DOCUMENTAÇÃO FORMAL

- PROPOSIÇÕES: expressões lógicas não V ou F.

Exemplo:

$1+2=5$

$1=1$

são proposições.

Não são proposições (i) $1=$

(ii) 3

(iii) $x<7$

(iii) é chamado de predicado e denotado por $P(x)$.

- Conectivos lógicos: "$\sim$" "$\wedge$" "$\vee$".

se X, Y forem proposições

X	Y	X ∧ Y	então X ∧ Y é proposição.
V	V	V	
F	V	F	
V	F	F	
F	F	F	

Ou: "V"

X	Y	X ∨ Y
V	V	V
V	F	V
F	V	V
F	F	F

NEGAÇÃO: ¬

X	¬X
F	V
V	F

Exemplo

1) $(2+3=5)$ e $(\neg(1+1=2))$ é F

2) Combinações de proposições

$\neg(X \vee Y) \wedge (X \wedge Y)$

3) $\neg(X \vee Y)$ e $\neg X \wedge \neg Y$ tem a mesma tabela verdade e dizemos que são equivalentes. O mesmo vale para: $\neg(X \wedge Y)$ e $\neg X \vee \neg Y$. (Regras de De Morgan).

Implicações: se x, y são proposições posso formar

$$x \Rightarrow y$$

com a seguinte tabela verdade

x	y	$x \Rightarrow y$
V	V	V
F	F	V
F	V	V
V	F	F

Por exemplo

$0=0 \Rightarrow 0=0$ V

$0=1 \Rightarrow 0=0$ V

$0=1 \Rightarrow 0=1$ V

$0=0 \Rightarrow 0=1$ F

outro operador: $\Leftrightarrow$

x	y	$x \Leftrightarrow y$
V	V	V
F	V	F
V	F	F
F	F	V

Formas "literárias" p/ $x \Rightarrow y$:

- se x então y
- x abonta somente se y abonta
- x é suficiente para y
- y é necessária p/ x

De forma análoga: $x \Leftrightarrow y$:

- x se e somente se y
- x é equivalente a y
- x é necessário e suficiente p/ y

Obs: Dado $x \Rightarrow y$, dizemos que

$y \Rightarrow x$ é sua recíproca, e

$\neg y \Rightarrow \neg x$ é sua contrapositiva.

x	y	$x \Rightarrow y$	$\neg y \Rightarrow \neg x$
V	V	V	V
F	V	V	V
F	F	V	V
V	F	F	F

Note que uma implicação e sua contrapositiva são equival.

Quantificadores:

Considere o predicado

$P(x)$: $x > 3$.

Então $P(4)$ é V e $P(1)$ é F.

Def: Seja $P(x)$ predicado indexado por x num conj. universo U.

Então

Para todo $x \in U$, $P(x)$

é proposição verdadeira somente se $P(x)$ p/ todo $x \in U$.

De forma análoga:

Existe $x \in U$, $P(x)$

é prop. verdadeira somente se existir $x \in U$ t.q. $P(x)$ é V.

AXIOMAS

- Exemplo:

Axioma (do conj. vazio)

Existe um conjunto que não contém elemento algum.

- Exemplo:

Axioma (do fio extra)

Um coreco que ganhar um fio extra de cabelo continuará careca.

TEO: Todos os seres humanos são carecas.

CONJUNTOS E FUNÇÕES

Axioma (conj. vazio) Existe conj. $\emptyset$ t.q. $(\forall x)(x \notin \emptyset)$

Dados dois conjuntos A, B definimos

- $A \subseteq B$, $A \not\subseteq B$, $A \not\subseteq B$
- Dizemos que $A = B$ se $A \subseteq B$ e $B \subseteq A$.

Axioma (da especificação)
Seja A um conjunto e p/ cada $x \in A$ seja $P(x)$ uma proposição. Então existe um único conj. B composto dos elementos x de A t.q. $P(x)$ seja verdade.

Notação: $\{x \in A : P(x)\}$

Abuso de notação: qdo "é claro" quem é o conj. A, escreve-se $\{x : P(x)\}$.

Exemplo: Conjunto dos pares

$\{x \in \mathbb{Z} : x \text{ é divisível por } 2\}$

ou $\{x : x \text{ é divisível por } 2\}$

ou $\{2x : x \in \mathbb{Z}\}$

ou $\{\ldots, -4, -2, 0, 2, 4, \ldots\}$

PARADOXO DE RUSSEL

Questão: Será que existe conj. universo U que contenha todos os conjuntos?

Se tal U existe então, usando o axioma da especificação, podemos formar

$$B = \{x \in U : x \text{ é conjunto e } x \notin x\}.$$

Pergunta: $B \in B$?

i) Se $B \in B$ então $B \notin B$ por definição de B

ii) Se $B \notin B$ então $B \in B$.

Então $B \notin U$. Então não existe conj. universo U que contenha todos os conjs.

Axioma (Regularidade) Se $A \neq \emptyset$ então A tem que possuir algum elemento que não seja conj. ou que seja disjunto de A.

OPERAÇÕES ENTRE CONJUNTOS

União:

Axioma (união) Para qualquer coleção de conjs, existe um conj. que contém todos os elementos que pertencem a pelo menos um dos conjs. da coleção.

Obs: note que o axioma acima não garante unicidade da união, somente existência. Mas a unicidade é fácil de ser obtida.

Com o axioma da especificação, podemos definir

- $A \cap B = \{x \in A : x \in B\}$. Dizemos que A, B são disjuntos se $A \cap B = \emptyset$.

- $A \setminus B = \{x \in A : x \notin B\}$. Outra notação: $A - B$.

(chamado complemento de B em relação a A).
Se for claro quem é A, escreve-se simplesmente $C(B)$.

Podemos generalizar as defs acima p/ uniões e interseções arbitrárias:

Se $I = \mathbb{N}$, por exemplo,

$$\bigcup_{i \in I} A_i = \{x : \text{existe } i \in I \text{ t.q. } x \in A_i\}$$

Notação: $\bigcup_{i \in \mathbb{N}} A_i = \bigcup_{i=1}^{\infty} A_i$.

Regras de De Morgan:

$$\left.\begin{aligned} C\left(\bigcup_{i \in \mathbb{N}} A_i\right) &= \bigcap_{i \in \mathbb{N}} C(A_i) \\ C\left(\bigcap_{i \in \mathbb{N}} A_i\right) &= \bigcup_{i \in \mathbb{N}} C(A_i) \end{aligned}\right\} \text{ exercício.}$$

PARES ORDENADOS

Dados dois elementos a, b queremos formar o par (a, b), e chamamos a e b de primeiro e segundo componentes de (a, b).

Dizemos que $(a, b) = (a', b')$ se $a = a'$ e $b = b'$.

Do ponto de vista axiomático definimos (a, b) por $\{a, \{a, b\}\}$.

Lema: Dados os pares $(a,b) = \{a, \{a,b\}\}$ e $(c,d) = \{c, \{c,d\}\}$ então

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

$\{a, \{a,b\}\} = \{c, \{c,d\}\}$.

Obs: Para demonstrar o lema, temos que mostrar que

$a = c$ e $b = d \iff \{a, \{a,b\}\} = \{c, \{c,d\}\}$

Def: Dados A, B conjs, definimos o chamado produto cartesiano como

$A \times B = \{(a,b) : a \in A \text{ e } b \in B\}$

Obs: A extensão p/ n-úplas ordenadas e produtos cartesianos com n conjuntos é "natural".

Exemplo: $\mathbb{R}^n = \overbrace{\mathbb{R} \times \mathbb{R} \times \cdots \times \mathbb{R}}^{n \text{ vezes}} = \{(x_1, x_2, \ldots, x_n) : x_i \in \mathbb{R} \text{ p/ } i = 1, \ldots, n\}$

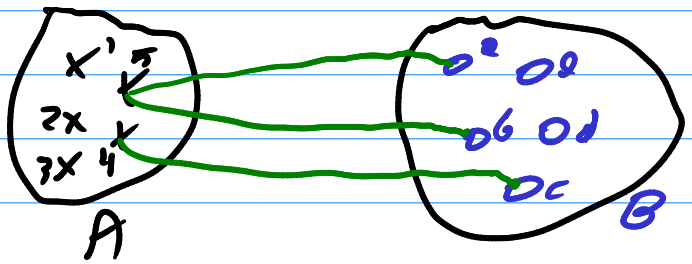
onde $n \in \mathbb{N} = \{1, 2, 3, \ldots\}$.

RELAÇÕES E PARTIÇÕES

Chamamos de relação entre conjs A e B a um subconjunto $R \subseteq A \times B$. Dizemos que $a \in A$ e $b \in B$ são relacionados

(e escrevemos aRb se $(a,b) \in R$.)
(escrevemos $a \not R b$ se $(a,b) \notin R$.)

Diagrama de Venn:



$R \subseteq A \times B = \{(4,c), (5,a), (5,b)\}$.

Exemplo: nos reais, $=$, $>$, $\leq$, etc, definem relações em $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$

"$=$" $\subseteq \mathbb{Z}^2$ onde "$=$" $= \{(i,i) : i \in \mathbb{Z}\}$

$= \{\ldots, (-1,-1), (0,0), (1,1), (2,2) \ldots\}$

Uma relação "em A" é uma relação de $A^2 = A \times A$.

Def: Dizemos que uma relação $\mathcal{R}$ em A é

i) completa se $\forall a, b \in A$ tem-se $a \mathcal{R} b$ ou $b \mathcal{R} a$

Exemplos: $\geq$, $\leq$, ... em $\mathbb{R}$

Não completos: $<$, $>$, $=$

ii) transitiva: $\forall a, b, c$,

$a \mathcal{R} b$ e $b \mathcal{R} c \Rightarrow a \mathcal{R} c$

Exemplos: $\geq$, $>$, $\leq$, $<$ em $\mathbb{R}$

$\subseteq$, $\supseteq$ em conjuntos

Não é transitiva: $\neq$: $3 \neq 5$, $5 \neq 3$ mas $3 \neq 3$ é falso.

iii) Reflexiva: $\forall a \in A$ tem-se $a \mathcal{R} a$

ex: $\geq$, $=$, $\leq$ ... , contra-exemplos: $<$, $>$, $\neq$

iv) simétricos, se $a \mathcal{R} b$ então $b \mathcal{R} a$

ex: $=$

contra-exemplo: $<$, $\leq$, ...

v) anti-simétrica: $a \mathcal{R} b \Rightarrow b \not\mathcal{R} a$

ex: $>$, $<$

não são: $\leq$, $=$, $\geq$, $\neq$

vi) antissimétrica: aRb e $bRa \Rightarrow a = b$

por vacuidade

ex: $>$, $\leq$, $=$, $\subset$, $\supset$

Não tem: relações de equivalência

Dada uma relação reflexiva R em X definimos sua parte assimétrica como sendo $P_X \subseteq X^2$ t.q.

$$P_R = \{(x,y) \in X^2 : xRy \text{ e } yRx\}$$

e $I_R = R \setminus P_R$ como parte simétrica.

Exemplo: ① Em $\mathbb{R}$, a relação $\leq$ tem $P_R = <$ como parte assimétrica e $I_R = '='$ como parte simétrica.

② Em conjuntos (i.e, X é uma coleção de conjuntos) a relação $\subseteq$ tem $\subsetneq$ como parte assimétrica e "$=$" como parte simétrica.

Uma relação de equivalência $\sim$ num conj. A é uma relação reflexiva, ($a \sim a$), simétrica ($a \sim b \Rightarrow b \sim a$), transitiva ($a \sim b, b \sim c \Rightarrow a \sim c$).

Exemplo: seja $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$ e $X = \mathbb{Z} \times \mathbb{Z}^*$ (pense nos racionais). Então

$(a,b) \sim (c,d)$ se $ad = bc$.

$\left(\frac{a}{b} = \frac{c}{d}\right)$

De fato, $\sim$ é

i) Reflexiva: $(a,b) \sim (a,b)$ pois $ab = ab$.

ii) Simétrica: seja $(a,b) \sim (c,d)$. Então $ad = bc$. Logo $bc = ad$ e portanto $(c,d) \sim (a,b)$

iii) Transitiva: seja $(a,b) \sim (c,d)$ e $(c,d) \sim (m,n)$

Então $ad = bc$ e $cn = dm$. Quero mostrar $an = bm$. Note que $and = bcn = bdm \Rightarrow an = bm$ (pois $d \neq 0$).

Seja agora um conjunto $X \neq \emptyset$ e $\mathcal{P}(X)$ o conjunto das partes de X, i.e., a coleção de todos os subconjuntos de X:

$$\mathcal{P}(X) = \{A : A \subseteq X\}$$

(outra notação: 2^X)

Exemplo: $X = \{1,2,3\}$, então

$$\mathcal{P}(X) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, X\}$$

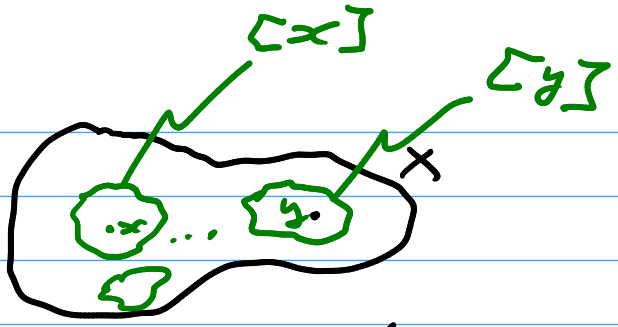
Exemplo: $X = \emptyset \Rightarrow \mathcal{P}(\emptyset) = \{\emptyset\}$

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

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

Dada uma relação de equivalência em X, podemos definir uma <u>classe de equivalência</u> para um elemento $x \in X$:

$$[x] \in \mathcal{P}(X); \quad [x] = \{\hat{x} \in X : \hat{x} \sim x\} \subseteq X.$$

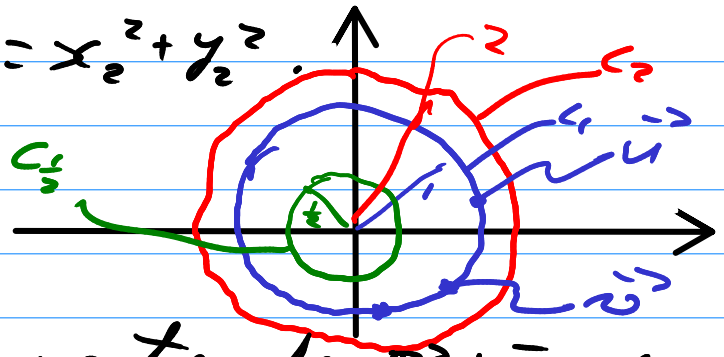


Seja agora a coleção

$$X/\sim \;=\; \{[x] : x \in X\} \subseteq \mathcal{P}(X).$$

Exemplo: no $\mathbb{R}^2$, seja $(x_1,y_1) \sim (x_2,y_2)$ se

$\|(x_1,y_1)\|^2 = x_1^2 + y_1^2 = x_2^2 + y_2^2$.



Dois pontos do $\mathbb{R}^2$ são equivalentes ($\sim$) se têm a mesma norma.

Dado $\vec{u} \in \mathbb{R}^2$:

$$[\vec{u}] = \{\vec{v} \in \mathbb{R}^2 : \|\vec{u}\| = \|\vec{v}\|\} = C_r ; r = \|u\|$$

$$\mathbb{R}^2/\sim \;= \{C_r : r \in [0,\infty)\}$$

Temos então o seguinte resultado:

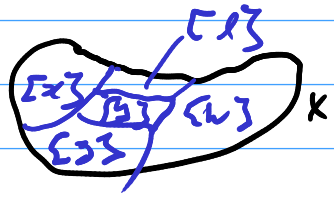
Teo: Seja $\sim$ Relação de equivalência em $X \neq \emptyset$. Então

i) Para todo $x \in X$, temos $x \in [x]$.

ii) " " $x, y \in X$, $x \sim y \Leftrightarrow [x] = [y]$.

iii) " " $x, y \in X$, $x \not\sim y \Leftrightarrow [x] \cap [y] = \emptyset$.

Note que as classes de equivalência "particionam" X:



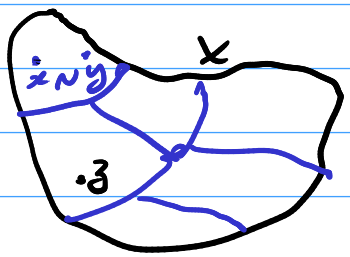
Def: Uma partição de $X \neq \emptyset$ é uma coleção $\tau \subseteq \mathcal{P}(X)$ t.q.

i) $\emptyset \notin \tau$
ii) Para todos $A, B \in \tau$ temos $A = B$ ou $A \cap B = \emptyset$
iii) Para todo $x \in X$ existe $A \in \tau$ t.q. $x \in A$.

Corolário (teo. acima) Seja $\sim$ uma relação de equivalência em $X \neq \emptyset$. Então

$X/\sim$ é uma partição de X.

Suponha agora que τ seja partição de X:



Note que τ "induz" uma relação de equivalência:

$x \sim y$ se existir $A \in \tau$ t.q. $x, y \in A$.

Teo: Seja $X \neq \emptyset$ e τ partição de X. Seja a relação de equivalência $\sim$ dada por

$$x \sim y \iff \exists A \in \tau \text{ t.q. } x \in A \text{ e } y \in A.$$

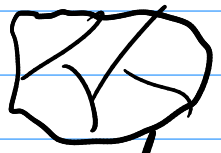
Além disto, as classes de equivalência são exatamente os elementos de τ, i.e.

$$X/\sim \; = \tau.$$

Dem:

Partição τ

"induz" $\Rightarrow$ Relação de equiv. $\Rightarrow$ "induz"



Partição τ

Dem: Vamos mostrar que $\sim$ é relação de equivalência:

i) $\sim$ é reflexiva, i.e., $x \sim x$ pois

$x \in X \Rightarrow x \in A$ p/ algum $A \in \mathcal{T}$.

$\Rightarrow$ "$x \in A$ e $x \in A$" $\Rightarrow x \sim x$.

ii) $\sim$ é simétrica, i.e., $x \sim y \Rightarrow y \sim x$:

De fato, $x \sim y \Rightarrow$ existe $A \in \mathcal{T}$ t.q. $x \in A$ e $y \in A$.

Logo $y \in A$ e $x \in A$ e então $y \sim x$.

iii) $\sim$ é transitiva, i.e., $x \sim y$ e $y \sim z \Rightarrow x \sim z$:

De fato $x \sim y \Rightarrow$ existe $A \in \mathcal{T}$ t.q. $x \in A$ e $y \in A$.

$y \sim z \Rightarrow$ existe $B \in \mathcal{T}$ t.q. $y \in B$ e $z \in B$.

Mas então $y \in A \cap B \Rightarrow A \cap B \neq \emptyset \Rightarrow A = B$

(pois $\mathcal{T}$ é partição). $\Rightarrow x \in A$ e $z \in A$

$\Rightarrow x \sim z$.

Portanto $\sim$ é relação de equivalência.

Quero mostrar agora que $X/_\sim = \tau$.

i) $X/_\sim \subseteq \tau$: Seja $[a] \in X/_\sim$. Então $a \in X$ e portanto existe $A \in \tau$ t.q. $a \in A$.

Mas então $[a] = A$ pois

(*) $x \in [a] \iff x \sim a \iff x \in A$.

Logo $[a] \overset{A}{\in} \tau$.

ii) $\tau \subseteq X/_\sim$: Seja $A \in \tau$. Então $A \neq \emptyset$, e portanto existe $a \in A$. Por (*), $[a] = A$.

$\Rightarrow A = [a] \in X/_\sim$.

RELAÇÕES DE ORDEM

Definimos uma pré-ordem $\lesssim$ em X como sendo uma relação transitiva e reflexiva (i.e. $x \lesssim x$, $\forall x \in X$).

Dizemos que uma preordem $\lesssim$ é uma ordenação parcial de X se $\forall x, y, z \in X$:

i) reflexiva: $x \lesssim x \quad \forall x \in X$
ii) antissimétrica: $x \lesssim y$ e $y \lesssim x \Rightarrow x = y$.

iii) transitividade: $x \lesssim y$ e $y \lesssim z \Rightarrow x \lesssim z$.

Uma ordenação parcial é linear (ou completa) se for total

i.e. $x \lesssim y$ ou $y \lesssim x$. $\forall x, y \in X$.

Denotamos a parte antissimétrica de $\lesssim$ por $<$ e a parte simétrica por $\sim$.

Exemplo: No $\mathbb{R}^2$ temos a "preferência" lexicográfica (ou alfabética) onde

$(x_1, x_2) \succcurlyeq (y_1, y_2)$ se

$$\begin{cases} x_1 > y_1 \text{ ou} \\ x_1 = y_1 \text{ e } x_2 \geq y_2 \end{cases}$$

Esta ordenação é total.

De fato, ela é:

i) Reflexiva? $(x_1, x_2) \succcurlyeq (x_1, x_2)$ pois $x_1 = x_1$ e $x_2 \succcurlyeq x_2$.

ii) transitiva: suponha $(x_1, x_2) \succcurlyeq (y_1, y_2)$ e $(y_1, y_2) \succcurlyeq (z_1, z_2)$. Quero mostrar $(x_1, x_2) \succcurlyeq (z_1, z_2)$. Considere os casos

a) se $x_1 > y_1$ então $x_1 > z_1$ (pois $y_1 \geq z_1$).

$\Rightarrow (x_1, x_2) \succcurlyeq (z_1, z_2)$

b) se $x_1 = y_1$ e $y_1 = z_1$ então $x_1 = z_1$. Como

$x_2 \succcurlyeq y_2$ e $y_2 \succcurlyeq z_2 \Rightarrow x_2 \succcurlyeq z_2 \Rightarrow$

$(x_1, x_2) \succcurlyeq (z_1, z_2)$

c) se $x_1 = y_1$ e $y_1 \succ z_1$, então $x_1 \succ z_1$

$\Rightarrow (x_1, x_2) \succ (z_1, z_2)$.

iii) antissimetria: suponha

$(x_1, x_2) \overset{*}{\succcurlyeq} (y_1, y_2)$ e $(y_1, y_2) \overset{**}{\succcurlyeq} (x_1, x_2)$.

Note que eu não posso ter $x_1 \succ y_1$ por (**).

nem $y_1 \succ x_1$ (por *). Então $x_1 = y_1$.

Do mesma forma não pode ter

$x_2 \succ y_2$ (por **) nem $y_2 \succ x_2$ (por *)

Então $x_2 = y_2$.

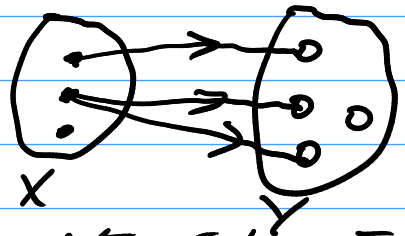
Em $\mathbb{R}^n$: $(x_1, \ldots, x_n) \succcurlyeq (y_1, \ldots, y_n)$ se

i) $x_1 \succ y_1$

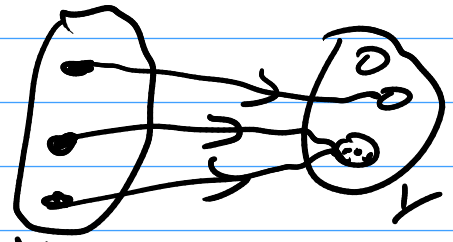
ii) $x_1 = y_1, \ldots, x_{k-1} = y_{k-1}$ e $x_k \succ y_k$ para algum $k \in \{2, \ldots, n\}$

iii) $(x_1, \ldots, x_n) = (y_1, \ldots, y_n)$.

FUNÇÕES



Não é função



é função

Ambos são relações, mas só o segundo é função.

Def: Uma função f é uma relação entre A e B (i.e. $f \in A \times B$) t.q.

i) $\forall a \in A$ existe $b \in B$ t.q. $(a, b) \in f$

ii) se $(a, b) \in f$ e $(a, b') \in f$ então $b = b'$.

Notação: representaremos f por $f: A \to B$.

se $(a, b) \in f$, escrevemos $f(a) = b$.

O conjunto de todas as funções de A em B pode ser denotado por B^A.

Chamamos A de domínio de f e B de contradomínio de f.

Se $E \subseteq A$ chamamos de imagem de E (por f) ao conj:

$$f(E) \overset{DEF}{=} \{f(a) \in B : a \in E\}$$

↑ notação

Similarmente definimos o conj. imagem inversa de um conj. H como

$$f^{-1}(H) = \{a \in A : f(a) \in H\}$$

↑ notação

Exemplo: Seja $f : (0,4) \to \mathbb{R}$, $x \mapsto \sqrt{x}$

Então $(0,4)$ é o domínio, $\mathbb{R}$ é contra-domínio, e

$f^{-1}((1,2)) = (1,4)$; $f^{-1}(\{2\}) = \{4\}$.

$f^{-1}((-3,-2)) = \emptyset$; $f^{-1}(\emptyset) = \emptyset$

$f((0,4)) = (0,2)$ (imagem).

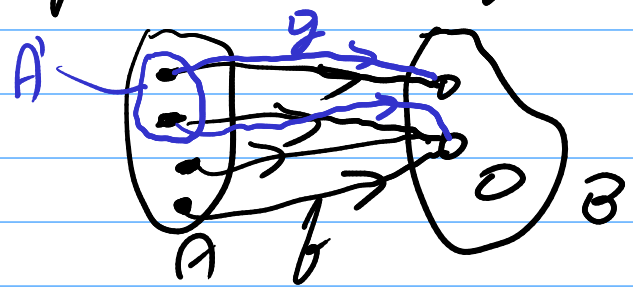
Def: Se $f: A \to B$ é tal que $f(A) = B$ chamamos f de sobrejetiva.

Dizemos que f é injetiva se $a, a' \in A$ e $f(a) = f(a')$ então $a = a'$. (outra forma $a \neq a' \Rightarrow f(a) \neq f(a')$)

Se f é injetiva e sobre, dizemos que f é bijeção.

Def: Dado $f: A \to B$ e $A' \subseteq A$ definimos a função restrição $g = f|_{A'}$ t.q.

$g: A' \to B$ e $g(a') = f(a')$ p/ todo $a' \in A'$



$g = f|_{A'}$ e f é extensão de g.

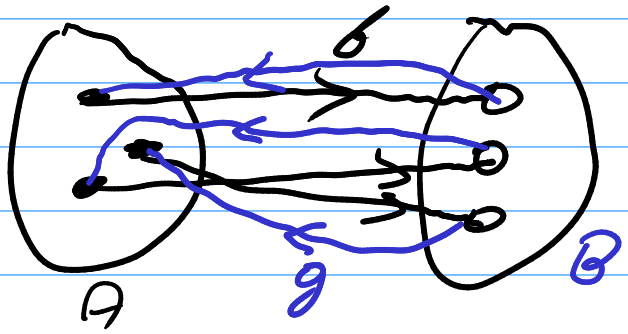
Dizemos que $h: A'' \to B$ é extensão de f se $A'' \supseteq A$ e $f = h|_A$.

Def: Dadas duas funções $f: A \to B$ e $g: B \to C$ definimos a função composta $gof: A \to C$ por $gof(a) = g(f(a))$, p/ todo $a \in A$.

Dizemos que $g: B \to A$ é inversa de $f: A \to B$ se

$$g(f(a)) = a \quad \text{p/ todo } a \in A$$

$$f(g(b)) = b \quad \text{p/ todo } b \in B.$$

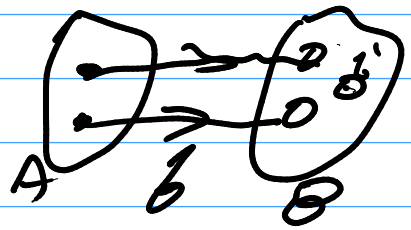


Pode a inversa existir denotamos por f^{-1}.

Sobre a existência do inverso:

Seja $f: A \to B$.

i) Se f não for sobre: então existe

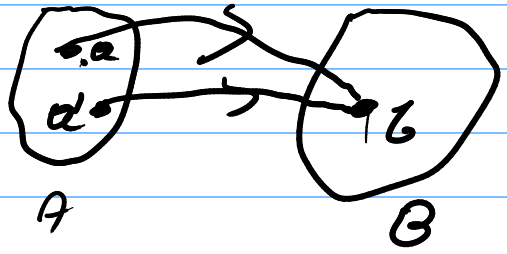


$b' \in B$ t.q. $b' \neq f(a)$ p/ todo $a \in A$.

Então p/ todo $g: B \to A$ eu nunca terei $f(g(b')) = b'$. Então f é não invertível.

ii) Se $f: A \to B$ não for injetiva:

Sejam $a \neq a' \in A$ e $b = f(a) = f(a')$



P/ qualquer $g: B \to A$ nunca teremos

$$a' = g(f(a')) = g(b)$$
$$\text{e} \quad \| \quad$$
$$a = g(f(a)) = g(b)$$

mas $a \neq a'$.

$\Rightarrow f$ não é invertível.

Temos que f invertível $\Rightarrow$ f bijetora

Na verdade a "volta" da implicação vale.

Lema: Sejam A, B conjuntos e $f: A \to B$.

Então f é invertível se e só se

f for bijeção.

Dem: ($\Rightarrow$) suponha f invertível e seja $g = f^{-1}$

P/ mostrar f sobre, seja $b \in B$. Seja

$a = g(b)$. Então $f(a) = f(g(b)) = b$.

$\Rightarrow$ f sobre.

P/ mostrar f injetiva, sejam $a, a' \in A$

t.q. $f(a) = f(a')$. Então

$a = g(f(a)) = g(f(a')) = a' \Rightarrow a = a'$.

$\Rightarrow$ f injetiva.

($\Leftarrow$) Suponha agora f bijeção. Tenho que construir $g: B \to A$ t.q. $g = f^{-1}$. Seja $b \in B$. Então existe $a \in A$ t.q. $f(a) = b$ (pois f é sobre). Note que este elemento a é único (pois f é injetiva). Seja $g(b) = a$. Então $g: B \to A$ está bem-definida. Note que $f(g(b)) = f(a) = b$ e

$$g(f(a)) = g(b) = a$$

por construção. Logo $g = f^{-1}$. ∎

Dizemos que duas funções são iguais se seus domínios e contra-domínios são iguais, e elas assumem os mesmos valores.

O gráfico de uma função $f: A \to B$ é o conjunto

$$Gr(f) = \{(x, f(x)) : x \in A\} \subseteq A \times B$$

Dados X, Y conjs, definimos a função projeção $\pi_X : X \times Y \to X$ t.q.

$\pi_X((x,y)) = x$. Análogo p/ $\pi_Y : X \times Y \to Y$.

Note que π_X é sobre.

Números Naturais, Conjuntos finitos e infinitos.

P/ definir $\mathbb{N}$ usamos os axiomas de Peano, que garantem a existência de um conjunto $\mathbb{N}$ e de uma função $s: \mathbb{N} \to \mathbb{N}$ t.q.

(P1) $s: \mathbb{N} \to \mathbb{N}$ é injetiva.

(P2) $s(\mathbb{N}) \setminus \mathbb{N}$ contém somente um elemento, que denotamos por 1.

(P3) Se $X \subseteq \mathbb{N}$ é t.q. $1 \in X$ e $(x \in X \Rightarrow s(x) \in X)$ então $X = \mathbb{N}$.

Notação: $\mathbb{N} = \{1, 2, 3, \ldots\}$.

Demonstração por indução: Coreada em (P3).

Exemplos de demonstrações por indução:

Demo: Para todo $n \in \mathbb{N}$ vale $s(n) \neq n$.

Dem: Seja $X = \{n \in \mathbb{N} : s(n) \neq n\}$.

Quero mostrar que $X = \mathbb{N}$.

Sei que $1 \neq s(n)$ (por P2) p/ todo $n \in \mathbb{N}$.

$\Rightarrow 1 \in X$.

Seja $n \in X$. Então $s(n) \neq n$. Como s é inj. (por P1), $s(s(n)) \neq s(n) \Rightarrow s(n) \in X$.

Por P3 temos $X = \mathbb{N}$. ∎

AULA 22/09/20

CONJUNTOS INFINITOS

Def: X é infinito se não for finito.

Exemplo: $\mathbb{N}$ é infinito. Para mostrar tenho que mostrar que não existe bijeção entre I_k e $\mathbb{N}$, $\forall k \in \mathbb{N}$.

Por contradição suponha $\varphi: I_k \to \mathbb{N}$ bijeção com $k \in \mathbb{N}$. Seja

$$p = \varphi(1) + \varphi(2) + \dots + \varphi(k) \in \mathbb{N}$$

Então $p \in \mathbb{N}$ mas $p > \varphi(j)$, $p/$ todo $j = 1, \dots, k$.

$\Rightarrow \varphi$ não é sobrejetivo.

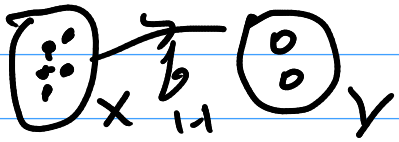
Exemplo: Seja $P = \{2j ; j \in \mathbb{N}\}$. Então

$\psi: P \to \mathbb{N}$ é bijeção.
$j \mapsto j/2$

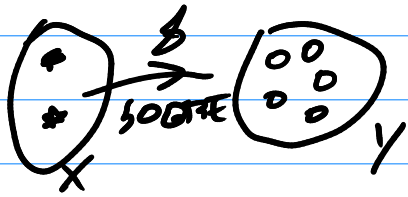
Logo não existe bijeção entre P e I_m, $m \in \mathbb{N}$. (se $\varphi: P \to I_m$ bijeção, então $I_m \xrightarrow{\varphi^{-1}} P \xrightarrow{\psi} \mathbb{N}$ seria bijeção entre I_m e $\mathbb{N}$.

Note que por resultados anteriores:

i) X infinito e $f: X \to Y$ injetiva implica em Y infinito.



ii) Y infinito e $f: X \to Y$ sobre implica em X infinito



iii) Se $X \not\subset Y$ e $f: X \to Y$ bijeção então X e Y não infinitos.

Exemplos: $\mathbb{Q}$ e $\mathbb{Z}$ não infinitos

pois $f: \mathbb{N} \to \mathbb{Q}$, $i \mapsto i$ e $g: \mathbb{N} \to \mathbb{Z}$, $i \mapsto i$

não injetivas e $\mathbb{N}$ é infinito

$\Rightarrow \mathbb{Q}$ e $\mathbb{Z}$ não infinitos.

CONJUNTOS ENUMERÁVEIS

Def: Dizemos que um conj. B é enumerável se B for finito ou se houver bijeção $\varphi: \mathbb{N} \to B$.

Exemplos: ① $P = \{2, 4, 6, \ldots\}$ é enumerável pois $\varphi: \mathbb{N} \to P$, $i \mapsto 2i$ é bijeção.

② $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, 3, \ldots\}$

$= \{0, 1, -1, 2, -2, 3, \ldots\}$ é enumerável

pois $\varphi: \mathbb{N} \to \mathbb{Z}$, $i \mapsto (-1)^i \left\lfloor \frac{i}{2} \right\rfloor$ é bijeção,

onde $\lfloor x \rfloor$ é "a parte inteira" de x.

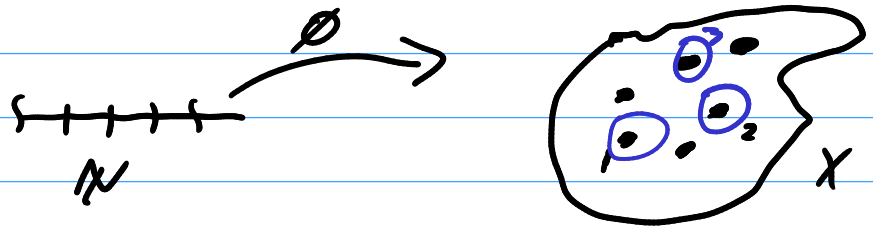
$\varphi(1) = (-1)^1 \left\lfloor \frac{1}{2} \right\rfloor = 0$

$\varphi(2) = (-1)^2 \left\lfloor \frac{2}{2} \right\rfloor = 1$

$\varphi(3) = (-1)^3 \left\lfloor \frac{3}{2} \right\rfloor = -1 \cdot 1 = -1$

Teo: Todo conjunto infinito contém um subconjunto infinito enumerável.

Dem:



Seja $\phi: \mathbb{N} \to X$ t.q. (por indução):

i) escolho $x_1 \in X$ e defino $\phi(1) = x_1$.

ii) suponha que $\phi(1) = x_1, \ldots, \phi(n) = x_n$ estejam definidos com $\phi(i) \neq \phi(j)$ p/ $i \neq j$.

iii) como X é infinito, escolha

$x_{n+1} \in X \setminus \{x_1, \ldots, x_n\}$ e defina $\phi(n+1) = x_{n+1}$

Logo $\phi(i) \neq \phi(j)$ $\forall i, j \in \mathbb{N}$ e então ϕ é injetiva. Logo $\phi: \mathbb{N} \to \phi(\mathbb{N})$ é sobrejetiva e portanto $\phi(\mathbb{N}) \subseteq X$ é infinito enumerável.

☞

Corolário: Um conjunto X é infinito se e somente se existe entre X e um subconjunto próprio de X.

Dem: ($\Leftarrow$) Se X for finito, não existe tal bijeção.

($\Rightarrow$) Seja X infinito. Pelo Teo. anterior existe $A \subseteq X$ infinito enumerável.

Seja $A = \{a_1, a_2, a_3, \ldots\}$.

Seja

$Y = X \setminus \{a_1, a_3, a_5, \ldots\}$

Então $Y \subsetneq X$. Seja $\varphi : X \to Y$ dada por

$$\varphi(x) = \begin{cases} x & \text{se } x \in X \setminus A = X \setminus \{a_1, a_2, a_3, a_4 \ldots\} \\ a_{2i} & \text{se } x = a_i. \end{cases}$$

Note que $\varphi(x) \notin \{a_1, a_3, a_5, \ldots\}$. Então φ é bijeção. $\square$

Teo: Seja $X \subseteq \mathbb{N}$. Então X é enumerável.

Dem: Se $X \subseteq \mathbb{N}$ for finito, então é enumerável. Suponha agora X infinito.

Seja $f: \mathbb{N} \to X$ dado por

i) $f(1)$ é o menor elemento de X.

ii) dado $n \in \mathbb{N}$ suponha $f(1), \dots, f(n)$ dados t.q. $f(1) < f(2) < \dots < f(n)$ e $f(n) < X$

p/ todo $x \in B_n = X \setminus \{f(1), \dots, f(n)\}$.

iii) $f(n+1)$ menor elemento de B_n.

Então f é bijeção. De fato, com $i < n$ então $f(n) < f(n)$.
P/ mostrar sobrejetividade, suponha $x \in X \setminus f(\mathbb{N})$.

Então $x \in B_n$ p/ todo $n \in \mathbb{N}$. Logo $x > f(n)$ $\forall n \in \mathbb{N}$. $\Rightarrow f(\mathbb{N})$ é limitada.

Isto é contradição com $f(\mathbb{N})$ ser infinito. ∎

Corolário:

i) Se $X \subseteq Y$ e Y for enumerável então X é enumerável

ii) Se $f: X \to Y$ injetivo e Y enumerável então X é enumerável.

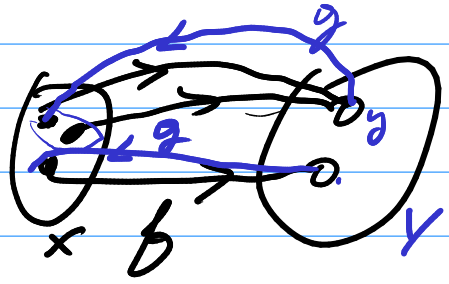
Dem: exercício.

Cor: Seja $X \subseteq \mathbb{N}$ infinito. Então existe bijeção crescente $f: \mathbb{N} \to X$.

Cor: Seja X enumerável e $f: X \to Y$ sobrejetivo. Então Y é enumerável.

Dem: Como $f: X \to Y$ é sobre então existe $g: Y \to X$ injetivo t. q. $f(g(y)) = y$.

$\Rightarrow Y$ é enumerável. □



$g(y) \in \{x \in X : f(x) = y\}$

$= f^{-1}(\{y\}) \neq \emptyset$

Produtos Cartesianos e Uniões:

Teo: Sejam A, B enumeráveis. Então $A \times B$ é enumerável.

Dem: Sejam $\varphi: A \to \mathbb{N}$ e $\psi: B \to \mathbb{N}$ injetivas (mostre!). Então

$$g: A \times B \to \mathbb{N} \times \mathbb{N}, \quad (a,b) \longmapsto (\varphi(a), \psi(b))$$ é injetiva.

Se $\mathbb{N} \times \mathbb{N}$ for enumerável então $A \times B$ será enumerável. Para ver que $\mathbb{N} \times \mathbb{N}$ é enumerável considere

$$f: \mathbb{N} \times \mathbb{N} \to \mathbb{N}, \quad (m,n) \longmapsto 2^m 3^n.$$ Então f é injetiva (mostre). Logo $\mathbb{N}$ é enumerável e f é injetiva. Então $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$ é enumerável. □

24/09/20

Uma contagem de $A \times B$:

Suponha $A = \{a_1, a_2, a_3, \ldots\}$

$B = \{b_1, b_2, b_3, \ldots\}$. Escrevo

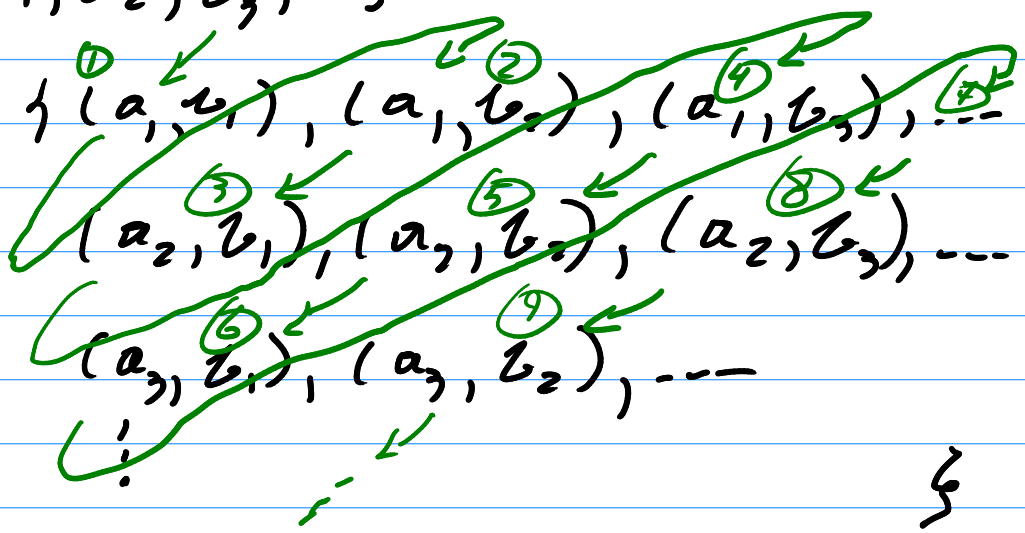
$A \times B = \{(a_1, b_1), (a_1, b_2), (a_1, b_3), \ldots$

$(a_2, b_1), (a_2, b_2), (a_2, b_3), \ldots$

$(a_3, b_1), (a_3, b_2), \ldots$

$\vdots$

$\}$



Esta é a "contagem diagonal".

Obs: Por indução, se $A_1, \ldots, A_k, A_{k+1}, \ldots$ forem enumeráveis então

$A_1 \times A_2 \times \ldots \times A_k = (A_1 \times A_2 \times \ldots \times A_{k-1}) \times A_k$

é enumerável (prova por indução).

Entretanto $A_1 \times A_2 \times \ldots \times A_k \times \ldots$ não será enumerável se $|A_j| \geq 2$ para infinitos "j's".

Corolário: $\mathbb{Q}$ é enumerável.

Dem: Como $\mathbb{Z}$ e $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$ são enumeráveis, então $\mathbb{Z} \times \mathbb{Z}^*$ é enumerável. Mas

$$\phi : \mathbb{Z} \times \mathbb{Z}^* \to \mathbb{Q}, \quad (p, q) \mapsto p/q$$

é sobrejetiva.

Então $\mathbb{Q}$ é enumerável. □

Corolário: Para $i \in \mathbb{N}$ seja X_i enumerável. Então $\bigcup_{i \in \mathbb{N}} X_i$ é enumerável.

Dem: Seja $X = \bigcup_{i \in \mathbb{N}} X_i$, e p/ cada $i \in \mathbb{N}$ seja $f_i : \mathbb{N} \to X_i$ sobrejetiva.

Seja $f : \mathbb{N} \times \mathbb{N} \to X$, $(m, n) \mapsto f_m(n)$.

Então f é sobrejetiva:

$$X = X_1 \cup X_2 \cup \ldots = \underbrace{\{f_1(1), f_1(2), f_1(3), f_1(4), \ldots\}}_{= X_1} \cup \underbrace{\{f_2(1), f_2(2), f_2(3), \ldots\}}_{= X_2} \cup \{f_3(1), \ldots\} \cup \ldots$$

$$= \underbrace{\{f(1,1), f(1,2), f(1,3), \ldots\}}_{= X_1} \cup \underbrace{\{f(2,1), f(2,2), \ldots\}}_{= X_2} \cup \ldots$$

Como f é sobrejetiva, e $\mathbb{N}^2$ é enumerável, então X é enumerável. ∎

Conjuntos não enumeráveis

Teo: Sejam $X_1, X_2, \ldots$ enumeráveis, com $|X_i| \geq 2$ p/ todo $i \in \mathbb{N}$. Então $\prod_{i \in \mathbb{N}} X_i = X_1 \times X_2 \times X_3 \times \ldots$ não é enumerável.

Dem: É fácil ver que $\prod_{i\in\mathbb{N}} X_i$ é infinito

Por contradição suponha que existe

$\phi: \mathbb{N} \to \prod_{i\in\mathbb{N}} X_i$ bijeção. Então podemos escrever

$$\phi(1) = (x_{1,1}, x_{1,2}, x_{1,3}, x_{1,4}, \dots) \in \prod_{i=1}^{\infty} X_i$$

$$\phi(2) = (x_{2,1}, x_{2,2}, x_{2,3}, \dots) \in \prod X_i$$

$$\phi(3) = (x_{3,1} \in X_1, x_{3,2} \in X_2, x_{3,3} \in X_3, \dots) \in \prod X_i$$

$$\vdots$$

Então p/ todo $\bar{x} \in \prod_{i\in\mathbb{N}} X_i$ temos $\bar{x} = \phi(j)$ p/ algum $j \in \mathbb{N}$.

Seja $\bar{x} = (\bar{x}_1 \in X_1, \bar{x}_2 \in X_2, \dots)$ t.q.

$\bar{x}_1 \neq x_{1,1}$, $\bar{x}_2 \neq x_{2,2}$, $\bar{x}_3 \neq x_{3,3}$, ...

Então $\bar{x} \neq \phi(i)$ $\forall i \in \mathbb{N}$. Contradição com

ϕ ser sobrejetiva.

$\square$

Cor: $\mathbb{R}$ não é enumerável.

Dem: $[0,1] \sim \prod_{i=1}^{\infty} A_i$ ← não enumerável, $A_i = \{0,1,\dots,9\}$

$\frac{1}{3} = 0,333\dots \sim (3,3,3,\dots)$

$0,79880\dots \sim (7,9,8,8,0,\dots)$

$\mathbb{R}$

CORPOS: Um corpo $\{K, +, \cdot\}$ é formado por um conjunto K e as operações $+$ e $\cdot$ sobre K t.q.:

1) A adição

i) $(x+y)+z = x+(y+z)$

ii) $x+y = y+x$

iii) $\exists\, 0 \in K$ t.q. $x+0=x \quad \forall x \in K$

iv) $\forall x \in K \ \exists -x \in K$ t.q. $x+(-x)=0$

2) A multiplicação

i) $x \cdot (y \cdot z) = (x \cdot y) \cdot z$

ii) $x \cdot y = y \cdot x$

iii) $\exists\, 1 \in K$ t.q $x \cdot 1 = x$

iv) $x \neq 0 \ \exists\, x^{-1} \in K$ t.q. $x \cdot x^{-1} = 1$

3) $x \cdot (y+z) = x \cdot y + x \cdot z$

Note que $(-1).(-1) = 1$ pois

$(-1).(-1) + (-1).1 = (-1)(-1+1) = -1 . 0 = 0$

$\Rightarrow (-1).(-1) = -(-1).1 = -(-1) = 1$

Exemplos

1) $\{\mathbb{Q}, +, .\}$ com

$$\frac{p}{q} + \frac{p'}{q'} = \frac{pq' + p'q}{qq'} \; ; \; \frac{p}{q} \cdot \frac{p'}{q'} = \frac{p'p}{qq'}.$$

2) $\mathbb{Z}_2 = \{0, 1\}$ com as operações

$0+0=0$; $0+1=1$; $1+0=1$; $1+1=0$.

$0.0 = 0.1 = 1.0 = 0$; $1.1 = 1$

Em geral $\mathbb{Z}_p$ é corpo p/ p primo, com as operações "usuais" e identificando

$m = n$ se m/p e n/p tem o mesmo resto:

$\mathbb{Z}_3 = \{0, 1, 2\}$

$1+2 = 3 \equiv 0$; $2.2 = 4 \equiv 1$ ...

Obs: Seja K corpo, se $x, y \in K$ t.q. $x^2 = y^2$ então

$$(x+y).(x-y) = x^2 - y^2 = 0$$

$\Rightarrow x+y=0$ ou $x-y=0 \Rightarrow x=-y$ ou $x=y$.

CORPOS ORDENADOS

Def: K é corpo ordenado se existir conjunto $P \subset K$ t.q.

i) $x, y \in P \Rightarrow x+y \in P$ e $x.y \in P$

ii) Se $x \in K$ então uma e apenas uma situação ocorre:

$$x \in P \;;\; x=0 \;;\; -x \in P. \quad (\Leftrightarrow x \in -P)$$

Chama os elementos de P de positivos e os elementos de

$$-P \overset{\text{Def}}{=} \{-x : x \in P\}$$

de negativos. Note que

$K = P \cup -P \cup \{0\}$, onde $P \cap -P = \emptyset$; $P \cap \{0\} = \emptyset$;

$-P \cap \{0\} = \emptyset$.

PROPRIEDADES

Lema: Seja K corpo com ordem P. Então

i) $a \in K,\ a \neq 0 \Rightarrow a^2 \in P$

ii) $1 \in P$

iii) Não existe $a \in K$ t.q. $a^2 = -1$

Prova: (i) Como $a \neq 0$ então $a \in P$ ou $a \in -P$.

Se $a \in P \Rightarrow a^2 = \underset{\in P}{a} \cdot \underset{\in P}{a} \in P$

Se $-a \in P \Rightarrow a^2 = \underset{\in P}{(-a)} \cdot \underset{\in P}{(-a)} \in P$

(ii) $1 = 1 \cdot 1 = 1^2 \in P$ por (i)

(iii) Por (ii) $-1 \in -P$ e $a^2 \in P \cup \{0\}$ p/ todo $a \in K$

$\Rightarrow a^2 \neq -1$ p/ todo $a \in K$. □

Cor: $\mathbb{C}$ não é ordenado

Dem: $i^2 = -1$ não acontece num corpo. □

Exemplo: Em $\mathbb{Q}$ temos $P = \{\frac{p}{q} : p \cdot q \in \mathbb{N}\}$

Exemplo: $\mathbb{Z}_2$ não é ordenado pois

$1 + 1 = 2 \equiv 0$ mas $1 \in P$ e $0 \notin P$.

$\mathbb{Z}_3$ também não é ordenado pois

$1 + 2 = 3 \equiv 0 \Rightarrow 2 \in -P$. Entretanto

$\overset{\in -P}{2} + \overset{\in -P}{2} = 4 \equiv \overset{\in P}{1}$.

29/09/20

Exemplo: Em $\mathbb{Q}(t)$ temos

$P = \{ \frac{p(t)}{q(t)} : $ o coeficiente de ordem maior

alta de $p(t)q(t)$ seja positivo$\}$

Então $\underbrace{\frac{-t^2+5t+3}{-t}} \in P$ pois

$$(-t^2+5t+3)(-t) = (+)t^3 + \dots$$

"Imitando" $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ em corpos:

Seja $1' \in K$ o elemento neutro da multiplicação

Seja $f: \mathbb{N} \to K$ t.q.

i) $f(1) = 1'$

ii) suponho $f(n)$ definido, p/ algum $n \in \mathbb{N}$

iii) $f(n+1) = f(n) + 1'$.

Por construção $f(m) + f(n) = f(m+n)$

Como $f(n) \in P$ então

$m < n \Rightarrow f(m) < f(n)$. (mostre)

$\Rightarrow f$ é injetiva.

Então $f: \mathbb{N} \to \underbrace{f(\mathbb{N})}_{\mathbb{N}'}$ é bijeção.

Na prática, identificamos $\mathbb{N}$ e $\mathbb{N}'$

e escrevemos $\mathbb{N} \subseteq K$.

Definimos então $\mathbb{Z} \subseteq k$ por

$$\mathbb{Z} = \{-n \in k : n \in \mathbb{N}\} \cup \{0\} \cup \mathbb{N}$$

Definimos $\mathbb{Q} \subseteq k$:

$$\mathbb{Q} = \{p \cdot q^{-1} : p \in \mathbb{Z}, q \in \mathbb{Z}^*\}$$

Def: Se k for corpo ordenado com ordem P, dizemos que $x > y$ se $x - y \in P$.

Segue-se da definição que

$$x > 0 \iff x \in P, \quad x < 0 \iff x \in -P$$

pois $x = x \cdot 0$. Note ainda que

i) transitividade: $x < y$ e $y < z \Rightarrow x < z$

de fato $(y-x) \in P$ e $(z-y) \in P \Rightarrow$

$$\underbrace{(y-x) + (z-y)}_{\in P} = z - x \Rightarrow z - x \in P \Rightarrow z > x$$

ii) tricotomia: há uma e somente uma possibilidade dentre

$$x > y \; ; \; x = y \; ; \; x < y$$

dados $x, y \in k$.

iii) monotonicidade da adição:

se $x < y$ então $x + z < y + z$ p/ todo $z \in K$:

De fato, se $y - x \in P$, então

$y - x = (y + z) - (x + z) \in P$

$\Rightarrow y + z > x + z$

iv) monotonicidade da adição:

se $x < y$ então $x \cdot z < y \cdot z$ p/ todo $z \in P$.

De fato, se $y - x \in P$ então p/ $z \in P$:

$(y - x) \cdot z \in P \Rightarrow yz - xz \in P \Rightarrow yz > xz$.

Obs: Note que num corpo ordenado

$0 < 1 < 1 + 1 < 1 + 1 + 1 < \ldots$

Portanto todo corpo ordenado é infinito.

Intervalos e módulos

Seja $\{K, +, \cdot\}$ ordenado. Então

$[a, b] = \{x \in K : a \leq x \text{ e } x \leq b\}$

$(a, b] = \{x \in K : a < x \text{ e } x \leq b\}$

$(a, +\infty) = \{x \in K : x > a\}$

$\vdots$

Por exemplo: em $\mathbb{Q}(t)$

$t^2 + t \in [3t, +\infty)$ pois $t^2 + t \geq 3t$

(já que $t^2 + t - 3t = t^2 - 2t \in P$)

Da mesma forma qquer polinômio

do forma $a_n t^n + a_{n-1} t^{n-1} + \cdots + a_1 t + a_0 \in [3t, \infty)$

desde que $\begin{cases} a_n > 0 & \text{se } n \geq 2 \text{ ou} \\ a_n \geq 3 & \text{se } n = 1 \end{cases}$

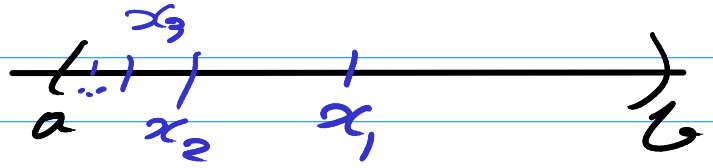
Note que $-t^2 \notin [3t, +\infty)$ pois

$-t^2 < 3t$ já que $3t - (-t^2) = t^2 + 3t \in P$.

Demo: Todo intervalo não degenerado é infinito.

Dem: SPG Seja $a < b$ e (a, b) intervalo.

Idéia:



Seja $x_1 = \frac{a+b}{2}$. Então $x_1 > a$ e $x_1 < b$.

pois $x_1 = \frac{a+b}{2} > \frac{a+a}{2} = a$ ...

Então $x_1 \in (a, b)$. De forma indutiva, dado $x_n \in (a, b)$ defino $x_{n+1} = \frac{(a+x_n)}{2}$

Então $x_{n+1} < x_n < x_{n-1} < \dots < b \Rightarrow x_{n+1} \in (a, b)$.

Logo, o conjunto infinito

$\{x_1, x_2, \dots\} \subseteq (a, b)$. ∎

Em $(K,+,\cdot)$ ordenado, definimos

$$|x| = \begin{cases} x & \text{se } x \in P \\ 0 & \text{se } x = 0 \\ -x & \text{se } x \in -P \end{cases}$$

Exemplo: $|t^2-3| = t^2-3$

$$\left|\frac{-t^5+4}{t^2+1}\right| = \frac{t^5-4}{t^2+1}.$$

em $Q(t)$

COTAS, SUPREMOS, ÍNFIMOS

Def: Seja $A \subseteq \mathbb{K}$. Dizemos que $c^* \in \mathbb{K}$ é cota superior de A se $c^* \geq a$ p/ todo $a \in A$.

Note que c^* é cota superior então c^*+1 também o é.

Exemplos: (i) $\mathbb{N}$ tem 0 1 como cota inferior

(ii) $\emptyset$: qualquer elemento de $\mathbb{K}$ é cota superior e inferior de $\emptyset$.

iii) Em $\mathbb{Q}(t)$, temos que $t \in \mathbb{Q}(t)$ é cota superior de $\mathbb{N}$ pois

$n < t$ p/ todo $n \in \mathbb{N}$.

$\Rightarrow \mathbb{N}$ é conjunto limitado em $\mathbb{Q}(t)$.

Dizemos que K é arquimediano se $\mathbb{N} \subseteq K$ for ilimitado.

Teo: Seja K corpo ordenado. São equivalentes:

i) $\mathbb{N}$ é ilimitado superiormente

ii) Para todo $a, b \in K$, $a > 0$ existe $n \in \mathbb{N}$ t.q. $na > b$.

iii) Para todo $a > 0$ existe $n \in \mathbb{N}$ t.q. $0 < \frac{1}{n} < a$.

Dem: (i) $\Rightarrow$ (ii) sejam $a, b \in K$, $a > 0$. Então b/a não é cota superior de $\mathbb{N}$. $\Rightarrow$ existe $n > b/a$.

(ii) $\Rightarrow$ (iii) Tome $b = 1$ em (ii) $\Rightarrow$ existe $n \in \mathbb{N}$ t.q. $na > 1$.

(iii) $\Rightarrow$ (i) Seja $b \in K$. Por (iii) existe $n \in \mathbb{N}$ t.q. $\frac{1}{n} < \frac{1}{b}$. Logo $n > b$. $\Rightarrow b$ não é cota superior de $\mathbb{N}$. ∎

01/10/20.

SUPREMO E ÍNFIMO

Def: Seja $A \neq \emptyset$, $A \subseteq \mathbb{R}$ limitado superiormente. Chamamos de supremo de A à menor de suas cotas superiores. Outra notação é $\sup A$.

Então $x^* = \sup A$ se

i) $a \leq x^*$ p/ todo $a \in A$

ii) se $v \in \mathbb{R}$ é cota superior de A então $v \geq x^*$.

Exemplos

i) Se $X \subseteq \mathbb{R}$ possuir elemento máximo, este será o $\sup X$.

ii) Seja $a < b$ e $Y = [a, b)$. Então $b \geq y$ p/ todo $y \in Y \Rightarrow b$ é cota superior.

Quero mostrar que $b = \sup Y$.
Seja $\bar{y} \in [a, b)$. Então $\bar{y}$ não é cota superior. De fato, seja $y' = \frac{\bar{y}+b}{2}$. Então

$y' > \bar{y} > a$ e $y' < b$. Logo $y' \in [a, b)$ com $y' > \bar{y} \Rightarrow \bar{y}$ não é cota superior.
$\Rightarrow b = \sup Y$. ∎

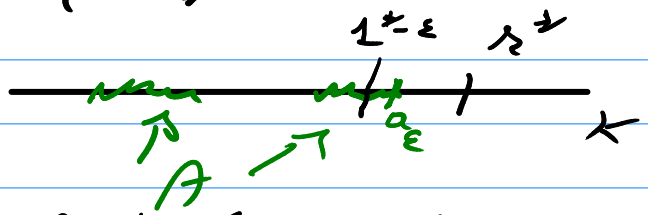
iii) $X = [a, b]$ então $a = \inf X$ e

$b = \sup X$, pelos mesmos argumentos do (ii).

Note de (ii) e (iii) que o sup X pode pertencer ou não à X.

Lema: Seja $A \subseteq \mathbb{R}$, $A \neq \emptyset$ e s^* cota superior de A. Então $s^* = \sup A$ se e somente se p/ todo $\varepsilon > 0$ existe $a_\varepsilon \in A$ t.q. $a_\varepsilon > a - \varepsilon$.

Intuição:



Dem: (=>) Seja $s^* = \sup A$. Dado $\varepsilon > 0$, $s^* - \varepsilon$ não é cota superior pois $s^* - \varepsilon < s^*$. Logo existe $a_\varepsilon \in A$ t.q. $a_\varepsilon > s^* - \varepsilon$.

(<=) Seja $c^* < s^*$. Quero mostrar que c^* não é cota superior. Seja $\varepsilon = s^* - c^* > 0$. Por hipótese existe $a_\varepsilon > s^* - \varepsilon$, $a_\varepsilon \in A$.

$\Rightarrow a_\varepsilon > s^* - (s^* - c^*) = c^* \Rightarrow c^*$ não é cota superior $\Rightarrow s^*$ é a menor das cotas superiores $\Rightarrow s^* = \sup A$.

Introdução:

Teorema (Pitágoras) Não existe $x \in \mathbb{Q}$ t.q. $x^2 = 2$.

Dem: Por contradição, suponha que $\left(\frac{p}{q}\right)^2 = 2$ onde $p, q \in \mathbb{Z}$, $q \in \mathbb{Z}^*$ e p, q sejam primos entre si.

Como $p^2 = 2q^2$, então p é par.

Escreva então $p = 2\bar{p}$, e

$4\bar{p}^2 = 2q^2 \Rightarrow q^2 = 2\bar{p}^2 \Rightarrow q$ é par.

Contradição com p, q serem primos entre si. □

Afirmativas (Elon Vol I)

Sejam

$$X = \{x \in \mathbb{Q} : x \geq 0 \text{ e } x^2 < 2\}$$

$$Y = \{x \in \mathbb{Q} : x \geq 0 \text{ e } x^2 > 2\}$$

Então

i) X não possui elemento máximo

ii) Y não possui elemento mínimo

iii) Todo elemento de Y é cota superior de X

Lema: Não existe $\sup X$ em $\mathbb{Q}$.

Dem: Suponha por contradição

$a = \sup X \in \mathbb{Q}$. Então $a > 0$ pois $1 \in X$.
Além disso $a \notin X$ pois caso contrário seria elemento máximo de X. $\Rightarrow a^2 \geq 2$.

Suponha $a^2 > 2$. $\Rightarrow a \in Y \Rightarrow$ Existe $\varepsilon > 0$ t.q $a - \varepsilon \in Y$ pois a não é elemento mínimo de Y. mas $a - \varepsilon$ é cota superior de X (por (iii) acima), contradição com $a = \sup X$. Logo $a \notin Y$. $\Rightarrow a^2 \leq 2$.
$\Rightarrow a^2 \geq 2$ e $a^2 \leq 2 \Rightarrow a^2 = 2$ contradição.

□

Números reais:

Dizemos que um corpo é completo se para todo conjunto limitado superiormente existir supremo.

Obs: $\mathbb{Q}$ não é completo

Axioma (Reais) Existe um corpo ordenado completo $\mathbb{R}$.

PROPRIEDADES DE $\mathbb{R}$

a) $\mathbb{R}$ não é limitado
b) $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$
c) $\mathbb{R}$ é arquimediano, i.e. vale o resultado a seguir

Lema: Para todo $x \in \mathbb{R}$ existe $n \in \mathbb{N}$ com $n > x$.

Dem:
Por contradição seja $x \in \mathbb{R}$ t.q. $x \geq n$ p/ todo $n \in \mathbb{N}$. Então x é cota superior de $\mathbb{N}$. $\Rightarrow \mathbb{N}$ é limitado superiormente, mas $\mathbb{N} \subseteq \mathbb{R}$ e $\mathbb{R}$ completo

$\Rightarrow$ existe $s = \sup \mathbb{N} \in \mathbb{R}$.

Logo s^*-1 não é cota superior de $\mathbb{N}$

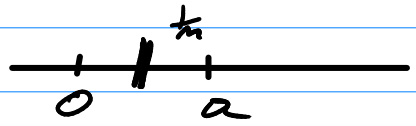
$\Rightarrow$ existe $n \in \mathbb{N}$ t.q. $n > s^*-1$.

$\Rightarrow n+1 > s^*$, $n+1 \in \mathbb{N}$

contradição com $s^* = \sup \mathbb{N}$. ∎

Lembrando:

- P/ todo $a \in \mathbb{R}$ existe $n \in \mathbb{N}$ t.q. $0 < \frac{1}{n} < a$



INTERVALOS ENCAIXANTES

Exemplo: Seja $I_n = [0, \frac{1}{n}]$. então

$\bigcap_{n \in \mathbb{N}} I_n = \{0\}$. De fato

- $\{0\} \subseteq \bigcap_{n \in \mathbb{N}} I_n$ pois $0 \in I_n$ P/ todo $n \in \mathbb{N}$

$\Rightarrow 0 \in \bigcap_{n \in \mathbb{N}} I_n \Rightarrow \{0\} \subseteq \bigcap_{n \in \mathbb{N}} I_n$

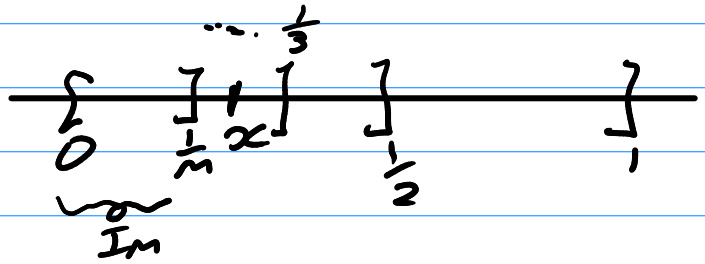
- Para ver que $\bigcap_{n \in \mathbb{N}} I_n \subseteq \{0\}$, vou mostrar que se $x \in \bigcap_{n \in \mathbb{N}} I_n$ então $x = 0$.

Se $x < 0$ então $x \notin I_1 \Rightarrow x \notin \bigcap_{n \in \mathbb{N}} I_n$ prop. arquim.

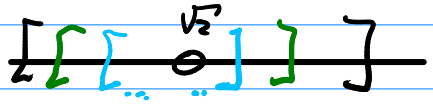
Se $x > 0$ então existe $n \in \mathbb{N}$ t.q. $\frac{1}{n} < x$

$\Rightarrow x \notin I_n = [0, \frac{1}{n}] \Rightarrow x \notin \bigcap_{n \in \mathbb{N}} I_n$

$\Rightarrow \bigcap_{n \in \mathbb{N}} I_n \subseteq \{0\}$



Em $\mathbb{Q}$: $I_n = [\sqrt{2} - \frac{1}{n}, \sqrt{2} + \frac{1}{n}] \cap \mathbb{Q}$



$\Rightarrow \bigcap_{n \in \mathbb{N}} I_n = \emptyset$.