_0 = f(0)$. A demonstração se resume à verificação de que

$$f(0) = \frac{(a_n q - a_0)}{(q-1)} = a_0$$

Para provar o passo de indução, devemos assumir a *hipótese de indução* $S_i = f(i)$ e provar a *tese de indução* $S_{i+1} = f(i+1)$. Temos $a_{i+1} = a_i\, q$, e $S_{i+1} = S_i + a_{i+1}$.
Portanto,

$$S_{i+1} = S_i + a_{i+1} = f(i) + a_{i+1} = \frac{(a_i q - a_0)}{(q-1)} + a_{i+1} = \frac{(a_{i+1} - a_0)}{(q-1)} + a_{i+1} =$$

$$= \frac{(a_{i+1} - a_0 + a_{i+1} q - a_{i+1})}{(q-1)} = \frac{(a_{i+1} q - a_0)}{(q-1)} = f(i+1).$$

□

Uma forma alternativa de indução, que pode facilitar as demonstrações, em vez de usar apenas o último resultado anterior P(i) para provar P(i+1), usa todos os resultados anteriores, ou seja, P(0), P(1), …, P(i).

Assim, para mostrar P(i) para todos os naturais i, mostramos

I. P(0)

II. $\forall j \leq i\ P(j) \Rightarrow P(i+1)$.

Indução em estrutura. Quando trabalhamos com estruturas que apresentam uma lei de formação bem definida, tais como cadeias, árvores, expressões, podemos usar para a indução um número natural, como, por exemplo, o tamanho da estrutura considerada; muitas vezes, entretanto, isso não é necessário, ou não é conveniente, e podemos fazer a indução de outra forma, baseada na própria estrutura.

Por exemplo, dados um conjunto I e uma propriedade Q, suponha um conjunto X definido como o menor conjunto, no sentido da inclusão, que satisfaz 1 e 2 a seguir:

1. todo $x \in I$ pertence a X, ou seja, $I \subseteq X$.
2. se $x \in X$ e Q(x,y), então $y \in X$.

Ou seja, um elemento x de X ou pertence a um conjunto inicial I, ou satisfaz a propriedade Q, que liga x a um (outro) elemento y de X. Para provarmos uma propriedade P(x) para todos os elementos de X, basta provar:

I. *(base da indução)*
se $x \in I$, P(x)

II. *(passo de indução)*
se $x \in X$, P(x) e Q(x,y), então P(y).

Este esquema pode ser generalizado para permitir várias propriedades Q, e para incluir a possibilidade que essas propriedades relacionem vários elementos de X a um (novo) elemento. Este caso mais geral de indução em estrutura está ilustrado a seguir.

Exemplo: Suponha que definimos uma expressão da seguinte maneira:
1. a, b, c são expressões.
2. Se α e β são expressões, então $\alpha+\beta$ é uma expressão.
3. Se α e β são expressões, então $\alpha*\beta$ é uma expressão.
4. Se α é uma expressão, $[\alpha]$ é uma expressão.

Suponha adicionalmente que queremos provar a propriedade: *"toda expressão tem comprimento (número de símbolos) ímpar"*. Vamos indicar *"α tem comprimento ímpar"* por P(α). Devemos então, para provar *"para qualquer expressão α, P(α)"*, provar:

1. P(a), P(b), P(c).
2. Se P(α) e P(β), então P(α+β).
3. Se P(α) e P(β), então P(α*β).
4. Se P(α), então P([α]).

Neste caso, (1) é a base da indução; (2)..(4) são passos de indução. Naturalmente, para mostrar (1), basta observar que

$|a| = |b| = |c| = 1$; αβ

para mostrar os demais, basta observar que

$|\alpha+\beta| = |\alpha| + |\beta| + 1$,

$|\alpha*\beta| = |\alpha| + |\beta| + 1$, e

$|[\alpha]| = |\alpha| + 2$.

□

(revisão de 27fev97)