Notas do Tales

Tales da Silva Amaral

26 de maio de 2024

Sumário

1 Introdução

O objetivo do seguinte "livro"é ser um "dicionário"de demonstrações e definições, onde são colocados o maior número possível de detalhes. Quem nunca leu um livro e se deparou com demonstrações incompletas, repletas de "é fácil ver que"e falas similares. Meu objetivo é reduzir isso, visto que PDF não tem limite de páginas.

2 Lógica

2.1 Cálculo Proposicional

Axioma 1. *Para todas fórmulas P, Q, R, são considerados teoremas as fórmulas:*

1. $P \implies (Q \implies P)$

Regra de Inferência 1. *É tomada como regra de inferência o modus ponens: Se P e $P \implies Q$ são teoremas, então Q é um teorema. Portanto*

$$\{P, P \implies Q\} \vdash Q.$$

2.2 Organizar

Tomando como termos primitivos: o alfabeto $\{a, b, c, \cdots\}$; e ($\wedge$); ou ($\vee$); negação ($\neg$); existe ($\exists$); igual ($=$).

Definição 2.1 ($\equiv$, Equivalência)**.** $p \equiv q$ significa p é equivalente a q.

Definição 2.2 ($\implies$, Implicação)**.** $p \implies q \equiv \neg p \vee q$. Diz-se "p implica q", "Se p, então q"etc.

Definição 2.3 ($\iff$)**.** $p \iff q \equiv (p \implies q) \wedge (q \implies p)$. Diz-se "p se, e somente se, q".

Definição 2.4 (c, Contradição)**.** A letra c é reservada para a "contradição".

Definição 2.5 (t, Tautologia)**.** A letra t é reservada para a "contradição".

Definição 2.6 ($\nexists x P(x)$, Não existe)**.** $\neg(\exists x P(x)) \equiv \nexists P(x)$. Diz-se "Não existe x tal que $P(x)$".

Definição 2.7 ($\forall$, Para todo)**.** $\forall x P(x) \equiv \neg \exists x (\neg P(x))$. Diz-se "Para todo x, temos $P(x)$".

Definição 2.8 ($\exists! x P(x)$, Existe um único)**.** $\exists! x P(x) \equiv \exists x P(x) \wedge \forall y (P(y) \implies y = x)$. Diz-se "Existe um único x tal que $P(x)$".

Axioma 2. *Para quaisquer $p, q,$, temos:*

1. $p \equiv p$
2. *Se* $p \equiv q$*, então* $q \equiv p$.
3. *Se* $p \equiv q$ *e* $q \equiv r$*, então* $p \equiv r$.
4. *Se* $p \equiv q$ *, então* $\not p \equiv \not q$.
5. $\neg(\neg p) \equiv p$.

Axioma 3. *Para quaisquer $p, q,$, temos:*

1. $p \vee q \equiv q \vee p$.
2. $(p \vee q) \vee r \equiv p \vee (q \vee r)$.
3. $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$.
4. $p \vee p \equiv p$
5. $\neg(p \vee q) \equiv (\neg p \wedge \neg q)$

3 Teoria de conjuntos

3.1 Axioma da Extensão

Conceito Primitivo 1 (Conjunto)**.** *Temos como conceito primitivo a noção de Conjunto, Coleção. Ou seja, não tentarei definir tal conceito.*

Conceito Primitivo 2 (Elementos de um Conjunto)**.** *A noção de elementos ou membros de um conjunto também será tomada como conceito primitivo.*

Definição 3.1 (Pertinência)**.** Se x é um elemento de A, ou x pertence a A, escrevemos $x \in A$.

Definição 3.2 (Não Pertinência)**.** Se x não pertence a A, escrevemos $x \notin A$. Ou seja:

$$x \notin A \iff \neg(x \in A)$$

Axioma 4 (Axioma da Extensão)**.** *Dois conjuntos são iguais se, e somente se, possuem os mesmos elementos. Ou seja:*

$$A = B \iff \forall x (x \in A \iff x \in B)$$

Definição 3.3 (Diferente)**.** Dois conjuntos A e B são diferentes se não são iguais e escrevemos $A \neq B$. Ou seja:

$$A \neq B \iff \neg(A = B)$$

Proposição 3.1. *Dois conjuntos A e B são diferentes se existe $x \in A$ com $x \notin B$ ou $x \in B$ com $x \notin A$. Ou seja:*

$$A \neq B \iff \exists x((x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A))$$

Demonstração.

$$\begin{aligned}
A \neq B &\iff \neg(A = B) \\
&\iff \neg(\forall x(x \in A \iff x \in B)) \\
&\iff \exists x(\neg(x \in A \iff x \in B)) \\
&\iff \exists x(\neg((x \in A \implies x \in B) \wedge (x \in B \implies x \in A))) \\
&\iff \exists x(\neg((x \notin A \vee x \in B) \wedge (x \notin B \vee x \in A))) \\
&\iff \exists x((x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A))
\end{aligned}$$

□

Definição 3.4 (Subconjunto)**.** Dizemos que A é um subconjunto de B se todo elemento de A for um elemento de B e escrevemos $A \subset B$. Ou seja:

$$A \subset B \iff \forall x(x \in A \implies x \in B)$$

Proposição 3.2.

$$A \subset A$$

Demonstração. Temos $p \implies p$ uma tautologia para toda fórmula p, logo $x \in A \implies x \in A$ é uma tautologia. Portanto $A \subset A \iff \forall x(x \in A \implies x \in A)$ é uma tautologia. □

Proposição 3.3.

$$A \subset B \wedge B \subset C \implies A \subset C$$

$$A \subset B \wedge B \subset C \implies A \subset C \iff \neg(A \subset B \wedge B \subset C) \vee A \subset C$$

Definição 3.5 (Subconjunto Próprio)**.** Se A e B são conjuntos tais que $A \subset B$ e $A \neq B$, então A é chamado de subconjunto próprio.

3.2 Organizar Ainda

Proposição 3.4.

$$(A - B) \cup B = A \cup B$$

Demonstração.

$$\begin{aligned}
x \in (A - B) \cup B &\iff \\
(x \in A \wedge x \notin B) \vee x \in B &\iff \\
(x \in A \vee x \in B) \wedge (x \notin B \vee x \in B) &\iff \\
(x \in A \vee x \in B) \wedge t &\iff \\
x \in A \vee x \in B &\iff \\
x \in A \cup B &\iff
\end{aligned}$$

□

Proposição 3.5.

$$A \times (B \cup C) = (A \times B) \cup (A \times C)$$

Demonstração.

$$\begin{aligned}
(x, y) \in A \times (B \cup C) &\iff x \in A \wedge (y \in B \cup C) \\
&\iff x \in A \wedge (y \in B \vee y \in C) \\
&\iff (x \in A \wedge y \in B) \vee (x \in A \wedge y \in C) \\
&\iff ((x, y) \in A \times B) \vee ((x, y) \in A \times C) \\
&\iff (x, y) \in (A \times B) \cup (A \times C)
\end{aligned}$$

□

Proposição 3.6. *Se $A \subset B$ e $B - A = \emptyset$, então $A = B$.*

Demonstração. O caso $A = B = \emptyset$ é trivial. Supondo $B \neq \emptyset$. Supondo $A \subset B$ e $B - A = \emptyset$. Como já temos $A \subset B$, basta provar $B \subset A$.

Supondo $x \in B$ e $x \notin A$. Como $B - A = \emptyset$, temos $x \in \emptyset$ (contradição). Logo se $x \in B$, devemos ter $x \in A$. Logo $B \subset A$. Logo $A = B$. □

Lema 1. *Existe uma bijeção entre* X *e* $X \times \{a\}$ *.*

Demonstração. Seja a função $g : X \to X \times \{a\}$, dada por $g(x) = (x, a)$. Temos $g(p) = g(q) \iff (p, a) = (q, a) \iff p = q$, logo g é injetiva. Dado $(x, a) \in X \times \{a\}$, temos $x \in X$ e $a \in \{a\}$. Logo existe $x \in X$ tal que $g(x) = (x, a)$. Portanto g é sobrejetiva. Como g é injetiva e sobrejetiva, temos g bijetiva. □

Lema 2. *Existe uma bijeção entre* X *e* $\mathcal{F}(\{a\}, X)$ *.*

Demonstração. Seja a função $g : X \to \mathcal{F}(\{a\}, X)$, dada por $g(x) = f_x$, onde $f_x : \{a\} \to X, f_x(a) = x$. Temos $g(p) = g(q) \iff f_p(a) = f_q(a) \iff p = q$, logo g é injetiva. Dado $f \in \mathcal{F}(\{a\}, X)$, seja $p = f(a)$. Temos $g(p) = f_p = f$. Logo existe $p \in X$ tal que $g(p) = f$. Portanto g é sobrejetiva. Como g é injetiva e sobrejetiva, temos g bijetiva. □

Lema 3. *Existe uma bijeção entre* $\mathcal{F}(X, Y) \times \mathcal{F}(\{a\}, Y)$ *e* $\mathcal{F}(X \cup \{a\}, Y)$*, com* $a \notin X$*.*

Demonstração. Seja $\phi : \mathcal{F}(X \cup \{a\}, Y) \to \mathcal{F}(X, Y) \times \mathcal{F}(\{a\}, Y)$. Que associa $f : X \cup \{a\} \to Y$ a (g, h), onde $g : X \to Y, g(x) = f(x)$ e $h : \{a\} \to Y, h(a) = f(a)$. Se $\phi(f_1) = \phi(f_2)$, temos $(g_1, h_1) = (g_2, h_2)$, que implica $g_1 = g_2$ e $h_1 = h_2$. Logo $f_1 = f_2$. Logo ϕ é injetiva.

Seja $(g_0, h_0) \in \mathcal{F}(X, Y) \times \mathcal{F}(\{a\}, Y)$. Seja $f : X \cup \{a\}$, $f(x) = \begin{cases} g_0(x), & x \in X \\ h_0(a), & x = a \end{cases}$.
Temos $\phi(f) = (g_0, h_0)$, logo ϕ é sobrejetiva.

Como ϕ é injetiva e sobrejetiva, temos ϕ bijetiva. □

Proposição 3.7. *Se* $f : X \to Y$ *e* $g : Y \to Z$ *são bijeções, então* $(g \circ f) : X \to Z$ *é uma bijeção.*

Demonstração. Temos $g(f(a)) = g(f(b)) \implies f(a) = f(b) \implies a = b$. Logo $g \circ f$ é injetiva.

Tomando $z \in Z$. Como g é sobrejetiva, existe $y \in Y$ tal que $g(y) = z$. Como f é sobrejetiva, existe $x \in X$ tal que $f(x) = y$. Logo existe $x \in X$ tal que $g(f(x)) = g(y) = z$. Logo $g \circ f$ é sobrejetiva. □

Proposição 3.8. *Seja* $f : X \to Y$ *uma função sobrejetiva.* f *admite inversa à direita.*

Demonstração. Para todo $y \in Y$, temos $f^{-1}(y) \neq \emptyset$, logo existe $x_y \in f^{-1}(y)$ tal que $f(x_y) = y$. Defina $g : Y \to X$, que associa $y \to x_y$ (axioma da escolha). Logo temos $f(g(y)) = f(x_y) = y$. □

Proposição 3.9. *Seja* $f : X \to Y$ *uma função injetiva.* f *admite inversa à esquerda.*

Demonstração. Queremos definir $g : Y \to X$. Dado $y \in f(X)$, existe um único $x \in X$ tal que $f(x) = y$. Defina $g(y) = x$. Para $y \in Y - f(x)$, colocamos $g(y) = x_0$, onde $x_0 \in X$ qualquer. Para todo $x \in X$, temos $f(x) \in f(X)$, logo $g \circ f(x) = x$. □

Proposição 3.10. *Se $f : X \to Y$ é uma função então $f' : X \to f(X)$, definida como $f'(x) = f(x)$, é uma sobrejeção.*

Demonstração. Seja $y \in f(X)$. Por definição de $f(X)$, existe $x \in X$ tal que $f(x) = f'(x) = y$. Logo f' é sobrejetiva. $\square$

Proposição 3.11. *Se $f : X \to Y$ é uma injeção então $f' : X \to f(X)$, definida como $f'(x) = f(x)$, é uma bijeção.*

Demonstração. Pela proposição anterior, f' é sobrejetiva. Dados $a, b \in X$ com $f'(a) = f(a) = f(b) = f'(b)$. Como f é injetiva, temos $a = b$, logo f' é injetiva. $\square$

Proposição 3.12. *Se $f : A \cup B \to C$ é uma bijeção, então $f' : A \to C - f(B)$, $a \mapsto f(a)$ é uma bijeção.*

Demonstração. Se $a, b \in A \subset A \cup B$, temos $f'(a) = f'(b) \iff f(a) = f(b) \implies a = b$ (f é injetiva). Logo f' é injetiva.

Tomando $y \in C - f(B)$. Como f é sobrejetiva, existe $x \in A \cup B$ tal que $f(x) = y$. Se $x \in B$, teríamos $f(x) \in f(B)$, logo $f(x) \notin C - f(b)$ (contradição). Logo devemos ter $x \in A$. Logo existe $x \in A$ tal que $f'(x) = f(x) = y$. Logo f' é sobrejetiva. $\square$

Proposição 3.13. *Se $f : A \to B$ é uma bijeção e $C \subset B$, então $f' : f^{-1}(C) \to C$, $x \mapsto f(x)$ é uma bijeção.*

Demonstração. Se $a, b \in f^{-1}(C) \subset A$, temos $f'(a) = f'(b) \iff f(a) = f(b) \implies a = b$ (f é injetiva). Logo f' é injetiva.

Tomando $y \in C$. Como f é sobrejetiva, existe $x \in A$ tal que $f(x) = y \in C$. Como $f(x) \in C$, temos $x \in f^{-1}(C)$. Logo existe $x \in f^{-1}(X)$ tal que $f(x) = f'(x) = y$. Logo f' é sobrejetiva. $\square$

Proposição 3.14. *Seja $f : A \to B$ uma função e $X \subset Y \subset B$. Temos $f^{-1}(X) \subset f^{-1}(Y)$.*

Demonstração. Se $x \in f^{-1}(X)$, temos $f(x) \in X$. Como $X \subset Y$, temos $f(x) \in Y$. Portanto $x \in f^{-1}(Y)$. Como $x \in f^{-1}(X) \implies x \in f^{-1}(Y)$, temos $f^{-1}(X) \subset f^{-1}(Y)$. $\square$

Proposição 3.15. *Seja $f : A \to B$ uma função bijetiva e $X, Y \subset B$. Temos $f^{-1}(X) = f^{-1}(Y) \iff X = Y$.*

Demonstração. Se $X = Y$ é direto. Supondo $f^{-1}(X) = f^{-1}(Y)$. Se $x \in X$, existe $a \in A$ tal que $f(a) = x$. Logo $a \in f^{-1}(X)$. Portanto $a \in f^{-1}(Y)$. Logo $x = f(a) \in Y$. Temos $x = f(a) \in X \implies x = f(a) \in Y$. Para $y \in Y$ é análogo. Logo temos $X = Y$. $\square$

Proposição 3.16. *Se existe a bijeção $f : \{a\} \to X$, então $X = \{b\}$ para algum b.*

Demonstração. Seja $b = f(a) \in X$. Seja $c \in X$. Como f é sobrejetiva, existe $k \in \{a\}$ tal que $f(k) = c$. Temos obrigatoriamente que $k = a$, logo $b = f(a) = c$. Logo $X = \{b\}$. $\square$

Proposição 3.17. *Se $f : A \to B$ e $g : C \to D$ são bijeções, então $h : A \times B \to B \times D$, $h(a, c) = (f(a), g(c))$ é uma bijeção.*

Demonstração. Seja $(b, d) \in B \times D$. Como f e g são sobrejetivas, existem $a \in A$ e $c \in C$ tal que $f(a) = b$ e $g(c) = d$. Logo existe $(a, c) \in A \times C$ tal que $h(a, c) = (f(a), g(c)) = (b, d)$. Logo h é sobrejetiva.

Suponha $h((a, b)) = h((c, d)) \iff (f(a), g(b)) = (f(c), g(d)) \iff f(a) = f(c) \wedge g(b) = g(d)$. Como f e g são injetivas, temos $f(a) = f(c) \implies a = c$ e $g(b) = g(d) \implies b = d$. Logo h é injetiva. Como h é injetiva e sobrejetiva, temos que h é bijetiva.

$\square$

Proposição 3.18. *Se $f : A \to B$ é uma bijeção, então existe uma bijeção entre $\mathcal{F}(A, C)$ e $\mathcal{F}(B, C)$.*

Demonstração. Definimos $\phi : \mathcal{F}(A, C) \to \mathcal{F}(B, C)$, que associa $g : A \to C$ a $h = g \circ f^{-1} : B \to C$. Se $\phi(p) = \phi(q)$, temos $p \circ f^{-1} = q \circ f^{-1}$, logo $(p \circ f^{-1}) \circ f = (q \circ f^{-1}) \circ f \implies p = q$, logo ϕ é injetiva. Seja $p \in \mathcal{F}(B, C)$. Seja $h = p \circ f : A \to C$. Temos $h \in \mathcal{F}(A, C)$ com $\phi(h) = (p \circ f) \circ f^{-1} = p$, logo ϕ é sobrejetiva. $\square$

Proposição 3.19. *Se $f : A \to B$ é uma bijeção, então existe uma bijeção entre $\mathcal{F}(C, A)$ e $\mathcal{F}(C, B)$.*

Demonstração. Definimos $\phi : \mathcal{F}(C, A) \to \mathcal{F}(C, B)$, que associa $g : C \to A$ a $h = f \circ g : C \to B$. Se $\phi(p) = \phi(q)$, temos $f \circ p = f \circ q$, logo $f^{-1} \circ (f \circ p) = f^{-1} \circ (f \circ q) \implies p = q$, logo ϕ é injetiva. Seja $p \in \mathcal{F}(C, B)$. Seja $h = f^{-1} \circ p : C \to A$. Temos $h \in \mathcal{F}(C, A)$ com $\phi(h) = f^{-1} \circ (f \circ p) = p$, logo ϕ é sobrejetiva. $\square$

Proposição 3.20. *Não existe sobrejeção entre X e $\mathcal{P}(X)$.*

Demonstração. Suponha que exista a sobrejeção $f : X \to \mathcal{P}(X)$. Seja $A = \{x \in X \mid x \notin f(x)\}$. Temos $A \in \mathcal{P}(X)$. Como f é sobrejetica, existe $p \in X$ tal que $f(p) = A$. Temos $p \in A$ ou $p \notin A$. Se $p \in A$, obtemos uma contradição, pois $x \in A \iff x \notin f(x)$ e $f(p) = A$. Se $p \notin A$, temos $p \in A$, pela definição de A. Em ambos os casos, obtemos uma contradição. Logo não existe sobrejeção entre X e $\mathcal{P}(X)$. $\square$

Proposição 3.21. *Existe injeção entre X e $\mathcal{P}(X)$.*

Demonstração. Seja $f : X \to \mathcal{P}(X), f(x) = \{x\}$. Temos $f(x) = f(y) \iff \{x\} = \{y\} \iff x = y$. Logo f é injetiva. $\square$

Proposição 3.22. *Existe injeção entre X e $\mathcal{F}(X, Y)$ se Y possui pelo menos 2 elementos.*

Demonstração. Y possuir 2 elementos implica na existência de $y_1, y_2 \in Y$ com $y_1 \neq y_2$. Logo seja $h : X \to \mathcal{F}(X,Y)$, que associa $a \in X$ a $g_a : X \to Y$, dada por

$$g_a(x) = \begin{cases} y_1, & x = a \\ y_2, & x \neq a \end{cases}.$$

Se $h(a) = h(b)$, temos $g_a = g_b$, logo $g_a(x) = g_b(x)$ para todo $x \in X$. Em particular, $g_a(a) = g_b(a)$. Se $a \neq b$, temos $g_a(a) = y_1 = y_2 = g_b(a)$ (contradição). Logo temos $a = b$. Logo h é injetiva.Logo existe injeção entre X e $\mathcal{F}(X,Y)$. $\square$

Proposição 3.23. *Não existe função sobrejetiva entre X e $\mathcal{F}(X,Y)$ se Y possui pelo menos 2 elementos.*

Demonstração. Seja $f : X \to \mathcal{F}(X,Y)$ uma função qualquer.Logo f associa $a \in X$ a uma função $\phi_a : X \to Y$. Para simplificar notação, chamaremos $f(a) = \phi_a$. Seja $g : \mathcal{P}(Y) - \emptyset \to Y$ a função escolha definida em $\mathcal{P}(Y) - \emptyset$. Seja $h : X \to Y$ definida por $h(a) = g(Y - \{\phi_a(a)\})$. Como Y tem pelo menos 2 elementos, temos $Y - \{\phi_a(a)\} \neq \emptyset$ para todo $a \in X$. Pela definição de função escolha, temos $h(a) \in Y - \{\phi_a(a)\}$, logo $h(a) \neq \phi_a(a)$ para todo $a \in X$. Logo temos $h \neq \phi_a$ para todo $a \in X$. Logo $h \notin f(X)$. Logo f não é sobrejetiva. $\square$

3.3 Produto Cartesiano

3.4 Relações

3.4.1 Definições iniciais

Definição 3.6 (Relação)**.** Uma relação R entre os conjuntos A e B é um subconjunto do conjunto $A \times B$.

Definição 3.7 ($a\ R\ b$)**.** Dado uma relação entre A e B, dizemos que $a \in A$ está relacionado a $b \in B$ se $(a,b) \in R$. Escrevemos nesse caso $a\ R\ b$. Portanto:

$$a\ R\ b \iff (a,b) \in R$$

Não utilizarei essa notação, mas algumas fontes usam.

3.4.2 Relações de Equivalência

Definição 3.8 (Relação de equivalência)**.** Uma relação $R \subset A \times A$ é de equivalência, se para todos $a, b, c \in A$:

- (Simetria) $(a,b) \in R \iff (b,a) \in R$.
- (Transitividade) $(a,b) \in R \wedge (b,c) \in R \implies (a,c) \in R$.
- (Reflexividade) $(a,a) \in R$.

Definição 3.9 ($\overset{R}{\sim}$)**.** Quando uma relação R entre A e B for de equivalência, escrevemos $a \overset{R}{\sim} b$ no lugar de $(a,b) \in R$.

Observação 3.1. Quando não houver confusão sobre a relação que estamos tratando, escreverei somente $a \sim b$ no lugar de $a \overset{R}{\sim} b$.

Observação 3.2. Re-escrevendo a definição de relação de equivalência usando a nova notação, temos:

Uma relação $R \subset A \times A$ é de equivalência, se para todos $a, b, c \in A$:

- (Simetria) $a \sim b \iff b \sim a$.
- (Transitividade) $a \sim b \wedge b \sim c \implies a \sim c$.
- (Reflexividade) $a \sim a$.

Definição 3.10 (Classe de equivalência)**.** Dado uma relação de equivalência $R \subset A \times A$, a classe de equivalência de um elemento $a \in A$ (denotada por $\bar{a}$) é dada por

$$\bar{a} = \{x \in A \mid x \sim a\}$$

.

Proposição 3.24. *Dada uma relação de equivalência $R \subset A \times A$ e $a \in A$, temos $a \in \bar{a}$.*

Demonstração. Temos $\bar{a} = \{x \in A \mid x \sim a\}$. Como $a \sim a$ pela reflexividade, temos $a \in \bar{a}$. □

Proposição 3.25. *Dado uma relação $R \subset A \times A$ e $a, b \in A$, as afirmações abaixo são equivalentes:*

(a) $\bar{a} = \bar{b}$

(b) $a \sim b$

(c) $\bar{a} \cap \bar{b} \neq \emptyset$

Demonstração. (a) $\implies$ (b): Supondo $\bar{a} = \bar{b}$. Como $a \in \bar{a}$, temos $a \in \bar{b}$ pela hipótese. Logo $a \sim b$ pela definição de $\bar{b}$.

(b) $\implies$ (c): Supondo $a \sim b$. Logo $a \in \bar{b}$. Como $a \in \bar{a}$ e $a \in \bar{b}$, temos $a \in \bar{a} \cap \bar{b} \implies \bar{a} \cap \bar{b} \neq \emptyset$.

(c) $\implies$ (a): Supondo $\bar{a} \cap \bar{b} \neq \emptyset$, logo existe $c \in \bar{a} \cap \bar{b}$, logo $c \sim a$ e $c \sim b$. Se $y \in \bar{a}$, temos $y \sim a$. Como $c \sim a$, temos $y \sim c$. Como $c \sim b$, temos $y \sim b \implies y \in \bar{b}$. Supondo $y \in \bar{b}$, logo $y \sim b$. De $y \sim b \wedge b \sim c \wedge c \sim a$, temos $y \sim a \implies y \in \bar{a}$. Logo $\bar{a} = \bar{b}$.

□

3.4.3 Relação de Ordem

Definição 3.11 (Ordem Parcial)**.** Uma relação $R \subset A \times A$ é uma ordem parcial, se para todos $a, b, c \in A$:

- (Anti-Simetria) $(a, b) \in R \wedge (b, a) \in R \iff a = b$.
- (Transitividade) $(a, b) \in R \wedge (b, c) \in R \implies (a, c) \in R$.
- (Reflexividade) $(a, a) \in R$.

Definição 3.12 $(\leq)$**.** Se R é uma ordem parcial de A, geralmente escrevemos $a \leq b$ no lugar de $(a, b) \in R$.

Observação 3.3. Re-escrevendo a definição de relação de ordem parcial usando a nova notação, temos:

Uma relação $R \subset A \times A$ é uma ordem parcial, se para todos $a, b, c \in A$:

- (Anti-Simetria) $a \leq b \wedge b \leq a \iff a = b$.
- (Transitividade) $a \leq b \wedge b \leq c \implies a \leq c$.
- (Reflexividade) $a \leq a$.

Definição 3.13 (Comparável)**.** Dado um conjunto A e uma relação de ordem R, dois elementos $a, b \in A$ são comparáveis se $a \leq b$ ou $b \leq a$.

Observação 3.4. Dois elementos de um conjunto parcialmente ordenado podem não ser comparáveis.

Definição 3.14 (Ordem Total)**.** Uma ordem parcial R onde quaisquer dois elementos são comparáveis é uma ordem total. Outros possíveis nomes são ordem linear ou ordem simples.

3.4.4 Funções

Definição 3.15 (Produto Cartesiano de uma Família)**.** Se $\{A_i\}_{i \in I}$ é uma família de conjuntos indexada por I, definimos $\prod_{i \in I} A_i$ como o conjunto de todas as funções $f : I \to \bigcup_{i \in I} A_i$ com $f(i) \in A_i$ para todo $i \in I$.

3.5 Números Naturais

3.5.1 Axiomas de Peano

Temos como conceitos primitivos o conjunto dos naturais, denotado por $\mathbb{N}$, cujos elementos são os números naturais, e uma função $s : \mathbb{N} \to \mathbb{N}$. Para cada $n \in \mathbb{N}$, o número $s(n)$ é o sucessor de n. Temos os axiomas:

Axioma 5. $s : \mathbb{N} \to \mathbb{N}$ *é injetiva.*

Axioma 6. $\mathbb{N} - s(\mathbb{N}) = \{1\}$. *Ou seja, só existe um número natural que não é sucessor de nenhum outro, e ele é denotado por* 1.

Proposição 3.26. *Todo natural diferente de* 1 *possui um antecessor.*

Demonstração. Seja $n \neq 1$ um número natural. Suponha que não exista n_0 natural com $s(n_0) = n$. Logo $n \notin s(\mathbb{N})$. Logo $n \in \mathbb{N} - s(\mathbb{N})$. Mas $\mathbb{N} - s(\mathbb{N}) = \{1\}$. Logo $n = 1$. Contradição. Logo existe $n_0 \in \mathbb{N}$ tal que $s(n_0) = n$. □

Observação 3.5. Observe que a função $s : \mathbb{N} \to \mathbb{N} \setminus \{1\}$ é injetiva por definição e sobrejetiva pela proposicao 3.26, logo é uma bijeção entre um subconjunto dos naturais com os naturais.

Axioma 7 (Princípio de indução)**.** *Se* $X \subset \mathbb{N}$ *é um subconjunto tal que:*

$$\begin{cases} 1 \in X \\ \\ n \in X \implies s(n) \in X \end{cases}$$

Então $\mathbb{N} = X$.

3.5.2 Soma nos Naturais

Definição 3.16 (Soma)**.** Dados $m, n \in \mathbb{N}$, sua soma $m + n$ é definida como:

$$m + n \coloneqq s^n(m).$$

A soma deve obedecer

$$m + 1 = s(m) \tag{1}$$

$$m + s(n) = s(m + n) \tag{2}$$

para todos os m, n naturais.

Observação 3.6. Dedekind prova o "Teorema da Definição por Indução"para garantir que a notação $s^n(m)$ faça sentido.

Proposição 3.27 (Associatividade da Soma)**.** *Para todos* $p, m, n \in \mathbb{N}$*, temos* $m + (n + p) = (m + n) + p$.

Demonstração. Seja $X = \{p \in \mathbb{N} \,|\forall m, n \in \mathbb{N} \,:\, m + (n + p) = (m + n) + p\}$. Da definição de adição, temos pra qualquer m, n que $n+1 = s(n)$, logo $m+(n+1) = m + s(n) = s(m + n) = (m + n) + 1 \implies m + (n + 1) = (m + n) + 1$. Logo $1 \in X$. Se $p \in X$, temos $m + (n + p) = (m + n) + p$. Logo

$$\begin{aligned} m + (n + s(p)) &= m + s(n + p) \\ \\ &= s\left(m + (n + p)\right) \\ \\ &= s\left((m + n) + p\right) \\ \\ &= (m + n) + s(p). \end{aligned}$$

Logo $p \in X \implies s(p) \in X$. Temos que $X = \mathbb{N}$ pelo princípio de indução. Logo a soma é associativa nos naturais. $\square$

Lema 4 (Comutatividade da soma com o 1)**.** *Para todo* $m \in \mathbb{N}$*, temos* $m+1 = 1+m$*.*

Demonstração. Seja $X = \{m \in \mathbb{N} \,|m + 1 = 1 + m\}$. Temos $1 \in X$, pois $1+1 = 1+1$. Supondo $m \in X$, logo $m+1 = 1+m$. Temos

$$\begin{aligned}
1 + s(m) &= s(1+m) \\
&= s(m+1) \\
&= (m+1)+1 \\
&= s(m)+1
\end{aligned}$$

Como $m \in X \implies s(m) \in X$ e $1 \in X$, temos $X = \mathbb{N}$. $\square$

Proposição 3.28 (Comutatividade da soma)**.** *Para todos* $m, n \in \mathbb{N}$*, temos* $m+n = n+m$*.*

Demonstração. Seja $X = \{m \in \mathbb{N} \,|\forall n \in \mathbb{N} : m+n = n+m\}$. Temos $1 \in X$ pelo Lema 4. Supondo $m \in X$, logo $m+n = n+m$ para todo $n \in \mathbb{N}$. Temos

$$\begin{aligned}
n + s(m) &= s(n+m) \\
&= s(m+n) \\
&= (m+n)+1 \\
&= 1+(m+n) \\
&= (1+m)+n \\
&= (m+1)+n \\
&= s(m)+n
\end{aligned}$$

Como $1 \in X$ e $m \in X \implies s(m) \in X$, temos $X = \mathbb{N}$ pelo princípio de indução. $\square$

Proposição 3.29 (Lei do corte)**.** *Para todos* $m, n, p \in \mathbb{N}$*, temos* $m + n = m + p \implies n = p$.

Demonstração. Seja $X = \{m \in \mathbb{N} \,|\forall n \in \mathbb{N}\, \forall p \in \mathbb{N} \,:\, m + n = m + p \implies n = p\}$. Temos $1 \in X$ pois $1+n = 1+p \implies n+1 = p+1 \implies s(n) = s(p) \implies n = p$ pela injetividade de s. Supondo $m \in X$, temos $m+n = m+p \implies n = p$ para todos n, p naturais. Temos

$$
\begin{aligned}
s(m) + n = s(m) + p &\implies \\
n + s(m) = p + s(m) &\implies \\
s(n + m) = s(p + m) &\implies \\
n + m = p + m &\implies \\
m + n = m + p &\implies \\
n = p.&
\end{aligned}
$$

Logo $s(m) + n = s(m) + p \implies n = p$. Como $1 \in X$ e $m \in X \implies s(m) \in X$, temos $X = \mathbb{N}$ pelo princípio de indução. ☐

Lema 5 (Não existem ciclos nos naturais)**.** *Para todos* $m, p \in \mathbb{N}$*, temos* $m \neq m + p$.

Demonstração. Suponha que $m = m + p$ com $m, p \in \mathbb{N}$. Logo $s(m) = s(m + p) \implies m + 1 = (m + p) + 1 \implies m + 1 = m + (p + 1) \implies 1 = p + 1 \implies s(p) = 1$. Como 1 não é sucessor de nenhum natural, temos uma contradição. Logo $m \neq m + p$ para todos naturais m, p. ☐

Lema 6 (Unicidade da Tricotomia)**.** *Dados dois naturais* m *e* n*, apenas uma das 3 possibilidades ocorre:*

$$
\begin{cases}
m = n \\
\exists p \in \mathbb{N} \,:\, m = n + p \\
\exists q \in \mathbb{N} \,:\, n = m + q
\end{cases}
$$

Demonstração. Pelo lema 5, se $m = n$, não podemos ter $m = n + p = m + p$ ou $n = m + q = n + q$ para algum $p, q \in \mathbb{N}$. Se $\exists p \in \mathbb{N} \,:\, m = n + p$, não podemos ter $m = n$ pelo lema 5 e não podemos ter $\exists q \in \mathbb{N} \,:\, n = m + q$, pois teríamos $m = n + p = (m + q) + p = m + (q + p) \implies m = m + (q + p)$, que contradiz o lema 5. ☐

Proposição 3.30 (Tricotomia)**.** *Dados dois naturais m e n, exatamente uma das 3 possibilidades ocorre:*

$$\begin{cases} m = n \\ \\ \exists p \in \mathbb{N} \,:\, m = n + p \\ \\ \exists q \in \mathbb{N} \,:\, n = m + q \end{cases}$$

Demonstração. Seja $X = \{m \in \mathbb{N} | \forall n \in \mathbb{N} \,:\, (m = n) \vee (\exists p \in \mathbb{N} \,:\, m = n + p) \vee (\exists q \in \mathbb{N} \,:\, n = m + q)\}$, ou seja: o conjunto dos números naturais que satisfazem pelo menos uma das condições da tricotomia para todo n.

$1 \in X$, pois dado $n \in \mathbb{N}$, temos $n = 1$ ou $n \neq 1$. Se $n = 1$, temos $m = 1 = n$. Se $n \neq 1$, como $\mathbb{N} - s(\mathbb{N}) = \{1\}$, temos que existe um $n_0 \in \mathbb{N}$ tal que $s(n_0) = n$. Logo $n = n_0 + 1 \implies \exists q \,:\, n = q + 1 = q + m$.

Supondo $m \in X$. Dado $n \in \mathbb{N}$, se $m = n$, temos $s(m) = s(n) = n + 1$, logo $\exists p \in \mathbb{N} \,:\, s(n) = n + p$. Se $\exists p \in \mathbb{N} \,:\, m = n + p$, temos $s(m) = s(n + p) = (n + p + 1) = n + s(p)$, logo $\exists p' \in \mathbb{N} \,:\, s(n) = n + p'$. Se $\exists q \in \mathbb{N} \,:\, n = m + q$ com $q = 1$, temos $n = m + 1 = s(m)$. Se $\exists q \in \mathbb{N} \,:\, n = m + q$ com $q \neq 1$, existe $q_0 \in \mathbb{N}$ tal que $s(q_0) = q$, logo temos $n = m + q = m + s(q_0) = m + (q_0 + 1) = m + 1 + q_0 = s(m) + q_0 \implies \exists q' \in \mathbb{N} \,:\, n = s(m) + q'$.

Como $1 \in X$ e $m \in X \implies s(m) \in X$, temos $X = \mathbb{N}$. Logo para todo par $m, n \in \mathbb{N}$, pelo menos uma das condições da tricotomia ocorre. Pelo lema 6, apenas uma das possbilidades ocorre. □

3.5.3 Ordem nos Naturais

Definição 3.17 ($<$)**.**

$$m < n \iff \exists p \in \mathbb{N} \,:\, n = m + p$$

Dados m, n naturais, dizemos que m é menor que n ($m < n$) quando existe $p \in \mathbb{N}$ tal que $n = m + p$.

Proposição 3.31. *Temos* $1 < n$ *para todo* $1 \neq n \in \mathbb{N}$.

Demonstração. Como $n \neq 1$, temos pela proposição 3.26 que n possui um antecessor. Logo existe n_0 tal que $s(n_0) = n \implies n = 1 + n_0$. Logo $1 < n$. □

Definição 3.18 ($\leq$)**.**

$$m \leq n \iff (m = n) \vee (m < n)$$

Proposição 3.32 (Transitividade da relação $<$)**.** $m < n \wedge n < p \implies m < p$

Demonstração. Se $m < n$ e $n < p$, temos $n = m + q$ e $p = n + r$ para algum par $q, r \in \mathbb{N}$. Logo $p = n + r = (m + q) + r = m + (q + r)$. Logo $m < p$. □

Proposição 3.33 (Tricotomia da relação $<$)**.** *Dados $m, n \in \mathbb{N}$, exatamente uma das afirmações ocorre: $m = n$, ou $m < n$, ou $n < m$.*

Demonstração. Segue diretamente da proposição 3.30. □

Proposição 3.34.

$$p \leq q \wedge q \leq p \iff p = q$$

Demonstração. Supondo $p = q$, temos $p \leq q$ e $q \leq p$.

Supondo $p \leq q \wedge q \leq p$. Se $p = q$, acabou a demonstração. Supondo $p \neq q$. Logo devemos ter $p < q$ e $q < p$ (contradição). Logo devemos ter $p = q$.

□

Proposição 3.35. *Dados m, n, p naturais, temos*

$$m + p < n + p \iff m < n.$$

Demonstração. Temos $m + p < n + p \implies \exists q \in \mathbb{N} : n + p = (m + p) + q \implies \exists q \in \mathbb{N} : n = m + q \implies m < n$. Se $m < n$, existe $q \in \mathbb{N}$ tal que $n = m + q$, daí $n + p = (m + q) + p = (m + p) + q$, logo $m + p < n + p$. □

Lema 7.

$$m < n + 1 \iff m \leq n$$

Demonstração. Supondo $m < n + 1$. Logo existe $q \in \mathbb{N}$ tal que $n + 1 = m + q$. Se $q = 1$, temos $n + 1 = m + 1 \implies n = m \implies m \leq n$. Se $q \neq 1$, existe q_0 tal que $s(q_0) = q$. Logo $n + 1 = m + s(q_0) = m + q_0 + 1 \implies n = m + q_0 \implies m < n \implies m \leq n$.

Se $m \leq n$, temos $m \leq n < n + 1 \implies m < n + 1$. □

Lema 8.

$$m < n \iff m + 1 \leq n$$

Demonstração. Pelo lema anterior:

$$m < n \iff m + 1 < n + 1 \iff m + 1 \leq n$$

□

3.5.4 Produto nos Naturais

Definição 3.19 (Multiplicação)**.** Para todo $m \in \mathbb{N}$, seja $f_m : \mathbb{N} \to \mathbb{N}$ que associa cada $p \in \mathbb{N}$ a $f_m(p) = m + p$. Dados $m, n \in \mathbb{N}$, o produto entre naturais satisfaz $m \cdot 1 = m$ e $m \cdot (n + 1) = (f_m)^n(m)$.

Lema 9 (Distributiva do sucessor)**.**

$$m \cdot (n + 1) = mn + m$$

Demonstração. Se $n = 1$, temos $m \cdot (1+1) = (f_m)^1(m) = f_m(m) = m + m = m \cdot 1 + m$. Se $n \neq 1$, existe $n_0 \in \mathbb{N}$ tal que $s(n_0) = n$. Logo temos $m \cdot (n+1) = (f_m)^n(m) = (f_m)^{s(n_0)}(m) = f_m((f_m)^{n_0}(m)) = f_m(m(n_0+1)) = f_m(m \cdot n) = mn + m$. $\square$

Proposição 3.36 (Distributiva à esquerda)**.**

$$m \cdot (n+p) = mn + mp$$

Demonstração. Seja $X = \{p \in \mathbb{N} | \forall m, n \in \mathbb{N} : n \cdot (m+p) = nm + np\}$. Temos $1 \in X$ pelo lema 3.5.4. Supondo $p \in X$. Temos

$$\begin{aligned} n \cdot (m + s(p)) &= n \cdot ((m+p)+1) \\ &= n \cdot (m+p) + n \\ &= nm + np + n \\ &= nm + n(p+1) \\ &= nm + n \cdot s(p) \end{aligned}$$

Como $p \in X \implies s(p) \in X$ e $1 \in X$, temos $X = \mathbb{N}$. $\square$

Proposição 3.37 (Distributiva à direita)**.**

$$(m+n) \cdot p = mp + np$$

Demonstração. Seja $X = \{p \in \mathbb{N} | \forall m, n \in \mathbb{N} : (m+n) \cdot p = mp + np\}$. Temos $1 \in X$, pos $(m+n) \cdot 1 = m + n = m \cdot 1 + n \cdot 1$. Supondo $p \in X$. Temos

$$\begin{aligned} (m+n) \cdot s(p) &= (m+n) \cdot (p+1) \\ &= (m+n) \cdot p + (m+n) \\ &= mp + np + m + n \\ &= mp + m + np + n \\ &= m(p+1) + n(p+1) \\ &= m \cdot s(p) + n \cdot s(p) \end{aligned}$$

Como $p \in X \implies s(p) \in X$ e $1 \in X$, temos $X = \mathbb{N}$. $\square$

Proposição 3.38 (Associatividade)**.**

$$m \cdot (n \cdot p) = (m \cdot n) \cdot p$$

Demonstração. Seja $X = \{p \in \mathbb{N} | \forall m, n \in \mathbb{N} : m \cdot (n \cdot p) = (m \cdot n) \cdot p\}$. Temos $m \cdot (n \cdot 1) = m \cdot n = (m \cdot n) \cdot 1$, logo $1 \in X$.

Supondo $p \in X$. Temos

$$\begin{aligned} m \cdot (n \cdot s(p)) &= m \cdot (n \cdot (p + 1)) \\ &= m \cdot (n \cdot p + n) \\ &= m \cdot (n \cdot p) + m \cdot n \\ &= (m \cdot n) \cdot p + (m \cdot n) \\ &= (m \cdot n) \cdot (p + 1) \\ &= (m \cdot n) \cdot s(p) \end{aligned}$$

Como $p \in X \implies s(p) \in X$ e $1 \in X$, temos $X = \mathbb{N}$. □

Lema 10 (Comutatividade com 1)**.**

$$m \cdot 1 = 1 \cdot m$$

Demonstração. Seja $X = \{m \in \mathbb{N} | m \cdot 1 = 1 \cdot m\}$. Temos $1 \cdot 1 = 1 \cdot 1$, logo $1 \in X$.

Supondo $m \in X$. Temos

$$\begin{aligned} s(m) \cdot 1 &= (m+1) \cdot 1 \\ &= m+1 \\ &= m \cdot 1 + 1 \cdot 1 \\ &= 1 \cdot m + 1 \cdot 1 \\ &= 1 \cdot (m+1) \\ &= 1 \cdot s(m) \end{aligned}$$

Como $m \in X \implies s(m) \in X$ e $1 \in X$, temos $X = \mathbb{N}$. □

Proposição 3.39 (Comutatividade)**.**

$$m \cdot n = n \cdot m$$

Demonstração. Seja $X = \{n \in \mathbb{N} | \forall m \in \mathbb{N} : m \cdot n = n \cdot m\}$. Temos $1 \in X$ pelo lema 10. Supondo $n \in X$. Temos

$$\begin{aligned} m \cdot s(n) &= m \cdot (n+1) \\ &= mn + m \cdot 1 \\ &= nm + 1 \cdot m \\ &= (n+1) \cdot m \\ &= s(n) \cdot m \end{aligned}$$

Como $p \in X \implies s(p) \in X$ e $1 \in X$, temos $X = \mathbb{N}$. □

Proposição 3.40 (Monotonicidade)**.**

$$m < n \implies mp < np$$

Demonstração. Supondo $m < n$. Logo $n = m + q$ com $q \in \mathbb{N}$. Logo $np = (m+q)p = mp + qp$. Como $qp \in \mathbb{N}$, temos $mp < np$. ☐

Proposição 3.41 (Lei do cancelamento)**.**

$$mp < np \implies m < n$$

Demonstração. Supondo $mp < np$. Pela tricotomia, temos $n < m$, $m = n$, ou $m < n$. Se $n < m$, temos $np < mp$ (contradição). Se $m = n$, temos $mp = np$ (contradição). Logo devemos ter $m < n$.

☐

Definição 3.20 (Elemento Mínimo)**.** Dado $X \subset \mathbb{N}$, dizemo que $p \in X$ é o menor elemento (ou elemento mínimo) de X se $\forall n \in X \,:\, p \leq n$.

Observação 3.7. Como $\forall n \in \mathbb{N} \,:\, 1 \leq n$, temos que $1 \in X$ implica 1 menor elemento de X.

Proposição 3.42. *O elemento mínimo de um conjunto $X \subset \mathbb{N}$, quando existir, é unico.*

Demonstração. Suponha que dado um conjunto $X \subset \mathbb{N}$, existam $p, q \in X$ elementos mínimos. Logo $p \leq q$ e $q \leq p$. Logo $p = q$. ☐

Definição 3.21 (Maior elemento)**.** Dado $X \subset \mathbb{N}$, dizemo que $p \in X$ é o maior elemento (ou elemento máximo) de X se $\forall n \in X \,:\, p \geq n$.

Proposição 3.43. *Os naturais não possuem maior elemento.*

Demonstração. Suponha que $x \in \mathbb{N}$ seja o maior elemento de $\mathbb{N}$. Teríamos $s(x) \in \mathbb{N}$ e $x < s(x)$ (contradição). Logo os naturais não possuem maior elemento. ☐

Proposição 3.44. *O elemento máximo de um conjunto $X \subset \mathbb{N}$, quando existir, é unico.*

Demonstração. Exercício. ☐

Definição 3.22 (I_n)**.**

$$I_n := \{x \in \mathbb{N} \mid x \leq n\}$$

Lema 11.

$$I_{n+1} = I_n \cup \{n+1\}$$

Demonstração.

$$\begin{aligned} x \in I_{n+1} &\iff \\ x \leq n+1 &\iff \\ x < n+1 \lor x = n+1 &\iff \\ x \leq n \lor x = n+1 &\iff \\ x \in I_n \lor x \in \{n+1\} &\iff \\ x \in I_n \cup \{n+1\} & \end{aligned}$$

$\square$

Teorema 1 (Princípio da boa Ordenação)**.** *Todo subconjunto $A \neq \varnothing$ dos naturais admite menor elemento.*

Demonstração. Dado $A \subset \mathbb{N}$ não vazio. Se $1 \in A$, temos 1 menor elemento.

Supondo $1 \notin A$. Logo $1 \in \mathbb{N} - A$. Seja $X = \{x \in \mathbb{N} \mid I_n \subset \mathbb{N} - A\}$. Como $1 \in \mathbb{N} - A$, temos $I_1 = \{1\} \subset \mathbb{N} - A$, logo $1 \in X$. Como A é não vazio, existe $a \in A$. Logo $a \notin \mathbb{N} - A$. Temos $a \leq a \implies a \in I_a$. Logo $I_a \not\subset \mathbb{N} - A$. Logo $a \notin X$. Temos $1 \in X$ e $X \neq \mathbb{N}$, logo o axioma da indução deve falhar. Logo deve existir $n \in X$ com $n + 1 = s(n) \notin X$.

Afirmo que $n+1$ é o menor elemento de A. Como $n \in X$, temos $I_n \subset \mathbb{N} - A$, logo $x \leq n \implies x \in \mathbb{N} - A$. Como $n + 1 \notin X$, temos $I_{n+1} \not\subset \mathbb{N} - A$. Logo existe um $m \in I_{n+1}$ com $m \notin \mathbb{N} - A \implies m \in A$. Observe que $m \in I_{n+1} \implies m \leq n + 1 \implies m = n + 1 \vee m < n + 1$. Se $m < n + 1$, temos pelo Lema 7 que $m \leq n$, que implica $m \in I_n$, logo $m \in \mathbb{N} - A$ (contradição). Logo devemos ter $m = n + 1$. Temos portanto que $n + 1 \in A$.

Suponha que exista $p \in A$ tal que $p < n + 1$. Teríamos $p \leq n \implies p \in I_n \implies p \in \mathbb{N} - A \implies p \notin A$. Contradição. Logo temos $n + 1 \leq p$ para todo $p \in A$. Logo $n + 1$ é o menor elemento de A. $\square$

Teorema 2 (Indução completa)**.** *Seja $X \subset \mathbb{N}$ tal que $(\forall m \in \mathbb{N} : m < n \implies m \in X) \implies n \in X$. Então $X = \mathbb{N}$*

Demonstração. Temos $1 \in X$, pois $1 \notin X$ implicaria na existência de um $m < 1$ com $m \notin X$. Supondo $X \neq \mathbb{N}$ e $A = \mathbb{N} - X$. Como $X \neq \mathbb{N}$, temos $A \neq \emptyset$. Logo A possui um menor elemento $a \in A$. Se $p \in \mathbb{N}$ com $p < a$, então $p \notin A$, logo $p \in X$. Como $\forall p \in \mathbb{N} : p < a \implies p \in X$, temos $a \in X$. Contradição. Logo A é vazio. Logo $X = \mathbb{N}$. $\square$

3.5.5 Exercícios

Exercício 3.5.1. Se $\phi : \mathbb{N} \to \mathbb{N}$ é estritamente crescente, então:

(a) $\forall n \in \mathbb{N} : \phi(n) \geq n$.

(b) ϕ é injetiva.

Demonstração.

(a) Seja $X = \{n \in \mathbb{N} \mid \phi(n) \geq n\}$. Temos $1 \in X$ pois $\forall p \in \mathbb{N}\, p \geq 1$. Suponha $n \in X$, logo $\phi(n) \geq n$. Daí temos $\phi(n+1) > \phi(n) \geq n \implies \phi(n+1) > n \iff \phi(n+1) \geq n+1$. Como $1 \in X$ e $n \in X \implies n+1 \in X$, temos $X = \mathbb{N}$.

(b) Se $a \neq b$, temos $a < b$ ou $a > b$, daí $\phi(a) > \phi(b)$ ou $\phi(a) < \phi(b)$. Em ambos os casos, temos $\phi(a) \neq \phi(b)$.

$\square$

3.6 Conjuntos Finitos e Infinitos

3.6.1 Conjuntos Finitos

Definição 3.23 (Conjuntos finitos)**.** Um conjunto X é finito quando for vazio ou quando existir para algum $n \in \mathbb{N}$ uma bijeção $\phi : I_n \to X$

Definição 3.24 (Tamanho de um conjunto)**.** Dado um conjunto finito. Dizemos que ele tem zero elementos se for vazio e que ele tem n elementos se tiver bijeção com I_n.

Observação 3.8. O conjunto I_n é finito e possui n elementos.

Observação 3.9. Denota-se $|A|$ como o tamanho do conjunto A.

Proposição 3.45. *Se $f : X \to Y$ é uma bijeção, então X é finito se, e somente se, Y for finito.*

Demonstração. Se X for finito, então existe um bijeção $\phi : I_n \to X$. A composição $(\phi \circ f) : I_n \to Y$ é uma bijeção, logo Y é finito. O caso Y finito é análogo. □

Teorema 3. *Seja $A \subset I_n$ não vazio. Se exite uma bijeção $f : I_n \to A$, então $A = I_n$.*

Demonstração. Seja $X = \{n \in \mathbb{N} \mid \forall A \subset I_n : (\text{Existe uma bijeção } f : I_n \to A) \implies A = I_n\}$. Temos $1 \in X$, pois $I_1 = \{1\}$ e $A \subset I_1 \implies A = \{1\} = I_1$. Supondo $n \in X$. Seja $A \subset I_{n+1}$ com uma bijeção $f : I_{n+1} \to A$. Restringindo f a I_n, obtemos $f' : I_n \to A - \{f(n+1)\}$, que é uma bijeção pela proposição 3.12.

Se $A - \{f(n+1)\} \subset I_n$, temos por $n \in X$ que $A - \{f(n+1)\} = I_n$. Como o contra-domínio de f é A e $A \subset I_{n+1}$, temos que $f(n+1) \in A \implies f(n+1) \in I_{n+1} \implies f(n+1) \in I_n \vee f(n+1) \in \{n+1\}$. Se $f(n+1) \in I_n$, temos $f(n+1) \notin A - \{f(n+1)\}$, logo $A - \{f(n+1)\} \neq I_n$ (contradição). Logo temos $f(n+1) = n+1$. Logo $f(n+1) = n+1 \in A$. Como $A - \{n+1\} = A - \{f(n+1)\} = I_n$, temos $(A - \{n+1\}) \cup \{n+1\} = I_n \cup \{n+1\} \implies A \cup \{n+1\} = I_{n+1} \implies A = I_{n+1}$. Logo temos $A = I_{n+1}$.

Se $A - \{f(n+1)\} \not\subset I_n$. Logo existe $a \in A$ tal que $a \notin I_n$ e $a \neq f(n+1)$. Mas $A \subset I_{n+1}$. Logo $a \in I_{n+1} = I_n \cup \{n+1\}$. Logo devemos ter $a = n+1$. Como f é sobrejetiva, existe $m \in I_{n+1}$ tal que $f(m) = n+1$. Definindo a função $g : I_{n+1} \to A$, como $g(x) = \begin{cases} f(x), & x \neq f(n+1) \wedge x \neq n+1 \\ n+1, & x = n+1 \\ f(n+1), & x = m \end{cases}$. Temos g uma bijeção. Logo a restrição $g' : I_n \to A - \{g(n+1)\}$ é uma bijeção com $A - \{g(n+1)\} \subset I_n$. Portanto temos $A - \{g(n+1)\} = I_n$ com $A = I_{n+1}$. □

Proposição 3.46. *Se existe uma bijeção $f : I_n \to I_m$, então $I_m = I_n$.*

Demonstração. Se $m \leq n$, então existe uma bijeção $f : I_n \to I_m$ com $I_m \subset I_n$. Logo pelo teorema anterior, temos $I_m = I_n$. Se $n > m$, temos a bijeção $f^{-1} : I_m \to I_n$ com $I_n \subset I_m$. Logo pelo teorema anterior $I_m = I_n$. □

Proposição 3.47. *Não existe uma bijeção $f : X \to Y$ entre um conjunto finito X e uma parte própia $Y \subset X$.*

Demonstração. Como X é finito, existe uma bijeção $g : I_n \to X$. Suponha que exista uma bijeção $f : X \to Y$. Como Y é parte própria, existe um $x \in X - Y$. Tome $A = g^{-1}(Y) \subset g^{-1}(X) = I_n$. Temos $g^{-1}(x) \notin A$, logo A é uma parte própria de I_n. Queremos achar uma bijeção $h : I_n \to A$. Restringindo g a A, obtendo a bijeção $g' : A \to Y$. Definindo a bijeção $h = (g') \circ f \circ g : I_n \to A$. Pelo teorema 3, temos que $A = I_n$. Uma contradição, pois A é parte própria de I_n. Logo não existe bijeção entre um conjunto finito X e uma parte própria $Y \subset X$. $\square$

Lema 12. *Todo subconjunto A de I_n é finito e temos $|A| \leq n$*

Demonstração. Seja $X = \{n \in \mathbb{N} \,|\, A \subset I_n \implies A \text{ finito } \wedge |A| \leq n\}$. Temos $1 \in X$, pois os subconjuntos de $I_1 = \{1\}$ são $\{\}$ e $\{1\} = I_1$, ambos finitos.

Suponha $n \in X$. Seja $A \subset I_{n+1} = I_n \cup \{n+1\}$. Se $n+1 \notin A$, então temos $A \subset I_n$. Pela hipótese de indução, temos A finito e $|A| \leq n < n+1$.

Supondo $n+1 \in A$. Se $A = \{n+1\}$, temos A finito e $|A| = 1 \leq n$. Supondo $A \neq \{n+1\}$, temos $B = A - \{n+1\} \neq \emptyset$ e $B \subset I_n$. Logo B é finito e temos $k = |B| \leq n$. Como B é finito, existe a bijeção $f : I_k \to B$. Definindo a bijeção $f' : I_{k+1} \to A$ pondo $f'(x) = f(x)$ para $x \in I_n$ e $f(k+1) = n+1$. Logo A é finito e temos $|A| = k+1 \leq n+1$.

$\square$

Lema 13. *Seja $A \subset I_n$. Temos $|A| = n \iff A = I_n$.*

Demonstração. Se $|A| = n$, existe a bijeção $f : I_n \to A$,com $A \subset I_n$, logo $A = I_n$. $\square$

Teorema 4. *Todo subconjunto Y de um conjunto finito X é finito e $|Y| \leq |X|$, com $|Y| = |X| \iff X = Y$.*

Demonstração. Se X é finito, existe uma bijeção $f : I_n \to X$. Seja $A = f^{-1}(Y) \subset I_n$ e seja a bijeção $f' : A \to Y$ a restrição de f a A. Como $A \subset I_n$, temos A finito e $|A| \leq n$. Logo Y é finito e $|Y| = |A| \leq n$. Temos $|Y| = |A| = n = |X| \iff |A| = I_n$. Logo $f^{-1}(Y) = I_n = f^{-1}(X)$. Logo $X = Y$. $\square$

Proposição 3.48. *Seja $f : X \to Y$ uma função injetiva. Se Y é finito, então X é finito e $|X| \leq |Y|$.*

Demonstração. Como existe a injeção $f : X \to Y$, temos a bijeção $f' : X \to f(X)$, com $f(X) \subset Y$. Como Y é finito, temos $f(X)$ finito e $|f(X)| \leq Y$. Como existe a bijeção $f' : X \to f(X)$, temos $|X| = |f(X)| \leq Y$. $\square$

Proposição 3.49. *Seja $f : X \to Y$ uma função sobrejetiva. Se X é finito, então Y é finito e $|Y| \leq |X|$.*

Demonstração. Como f é sobrejetiva, ela admite inversa à direita. Seja $g : Y \to X$ a inversa à direita de f. Se $g(y) = g(y')$, temos $f(g(y)) = f(g(y'))$, logo $y = y'$. Logo g é injetiva. Pela proposição anterior, temos Y finito com $|Y| \leq |X|$. □

3.6.2 Conjuntos Infinitos

Definição 3.25 (Conjunto infinito)**.** Um conjunto é infinito quando não for finito.

Observação 3.10. A função sucessor com o contradomínio reduzido é uma bijeção entre uma parte dos naturais com os naturais:

$$s : \mathbb{N} \to \mathbb{N} - \{1\}$$

Logo os naturais são infinitos.

Definição 3.26 (Conjunto limitado)**.** Um conjunto $X \subset \mathbb{N}$ é limitado quando existe $p \in \mathbb{N}$ tal que $\forall n \in X \ : \ n \leq p$.

Teorema 5. *Seja $X \subset \mathbb{N}$ não vazio. As seguintes afirmações são equivalentes:*

- *X é finito.*
- *X é limitado.*
- *X possui maior elemento.*

Demonstração. (a) $\implies$ (b)

Seja $A = \{n \in \mathbb{N} \mid |X| = n \implies X \text{ limitado }\}$. Se $|X| = 1$, temos que $X = \{a\}$ para algum $a \in \mathbb{N}$. Logo X é limitado pelo a, pois $a \leq a$. Supondo $n \in X$. Seja $|X| = n + 1$. Logo existe uma bijeção $f : I_{n+1} \to X$. Tomando a bijeção $f' : I_n \to X - \{f(n+1)\}$. Logo $X - \{f(n+1)\}$ tem tamanho n. Pela hipótese de indução, temos $X - \{f(n+1)\}$ limitado por um $p \in \mathbb{N}$, ou seja: $\forall t \in X - \{f(n+1)\} \ : \ t \leq p$. Se $f(n+1) \leq p$, temos que p limita X. Se $p \leq f(n+1)$, temos para todo $t \in X - \{f(n+1)\}$ que $t \leq p \leq f(n+1)$ e $f(n+1) \leq f(n+1)$, logo $f(n+1)$ limita X.

Como $1 \in A$ e $n \in A \implies n + 1 \in A$, temos $A = \mathbb{N}$

(a) $\implies$ (b) [Outra forma]

Seja $X = \{x_1, x_2, \cdots x_n\}$, defina $a = x_1 + x_2 + \cdots x_n$. Temos $x \leq a$ para todo $x \in X$, logo X é limitado.

(b) $\implies$ (c)

Como X é limitado, existe um $p \in \mathbb{N}$ tal que $\forall n \in X \ : \ n \leq p$. É natural pensar que o maior elemento será o menor dos "limitadores". Logo seja $A = \{p \in \mathbb{N} \mid \forall n \in X \ : \ n \leq p\}$. A é não vazio, logo é limitado inferiormente por um $a \in A$. Se $a \in X$, a é o maior elemento de X. Supondo $a \notin X$. Logo temos para todo $n \in X$ que $n \leq a$, mas nunca $n = a$, logo temos $n < a$. Se $a = 1$, temos $n < 1$ (contradição) . Se $a \neq 1$, existe a_0 tal que $a_0 + 1 = a$. Pelo lema 7, obtemos $n < a_0 + 1 \implies n \leq a_0$ para todo $n \in X$. Uma contradição, pois $a_0 \in A$ com $a_0 < a$ (a é o menor elemento de A). Logo devemos ter $a \in X$. Logo X possui maior elemento.

(c) $\implies$ (a)

Seja $p \in X$ o maior elemento de X. Conjecturo que $|X| \leq p$. Vamos mostrar que $X \subset I_p$. Seja $x \in X$. Como p é o maior elemento de X, temos $x \leq p$. Como $X \subset \mathbb{N}$, temos $x \in \mathbb{N}$. Como $x \in \mathbb{N}$ e $x \leq p$, temos $x \in I_p$. Como $x \in X \implies x \in I_p$, temos $X \subset I_p$. Logo X é finito e $|X| \leq p$. □

Teorema 6. *Sejam X, Y conjuntos finitos disjuntos, então $X \cup Y$ é finito e $|X \cup Y| = |X| + |Y|$.*

Demonstração. Sejam $f_x : I_n \to X$ e $f_y : I_m \to Y$ bijeções. Seja $f_{xy} : I_{n+m} \to X \cup Y$ definida como:

$$f_{xy}(p) = \begin{cases} f_x(p), & p \leq n \\ f_y(r), & n < p \leq n+m \end{cases}$$

Se $n < p$, existe $r \in \mathbb{N}$ tal que $p = n + r$. Como $p \leq n + m$, temos $r \leq m$.

Supondo $f_{xy}(p) = f_{xy}(q)$ com $p \neq q$. Logo $p < q$ ou $q < p$. Supondo sem perda de generalidade que $p < q$. Se $n < q \leq n + m$ e $p \leq n$, temos $f_x(p) = f_y(q)$, mas X e Y são disjuntos, logo devemos ter ou $p < q \leq n$ ou $n < p < q \leq m+n$. Se $p < q \leq n$, temos $f_x(p) = f_x(q) \implies p = q$ (f_x injetiva). O caso $n < p < q \leq m + n$ é analogo. Logo $f_{xy}(p) = f_{xy}(q) \implies p = q$ (contradição). Logo devemos ter $p = q$. Logo f_{xy} é injetiva.

Seja $p \in X \cup Y$. Logo $p \in X$ ou $p \in Y$. Supondo $p \in X$. Como f_x é sobrejetiva, existe $n_x \in I_n$ tal que $f_x(n_x) = p$. Como $n_x \leq n$, temos $f_{xy}(n_x) = f_x(n_x) = p$. Se $p \in Y$. Como f_y é sobrejetiva, existe $n_y \in I_m$ tal que $f_y(n_y) = p$. Como $n_y \leq m$, temos $n < n + n_y \leq m$ e $f_{xy}(n + n_y) = f_y(n_y) = p$ $(n_y = r)$. Logo f_{xy} é sobrejetiva.

Logo f_{xy} é bijetiva.

Logo $X \cup Y$ é finito e tem tamanho $n + m = |X| + |Y|$.

□

Proposição 3.50. *Sejam X, Y conjuntos finitos , então $X \cup Y$ é finito e $|X \cup Y| \leq |X| + |Y|$.*

Demonstração. Sejam $f_x : I_n \to X$ e $f_y : I_m \to Y$ bijeções. Seja $f_{xy} : I_{n+m} \to X \cup Y$ definida como:

$$f_{xy}(p) = \begin{cases} f_x(p), & p \leq n \\ f_y(r), & n < p \leq n+m \end{cases}$$

Se $n < p$, existe $r \in \mathbb{N}$ tal que $p = n + r$. Como $p \leq n + m$, temos $r \leq m$.

Seja $p \in X \cup Y$. Logo $p \in X$ ou $p \in Y$. Supondo $p \in X$. Como f_x é sobrejetiva, existe $n_x \in I_n$ tal que $f_x(n_x) = p$. Como $n_x \leq n$, temos $f_{xy}(n_x) =$

$f_x(n_x) = p$. Se $p \in Y$. Como f_y é sobrejetiva, existe $n_y \in I_m$ tal que $f_y(n_y) = p$. Como $n_y \leq m$, temos $n < n + n_y \leq m$ e $f_{xy}(n + n_y) = f_y(n_y) = p$ $(n_y = r)$. Logo f_{xy} é sobrejetiva.

Logo $X \cup Y$ é finito e $|X| + |Y| \leq |X| + |Y|$.

$\square$

Proposição 3.51. *Temos para todos $m, n \in \mathbb{N}$ que $I_n \times I_m$ é finito e $|I_n \times I_m| = n \cdot m$.*

Demonstração. Seja $X = \{n \in \mathbb{N} \mid \forall m \in \mathbb{N} : |I_n \times I_m| = n \cdot m\}$. Temos $1 \in X$, pois para qualquer $m \in \mathbb{N}$, existe uma bijeção entre I_m e $I_m \times I_1$, logo $I_m \times I_1$ é finito e $|I_m \times I_1| = |I_m| = m = 1 \cdot m$.

Supondo $n \in X$. Dado $m \in \mathbb{N}$, seja $I_m \times I_{n+1} = I_m \times (I_n \cup \{n+1\}) = (I_m \times I_n) \cup (I_m \times \{n+1\})$. Temos $(I_m \times I_n)$ finito e $|I_m \times I_n| = m \cdot n$ (hipótese de indução) e $I_m \times \{n+1\}$ finito com $|I_m \times \{n+1\}| = m$. Logo $|I_m \times I_{n+1}| = |(I_m \times I_n) \cup (I_m \times \{n+1\})| = mn + m = m \cdot (n+1)$.

Como $1 \in X$ e $n \in X \implies n+1 \in X$, temos $X = \mathbb{N}$. $\square$

Proposição 3.52. *Sejam X, Y conjuntos finitos , então $X \times Y$ é finito e $|X \times Y| = |X| \times |Y|$.*

Demonstração. Sejam $f_x : I_n \to X$ e $f_y : I_m \to Y$ bijeções. Logo $g : I_n \times I_m \to X \times Y$, definida por $g(p,q) = (f_x(p), f_y(q))$ é uma bijeção. Logo $|X \times Y| = |I_n \times I_m| = m \cdot n = |X| \times |Y|$.

$\square$

Proposição 3.53. *Temos para todos $m, n \in \mathbb{N}$ que $\mathcal{F}(I_n, I_m)$ é finito e $|\mathcal{F}(I_n, I_m)| = m^n$.*

Demonstração. Seja $X = \{n \in \mathbb{N} \mid \forall m \in \mathbb{N} : |\mathcal{F}(I_n, I_m)| = m^n\}$. Temos $1 \in X$, pois para qualquer $m \in \mathbb{N}$, existe uma bijeção entre I_m e $\mathcal{F}(I_1, I_m)$, logo $\mathcal{F}(I_1, I_m)$ é finito e $|\mathcal{F}(I_1, I_m)| = |I_m| = m = m^1$.

Supondo $n \in X$. Temos $\mathcal{F}(I_{n+1}, I_m) = \mathcal{F}(I_n \cup \{n+1\}, I_m)$. Existe uma bijeção entre $\mathcal{F}(I_n \cup \{n+1\}, I_m)$ e $\mathcal{F}(I_n, I_m) \times \mathcal{F}(\{n+1\}, I_m)$. Existe uma bijeção entre $\mathcal{F}(\{n+1\}, I_m)$ e $\mathcal{F}(I_1, I_m)$. Logo existe uma bijeção entre $\mathcal{F}(I_n, I_m) \times \mathcal{F}(\{n+1\}, I_m)$ e $\mathcal{F}(I_n, I_m) \times \mathcal{F}(I_1, I_m)$. Como $\mathcal{F}(I_n, I_m)$ é finito e possui tamanho m^n e $\mathcal{F}(I_1, I_m)$ é finito epossui tamanho m^1, temos $\mathcal{F}(I_n, I_m) \times \mathcal{F}(I_1, I_m)$ finito e de tamanho $m^n \cdot m = m^{n+1}$. Como existe uma bijeção entre $\mathcal{F}(I_n, I_m) \times \mathcal{F}(I_1, I_m)$ e $\mathcal{F}(I_{n+1}, I_m)$, temos $\mathcal{F}(I_{n+1}, I_m)$ finito e de tamaho m^{m+1}.

Como $n \in X \implies n+1 \in X$ e $1 \in X$, temos $X = \mathbb{N}$. $\square$

Definição 3.27 (Conjunto Enumerável)**.** Um conjunto é dito enumerável se é finito ou se existe uma bijeção $f : \mathbb{N} \to X$.

Lema 14. *$\mathbb{N}$ é enumerável*

Demonstração. Seja $f : \mathbb{N} \to \mathbb{N}$ a função indentidade. f é uma bijeção, logo $\mathbb{N}$ é enumerável. $\square$

Proposição 3.54. *Se existe uma injeção $f : \mathbb{N} \to Y$, então $f(\mathbb{N})$ é enumerável.*

Demonstração. Definindo a bijeção $f' : \mathbb{N} \to f(\mathbb{N}), f'(x) = f(x)$. Temos $f(\mathbb{N})$ contável. $\square$

Proposição 3.55. *Todo conjunto infinito X tem um subconjunto enumerável.*

Demonstração. Basta construir uma injeção $f : \mathbb{N} \to X$. Seja $A = \mathcal{P}(X) - \emptyset$. Temos $\bigcup A = X$ e $\emptyset \notin A$. Seja $g : A \to X$ a função escolha aplicada em A. Logo temos $g(a) \in a \subset X$ para todo $a \in A$. Seja $f : \mathbb{N} \to X$ definida indutivamente por

$$\begin{cases} f(1) = g(A) \\ f(n+1) = g(A - f(I_n)) \end{cases}.$$

Se $A - f(I_n) = \emptyset$, teríamos $A = f(I_n)$, uma contradição, pois A é infinito e $f(I_n)$ é finito. Logo $A - f(I_n) \neq \emptyset$ para todo $n \in \mathbb{N}$. Logo $g(A - f(I_n))$ está sempre definida.

Queremos mostrar que f é injetiva. Suponha $f(m+1) = f(n+1)$ com $m \neq m$. Suponha sem perda de generalidade que $n < m$. Logo temos $n+1 \in I_m \implies f(n+1) \in f(I_m)$. Por definição, temos $f(n+1) = f(m+1) = g(A - f(I_m)) \in A - f(I_m)$. Contradição, pois $f(n+1) \in f(I_m) \implies f(n+1) \notin A - f(I_m)$. Logo $f(m+1) = f(n+1) \implies m = n$. Logo f é injetiva. Logo $f' : \mathbb{N} \to f(\mathbb{N})$ é bijetiva e $f(\mathbb{N})$ é contável. Logo existe um subconjunto $f\,(\mathbb{N})$ de X contável. $\square$

Proposição 3.56. *Um conjunto X é infinito se, e somente se, existir uma bijeção entre X e uma parte própria.*

Demonstração. Pela proprosição 3.6.1, se existir bijeção X não é finito.

Suponto X infinito. Logo existe subconjunto $Y \subset X$ enumerável. Seja $f : \mathbb{N} \to Y$ uma bijeção (uma enumeração). Vamos usar o fato da função $s : \mathbb{N} \to \mathbb{N} - \{1\}$ ser uma bijeção. Seja $A = (X - f\,(\mathbb{N})) \cup f(\mathbb{N} - \{1\}) = (X - Y) \cup (Y - \{f(1)\})$. Temos $f(1) \notin A$, logo A é parte própria de X. Seja $h : A \to X$ definida por

$$h(x) = \begin{cases} x, & x \in X - Y \\ f(s^{-1}(f^{-1}(x))), & x \in Y - \{f(1)\} \end{cases}$$

Se $x \in Y - \{f(1)\}$, temos $x \in Y$, logo $x \notin X - Y$. Se $x \in Y - \{f(1)\} = f(\mathbb{N} - \{1\})$, temos $f^{-1}(x) \in \mathbb{N} - \{1\}$, logo $s^{-1}(f^{-1}(x))$ está definida. . Logo h está bem definida.

Se $h(x) = h(y)$, com $x, y \in X - Y$, temos $h(x) = h(y) \implies x = y$. Se $h(x) = h(y)$ com $x, y \in Y - \{f(1)\}$, temos $f(s^{-1}(f^{-1}(x))) = f(s^{-1}(f^{-1}(y))) \implies x = y$ (f, s^{-1} são bijeções). Se $h(x) = h(y)$ com $x \in X - Y$ e $y \in Y - \{f(1)\}$, temos $h(x) = x = f(s^{-1}(f^{-1}(y))) = h(y)$. Temos $f(a) \in Y$ para todo $a \in \mathbb{N}$. Logo $f(s^{-1}(f^{-1}(y))) = x \in Y$. Contradição, pois $x \in X - Y$. Logo h é injetiva.

Seja $x \in X$. Temos $x \in Y$ ou $x \notin Y$. Se $x \notin Y$, temos $x \in X - Y$, logo $h(x) = x$. Se $x \in Y$, temos $x = f(n)$ com $n \in \mathbb{N}$. Temos $s(n) \in \mathbb{N} - \{1\}$, logo

$y = f(s(n)) \in Y - \{f(1)\}$. Logo $h(y) = f(s^{-1}(f^{-1}(y))) = f(n) = x$. Logo h é sobrejetiva.

Como $h : A \to X$ é bijetiva, existe bijeção entre X e uma parte própria de X. $\square$

Proposição 3.57. *Todo subconjunto $X \subset \mathbb{N}$ é enumerável.*

Demonstração. Se X for finito, ele é enumerável por definição. Se X for infinito. Seja $f : \mathbb{N} \to X$ definida indutivamente por

$$\begin{cases} f(1) = \min(X) \\ f(n+1) = \min(X - f(I_n)) \end{cases}$$

Como $f(I_n)$ é sempre finito, temos $X - f(I_n) \neq \emptyset$ para todo $n \in \mathbb{N}$. Logo o princípio da boa ordenação vale para $X - f(I_n)$. Logo f está bem definida.

Se $f(x+1) = f(y+1)$, com $x < y$ (sem perda de generalidade), temos $x+1 \leq y$, portanto $x+1 \in I_y \implies f(x+1) \in f(I_y)$. Logo $f(x+1) \notin X - f(I_y)$. Logo $f(x+1) \neq f(y+1)$, pois $f(y+1) \in X - f(I_y)$ (contradição). Logo f é injetiva.

Suponha $X \neq f(\mathbb{N})$. Logo $X - f(\mathbb{N}) \neq \emptyset$. Seja $y \in X - f(\mathbb{N})$. Seja $x \in f(\mathbb{N})$ qualquer. Logo $x = f(n)$ para algum $n \in \mathbb{N}$. Se $n = 1$, temos $x = f(1) = \min(X)$. Como $y \in X$, temos $x \leq y$. Se $n \neq 1 \implies \exists n_0 \in \mathbb{N} : n = n_0 + 1$, temos $x = f(n) = f(n_0+1) = \min(X - f(I_{n_0}))$. Como $y \in X - f(\mathbb{N}) \subset X - f(I_{n_0})$, temos $y \in X - f(I_{n_0})$, logo $x = f(n) = \min(X - I_{n_0}) \leq y$. Ou seja: $\forall x \in f(\mathbb{N}) : x \leq y$. Logo $f(\mathbb{N})$ é limitado superiormente por y. Contradição (conjunto infinito não possui limite superior). Logo $X = f(\mathbb{N})$.

Como f é injetiva e sobrejetiva, temos f bijetiva. Logo X é enumerável.

$\square$

Observação 3.11. A função construída na proposição anterior é estritamente crescente. De fato, seja $Y = \{p \in \mathbb{N} \,|\, \forall n \in \mathbb{N} : f(n+p) > f(n)\}$.

Temos $1 \in Y$. De fato, temos $f(n+1) = \min(X - f(I_n))$, logo $f(n+1) \in X - f(I_n)$, logo $f(n+1) \neq f(n)$, pois $f(n) \in f(I_n)$. Se $n = 1$, temos $f(2) \in X - f(I_1) \implies f(2) \in X \implies f(2) \leq f(1)$, pois $f(1) = \min X$. De $f(2) \neq f(1)$, obtemos $f(2) < f(1)$. Se $n \neq 1$, existe $n_0 \in \mathbb{N}$ tal que $n = n_0 + 1$. Daí $f(n+1 \in X - f(I_n) \subset X - f(I_{n_0})$, logo $f(n+1) = \min(X - f(I_n)) \leq \min(X - f(I_{n_0})) = f(n)$. Como $f(n+1) \neq f(n)$, temos $f(n+1) > f(n)$. Logo $1 \in Y$. Supondo $p \in Y$, temos para todo $n \in \mathbb{N}$ que $f(n+p) > f(n)$. Como $1 \in Y$, temos $f(p+1) > f(p) > f(n)$, logo $p+1 \in Y$. Logo $Y = \mathbb{N}$.

Se $m > n$, temos $m = n + p$ para algum $p \in \mathbb{N}$, daí $f(m) > f(n)$. Logo f é crescente.

Essa é outra forma de mostrar a injetividade da função f.

Proposição 3.58. *Se $f : X \to Y$ é uma bijeção e Y é enumerável, então X é enumerável.*

Demonstração. Se X for finito, ele é enumerável. Se X for infinito, então Y é infinito. Como Y é enumerável, existe uma bijeção $g : Y \to \mathbb{N}$. Logo existe a bijeção $g \circ f : X \to \mathbb{N}$. Logo X é enumerável. $\square$

Proposição 3.59. *Todo subconjunto X de um conjunto enumerável Y é enumerável.*

Demonstração. Se X for finito, ele é enumerável. Se X for infinito, então Y é infinito. Logo existe uma bijeção $f : Y \to \mathbb{N}$. Seja a bijeção $f' : X \to f(X)$ a restrição de f a X. Como $f(X) \subset \mathbb{N}$, temos $f(X)$ enumerável. Como existe uma bijeção entre X e um conjunto enumerável, temos X enumerável. $\square$

Proposição 3.60. *Se $f : X \to Y$ é uma injeção e Y é enumerável, então X é enumerável.*

Demonstração. Se X for finito, ele é enumerável. Se X for infinito, então Y é infinito. Temos $f(X) \subset Y$ é enumerável (subconjunto de conjunto enumerável). Seja a bijeção $f' : X \to f(X)$ a restrição de f a X. Como existe uma bijeção entre X e um conjunto enumerável, temos X enumerável. $\square$

Proposição 3.61. *Se $f : X \to Y$ é uma sobrejeção e X é enumerável, então Y é enumerável.*

Demonstração. Como f é sobrejetiva, ela admite inversa à direita. Seja $g : Y \to X$ a inversa à direita de f. Se $g(y) = g(y')$, temos $f(g(y)) = f(g(y'))$, logo $y = y'$. Logo g é injetiva. Pela proposição anterior, temos Y enumerável. $\square$

Lema 15. *Um conjunto X é enumerável se, e somente se, existir uma injeção $f : X \to \mathbb{N}$.*

Demonstração. Supondo X for enumerável. Se X for finito, existe uma bijeção $h : X \to I_n$. Como $I_n \subset \mathbb{N}$, existe uma injeção $X \to \mathbb{N}$. Se X for infinito, existe uma bijeção $g : X \to \mathbb{N}$. Em ambos os casos existe uma injeção entre X e $\mathbb{N}$.

Supondo que existe uma injeção $f : X \to \mathbb{N}$. Como $\mathbb{N}$ é enumerável, temos X enumerável. $\square$

Lema 16. ***(Teorema fundamental da aritmética)*** *Todo número natural ou é primo ou se escreve de modo único como um produto de números primos.*

Demonstração. Aritmética, Ahbramo. $\square$

Lema 17. $\mathbb{N} \times \mathbb{N}$ *é enumerável*

Demonstração. Seja $h : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $h(m, n) = 2^m \cdot 3^n$. Se $h(m, n) = h(v, w)$, temos $2^m \cdot 3^n = 2^v \cdot 3^w$. Pelo lema anterior, temos $m = v$ e $n = w$. Logo $(m, n) = (v, w)$. Logo h é injetiva. Logo $\mathbb{N} \times \mathbb{N}$ é enumerável. $\square$

Proposição 3.62. *Se X, Y são enumeráveis, temos $X \times Y$ enumerável.*

Demonstração. Existem injeções $f : X \to \mathbb{N}$ e $g : Y \to \mathbb{N}$. Logo a função $h : X \times Y \to \mathbb{N} \times \mathbb{N}$, $h(x, y) = (f(x), g(y))$ é uma injeção entre $X \times Y$ e um conjunto enumerável. Logo $X \times Y$ é enumerável. $\square$

Proposição 3.63. *Seja $(X_\lambda)_{\lambda\in L}$ uma família enumerável de conjuntos enumeráveis. Temos $Y = \bigcup_{\lambda\in L} X_\lambda$ enumerável.*

Demonstração. Como X_λ é enumerável para todo $\lambda \in L$, temos que existe uma função $f_\lambda : X \to \mathbb{N}$ injetiva para todo $\lambda \in L$. Definindo $g : Y \to \mathbb{N}$, dada por $g(x) = \min\{n \in \mathbb{N} | x \in X_n\}$. Se $x \in Y$, temos $x \in X_\lambda$ para algum $\lambda \in L$, logo $\{n \in \mathbb{N} | x \in X_n\}$ é não vazio. Para simplificar notação, vamos chamar $g(x) = n_x$. Seja $h : Y \to \mathbb{N}\times\mathbb{N}$, definida por $h(x) = (f_{n_x}(x), n_x)$. Afirmo que h é injetiva. De fato, se $h(x) = h(y)$, temos $(f_{n_x}(x), n_x) = (f_{n_y}(y), n_y) \iff f_{n_x}(x) = f_{n_y}(y) \wedge n_x = n_y$. Como $n_x = n_y$, temos $f_{n_x} = f_{n_y}$, logo $f_{n_x}(x) = f_{n_y}(x) = f_{n_y}(y)$. Mas f_y é injetiva, logo $x = y$. Logo h é injetiva. Logo Y é enumerável. □

Proposição 3.64. *Dados dois conjuntos X, Y, apenas um das 3 possibilidades ocorre:*

- *Existe uma injeção $f : X \to Y$ e não existe sobrejeção $g : X \to Y$.*
- *Existe bijeção $f : X \to Y$.*
- *Existe uma injeção $f : Y \to X$ e não existe sobrejeção $g : Y \to X$.*

Demonstração. Naive Set Theory. □

Definição 3.28. Definimos para conjuntos infinitos $\text{card}(X) = \text{card}(Y)$ se, e somente se, existir bijeção $f : X \to Y$. Definimos $\text{card}(X) < \text{card}(Y)$ se existir injeção $f : X \to Y$ e não existir sobrejeção $g : X \to Y$. E $\text{card}(X) > \text{card}(Y)$ caso contrário.

Proposição 3.65. ***(Cantor-Bernstein-Schröder Theorem)*** *Se existir injeções $f : X \to Y$ e $g : Y \to X$, então existe bijeção $h : X \to Y$.*

Demonstração. □

Proposição 3.66. *Seja $(X_\lambda)_{\lambda\in\mathbb{N}}$ uma família de conjuntos de tamanho maior ou igual a 2. Temos $Y = \prod_{\lambda\in\mathbb{N}} X_\lambda$ não é enumerável.*

Demonstração. Lembrando que cada elemento de Y é uma função $\phi : \mathbb{N} \to \bigcup_{\lambda\in\mathbb{N}} X_\lambda$, onde $\phi(n) \in X_n$. Suponha Y enumerável. Logo existe uma bijeção $f : \mathbb{N} \to Y$. Para simplificar a notação, denotaremos a função $f(n)$ por f_n. Como X_λ possui pelo menos 2 elementos, existem $a_\lambda, b_\lambda \in X_\lambda$ para todo $\lambda \in \mathbb{N}$. Seja $h : \mathbb{N} \to \bigcup_{\lambda\in\mathbb{N}} X_\lambda$, definida por

$$h(x) = \begin{cases} a_x, & f_x(x) \neq a_x \\ b_x, & f_x(x) = a_x \end{cases}.$$

Temos $h(n) \neq f_n(n)$ para todo $n \in \mathbb{N}$, logo $h \neq f_n$ para todo $n \in \mathbb{N}$. Como $h \in Y$ e $h \notin f(\mathbb{N})$, temos que f não é sobrejetiva. Logo f não é bijetiva (contradição). Logo Y não é enumerável. $\square$

3.6.3 Exercícios

Exercício 3.6.1. Se $X \subset \mathbb{N}$ é infinito, então existe uma única bijeção $\phi : \mathbb{N} \to \mathbb{X}$ estritamente crescente.

Demonstração. A existência é pela observação 3.11. Se $\phi, f : \mathbb{N} \to X$ são bijeções estritamente crescentes. Seja $Y = \{n \in \mathbb{N} | \phi(n) = f(n)\}$. Seja $p = f^{-1}(\min X)$, se $p \neq 1$, temos $f(p) \leq f(1)$ com $p > 1$. Logo $f(1) = \min X$. O argumento é análogo para $\phi(1) = \min X$. Logo $f(1) = \min X = \phi(1) \implies 1 \in X$. Suponha $n \in X$. Se $f(n+1) \neq \phi(n+1)$, temos $\phi(n+1) < f(n+1)$ ou $f(n+1) < \phi(n+1)$. Suponha sem perda de generalidade que $\phi(n+1) < f(n+1)$. Seja $p = f^{-1}(\phi(n+1))$. Se $p > n+1$, temos $f(p) < f(n+1)$ (contradição). Se $p < n+1$, temos $p \neq n$, pois $f(p) = \phi(n+1) > \phi(n) = f(n)$. Logo $p < n$ com $f(p) > f(n)$ (contradição). Logo não podemos ter $\phi(n+1) \neq f(n+1)$. Logo $n+1 \in Y$. Logo $\phi = f$. $\square$

4 Anéis

4.1 Definições iniciais

Definição 4.1 (Anel)**.** Seja A um conjunto e $+ : A \times A \to A$, $\cdot : A \times A \to A$ funções. Dizemos que $(A, +, \cdot)$ é um anel se :

1. $\forall x, y, z \in A \, : \, x + (y + z) = (x + y) + z$
2. $\forall x, y \in A \, : \, x + y = y + x$
3. Existe $0_A \in A$ tal que para todo $x \in A$,
$$x + 0_A = x$$
.
4. Para todo $x \in A$, existe $x' \in A$ tal que:
$$x + x' = 0_A$$
5. $\forall x, y, z \in A \, : \, x \cdot (y \cdot z) = (x \cdot y) \cdot z$.
6. $\forall x, y, z \in A \, :$
$$x \cdot (y + z) = x \cdot y + x \cdot z$$
$$(x + y) \cdot z = x \cdot z + y \cdot z$$

7. Existe um elemnto $1_A \in A$ tal que para todo $x \in A$:

$$x \cdot 1_A = 1_A \cdot x = x.$$

8. $\forall x, y \in A \, : \, x \cdot y = y \cdot x$.

Proposição 4.1. *Existe um único elemento $0_A \in A$ tal que $\forall x \in A : x + 0_A = x$.*

Demonstração. Suponha que existam $0_A, 0'_A \in A$ tal que $\forall x \in A : \begin{cases} x + 0_A = x \\ x + 0'_A = x \end{cases}$.
Como $0_A, 0'_A \in A$, temos $0'_A + 0_A = 0'_A$ e $0_A + 0'_A = 0_A$. Logo pela comutatividade da soma $0'_A = 0'_A + 0_A = 0_A + 0'_A = 0_A \iff 0_A = 0'_A$. Logo existe um único $0_A \in A$ tal que $\forall x \in A \, : \, x + 0_A = x$. □

Definição 4.2 (Elemento Neutro da Soma)**.** O único elemento $0_A \in A$ tal que $\forall x \in A \, : \, x + 0_A = x$ é chamado de elemento neutro da soma.

Proposição 4.2. *Para todo $x \in A$, existe um único $y \in A$ tal que $x + y = 0_A$.*

Demonstração. Suponha que existam $y, y' \in A$ tal que $x + y = x + y' = 0$. Logo $y = y + 0_A = y + (x + y') = y + (x + y') = (y + x) + y' = (x + y) + y' = 0_A + y' = y' + 0_A = y' \iff y = y'$.

Logo existe um único $y \in A$ tal que $x + y = 0_A$. □

Definição 4.3 (Simétrico)**.** Dado $x \in A$, chamamos o único elemento $y \in A$ tal que $x + y = 0_A$ de simétrico e escrevemos $y = -x$. Logo $x + (-x) = 0_A$.

Definição 4.4 (Subtração)**.** A operação "somar com inverso"é chamada subtração e escrevemos

$$x + (-y) = x - y$$

.

Proposição 4.3. *Existe um único elemento $1_A \in A$ tal que $\forall x \in A \; x \cdot 1_A = 1_A \cdot x = x$.*

Demonstração. Suponha que existam $1_A, 1'_A \in A$ tal que $\forall x \in A : \begin{cases} x \cdot 1_A = x \\ x \cdot 1'_A = x \end{cases}$.
Em particular, temos $\begin{cases} 1'_A \cdot 1_A = 1'_A \\ 1_A \cdot 1'_A = 1_A \end{cases} \implies 1'_A = 1'_A \cdot 1_A = 1_A \cdot 1'_A = 1_A$. Logo existe um único elemento $1_A \in A$ tal que $\forall x \in A \; x \cdot 1_A = 1_A \cdot x = x$. □

Definição 4.5 (Elemento Neutro do Produto)**.** O único elemento $1_A \in A$ tal que $\forall x \in A \; x \cdot 1_A = 1_A \cdot x = x$ é chamado de elemento neutro do produto.

Proposição 4.4. *Se A é um anel $x, y, z \in A$, então $x + z = y + z \implies x = y$.*

Demonstração. Supondo $x + z = y + z$, temos $y = y + 0_A = y + (z - z) = (y + z) - z = (x + z) - z = x + (z - z) = x + 0_A = x$. Logo $x + z = y + z \implies x = y$. □

Proposição 4.5. *Se A é um anel, então $\forall x \in A : x \cdot 0_A = 0_A$*

Demonstração. Temos $x \cdot 0_A = x \cdot (0_A + 0_A) = x \cdot 0_A + x \cdot 0_A \iff x \cdot 0_A + 0_A = x \cdot 0_A + x \cdot 0_A \implies x \cdot 0_A = 0_A$ pela proposição anterior. □

Proposição 4.6. *Seja A um anel. Para todos $x, y, z \in A$, temos:*

(a) $-(-x) = x$

(b) $-(xy) = (-x)y = x(-y)$

(c) $(-x)(-y) = xy$

(d) $(-1_A)x = -x$

Demonstração.

(a) Definimos $-y = z$ como o único elemento $z \in A$ tal que $y + z = 0_A$. Logo $(-x) + (-(-x)) = 0_A$ por definição. Mas $x + (-x) = 0_A$. Logo pela unicidade, temos $x = -(-x)$.

(b) Temos $(-x)y + xy = (-x + x)y = 0_A y = 0_A$ e $x(-y) + xy = x(-y + y) = x \cdot 0_A = 0_A$, que implica $(-x)y$ e $x(-y)$ inversos aditivos de xy. Da unicidade, temos $-(xy) = (-x)y = x(-y)$.

(c) Pelos itens anteriores, temos $(-x)(-y) = -(x \cdot (-y)) = -(-(xy)) = xy$.

(d) Do item (b), temos $(-1_A)x = -(1_A \cdot x) = -x$.

□

4.1.1 Exercícios

Exercício 4.1.1. Se A é um anel e $x, y, z \in A$, então $x + y = x \implies y = 0_A$.

Demonstração. Se $x + y = x$, temos $x + y = x = x + 0_A \implies y = 0_A$, pelo item anterior. □

4.2 Invertibilidade

Definição 4.6 (Invertível)**.** Um elemento $x \in A$ é invertível em A se existe $y \in A$ tal que

$$x \cdot y = 1_A.$$

Proposição 4.7. *Se $x \in A$ é invertível, então existe um único $y \in A$ tal que $x \cdot y = 1_A$.*

Demonstração. Dado $x \in A$ invertível, suponha que existam $y, y' \in A$ tal que $x \cdot y = x \cdot y' = 1_A$.

Logo $y' = 1_A \cdot y' = (x \cdot y) \cdot y' = x \cdot (y \cdot y') = x \cdot (y' \cdot y) = (x \cdot y') \cdot y = 1_A \cdot y = y \iff y' = y$.

Logo existe um único $y \in A$ tal que $x \cdot y = 1_A$. □

Definição 4.7 (Inverso multiplicativo)**.** Dado um anel A e $x \in A$ invertível, definimos x^{-1} como o único elemento de A tal que $x \cdot x^{-1} = 1_A$.

Definição 4.8 (Conjunto dos invertíveis)**.** Dado um anel A, o conjunto dos invertíveis em A é denotado por $A^\times$.

Definição 4.9 (Conjunto dos não-nulos)**.** Dado um anel A, o conjunto dos não-nulos em A é denotado por $A^* = A - \{0\}$.

Definição 4.10 (Anel Nulo)**.** Dizemos que um anel A é nulo se $A = \{0_A\}$.

4.3 Corpos, domínios e anéis reduzidos

Definição 4.11 (Divisor de Zero)**.** Dado A um anel, $x \in A$ é um divisor de zero em A se existe $y \in A - \{0\}$ tal que $xy = 0_A$.

Proposição 4.8. *Dado um anel não-nulo A, 0_A é um divisor de zero.*

Demonstração. Como A é não nulo, existe $y \in A - \{0\}$. Além disso, $0_A \cdot y = 0_A$. Logo 0_A é um divisor de zero. □

Definição 4.12 (Domínio)**.** Um anel não nulo A é um Domínio se $0_A \in A$ for o único divisor de zero.

Proposição 4.9. *Dado um anel A não nulo, as afirmações a seguir são equivalentes:*

(a) A *é um Domínio;*

(b) $\forall x, y \in A - \{0_A\} \, : \, xy \neq 0_A$

(c) $\forall x, y \in A \, : \, xy = 0_A \implies x = 0_A \vee y = 0_A$

Demonstração. (a) $\implies$ (b): Supondo A um domínio. Dados $x, y \in A$ com $x, y \neq 0_A$, se $xy = 0_A$, teríamos x, y divisores de zero em A. Logo teríamos divisores de zero em A diferentes de 0_A. Logo A não seria um domínio (contradição). Portanto devemos ter $xy \neq 0_A$.

(b) $\implies$ (c): Supondo $x, y \in A$ com $xy = 0_A$. Se $x, y \neq 0_A$, teríamos de (b) que $xy \neq 0_A$, logo devemos ter $x = 0_A$ ou $y = 0_A$.

(c) $\implies$ (a): Supondo x um divisor de zero em A, logo $xy = 0_A$ com $y \in A - \{0_A\}$. De (c), temos $xy = 0_A \implies x = 0_A \vee y = 0_A$. Como $y \neq 0_A$, devemos ter $x = 0_A$. Mostramos que qualquer divisor de zero em A é igual a 0_A. Logo A é um domínio.

□

Proposição 4.10. *Se A é um domínio, $n \in \mathbb{N}$ e $x_1, \cdots x_n \in A - \{0_A\}$, então $x_1 \cdot \cdots \cdot x_n \neq 0_A$.*

Demonstração. A prova será por indução. Para $n = 1$, é imediato. Para $n = 2$, segue da proposição anterior. Supondo válido para um $n \in \mathbb{N}$ qualquer. Supondo $x_1, \cdots x_n, x_{n+1} \in A - \{0_A\}$, então $x_1 \cdot x_2 \cdots x_n \cdot x_{n+1} = (x_1 \cdot x_2 \cdots x_n) \cdot x_{n+1}$. Pelo passo de indução, temos $y = x_1 \cdot x_2 \cdots x_n \neq 0_A$. Como $y \neq 0_A$ e $x_{n+1} \neq 0_A$, temos $y \cdot x_{n+1} \neq 0_A$ pelo caso $n = 2$. Logo vale para qualquer $n \in \mathbb{N}$. □

Proposição 4.11. *Se A é um domínio, $n \in \mathbb{N}$ e $x \in A - \{0_A\}$, então $x^n \neq 0_A$.*

Demonstração. Tomando $x \in A - \{0\}$ e $x^n = \underbrace{x \cdot x \cdot \cdots \cdot x}_{n \text{ vezes}}$ e usando a proposição anterior com $x_1 = x_2 = \cdots = x_n = x \neq 0$, temos $x^n \neq 0$. □

Proposição 4.12 (Lei do Corte)**.** *Seja A um domínio. Se $a, x, y \in A$ e $a \neq 0_A$, então*

$$ax = ay \implies x = y.$$

Demonstração. Supondo $a, x, y \in A$ com $a \neq 0_A$ e $ax = ay$. Temos $ax - ay = 0_A \iff a(x - y) = 0_A \implies a = 0_A \vee x - y = 0_A$. Como $a \neq 0_A$, temos $x - y = 0_A \implies x = y$. □

Definição 4.13 (Nilpotente)**.** Dado um anel A. Um elemento $x \in A$ é nilpotente se $x^n = 0_A$ para algum $n \in \mathbb{N}$.

Proposição 4.13. *Dado um anel A, $0_A \in A$ é nilpotente.*

Demonstração. Tems $0_A^1 = 0_A$, logo 0_A é nilpotente. □

Definição 4.14 (Anel Reduzido)**.** Um anel A é um Anel Reduzido se o único elemento nilpotente de A for 0_A.

Definição 4.15 (Corpo)**.** Um anel não nulo A é um corpo se $A^* = A^\times$, ou seja, todo elemento não nulo for invertível.

Proposição 4.14. *Se um anel A é um corpo, então é um domínio.*

Demonstração. Supondo A um corpo. Supondo $x, y \in A$ com $xy = 0_A$. Queremos mostrar que $x = 0_A$ ou $y = 0_A$. Se $y = 0_A$, não temos nada a demonstrar, supondo $y \neq 0_A$. Logo $y \in A^* = A^\times$ (A é um corpo). Logo $x = x \cdot 1_A = x \cdot (y \cdot y^{-1}) = (x \cdot y) \cdot y^{-1} = 0_A \cdot y^{-1} = 0_A$. Logo A é um domínio. □

Proposição 4.15. *Se um anel A é um domínio, então é um reduzido.*

Demonstração. Supondo A um domínio. Seja $x \in A$ nilpotente, ou seja, $x^n = 0_A$ com $n \in \mathbb{N}$. Se $x \neq 0$, temos pela proposição 4.11 que $x^n \neq 0$. Logo devemos ter $x = 0$. □

5 Aritmética

6 Análise Real

6.1 Números Reais

6.1.1 Corpos ordenados

Definição 6.1 (Corpo Ordenado)**.** Um corpo K é ordenado se existe um conjunto $P \subset K$ tal que :

1. Para todos $x, y \in P$, temos $x + y \in P$ e $x \cdot y \in P$.

2. Dado $x \in K$, apenas uma das possibilidades ocorre: ou $x \in P$, ou $x = 0_K$ ou $-x \in P$.

Definição 6.2 (Positivos)**.** Dado um corpo ordenado K, chamamos os elementos $x \in P$ de positivos.

Definição 6.3 (Negativos)**.** Dado um corpo ordenado K, chamamos os elementos $y = -x$ com $x \in P$ de negativos.

Definição 6.4 (Conjunto dos Negativos)**.** Dado um corpo ordenado K, denotamos por $-P = \{-x \mid x \in P\}$ como o conjunto dos elementos negativos.

Proposição 6.1. *Se K é um corpo ordenado, $K = (-P) \cup \{0_K\} \cup P$.*

Demonstração. Dado $x \in K$, pela definição, temos $x \in P$ ou $x = 0_K \iff x \in \{0_K\}$ ou $-x \in P \iff x \in -P$, logo $x \in (-P) \cup \{0_K\} \cup P$. Temos $P, \{0_K\}, -P \subset K$, logo $(-P) \cup \{0_K\} \cup P \subset K$. Portanto $(-P) \cup \{0_K\} \cup P = K$. □

Proposição 6.2. *Se K é um corpo ordenado, $(-P) \cap \{0_K\} \cap P = \emptyset$.*

Demonstração. Dado $x \in K$, pela definição, apenas um dos três ocorre: $x \in P$ ou $x = 0_K \iff x \in \{0_K\}$ ou $-x \in P \iff x \in -P$. Logo $(-P) \cap \{0_K\} \cap P = \emptyset$. □

Proposição 6.3. *Se K é um corpo ordenado, temos $\forall a \in K - \{0_K\} : a^2 \in P$.*

Demonstração. Dado $a \in K - \{0_K\}$, temos $-a \in P$ ou $a \in P$. Se $a \in P$, temos $a^2 = a \cdot a \in P$. Se $-a \in P$, temos $(-a) \cdot (-a) = a^2 \in P$. Em ambos os casos, temos $a^2 \in P$. □

Proposição 6.4. *Se K é um corpo ordenado, então $1_K \in P$.*

Demonstração. Temos $1_K = 1_K \cdot 1_K = 1_K^2 \implies 1_K \in P$, pela proposição anterior. □

Observação 6.1. Segue da proposição anterior que $-1_K \in -P$ para todo corpo ordenado K. Logo num corpo ordenado -1_K nunca é um quadrado.

Definição 6.5 ($<$)**.** Num corpo ordenado K com $x, y \in K$, definimos:

$$x < y \iff y - x \in P.$$

Definição 6.6 ($>$)**.** Num corpo ordenado K com $x, y \in K$, definimos:

$$y > x \iff x < y.$$

Proposição 6.5. *Dado um corpo ordenado K, temos para todos $x, y, z \in K$:*

1. $x < y \wedge y < z \implies x < z$
2. *Apenas uma das três possibilidades ocorre: $x < y$ ou $x = y$, ou $y < x$.*
3. $x < y \iff x \pm z < y + z$
4. *Se $z > 0$, temos $x < y \implies xz < yz$*
5. *Se $z < 0$, temos $x < y \implies xz > yz$*

Demonstração.

1. Se $x < y$ e $y < z$, temos $y - x \in P$ e $z - y \in P$, logo $(y - x) + (z - y) = z - x \in P$, que equivale a $x < z$.
2. Dado $x, y \in K$, tomando $w = x - y \in K$, temos $w \in P$, ou $w = 0$ ou $-w \in P$. Logo $x - y$ıP, ou $x - y = 0$ ou $-(x - y) = y - x \in P$. Portanto $y < x$, ou $x = y$¡ ou $x < y$.
3. Se $x < y$, temos $y - x \in P$. Logo $y - x = y + 0_K - x = y + (z - z) - x = (y + z) - (x + z) \in P \iff x + z < y + z$.
4. Se $z > 0$ e $x < y \iff y - x \in P$, temos que $yz - xz = (y - x) \cdot z \in P \iff xz < yz$.
5. Se $z < 0 \iff -z \in P$ e $x < y \iff y - x \in P$, temos que $xz - yz = (y - x) \cdot (-z) \in P \iff yz < xz$.

□

Proposição 6.6. *Dado um corpo ordenado K, temos para todos $x, y, z, w \in K$:*

$$x < y \wedge z < w \implies x + z < y + w$$

Demonstração. Temos $x < y \implies x + z < y + z$ e $z < w \implies y + z = z + y < w + y = y + w$, logo $x + z < y + w$. □

Proposição 6.7. *Dado um corpo ordenado K, temos para todos $x, y, z, w \in K$:*

$$0 < x < y \wedge 0 < z < w \implies 0 < xz < yw$$

Demonstração. Como $z > 0$ e $x < y$, temos $xz < yz$. Como $y > 0$ e $z < w$, temos $yz < yw$. Logo $xz < yw$. □

Definição 6.7 ($\leq$ e $\geq$)**.** Num corpo ordenado K com $x, y \in K$, definimos:

$$y \geq x \iff x \leq y \iff x < y \vee x = y$$

6.1.2 Números reais

Definição 6.8 (Cota Superior)**.** Seja K um corpo ordenado e $X \subset K$. Um elemento $s \in K$ é cota superior de X quando

$$\forall x \in X \ : \ x \leq s.$$

Definição 6.9 (Limitado superiormente)**.** Seja K um corpo ordenado e $X \subset K$. Dizemos que X é limitado superiormente se existe uma cota superior de X.

Definição 6.10 (Supremo)**.** Seja K um corpo ordenado e $X \subset K$. Um elemento $s \in K$ é o supremo de X quando:

1. s é cota superior de X.
2. Se $c \in K$ é cota superior de X, então $s \leq c$.

Observação 6.2*.* Uma forma mais humana de dizer a definição de supremo é: O supremo de um conjunto X é a menor cota superior deste conjunto.

Observação 6.3*.* Podemos tomar a contrapositiva na segunda condição e obter: Se $c < s$, então c não é cota superior. Mas não ser cota superior é o mesmo que existir um $x \in X$ com $c < x$. Logo obtemos uma definição equivalente:
Seja K um corpo ordenado e $X \subset K$. Um elemento $s \in K$ é o supremo de X quando:

1. s é cota superior de X.
2. Se $c \in K$ com $c < s$, então existe $x \in X$ com $c < x$.

Proposição 6.8. *Podemos trocar a segunda condição da definição de supremo do conjunto X por:*

$$\forall \varepsilon > 0 \, \exists x \in X \ : \ x > s - \varepsilon$$

Demonstração. Seja s o supremo de X pela definição usual. Dado $\varepsilon > 0$, sabemos que $s - \varepsilon < s$, logo existe $x \in X$ com $s - \varepsilon < x$ pela definição equivalente acima.

Supondo que s seja cota superior de X e $\forall \varepsilon > 0 \, \exists x \in X \ : \ x > s - \varepsilon$. Se c é uma cota superior de X com $c < s$, temos $s - c > 0$. Tomando $\varepsilon = s - c > 0$, existe $x \in X$ tal que $x > s - \varepsilon = s - (s - c) = c$, logo c não é cota superior (contradição). Logo se c é uma cota superior de X, temos $s \leq c$. Logo s é a menor cota superior. Logo s é um supremo de X. □

Observação 6.4*.* Vou usar a segunda condição que for mais conveniente na situação.

Proposição 6.9. *O supremo de um conjunto $X \subset K$, quando existir, é único.*

Demonstração. Suponha que $s_0, s_1 \in K$ sejam supremos do conjunto X. Temos que ambos são cotas superiores para X (condição 1). Da condição 2, obtemos $s_0 \leq s_1$ e $s_1 \leq s_0$, logo $s_0 = s_1$. □

Definição 6.11 (sup X)**.** Quando existir o supremo de um conjunto $X \subset K$, escreveremos sup X.

Definição 6.12 (Corpo Completo)**.** Um corpo ordernao K é completo se todo subconjunto não-vazio $X \subset K$, limitado superiormente, possui supremo em K.

Axioma 8. *Existe um corpo ordenado completo, denotado por* $\mathbb{R}$.

6.2 Sequências e Séries de Números Reais

6.2.1 Sequências

Definição 6.13 (Sequência)**.** Uma sequência é uma função $x : \mathbb{N} \to K$, onde K é um conjunto qualquer não-vazio. Nos importaremos aqui com $K = \mathbb{R}$.

Definição 6.14 (x_n)**.** Dada uma sequência $x : \mathbb{N} \to K$, Utilizaremos a notação $x_n \coloneqq x(n)$ para todo $n \in \mathbb{N}$. O termo x_n é chamado termo de ordem n, ou $n-$ésimo termo da sequência.

Definição 6.15 ((x_n))**.** Dada uma sequência $x : \mathbb{N} \to K$, será útil representar ela como $(x_1, x_2, \cdots)$ ou (x_n) ou $(x_n)_{n\in\mathbb{N}}$.

Definição 6.16 (Dois a dois Distintos)**.** Quando a sequência (x_n) é injetiva, isto é, $m \neq n \implies x_m \neq x_n$, dizemos que (x_n) é uma sequência de termos dois a dois distintos.

Definição 6.17 (Sequência Limitada Inferiormente)**.** A sequência (x_n) é limitada inferiormente quando $x(\mathbb{N})$ é limitado inferiormente. Ou seja: Existe $c \in \mathbb{R}$ $\forall n \in \mathbb{N} \,:\, x_n \geq c$.

Definição 6.18 (Sequência Limitada Superiormente)**.** A sequência (x_n) é limitada superiormente quando $x(\mathbb{N})$ é limitado superiormente. Ou seja: Existe $c \in \mathbb{R}$ $\forall n \in \mathbb{N} \,:\, x_n \leq c$.

Definição 6.19 (Sequência Limitada)**.** A sequência (x_n) é limitada quando é limitada superiormente e inferiormente. Ou seja: Existem $a, b \in \mathbb{R}$ tal que $\forall n \in \mathbb{N} \,:\, a \leq x_n \leq b$.

Proposição 6.10. *Uma sequência* (x_n) *é limitada se, e somente se, existe* $c \in \mathbb{R}$ *com* $c \geq 0$ *e* $\forall n \in \mathbb{N} : |x_n| \leq c$.

Demonstração. Se (x_n) é limitada, existem $a, b \in \mathbb{R}$ tal que $\forall n \in \mathbb{N} \,:\, a \leq x_n \leq b$. Tomando $c = \max\{|a|, |b|\}$. Temos $-c \leq -|a| \leq a$ e $b \leq |b| \leq c$, daí $\forall n \in \mathbb{N} - c \leq a \leq x_n \leq b \leq c$, que implica $\forall n \in \mathbb{N} \,:\, |x_n| \leq c$. Se $\forall n \in \mathbb{N} \,:\, |x_n| \leq c$, temos $\forall n \in \mathbb{N} \,:\, -c \leq x_N \leq c$. Daí tomamos $a = -c$ e $b = c$. $\square$

Proposição 6.11. (x_n) *é limitada, se e somente se,* $(|x_n|)$ *é limitada.*

Demonstração.

$$(x_n) \text{ é limitada } \iff \forall n \in \mathbb{N} : |x_n| \leq c \iff \forall n \in \mathbb{N} : ||x_n|| \leq c \iff (|x_n|) \text{ é limitada}$$

□

Definição 6.20 (Subsequência)**.** Dada uma sequência $x : \mathbb{N} \to \mathbb{R}$, uma subseqência é uma composição $x \circ \phi : \mathbb{N} \to \mathbb{R}$, onde $\phi : \mathbb{N} \to \mathbb{N}$ é uma função estritamente crescente. Denotaremos por $(x_{\phi(n)})$.

Proposição 6.12. *Uma sequência (x_n) é limitada se, e somente se, qualquer subsequência $(x_{\phi(n)})$ é limitada.*

Demonstração. Se (x_n) é limitada. Seja $(x_{\phi(n)})$ uma subsequência. Existe $c \in \mathbb{R}$ tal que $\forall n \in \mathbb{N} : |x_n| \leq c$. Daí $\phi(n) \in \mathbb{N} \implies |x_{\phi(n)}| \leq c$.

Se qualquer subsequência $(x_{\phi(n)})$ é limitada, tomando $\phi : \mathbb{N} \to \mathbb{N}$ com $\phi(n) = n$, temos $(x_n) = (x_{\phi(n)})$, logo (x_n) é limitada, pois $(x_{\phi(n)})$ é limitada. □

Definição 6.21 (Sequência estritamente crescente)**.** Uma sequência (x_n) é estritamente crescente se $\forall n \in \mathbb{N} : x_{n+1} > x_n$.

Definição 6.22 (Sequência crescente)**.** Uma sequência (x_n) é crescente se $\forall n \in \mathbb{N} : x_{n+1} \geq x_n$.

Proposição 6.13. *Uma sequência é estritamente crescente se, e somente se, $\forall m, n \in \mathbb{N} : m > n \implies x_m > x_n$.*

Demonstração. Supondo (x_n) crescente. Logo $\forall n \in \mathbb{N} : x_{n+1} > x_n$. Seja $X = \{p \in \mathbb{N} \,|\, \forall n \in \mathbb{N} : x_{n+p} > x_n\}$. Temos $1 \in X$, pois (x_n) é crescente. Supondo $m \in X$. Logo $\forall n \in \mathbb{N} : x_{n+m} > x_n$. Tomando $n \in \mathbb{N}$ qualquer, temos $x_{n+m+1} = x_{(n+m)+1} > x_{n+m} > x_n \implies x_{n+m+1} > x_n$. Logo $m + 1 \in X$. Logo $X = \mathbb{N}$. Se $m > n$, temos $m = n + p$, com $p \in \mathbb{N}$, logo $x_m = x_{n+p} > x_n$.

Supondo $\forall m, n \in \mathbb{N} : m > n \implies x_m > x_n$. Temos $\forall n \in \mathbb{N} : n + 1 > n \implies x_{n+1} > x_n$. Logo (x_n) é crescente. □

Definição 6.23 (Sequência estritamente decrescente)**.** Uma sequência (x_n) é estritamente decrescente se $\forall n \in \mathbb{N} : x_{n+1} < x_n$.

Definição 6.24 (Sequência decrescente)**.** Uma sequência (x_n) é decrescente se $\forall n \in \mathbb{N} : x_{n+1} \leq x_n$.

Proposição 6.14. *Uma sequência é estritamente decrescente se, e somente se, $\forall m, n \in \mathbb{N} : m > n \implies x_m < x_n$.*

Demonstração. Supondo (x_n) decrescente. Logo $\forall n \in \mathbb{N} : x_{n+1} < x_n$. Seja $X = \{p \in \mathbb{N} \,|\, \forall n \in \mathbb{N} : x_{n+p} < x_n\}$. Temos $1 \in X$, pois (x_n) é decrescente. Supondo $m \in X$. Logo $\forall n \in \mathbb{N} : x_{n+m} < x_n$. Tomando $n \in \mathbb{N}$ qualquer, temos $x_{n+m+1} = x_{(n+m)+1} < x_{n+m} < x_n \implies x_{n+m+1} < x_n$. Logo $m + 1 \in X$. Logo $X = \mathbb{N}$. Se $m > n$, temos $m = n + p$, com $p \in \mathbb{N}$, logo $x_m = x_{n+p} < x_n$.

Supondo $\forall m, n \in \mathbb{N} : m > n \implies x_m < x_n$. Temos $\forall n \in \mathbb{N} : n + 1 > n \implies x_{n+1} < x_n$. Logo (x_n) é decrescente. □

Definição 6.25 (Sequência monótoma)**.** Uma sequência (x_n) é monótoma se é crescente ou decrescente.

Proposição 6.15. *Uma sequência monótoma* (x_n) *é limitada superiormente ou inferiormente.*

Demonstração. Se (x_n) é monótoma, ela é crescente ou decrescente. Se (x_n) é crescente, temos $n \geq 1$ para todo $n \in \mathbb{N}$, logo $x_n \geq x_1$, logo x_n é limitada inferiormente. Se (x_n) é decrescente, temos $x_n \leq x_1$ para todo $n \in \mathbb{N}$. Logo (x_n) é limitada superiormente. $\square$

Proposição 6.16. *Uma sequência monótoma* (x_n) *é limitada se, e somente se, existe uma subsequência* $(x_{\phi(n)})$ *limitada.*

Demonstração. Se (x_n) é limitada, qualquer subsequência $(x_{\phi(n)})$ será limitada, em particular a subsequência $\phi : \mathbb{N} \to \mathbb{N}$ com $\phi(n) = n$ é limitada. Se existe uma subsequência $(x_{\phi(n)})$ limitada, temos $\forall n \in \mathbb{N} : |x_{\phi(n)}| \leq c$ para algum $c \in \mathbb{R}$. Se (x_n) é crescente, temos (x_n) limitada inferiormente por x_1. Dado $n \in \mathbb{N}$, temos $\phi(n) \geq n$, logo $x_1 \leq x_n \leq x_{\phi(n)} \leq c$. Logo (x_n) é limitada. Se (x_n) é decrescente, temos (x_n) limitada superiormente pode x_1 e de $\phi(n) \geq n$, obtemos $-c \leq x_{\phi(n)} \leq x_n \leq x_1$, logo (x_n) é limitada. $\square$

6.2.2 Limite de uma sequência

Definição 6.26 (Limite de Sequência)**.** Dizemos que $a \in \mathbb{R}$ é limite da sequência (x_n) se para cada $\varepsilon \in \mathbb{R}$ com $\varepsilon > 0$, existe $n_0 \in \mathbb{N}$ (que depende de ε) tal que $|x_n - a| < \varepsilon$ sempre que $n \in \mathbb{N}$ com $n > n_0$. Ou:

$$\forall \varepsilon > 0 \, \exists n_0 \in \mathbb{N} \, \forall n \in \mathbb{N} : n > n_0 \implies |x_n - a| < \varepsilon$$

Observação 6.5. Quando existir um limite da sequência (x_n), diremos que (x_n) converge ou é convergente. Além disso, se $a \in \mathbb{R}$ for limite de (x_n), diremos que (x_n) tende a a. Quando o limite não existir para nenhum $a \in \mathbb{R}$, diremos que a sequência é divergente.

Proposição 6.17. *O limite de uma sequência* (x_n)*, quando existir, é único.*

Demonstração. Suponha que a sequência (x_n) tenha como limites os números $a, b \in \mathbb{R}$ com $a \neq b$. Daí $|a - b| \neq 0 \implies |a - b| > 0$. Tomando $\varepsilon = |a - b|$,

$$\exists n_0 \in \mathbb{N} \, : \, \forall n \in \mathbb{N} \, n > n_0 \implies |x_n - a| < \frac{|a-b|}{2}$$

$$\exists n_1 \in \mathbb{N} \, : \, \forall n \in \mathbb{N} \, : \, n > n_1 \implies |x_n - b| < \frac{|a-b|}{2}$$

Tomando $n = \max\{n_0, n_1\} + 1$, temos $n_3 > n_0$ e $n_3 > n_1$, logo $|a - b| = |a + x_n - x_n - b| \leq |a - x_n| + |x_n - b| < \dfrac{|a-b|}{2} + \dfrac{|a-b|}{2} = |a - b| \implies |a - b| < |a - b|$. Contradição. $\square$

Definição 6.27 ($\lim x_n$)**.** Quando o limite da sequência (x_n) existir e for $a \in \mathbb{R}$, denotaremos por $a = \lim x_n$.

Proposição 6.18. *Temos* $\lim x_n = a$ *se, e somente se, para todo* $\varepsilon > 0$, *o conjunto* $\mathbb{N} - x^{-1}((a-\varepsilon, a+\varepsilon))$ *é finito.*

Demonstração. Se $\lim x_n = a$, dado $\varepsilon > 0$, existe $n_0 \in \mathbb{N}$ tal que $n > n_0 \implies |x_n - a| < \varepsilon \iff x_n \in (a-\varepsilon, a+\varepsilon) \iff n \in x^{-1}((a-\varepsilon, a+\varepsilon))$. Logo $n \in \mathbb{N} - x^{-1}((a-\varepsilon, a+\varepsilon)) \implies n \notin x^{-1}((a-\varepsilon, a+\varepsilon)) \implies n \leq n_0$. Como o conjunto $\mathbb{N} - x^{-1}((a-\varepsilon, a+\varepsilon))$ é limitado, temos que ele é finito. Se o conjunto $X = \mathbb{N} - x^{-1}((a-\varepsilon, a+\varepsilon))$ é finito para todo $\varepsilon > 0$, então é limitado. Logo existe um maior elemento $n_0 \in X$. Se $n > n_0$, temos $n \notin X$, logo $n \in x^{-1}((a-\varepsilon, a+\varepsilon)) \iff x_n \in (a-\varepsilon, a+\varepsilon) \iff |x_n - a| < \varepsilon$. Logo $\lim x_n = a$. □

Proposição 6.19. *Se* $\lim x_n = a$, *então toda subsequência de* (x_n) *converge para* a.

Demonstração. Seja $\lim x_n = a$ e $\phi : \mathbb{N} \to \mathbb{N}$ uma função crescente. Dado $\varepsilon > 0$, existe $n_0 \in \mathbb{N}$ tal que $n > n_0 \implies |x_n - a| < \varepsilon$. Temos $\phi(n) \geq n > n_0$, logo $|x_{\phi(n)} - a| < \varepsilon$. Logo $\lim x_{\phi(n)} = a$. □

Proposição 6.20. *Toda sequência convergente é limitada.*

Demonstração. Se (x_n) é convergente com $\lim x_n = a \in \mathbb{R}$. Existe $n_0 \in \mathbb{N}$ tal que $n > n_0 \implies |x_n - a| < 1$. Daí tomando $c = \max\{|x_1 - a|, |x_2 - a|, \cdots, |x_{n_0} - a|, 1\}$. Dado $n \in \mathbb{N}$, temos que ou $n > n_0$ ou $n \leq n_0$. Se $n > n_0$, temos $|x_n - a| < 1 \leq c \implies a - c \leq x_n \leq a + c$. Se $n \leq n_0$, temos $|x_n - a| \leq c \implies a - c \leq x_n \leq a + c$. Logo (x_n) é limitada. □

Teorema 7. *Toda sequência monótona limitada é convergente.*

Demonstração. Suponha (x_n) uma sequência monótoma limitada. Logo (x_n) é crescente ou decrescente. Supondo que (x_n) seja crescente. Temos de (x_n) ser limitada que $X = \{x_n \mid n \in \mathbb{N}\}$ é limitado e não vazio. Logo existe $s = \sup X$. Temos que $\forall \varepsilon > 0 \exists x \in X : x > s - \varepsilon$, logo existe $n_0 \in \mathbb{N}$ tal que $x_{n_0} > s - \varepsilon \iff x_{n_0} - s > -\varepsilon \iff s - x_{n_0} < \varepsilon$. Como (x_n) é crescente, temos $m > n_0 \implies x_m \geq x_{n_0} \iff s - x_m \leq s - x_{n_0} < \varepsilon$. Como s é cota superior, temos para todo $n \in \mathbb{N}$ que $s - x_n \geq 0 > -\varepsilon$. Logo existe $n_0 \in \mathbb{N}$ tal que $m > n_0 \implies -\varepsilon < s - x_m < \varepsilon \iff |s - x_m| < \varepsilon$, logo $\lim x_n = s$.

Se (x_n) é decrescente, tomando $X = \{x_n \mid n \in \mathbb{N}\}$, temos que $\forall \varepsilon > 0 \, \exists n_0 \in \mathbb{N} : x_{n_0} > \inf X + \varepsilon$. Temos $m > n_0 \implies x_m \leq x_{n_0} \iff x_m - \inf X \leq x_{n_0} - \inf X < \varepsilon$, logo $m > n_0 \implies -\varepsilon \leq 0 \leq x_m - \inf X < \varepsilon \iff |x_m - \inf X| < \varepsilon$. Logo $\lim(x_n) = \inf X$. □

6.2.3 Propriedades aritméticas dos limites

6.2.4 Subsequências

Proposição 6.21. *Seja (x_n) é uma sequência em $\mathbb{R}$. Temos que a é limite de alguma subsequência de (x_n) se, e somente se, $x^{-1}((a-\varepsilon, a+\varepsilon))$ é infinito para todo $\varepsilon > 0$.*

Proposição 6.22. *Toda sequência (x_n) possui uma subsequência monótoma.*

Demonstração. Dizemos que a sequência (x_n) é eventualmente crescente se existe uma subsequência $\phi : \mathbb{N} \to \mathbb{N}$ tal que $(x_{\phi(n)})$ é crescente. Se a sequência (x_n) for eventualmente crescente, temos que a sequência $(x_{\phi(n)})$ é uma subsequência monótoma. Supondo que a sequência (x_n) não é eventualmente crescente. Para todo $k \in \mathbb{N}$, a subsequência (x_{n+k}) não é crescente. Definindo $\phi : \mathbb{N} \to \mathbb{N}$, com $\phi(1) = 1$ e, supondo $\phi(n)$ definida, temos que a sequência $(x_{n+\phi(n)})$ não é crescente, logo existe $p, q \in \mathbb{N}$ tal que $n + p > n + q$ e $x_{n+p} < x_{n+q}$ □

6.2.5 Sequências de Cauchy

6.2.6 Limites infinitos

6.2.7 Séries numéricas

6.3 Topologia da Reta

6.3.1 Conjuntos abertos

6.3.2 Conjuntos fechados

6.3.3 Pontos de acumulação

6.3.4 Conjuntos compactos

6.4 Limites de Funções

6.4.1 Definição e propriedades do limite

6.4.2 Exemplos de limites

6.4.3 Limites laterais

6.4.4 Limites no infinito

6.4.5 Valores de aderência de uma função; lim sup e lim inf

6.5 Funções Contínuas

6.5.1 A noção de função contínua

6.5.2 Descontinuidades

6.5.3 Funções contínuas em intervalos

6.5.4 Funções contínuas em conjuntos compactos

6.5.5 Continuidade uniforme

6.6 Derivadas

6.6.1 Definição e propriedades da derivada num ponto

6.6.2 Funções deriváveis num intervalo

6.6.3 Fórmula de Taylor

6.6.4 Série de Taylor, funções analíticas

6.7 Integral de Riemann

6.7.1 Integral superior e integral inferior

6.7.2 Funções integráveis

6.7.3 O Teorema Fundamental do Cálculo

6.7.4 Fórmulas clássicas do Cálculo Integral

6.7.5 A integral como limite de somas

6.7.6 Caracterização das funções integráveis

6.7.7 Logaritmos e exponenciais

6.8 Sequências e Séries de Funções

6.8.1 Convergência simples e convergência uniforme

6.8.2 Propriedades da convergência uniforme

Demonstração. Como A, B são limitados, então existe $\sup A$ e $\sup B$. Dado $(a, b) \in A \times B$, temos $0 \leq a \leq \sup A$ e $0 \leq b \leq \sup B$, logo $0 \leq ab \leq \sup A \cdot \sup B$, logo $\sup A \sup B$ é uma cota superior para $C = \{ab | (a, b) \in A \times B\}$. Portanto C é limitado. Além disso $\sup C \leq \sup A \cdot \sup B$.

Seja $(x_n)_{n \in \mathbb{N}}$ uma sequência em A com $\lim x_n = \sup A$ e $(y_n)_{n \in \mathbb{N}}$ uma sequência em B com $\lim y_n = \sup B$, temos $(x_n \cdot y_n)_{n \in \mathbb{N}}$ uma sequência em C com $\lim x_n \cdot y_n = \sup A \sup B$. Logo $\sup A \cdot \sup B \leq \sup C$.

Como $\sup A \sup B \leq \sup C$ e $\sup C \leq \sup A \sup B$, temos $\sup C = \sup A \sup B$. $\square$

Proposição 6.24. *Sejam $A, B \subset \mathbb{R}^+ - \{0\}$ limitados, então $C = \{ab \mid (a, b) \in A \times B\}$ é limitado e $\sup C = \sup A \times \sup B$.*

Demonstração. Exercício. $\square$

7 Geometria Analítica

8 Álgebra Linear

8.1 Posto

Proposição 8.1. *Seja A uma matriz $m \times n$.*

$$\operatorname{rank} A = \operatorname{rank} AA^T = \operatorname{rank} A^T A$$

Demonstração. Se $x \in \text{Null}(A)$, temos $Ax = 0 \implies A^T(Ax) = A^T \cdot 0 \implies (A^T A)x = 0 \implies x \in \text{Null}(A^T A)$. Se $x \in \text{Null}(A^T A)$, temos $(A^T A)x = 0 \implies x^T(A^T A)x = 0 \implies (x^T A^T)(Ax) = 0 \implies (Ax)^T(Ax) = 0 \implies Ax = 0 \implies x \in \text{Null}(A)$. Logo $\text{Null}(A) = \text{Null}(A^T A)$. Pelo Teorema do posto e da unidade, temos que $\operatorname{rank} A + \text{Null}\, A = m$ e que $\operatorname{rank} A^T A + \text{Null}\, A =$ $\square$

9 Análise no $\mathbb{R}^n$

9.1 Topologia do Espaço Euclidiano

9.1.1 O espaço vetorial $\mathbb{R}^n$

9.1.2 Métrica, Produto interno e norma

Definição 9.1 (Métrica)**.** Dado um espaço vetorial E sobre um corpo K, uma métrica é uma função $d : E \times E \to \mathbb{R}$, que satisfaz para todos $a, b \in E$ e $\lambda \in K$:

1. $d(a, b) \geq 0$
2. $d(a, b) = 0 \iff a = b$
3. $d(a, b) = d(b, a)$

4. $d(a,b) \leq d(a,c) + d(c,b)$

Definição 9.2 (Norma)**.** Dado um espaço vetorial E sobre um corpo K, uma norma é uma função $\|\cdot\| : E \to \mathbb{R}$, que satisfaz para todos $x, y \in E$ e $\lambda \in K$:

1. $\|x\| = 0 \implies x = 0$
2. $\|\lambda x\| = |\lambda| \cdot \|x\|$
3. $\|x + y\| \leq \|x\| + \|y\|$

Proposição 9.1. *Dada uma norma $\|\cdot\| : E \to \mathbb{R}$, temos:*

$$\|x\| = 0 \iff x = 0$$

Demonstração. Temos $\|x\| = 0 \implies x = 0$ por definição. Basta mostrar que $\|\vec{0}\| = 0$ Temos $\|\vec{0}\| = \|0 \cdot \vec{0}\| = |0| \cdot \|\vec{0}\| = 0 \cdot \|\vec{0}\| = 0$. □

Proposição 9.2. *Dada uma norma $\|\cdot\| : E \to \mathbb{R}$, temos para todo $x \in E$:*

$$\|x\| \geq 0$$

Demonstração. Temos para todo $x, y \in E$ que $\|x + y\| \leq \|x\| + \|y\|$. Tomando $y = -x$, temos $\|x - x\| \leq \|x\| + \|-x\| \iff \|0\| \leq \|x\| + |-1| \cdot \|x\| \iff 0 \leq \|x\| + \|x\| \iff 2\|x\| \geq 0 \iff \|x\| \geq 0$. □

Proposição 9.3. *Dada uma norma $\|\cdot\| : E \to \mathbb{R}$, a função $d : E \times E \to \mathbb{R}$, $d(a,b) = \|a - b\|$ é uma métrica.*

Demonstração. Para todo $a, b, c \in E$, temos:

- $d(a,b) = |a - b| \geq 0$.
- $d(a,b) = 0 \iff |a - b| = 0 \iff a - b = 0 \iff a = b$.
- $d(a,b) = |a - b| = |b - a| = d(b,a)$
- $d(a,b) = |a - b| = |a - c + c - b| \leq |a - c| + |c - b| = d(a,c) + d(c,b)$.

□

Definição 9.3 (Métrica proveniente da norma)**.** Dada uma norma $\|\cdot\| : E \to \mathbb{R}$, a função $d : E \times E \to \mathbb{R}$, $d(a,b) = \|a - b\|$ é chamada de métrica proveniente da norma.

Proposição 9.4. *Num espaço vetorial E, uma métrica d é proveniente de uma norma, se e somente se, para quaisquer $x, y, a \in E$ e $\lambda \in K$, tem-se $d(x+a, y+a) = d(x,y)$ e $d(\lambda \cdot x, \lambda \cdot y) = |\lambda| \cdot d(x,y)$.*

Demonstração. Se d provém de uma métrica, para $x, y, a \in E$ e $\lambda \in K$, temos $d(x+a, y+a) = \|(x+a)-(y+a)\| = \|x-y\| = d(x,y)$ e $d(\lambda \cdot x, \lambda \cdot y) = \|\lambda \cdot x - \lambda \cdot y\| = \|\lambda \cdot (x-y)\| = |\lambda| \cdot \|x-y\| = |\lambda| \cdot d(x,y)$.

Supondo d uma métrica qualquer com $d(x+a, y+a) = d(x,y)$ e $d(\lambda \cdot x, \lambda \cdot y) = |\lambda| \cdot d(x,y)$. Definindo $\|\cdot\| : E \to \mathbb{R}$, com $\|x\| = d(x,0)$. De fato, $\|\cdot\|$ é uma norma, pois:

1. $\|x\| = 0 \iff d(x,0) = 0 \iff x = 0$.
2. $\|\lambda \cdot x\| = d(\lambda \cdot x, 0) = d(\lambda \cdot x, \lambda \cdot 0) = |\lambda| \cdot d(x,0) = |\lambda| \cdot \|x\|$.
3. $\|x+y\| = d(x+y, 0) \leq d(x+y, y) + d(y,0) = d(x,0) + d(y,0) = \|x\| + \|y\| \implies \|x+y\| \leq \|x\| + \|y\|$.

Logo $\|\cdot\|$ é uma norma que induz d. □

Proposição 9.5.

$$|\|x\| - \|y\|| \leq \|x-y\|$$

Demonstração. Temos $\|x\| = \|x-y+y\| \leq \|x-y\| + \|y\| \implies \|x\| - \|y\| \leq \|x-y\|$. Além disso $\|y\| \leq \|y-x\| + \|x\| = \|x-y\| + \|x\| \implies \|y\| - \|x\| \leq \|x-y\| \implies -\|x-y\| \leq \|x\| - \|y\|$.

Como $-\|x-y\| \leq \|x\| - \|y\| \leq \|x-y\|$, temos $|\|x\| - \|y\|| \leq \|x\| - \|y\|$.

□

Definição 9.4 (Normas equivalentes)**.** Duas normas $\|\cdot\|_1, \|\cdot\|_2 : E \to \mathbb{R}$ são equivalentes se existirem $C_1, C_2 > 0$ tal que

$$C_1 \cdot \|x\|_1 \leq \|x\|_2 \leq C_2 \cdot \|x\|_1$$

Proposição 9.6. *Se um espaço normado E tiver dimensão finita, então todas as suas normas são equivalentes.*

9.1.3 Números complexos

9.1.4 Bolas e conjuntos limitados

9.1.5 Sequências no espaço euclidiano

9.1.6 Pontos de acumulação

9.1.7 Aplicações contínuas

9.1.8 Homeomorfismos

9.1.9 Limites

9.1.10 Conjuntos abertos

9.1.11 Conjuntos fechados

9.1.12 Conjuntos compactos

Definição 9.5 (Conjunto Compacto)**.** Um conjunto $X \subset \mathbb{R}^n$ é compacto $\iff$ é fechado e limitado.

Proposição 9.7. *Um conjunto $X \subset \mathbb{R}^n$ é compacto $\iff$ toda sequência (x_n) em X possui uma subsequência convergente com limite em X.*

Demonstração. Supondo $X \subset \mathbb{R}^n$ compacto. Seja (x_n) uma sequência em X. Como X é limitado, (x_n) admite uma subsequência $(x_{\phi(n)})$ convergente. Como X é fechado, temos que $\lim x_{\phi(x)} = x \in X$.

Tomando a contrapositiva, suponha que X não seja compacto. Logo X não é fechado ou não é limitado. Se X não é fechado, existe um $x \in \overline{X} \backslash X$. Logo existe uma sequência $(x_n) \in X$ com $\lim x_n = x$. Qualquer subequência $\phi : \mathbb{N} \to \mathbb{N}$ de (x_n) terá $\lim x_{\phi(n)} = x$. Logo existe uma sequência (x_n) tal que nenhuma subsequência $(x_{\phi(n)})$ tenha limite $x \in X$. Suponha que X não seja limitado, logo para todo ε, existe $x \in X$ tal que $|x| > \varepsilon$. Daí tomando $x_n \in X$ tal que $|x_n| > n$, temos que a sequência não admite valores de aderência. Logo não existe subsequência convergente.

□

Definição 9.7 ($L(\mathbb{R}^n)$)**.**

$$L(\mathbb{R}^n) = L(\mathbb{R}^n, \mathbb{R}^n)$$

Definição 9.8 ($GL(\mathbb{R}^n)$)**.**

$$GL(\mathbb{R}^n) = \{T \in L(\mathbb{R}^n) \mid T \text{ é bijetiva}\}$$

Proposição 9.8. *$GL(\mathbb{R}^n)$ é aberto.*

Demonstração. Seja $T \in GL(\mathbb{R}^n$. Logo T é invertível (bijetiva). □

Proposição 9.9. *$f : GL(\mathbb{R}^n) \to GL(\mathbb{R}^n)$, dada for $f(T) = T^{-1}$ é contínua.*

Demonstração. □

9.9 Diferenciação

Proposição 9.10. *Seja $f : GL(\mathbb{R}^n) \to GL(\mathbb{R}^n)$, dada por $f(T) = T^{-1}$. Temos f diferenciável.*

Demonstração. Temos

$$(T+H)(T+H)^{-1} = I \iff$$

$$T(T+H)^{-1} + H(T+H)^{-1} = I \iff$$

$$T(T+H)^{-1} = I - H(T+H)^{-1} \iff$$

$$(T+H)^{-1} = T^{-1}(I - H(T+H)^{-1}) \iff$$

Vou substituir $(T+H)^{-1}$ na equação acima.

$$\begin{aligned}
(T+H)^{-1} &= T^{-1}(I - H(T+H)^{-1}) \\
&= T^{-1}(I - H\left[T^{-1}(I - H(T+H)^{-1})\right]) \\
&= T^{-1}(I - HT^{-1}(I - H(T+H)^{-1})) \\
&= T^{-1}(I - HT^{-1} + HT^{-1}H(T+H)^{-1}) \\
&= T^{-1} - T^{-1}HT^{-1} + T^{-1}HT^{-1}H(T+H)^{-1}
\end{aligned}$$

Se chamarmos $S_T(H) = -T^{-1}HT^{-1}$, temos

$$\begin{aligned} f(T+H) &= (T+H)^{-1} \\ &= T^{-1} - T^{-1}HT^{-1} + T^{-1}HT^{-1}H(T+H)^{-1} \\ &= f(T) + S_T(H) + T^{-1}HT^{-1}H(T+H)^{-1} \end{aligned}$$

Afirmo que $S_T(H) = Df(T)(H)$. De fato, S_T é linear (confia) e temos

$$\begin{aligned} \lim_{H\to 0} \frac{|f(T+H) - f(T) - S_T(H)|}{|H|} &= \lim_{H\to 0} \frac{|+T^{-1}HT^{-1}H(T+H)^{-1}|}{|H|} \\ &\leq \lim_{H\to 0} \frac{|T^{-1}| \cdot |H| \cdot |T^{-1}| \cdot |H| \cdot |(T+H)^{-1}|}{|H|} \\ &= \|T^{-1}\|^2 \cdot \lim_{H\to 0} |H| \cdot |(T+H)^{-1}| \\ &= 0 \end{aligned}$$

□

9.10 Integração

Definição 9.9 (Retângulo)**.** Um retângulo ou bloco é um produto cartesiano $A = \prod_{i=1}^{m} [a_i, b_i] \subset \mathbb{R}^m$, com $a_i < b_i$ para $i \in \{1, 2, \cdots, m\}$.

Definição 9.10 (Partição do intervalo)**.** Uma partição de um intervalo $[a, b] \subset \mathbb{R}$ é uma sequência $t_1, t_2, \cdots, t_k$ com $a = t_1 \leq t_2 \leq \cdots \leq t_k = b$.

Definição 9.11 (Partição de um retângulo)**.** Uma partição de um retângulo $A \subset \mathbb{R}^m$ é uma coleção $P = (P_1, P_2, \cdots P_m)$, onde P_i é uma partição do intervalo $[a_i, b_i]$ para todo $i \in \{1, 2, \cdots, m\}$.

Definição 9.12 (Subretângulo de uma Partição)**.** Dada uma partição $P = (P_1, P_2, \cdots P_m)$ do retângulo $A \subset \mathbb{R}^n$, um subretângulo S de P é um retângulo da forma $S = \prod_{j=1}^{m} I_j$, onde I_j é um intervalo da partição P_j.

Definição 9.13 (Refinamento de uma partição)**.** Dada uma partição P de um retângulo A, dizemos que Q é um refinamento de P se todo subretângulo de Q está contido em um subretângulo de P.

Definição 9.14 (Medida Nula). Um conjunto $A \subset \mathbb{R}^n$ tem medida nula se para todo $\varepsilon > 0$, existe uma cobertura enumerável $\{U_i\}_{i \in L}$ de A por retângulos fechados tal que $\displaystyle\sum_{i=1}^{\infty} v\left(U_i\right) < \varepsilon$.

Definição 9.15 (Conteúdo Nulo). Um conjunto $A \subset \mathbb{R}^n$ tem conteúdo nulo se para todo $\varepsilon > 0$, existe uma cobertura finita $\{U_i\}_{i \in L}$ de A por retângulos fechados tal que $\displaystyle\sum_{i=1}^{\infty} v\left(U_i\right) < \varepsilon$.

Proposição 9.11. *Se A tem conteúdo nulo, então A tem medida nula.*

Demonstração. Se A tem conteúdo nulo, então dado ε, existe uma cobertura finita $\{U_i\}_{i \in L}$ de A tal que $\displaystyle\sum_{i=1}^{\infty} v\left(U_i\right) < \varepsilon$. Como todo conjunto finito é enumerável, temos $\{U_i\}_{i \in L}$ enumerável, logo A tem medida nula. □

Proposição 9.12. *Uma união enumerável de conjuntos com medida nula tem medida nula.*

Demonstração. □

Proposição 9.13. *Se A é compacto e tem medida nula, então A tem conteúdo nulo.*

Demonstração. □

9.10.1 Exercícios

Exercício 9.10.1. Sejam $f : A \to \mathbb{R}$, $g : B \to \mathbb{R}$ funções limitadas não-negativas nos blocos A, B. Defina $\phi : A \times B \to \mathbb{R}$ pondo $\phi(x, y) = f(x) \cdot g(y)$. Prove que

$$\overline{\int_{A \times B}} \phi(z) \underset{\cdot}{d} z = \overline{\int_A} f(x) \underset{\cdot}{d} x \cdot \overline{\int_B} g(y) \underset{\cdot}{d} y$$

e que vale um resultado análogo para integrais inferiores.

Demonstração. Temos $\displaystyle\overline{\int_{A \times B}} \phi(z) \underset{\cdot}{d} z = \inf_Q \{U(\phi; Q)\}$. Seja $Q = (P, P')$ uma partição de $A \times B$. Temos P partição de A e P' partição de B. Seja $S_b = S \times S'$ um subretângulo de Q, temos S subretângulo de P e S' subretângulo de P'. Temos $\forall x \in S \ : \ 0 \leq f(x) \leq M_S(f)$ e $\forall y \in S' \ : \ 0 \leq g(y) \leq M_{S'}(g)$, logo $\forall (x, y) \in S \times S' = S_b : 0 \leq f(x) \cdot g(y) \leq M_S(f) \cdot M_{S'}(g)$. Logo $M_s(f) \cdot M_{S'}(g)$ é cota superior para $f(x) \cdot g(y)$ em $S \times S'$, logo $\sup \{f(x) \cdot g(y) \mid (x, y) \in S \times S'\} = M_{S \times S'}(\phi) \leq M_S(f) \cdot M_{S'}(g)$.

Se $M_S(f) = 0$, temos $0 \leq f(x) \leq M_S(f) \leq 0 \implies f(x) = 0$ para todo $x \in S$, logo $\forall (x, y) \in (S \times S') : f(x) \times g(y) = 0 \cdot g(y) = 0$, logo $M_{S \times S'}(\phi) = 0$. É análogo se $M_{S'}(g) = 0$.

Supondo $M_S(f) \neq 0$ e $M_{S'}(g) \neq 0$. Dado $\varepsilon > 0$, existe $x_1 \in S$ tal que $f(x_1) > M_S(f) - \dfrac{\varepsilon}{2 \cdot M_{S'}(g)}$ e existe $y_1 \in S'$ tal que $g(y_1) > M'_S(g) - \dfrac{\varepsilon}{2 \cdot M_S(f)}$. Logo existe $(x_1, x_2) \in S \times S'$ tal qu $f(x_1) \cdot f(x_2) > \left(M_S(f) - \dfrac{\varepsilon}{2 \cdot M_{S'}(g)}\right) \cdot \left(M_{S'}(g) - \dfrac{\varepsilon}{2 \cdot M_S(f)}\right) = M_S(f) \cdot M_{S'}(g) - \dfrac{\varepsilon}{2} - \dfrac{\varepsilon}{2} + \dfrac{\varepsilon^2}{2M_S(f) \cdot M_{S'}(g)} > M_S(f) \cdot M_{S'}(g) - \varepsilon$. Como dado $\varepsilon > 0$, existem $(x_1, y_1) \in S \times S'$ tal que $f(x_1) \cdot g(y_1) < M_S(f) \cdot M_{S'}(g) - \varepsilon$ e $M_S(f) \cdot M_{S'}(g)$ é cota superior para $\{f(x) \cdot g(y) | (x, y) \in S \times S'\}$, temos $M_{S \times S'}(\phi) = M_S(f) \times M_S(g)$.

Logo

$$\begin{aligned}
U(\phi, Q) &= \sum_{S \times S' \in (P, P')} M_{S \times S'}(\phi) \cdot V(S \times S') \\
&= \sum_{S \times S' \in (P, P')} M_S(f) \cdot M_{S'}(g) \cdot V(S) \cdot V(S') \\
&= \sum_{\substack{S \in P, \\ S' \in P'}} [M_S(f) \cdot V(S)] \cdot [M_{S'}(g) \cdot V(S')] \\
&= \sum_{S \in P} \sum_{S' \in P'} [M_S(f) \cdot V(S)] \cdot [M_{S'}(g) \cdot V(S')] \\
&= \sum_{S \in P} [M_S(f) \cdot V(S)] \cdot \sum_{S' \in P'} [M_{S'}(g) \cdot V(S')] \\
&= \left[\sum_{S' \in P'} M_{S'}(g) \cdot V(S')\right] \cdot \left[\sum_{S \in P} M_S(f) \cdot V(S)\right] \\
&= U(f, P) \cdot U(g, P')
\end{aligned}$$

Logo $\overline{\int_{A \times B}} \phi(z) \text{d̩}z = \inf_Q \{U(\phi; Q)\} = \inf_{(P,P')} \{U(f, P) \cdot U(g, P')\} = \inf_P \{U(f, P)\} \cdot \inf_{P'} \{U(g, P')\} = \overline{\int_A} f(x) \text{d̩}x \cdot \overline{\int_B} g(y) \text{d̩}y$

□

Exercício 9.10.2. Se $X \subset \mathbb{R}^m$ tem medida nula, então para todo $Y \subset \mathbb{R}^m$, o produto cartesiano $X \times Y \subset \mathbb{R}^{m+n}$ tem medida nula.

Demonstração. Basta provar que se $X \subset \mathbb{R}^n$ tem medida nula, então $X \times \mathbb{R}^m$ tem medida nula. Pois uma cobertura do conjunto $X \times \mathbb{R}^m$ cobre o conjunto $X \times Y \subset X \times \mathbb{R}^m$.

Chamando $C_p = \prod_{i=1}^{m} [-p,p] = \underbrace{[-p,p] \times [-p,p] \times \cdots \times [-p,p]}_{m \text{ vezes}} \subset \mathbb{R}^m$. Temos $\mathbb{R}^m = \bigcup_{p \in \mathbb{N}} C_p$, logo $X \times \mathbb{R}^m = X \times \bigcup_{p \in \mathbb{N}} C_p = \bigcup_{p \in \mathbb{N}} X \times C_p$. Como é uma união enumerável de conjuntos, basta mostrar que $X \times C_p$ tem medida nula para todo $p \in \mathbb{N}$.

Fixando $p \in \mathbb{N}$, temos $v\left(C_p\right) = (2p)^m$. Dado $\varepsilon > 0$, existe uma cobertura enumerável $\{U_i\}_{i \in L}$ de retângulos fechados tal que $\sum_{i \in L} v\left(U_i\right) < \frac{\varepsilon}{(2p)^m}$. Temos $X \times C_p \subset \left(\bigcup_{i \in L} U_i\right) \times C_p = \bigcup_{i \in L} U_i \times C_p$. Como C_p e U_i são retângulos, temos $v\left(U_i \times C_p\right) = v\left(U_i\right) \cdot v\left(C_p\right)$. Logo temos $\sum_{i \in L} v\left(U_i \times C_p\right) = \sum_{i \in L} v\left(U_i\right) \cdot v\left(C_p\right) = \sum_{i \in L} v\left(U_i\right) \cdot (2p)^m = (2p)^m \cdot \sum_{i \in L} v\left(U_i\right) < (2p)^m \cdot \frac{\varepsilon}{(2p)^m} = \varepsilon$. Logo $X \times C_p$ tem medida zero para todo $p \in \mathbb{N}$.

Como $X \times \mathbb{R}^n = \bigcup_{p \in \mathbb{N}} X \times C_p$ é uma união enumerável de conjuntos de medida nula, temos que $X \times \mathbb{R}^n$ tem medida nula.

□

10 Geometria diferencial

10.1 Superfícies Regulares

Definição 10.1 (Superfície)**.** Um subconjunto $S \subset \mathbb{R}^n$ é uma superfície de dimensão m quando, para todo $x \in S$, existe $A \subset S$ aberto em S contendo x, A_0 aberto em $\mathbb{R}^m$ e um homeomorfismo $\phi : A_0 \to A$.

Observação 10.1. Observe que A é aberto em S se, e somente se, existe um aberto $V \subset \mathbb{R}^n$ tal que $A = V \cap S$.

Observação 10.2. Aqui estamos preocupados quando $n = 3$ e $m = 2$.

Definição 10.2 (Superfície regular)**.** Um conjunto $S \subset \mathbb{R}^3$ é uma superfície regular se, para todo $p \in S$, existe um aberto $V \subset \mathbb{R}^3$ com $p \in V$ e uma aplicação $x : U \to V \cap S$ tal que:

1. x é diferenciável;
2. x é um homeomorfismo.
3. x é uma imersão.

Proposição 10.1. *Se $f : U \to \mathbb{R}$ é uma função diferenciável em um conjunto aberto $U \subset \mathbb{R}^2$, então o gráfico de f é uma superfície regular.*

Demonstração. Seja $S = \text{Graf}(f) = \{(x, y, z) \in \mathbb{R}^3 | (x, y) \in U \wedge z = f(x, y)\}$. Tomando $\phi : U \to S \cap \mathbb{R}^3 = S$ com $\phi(x, y) = (x, y, f(x, y))$. Temos ϕ diferenciável com $(\phi)^{-1} = \pi_{|S}$, logo é um homeomorfismo. Além disso, $D\phi(x, y) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ f_1(x,y) & f_2(x,y) \end{bmatrix}$ com $\text{rank}(D\phi(x, y)) = 2$ para todo $(x, y) \in U$, logo é uma imersão. □

Definição 10.3. Dada uma aplicação diferenciável $F : U \subset \mathbb{R}^n \to \mathbb{R}^m$ definida em um aberto U, dizemos que $p \in U$ é um ponto crítico de F se $\text{rank}(DF(p)) < m$. A imagem $F(p) \in \mathbb{R}^m$ de um ponto crítico é chamado um valor crítico de F. Um ponto de $\mathbb{R}^m$ que não é valor crítico é chamado um valor regular de F.